creative commons
COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

조선대학교
CHOSUN UNIVERSITY

February 2022

PhD Dissertation

Enhancing the Performance of Routing Protocols for Location Privacy Protection in Event Monitoring Wireless Networks

Graduate School of Chosun University

Department of Computer Engineering

Lilian Charles Mutalemwa

조선대학교
CHOSUN UNIVERSITY

Enhancing the Performance of Routing Protocols for Location Privacy Protection in Event Monitoring Wireless Networks

이벤트 모니터링 무선 네트워크에서 위치 정보 보호를 위한 라우팅 프로토콜의 성능 개선

February 25, 2022

Graduate School of Chosun University

Department of Computer Engineering

Lilian Charles Mutalemwa

조선대학교
CHOSUN UNIVERSITY

Enhancing the Performance of Routing Protocols for Location Privacy Protection in Event Monitoring Wireless Networks

Advisor: Prof. Seokjoo Shin

A dissertation submitted in partial fulfillment of the requirements for the Degree of Doctor of Philosophy

October 2021

Graduate School of Chosun University

Department of Computer Engineering

Lilian Charles Mutalemwa

조선대학교
CHOSUN UNIVERSITY

Lilian Charles Mutalemwa 의
박사학위논문을 인준함

위원장	조선대학교	교 수	모상만(인)
위 원	조선대학교	교 수	강문수(인)
위 원	조선대학교	교 수	최우열(인)
위 원	ETRI	책임연구원	이현우(인)
위 원	조선대학교	교 수	신석주(인)

2022 년 1 월

조선대학교 대학원

조선대학교
CHOSUN UNIVERSITY

DEDICATION

To my daughter, Evelyn…

You are the best.

조선대학교
CHOSUN UNIVERSITY

TABLE OF CONTENTS

조선대학교
CHOSUN UNIVERSITY

조선대학교
CHOSUN UNIVERSITY

조선대학교
CHOSUN UNIVERSITY

ABBREVIATIONS

WSN	Wireless sensor network
IoT	Internet of Things
6G	Sixth generation wireless technology
SLP	Source location privacy
PDR	Packet delivery ratio
EED	End-to-end delay
N_{SL}	Network side length
N_{SN}	Number of sensor nodes in a WSN
N_{Sink}	Number of sink nodes in a WSN
S_{CR}	Sensor node communication range
S_{SR}	Sensor node sensing range
S_{IE}	Sensor node initial energy
SN	Source node
SN_{PR}	Source node packet generation rate
P_{SZ}	Size of packet
A_{HR}	Adversary hearing range
A_{WT}	Adversary waiting timer
SP	Safety period
ASR	Attack success rate
CR	Capture ratio
DR	Detection ratio
TDR	Tree-based diversionary routing protocol
FPR	Fake source with phantom source routing protocol
DDR	Data dissemination protocol
PRR	Probabilistic source location privacy protection protocol

조선대학교
CHOSUN UNIVERSITY

RIN Random intermediate node routing protocol

PhaT Proposed two-level phantom with a backbone route protocol

PhaP Proposed two-level phantom with a pursue ring protocol

TreeR Tree routing protocol with diversionary routes

ProbR Probabilistic routing protocol

Pha Phantom single-path routing protocol

P_{ring} Pursue ring in PhaP

dP_{in} Distance from the sink node to the inner ring of the P_{ring} in PhaP

dP_{out} Distance from the sink node to the outer ring of the P_{ring} in PhaP

P_{Nfst} First level phantom node

P_{Nsec} New second level phantom node

θ Sensor node offset angle

T_P A bias threshold value in PhaP

R_N A random number distributed between [0, 1] in PhaP

epN Existing first level phantom node adopted from TreeR

npN New second level phantom node

d_{NB} Distance between inner and outer boundaries of the near network border region

d_{SB} Distance from a sensor node to the network border

N_{NB} Nodes which are located in the near network border regions

R_dR Restricted region around *epN*

d_P Hop distance between *epN* and *npN*

d_H Radius of R_dR

T A bias threshold value

$_BN$ Initial node of the backbone route which is a neighbor of *npN*

SF A random selection factor distributed between [0, 1] in PhaT

Strat-R Strategic location-based random routing scheme

Proxy-R Proxy node routing scheme

Angle-Strat Proposed angle-based Strat-R

조선대학교
CHOSUN UNIVERSITY

Angle-Proxy Proposed angle-based Proxy-R

CR Contrived region in Angle-Strat and Angle-Proxy

FR Forwarding regions

θ_{range} Range of θ

A_F Arbitrary factor in Angle-Strat and Angle-Proxy

R_F A random selection factor distributed between [0.1, 0.9] in Angle-Strat and Angle-Proxy

r_H Radius of near-sink region in Strat-R

r_D A ring where diversion nodes are located

r_{HD} Radius of r_D

r_M A ring where mediate nodes are located

r_{HM} Radius of r_M

r_{SR} Radius of near-sink region in Angle-Strat

$Proxy_R$ A proxy region where proxy nodes are strategically located in Proxy-R

L Length of WSN domain in Proxy-R

C Width of WSN domain in Proxy-R

V Side length of near-sink region in Angle-Proxy

ReRR Relay ring routing protocol

DissR Data dissemination routing protocol

DistrR Distributed fake source with phantom node protocol

PhanR Phantom single-path routing protocol

R_{ZF} Randomization factor

rN Relay node

R_{ring} Relay node ring in ReRR

R_{width} Width of the R_{ring}

d_{Rin} Distance between the sink node and the inner boundary of the R_{ring}

d_{Rout} Distance between the sink node and the outer boundary of the R_{ring}

d_T Threshold hop distance

d_S Hop distance between a sensor node and the sink node

조선대학교
CHOSUN UNIVERSITY

RR	Relay region
RS	Routing strategy
γ	Level of SLP in terms of SP or CR
γ_{Ach}	Achieved γ
γ_{Req}	Application-specific required γ
R_{γ}	γ realiability
Δ_{γ}	Difference between the γ_{Ach} and γ_{Req}
γ_{Ave}	Average of the γ_{Ach} and γ_{Req}
R_{SP}	SP reliability
R_{CR}	CR reliability
DERs	Distributed energy resources

조선대학교
CHOSUN UNIVERSITY

LIST OF TABLES

조선대학교
CHOSUN UNIVERSITY

LIST OF FIGURES

조선대학교
CHOSUN UNIVERSITY

조선대학교
CHOSUN UNIVERSITY

조선대학교
CHOSUN UNIVERSITY

LIST OF ALGORITHMS

조선대학교
CHOSUN UNIVERSITY

ABSTRACT

Enhancing the Performance of Routing Protocols for Location Privacy Protection in Event Monitoring Wireless Networks

Lilian C. Mutalemwa
Advisor: Prof. Seokjoo Shin
Department of Computer Engineering
Graduate School of Chosun University

Sensor-based Internet of Things (IoT) networks will play a vital role in the anticipated sixth generation (6G) and beyond wireless technology. The networks will utilize modern wireless sensor network (WSN) technology. Often, WSNs operate in unattended, harsh, and complex environments. Furthermore, WSNs are mostly battery-powered and resource-constrained. Therefore, performance of WSNs is vulnerable to energy and environmental factors. Moreover, WSNs are usually deployed in random areas with no protection. Consequently, the networks are vulnerable to traffic analysis attacks. In the attacks, adversaries focus on analyzing the network traffic to obtain critical information about the location of important sensor nodes such as source nodes. Thereafter, adversary identifies the event location. Therefore, to preserve the privacy of the source nodes and provide security, it is important to protect the source location privacy (SLP).

To address the challenge of SLP, numerous SLP routing protocols are presented in the literature. However, many state-of-the-art SLP protocols provide high levels of SLP protection at the expense of high communication cost and increased network overhead. For example, fake packet-based SLP protocols provide high levels of SLP protection by distributing large amount of fake packet traffic in the network. Consequently, the protocols are energy-inefficient, they incur limited network lifetime, and have high probability of packet collision events which result in reduced packet delivery ratio

조선대학교
CHOSUN UNIVERSITY

(PDR) and increased end-to-end delay (EED).

In this work, series of experiments are conducted to evaluate the performance of various state-of-the-art SLP protocols. Subsequently, based on the observations, some recommendations are presented to address the limitations of the protocols. Furthermore, to address the shortcomings of the existing SLP protocols, several new SLP protocols are developed. A two-level phantom with a pursue ring (PhaP) protocol is proposed to address the limitations of a recently proposed protocol. Simulation results show that PhaP achives high levels of SLP protection and reduced energy consumption in the near-sink regions. A two-level phantom with backbone route (PhaT) protocol is developed. It is demonstrated that PhaT achieves improved energy consumption, PDR, and EED. Angle-based strategic location-based random routing (Angle-Strat) and proxy node routing (Angle-Proxy) protocols are devised to address the limitations of recently proposed protocols. Both Angle-Strat and Angle-Proxy protocols achieve high levels of SLP protection by employing cost-effective routing paths. A relay node routing (ReRR) protocol is proposed to address the limitations of fake packet-based SLP protocols. It is established that ReRR guarantees improved performance in terms of long-term SLP protection, energy efficiency, and network lifetime.

In addition, it is observed that previous studies fail to evaluate the SLP reliability of the protocols. Therefore, novel approaches are proposed to realize the SLP reliability. Then, experiments are conducted to measure the SLP reliability. It is shown that the proposed ReRR protocol presents superior performance in terms of long-term SLP reliability.

조선대학교
CHOSUN UNIVERSITY

요약

이벤트 모니터링 무선 네트워크에서 위치 정보 보호를 위한 라우팅 프로토콜의 성능 개선

릴리안 찰스 무타람와

지도교수: 신석주

컴퓨터 공학과

조선대학교 대학원

센서 기반 사물인터넷(IoT) 네트워크는 6세대 이동통신(6G)과 무선 기술 분야에서 매우 중요한 역할을 할 것이다. IoT는 무선 센서 네트워크 (WSN) 기술을 활용하며 무선환경과 가혹하고 복잡한 환경에서 작동할 수 있다. 일반적으로 WSN은 대부분 배터리로 작동되고 자원은 제한적이다. 따라서 WSN의 성능은 에너지 및 환경 요소에 취약하고 일반적으로 무방비, 무작위로 배치되는 특성을 갖는다. 따라서 WSN 네트워크는 트래픽 분석 공격에 취약하다. 네트워크 공격자들은 센서 노드의 위치 정보와 같은 중요한 정보를 얻기 위해 네트워크 트래픽을 분석하는 데 집중할 수 있다. 예를 들어 WSN 모니터링에서 공격자는 트래픽 분석 공격을 수행하여 소스 노드의 위치를 식별한 후 모니터링된 자산을 획득하거나 의도적으로 파괴할 수 있다. 따라서 소스 노드의 개인 정보를 보호하고 WSN의 보안을 보장하기 위해서는 SLP(소스 위치 개인 정보)를 보장하는 것이 필요하다. 따라서 SLP는 IoT WSN 환경에서 풀어야 할 주요 과제 중 하나라고 판단된다.

SLP 문제를 해결하기 위해, 문헌에서는 수많은 SLP 라우팅 프로토콜이 제시되어 있다. 그러나 많은 SLP 프로토콜들은 높은 통신 비용과 네트워크 오버헤드 증가를 희

조선대학교
CHOSUN UNIVERSITY

생하면서 높은 수준의 SLP 보호를 제공한다. 예를 들어 가짜 패킷 기반 SLP 프로토콜은 네트워크에 대량의 가짜 패킷 트래픽을 분산시켜 높은 수준의 SLP 보호를 제공하지만 종종 에너지 효율성이 떨어지고 네트워크 수명이 짧으며 패킷 충돌 이벤트 발생 가능성이 높아 패킷 전달 비율(PDR)이 감소하고 종단 간 지연(EED)이 증가한다.

본 논문에서는 다양한 SLP 프로토콜의 성능을 평가하기 위한 종합적인 실험과 성능 비교 분석을 진행하였다. 이후에는 비교 관찰에 기초하여 각 프로토콜의 한계를 다루기 위한 몇 가지 요구사항을 정의하였다. 최종적으로, 기존 SLP 프로토콜의 단점을 해결하기 위해 몇 가지 새로운 SLP 프로토콜을 새로 제안하고 성능 검증을 통해 비교 우위를 확보하였다. 상세히 기술하면, 기존 프로토콜들의 한계를 해결하기 위해 추적 링(PhaP) 프로토콜이 있는 2단계 팬텀이 제안되었다. 시뮬레이션 결과에 따르면 PhaP는 높은 수준의 SLP 보호 기능을 제공하고 싱크노드에 가까운 지역에서는 에너지 소비량을 감소시킨다. 기존 프로토콜의 한계를 해결하기 위해 백본 경로(PhaT) 프로토콜이 포함된 2단계 팬텀이 제안되었다. PhaT는 에너지 소비량, PDR 및 EED 개선을 달성한 것으로 검증되었다. 각도 및 전략적 위치 기반 랜덤 라우팅(Angle-Strat)과 프록시 노드 라우팅(Angle-Proxy) 프로토콜은 최근에 문헌에서 제안된 프로토콜의 한계를 해결하기 위해 본 연구에서 제안되었다. Angle-Strat 및 Angle-Proxy 프로토콜은 모두 비용 효율적인 라우팅 경로를 사용하여 높은 수준의 SLP 보호를 달성한다. 더불어, 가짜 패킷 기반 SLP 프로토콜의 한계를 해결하기 위해 릴레이 노드 라우팅(ReRR) 프로토콜을 제안하였다. ReRR은 장기적 SLP 보호, 에너지 효율성, 네트워크 수명 측면에서 향상된 성능을 보장하는 것으로 분석되었다.

마지막으로 이전 연구에서는 프로토콜의 SLP 신뢰성에 관련된 연구가 수행되지 못하였다. 따라서, SLP 신뢰성을 실현하기 위한 새로운 접근법이 본 연구에서 제안되었으며, SLP 신뢰성을 측정하기 위한 실험을 수행하였다. 제안된 ReRR 프로토콜은 장기적인 SLP 신뢰성 측면에서 우수한 성능을 제공하는 것으로 검증되었다.

조선대학교
CHOSUN UNIVERSITY

Chapter 1

Introduction

1.1. Research Background

Wireless sensor network (WSN) technology plays a significant role and constitute the founding pillar of the Internet of Things (IoT) [1]-[10]. Therefore, with the growing demand for IoT, individuals and organizations are relying more on WSN technology [11]-[16]. Moreover, sensor-based IoT communication is a popular use case in the anticipated sixth generation (6G) and beyond wireless technology which will support modern real-time applications such as surveillance, object condition tracking, and autonomous mobile robots.

In recent years, WSN technology has attracted worldwide attention in wide range of application domains including smart home development, medical treatment, environmental monitoring, natural disaster prevention, intelligent industrial monitoring, water quality controlling, intelligent transportation systems, military surveillance, and national security [9], [16]-[21]. For example, for city navigation, WSNs can be used to guide drivers. In mobile applications, users can find things of interest by using a location-based service. In the military domain, troops and other personnel can win more battles with the help of WSNs [12]. Based on scientific predictions, the total number of wireless sensors deployed will reach 60 trillion at the end of the year 2022 [17]. Also, IoT market will grow from more than 15 billion devices in 2015 to more than 75 billion in 2025 [17].

Different from traditional wired networks, WSNs are usually deployed in unattended, harsh, and complex environments. Therefore, performance of WSNs is vulnerable to environmental factors [19], [22]-[27]. Furthermore, due to the unattended openness and self-organized nature of WSNs, the networks are vulnerable to traffic analysis attacks [24], [28]-[33]. Thus, WSNs are under increasing threat of privacy disclosure, interception, or tampering, even if a high density complex data encryption algorithm is employed [34]. Hence, security and privacy are significant challenges in WSNs [28], [29], [33]-[42].

조선대학교
CHOSUN UNIVERSITY

A classification of the privacy issues in WSNs is shown in Fig. 1.1. Traffic analysis attacks present serious threats on the data privacy and context privacy in WSNs [12], [31], [38], [43]-[45]. Data privacy is related to the contents of the packets which are being transmitted in the WSNs. Data privacy ensures that the contents may not be disclosed/modified by the third party via any means [12], [43], [44]. Thus, it provides integrity, non-repudiation, and confidentiality of the contents [44]. To ensure data privacy, techniques such as sophisticated encryption algorithms [12], [43], *k*-anonymity [12], and *k*-nearest neighbor [12] may be used. The focus of this work is on context privacy.

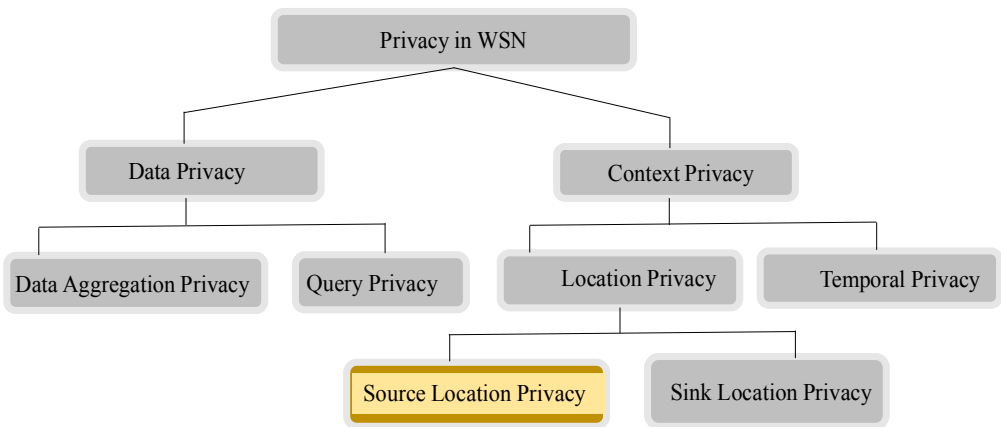


Figure 1.1: Classification of privacy issues in WSNs.

Context privacy is concerned with protecting the context associated with the sensed data in the course of measurement and transmission. It comprises of hiding the identity, location of nodes, and traffic flow in the WSN. It covers temporal privacy which is concerned with the time when sensitive data is created at the source node, collected by a sensor node, and delivered to the sink node [38]. Location privacy includes source and sink node location privacy [12], [43], [44]. In this work, we focus on the issues of source location privacy which often involve a presence of an adversary who performs traffic analysis attacks. The main goal of an adversary is to identify the source node location and thereafter capture the monitored asset. Hence, when WSNs are used in safety-critical applications, it is important to provide SLP protection. To achieve SLP protection, numerous SLP routing

조선대학교
CHOSUN UNIVERSITY

protocols are presented in the literature [28], [29], [33], [35]-[42]. In this work, we explore the performance features of various SLP routing protocols and propose new SLP routing protocols to provide SLP protection in event monitoring WSNs.

1.2. Source Location Privacy in Event Monitoring WSNs

Usually, a WSN consists of a large number of small sensor nodes which are self-organized as an ad hoc network to monitor a target [11], [34], [43], [46]. In monitoring WSNs, the main function of the sensor nodes is to sense an event (asset) and report to the sink node. The node that senses an event becomes a source node and periodically sends the event reports to the sink node [31], [40], [43]. To be able to detect the event, tracking devices such as radio frequency identification (RFID) tags are attached to the assets [38], [47]-[55]. The RFID tags use radio waves to transfer the sensed data to the source nodes.

Monitoring WSNs are used in safety-critical applications such as tracking the movements of troops in a field and habitat monitoring of rare animals in forests [40], [43], [45]. Also, in wildlife protection and monitoring of endangered species where poachers may be tempted to infer the location of the animal to capture it [45], [56], [57]. Real world implementation examples include monitoring badgers and the wildlife crime technology project [45], [57]. The project is operated by the World Wildlife Fund.

Considering the importance and sensitivity of the source node in monitoring WSNs, an eavesdropping adversary may focus on analyzing the network traffic to obtain critical information such as the location information of the source node. Thereafter, adversary may capture the monitored asset [24], [28]-[32], [57]. Therefore, to protect the location privacy of the source nodes and ensure security of the WSNs, it is important to provide SLP protection [11], [13], [31]. Thus, SLP protection is defined as the process of minimizing the traceability and observability of a source node by an adversary in monitoring WSNs. SLP protection ensures that location of the source node is hidden from adversaries [11], [31], [40], [56]-[58]. The SLP problem was introduced in [59]. It was recently presented in [11], [33] that SLP is a significant challenge in industrial IoT. Also, the work in [12]

조선대학교
CHOSUN UNIVERSITY

highlighted the importance of SLP protection in WSNs for IoT.

1.3. Source Location Privacy Routing Protocols

The topic of SLP protection in WSNs has received a lot of attention in the literature since it was first introduced in 2004 [28], [29], [60]. Numerous SLP routing protocols are presented in the literature. Many of the protocols are discussed in [28], [29], [33], [35]-[42]. Some of the recently proposed SLP protocols include the two-level phantom with a pursue ring protocol [29], unified single and multi-path routing protocol [30], dynamic multipath routing protocol [11], grid-based single phantom node protocol [39], data dissemination protocol [61], and the protocol based on anonymity cloud [56]. Other recently proposed SLP protocols include the cloud-based with multi-sinks protocol [31], protocol based on phantom nodes, rings, and fake paths [33], phantom walkabouts protocol [45], grid-based dual phantom node protocol [39], two-level phantom with a backbone route protocol [29], probabilistic routing protocol [62], and the circular trap protocol [63].

In [28], the SLP protocols were classified into many categories, including (1) phantom routing protocols, (2) fake packet injection protocols, (3) the multiple routing path protocols, (4) random walk routing, (5) hiding protocols, (6) ring routing protocols, (7) protocols based on the ring routing and the fake packet injection, (8) protocols based on the phantom routing and the fake packet injection, (9) data mule protocols, (10) cryptography and authentication protocols, (11) network encoding protocols, (12) directional communication protocols, and (13) the isolation protocols. In [36], the routing protocols were classified into the following categories: (1) phantom node routing, (2) fake source routing, (3), intermediate node routing, (4) tree-based routing, and (5) the angle-based routing protocols. In [60], the solutions for SLP protections were categorized into several strategies including (1) random walk routing, (2) fake source packet routing, (3) cyclic entrapment, and (4) geographic routing. In [37], the solutions for providing the SLP protection were classified into many categories including (1) fake source packet routing, (2) random walk routing, (3) geographic routing, (4) cyclic entrapment, (5) separate path routing, (6) location anonymization, (7) cross-layer routing, (8) network coding, (9) delay, and (10) limiting the node detectability. Various types of the SLP

조선대학교
CHOSUN UNIVERSITY

protocols are presented in the section of related work in Chapter 3, Chapter 4, and Chapter 5.

1.4. Motivation and Research Contributions

Motivated by the contributions of various existing studies in the literature, this work presents some investigations and new findings on the problem of SLP. Also, five new SLP protocols are presented. The protocols were developed and published in recent work.

The study in chapter 3 is motivated by the discussions in [28], [29], [36], [42], [56], [64], and [65]. It is considered that it is important to provide effective and long-term SLP protection in safety-critical monitoring applications. However, fake packet-based SLP protocols are often energy-inefficient, they incur limited network lifetime, and have high probability of packet collision events. Therefore, it is important to explore various features such as the ability of the protocols to guarantee long-term SLP protection and reliable packet delivery. Nevertheless, previous studies show some deficit in the performance evaluation of the protocols. Consequently, chapter 3 presents some investigations on the performance of fake packet-based SLP protocols. Comprehensive performance analysis of four existing protocols is done under varied network parameters and configurations. Experiments are conducted to observe the performance of the protocols under varied sensor node residual energy, source-sink distance, lifetime, source packet rate, network size, and node density. In the analysis, various performance metrics are considered such as the safety period (SP), capture ratio (CR), detection ratio (DR), energy consumption, network lifetime, packet delivery ratio (PDR), and end-to-end delay (EED). Based on the observations, we provide some recommendations to improve the performance of the protocols.

Chapter 4 presents two studies. The first study is motivated by the discussions in [32], [62]. In the study, fake source packet routing protocols are employed to provide SLP protection. The protocols rely on broadcasting fake packets from fake sources concurrently with the transmission of real packets from the real source nodes to obfuscate the adversaries. However, fake source packet routing protocols have demonstrated some performance limitations including high energy consumption, low PDR, and long EED. New phantom-based SLP routing protocols are proposed to

조선대학교
CHOSUN UNIVERSITY

address the limitations of existing fake source packet routing protocols. Each proposed protocol introduces a two-level phantom routing strategy to ensure two adversary confusion phases. When the adversaries perform traffic analysis attacks against the proposed routing algorithms, they encounter two levels of obfuscation. It is shown that the proposed protocols present superior performance features. The protocols guarantee strong SLP protection throughout the WSN domain with controlled energy consumption, PDR, and EED. Furthermore, it is established that the proposed protocols achieve more practical results under varied network configurations.

The second study in chapter 4 is motivated by the discussions in [40], [58]. It is considered that battery power is a limited resource in WSNs. Therefore, SLP routing protocols must be energy-efficient and overall cost-effective. It is observed that angle-based routing protocols present cost-effective solutions for SLP protection. Therefore, a new angle-based routing algorithm is proposed to improve the communication cost of two existing SLP routing protocols. The proposed algorithm considers path node offset angles, arbitrary factors, and contrived regions to compute relatively short but greatly randomized routing paths. The routing paths offer a reduced number of packet forwarding events in the near-sink regions and eventually diminish the packet transmission cost. It is demonstrated that the proposed path node offset angle routing algorithm effectively improves the packet transmission cost of the protocols. Also, it guarantees strong SLP protection throughout the WSN domain. Moreover, it is observed that the proposed path node offset angle routing algorithm is capable of alleviating the energy-hole problem in WSNs.

The study in chapter 5 is motivated by the discussions in [18], [20], [35], [66]-[69]. In [35], it was shown that the data dissemination routing (DissR) and distributed fake source with phantom node (DistrR) protocols achieve short-term SLP protection and limited network lifetime due to high energy consumption. Furthermore, it was shown that DissR incurs unbalanced energy distribution. The challenge of unbalanced energy distribution in WSNs was also highlighted in [18], [20]. Then, it was presented that when the challenge of unbalanced energy distribution is addressed, it can result in improved network lifetime and reliability. In the discussions of [66]-[69], it was presented that to ensure reliable network operations in WSNs, it is essential to develop reliable routing protocols and

조선대학교
CHOSUN UNIVERSITY

provide a means to evaluate the reliability of different routing protocols. Therefore, chapter 5 presents a new relay ring routing (ReRR) protocol. The ReRR protocol employs an energy-efficient routing algorithm and achieves reliable long-term SLP protection to outperform the DissR and DistrR protocols. In addition, a novel approach is proposed to evaluate the SLP reliability of the protocols. To the best of our knowledge, SLP reliability has never been measured in previous studies.

More detailed summaries of the contributions are presented in Chapter 3, Chapter 4, and Chapter 5.

1.5. Organization of the Thesis

The rest of this thesis is organized as follows. Chapter 2 conveys some assumptions and details of the network, adversary, energy consumption, and network lifetime models. Chapter 3 discusses the the underlying routing strategies of the fake packet-based SLP routing protocols and investigates the performance of the protocols under varied network parameters and configurations. In chapter 4, several new routing algorithms are presented to devise new SLP protocols. Also, chapter 4 discusses the performance of protocols to show improved performance in terms of SLP protection and/or communication overhead. Chapter 5 points out that the SLP reliability of the protocols has not been measured. Then, it presents novel approaches to realize the SLP reliability. Chapter 6 provides some concluding remarks and future research opportunities.

조선대학교
CHOSUN UNIVERSITY

Chapter 2

Models

To enable comprehensive performance analysis and experimental evaluation, the assumptions and models are presented in this chapter. The network, adversary, energy consumption, and network lifetime models are presented in sections 2.1, 2.2, 2.3, and 2.4, respectively.

2.1. Network Model

The network model is based on the famous panda-hunter model that was proposed by the seminal work in [59] and considered in many studies including [28], [32], [39], [43], [45], [62], [70]-[72]. The WSN comprises a large number of homogeneous sensor nodes randomly deployed to continuously monitor a target field. The network is two-dimensional and contains a set of sensor nodes and links. A wireless sensor node is a computing device enabled with a wireless interface, limited set of computational capabilities and has a unique identifier (ID). Each sensor node has several properties including the sensing range and communication range. Distance between any two points in the network is computed using the Euclidean distance equation shown in equation (1). As an example, equation (1) shows the parameters for calculating the distance between point V at (x_V, y_V) and point W at (x_W, y_W).

$$d_{VW} = \sqrt{(x_V - x_W)^2 + (y_V - y_W)^2} \tag{1}$$

Communication from a node is modeled with a circular communication range centered at the node. Sensor nodes are able to communicate with each other if they are located at a distance which is less than or equal to their communication range. Thus, nodes in direct communication with each other through single-hop communication are considered neighboring nodes and are able to exchange data. A sensor is able to sense all points within its sensing range. Three types of sensor nodes and sensor node functionalities exist in the network: sink node, source nodes, and ordinary nodes. The sink node is responsible for collecting data from other nodes and acts as a link between the WSN and the external world. The sink node is more powerful than the ordinary nodes. It has sufficient

조선대학교
CHOSUN UNIVERSITY

resources in terms of memory capacity, data transmission, and computational power. The source node is responsible for sensing the event and forwarding the sensed data to the sink node through multi-hop communication. Ordinary nodes are used to relay packets from the source node to the sink node.

The network is event-triggered. Thus, when a source node detects an event it starts sending packets periodically to the sink node. Similar to [56], the *k*-nearest neighbor tracking approach [73] is employed to track the target/asset. When a node detects an asset in its monitoring area, it remains active until the asset moves out of its monitoring area. When the asset moves to a new location, it activates another sensor node to become a new source node. When no asset is detected, the nodes may follow a sleeping schedule. Transmitted packets are encrypted and contain source node ID that only the sink node can infer as the event location.

During the network deployment phase, the network initialization process is performed for localization of the sensor nodes. It is assumed that the sink node acquires its location information by using a global positioning system (GPS). Once the sink node is aware of its location, it can lead the network initialization process by broadcasting a beacon packet to other sensor nodes. Other sensor nodes use the beacon packet to approximate their location and rebroadcast the packet to the neighboring nodes. Thus, each node receives the beacon packet, stores the hop counter value with a sender node ID, increments the hop counter by one, and rebroadcasts the beacon packet to its neighboring nodes. The hop counter number indicates the hop distance between a sensor node and the sink node. If a sensor node receives multiple packets, it only stores the minimum hop count in its buffer and deletes other hop counter information. At the end of the network initialization process, each node in the network is aware of its location, location of its neighboring nodes and IDs, and the location of the sink node. In the angle-based SLP routing protocols which are proposed in this work, the network initialization process includes the computation of node offset angle (θ). In the computation of θ, an X–Y coordinate is generated, centered at the sink node. The θ is an inclination angle formed between the X-axis and the imaginary line connecting the sink node and the node that is computing the θ. As an example, to compute the θ for node Z (θ_Z) at (x_Z, y_Z), distances d_{SZ} and d_{ZA} are considered. Line ZA is an imaginary line from node Z to the X-axis. The line ZA connects to the

조선대학교
CHOSUN UNIVERSITY

X-axis at point A located at (x_A, y_A). Then, θ_Z is computed according to equation (2).

$$\theta_Z = \sin^{-1}\left(\frac{d_{ZA}}{d_{SZ}}\right) \quad (2)$$

2.2. Adversary Model

There are many types of adversary models in the literature including the patient adversary [40], [43], [45], [58], [71], [74], cautious adversary [35], [58], [59], [63], [71], [74], direction-oriented adversary [32], estimating adversary [62], hotspot-locating adversary [11], [31], [56], [75], and the enhanced hotspot-locating adversary [56]. Often, the adversaries may perform passive or active attacks [37], [38], [76]. A passive adversary performs passive attacks such as simply eavesdropping on the sensor nodes communication and performing a back tracing attack on the packet routes [33], [46]. The passive adversary does not interfere with the normal operations of the network to avoid getting noticed by the network operator. Thus, the adversaries refrain from actions such as modifying the packets, altering the routing paths, or destroying the sensor devices.

In contrast, an active attack occurs when the adversary attempts to alter the network traffic by modifying the packets' header, the packets' content, or even by injecting new packets into the network to apply some attacks such as denial-of-service [38]. Active adversaries are highly motivated and can interfere with the normal operation of nodes by blocking packets from a portion of the network or by reprogramming the sensor software [37], [76]. However, active adversaries are less common because they have more chances of being caught by the network operator if they interfere with the normal operation of the WSN. Furthermore, an adversary can have a local or global view of the network [56]. A local adversary has a partial view of the network, limited resources, and is only able to analyze local traffic [33]. On the other hand, a global adversary has a full view of the network, unlimited power, sufficient resources, and can analyze the entire traffic of the network [38], [45], [58].

The patient and cautious adversaries are the most common adversary models in the literature. The cautious adversary has more computational power than the patient adversary. A cautious adversary was assumed in the seminal work of [59], [71], [74], and in numerous studies including [35], [58], [63]. Similarly, this work assumes a local cautious adversary.

조선대학교
CHOSUN UNIVERSITY

The cautious adversary is well-equipped with enough storage, energy, powerful transceivers, and spectrum analyzers to enable detection of packet signals and traffic patterns. The adversary is mobile, initially residing in the vicinity of the sink node listening for arriving packets. When the adversary initial location is in the vicinity of the sink node, it improves the probability of the adversary overhearing the sensor node communications since there is a large amount of packet traffic in the neighborhood of the sink node [45]. This is mainly because sink node is the destination node for all the packet traffic.

On detecting a packet transmission, adversary can measure the angle of arrival of the signal and the received signal strength to identify the immediate sender node and perform back tracing attack by moving to the immediate sender node location without any delay. Once at the immediate sender node, the adversary keeps on listening on the communications between the node and its neighboring nodes and continues to perform hop-by-hop back tracing attack towards the source node, until it reaches at the location of the source node. The adversary never misses a packet when transmission is within the adversary hearing range. Adversary may capture information such as message type, sequence number, and sender node ID. When the source node is found, the adversary can successfully capture the monitored asset. Hence, the security of the network is compromised. The adversary performs passive attacks.

The cautious adversary has computational power to limit its waiting time at any immediate sender node. It uses a waiting timer. If the timer expires, the adversary will roll back to its previous immediate sender node and resume the packet listening process at that node. Moreover, the cautious adversary has the ability to escape from getting trapped in a loop. It collects and stores the information of all the visited immediate sender nodes to avoid revisiting nodes which have already been visited.

2.3. Energy Consumption Model

The energy consumption model is based on the standard energy consumption model that was proposed in [77] and considered in many studies including [11], [18], [31], [32], [78]-[83]. It is

조선대학교
CHOSUN UNIVERSITY

Table 2.1: Energy consumption model parameters

Parameter	Description	Value
E_{loss} (nJ/bit)	Transmitting circuit energy loss	50
E_{fs} (pJ/bit/m^2)	Energy for power amplification in the free-space model	10
E_{amp} (pJ/bit/m^4)	Energy for power amplification in the multi-path attenuation model	0.0013
d_o (m)	Threshold distance for the channel models	87
l (bit)	Size of the packets	1024

assumed that to transmit an l-bit packet to a transmission distance d, transmission energy, E_{trans}, and receive energy, E_{rec}, follow equations (3) and (4), respectively. The model assumes that the energy consumption for packet transmission is an exponential function of d. E_{loss} is the transmitting circuit loss. The model uses both free-space (d^2 power loss) and multi-path fading (d^4 power loss) channel models, depending on the distance between the transmitter and receiver. Power control can be used to invert the loss by appropriately setting the power amplifier. Thus, if the transmission distance is less than the threshold distance, d_0, the power amplifier loss is based on the free-space model. Otherwise, the multi-path attenuation model is used. The d_0 is computed according to equation (5). E_{fs} and E_{amp} are the energies required by power amplification in the two power loss models. The energy parameter E_{loss} depends on factors such as modulation, coding, and filtering [18]. When the number of bits is increased, it increases the amount of energy dissipated in the electronics of the radio. Table 2.1 shows the energy consumption model parameters.

$$E_{trans} = \begin{cases} lE_{loss} + lE_{fs}d^2, & if\ d\ <\ d_0 \\ lE_{loss} + lE_{amp}d^4, & otherwise. \end{cases} \tag{3}$$

$$E_{rec} = lE_{loss} \tag{4}$$

$$d_0 = \sqrt{\frac{E_{fs}}{E_{amp}}} \tag{5}$$

2.4. Network Lifetime Model

The network lifetime model is adopted from [32], [83]. The model assumes that there is no direct relationship between the network lifetime and the total energy consumption of the network. However,

조선대학교
CHOSUN UNIVERSITY

there is a direct relationship between the network lifetime and the total energy consumption of the sensor nodes in the near-sink regions. The main reason for the assumption is that, the sensor nodes in the near-sink regions forward their own packets and act as relay nodes for the sensor nodes which are located away from the sink node. As a result, the sensor nodes incur exhaustive energy consumption. A phenomenon called energy-hole can happen when the sensor nodes in the near-sink regions exhaust their energies. Subsequently, a ring of dead nodes may form around the sink node and the network lifetime may be affected. Therefore, the network lifetime is maximized when the energy consumption of the sensor node with maximum energy consumption is minimized, as shown in equation (6). In the equation, NL is the network lifetime and NE_i is the energy consumption of node i.

Therefore, based on the model, the network lifetime is defined as the period between the start of the network operation and the first sensor node power outage.

$$\max\ (NL) = \min \max_{0<i\leq k}\ (NE_i) \tag{6}$$

조선대학교
CHOSUN UNIVERSITY

Chapter 3

Performance of Source Location Privacy Protocols

3.1. Background

It is critical that the limitations of WSNs are considered during the designing of routing protocols for IoT systems [26], [78], [84]. The limitations of WSNs include limited power, memory, bandwidth, and processing capability [21], [29], [85]. When the WSNs are used in safety-critical and long-term monitoring applications such as monitoring of high value assets, the routing protocols are expected to warranty desirable features such as energy efficiency, low delay, reliable packet delivery, and high levels of SLP protection. It is important to ensure energy efficiency and long network lifetime in the WSNs because the networks are often deployed in harsh and inaccessible environments. Thus, energy-efficient routing protocols enable the WSNs to achieve long unattended operation time [78].

This study is focused on investigating the performance of SLP routing protocols. In particular, investigations are done on a category of protocols which utilize fake source packet routing strategies. The protocols rely on obfuscating the adversaries by employing mimicking fake packet sources to imitate the real packet sources [56], [86]. The real and fake packet sources transmit packets in a synchronized manner. The main objective of the fake packet sources is to transmit fake packets which are capable of misleading the adversary into tracing back the fake packet routes while keeping the real packet routes secured. When the adversary is tricked into back tracing the fake packet routes, it is steered away from the location of the real source node and the SLP is protected [87]. The operations of the real and fake packet sources may be depicted as two teams in a tug-of-war game [87]. In the game, the two teams create a pull effect on a piece of rope. The team with a greater pull effect wins. Similarly, for the real and fake sources, the fake source nodes create a pull effect to pull the adversary away from the real source node. If the pull effect of the fake source node is greater, the fake source wins by keeping the adversary away from the location of the real source node. Subsequently, the SLP is protected.

조선대학교
CHOSUN UNIVERSITY

There exist other categories of SLP protocols including the phantom routing, intermediate node routing, ring routing, angle routing, random walk routing, tree routing, data mule mechanism, directional communication mechanism, isolation mechanism, and the hiding mechanism [28], [37]. The main reason for choosing to investigate the protocols which utilize fake source packet routing techniques is that, the protocols are often criticized for their high communication cost including significantly high energy consumption and low packet delivery reliability [28], [36], [37], [64]. Exhaustively high energy consumption may result in short-term SLP protection and reduced network lifetime. When the sensor nodes exhaust their energies at a fast rate, the protocols may preserve the SLP but only for a limited period of time. Thus, it is interesting to investigate the performance of the protocols under varied network parameters and configurations. More details about the motivation for this study are presented in section 3.3.

Four fake packet-based SLP protocols are included in the investigations: the tree-based diversionary routing protocol (TDR) [32], data dissemination routing protocol (DDR) [61], distributed protocol with fake source and phantom source routing (FPR) [44], and the probabilistic source location privacy protection protocol (PRR) [62]. The four protocols were selected for investigations based on features and key differences in their routing strategies as shown in Fig. 3.1. The following differences are considered. (1) TDR employs fake packet sources far away from the sink node, in the diversionary routes. DDR employs fake packet sources away from the sink node, outside the blast ring. PRR employs fake packet sources in the near-sink regions. FPR employs fake packet sources at variable distances from the sink node, throughout the WSN domain. (2) In TDR and FPR the fake packet sources are not isolated from the real source nodes but in DDR and PRR the fake packet sources are isolated from the real source nodes. (3) TDR broadcasts a large number of fake packets in the network from multiple fake packet sources, employing numerous fake sources per real source node. DDR broadcast multiple fake packets from a single fake packet source, employing one fake source per real source node. PRR broadcasts one fake packet from a single fake

조선대학교
CHOSUN UNIVERSITY

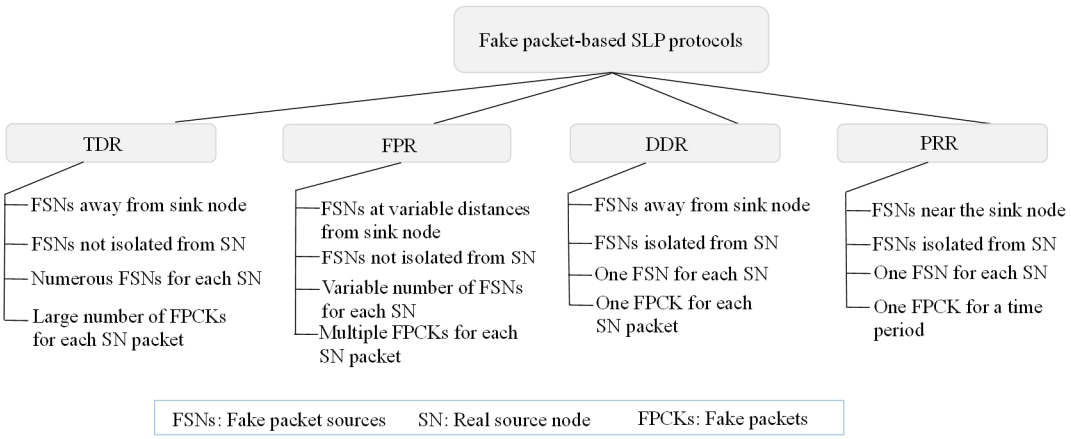


Figure 3.1: Features and routing strategies of the TDR, FPR, DDR, and PRR protocols.

packet source for a time period, employing one fake source per real source node for a time period. FPR broadcasts a variable number of fake packets from multiple fake packet sources which may be less than in TDR, employing multiple fake sources per real source node. (4) TDR broadcasts numerous fake packets per real source packet. DDR broadcast one fake packet per real source packet. PRR broadcasts one fake packet for a time period for each real source packet. FPR broadcasts multiple fake packets per real source packet which may be less than in TDR. Similar to other fake packetbased protocols, the TDR, DDR, PRR, and FPR protocols incur high energy consumption due to the distribution of fake packet traffic in the network [28], [29], [36], [42], [64]. Furthermore, the protocols incur unreliable packet delivery due to high probability of packet collision and packet loss events [29], [56].

The performance of TDR, DDR, PRR, and FPR protocols is investigated using important performance metrics: SP, CR, DR, energy consumption, network lifetime, EED, and PDR. For comparative analysis, the traditional random intermediate node routing (RIN) protocol [88] is included in the analysis as a reference protocol.

3.1.1. Contributions

The main contributions of this study can be summarized as follows. (1) Expose the underlying routing

조선대학교
CHOSUN UNIVERSITY

strategies of the fake packet-based SLP routing protocols and their influence on the privacy performance and packet delivery reliability. (2) Conduct a series of experiments to evaluate the SLP protection, energy consumption, network lifetime, EED, and PDR performance of the TDR, DDR, PRR, and FPR protocols under varied network configurations. (3) Contrast the performance of the TDR, DDR, PRR, and FPR protocols with the performance of the traditional RIN protocol through comprehensive experimental analysis. (4) Investigate the ability of the TDR, DDR, PRR, and FPR protocols to preserve the SLP in long-term monitoring networks and the effects of distributing fake packet traffic in various regions of the WSN domain. (5) Provide some recommendations to address the limitations of the TDR, DDR, PRR, and FPR protocols based on state-ofthe-art techniques.

3.2. Related Work

Various routing strategies have been proposed for SLP protection [28], [29], [36], [37], [38]. In [71], it was established that baseline fake packet routing and probabilistic fake packet routing strategies can be used to preserve SLP in monitoring WSNs. Since then, the fake packet routing strategies have been adopted in numerous protocols. The key procedures in the operation of the fake packet-based protocols include the process of selecting a subset of the sensor nodes in the WSN to act as fake source nodes by imitating the real source nodes. The fake sources and real sources send packets concurrently to confuse the adversary. In this section, we explore the operational features of the protocols.

Fake packet routing strategies have been adopted in the cloud-based with multi-sinks protocol [31], dummy packet injection protocol [89], dynamic fake source-based protocol [87], tree-based diversionary routing protocol [32], hybrid online dynamic single path routing protocol [41], dummy uniform distribution protocol [90], and the data dissemination routing protocol [61]. Other protocols which adopt the fake packet routing strategies include the probabilistic source location privacy protection protocol [62], timed efficient privacy preservation protocol [91], fake network traffic-based protocol [92], bidirectional tree protocol [74], dummy adaptive distribution protocol [90], distributed fake source and phantom source protocol [44], controlled dummy adaptive distribution

조선대학교
CHOSUN UNIVERSITY

protocol [90], and the redundancy branch convergence-based privacy protocol [83].

3.3. Problem Statement

Many of the existing studies such as [28], [29], [36], [42], [56], [64], and [65] point out that fake packet-based routing protocols are capable of effectively protecting the SLP in the monitoring networks. The studies also highlight some limitations of the protocols which result from the distribution of fake packet traffic in the network. The limitations include increased communication cost and network overhead. Also, the protocols incur unreliable packet delivery due to increased probability of packet collision and packet loss events. To mitigate the limitations while achieving high levels of SLP protection, the protocols employ unique features and strategies as described in section 3.2.

Although many studies have analyzed the performance of the fake packet-based routing protocols, the evaluations are often not comprehensive. As a result, some factors are often overlooked. For example, the ability of the protocols to ensure effective SLP protection for prolonged periods of time or the ability of the protocols to provide reliable packet delivery under varied network conditions are often disregarded. It is therefore essential that comprehensive performance evaluation is conducted while considering various factors including the following. (1) The protocols are energy-inefficient with high probability of energy exhaustion in the sensor nodes. If large amounts of fake packets are broadcasted in a region of the WSN domain, sensor nodes may drain their energies at a fast rate and the SLP protection may become short-lived. (2) Broadcasting large amounts of fake packet traffic in the network may result in increased number of packet collision events to degrade the reliability of the protocols.

Thus, in this study, we conduct comprehensive performance evaluation of four representative fake packetbased protocols which employ different fake packet routingstrategies. We evaluate the performance of the tree-based diversionary routing protocol (TDR) [32], data dissemination routing protocol (DDR) [61], distributed protocol with fake source and phantom source routing (FPR) [44], and the probabilistic source location privacy protection protocol (PRR) [62]. The key features and

조선대학교
CHOSUN UNIVERSITY

routing strategies of the TDR, DDR, FPR, and PRR protocols are summarized in Fig. 3.1. To ensure comprehensive analysis, we investigate the performance of the protocols under varied network parameters and configurations. Performance is observed under varied sensor node residual energy, source-sink distance, network operation duration, network size, source packet rate, and node density. We include performance metrics such as safety period, capture ratio, detection ratio, energy consumption, network lifetime, EED, and PDR. Based on the observations from the investigations, we include some recommendations for improvements. For protocols with exhaustively high energy consumption, energy harvesting technologies are recommended to ensure effective long-term monitoring.

3.4. Performance Analysis

The network model in section 2.1 and adversary model in section 2.2 were assumed. Then, a series of experiments were done to investigate the performance of the TDR, DDR, FPR, and PRR protocols. For comparative analysis, the traditional random intermediate node routing protocol (RIN) is included in the analysis. The RIN protocol employs a simple routing algorithm which does not involve fake packet routing. When a source node has a packet to send to the sink node, the RIN protocol allows a random selection of an intermediate node which is located at a safe distance from the source node. Thereafter, the packet is sent to the sink node through the selected intermediate node [88]. The following performance metrics were used for analysis: SP, CR, DR, energy consumption, network lifetime, EED, and PDR.

3.4.1. Simulation Parameters and Values

MATLAB simulation environment was used to simulate a WSN with a network side length (N_{SL}) of 2000 m. A total of 2500 sensor nodes were randomly distributed in the WSN domain. Thus, the number of sensor nodes (N_{SN}) was 2500. Only one sink node was assumed. Thus, number of sink nodes (N_{Sink}) was 1. The sensor node communication range (S_{CR}) was set to 30 m to ensure multi-hop communications and energy conservation. A cautious adversary was deployed with initial location in the locality of the sink node to ensure maximum probability of packet capture. The adversary hearing

조선대학교
CHOSUN UNIVERSITY

range (A_{HR}) was set to 30 m, similar to the S_{CR} to ensure the adversary performs hop-by-hop back tracing attack. The cautious adversary waiting timer (A_{WT}) was set to 4 source packets. The size of the packet (P_{SZ}) was 1024 bits. The source nodes generated packets at various source node packet rate (SN_{PR}) and the sensor node initial energy (S_{IE}) was assumed to be 0.5 J. Simulations were run for 500 iterations and average values were considered. The network simulation parameters are summarized in Table 3.1.

Table 3.1: Network simulation parameters

Parameter	Value
N_{SL} (m)	2000
N_{SN}	2500
N_{sink}	1
S_{CR} (m)	30
A_{HR} (m)	30
A_{WT} (source packets)	4
P_{sz} (bit)	1024
SN_{PR} (packet/second)	Varied from 1 to 6
S_{IE} (J)	0.5
Adversary initial location	In the locality of sink node

3.4.2. Simulation Results and Discussions

- **Safety Period**

SP is the time required for an adversary to perform back tracing attack and capture the monitored asset. It is used to measure the privacy performance of the protocols. Equation (7) shows that longer SP corresponds to higher levels of SLP protection [29], [32]. We measure the SP by counting the number of hops during the adversary back tracing attack.

$$\max\ (SP) = \max\ (SLP_{Protection}) \tag{7}$$

Fig. 3.2 shows the privacy performance of the protocols. In the experiment scenarios for the results in Fig. 3.2 (a), the SP was observed at various source-sink distances with a fixed source packet rate of 1 packet/second. It is shown in Fig. 3.2 (a) that the TDR, FPR and DDR protocols can achieve significantly longer SP than the RIN protocol. In TDR, the long SP is achieved by employing multiple routing strategies. The protocol employs phantom nodes which are located away from the source node. It creates long backbone routes which diverge to the network border regions. It generates

조선대학교
CHOSUN UNIVERSITY

diversionary routes as branches of the backbone routes and distributes large amounts of fake packet traffic in the diversionary routes. As a result, the protocol can effectively obfuscate the adversary and long SP is achieved. Furthermore, the packet routes in TDR protocol are designed to ensure a back tracing adversary is encountered with multiple routes and multiple incoming packets, making it difficult for the adversary to predict the correct path to the real source node.

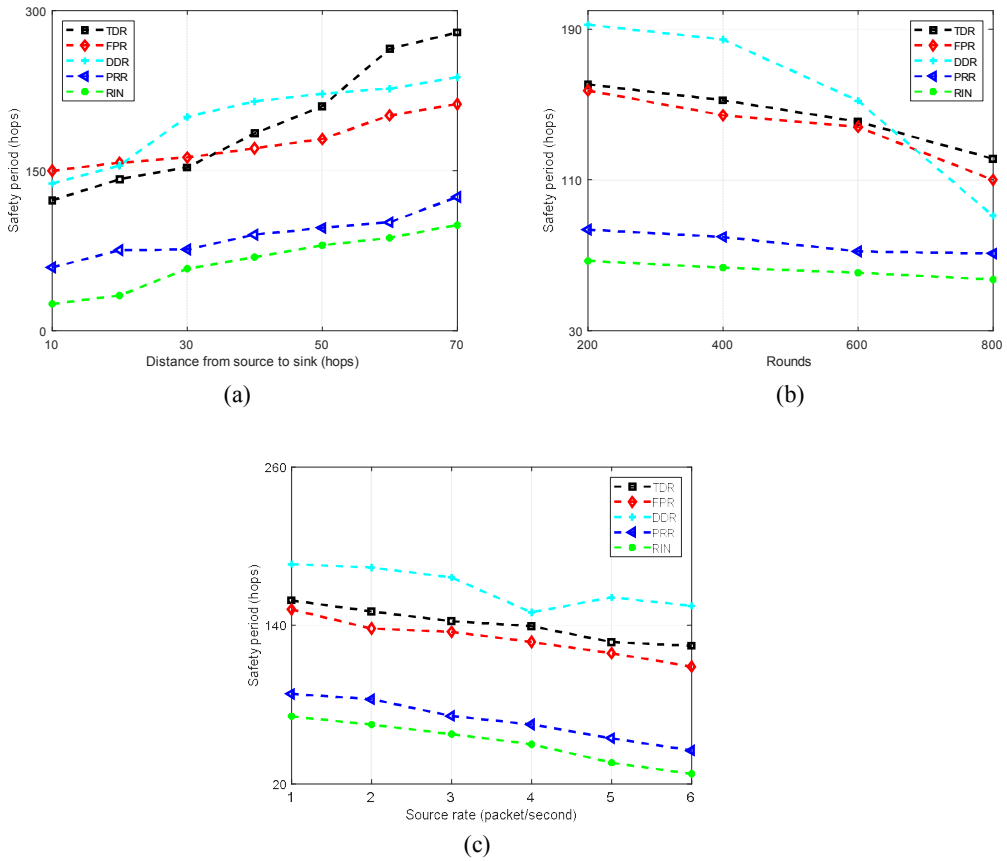


Figure 3.2: Privacy performance of the routing protocols. (a) SP against source-sink distance. (b) SP against rounds. (c) SP against source rate.

The FPR protocol distributes a considerable amount of fake packet traffic around the source node, simultaneously with the transmission of the real packets. As a result, the adversary is tackled with multiple packets and finds it difficult to identify the exact immediate sender node of the real packets. Therefore, the back tracing attack is made more complex and longer SP is achieved. The

조선대학교
CHOSUN UNIVERSITY

results also show that the privacy performance of TDR and FPR improves when larger numbers of fake packet sources are employed in a region of the network. FPR employs a larger number of fake packet sources than TDR in the near-sink regions while TDR employs a larger number of fake packet sources than FPR in the near network border regions. Consequently, the FPR protocol achieves longer SP than the TDR in the near-sink regions and TDR achieves longer SP in the network border regions.

To analyze the performance of the DDR protocol, all the sensor nodes with source-sink distance less or equal to 20 hops were assumed to be located inside the blast ring. The DDR protocol is capable of achieving longer SP than the TDR protocol inside the blast ring regions because it employs a probabilistic flooding mechanism. When the flooding mechanism is employed, multiple random nodes are selected to broadcast each packet. Thus, a packet may arrive at the sink node using multiple random routing paths. Furthermore, packets from a source node appear to arrive at the sink node from all possible angles. As a result, the tracing back attack becomes a complex and time consuming task. Moreover, the cautious adversary is restricted from revisiting the immediate sender nodes. To some extent, the restriction increases the complexity of the adversary back tracing attack when the flooding mechanism is used. It was also observed that the FPR protocol achieves slightly longer SP than DDR, inside the blast ring. The main reason is that, in some scenarios, the fake packet sources in the FPR protocol were able to pull the adversary to a location further away from the real source nodes to prolong the SP.

Outside the blast ring, the DDR achieves significantly longer SP than the TDR and FPR protocols because the progress of the adversary back tracing attack is significantly hindered near the sink node regions. When source nodes are located outside the blast ring, the DDR creates two isolated routing paths. One path is used to route packets from the fake source node and the other path routes packets from the real source node. Both routes create a pull effect on the eavesdropping adversary. Furthermore, both real packets and fake packets are flooded inside the blast ring to prolong the SP. However, for source nodes with source-sink distance greater than 52 hops, the TDR protocol achieves longer SP than the other protocols. The main reason for the longer SP is that, in that region, TDR broadcasts a considerable amount of fake packet traffic to pull the adversary away from the real

조선대학교
CHOSUN UNIVERSITY

source node. Also, TDR broadcasts fake packet traffic near the phantom node to increase the adversary obfuscation effect at the phantom node. On the other hand, DDR isolates the fake packets from the phantom node. Consequently, in DDR, the adversary has a higher probability of capturing the source node in a short time if it successfully captures the phantom node.

The PRR protocol employs only one fake packet source at a time for each real source node. As a result, the obfuscation effect on the adversary is reduced and the SP is only slightly longer than RIN. Furthermore, in PRR, the fake packet sources are located near the sink node, making the fake packet routes short and easy to predict by the adversary. After sometime of back tracing, the adversary can easily identify the fake packet sources and isolate the fake packet routes. If the fake packet routes are obvious, the adversary can focus the attack on the real packet routes and increase the probability of success in the back tracing attack. Consequently, the SP is reduced. Moreover, in the PRR protocol, the fake packet sources are isolated from the real packet sources. These noticeable locations may make it easy for the adversary to predict the real packet routes and make the adversary back tracing attack a less complex task. As a result, the SP is reduced.

In the RIN protocol, packets are routed from the source node to the sink node through a randomly selected intermediate node. However, packet routing between the intermediate nodes and sink node is done through less random routing paths. Consequently, the RIN protocol achieves significantly short SP because it becomes easy for the adversary to back trace the less random routing paths. Furthermore, when the source node is near the sink node, there is a high probability of the selected intermediate node to be located near the sink node. If the intermediate node is located near the sink node, short routing paths are created. The short routing paths are less effective at obfuscating the adversary. Therefore, short SP is achieved. For all the protocols, the SP improves with the increase in source-sink distance because the adversary back tracing attack becomes more complex with longer routing paths. When the source node is located at a long distance from the sink node, the routing paths can be created with high path diversity and it becomes more challenging for the adversary to successively perform back tracing attacks. Hence, long SP is achieved.

To evaluate the capability of the protocols to provide effective SLP protection for prolonged

조선대학교
CHOSUN UNIVERSITY

operational times, the SP of the protocols was observed at different network operation durations. Analysis was done for source nodes at source-sink distance of 35 hops. The results are shown in Fig. 3.2 (b). The results show that the SP of the PRR, and RIN protocols does not vary very much throughout the 800 rounds. For TDR, FPR and DDR, the protocols achieve reduced SP when the number of rounds increases. The main reason for the reduced SP in TDR is that, TDR relies on obfuscating the adversary by broadcasting a large amount of fake packet traffic in the diversionary routes. When the network has operated for many rounds, some of the sensor nodes drain their energies and become dead nodes. Therefore, the number of active sensor nodes in the regions of the diversionary routes is reduced and small number of fake packets is broadcasted. Subsequently, the adversary becomes less obfuscated and the SP is reduced. The main reason for the reduced SP in FPR is that, the number of candidate fake packet sources is highly dependent on the value of the sensor node residual energy. For a sensor node to become a candidate fake packet source, one of the criteria is that the value of the sensor node residual energy must be greater than a threshold value. In our analysis, a threshold value of 0.25 J was assumed. At 800 rounds, the residual energy of some of the sensor nodes was less than the threshold value. As a result, small numbers of fake packet sources were generated. Subsequently, the amount of fake packet traffic was reduced, the adversary became less obfuscated, and the SP was reduced.

For DDR, the protocol depends highly on flooding mechanism to obfuscate the adversary. When the source nodes are outside the blast ring, DDR ensures both real packets and fake packets are flooded inside the blast ring. As a result, a significant amount of sensor nodes energy is consumed to transmit a single packet. Consequently, the sensor nodes drain their energies at a fast rate. At 800 rounds, a significant number of sensor nodes inside the blast ring have exhausted their battery power. Therefore, a reduced number of sensor nodes can participate in the flooding mechanism. Hence, the adversary becomes less obfuscated and the SP is reduced. The SP of the PRR protocol does not vary very much during the 800 rounds because PRR broadcasts one fake packet for a time period. Therefore, the sensor nodes drain their energies at a slow rate. Hence, a great number of sensor nodes take part to route packets and obfuscate the adversary for prolonged periods of time. Similar to PRR,

조선대학교
CHOSUN UNIVERSITY

the SP of the RIN protocol does not vary during the 800 rounds because the routing strategy of RIN ensures that the sensor nodes drain their energies at a slow rate. Therefore, sensor nodes can participate to route packets and obfuscate the adversary for prolonged periods of time. However, the SP of RIN is significantly short.

In the experiment scenarios for the results in Fig. 3.2 (c), the SP was observed under varied source rate. The source rate was varied between 1 and 6 packet/second. The source nodes were randomly positioned at source-sink distance of 35 hops. It is shown in Fig. 3.2 (c) that all the protocols achieve reduced SP as the source rate increases. The main reason for the reduced SP is that, as more packets are generated in the network, the packet traffic is increased and the probability that the adversary captures successive packets is also increased. At higher data rates, the cautious adversary is capable of capturing enough number of successive packets to allow it to make a successful back tracing attack within a short period of time. For DDR protocol, it was observed that the SP was significantly reduced when the adversary was able to locate the initial blast ring node which received packets from the phantom node. In Fig. 3.2 (c), such scenario was observed at the source rate of 4 packet/second. The main reason for the sharp reduction in SP once the initial blast ring node was located is that, the routing paths for the real packets and fake packets are isolated. Therefore, DDR does not distribute fake packets near the phantom nodes. Consequently, the adversary obfuscation effect between the phantom nodes and source nodes is reduced. Thus, it becomes easy for the adversary to successfully locate the source nodes and the SP is reduced. For RIN protocol, at high data rates, the adversary is capable of locating the source nodes within a significantly short period of time due to the easily predictable routing paths.

- **Capture Ratio**

CR is the ratio of the number of experiments where the adversary ends in capturing the source node to the total number of experiments. To locate the source node, adversary must back trace the packet routes and reach at the location of the source node. Thus, adversary must co-locate with the source node. To compute the CR, equation (8) was assumed [93].

조선대학교
CHOSUN UNIVERSITY

$$CR = \frac{Number\ of\ experiments\ ending\ with\ captured\ source\ node}{Total\ number\ of\ experiments} \quad (8)$$

The CR and SP parameters have an inversely proportional relationship. When the SP of a protocol is maximized, the CR is minimized, as shown in equation (9).

$$\max\ (SP) = \min\ (CR) \quad (9)$$

Fig. 3.3 shows the privacy performance of the protocols using the CR metric. In the experiment scenarios for the results in Fig. 3.3 (a), CR was observed against varied network size. The parameter ‘‘Length’’ represents the side length of the network. The source nodes were randomly positioned at a source-sink distance of 40 hops. The results show that the CR for DDR, PRR, FPR, and RIN does not vary very much when the network size is varied. The main reason is that, if the source-sink distance is fixed, the change in network size causes insignificant effect on the location configuration of the fake packet sources in PRR and FPR or intermediate nodes in RIN. Therefore, the configurations of the routing paths remain the same and the CR does not vary significantly. For DDR, when the radius of the blast ring is kept constant, the change in the network size causes insignificant effect on the packet routing algorithm and the CR remains unchanged. However, for TDR, the increase in network size causes a reduction in CR. This is mainly due to the fact that, TDR locates the fake packet sources in the diversionary routes, towards the network border regions. If the

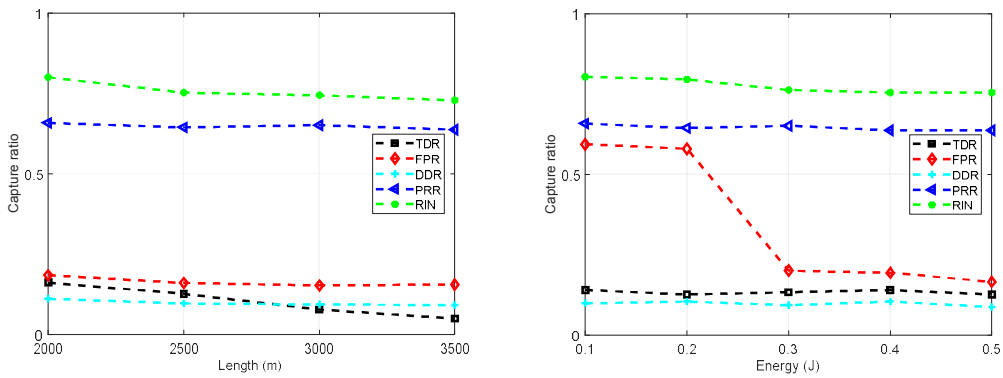


Figure 3.3: Privacy performance of the routing protocols. (a) CR against network size. (b) CR against energy of sensor node.

조선대학교
CHOSUN UNIVERSITY

intermediate node is kept at a constant location in the network, the length of the diversionary routes increases with the increase in network size. As a result, the ability of the protocol to obfuscation the adversary is increased. When the adversary is tricked into tracing back the fake packets which are transmitted in the long diversionary routes, it is steered far away from the real source node and the CR is reduced.

In the experiment scenarios for the results in Fig. 3.3 (b), CR was observed against the residual energy of the sensor nodes. For analysis, we observed the residual energy of 90% of the sensor nodes which were located within 6 hops from the source nodes. The source nodes were located at sourcesink distance of 40 hops. The results in Fig. 3.3 (b) show that, the CR for the TDR, DDR, PRR, and RIN protocols does not vary very much when the residual energy of the sensor nodes is varied. However, for the FPR protocol, the CR was high when the residual energy of the sensor nodes was below the threshold value of 0.25 J. The reason for the increased CR below 0.25 J is that, FPR uses the residual energy as one of the criteria for the selection of candidate fake packet sources. When the residual energy of some of the sensor nodes was below the threshold value, smaller numbers of fake packet sources were selected. Consequently, reduced amounts of fake packet traffic were broadcasted and the adversary was less obfuscated. Hence, the adversary was able to improve its attack success rate and high CR was achieved. When the residual energy of the sensor nodes was above the threshold value of 0.25 J, increased numbers of sensor nodes were able to meet the conditions for becoming candidate fake packet sources. Subsequently, large amounts of fake packet traffic were broadcasted in the network. As a result, the adversary became effectively obfuscated and the CR was reduced.

- **Detection Ratio**

DR is the ratio between the number of packets detected by the adversary and the total number of packets sent by the source node during the back tracing attack. To compute the DR, equation (10) was assumed.

At all times, the adversary uses its spectrum analyzer to eavesdrop on the communication and detect the packets which are transmitted between the sensor nodes. Since the adversary hearing range

조선대학교
CHOSUN UNIVERSITY

is assumed to be equal to the sensor node communication range, a packet is detected when it is received from an immediate sender node which is located 1 hop away from the adversary location.

$$DR = \frac{Number\ of\ detected\ packets}{Total\ number\ of\ packets\ sent\ by\ source\ node} \tag{10}$$

To successfully locate the real source nodes, the adversary must detect a sufficient number of successive packets from the source nodes and make significant progress in the back tracing attack. However, when the routing paths have high path diversity, the number of detected packets is significantly reduced. Consequently, the DR is reduced and SP is increased. Therefore, minimum DR corresponds to maximum SP as shown in equation (11). Thus, when the DR is close to 0, the SP is prolonged and the level of SLP protection is improved. However, when the DR is close to 1, the SP is minimized and the level of SLP protection is reduced.

$$\min\ (DR) = \max\ (SP) \tag{11}$$

Fig. 3.4 shows the privacy performance of the protocols using the DR metric. In the experiment scenarios for the results in Fig. 3.4 (a), DR was computed for source nodes at different source-sink distances. 400 packets were sent from each source node. The source rate was fixed at 1 packet/second. The results show that the DR for the TDR, FPR, PRR and RIN protocols tend to decrease when the source-sink distance is increased. The main reason for the decrease in DR is that, the routing paths

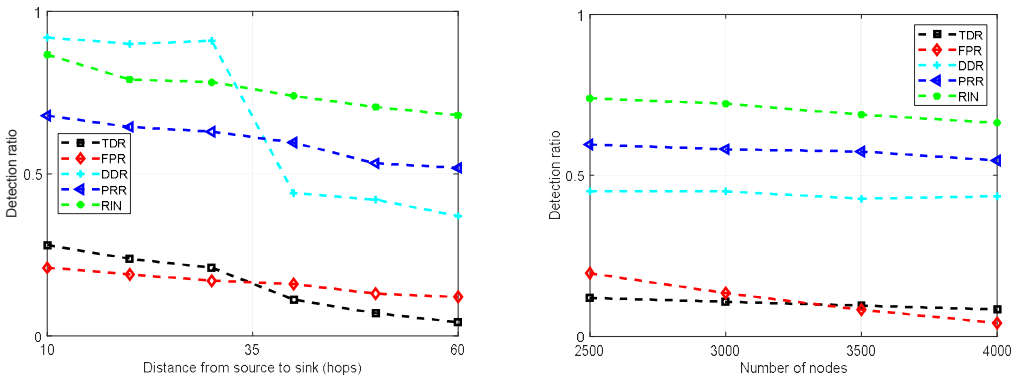


Figure 3.4: Privacy performance of the routing protocols. (a) DR against source-sink distance. (b) DR against node density.

조선대학교
CHOSUN UNIVERSITY

become more diverse when the distance between the source nodes and sink node increases. As a result, the routing paths become more obfuscating to the adversary and the DR is reduced. The results also show that FPR achieves lower DR than TDR when the sourcesink distance is below 34 hops. This is mainly due to the fact that FPR employs larger amounts of fake packet traffic in the near-sink regions to achieve higher levels of adversary obfuscation and lower DR.

To analyze the DR of the DDR protocol, all source nodes with source-sink distance less or equal to 30 hops were assumed to be located inside the blast ring. It is shown in Fig. 3.4 (a) that the adversary was able to achieve high DR when the source nodes were located inside the blast ring. This is mainly due to the flooding of the packets inside the blast ring. When the adversary is initially located at the sink node, it is capable of detecting a significant number of packets from the source nodes to increase its DR. For the source nodes outside the blast ring, the DR is significantly reduced. The main reason for the reduced DR is that, outside the blast ring, the DDR protocol creates two isolated routing paths. One path is used to route packets from the fake source node and the other path routes packets from the real source node. Furthermore, both fake packets and real packets are flooded when they arrive inside the blast ring. As a result, the fake packets and real packets are transmitted to the sink node with equal probability. Therefore, the eavesdropping adversary has a reduced chance of detecting the real packets and the DR is reduced. Unlike the TDR and FPR protocols, the DDR protocol can achieve long SP despite the high DR. The main reason for the high DR and long SP is that, the adversary is flooded with many packets from multiple immediate sender nodes. Given that probabilistic flooding is used, the adversary is encountered with a complex back tracing task and long SP is achieved. Hence, the obfuscation ability of the DDR protocol is high despite the high DR.

In the experiment scenarios for the results in Fig. 3.4 (b), DR was computed under varied node density. The source nodes were assumed at source-sink distance of 40 hops. The number of sensor nodes in the network was varied between 2500 and 4000. The source rate was fixed at 1 packet/second. The results show that, at source-sink distance of 40 hops, the DR for the TDR, DDR, PRR and RIN protocols does not vary very much when the number of sensor nodes in the network is increased. However, the DR for the FPR protocol tends to decrease when the number of nodes is

조선대학교
CHOSUN UNIVERSITY

increased. The main reason for the reduced DR is that, FPR randomly selects candidate fake packet sources from the neighborhood regions of the source node. When the number of sensor nodes increases, it increases the probability of a higher number of candidate fake packet sources. When a large number of fake packet sources is selected, large amounts of fake packet traffic can be broadcasted to obfuscate the adversary. Consequently, the DR is reduced. For the DDR protocol, when the number of nodes is increased, the DR remains unchanged because both fake packets and real packets are flooded with equal probability.

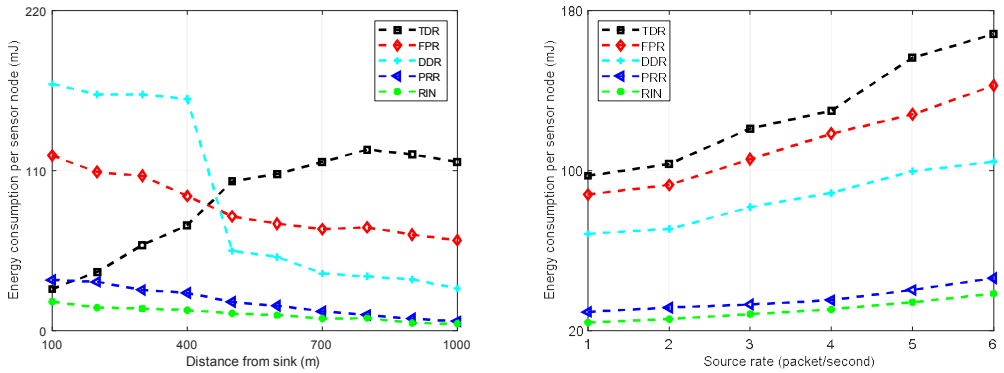
- **Energy Consumption**

Energy consumption is the energy consumed by the sensor nodes for transmitting and receiving packets. It is assumed that packet transmission and reception are the most energy consuming tasks for the sensor nodes [94]. Thus, the energy consumption or energy efficiency of a protocol may be indicated by the number of packets which are being transmitted in the network [76]. Therefore, the fake packet-based protocols are prone to low energy efficiency because they transmit large amounts of packet traffic.

In the experiments, the energy consumption model in section 2.3 was assumed. Fig. 3.5 shows the energy consumption performance of the protocols. In the experiment scenarios for the results in Fig. 3.5 (a), 25 source nodes were assumed at different source-sink distances. 1000 packets were sent from each source node to the sink node and the energy consumption per sensor node was computed. For the DDR protocol, the boundary of the blast ring was assumed at 400 m from the sink node. The results in Fig. 3.5 (a) show that the TDR protocol has the highest energy consumption near the network border regions while the DDR protocol has the highest energy consumption in the near-sink regions. Also, the FPR incurs significantly high energy consumption. The main reason for such kind of distribution in the energy consumption is that, the TDR broadcasts large amounts of fake packet traffic in the diversionary routes, towards the network border. In the near-sink regions, TDR employs a backbone route to route real packets. It does not broadcast any fake packets in the near-sink regions. On the other hand, the DDR protocol employs packet flooding mechanism in the near-sink regions

조선대학교
CHOSUN UNIVERSITY

which causes significantly high energy consumption. Moreover, both real packets and fake packets are flooded when the source nodes are located outside the blast ring. Outside the blast ring region, the energy consumption of DDR is significantly reduced because the protocol employs only one fake packet for each real packet.



(a) (b)

Figure 3.5: Energy consumption of the protocols. (a) Energy consumption against source-sink distance. (b) Energy consumption against source rate.

The FPR protocol distributes a significant amount of fake packet traffic throughout the network domain, depending on the location of the source node. The fake packets are routed towards the sink node. Hence, higher energy consumption in the near-sink regions. The PRR protocol employs one fake packet source for a period of time. As a result, it broadcasts significantly lower amounts of packet traffic than the FPR. Furthermore, the fake packets are broadcasted in the near-sink regions. Hence, PRR incurs considerably lower energy consumption than FPR. The RIN protocol has the lowest energy consumption because it does not involve the transmission of fake packet traffic. Only real packets are transmitted between the sensor nodes. As a result, the sensor nodes consume less energy. Comparing the results in Fig. 3.2 (a) and Fig. 3.5 (a), it is shown that the ability of the TDR and FPR protocols to achieve strong SLP protection is highly influenced by the amount of fake packet traffic. As a result, the energy cost of TDR and FPR protocols is high.

In the experiment scenarios for the results in Fig. 3.5 (b), energy consumption per sensor node was observed for sensor nodes located at 500 m from the sink node. The energy consumption was

조선대학교
CHOSUN UNIVERSITY

measured against varied source rate. The source rate was varied between 1 and 6 packet/second. The results in Fig. 3.5 (b) show that the energy consumption of the protocols tend to increase when the source rate is increased. The main reason for the increase in the energy consumption is that, when more packets are generated per second, the packet traffic in the network is increased. As a result, the sensor nodes spend more energy to transmit the packets in the network. For the TDR and FPR protocols, the energy consumption increases at a fast rate because of the presence of large amounts of fake packet traffic in the network. With the large amounts of fake packet traffic, the number of packet collision and packet retransmission events is increased. Consequently, the energy consumption is increased. In DDR, packet collision and packet retransmission events occur due to the flooding of real packets and fake packets. Subsequently, the energy consumption of DDR increases at a faster rate than in PRR and RIN protocols. The energy consumption for the PRR and RIN protocols increases at a slow rate. This is due to the fact that, at 500 m from the sink node, PRR and RIN employ routing strategies with smaller amounts of packet traffic than in the TDR and FPR protocols. Therefore, fewer events of packet retransmission occur and the sensor nodes spend less energy.

- **Network Lifetime**

To analyze the network lifetime of the protocols, the network lifetime model in section 2.4 was assumed. In the experiments, all the sensor nodes with source-sink distance less or equal to 20 hops were assumed to be located in the near-sink region. The source nodes were randomly distributed at various source-sink distances. 2000 packets were sent from each source node. The network lifetime was observed under varied source rate. Fig. 3.6 shows the results of the network lifetime analysis. It shows that the TDR and RIN protocols achieve long network lifetime. Also, it is shown that the TDR and RIN protocols have comparable network lifetime performance. The TDR achieves long network lifetime because it employs shortest routing paths in the near-sink regions. Furthermore, TDR broadcasts small amounts of packet traffic in the near-sink regions to minimize the sensor node energy consumption. RIN protocol achieves long network lifetime because it employs relatively short

조선대학교
CHOSUN UNIVERSITY

routing paths between the intermediate nodes and sink node. Similar to TDR, the RIN protocol distributes relatively small amounts of packet traffic in the near-sink regions to minimize the sensor node energy consumption.

The FPR and PRR protocols employ both, real packets and fake packets in the near-sink regions. Hence, more energy is consumed by the sensor nodes and the network lifetime is reduced. Moreover, the FPR employs larger amounts of fake packet traffic than the PRR. Consequently, the FPR achieves reduced network lifetime. The DDR achieves significantly short network lifetime because it employs packet flooding mechanism to route fake packets and real packets in the nearsink regions. When packet flooding is used, a large number of sensor nodes participate in transmitting each packet. As a result, the sensor nodes drain their energies at a fast rate and the network lifetime is affected.

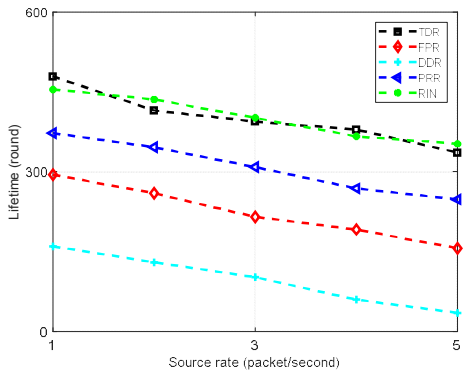


Figure 3.6: Network lifetime under varied source packet rate.

The results also show that the network lifetime of the protocols tend to decrease when the source rate is increased. The main reason for the reduced network lifetime at higher source rates is that, more packet traffic is broadcasted in the network per unit time when the source rate is high. Therefore, the sensor nodes consume more energy per unit time and the network lifetime is reduced.

- **Packet Delivery Ratio**

PDR is the ratio between the total number of packets successfully delivered at the destination sink node and the number of packets transmitted by the source nodes. Equation (12) was used to compute the PDR [29]. In the equation, P_{Rec} is the total number of data packets successfully received by the

조선대학교
CHOSUN UNIVERSITY

destination sink node. P_{Trans} is the number of packets transmitted by the source nodes. n is the number of source nodes.

$$PDR = \frac{P_{Rec}}{\sum_{i=1}^{n} P_{Trans_i}} \tag{12}$$

Fig. 3.7 shows the PDR performance of the protocols. In the experiment scenarios for the results in Fig. 3.7 (a), 20 source nodes were assumed at various source-sink distances. Each source node transmitted 100 packets to the sink node. The source packets were generated at a rate of 1 packet/second. The results in Fig. 3.7 (a) show that the PDR of the protocols tends to decrease when the source-sink distance is increased. The main reason for the reduced PDR is that, the routing paths become longer when the source-sink distance is increased. As a result, the probability of packet loss events increases and the PDR is reduced. The TDR and FPR protocols achieve significantly low PDR for source nodes which are located at long distances from the sink node due to the distribution of large amounts of fake packet traffic. The probability of packet collision and packet loss events increases when large amounts of fake packet traffic is distributed in the network.

The PRR protocol achieves higher PDR than the TDR and FPR protocols because it broadcasts only one fake packet for each real packet transmission. Furthermore, the fake packet sources in PRR are isolated from the real source nodes. As a result, less packet collision and packet loss events occur.

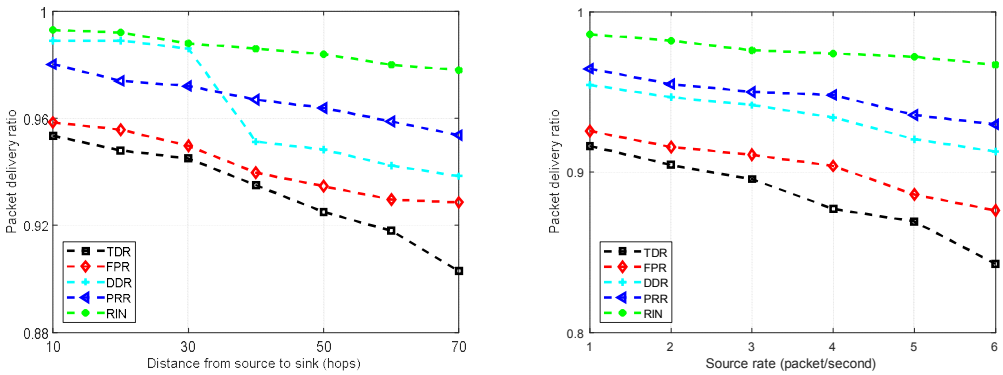


Figure 3.7: Packet delivery ratio of the routing protocols. (a) PDR against varied source-sink distance. (b) PDR against varied source rate.

조선대학교
CHOSUN UNIVERSITY

To analyze the PDR of the DDR protocol, the boundary of the blast ring was configured at source-sink distance of 30 hops. The results show that the DDR protocol is capable of achieving high PDR inside the blast ring due to packet flooding. However, the PDR is reduced when the source nodes are located outside the blast ring. The reduced PDR is mainly due to the increased probability of packet collision events which occur when both real and fake packets are flooded inside the blast ring. The RIN protocol achieves significantly high PDR because it incurs reduced number of packet loss events.

In the experiment scenarios for the results in Fig. 3.7 (b), the PDR performance was observed for the source nodes located at source-sink distance of 35 hops. The source rate was varied between 1 and 6 packet/second. The results show that the PDR tends to decrease when the source rate is increased. The reduction in PDR is due to the fact that more packets are generated in the network when the source rate is high. Consequently, the probability of packet collision and packet loss events is increased and the PDR is reduced. The PDR of the TDR and FPR protocols decreases at a fast rate due to the high probability of packet collision events. For DDR, at source-sink distance of 35 hops, the fake packets and real packets have equal probability of transmission through packet flooding. Therefore, the probability of packet collision is high and the PDR is reduced. The PRR protocol has a low probability of packet collision events. As a result, the PDR decreases at a slower rate than in TDR and FPR protocols. The PDR of the RIN protocol decreases at a much slower rate than in TDR and FPR because RIN employs less random routing paths with small amounts of packet traffic. As a result, the increase in packet rates causes less impact on the PDR performance.

- **End-to-End Delay**

EED is the time taken for a packet to be transmitted across the network from a source node to the destination sink node. Equation (13) was used to compute the EED [29]. T_{Rec} is the time when a data packet is received by the sink node. T_{Trans} is the time when a data packet is transmitted by a source node. P_{Rec} is the total number of data packets received at the destination sink node.

$$EED = \frac{\sum_{i=1}^{P_{Rec_i}} (T_{Rec_i} - T_{Trans_i})}{P_{Rec}} \tag{13}$$

조선대학교
CHOSUN UNIVERSITY

Fig. 3.8 shows the EED performance of the protocols. In the experiment scenarios for the results in Fig. 3.8 (a), 20 source nodes were assumed at various source-sink distances. Each source node transmitted 100 packets to the sink node. The source packets were generated at a rate of 1 packet/second. It is shown in the Fig. 3.8 (a) that the EED tends to increase when the source-sink distance is increased. This is mainly due to the fact that increased number of packet forwarding instances (hops) occur when the distance between the source node and sink node is long. Some EED is incurred at each hop. Consequently, the EED increases with the increase in hop distance. The EED for TDR and FPR is relatively long because of the occurrence of packet collision events. When many packet collision and packet loss events occur, the instances of packet retransmission events increaese. Subsequently, the EED is increased. The DDR and PRR protocols employ small amounts of fake packet traffic to ensure fewer events of packet collision and retransmission. As a result, the EED is not significantly long. The PRR achives slightly shorter EED than DDR because it isolates the fake packet routes from the real packet routes to reduce the packet collison events and improve the EED. The routing paths of the RIN protocol are less random. Moreover, the RIN protocol transmits only real packets to ensure reduced number packet loss and retransmission events. Hence, relatively short EED is achieved by the RIN protocol.

In the experiment scenarios for the results in Fig. 3.8 (b), the EED performance was observed

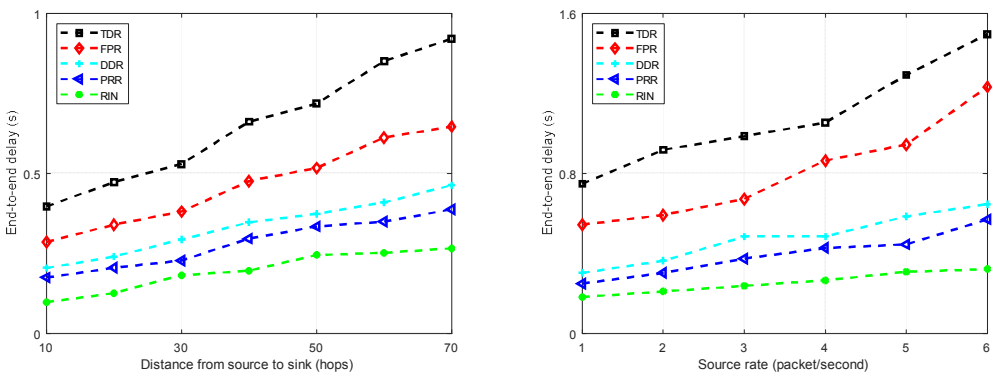


Figure 3.8: End-to-end delay of the routing protocols. (a) EED under varied source-sink distance. (b) EED under varied source rate.

조선대학교
CHOSUN UNIVERSITY

for source nodes with source-sink distance of 40 hops. The source rate was varied between 1 and 6 packet/second. It is shown in Fig. 3.8 (b) that the EED tends to increase when the source rate is increased. This is due to the fact that the probability of packet collision, packet loss, and packet retransmission events is increased when more packets are generated per second. The EED is significantly affected when many packet retransmission events occur. The EED of TDR and FPR protocols increases at a fast rate due to the presence of large amounts of fake packet traffic. The large amounts of fake packet traffic triggers increased number of packet collision events. Hence, increased number packet retransmission events occur when the source rate is high.

3.5. Summary and Recommendations

Table 3.2 provides a summary of the findings from the performance analysis. The SLP protection, energy consumption, and network lifetime performance are summarized. Packet delivery reliability is included in the summary. The packet delivery reliability is measured by the PDR. High PDR corresponds to high delivery reliability while low PDR corresponds to low reliability.

Comparing the performance of the TDR, DDR, PRR and FPR protocols with the performance of the traditional RIN protocol, it is presented in the Table 3.2 that the TDR, DDR, PRR and FPR protocols achieve improved SLP protection. However, the protocols incur costs in energy consumption, network lifetime, and delivery reliability. The TDR protocol shows some interesting performance features for energy consumption and network lifetime. The protocol is capable of achieving long network lifetime despite the high energy cost. It guarantees long network lifetime by consuming most of the energy in the near network border regions. In the nearsink regions, it employs short routing paths to minimize the energy consumption. Minimizing the energy consumption in the near-sink regions is particularly useful in improving the network lifetime. On the other hand, the DDR protocol disregards the idea of minimizing the energy consumption in the near-sink regions. As a result, the network lifetime of DDR is shortened. Another interesting observation was made from the performance analysis of the TDR, FPR, and DDR protocols. It was observed that, although the TDR, FPR, and DDR protocols can guarantee effective SLP protection, the privacy protection

조선대학교
CHOSUN UNIVERSITY

Table 3.2: Summary of the results.

Protocol	SLP Protection	Energy Consumption	Network Lifetime	Delivery Reliability
TDR [32]	Significantly higher than RIN in near network border regions due to distribution of large amount of fake packet traffic in diversionary routes.	Significantly higher than RIN due to distribution of large amount of fake packet traffic in diversionary routes.	Comparable with RIN due to minimized energy consumption in the near-sink regions.	Significantly lower than RIN due to packet collision events.
DDR [61]	Significantly higher than RIN due to flooding of fake and real packets inside the blast ring.	Significantly higher than RIN due to packet flooding inside the blast ring.	Significantly shorter than RIN due to flooding of fake and real packets inside the blast ring.	Lower than RIN due to packet collision events when source node is outside of the blast ring.
FPR [44]	Significantly higher than RIN due to distribution of fake packet traffic throughout the network domain.	Significantly higher than RIN due to distribution of fake packet traffic throughout the network domain.	Shorter than RIN due to distribution of fake packet traffic throughout the network domain.	Significantly lower than RIN due to packet collision events.
PRR [62]	Slightly higher than RIN due to distribution of small amount of fake packet traffic.	Slightly higher than RIN due to distribution of fake packet traffic in the near-sink regions.	Shorter than RIN due to distribution of fake packet traffic in the near-sink regions.	Slightly lower than RIN due to packet collision events.
RIN [88]	Low.	Low.	Long.	High.

may be short-term.

Based on the analysis results and observations, we present some recommendations to address the limitations of the protocols. To minimize the communication cost while achieving high levels of adversary obfuscation, the DDR, TDR, PRR, and FPR protocols can integrate node offset angle routing strategies in their routing algorithms. The effectiveness of the node offset angle routing algorithms was demonstrated in [29], [34], and [94]. To improve the privacy performance of the PRR protocol, the real packet routes and fake packet routes must be homogenous. When the routes are homogenous, the adversary becomes more obfuscated and high levels of SLP protection can be achieved. Furthermore, a more strategic location of the fake packet sources is required in the PRR protocol. Currently, the fake packet sources are isolated from both, real source nodes and phantom nodes. To improve the privacy performance, the location of the fake packet sources must provide some adversary obfuscation effect near the phantom nodes. On the other hand, the TDR protocol does not isolate the fake packet sources from the phantom nodes. As a result, TDR is capable of providing effective adversary obfuscation even when the phantom node has been captured by the adversary. Some of the existing studies have presented a few techniques which may be useful in

조선대학교
CHOSUN UNIVERSITY

addressing the limitations of the protocols. The DDR and FPR protocols can adopt the routing techniques in [43], [83] to address the limitation of exhaustively high energy consumption in the near-sink regions. Also, some of the limitations of the TDR and PRR protocols were recently addressed in [29].

The performance of the FPR protocol can also be improved by improving the algorithm for selecting candidate fake packet sources. Currently, a simple technique is used where the sensor node residual energy is used as one of the criteria for selecting the candidate fake packet sources. The technique is not very effective since it results in reduced performance when the residual energy of the sensor nodes is below a threshold value. Instead, a criterion such as hop count can be used. As an example, together with the other criteria, a sensor node may become a candidate fake source depending on the value of its hop count to the sink node. If a sensor node meets the other criteria and has longer hop distance to the sink node than the source node itself, it becomes a candidate fake source, otherwise it ignores the fake source request. In such scenarios, the selection of the candidate fake sources becomes less dependent on the sensor node energy. Subsequently, effective number of fake packet sources may be guaranteed for longer durations. An improved algorithm for selecting candidate fake packet sources was proposed in [31]. The performance of FPR protocol can also be improved by using energy harvesting wireless sensor networks (EHWSNs) schemes. Using the techniques discussed in [84], EHWSNs may be utilized to improve the availability of effective candidate fake packet sources by ensuring the residual energy of the sensor nodes is maintained above the threshold values.

The TDR, DDR, and FPR protocols incur considerably high energy consumption. Consequently, the privacy protection of the protocols is short-lived. Therefore, TDR, DDR, and FPR protocols may not be practical in monitoring systems which require effective SLP protection for prolonged time periods. Thus, to enable long-term monitoring, the TDR, DDR, and FPR protocols may require additional network and hardware configurations to manage the energy of the sensor nodes. The work in [84], [85], [95]-[98] presented some of the techniques for sensor node energy management in energy hungry WSNs. EHWSNs can be used to replenish the energy of the sensor

조선대학교
CHOSUN UNIVERSITY

nodes to ensure effective long-term monitoring. A trust-based routing protocol was proposed in [98] to ensure security of data and maximized use of available energy in EHWSNs. Some state-of-the-art energy management techniques were presented in [84], [85], [96], and [97]. An on-board recharging circuit to harvest energy from any unregulated energy source was discussed in [85]. In [96], rechargeable WSNs used the sensor nodes to harvest energy from both, solar and the radio frequency transmissions of their neighbors. However, it is important to note that the EHWSNs may not be infinitely supplemented with energy because energy harvesting requires additional hardware cost.

3.6. Remarks

Fake packet-based SLP protocols are analyzed. Experimental evaluation of the SLP protection, energy consumption, network lifetime, EED, and PDR performance is done. Various experiment scenarios are assumed with varied network parameters and configurations. The experiment results support some interesting conclusions. (1) The level of SLP protection for the protocols is strongly influenced by the amount of the fake packet traffic in the network. (2) Integrating fake packet routing and packet flooding techniques can improve the privacy performance of a protocol. However, high energy cost is incurred and the network lifetime is shortened. (3) Using a threshold value of the sensor node residual energy as a criterion for selecting candidate fake packet sources may result in short-term SLP protection. (4) In many scenarios, the protocols maintain high levels of adversary obfuscation when the fake packet sources are not isolated from the phantom nodes. However, such configurations often result in reduced packet delivery reliability due to increased number of packet collision events. (5) Increasing the source packet rate can impact some negative effects on the privacy performance of the protocols. (6) Long source-sink distances allow for improved adversary obfuscation effects and strong SLP protection. (7) The protocols have high probability of packet collision and packet loss events which may result in reduced packet delivery reliability. (8) The energy consumption, network lifetime, EED, and PDR performance of the protocols can be affected when the source packet rate is increased.

조선대학교
CHOSUN UNIVERSITY

Chapter 4

Proposed Source Location Privacy Protocols

This chapter presents several new routing algorithms. New SLP routing protocols are proposed to achieve improved performance and outperform some of the existing SLP routing protocols. Two studies are presented:

4.1. Secure Routing Protocols for Source Node Privacy Protection in Multi-Hop Communication Wireless Networks

4.2. Regulating the Packet Transmission Cost of Source Location Privacy Routing Schemes in Event Monitoring Wireless Networks

4.1. Secure Routing Protocols for Privacy Protection

4.1.1. Background

WSNs are resource-constrained with limited processing power, memory, battery, and bandwidth. In monitoring applications, the WSNs are often deployed in open and inaccessible locations that are difficult to control, manage or safeguard from unauthorized physical access [28], [38]. Consequently, packet transmission in WSNs is susceptible to eavesdropping adversaries. Furthermore, the transmissions may result in lost or corrupted packets due to routing failures or collisions. Subsequently, the design of security protocols for WSNs must take into consideration the performance features of the WSNs. The networks may be faced with many types of attacks including privacy attacks where an adversary focuses on monitoring and analyzing the network traffic to obtain critical information such as the location information of important nodes [38]. To address the issue of privacy attacks in WSNs, numerous SLP protocols have been proposed in the literature. SLP protection warranties the security of the source nodes by ensuring the information which is gathered by the source nodes is only observed or deciphered by the authorized parties [36], [37], [40], [57], [61], [99].

There exist many types of SLP routing protocols [28], [36], [37]. In this study, we focus on routing protocols which are based on phantom routing and fake packet routing strategies. In the

조선대학교
CHOSUN UNIVERSITY

phantom routing strategy, phantom nodes are selected and packets from the source nodes are first sent to the phantom nodes through random routing paths. Then, the packets are transmitted from the phantom node to the destination sink node through flooding, single-path routing, or some alternative strategies [28], [89]. The phantom routing strategy is simple and offers low SLP protection when used in its simple form [45]. In the fake packet routing strategy, fake sources are designed to mimic the functions of the real source nodes. The fake sources transmit fake packets simultaneously with the transmission of real packets from the real source nodes [36], [38], [76], [86], [87]. Often, the fake packets are of the same size as the real packets and they are transmitted at the same transmission interval and transmission rate as the real packets. Fake packet routing protocols are effective at preserving the SLP because it is difficult for adversaries to differentiate the real packets from the fake packets. However, to effectively obfuscate an adversary, the protocols often distribute a large amount of fake packet traffic in the network. Consequently, the protocols incur exhaustive energy consumption, routing congestion problems, packet collisions and packet loss events [28], [41], [45], [65], [100]. As a result, the PDR and EED performance of the protocols are affected [36].

There exist several SLP routing protocols which integrate the phantom routing and fake packet routing strategies. Examples of the protocols include the tree routing protocol with diversionary routes (TreeR) [32] and the probabilistic routing protocol (ProbR) [62]. The TreeR protocol achieves strong SLP protection by integrating many routing strategies. It employs phantom nodes which are located far away from the source node. It creates backbone routes which are directed to the network border with many diversionary routes. At the end of each diversionary route, fake packets are emitted periodically to obfuscate the adversary. The protocol incurs significant energy consumption, low PDR and long EED due to the distribution of large amount of fake packets, some long routing paths, and long diversionary routes which diverge to the network border. The ProbR protocol considers transmission of two types of packets, fake packets and real packets as an efficient strategy to obfuscate an eavesdropping adversary. Real sources send packets to the sink node through phantom nodes. Concurrently, fake packets are transmitted to the sink node. The protocol achieves less effective SLP protection compared to the TreeR protocol.

조선대학교
CHOSUN UNIVERSITY

The TreeR and ProbR protocols have three main differences in their key features: (1) the TreeR employs fake source packets far away from the sink node, while ProbR employs fake source packets in the near-sink regions, (2) TreeR distributes a large amount of fake packets in the network while ProbR distributes only one fake packet at a time interval, and (3) TreeR distributes some fake packets near the phantom routes while ProbR locates the fake packet sources away from the phantom nodes. In this study, the performance of the TreeR and ProbR protocols is analyzed using five important performance metrics: safety period, attack success rate, energy consumption, PDR and EED. Furthermore, two new phantom-based routing protocols, 2-Level phantom with a backbone route (PhaT), and 2-Level phantom with a pursue ring (PhaP) are proposed to address the limitations of TreeR and ProbR protocols, respectively. The proposed protocols introduce a new second level phantom node which is designed to provide second level adversary confusion phase. First level adversary confusion phase is provided by the first level phantom nodes which are adopted from the already existing phantom nodes in TreeR and ProbR. If an adversary embarks on back tracing the routing paths of the proposed protocols, it is encountered with two levels of adversary confusion phases. Consequently, the adversary makes insignificant progress towards the source node and strong SLP protection is guaranteed.

The packet routing process of the proposed PhaP and PhaT protocols is done in three phases. Phase 1 involves the process of packet routing between the source node and the first level phantom node. The strategies for phase 1 in the PhaP and PhaT are adopted from the ProbR and TreeR protocols, respectively. Phase 2 involves the process of packet routing between the first level phantom node and the new second level phantom node. A new routing strategy is proposed for phase 2 to ensure second level phantom nodes are randomly and tactically positioned in the network. The random positions guarantee that the routing paths are highly unpredictable to the adversaries, for strong SLP protection. Phase 2 may be considered as a replacement of the fake packet sources which exist in the TreeR and ProbR. Phase 3 involves the process of packet routing between the second level phantom node and the sink node. In PhaP, phase 3 is accomplished by utilizing a directed random-walk routing strategy. In PhaT, phase 3 is accomplished by utilizing a random backbone

조선대학교
CHOSUN UNIVERSITY

Table 4.1: Summary of the performance features of TreeR, ProbR, PhaT, and PhaP.

Protocol	Routing Strategy	Features	Influence
TreeR [32]	Integrates phantom routing and fake source packet routing.	• Employs fake source packets near network border regions.	• Positive effect on SLP protection. • Negative effect on energy consumption in near network border regions. • Negative effect on PDR, and EED performance.
		• Broadcasts large amount of fake packets in some regions of the network.	• Positive effect on SLP protection. • Negative effect on energy consumption, PDR, and EED performance.
		• Distributes fake packets near phantom node route.	• Positive effect on SLP protection.
ProbR [62]	Integrates phantom routing and fake source packet routing.	• Employs fake source packets in the near-sink region.	• Insignificant effect on SLP protection. • Negative effect on energy consumption performance in near-sink regions.
		• Broadcasts one fake packet at a time.	• Insignificant effect on SLP protection. • Some negative effect on energy consumption, PDR, and EED performance.
		• Isolates the fake packet sources from the phantom node.	• Insignificant effect on SLP protection.
Proposed PhaT	Replaces the fake source packets in TreeR with a second level phantom node.	• Employs a second level phantom node near network border regions.	• Positive effect on SLP protection. • Improved energy consumption, PDR, and EED performance compared to TreeR.
Proposed PhaP	Replaces the fake source packets in ProbR with a second level phantom node.	• Employs a second level phantom node in pursue ring regions.	• Positive effect on SLP protection. • Stronger SLP protection than ProbR. • Lower energy consumption than ProbR for near-sink regions.

route which is generated between the sink node and a neighboring node of the second level phantom node. By removing the fake packets in the network, the proposed PhaP and PhaT protocols achieve controlled energy consumption, PDR, and EED. The PhaP protocol preserves stronger SLP protection than its contender ProbR protocol. The communication overhead in PhaT protocol is significantly

조선대학교
CHOSUN UNIVERSITY

improved as compared to its contender TreeR protocol. Furthermore, unlike the TreeR protocol, PhaT is more capable of controlling the communication overhead under varied network conditions such as varied source packet rate, varied network size, and varied source-sink distance. A summary of the performance features of the existing and proposed protocols is shown in Table 4.1.

- **Contributions**

The main contributions of this study can be outlined as follows: (1) to propose two new routing protocols which employ a 2-level phantom routing strategy with two adversary confusion phases; (2) to conduct a sequence of experiments to evaluate and compare the privacy performance of the proposed protocols with the existing TreeR and ProbR; (3) to demonstrate that the proposed protocols provide strong SLP protection with controlled communication overhead; (4) to conduct a range of experiments to investigate the SLP protection, energy consumption, PDR, and EED performance of the protocols under varied network configurations.

4.1.2. Related Work

This study focuses on phantom routing, fake source packet routing, and the protocols which adopt both phantom routing and fake source packet routing. The phantom routing technique involves two main phases during the packet routing. In the first phase, packets are routed from the source node to a location where a phantom source is located through a random walk. At the phantom source, the packets are then forwarded to the sink node through flooding, single-path routing, or other strategies. The phantom routing strategy has been widely explored in the literature, and it has been adopted in many existing protocols. Examples of routing protocols which adopt phantom routing include the trace cost based source location privacy protection scheme [99], phantom walkabouts routing protocol [45], the phantom routing with locational angle [101], and the energy efficient privacy preserved routing algorithm [102]. Similarly, the phantom routing strategy is adopted in the multiple-phantom nodes routing scheme [103], the grid-based single phantom node and grid-based dual phantom node source location privacy protection schemes [39], the self-adjusting directed random walk approach [104], and the pseudo normal distribution-based phantom routing protocol [105].

조선대학교
CHOSUN UNIVERSITY

The baseline phantom routing protocol offers low levels of SLP protection because it employs short and predictable routing paths. Adversary can successfully perform back tracing attack on the short routing paths within a short time period. Furthermore, the phantom routing offers reduced levels of SLP protection when multiple source nodes exist in the network [93].The fake source packet routing protocols involve the process of selecting a set of nodes in the WSN to act as fake sources and mimic the real sources. The fake sources and real sources send packets simultaneously to confuse the adversary. The fake source packet routing strategy has been adopted in many existing protocols including the dummy packet injection scheme [89], the dynamic fake sources-based algorithm [87], and the hybrid online dynamic single path routing algorithm [41]. Similarly, the fake source packet routing strategy is adopted in the forward random walk and bidirectional tree schemes [74], the fake network traffic-based scheme [92], the timed efficient source privacy preservation scheme [91], and the dummy uniform distribution, dummy adaptive distribution, and controlled dummy adaptive distribution protocols [90]. Often, the fake source packet routing protocols are criticized because of their high energy consumption, mainly because they rely on injecting a large amount of fake packets to effectively protect the SLP. Furthermore, the protocols incur poor PDR and EED performance due to collisions between the packets.

There exist several protocol designs which adopt both the phantom routing and fake source packet routing strategies. The protocols include the tree-based diversionary routing [32], the enhanced source location privacy based on data dissemination protocol [61], the probabilistic source location privacy protection protocol [62], and the distributed protocol that combines fake source routing and phantom source routing [44].

Although many routing strategies exist in the literature, a limited number of studies have addressed the limitations of the recently proposed fake packet routing protocols. Specifically, multi-level phantom node routing strategies have not been widely explored as an approach to address the limitations of fake packet routing protocols. In this study, we address the limitations of the fake packet routing protocols in [32] and [62] by using 2-level phantom routing protocols. In its baseline form, the phantom routing protocol is cost-effective. However, it offers low levels of SLP protection.

조선대학교
CHOSUN UNIVERSITY

We take advantage of the cost-effective phantom routing protocol. We propose two new 2-level phantom routing protocols which offer high levels of SLP protection. The proposed protocols are PhaP and PhaT protocols. The PhaP protocol offers higher levels of SLP protection than the protocol in [62]. Furthermore, the PhaP protocol achieves controlled energy consumption, PDR, and EED. In the near-sink region, the PhaP protocol achieves lower energy consumption than the protocol in [62]. The PhaT protocol offers slightly lower levels of SLP protection than the protocol in [32]. Nonetheless, the privacy protection of PhaT is effectively high. Comparing the communication overhead of the PhaT protocol and the protocol in [32], the PhaT protocol achieves significantly lower energy consumption, significantly higher PDR, and lower EED.

4.1.3. Proposed Phantom Routing Protocols

Two new routing protocols, 2-level phantom with a pursue ring (PhaP) and 2-level phantom with a backbone route (PhaT) are proposed. The two main goals of the proposed protocols are to: (1) provide strong SLP protection throughout the WSN domain, and (2) control the communication overhead by removing the fake packet traffic in the network. The PhaP and PhaT protocols introduce a two-level phantom routing strategy. In the strategy, packet routing is done in three phases. In phase 1, packets are routed from the source node to the first level phantom node. The routing strategy for phase 1 in the PhaP and PhaT are adopted from the ProbR and TreeR protocols, respectively. Phase 2 involves the process of packet routing from the first level phantom node to the new second level phantom node using two new routing strategies. The new routing strategies are explained in details in the next sub-sections. Phase 3 involves the process of packet routing from the second level phantom node to the sink node. In PhaP, phase 3 is accomplished by utilizing a directed random-walk strategy. In PhaT, phase 3 is accomplished by utilizing a random backbone route which is generated between the sink node and a neighboring node of the the second level phantom node. A new backbone routing strategy is proposed. For both PhaP and PhaT protocols, the two-level phantom routing strategy is designed to provide two adversary confusion phases. The first level phantom node provides first level adversary confusion phase while the second level phantom node provides second level adversary

조선대학교
CHOSUN UNIVERSITY

confusion phase. If an adversary embarks on back tracing the routing paths, it encounters two levels of adversary confusion phases. Thus, strong SLP protection is guaranteed. The proposed PhaP and PhaT routing algorithms are summarized in algorithms 4.1 and 4.2, respectively.

- **Proposed Two-Level Phantom with a Pursue Ring (PhaP) Protocol**

A) PHASE 0: Network Configuration

For proper functioning of the PhaP protocol, a pursue ring (P_{ring}) is computed during the network configuration phase, after the network initialization process. The network initialization process is explained in section 2.1. The P_{ring} is computed during network configurationphase to minimize delay during packet routing. To begin the P_{ring} computation process, an X-Y coordinate is generated at the sink node location and two distances are defined, the distance from sink node to the inner ring of the P_{ring} (dP_{in}) and the distance from sink node to the outer ring of the P_{ring} (dP_{out}). Distance between any two points in the network is calculated using the Euclidean distance equation shown in equation (1). A ring with dP_{in} and dP_{out} is generated. The configuration of the P_{ring} regions in the WSN domain is shown in Fig. 4.1.

All sensor nodes which are located in the P_{ring} are recoded in a list of candidate second level phantom nodes (P_{Nsec}). To diversify the routing paths, the P_{ring} is divided into four parts: north-east region of P_{ring} (P_{rNE}), south-east region of P_{ring} (P_{rSE}), north-west region of P_{ring} (P_{rNW}), and south-west region of P_{ring} (P_{rSW}). To specify the P_{ring} regions, the θ of all the sensor nodes in the P_{ring} is computed according to the θ computation process in section 2.1. The sensor nodes with θ in the range $0° \leq \theta < \pi/2$, $\pi/2 \leq \theta < \pi$, $\pi \leq \theta < 3\pi/2$, and $3\pi/2 \leq \theta < 2\pi$ are assigned in P_{rNE}, P_{rNW}, P_{rSW}, and P_{rSE}, respectively.

B) PHASE 1: Selection of P_{Nfst} and packet routing from source node to P_{Nfst}

After the P_{ring} is configured, the network is ready for packet routing. The proposed PhaP routing algorithm is summarized in algorithm 4.1. The packet routing process is done in three phases. Phase 1 routing is activated by the source node when the source node detects an asset. The source node selects a random first level phantom node (P_{Nfst}) using similar phantom node selection algorithm as

조선대학교
CHOSUN UNIVERSITY

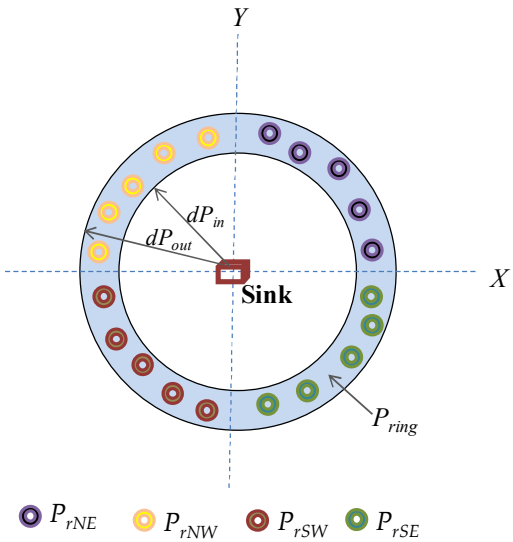


Figure 4.1: Configuration of the P_{ring} regions in the proposed PhaP protocol.

Table 4.2: Selection of P_{Nsec} according to P_{Nfst} location and value of R_N.

Location of P_{Nfst}	**Selection of P_{Nsec}**	
	$R_N < T_P$	**$R_N \geq T_P$**
X-coordinate < 0	P_{rNW}	P_{rSE}
X-coordinate ≥ 0	P_{rNE}	P_{rSW}

in ProbR. After P_{Nfst} is selected, it sends packet to the P_{Nfst} using a directed random-walk routing strategy. The directed random-walk routing strategy involves a process of next-hop node selection at every packet forwarding instance. The forwarding node computes a set of neighboring nodes with a shorter hop distance to the destination node than the forwarding node itself. Then it randomly selects one neighboring node from the set as the next-hop node. The next-hop node becomes the forwarding node and forwards the packet. For easy of understanding, the group of neighboring nodes with shorter hop distance to the destination node is termed as SDR_N, in algorithms 4.1 and 4.2. Also, the selected next-hop node from the SDR_N is termed as DR_N and the destination nodes are termed as target node.

조선대학교
CHOSUN UNIVERSITY

Algorithm 4.1: Proposed algorithm for PhaP protocol

Input:

S_{LOC}: Location of sink node;

S_{hop}: Hop count at sink node;

Output:

Routing path to sink node;

Phase 0: Network configuration

network initialization
generate *X-Y* coordinate centered at S_{LOC}
create P_{ring} according to Fig. 4.1
compute θ
if ($0^{\circ} \leq \theta < \pi/2$)
    assign node into P_{rNE}
else if ($\pi/2 \leq \theta < \pi$)
    assign node into P_{rNW}
else if ($\pi \leq \theta < 3\pi/2$)
    assign node into P_{rSW}
else if ($3\pi/2 \leq \theta < 2\pi$)
    assign node into P_{rSE}
end if

Phase 1: Selection of P_{Nfst} and packet routing from source node to P_{Nfst}

sensor node become *sourceNode*
select P_{Nfst}
packet routing(*sourceNode*, P_{Nfst}) // *sourceNode* send packet to P_{Nfst} using directed random-walk routing

Phase 2: Selection of P_{Nsec} and packet routing from P_{Nfst} to P_{Nsec}

biasThreshold = T_P
P_{Nfst} generates R_N
if (*X*-coordinate_of_P_{Nfst} < *X*-coordinate_of_*sink*)
    if ($R_N < T_P$)
        select P_{Nsec} from P_{rNW}
    else
        select P_{Nsec} from P_{rSE}
    end if
else if (*X*-coordinate_of_P_{Nfst} ≥ *X*-coordinate_of_*sink*)
    if ($R_N < T_P$)
        select P_{Nsec} from P_{rNE}
    else
        select P_{Nsec} from P_{rSW}
    end if
end if
packet routing(P_{Nfst}, P_{Nsec}) // P_{Nfst} send packet to P_{Nsec} using directed random-walk routing

Phase 3: Packet routing from P_{Nsec} to sink node

packet routing(P_{Nsec}, *sink*) // P_{Nsec} send packet to *sink* using directed random-walk routing
function Packet routing(*senderNode*, *targetNode*) // directed random walk routing
generate SDR_N
select DR_N
while (DR_N != *targetNode*)
    senderNode = DR_N
    senderNode generate SDR_N
    senderNode select DR_N
end while
end function

C) PHASE 2: Selection of P_{Nsec} and packet routing from P_{Nfst} to P_{Nsec}

조선대학교
CHOSUN UNIVERSITY

After the P_{Nfst} receives a packet from P_{Nfst}, it sets a bias threshold value, T_P. Then it generates a random number, R_N, between [0, 1]. The R_N and T_P values are compared and a random P_{Nsec} is selected according to Table 4.2. The P_{Nsec} selection process is highly dependent on the location of the P_{Nfst} with respect to the sink node. The P_{Nfst} may be located on the east or west side of the sink node according to the *Y*-axis. After the P_{Nsec} is selected, P_{Nfst} forwards the packet to the randomly selected P_{Nsec} using the directed random-walk routing strategy. To guarantee high path diversity for successive packets, new P_{Nfst} and P_{Nsec} are selected for each packet transmission.

D) PHASE 3: Packet routing from P_{Nsec} to sink node

After packets arrive at the P_{Nsec}, they are forwarded to the sink node using the directed random-walk routing strategy. At the P_{Nsec}, the destination node is the sink node as shown in algorithm 4.1.

- **Proposed Two-Level Phantom with a Backbone Route (PhaT) Protocol**

A) PHASE 0: Network Configuration

In the PhaT protocol, it is assumed that the near network border region is defined during the network configuration phase. The outer boundary of the near network border region is the network border. The inner boundary of the near network border region is defined at distance d_{NB} from the network border. All sensor nodes which are located within distance d_{NB} from the network border are identified as nodes in the near network border regions (N_{NB}). The d_{SB} is a distance from location of a sensor node to the network border. For any sensor node, if $d_{SB} \leq d_{NB}$, the sensor node is added in the list of N_{NB}. All N_{NB} may be selected as a first level phantom node (*epN*) during packet routing. The algorithm for PhaT protocol is summarized in algorithm 4.2.

The last task in the network configuration phase is the process where each N_{NB} computes a list of candidate second level phantom nodes (*npN*). For each N_{NB}, an *npN* is a sensor node which is located at hop distance, d_P, away. For example, if node N_{20} is in the list of N_{NB}, and d_P is specified as 4 hops, then N_{20} will compute a list of all sensor nodes which are located 4 hops away. As an example, N_{20} may compute a list containing nodes N_8, N_{30}, N_{14}, and N_{57}. During packet routing, if N_{20} is selected as *epN*, then it may select N_8, N_{30}, N_{14}, or N_{57} as the second level phantom node (*npN)*. Fig. 4.2 shows

조선대학교
CHOSUN UNIVERSITY

the configuration of sensor nodes in the proposed PhaT protocol.

Algorithm 4.2: Proposed algorithm for PhaT protocol

Input:
S_{LOC}: Location of sink node;
S_{hop}: Hop count at sink node;
Output:
Routing path to sink node;
Phase 0: Network configuration
network initialization
$d_{NB} = \sqrt{(x_N - x_B)^2 + (y_N - y_B)^2}$
$d_{SB} = \sqrt{(x_S - x_B)^2 + (y_S - y_B)^2}$
if $d_{SB} \leq d_{NB}$
    add sensor node to list of *epN*
    each *epN* generate a list of *npN*
    if (*Y*-coordinate_of_*npN* > *Y*-coordinate_of_*epN*)
        assign *npN* into *northR*
    else
        assign *npN* into *southR*
    end if
end if
Phase 1: Selection of *epN* and packet routing from source node to *epN*
sensor node become *sourceNode*
select *epN* from list of *epN*
Packet routing(*sourceNode*, *epN*) // source node send packet to *epN* using directed random-walk routing
Phase 2: Selection of *npN* and packet routing from *epN* to *npN*
biasThreshold = *T*
generate *SF*
if (*SF* > *T*)
    select *npN* from *northR*
else
    select *npN* from *southR*
end if
Packet routing(*epN*, *npN*) // *epN* send packet to *npN* using directed random-walk routing
Phase 3: Selection of $_B$*N* and packet routing from *npN* to sink node
npN select $_B N$
$_B N$ select N_{WSD}
while (N_{WSD} != *sink*)
    $FW_N = N_{WSD}$
    FW_N select N_{WSD}
end while
npN send packet to $_B N$ and $_B N$ forward packet to sink using shortest path routing
function PacketRouting(*sendNode*, *targetNode*) // directed random-walk routing strategy
generate SDR_N
select DR_N
while (DR_N != *targetNode*)
    sendNode = DR_N
    sendNode generate SDR_N
    sendNode select DR_N
end while
end function

조선대학교
CHOSUN UNIVERSITY

The location configuration of the candidate *npN*s is guarded by a restricted region, R_dR, around the *epN*. R_dR is defined by radius of hop distance d_H from *epN*. d_H is used to ensure a safe distance between *epN* and *npN*. All the neighboring nodes of *epN* are located inside the R_dR. The distances d_H and d_P have a relationship which satisfy the equation $d_H = d_P - 1$. While d_H specifies the sensor nodes which are restricted from becoming *npN*, d_P is used to specify the sensor nodes which are good candidate for *npNs*. The *npN* are located outside the R_dR to ensure the *epN* and *npN* are not neighboring nodes. Longer d_P increases the distance between the *epN* and *npN*, increases the complexity for the adversary back tracing attack, and improves the SLP protection. To guarantee routing paths with high path diversity, two unique regions of *npNs* are defined. The regions are north of *epN* (*northR*) and south of *epN* (*southR*). If a node is a candidate *npN* with *Y*-coordinate greater than the *Y*-coordinate of the *epN*, it is identified as a candidate *npN* in *northR*. Otherwise, if a node is a candidate *npN* with *Y*-coordinate less than or equal to the *Y*-coordinate of the *epN*, it is identified as a candidate *npN* in *southR*.

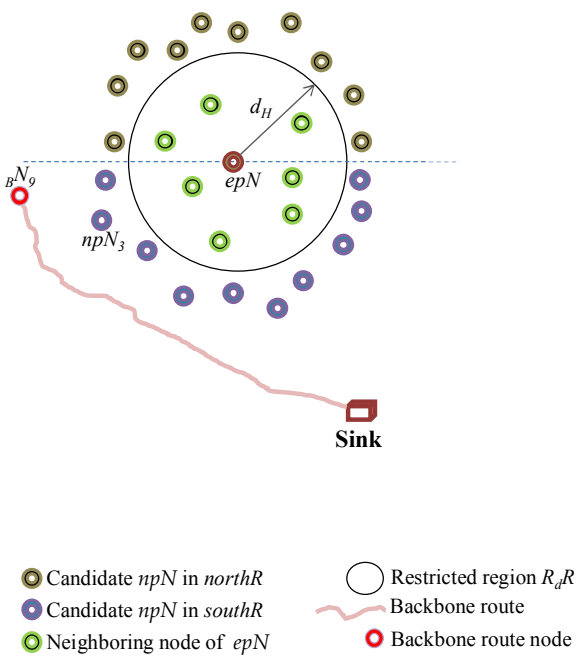


Figure 4.2: Configuration of the sensor nodes in the proposed two-level phantom with a backbone (PhaT) protocol.

조선대학교
CHOSUN UNIVERSITY

The protocol employs the phantom nodes in the near network border regions to ensure effectively long and diversified routing paths. To control the communication overhead of the protocol, the near network border regions must be configured according to the network topology to ensure the routing paths are not excessively long. If the network size is very large, the distance between phantom nodes and the sink node may be excessively long and the protocol may incur high communication overhead. To route packets, the protocol operates in three phases as shown in algorithm 4.2.

B) PHASE 1: Selection of *epN* and packet routing from source node to *epN*

Phase 1 routing is activated by the source node upon event detection. The *epN* is selected and source node sends packet to *epN* using similar algorithm as in TreeR protocol.

C) PHASE 2: Selection of *npN* and packet routing from *epN* to *npN*

When the *epN* receives the packet from the source node, it activates the *npN* selection process to select one *npN* from the list of *npN*. A random selection factor (*SF*) is generated by the *epN*. The *SF* is distributed between [0, 1]. If $SF > T$, *npN* is randomly selected from the candidate *npNs* in *northR*. Otherwise, *npN* is selected from the candidate *npNs* in *southR*. After *npN* is selected, phase 2 packet routing is done. The *epN* forwards the packet to the *npN* using the directed random-walk strategy.

D) PHASE 3: Selection of ${}_{B}N$ and packet routing from *npN* to sink node

After the *npN* receives the packet, it activates the process to select an initial backbone route node (${}_{B}N$) which is used to create a backbone route to the sink node. The *npN* selects a neighboring node with the longest hop distance to the sink node as the ${}_{B}N$. As an example, in Fig. 4.2, if npN_3 receives a packet from *epN*, ${}_{B}N_9$ may be selected as the ${}_{B}N$. If multiple nodes have equal longest hop distance to the sink node, one of the nodes is randomly selected. After the ${}_{B}N$ is selected, phase 3 packet routing is done. The *npN* forwards the packet to the ${}_{B}$N and the ${}_{B}$N forwards the packet to the sink node through a backbone route. The backbone route employs the shortest path routing strategy. At each forwarding node (FW_N), the node with the shortest hop distance to the sink node (N_{WSD}) is selected as the next-hop node. When the N_{WSD} is the sink node, the packet is delivered at the sink node. The shortest path routing strategy is employed to ensure controlled communication overhead.

조선대학교
CHOSUN UNIVERSITY

New *epN*, *npN*, *SF*, and backbone route are computed for each successive packet to guarantee high path diversity and strong SLP protection.

4.1.4. Performance Analysis

Performance analysis to evaluate the performance of the proposed protocols was done using MATLAB simulation environment. A total of five protocols were included in the analysis: the ProbR, PhaP, TreeR, PhaT, and the phantom single-path routing (Pha). The Pha protocol was included in the analysis as a representative protocol for the traditional SLP routing protocols, for comparative analysis. Only real packets were transmitted in the PhaP and PhaT protocols. In the ProbR and TreeR, real packets and fake source packets were transmitted simultaneously. The following performance metrics were used for analysis: SP, attack success rate (ASR), energy consumption, network lifetime, EED, and PDR.

- **Simulation Parameters and Values**

The network model in section 2.1 and adversary model in section 2.2 were assumed. A WSN with N_{SL} of 2000 m was simulated. For good coverage in the network, 2500 sensor nodes were randomly distributed. Thus, N_{NS} was 2500. The sink node was the destination for all the packet transmissions. The location of the sink node was assumed at the center of the network. The S_{CR} was set to 30 m to guarantee multi-hop communications between source nodes and sink node. The network configuration for the PhaP protocol was done according to Fig. 4.1. The network parameters were configured as follows: dP_{in} = 400 m, dP_{out} = 600 m, and T_p = 0.5. For PhaT protocol, d_{NB} = 200 m, d_H = 3 hops, d_P = 4 hops, and T = 0.5. A cautious adversary was deployed with initial location in the vicinity of the sink node to ensure maximum probability of packet capture. The A_{HR} was set to 30 m similar to S_{CR} to guarantee that the adversary performs hop-by-hop back tracing attack. The A_{WT} was set to 4 source packets. The network simulation parameters are summarized in Table 4.3. Simulations were run for 500 iterations and average values were considered.

- **Simulation Results and Discussions**

Two experiment scenarios, experiment scenarios (a) and experiment scenarios (b), were done for the

조선대학교
CHOSUN UNIVERSITY

Table 4.3: Network simulation parameters

Parameter	Value
N_{SL} (m)	2000
N_{SN}	2500
N_{sink}	1
S_{CR} (m)	30
A_{HR} (m)	30
A_{WT} (source packets)	4
dP_{in} (m)	400
dP_{out} (m)	600
T_P	0.5
d_H (hops)	3
d_P (hops)	4
d_{NB} (m)	200
T	0.5
P_{sz} (bit)	1024
SN_{PR} (packet/second)	Varied from 1 to 7
S_{IE} (J)	0.5
Adversary initial location	In the vicinity of sink node

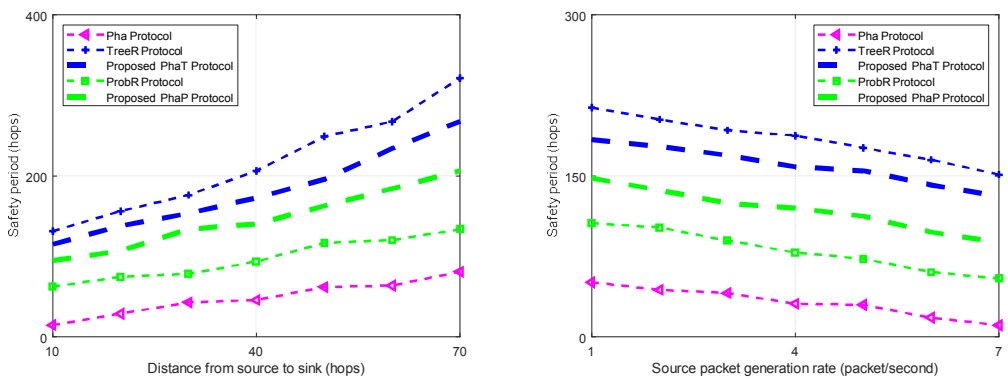
performance analysis of SP, energy consumption, PDR, and EED. In the scenarios (a), the performance was observed under fixed source packet rate of 1 packet/second against varied source-sink distance. The source-sink distance was varied between 10 and 70 hops. In scenarios (b), performance was observed under fixed source-sink distance against varied source packet generation rate. The source packet generation rate was varied from 1 to 7 packet/second. For the analysis of ASR, three experiment scenarios were done. In scenario (a), the ASR was observed against varied number of sensor nodes in the network. In scenario (b), the ASR was observed at varied network size. In scenario (c), the ASR was observed against varied adversary hearing range.

A) Safety Period

The privacy performance of the protocols is shown in Fig. 4.3. It is shown that the TreeR protocol achieves long SP. The TreeR achieves long SP by integrating many routing techniques. It employs phantom nodes located far away from the source node. It also employs significantly long backbone routes with many diversionary routes. At the end of each diversionary route, fake packets are emitted periodically. As a result, the eavesdropping adversary is effectively obfuscated and long SP is guaranteed. However, the use of long backbone routes, diversionary routing paths which diverge to

조선대학교
CHOSUN UNIVERSITY

the network border regions, and the distribution of fake packet traffic at the end of each diversionary route introduce very high communication overhead as shown in the next paragraphs. It is also shown that the proposed PhaT protocol achieves relatively short SP compared to the TreeR protocol. However, compared to the traditional Pha protocol, the PhaT protocol offers significantly longer SP. For example, at 60 hops from the sink node, the SP of the PhaT is approximately 4 times longer than Pha protocol. Since PhaT can achieve approximately 4 times higher SP than the Pha protocol, we consider the level of SLP protection for PhaT to be effectively strong.



(a) (b)

Figure 4.3: Privacy performance of the protocols. (a) SP against source-sink distance. (b) SP against source packet generation rate.

Also shown in the Fig. 4.3 (a), the proposed PhaP protocol achieves significantly longer SP than the existing ProbR protocol. The ProbR protocol achieves a relatively short SP because the fake packet source is located away from the real source node, on the opposite side of the real source node. Also, the real packet routes and fake packet routes are not exactly homogeneous due to the location of the fake packet sources being in the near-sink region. The fake packet routes are relatively short. As a result, it has a small effect on the privacy protection. After sometime of traffic analysis attack, adversary can predict the real packet routes and perform a more focused back tracing attack to improve its attack success rate. Furthermore, the ProbR protocol distributes only one fake packet at a time. As a result, the adversary is not effectively distracted from the real packet routes and short SP is achieved by the ProbR protocol. The SP of Pha protocol is significantly lower because the protocol

조선대학교
CHOSUN UNIVERSITY

employs a simple routing algorithm with short and fixed routes. The adversary is capable of successfully back tracing the routing paths of the Pha within a short time. For all the protocols, the privacy performance improves with the increase in source-sink distance.

Fig. 4.3 (b) shows the privacy performance of the protocols at a source-sink distance of 40 hops against varied source packet generation rate. The protocols provide reduced SP as the source packet rate increases. The main reason for the reduced SP is that, as more packets are sent in the network, the probability that the cautious adversary will capture successive packets within the specified waiting timer is increased. At higher data rates, the cautious adversary is capable of capturing enough number of successive packets to allow it to make a successful back tracing attack and capture the asset. Therefore, the level of SLP protection is reduced.

B) Attack Success Rate

ASR is the measure of the rate of source node traceability when an eavesdropping adversary is back tracing against a SLP routing protocol. It is computed by counting the number of successful adversary attempts [40]. ASR has an inversely proportional relationship with the SP as shown in equation (14). When a protocol achieves long SP, the ASR is reduced and high level of SLP is achieved.

$$\max \ (SP) = \min \ (ASR) \tag{14}$$

The ASR of the adversary against the routing protocols is shown in Fig. 4.4. In the analysis, the source packet generation rate was 1 packet/second, the adversary trace time was 900 source packets, and the source-sink distance was fixed at 50 hops. For the results in Fig. 4.4 (a), the ASR was observed against varied number of sensor nodes in the network. The number of sensor nodes was varied between 2500 and 4000 nodes. It is shown that the ASR of all the protocols tend to decrease with the increase in the number of sensor nodes in the network. However, for the proposed protocols, the ASR decreases at a slightly higher rate. This means that, the SLP protection in the proposed protocols increases at a higher rate that in the other protocols. The main reason for the increased SLP protection with the increase in node density is that, when the number of nodes in the network increases, the number of neighboring nodes and candidate phantom nodes also increase.

조선대학교
CHOSUN UNIVERSITY

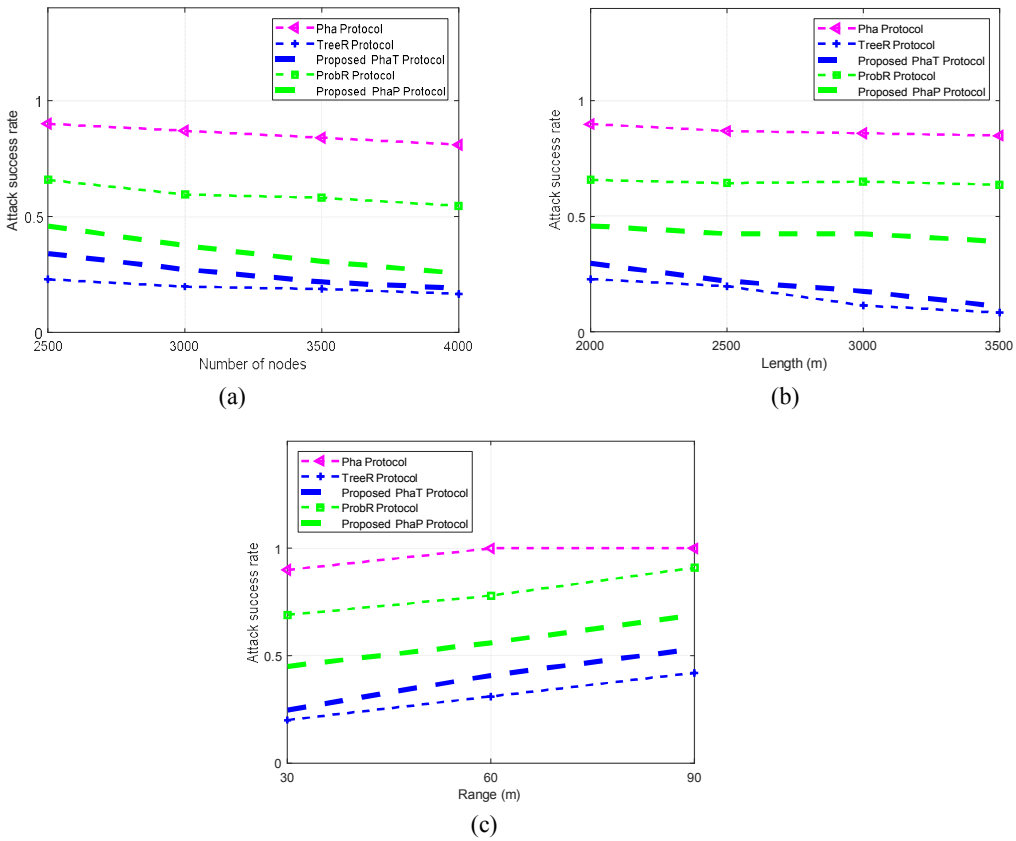


Figure 4.4: Privacy performance of the routing protocols. (a) ASR under varied number of nodes in network. (b) ASR under varied network size. (c) ASR under varied adversary hearing range.

As an example, in PhaP protocol, when the node density increases it also increases the probability of more number of nodes in the P_{ring}. Therefore, the number of candidate P_{Nsec} for each successive packet also increases. As a result, there is a higher probability that a different P_{Nsec} is selected for each successive packet and the routing paths becomes less predictable to the eavesdropping adversary. Also, the number of random routing paths increases with the increase in number of neighboring nodes of the P_{Nfst} and P_{Nsec}. As an example, if a source node has w neighboring nodes with shorter hop distance to P_{Nfst}, the probability of the source node selecting a particular neighboring node as the next-hop node during the directed random-walk is $1/w$. If P_{Nfst} has k neighboring nodes with shorter hop distance to P_{Nsec}, the probability of P_{Nfst} selecting a particular

조선대학교
CHOSUN UNIVERSITY

neighboring node as the next-hop node during the directed random-walk is $1/k$. If P_{Nsec} has v neighboring nodes with shorter hop distance to sink, the probability of *PNsec* selecting a particular neighboring node as the next-hop node during the directed random-walk is $1/v$. Overall, there can be up to $w \times k \times v$ random routes between the source node and the sink node. That is, Total number of routes = $w \times k \times v$. It is therefore evident that the SLP protection will increase with the increase in node density. As a result, ASR decreases with the increase in node density. This effect is similar in the PhaT protocol. The ProbR protocol employs only one phantom node and one fake packet source in the near-sink region. As a result, the increase in node density has a small effect on limiting the ASR. The TreeR depends highly on the fake packet routes to obfuscate the adversary. Since the number of diversionary routes remained the same, obfuscation of the adversary on the backbone route does not improve very much with the increase in node density. As a result, ASR decreases at a slow rate. The Pha protocol selects the shortest paths which may become fixed, as a result, the increase in node density has little effect on the ability of protocol to limit the ASR.

Fig. 4.4 (b) shows the ASR of the adversary against varied network size. The network has a square structure. For analysis, we use the term “Length” which means the length or width of the network. In the experiments, the length was varied between 2000 and 3500 m. It is shown that the ASR against the Pha, ProbR, and PhaP protocols has insignificant change as the length increases. The main reason for the insignificant change is that the routing paths of the protocols are directed towards the sink node. Since the source-sink distance remained the same and the phantom node selection criteria did not change, the change in the network size had no significant impact on the performance of protocols. In the PhaT protocol, the ASR decreases significantly with the increase in length. The main reason for the improved privacy performance as length increases is that, since the location of the sink node is constant at the center of the network, then the distance between the sink node and phantom nodes increases with the increase in length. This is mainly because the phantom nodes are located in the near network border regions.

Also, since the source-sink distance was fixed at 50 hops, the distance between the source node and phantom nodes increase with the increase in length. As a result, the routing paths become longer

조선대학교
CHOSUN UNIVERSITY

and the directed random-walk routing strategy becomes more obfuscating to the adversary. Consequently, the adversary takes longer time to back trace the packet routes, makes insignificant progress towards the source node, and the ASR is limited. However, for the proposed PhaT protocol, it is important to control the length. If the length is too long, it may lead to excessively long routing paths which incur high communication overhead. In the TreeR protocol, when the intermediate node is kept at a fixed location, it is possible to increase the length of the diversionary routes as the network size increase. As a result, the obfuscation ability of the protocol is increased. When the adversary is misled into back tracing the diversionary routes which become longer with the increase in length, the adversary may be misled into regions further away from the source node. Hence, the ASR is reduced.

Fig. 4.4 (c) shows the ASR under varied adversary hearing range. The adversary hearing range was varied between 30 and 90 m. It is shown that the ASR increases with the increase in adversary hearing range. This is mainly due to the fact that adversary becomes more powerful when it has a longer hearing range. The traffic analysis attacks become less complex when the adversary can detect a packet sent from a sensor node which is more than 1 hop away. It shows that, when a source node is 50 hops away from the sink node, at a trace time of 900 source packets, an adversary with 60 m hearing range can achieve up to 100% ASR against the Pha protocol. An adversary with 90 m hearing range can achieve up to 90% ASR against the ProbR protocol and up to 65% ASR against the PhaP protocol. For PhaT and TreeR protocols, an adversary with 90 m hearing range can achieve less than 55% ASR. These results establish that, amongst all the analyzed protocols, the PhaT and TreeR protocols have the strongest SLP protection and when the adversary has 30 m hearing range, the protocols are capable of limiting the adversary ASR to less than 25%.

C) Energy Consumption

Fig. 4.5 shows the energy consumption performance of the protocols. In the energy consumption analysis, 15 experiment scenarios were assumed, each scenario with a different source node location. Packets were sent from source nodes to the sink node. After all the packets were received at the destination sink node, for each scenario, the average energy consumption per sensor node was

조선대학교
CHOSUN UNIVERSITY

computed according to equations (3) and (4). For both TreeR and ProbR protocols, real packets and fake packets were transmitted simultaneously. Fig. 4.5 (a) shows the energy consumption per sensor node for sensor nodes at different locations. It is shown that the energy consumption of TreeR protocol is significantly high. The high energy consumption is due to the integration of many routing techniques. The backbone routes which divert to the network border cause the protocol to generate long routing paths. Also the multiple diversionary routes which act as branches for the backbone routes distribute a large amount of fake packets. Fake packets are also distributed along the phantom route. As a result, the sensor nodes incur exhaustive energy consumption.

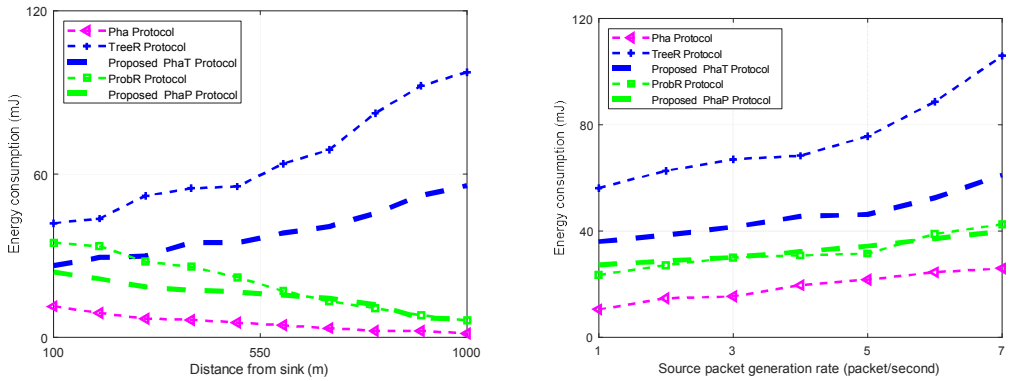


Figure 4.5: Energy consumption of the protocols. (a) Energy consumption against varied source–sink distance. (b) Energy consumption against varied source packet generation rate.

Furthermore, multiple fake packets are transmitted for each real packet transmission. As shown in equations (3) and (4), each hop involves consumption of transmit and receive energy. As a result, more energy is consumed for each real packet transmission. Moreover, the distribution of fake packets in the network increases the probability of packet collision events which result in packet retransmission incidents. Hence, higher energy consumption is incurred by the TreeR protocol. The proposed PhaT has significantly lower energy consumption than the TreeR protocol mainly because while the PhaT protocol employs a single route for each packet transmission, the TreeR protocol employs multiple routes which include a route for real packet transmission and multiple diversionary

조선대학교
CHOSUN UNIVERSITY

routes for fake packets transmission. Both TreeR and PhaT protocols employ backbone route near the sink region to minimize the energy consumption in the region. The energy consumption of PhaT is higher than in the ProbR, PhaP, and Pha protocols. The main reason for the high energy consumption is that, PhaT locates the phantom nodes in the network border regions which results in longer and highly diversified routing paths.

In the near-sink regions, ProbR protocol incurs higher energy consumption than the proposed PhaP because ProbR transmits multiple packets for each event packet. A fake source packet is transmitted with every real packet transmission. Sensor nodes in the near-sink region experience exhaustive energy consumption due to the big load of packet forwarding. The sensor nodes not only transmit their own packets to the sink node, they also forward packets originating from the sensor nodes in the away from sink regions. The PhaP protocol ensures the energy consumption of the sensor nodes in the near-sink region is minimized. In the away from the sink regions, PhaP and Prob incur same amount of energy consumption because the protocols employ a similar phantom node routing strategy in the away from the sink regions. The energy consumption of the Pha protocol is significantly lower because the protocol employs a simple routing algorithm with short routes.

Fig. 4.5 (b) shows the energy consumption of sensor nodes at 600 m from the sink node, against varied source packet generation rate. The energy consumption of the sensor nodes increases with the increase in source packet generation rate. At higher packet rates, more packet traffic is generated in the network. Consequently, the sensor nodes consume more energy to transmit the packets. The energy consumption of TreeR protocol increases at a faster rate because more packet collision events occur due to the transmission of both, real packet and fake packets. More packet collision events result in packet loss and packet retransmission events. As a result, the energy consumption of the sensor nodes is increased.

D) Packet Delivery Ratio

Fig. 4.6 shows the PDR of the protocols. Fig. 4.6 (a) shows the PDR performance of the protocols at a fixed source packet rate. The analysis included source nodes at different source-sink distances. 100

조선대학교
CHOSUN UNIVERSITY

packets were transmitted from each source node to the sink node with a fixed source packet generation rate of 1 packet/second. Average values for PDR were found according to equation (12) from [106], [107]. It is shown that PDR of all the protocols decreases with the increase in source-sink distance. This is due to the fact that as the distance between the source node and sink node increases, more hops are included in the transmission and the probability of packet loss increases. Therefore, the PDR performance is affected. Also, it is shown in Fig. 4.6 (a) that the TreeR protocol incurs low PDR. The low PDR performance of TreeR is due to the integration of many routing strategies. The use of phantom nodes, backbone routes, and diversionary routes result in routing paths which have high probability of packet loss events and low PDR. Furthermore, the distribution of fake packets in the network results in high probability of packet collision events and low PDR is achieved. The proposed PhaT protocol achieves higher PDR than the TreeR protocol because it incurs few packet collision and packet loss events due to the absence of fake packet distribution. The ProbR protocol achieves higher PDR than the TreeR protocol because it employs shorter routing paths with only one fake packet source at a time period. The ProbR and PhaP protocols have comparable PDR performance because they both employ phantom node routing with routing paths which are directed towards the sink node.

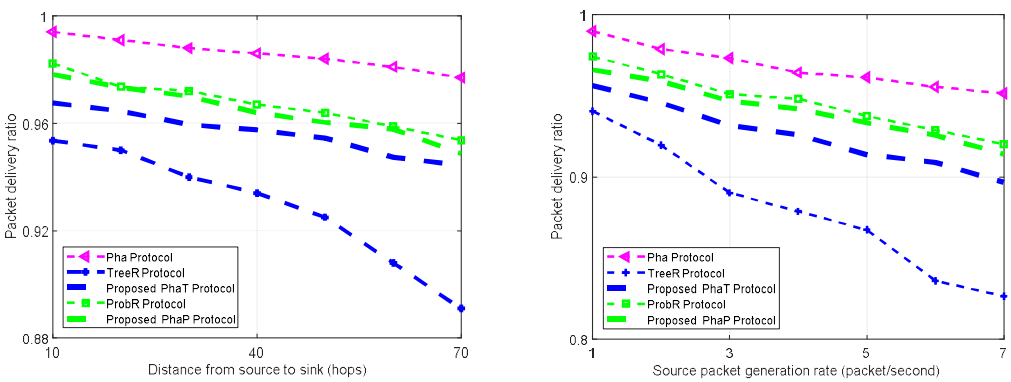


Figure 4.6: Packet delivery ratio of the protocols. (a) PDR against varied source-sink distance. (b) PDR against varied source packet rate.

조선대학교
CHOSUN UNIVERSITY

The fake packet sources in the ProbR are located far away from the real sources. Consequently, the fake packets incur less significant effect on the PDR of the protocol. The PDR of the Pha protocol is significantly high because the protocol employs a simple routing algorithm with short and fixed routing paths. The short and fixed routing paths incur few events of packet loss and packet collision. Fig. 4.6 (b) shows the PDR performance of the protocols at a fixed source-sink distance of 40 hops. The experiment scenarios included multiple source nodes. 100 packets were sent from each source node to the sink node at varied source packet rate, from 1 to 7 packet/second. It is shown that PDR of all the protocols decreases with the increase in source packet rate. When more packets are generated per second, the probability of packet collision and packet loss is increased and PDR is affected. The TreeR protocol incurs the worst PDR performance at high source packet rates due to the increasing number of packet collision events between the real and fake packets.

E) End-to-End Delay

Fig. 4.7 shows the EED of the protocols. Fig. 4.7 (a) shows the EED performance of the protocols at different source-sink distances. Investigations were done for multiple source nodes at different source-sink distances. 100 packets were sent from each source node to the sink node with a fixed source packet generation rate of 1 packet/second. Average values for EED were found according to equation (13) from [106], [107]. It shows that the EED of the protocols tend to increase with the increase in the source-sink distance. This is due to the fact that as the distance between the sourcenode and sink node increases, the number of packet forwarding events (hops) also increases. Each hop incurs some EED. Hence, the overall EDD is increased. Furthermore, longer routing paths have a higher probability of packet loss and packet retransmission events which have negative effect on the EED performance. The TreeR and PhaT protocols employ long routing paths. Consequently, the EED for the TreeR and PhaT protocols is long. The location of phantom nodes in the ProbR and PhaP protocols guarantee relatively short routing paths with better EED performance than the TreeR and PhaT protocols. The fake source packets in ProbR are located far away from the real source node. As a result, the fake packets have less significant effect on the EED performance of the protocol. The

조선대학교
CHOSUN UNIVERSITY

Pha protocol has significantly low EED because the protocol employs a simple routing algorithm with short and fixed routing paths.

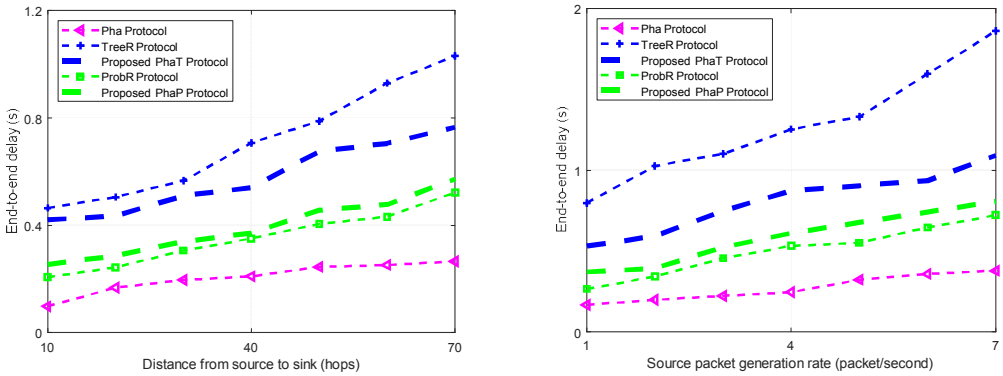


Figure 4.7: End-to-end delay of the protocols. (a) EED against varied source-sink distance. (b) EED against varied source packet rate.

Fig. 4.7 (a) also shows the impact of adding a second level phantom node routing on the EED of the PhaP and PhaT protocols. The PhaP has a slightly longer EED than ProbR. The increase in EED is controlled by the strategic location of the P_{ring} which guarantees that the directed random-walk routing is directed towards the sink node. The PhaT has considerably lower EED than the TreeR. However, the EED of PhaT is significantly high. The EED of PhaT can be up to 3 times the EED of the traditional Pha protocol which employs only one level of phantom node routing. The long EED is mainly due to the designated location of the phantom nodes which results in elongated routing paths. Packets are first routed to the near network border regions before they are routed to the sink node. These results demonstrate that the PhaP and PhaT protocols incur some tradeoffs between privacy protection and the EED performance.

Fig. 4.7 (b) shows the EED performance of the protocols at a fixed source-sink distance of 40 hops. The experiment scenarios included multiple source nodes. 100 packets were sent from each source node to the sink node at varied source packet rate from 1 to 7 packet/second. It is shown that EED of all the protocols increases with the increase in source packet rate. This is due to the fact that

조선대학교
CHOSUN UNIVERSITY

as more packets are generated per second, the probability of packet collision, packet loss, and packet retransmission events is increased. When packet retransmission events occur, the EED is significantly increased. The EED for the TreeR protocol increases at a higher rate due to the presence of a considerable amount of fake packets which increase the probability of packet collision events. The EED of ProbR protocol increases at a slower rate because the protocol distributes only one fake source packet at a time period. There is no fake source packet distribution in the PhaT and PhaP protocols. Consequently, the EED of the protocols increases at a slower rate.

In summary, the analysis results have demonstrated that factors such as the location of fake packet sources, location of phantom nodes, source packet generation rate, source-sink distance, and the amount of distributed fake packets can present significant impact on the SLP protection, energy consumption, PDR, and EED performance of the protocols. The TreeR protocol which positions the fake packet sources near the network border guarantees more obfuscating routing paths with strong SLP protection than the ProbR protocol which locates the fake packet sources near the sink node. The proposed PhaT protocol positions the phantom nodes in the near network border regions. Subsequently, it guarantees strong SLP protection than the PhaP protocol which positions the phantom nodes in the phantom ring located at some distance from the sink node. However, the TreeR and PhaT protocols incur relatively high energy consumption, low PDR and long EED. The TreeR protocol distributes a considerable amount of fake packets in the network. As a result, it achieves significantly higher SLP protection than the ProbR protocol which distributes only one fake packet at a time.

All the analyzed protocols offer lower SLP protection when the source packet generation rate is increased. Longer source-sink distance increases the complexity of the adversary tracing back attack which results in higher degree of SLP protection for all the protocols. By eliminating the fake packet traffic in the network, the proposed PhaT and PhaP protocols achieve strong SLP protection with controlled energy consumption, PDR, and EED. The PhaT protocol preserves effective SLP protection with better communication overhead than its contender TreeR protocol. Similarly, the PhaP protocol preserves stronger SLP protection than its contender ProbR protocol with controlled

조선대학교
CHOSUN UNIVERSITY

communication overhead. An additional superior feature of the PhaP protocol is that, it achieves minimized energy consumption in the near-sink region where the sensor nodes experience exhaustive energy consumption. High energy consumption for the sensor nodes in the near-sink region greatly affects the network lifetime [32], [94]. Thus, PhaP may be considered as a better candidate than ProbR when network lifetime maximization is an important requirement.

- **Summary and Recommendations**

The proposed protocols demonstrate more practical performance features than their contender ProbR and TreeR protocols. An important design issue of the proposed protocols is the additional computation load which is caused by the addition of the new second level phantom node. To reduce the computation load on the sensor node, one approach may be to introduce a new parameter called "Forward sessions". The parameter may be used to allow one route to forward multiple successive packets before a new route is created. This approach may reduce the computation load. However, the privacy protection level may be jeopardized. The practicality of the approach will be investigated in our future work. To minimize the EED which may be caused by the addition of the new second level phantom node in the proposed protocols, the computation of candidate second level phantom nodes is done during the network configuration phase. In PhaP, the computation of the P_{ring} is done during the network configuration phase and in PhaT the computation of N_{NB} and candidate npN is done during the network configuration phase. Furthermore, the P_{ring} is strategically positioned to ensure the packet routes are directed towards the sink node. Although the PhaT protocol incurs shorter EED than the TreeR, the EED is significantly high. One approach to improve the EED may be to introduce node offset angle routing technique during phantom node selection process. In [94], it was shown that the use of node offset angle during route creation process can improve the latency of a protocol. The use of node offset angle during phantom node selection process will be investigated in our future work. Comparing the complexity of the proposed PhaT and the TreeR protocol, the complexity of the TreeR protocol is significantly high. The TreeR protocol incurs high complexity due to the computation of the diversionary routes which route fake packets. For every packet transmission from

조선대학교
CHOSUN UNIVERSITY

a source node, a single backbone route of the TreeR protocol may create about nine diversionary routes. Each node in a diversionary route is required to send request messages for fake packets, also to transmit and receive the fake packets. As a result, the protocol is complex. The complexity of the proposed PhaP protocol is slightly higher than the complexity of ProbR protocol mainly due to the selection of the random second level phantom node. The privacy protection of the proposed PhaT protocol improves with the increase in network size. This is mainly due to the fact that larger networks facilitate the creation of longer and highly diversified routing paths. However, the communication overhead of the PhaT protocol increases with the increase in network size. This is due to the fact that the routing paths are designed to first diverge to the near network border regions where the phantom nodes are located, from the phantom nodes the packets are routed towards the sink node. Therefore, the location of the phantom nodes must be configured according to the network size to ensure controlled communication overhead. Both PhaT and TreeR protocols work well in WSNs which locate the sink node at the center of the WSN domain.

4.1.5. Remarks

This study has investigated the performance of fake source packet routing and phantom node routing protocols. The protocols are used for source location privacy (SLP) protection in monitoring WSNs. Fake source packet routing protocols have demonstrated some limitations including exhaustive energy consumption, low PDR and long EED. To address the limitations, this study has proposed two new phantom-based routing protocols, the PhaP and PhaT protocols. Based on strategies of two existing fake source packet routing protocols, the proposed protocols introduce new two-level phantom routing techniques. The routing strategies in the PhaP and PhaT protocols ensure two adversary confusion phases. Packets are routed from the source node to the destination sink node through the first adversary confusion phase and then through the second adversary confusion phase. In the PhaP protocol, the second level adversary confusion phase is executed inside a pursue ring located at some distance away from the sink node and a directed random-walk routing strategy is employed. In the PhaT protocol, the second level adversary confusion phase is executed inside a

조선대학교
CHOSUN UNIVERSITY

region near the network border and a backbone route is employed.

Analysis results show that the proposed PhaP and PhaT protocols demonstrate superior performance features to outperform the fake-packet based routing protocols. The PhaT protocol achieves strong SLP protection with improved communication overhead than its contender TreeR protocol. Equally, the PhaP protocol provides stronger SLP protection than its contender ProbR protocol with controlled communication overhead. Moreover, the experimental analysis reveal that the proposed protocols show practical results under varied network configurations. The proposed protocols can be practical in monitoring systems which guarantee strong SLP protection with strict requirements on energy efficiency. As part of future work, approaches to reduce the complexity of the protocols and techniques to improve reliability will be explored. Furthermore, the influence of the routing protocols on the network lifetime performance will be investigated.

4.2. Cost-effective Source Location Privacy Protocols

4.2.1. Background

Designing of the SLP routing schemes must consider one critical parameter, the energy consumption of sensor nodes. The sensor nodes usually run on battery power and are often deployed in remote and inaccessible areas where it is difficult to recharge or replace the batteries. For example, the Berkeley mote, which is powered by two AA batteries [108], can be used for monitoring applications in remote areas such as in ocean environments or in game reserves like the Serengeti national park. In such applications, the sensor nodes must be energy-efficient to allow for a long operational period of the nodes and long network lifetime. Many effective SLP routing schemes have a drawback of high energy consumption. For example, the schemes in [32], [40], [58] achieve strong SLP protection. However, the schemes incur very high packet transmission cost [79], [109]. In particular, the tree-based diversional routing scheme in [32] can have a total energy consumption of almost 20 times that of the traditional phantom routing scheme.

The SLP routing schemes in [40] and [58] incur high energy consumption especially for the sensor nodes located in the near-sink regions. The schemes use diversion and proxy nodes,

조선대학교
CHOSUN UNIVERSITY

respectively, to route packets originating from the near-sink regions. Due to the location of the diversion and proxy nodes, the routes become longer and introduce higher energy consumption. In many network configurations, the near-sink region has a greater load of packets to forward to the sink node which results into exhaustive energy consumption of the sensor nodes [32], [80], [110], [111]. In this study, we assume that exhaustive energy consumption in near-sink regions is a limitation for the schemes in [40] and [58]. The exhaustive energy consumption in [40] is also pointed out in other recent studies including [43], [62]. Due to the exhaustive energy consumption, the sensor nodes around the sink node deplete their battery power at a fast rate and become dead nodes. The limitation may further affect the network performance by triggering the energy-hole problem and shortening the network lifetime [32], [80], [81], [108], [110]-[112]. To address the performance issues of the schemes in [40] and [58], we design a new routing algorithm to provide strong SLP protection and minimize the energy consumption in the near-sink region. The routing algorithm also improves other packet transmission cost parameters such as packet delivery latency and delivery ratio.

A new path node offset angle routing algorithm is proposed. In the proposed algorithm, all ordinary sensor nodes compute and record their θ with respect to the sink node. When a source node in the near-sink region wishes to send packets to the sink node, the source node first determines its contrived region, randomly generates three candidate path nodes in three different forwarding regions, and computes a random value of an arbitrary factor. Based on the values of the computed arbitrary factor and the path node θ, a packet route is created through a randomly selected path node in one of the three forwarding regions. By using the proposed algorithm, successive packets are randomly routed in the network and the routing paths achieve high path diversity. The routing paths of the proposed algorithm are relatively shorter than the routing paths in [40] and [58]. However, the utilization of the path node θ and arbitrary factor parameters guarantee that the routes are highly randomized and provide similar levels of SLP protection for the source nodes in the near-sink region. Furthermore, the proposed algorithm offers cost-effective routing paths. Table 4.4 summarizes the limitations of the schemes in [40], [58] and the strategies for improvement.

조선대학교
CHOSUN UNIVERSITY

Table 4.4: Limitations of the existing schemes and strategies for improvement in proposed algorithm.

Limitations	Strategy for improvement in proposed routing algorithm
Both [40] and [58] use elongated routes which first divert to a diversionary [40] or proxy [58] node located outside the near-sink region.	Path nodes are located within the near-sink region to create relatively short routing paths.
Elongated routes increase the packet transmission cost including the energy consumption and packet delivery latency.	Relatively short routing paths effectively regulate the packet transmission cost.
Each source node has only two candidate diversionary or proxy nodes for the random route creation process.	Each source node has three candidate path nodes to guarantee highly dynamic route creation process with high path diversity.
Diversionary or proxy node selection process is based on the computation of a random bias number and a pre-defined threshold value.	Path node selection process is based on the computation of path node offset angles and arbitrary factors, and the location of contrived regions for vastly random routing paths.
A selected diversionary or proxy node has a small probability of near source node location.	Contrived regions are designed to guarantee selected path nodes are located far from the source node, to make the adversary tracing back process more complex and preserve strong SLP protection.

- **Contributions**

Specifically, this study addresses the limitations of the schemes in [40] and [58]. Thus, the objectives of the study are to: (1) improve the performance of the routing schemes in [40] and [58] by exploiting the proposed path node offset angle routing algorithm, (2) reduce the energy consumption for sensor nodes in the near-sink regions and avert the energy-hole problem, and (3) evaluate the performance of the proposed schemes to demonstrate their superiority over the existing schemes.

4.2.2. Related Work

The use of angle-based routing for costeffective packet routing was demonstrated in [34], [113]. In [34], the scheme uses the transmitting offset angles and constrained probability to prevent an adversary from tracing back to locate the source node. Each sending node determines a specific selection domain for the next-hop node according to the dangerous distance and the wireless communication range. Then, it analyzes the angles of the candidate nodes based on the direction of the nodes to the sink node. Lastly, the sending node calculates the selected weights of the candidate nodes according to their angles, and the selected weights are used to decide which node becomes the next-hop node. By randomly selecting the next-hop node under constrained angles, the scheme can

조선대학교
CHOSUN UNIVERSITY

ensure that relay nodes are relatively close to the sink node. When relay nodes are close to the sink node, the routing paths become relatively short to minimize the energy consumption of the scheme. In [113], the anglebased dynamic routing scheme uses location information of the nodes and calculates inclination angles formed between the nodes. The angles include the inclination angle between a sending node and a receiving node, and the inclination angle between a sending node and the sink node. Based on the angles, the scheme generates a set of candidate neighboring nodes. The candidate set changes at every packet forwarding event to form dynamic paths toward the sink node. The analysis results in [34], [113] revealed that the angle-based routing schemes were capable of protecting the privacy of source nodes with controlled packet transmission cost.

Other angle-based routing schemes were proposed in [101], [114], [115]. In [101], the phantom routing with the location angle scheme modified the phantom single-path routing scheme by introducing inclination angles of sensor nodes in the random-walk section of the phantom single-path routing. The scheme assigned different probabilities to the nexthop nodes in the random-walk area to optimize the routing paths for source location privacy protection. In [114], the two-phantom angle-based routing scheme considered a triplet for selecting the phantom nodes. A triplet was considered to be a group of three nodes formed on the basis of three parameters: distance from the sink node, location information, and the inclination angle between them. Phantom selection was performed for every packet forwarding instance to create dynamic routing paths for the packets. In [115], the anglebased intermediate node scheme allowed the source node to determine two types of angles: a maximum angle between the last intermediate node and the source node according to the sink node, and an actual angle between the last intermediate node and itself according to the sink node. Then, the source determined the number of intermediate nodes and generated the distances between the source node and the intermediate nodes. Based on the angles and distances, intermediate nodes were selected for packet routing.

Other effective techniques for regulating the packet transmission cost in WSNs and alleviating the energy-hole problem were discussed in [80], [81], [108], [110]-[112]. The techniques include the following strategies: (1) Provide effective routing protocols through power-aware routing, by

조선대학교
CHOSUN UNIVERSITY

providing multiple routing paths to balance the energy consumption, and selecting the optimal path from the available paths based on the cost of each path. (2) Allow sensor nodes to use different transmission power levels for energy-efficient data transmission. For example, the transmission power of a Berkeley mote can be made adjustable to regulate its transmission power according to the distance between the transmitter and the receiver node. The Berkeley motes have 100 transmission power levels [111]. Using lower transmission power in the nearsink region and higher transmission power in the regions farther away from the sink can effectively balance the energy consumption in the network. (3) Use mobile relays to share the load of sensor nodes around the sink node, the mobile relays only need to be within two hops from the sink. (4) Deploy sensor nodes with greater initial energy, or more sensor nodes in the regions which consume large amounts of energy. (5) Employ a mobile sink node to balance the energy consumption. With a mobile sink, nodes near the sink would change over time and share the load. Static sensor nodes only send their data when the sink is within their communication range. (6) Exploit the non-uniform clustering algorithms. Cluster-based networks can achieve higher energy efficiency than flat networks. Using an unequal cluster-radius can be effective at balancing the energy consumption. (7) Construct load-balancing networks.

4.2.3. Problem Statement

Based on the limitations in Table 4.4, the primary focus of this study is to design a new path node offset angle SLP routing algorithm with the main objective of minimizing the packet transmission cost for the schemes in [40] and [58]. To achieve the objective, two tasks are performed: design the new routing algorithm to maximize the SLP protection, and minimize the energy consumption (E). To characterize the performance of the proposed and existing schemes, equations (15) and (16) are assumed.

The energy consumption model in section 2.3 assumes that the sensor nodes consume most of their energy while transmitting and receiving packets. Also, the energy consumption of the sensor nodes is characterized by the distance, d, and size of the packets, l, as shown in Fig. 4.8. The proposed routing algorithm employs relatively short but highly randomized routing paths, with fewer packet

조선대학교
CHOSUN UNIVERSITY

transmission and reception events (hops). If each hop involves consumption of E_{trans} and E_{rec}, the total energy consumption, E, for delivering a packet at the sink node is computed using equation (15). To minimize the energy consumption, equation (16) is assumed. In the equations, h represents the number of hops.

$$E = \sum_{i=1}^{h} \left(E_{trans_i} + E_{rec} \right) \tag{15}$$

$$\min\ (E) = \min\ (h) \tag{16}$$

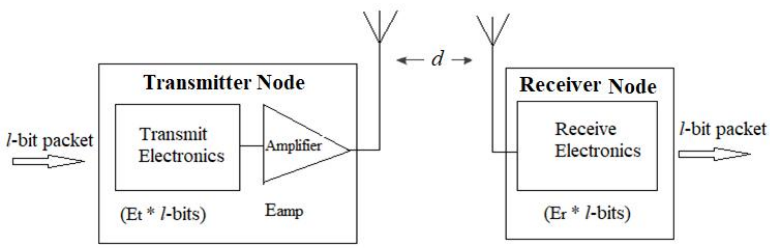


Figure 4.8: Energy consumption parameters for transmitting and receiving *l*-bit packet between two nodes of a WSN.

4.2.4. Proposed Path Node Offset Angle Routing

The proposed routing algorithm aims to provide a high degree of source location privacy protection while improving the packet transmission cost of strategic location-based random routing [40] and proxy node routing [58] schemes. Hereafter, we refer to the strategic location-based random routing scheme as ‘‘Strat-R’’and the proxy node routing scheme as ‘‘Proxy-R.’’ The proposed path node offset angle routing algorithm is adopted into both schemes, Strat-R and Proxy-R, to produce modified schemes, namely ‘‘Angle-Strat’’ and ‘‘Angle-Proxy’’, respectively. The key difference between the proposed Angle-Strat and Angle-Proxy schemes is the structure of the WSN domains. Angle-Strat locates the sink node at the center of the network with a circular near-sink region while Angle-Proxy locates the sink node toward the network edge with a square near-sink region.

조선대학교
CHOSUN UNIVERSITY

- **Overview of the Proposed Path Node Offset Angle Routing Algorithm**

The algorithm employs a sink node at the center of the WSN domain. It divides the WSN into two regions: the near-sink region and the region away from sink. The near-sink region is further divided into four quadrants as shown in Fig. 4.9. An $X-Y$ coordinate is generated at the sink node location as shown in the Fig. 4.9 and five parameters are introduced. The parameters are identified as follows.

Path node (pathNode): the relay node in the network domain randomly generated and then selected during the route creation process. A routing path of any packet from a source node must pass through a randomly selected path node.

Contrived region (CR): the quadrant where the source node is located. It is the restricted region around the source node where the path node cannot be located. Locating the path node outside the contrived region ensures an increased complexity for the adversary during the back tracing attack, to maximize the SLP protection. It also ensures stronger SLP protection than that of the traditional schemes such as the shortest path routing [59], phantom single-path routing [71], and the intermediate node routing protocol [88] schemes. For every source node, one out of the four quadrants is a contrived region.

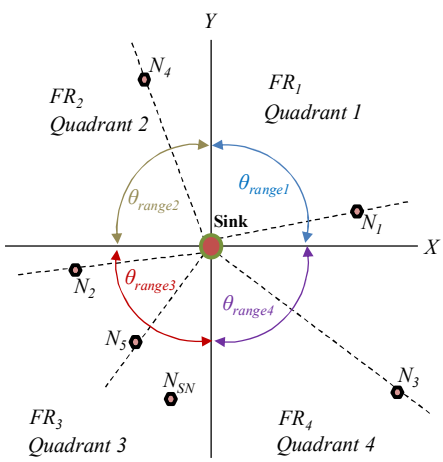


Figure 4.9: Configuration of the near-sink region in the proposed path node offset angle routing algorithm.

조선대학교
CHOSUN UNIVERSITY

Forwarding regions (FR): the three regions (quadrants) in the near-sink region where path nodes are located. A source node identifies the quadrant of its location as its contrived region. The other three quadrants become forwarding regions.

Path node offset angle (θ): the angle formed between the *X*-axis and the imaginary line connecting the path node and the sink node.

Arbitrary factor (AF): the route creation factor. *AF* is computed by a source node during the path node selection process. *AF* is designed to ensure exposure of the path node location information to the adversary is minimized by randomizing the path node location for each successive packet.

Before any packet transmission is done in the network, it is assumed that the network initialization process is performed by a network planner to determine the network architecture according to Figures 4.11, 4.12, 4.13, 4.14. The network initialization process is explained in section 2.1. Also, the process is explained in detail in [116]. At the end of the initialization process, all nodes are localized and become aware of their locations as well as the location of their neighboring nodes and the sink node. Furthermore, the process enables the sensor nodes to realize the location of their contrived region and forwarding regions. Thereafter, the θ is computed according to the process in section 2.1.

The θ for each seansor node is computed according to quadrants. For example, in Fig. 4.9, sensor nodes N_1, N_4, N_2 and N_5, and N_3 compute their θ in ranges θ_{range1}, θ_{range2}, θ_{range3}, and θ_{range4}, respectively. The θ for each sensor node is a fixed value and it is appended to the sensor node parameters together with other features such as the node ID. Upon asset detection, a source node randomly generates a set of three candidate path nodes, one path node in each forwarding region. It records the values of the θ for each candidate path node. Then it computes an arbitrary factor, A_F, according to equation (17). K is a constant number 0.9. R_F is a generated random factor with values distributed from 0.1 to 0.9. Nine different values of A_F are possible as shown in Table 4.5. The source node computes a random value of A_F to use in the path node selection process. Two threshold values of A_F are used: Th_P and Th_Q. The values of Th_P and Th_Q are 0.55 and 0.65.

조선대학교
CHOSUN UNIVERSITY

$$A_F = \frac{K}{1 + R_F} \tag{17}$$

Table 4.5: Determination of A_F value.

R_F	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
A_F	0.81	0.75	0.69	0.64	0.6	0.56	0.52	0.5	0.47

Using the value of A_F, one path node is selected from the set of candidate path nodes according to the path node selection process summarized in Table 4.6. The path node selection algorithm is shown in algorithm 4.3. Randomly selecting one path node from the three different forwarding regions provides packet routes which appear as if they originate from a broader range of source node locations, making the routes less predictable to the adversary. For example, in Fig. 4.9, assuming N_{SN} is the source node, then FR_3 becomes the CR and N_1, N_3, and N_4 may be candidate path nodes. N_1 may be selected as the random path node for route creation.

Table 4.6: Path node selection process based on the path node θ, A_F, and CR parameters.

Source node location	CR	θ_{range} identification for path node selection		
		$A_F < Th_P$	$Th_P < A_F < Th_Q$	$A_F > Th_Q$
Quadrant 1	FR_1	θ_{range2}	θ_{range3}	θ_{range4}
Quadrant 2	FR_2	θ_{range3}	θ_{range4}	θ_{range1}
Quadrant 3	FR_3	θ_{range4}	θ_{range1}	θ_{range2}
Quadrant 4	FR_4	θ_{range1}	θ_{range2}	θ_{range3}

After the path node selection process, the source node randomly sends the packets to the selected path node using a random-walk routing strategy. Upon reception of the packets, the path node randomly forwards the packet to the destination sink node using random-walk routing. The random-walk routing strategy involves a next-hop selection process at every packet forwarding instance. In the process, the sending node determines a group of neighboring nodes with a shorter hop distance to the destination node than the sending node itself. One neighboring node from the group is randomly selected as the next-hop node. At the source node, the destination node is the

조선대학교
CHOSUN UNIVERSITY

Algorithm 4.3: Proposed path node selection algorithm

Input:
S_{LOC}: Location of sink node;
S_{hop}: Hop count at sink node;
Output:
Routing path to sink node;
Begin

```
network initialization
compute θ
sensor node become sourceNode
determine CR
generate a set of candidate pathNode
compute A_F
if (CR == FR1) do
    if (A_F < Th_P) then
        select pathNode with θ within θ_range2
    else if (Th_P < A_F < Th_Q) then
        select pathNode with θ within θ_range3
    else if ( A_F > Th_Q) then
        select pathNode with θ within θ_range4
    end
else if (CR == FR2) do
    if (A_F < Th_P) then
        select pathNode with θ within θ_range3
    else if (Th_P < A_F < Th_Q) then
        select pathNode with θ within θ_range4
    else if ( A_F > Th_Q) then
        select pathNode with θ within θ_range1
    end
else if (CR == FR3) do
    if (A_F < Th_P) then
        select pathNode with θ within θ_range4
    else if (Th_P < A_F < Th_Q) then
        select pathNode with θ within θ_range1
    else if (A_F > Th_Q) then
        select pathNode with θ within θ_range2
    end
else if (CR == FR4) do
    if (A_F < Th_P) then
        select pathNode with θ within θ_range1
    else if (Th_P < A_F < Th_Q) then
        select pathNode with θ within θ_range2
    else if ( A_F > Th_Q) then
        select pathNode with θ within θ_range3
    end
 end
```

selected path node. At the path node, the destination node is the sink node. Fig. 4.10 shows the random-walk routing strategy between the source node and path node, and between the path node and the sink node. For example, in Fig. 4.10, if a packet is from the source node to the sink node through the path node, nodes N_7 and N_8 are the next-hop nodes for the source node and N_7,

조선대학교
CHOSUN UNIVERSITY

respectively, while nodes N_9 and N_{10} are the next-hop nodes for the path node and N_9, respectively.

To guarantee minimized exposure of the path node location information to the adversary, the proposed algorithm uses the A_F parameter to ensure a new path node is randomly selected from a different forwarding region, for each successive packet forwarding event. If successive packets arrive at the sink node from a wide range of directions, the adversary becomes highly confused, makes insignificant progress towards the path nodes and the vulnerability of the path nodes is very much reduced.

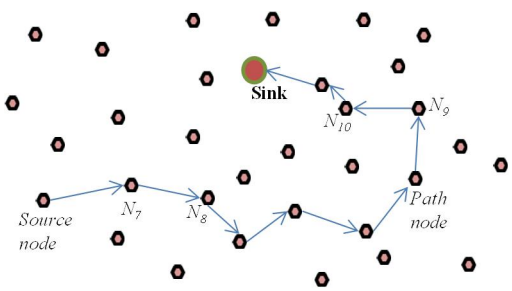


Figure 4.10: Random-walk routing strategy of the proposed routing schemes.

- **Overview of the Proposed Angle-Strat Routing Scheme**

The Angle-Strat routing scheme adopts the path node offset angle routing algorithm to route packets for source nodes located in the near-sink region. For the regions away from the sink, the routing strategy is similar to the Strat-R scheme. It is assumed that Strat-R is adequately cost-effective for the source nodes that are distant from the sink region. Fig. 4.11 shows the distribution of the network regions in the Strat-R scheme. The scheme divides the sensor domain into two regions: the near-sink region and region away from the sink. For Strat-R, nodes in the near-sink region route their packets through diversion nodes, while nodes in regions away from the sink route their packets through the mediate nodes. Diversion nodes are located in ring r_D, where the width of $r_D = r_{HD} - r_H$. Mediate nodes are located in ring r_M, where $r_M = r_{HM} - r_{HD}$.

In the Angle-Strat scheme, the near-sink region has a circular structure and is defined by the radius r_{SR} as shown in Fig. 4.12. For a smooth modification of Strat-R into the Angle-Strat scheme,

조선대학교
CHOSUN UNIVERSITY

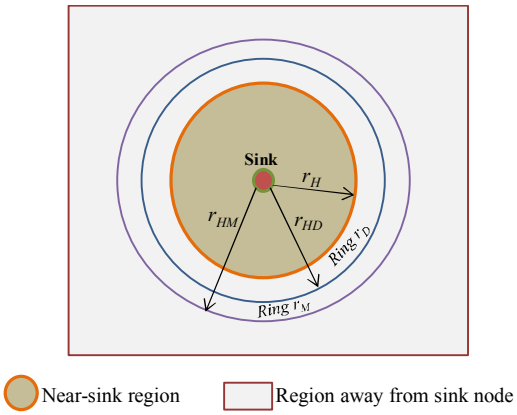


Figure 4.11: Distribution of the WSN regions for Strat-R scheme.

the radius r_{SR} is assumed to be equal to the radius r_H. i.e., $r_{SR} = r_H$. All nodes which are located within distance r_{SR} from the sink node are considered as nodes in the near-sink region and adopt the path node offset angle routing algorithm. When a source node detects an asset, it computes the path node selection process according to Table 4.6 and algorithm 4.3. Fig. 4.12 also shows the forwarding regions, the $X-Y$ coordinate generated at the sink node, the path node offset angle ranges, example candidate path nodes, and the boundary of the near-sink region in the proposed Angle-Strat routing

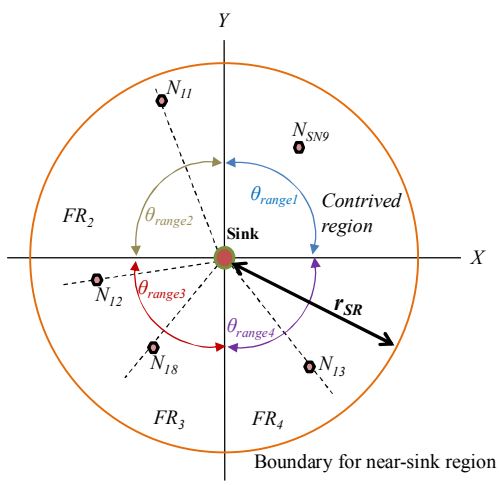


Figure 4.12: Configuration of near-sink region in the proposed Angle-Strat routing scheme.

조선대학교
CHOSUN UNIVERSITY

scheme. If node N_{SN9} is assumed as a source node, quadrant 1 becomes the contrived region and N_{11}, N_{13} and N_{18} may be generated as candidate path nodes. Consequently, N_{11}, N_{13} or N_{18} may be selected for route creation process.

- **Overview of the Proposed Angle-Proxy Routing Scheme**

Similar to Angle-Strat, the Angle-Proxy model adopts the path node offset angle routing algorithm to route packets for source nodes located in the near-sink region. Fig. 4.13 shows the distribution of the network regions in the Proxy-R scheme. The scheme divides the WSN domain into four quadrants as shown in the Fig. 4.13. The sink node is positioned at the center of Quadrant1. The proxy nodes are strategically located in proxy regions $Proxy_{R2}$, $Proxy_{R3}$, and $Proxy_{R4}$ in Quadrants 2, 3 and 4, respectively. During packet routing, a source node randomly selects a proxy region of a quadrant other than its own. Packets are routed through the selected proxy nodes. Source nodes in the near-sink region route their packets through proxy regions $Proxy_{R2}$ or $Proxy_{R4}$.

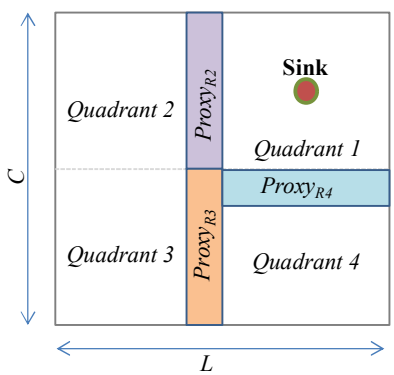


Figure 4.13: Distribution of the WSN regions for Proxy-R scheme.

The Angle-Proxy scheme considers the Quadrant 1 region shown in Fig. 4.13 as the near-sink region. The scheme further divides the region into four quadrants as shown in Fig. 4.14. V is the width of the near-sink region. The sink node is located at the center of the region. All nodes which are located within width V are considered as nodes in the near-sink region and adopt the path node offset angle routing algorithm. When a source node detects an asset, it computes the path node selection process according to Table 4.6 and algorithm 4.3. After the path node is selected, packets

조선대학교
CHOSUN UNIVERSITY

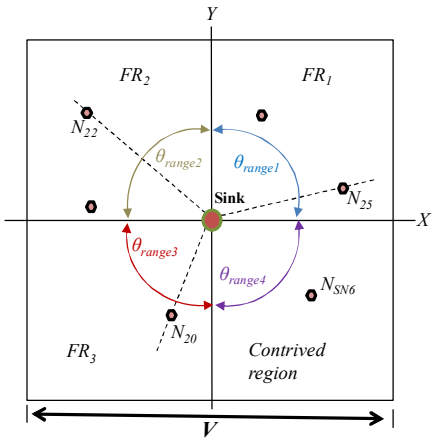


Figure 4.14: Configuration of the near-sink region in the Angle-Proxy routing scheme.

are routed from the source node to the path node through random-walk routing as illustrated in Fig. 4.10. Similarly, the path node forwards the packets to the sink node through random-walk routing strategy.

4.2.5. Performance Analysis

MATLAB simulation environment was used for performance analysis of the proposed Angle-Strat and Angle-Proxy schemes. A total of six schemes were included in the analysis: the Strat-R, Proxy-R, Angle-Strat, Angle-Proxy, RIN, and Pha. The Pha and RIN schemes were included in the analysis as representative schemes for the traditional SLP routing schemes, for comparative analysis. Performance evaluation of the schemes was done using five performance metrics: SP, ASR, energy consumption, packet delivery latency, and PDR. The SP and ASR metrics measured the privacy performance of the schemes while energy consumption, packet delivery latency, and PDR metrics measured the packet transmission cost.

- **Simulation Parameters and Values**

The network model in section 2.1 and adversary model in section 2.2 were assumed. MATLAB simulation environment was used to simulate a WSN with N_{SL} of 2000 m. For good coverage in the network, a total of 2500 sensor nodes were randomly distributed in the WSN domain. Thus, N_{SN} was 2500. Only one sink node was assumed. The S_{CR} was set to 30 m to ensure multi-hop communications

조선대학교
CHOSUN UNIVERSITY

and energy conservation. A cautious adversary was deployed with initial location in the locality of the sink node to ensure maximum probability of packet capture. The A_{HR} was set to 30 m, similar to the S_{CR} to ensure the adversary performs hop-by-hop back tracing attack. The A_{WT} was set to 4 source packets. The following configurations were done. For Strat-R, r_H = 400 m; r_D = 200 m and r_M = 200 m, following the distribution shown in Fig. 4.11. For Proxy-R, L = 2000 m and C = 2000 m. The length and width of the proxy regions were as follows: the lengths of $Proxy_{R2}$, $Proxy_{R3}$, and $Proxy_{R4}$ were $0.5C$, $0.5C$, and $0.5L$, respectively. The widths of $Proxy_{R2}$, $Proxy_{R3}$, and $Proxy_{R4}$ were $0.2L$, $0.2L$, and $0.2C$, respectively. The configuration of the Proxy-R network followed the distribution of the regions shown in Fig. 4.13. For AngleStrat, $r_{SR} = r_H$ = 400 m, according to the distribution in Fig. 4.11 and Fig. 4.12. For Angle-Proxy, V = 1000 m, according to the distribution in Fig. 4.14. The network simulation parameters are summarized in Table 4.7. The simulation was run for 500 iterations and average values were considered.

Table 4.7: Network simulation parameters

Parameter	Value
N_{SL} (m)	2000
N_{SN}	2500
N_{sink}	1
S_{CR} (m)	30
A_{HR} (m)	30
A_{WT} (source packets)	4
r_H (m)	400
r_D (m)	200
r_M (m)	200
r_{SR} (m)	400
V (m)	1000
L (m)	2000
C (m)	2000
P_{sz} (bit)	1024
SN_{PR} (packet/second)	1
S_{IE} (J)	0.5
Adversary initial location	In the vicinity of sink node

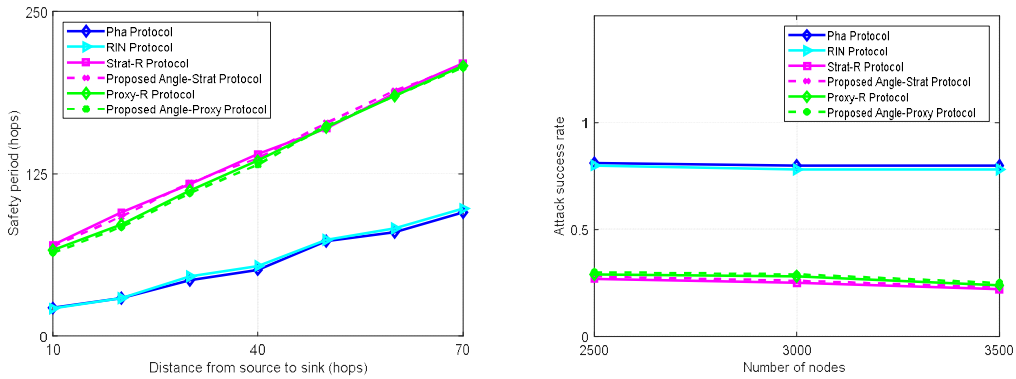
- **Simulation Results and Discussions**

The results in Fig. 4.15 (a) show that the four schemes: Strat-R, Proxy-R, the proposed Angle-Strat, and Angle-Proxy have somewhat comparable privacy performance. In the near-sink region, Strat-R

조선대학교
CHOSUN UNIVERSITY

offers slightly longer safety period than the Proxy-R because the use of strategically positioned diversion nodes provides a marginal increase in path diversity. Despite the relatively short packet routes, the proposed schemes are able to achieve a high degree of privacy protection similar to the other schemes because they employ path node offset angle routing strategy. The schemes use contrived regions to ensure that the path nodes are located away from the source nodes to obfuscate the adversary when it tries to back-trace the packet routes. Furthermore, the use of A_F ensures that successive packets use path nodes selected from a diverse range of path node offset angles to guarantee the packet routes are equally obfuscating to the adversary as compared to Strat-R, and Proxy-R schemes. For example, in Fig. 4.16, if packets from source node 1 are routed using the proposed Angle-Strat or Angle-Proxy schemes, path node 2 (*PN2*) with $\theta = \theta_2$ may be selected when θ selection falls under θ_{range1}. *PN3* with $\theta = \theta_3$ or *PN1* with $\theta = \theta_1$ may be selected when the θ selection falls under θ_{range2} or θ_{range4}, respectively. For the next packet, the source node 1 may generate other path nodes such as *PN4*, *PN7*, and *PN8*, and one *PN* is randomly selected for the packet routing. Similarly, for source node 2, the source node may generate path nodes such as *PN5*, *PN6*, and *PN9*, and one *PN* is randomly selected.

The process of generating a set of candidate path nodes at different path node offset angles improves the path diversity and randomness of the routing paths. As a result, it becomes a complex



(a) (b)

Figure 4.15: Privacy performance of the routing schemes. (a) SP at various source-sink distances. (b) ASR against varied number of sensor nodes.

조선대학교
CHOSUN UNIVERSITY

task for the adversary to capture successive packets. Adversary can make significant progress in the back tracing attack only if it captures a sufficient number of successive packets. In the proposed schemes, the adversary attack progress is very much hindered.

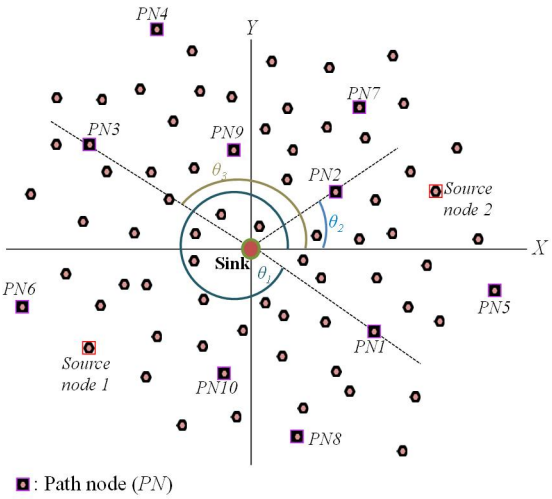


Figure 4.16: Example path node selection in the proposed routing schemes for the near-sink regions.

The Pha and RIN schemes offer the lowest privacy level because they use fixed routes between the phantom/intermediate nodes and the sink node. The fixed routes can easily be traced by the adversary. Moreover, the schemes have a higher probability of the phantom or intermediate nodes for successive packets to be located very near the sink node, when a source node is located in the near-sink region. Continuously selecting a phantom or intermediate node which is located very near the sink node causes weak privacy protection, since it will take a short time for an adversary to successfully backtrace the routes to the nodes. Fig. 4.15 (b) shows the ASR of the schemes at a trace time of 800 source packets for different node density. In this study, trace time refers to the time spent by the adversary since it initiated the back tracing attack at the sink node. The proposed Angle-Strat and Angle-Proxy schemes are capable of achieving low ASR. The ASR for the schemes tend to decrease with the increase in the number of sensor nodes. The Fig. 4.15 (b) shows similar privacy performance between the Strat-R, Proxy-R, Angle-Strat, and Angle-Proxy schemes.

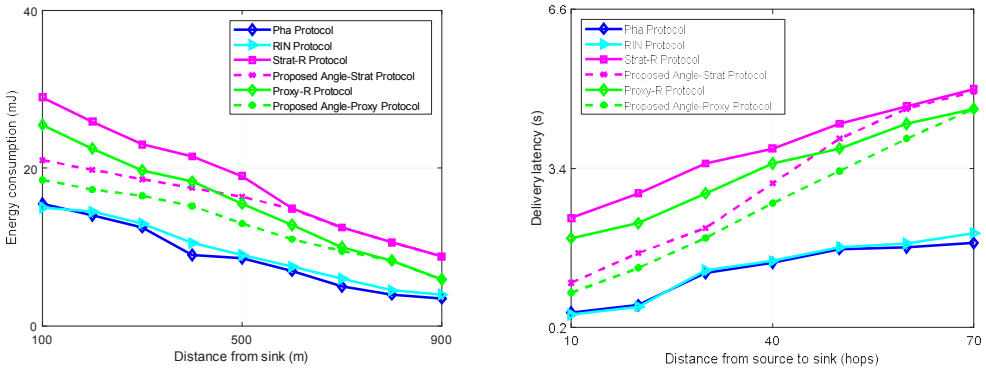
조선대학교
CHOSUN UNIVERSITY

The results in Fig. 4.17 show the packet transmission cost of the routing schemes for delivering packets to the sink node. The energy consumption per packet delivery was computed using the energy consumption model in section 2.3. In the energy consumption analysis, 24 experiment scenarios were assumed, each scenario with a different source node location. 12 scenarios were run for source nodes in the near-sink regions and 12 scenarios in the regions away from sink node. For the near-sink region scenarios, three scenarios were run in each quadrant. In each scenario, 1000 packets were transmitted from a source node to the sink node using the six analyzed schemes. After all the packets were delivered at the sink node, for each scenario, the energy consumption per sensor node was observed at different node locations.

Fig. 4.17 (a) show the energy consumption per sensor node at various sensor node locations. It shows that the sensor nodes using the proposed Angle-Strat and Angle-Proxy schemes have lower energy consumption near the sink region. The schemes achieve lower energy consumption by using routing paths which are shorter than the routes of Strat-R and ProxyR as demonstrated in Fig. 4.18. While Strat-R and Proxy-R use longer routes to obfuscate the adversary for source nodes in the near-sink region, the proposed schemes apply relatively short routing paths. Shorter routing paths incur fewer packet forwarding events in the near-sink region. With fewer packet forwarding events, the sensor nodes consume less transmit and receive energy. The proposed schemes achieve strong SLP protection while being more energy-efficient in the nearsink region. For example, in Fig. 4.17 (a), at a distance of 200 m from the sink node where it is assumed to be in the nearsink region, the total energy consumption of sensor nodes when using routing schemes Strat-R, Angle-Strat, Proxy-R, and Angle-Proxy are 25.9 mJ, 19.6 mJ, 22.5 mJ, and 17.1 mJ, respectively.

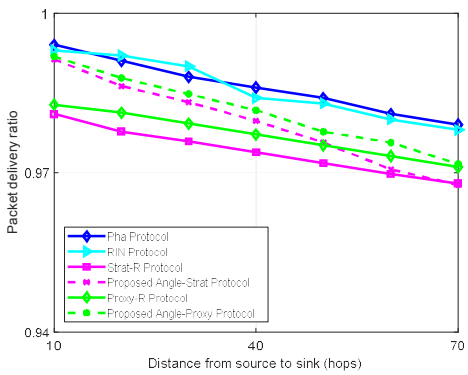
The graphs for Strat-R and Angle-Strat converge at 600 m from the sink node while the graphs for Proxy-R and AngleProxy converge at 700 m from the sink node. This structure of the graphs illustrates that the modified schemes consume lower energy in the near-sink regions due to the adoption of the path node offset angle routing algorithm. Beyond the near-sink region, the schemes assume the same routing strategies as their contender schemes. Hence, the same energy consumption performance is experienced. Despite the near-sink region boundary being at 400 m for both Strat-R

조선대학교
CHOSUN UNIVERSITY



(a)

(b)



(c)

Figure 4.17: Packet transmission cost of the routing schemes. (a) Energy consumption. (b) Packet delivery latency. (c) Packet delivery ratio.

and Angle-Strat, the region between 400 m and 600 m in the StratR scheme has higher energy consumption, because this region has more packet forwarding events through the diversion nodes. In the Angle-Strat scheme, the diversion node region is not defined, instead, nodes in the region are used simply as relay nodes with fewer packet forwarding events. Similarly, despite the near-sink region boundary being at 500 m for both Proxy-R and Angle-Proxy, the region between 500 m and 700 m in the Proxy-R scheme has more packet forwarding events through the proxy nodes. This work embraces the conclusion that the reduced energy consumption in the nearsink region can have a positive impact on the performance of the network, including improved network lifetime and an alleviated energy-hole problem. Comparing the energy consumption of the proposed schemes and

조선대학교
CHOSUN UNIVERSITY

that of the traditional Pha or RIN, the proposed schemes incur an acceptable increase in energy cost.

Fig. 4.18 further demonstrates the relatively short and energy-efficient routing paths of the proposed schemes. The Fig. 4.18 shows the length of the routing paths for 30 successive packets sent from a source node in the near-sink region. For example, the path length of the Strat-R, Angle-Strat, Proxy-R, Angle-Proxy, Pha, and RIN schemes for delivering packet number 18 to the sink node are, 46 hops, 30 hops, 24 hops, 17 hops, 11 hops, and 15 hops, respectively. Assuming each hop involves consumption of E_{trans} at the transmitting node and E_{rec} at the receiving node, the total energy consumption E_{tot} for delivering one packet at the sink node can be approximated as $E_{tot} = E_{trans} * N_{hop} + E_{rec} * N_{hop}$. It is evident that the proposed schemes will incur lower energy cost per packet transmission compared to their contender schemes. Similarly, the short routing paths will result in improved packet delivery latency and delivery ratio.

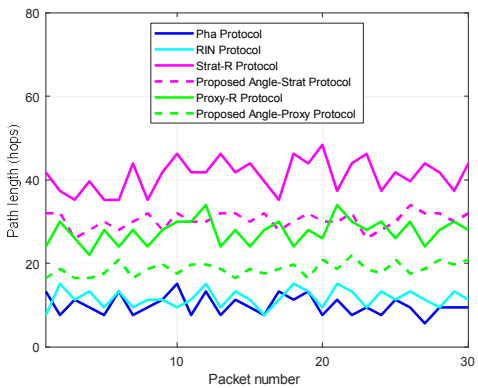


Figure 4.18: Path length of the routing schemes.

The experimental evaluation of the schemes included the analysis of packet delivery latency and delivery ratio. In this study, packet delivery latency is defined as, the time required to transmit a packet of data from a source node to the sink node. It is highly dependent on the length of the routing paths. Longer routing paths incur higher delivery latency. Delivery ratio is the ratio of the number of packets successfully delivered at the sink node to the total number of packets sent from a source node. The experiment scenarios included source nodes at different source-sink distances. 100 packets were

조선대학교
CHOSUN UNIVERSITY

sent from each source node to the sink node and average values for delivery latency and delivery ratio were found. Figures 4.17 (b), (c) show that the Angle-Strat and Angle-Proxy have better packet delivery latency and delivery ratio than their contenders Strat-R and Proxy-R. Strat-R and Proxy-R achieve high privacy protection by ensuring longer routing paths hence high delivery latency. The short routing paths of the proposed Angle-Strat and Angle-Proxy schemes ensure fewer packet forwarding events to minimize the delivery latency for the near-sink regions. Beyond the near-sink region, the graphs for Strat-R and Angle-Strat, and for Proxy-R and Angle-Proxy, converge. The convergence is due to similar performance since the path node offset angle routing algorithm is adopted only in the near-sink regions. These results can be a clear indication that the Angle-Strat and Angle-Proxy schemes are capable of controlling the packet transmission costs in the network, and can be considered when parameters such as delivery latency and reliable packet transmission are important. From these findings, this work can conclude that the proposed Angle-Proxy scheme is a more cost-effective SLP scheme and practical for WSNs which

locate the sink node towards the network edge while the proposed Angle-Strat is more practical for WSNs which locate the sink node at the center of the WSN domain. Furthermore, the schemes can be more appropriate for network scenarios where network reliability is required and the energy-hole problem is undesirable.

A possible limitation of the proposed routing schemes may happen when a source node is located near the *X*-axis or *Y*-axis and it randomly selects a path node which is located adjacent to the axis. In such scenarios, the location information about the source node may be exposed to the adversary. However, this limitation is minimized by using the A_F parameter which guarantees high path diversity. A_F is designed to ensure a high probability that, path nodes for successive packets are selected from different forwarding regions. If successive packets are routed randomly in different regions of the network, it becomes difficult for the adversary to capture the packets. Hence, it makes no significant progress towards the source node. Based on the value of *AF*, successive packets from the same source node are guaranteed to use completely different routes to sustain strong SLP protection. When considering the storage cost of the proposed algorithm, there is a slight increase in

조선대학교
CHOSUN UNIVERSITY

the required memory size of the sensor nodes compared to the Strat-R and Proxy-R schemes. The proposed algorithm requires an additional one byte memory for each sensor node to store the θ information. We assume that the additional memory space is acceptable for event monitoring WSNs.

4.2.6. Remarks

It is typical for individuals and organizations to use WSN technology to secure and monitor assets of great value. When the WSNs are deployed in remote areas, it becomes difficult to recharge or replace the batteries in the sensor nodes. It is then essential that network designers offer energy-efficient source location privacy routing schemes. Realizing the need, this study has proposed a new path node offset angle routing algorithm. The study has also demonstrated the adoption of the algorithm to improve the packet transmission cost of two existing schemes. The modified schemes effectively utilize routing paths which are relatively short but vastly diverse. The tactical use of path node offset angles, contrived regions, and arbitrary factors during the path node selection process guarantees cost-effective routing paths. The modified schemes are well-suited for systems which require strong source location privacy protection with controlled packet transmission cost. Moreover, the schemes are capable of alleviating the energy-hole problem in WSNs. As part of future work, techniques to regulate the packet transmission cost in the regions away from the sink node will be considered. In addition, the feasibility of the schemes in various event-driven and resource-constrained application scenarios will be investigated.

조선대학교
CHOSUN UNIVERSITY

Chapter 5

Privacy Protection Reliability of Routing Protocols

5.1. Background

In recent years, WSN technology has gained increasing popularity in ubiquitous support of sensing system services [117]. Often, WSNs are battery-operated in unattended, harsh, and complex environments. Therefore, performance of WSNs is vulnerable to energy and environmental factors [19], [22]-[26]. Furthermore, WSNs are usually deployed in random areas with no protection. Consequently, the networks are vulnerable to traffic analysis attacks. In the attacks, adversaries focus on analyzing the network traffic to obtain critical information such as the location information of important sensor nodes [24], [28]-[32]. Therefore, it is important to ensure energy-efficient communications and location privacy protection in WSNs [11], [30], [33], [45]. Moreover, the dynamicity of WSNs is greater as sensor nodes fail more often due to limited battery power and harsh application environments [66]. Thus, it is essential to guarantee reliability in WSNs and ensure reliable network operations [66]-[69], [118]-[123].

In this study, an energy-efficient and reliability-aware source location privacy (SLP) routing protocol is proposed to provide SLP protection in monitoring WSNs. Similar to [69], it is considered that to achieve reliable communications within WSNs, it is essential to design reliable routing protocols and provide a means to evaluate the reliability performance of the protocols. Subsequently, we propose a new approach to evaluate the SLP reliability of SLP routing protocols. To the best of our knowledge, this is the first study attempting to measure the SLP reliability. The ability of the SLP routing protocols to achieve SLP protection according to application-specific requirements is quantified. Thus, the main difference between this study and previous studies is that, previous studies focus solely on measuring the magnitude of the SLP protection using performance metrics such as SP, CR, ASR, and capture probability but fail to measure the SLP reliability. Moreover, many of the existing studies focus on connectivity-oriented and flow-oriented reliability in WSNs [66].

조선대학교
CHOSUN UNIVERSITY

To address the challenge of SLP, a new ReRR protocol is proposed. The ReRR protocol aims to outperform two existing protocols: DistrR [44] and DissR [61] protocols. The proposed ReRR protocol outperforms the DistrR and DissR protocols in terms of long-term SLP protection, energy efficiency, network lifetime, and SLP reliability.

Exhaustive energy consumption of sensor nodes and unbalanced energy distribution can seriously affect the operation of WSNs, resulting in limitations such as limited network lifetime [18]-[21], [23], [78], [117], and short-term SLP protection [35]. Therefore, to outperform the DissR and DistrR protocols, ReRR regulates the energy consumption of the sensor nodes by reducing the amount of packet traffic in the network. Hence, unlike the DissR and DistrR protocols that distribute large amounts of fake packet traffic or floods real and fake packets in particular regions of the network, ReRR generates a reduced amount of packet traffic. The routing algorithm of ReRR guarantees that only real packets are transmitted to the sink node.

To achieve high levels of SLP protection, ReRR employs a dynamic routing strategy that involves two routing techniques. The process of selecting a routing technique is based on the location of the source node with respect to the sink node location. ReRR creates random routing paths with high path diversity by computing parameters such as randomization factor and node offset angle. Furthermore, to realize the random routing paths, ReRR provides three candidate relay nodes for each source node packet forwarding instance and randomly selects one relay node during the route creation process. Multiple relay ring sections and relay regions are generated between a source node and relay nodes to ensure the location of any relay node is safeguarded. Thus, the location information of the source nodes is not easily leaked to the adversary even after the adversary locates a relay node. The strategic configuration of the relay ring sections and relay regions, and the dynamic route creation process guarantee that the routing paths for successive packets are unpredictable to the adversary. As a result, the adversary is obfuscated and the SLP is preserved.

5.1.1. Contributions

The main contributions of this study can be summarized as follows. (1) Identify the limitations of the

조선대학교
CHOSUN UNIVERSITY

DissR and DistrR protocols that are caused by various packet routing techniques. Explore the limitations that are caused by the distribution of fake packet traffic in particular regions of the WSN domain and flooding of real and fake packets. (2) Develop the new ReRR protocol. Design the routing algorithm of ReRR to guarantee high path diversity, high levels of adversary obfuscation, and improved energy efficiency. (3) Conduct a series of experiments to evaluate the performance of ReRR protocol and demonstrate the superiority of ReRR over DissR and DistrR protocols. Demonstrate that ReRR outperforms DissR and DistrR in terms of long-term SLP protection, energy efficiency, and network lifetime. (4) Propose a new approach to measure the SLP reliability of SLP routing protocols. Then, using the proposed approach, evaluate the SLP reliability of the ReRR, DissR, and DistrR protocols. Also, exhibit that ReRR achieves improved SLP reliability to outperform DissR and DistrR protocols.

5.2. Related Work

Numerous SLP protocols are presented in the literature. The protocols may be classified into many categories including fake packet routing, tree-based routing, intermediate node routing, phantom node routing, angle-based routing, and ring routing. Fake packet-based protocols include the path extension protocol, dummy packet injection routing, protocol based on anonymity cloud, distributed fake source with phantom node routing, protocol based on phantom nodes, rings, and fake paths, fake network traffic-based routing, data dissemination routing, dynamic fake sources-based routing, hybrid online single path routing, and the probabilistic routing protocol [24], [29], [33], [35], [56], [62].

Tree-based routing protocols include the tree-based diversionary routing, bidirectional tree, dynamic bidirectional tree, and zigzag bidirectional tree routing [32]. Intermediate node-based protocols include the randomly selected intermediary node routing, strategic location-based routing, three-phase intermediate node routing with network mixing ring, sink toroidal region routing, and the all-direction random routing protocol [32], [40]. Phantom node-based routing protocols include the phantom single-path routing, phantom routing with locational angle, phantom walkabouts, two-

조선대학교
CHOSUN UNIVERSITY

level phantom with a backbone route protocol, pseudo normal distribution-based phantom routing protocol, greedy random walk routing, and the probabilistic routing protocol [28], [29], [45]. Angle-based routing protocols include the angle-based intermediate node routing, angle-strategic routing, angle-based dynamic routing, angle-proxy routing, constrained random routing, and the two-phantom angle-based routing [28], [34], [94].

Some of the SLP protocols employ multiple routing strategies. For example, in [33], phantom routing was integrated with ring routing and fake packet routing. In [32], [44], [61], [62], phantom routing was integrated with fake packet routing. Other protocols employ multiple sink nodes. For instance, the protocols in [11], [31], [124] employed multiple sink node routing strategies.

The study in [35] analyzed the performance of several fake packet-based protocols including DissR [61] and DistrR [44]. It was observed that the DissR and DistrR protocols were capable of achieving high levels of SLP protection to outperform the other protocols. However, the SLP protection of the DissR and DistrR protocols was short-term. Furthermore, the DissR and DistrR protocols incurred the highest energy consumption in the near-sink regions. As a result, DissR and DistrR achieved limited network lifetime. To address the challenges of DissR and DistrR protocols, this study develops the new ReRR protocol. The proposed ReRR outperforms DissR and DistrR in terms of long-term SLP protection, energy efficiency, and network lifetime. Moreover, ReRR achieves improved SLP reliability. The operational features of the DissR and DistrR protocols are presented below.

To insure improved performance in the proposed ReRR protocol, it is assumed that multi-hop data transfer technique leads to exhaustive energy consumption for sensor nodes in the near-sink regions. This is due to the fact that the sensor nodes in the near-sink regions have increased load of packet traffic, since the sink node is the destination node for the packet traffic. Thus, the sensor nodes in the near-sink regions have to burden the data forwarding for nodes in the away from sink node regions [18], [32], [94]. Furthermore, multi-hop data transfer technique results in non-uniform energy consumption across the network and the sensor nodes in the near-sink regions deplete their energy at a fast rate [18]. This phenomena results in short-term SLP protection and limited network lifetime,

조선대학교
CHOSUN UNIVERSITY

especially in the DissR and DistrR protocols which distribute large amounts of packet traffic. Therefore, the main goal of ReRR is to reduce the energy consumption of the sensor nodes by reducing the amount of packet traffic in the WSN domain. To highlight the significance of the proposed ReRR protocol, Table 5.1 summarizes the achievements of DissR, DistrR, and ReRR protocols.

Table 5.1: Summary of the achievements in DissR, DistrR, and ReRR protocols.

Protocol	Level of SLP protection in short-term	Effective long-term SLP protection	Exhaustive energy consumption	Long network lifetime	Long-term SLP reliability
DissR [61]	Very high	No	Yes	No	No
DistrR [44]	Very high	No	Yes	No	No
Proposed ReRR	High	Yes	No	Yes	Yes

5.3. Novel Reliable Relay Ring Routing (ReRR) Protocol

Generally, SLP protection is achieved by injecting fake packet traffic in the network or increasing the randomness of the routing paths [31]. The proposed ReRR protocol considers the techniques to increase the randomness of the routing paths while the existing DissR and DistrR protocols employ fake packet injection techniques. Thus, the proposed ReRR protocol presents two main design goals to guarantee improved performance. The main design goals of ReRR are summarized as follows.

- Reduce the energy consumption of the sensor nodes by reducing the amount of packet traffic in the network. It was shown in [35] that exhaustive energy consumption of the sensor nodes can result in short-term SLP protection. Furthermore, packet transmission and reception are the most energy consuming tasks for the sensor nodes [35], [94]. Therefore, unlike the DissR and DistrR protocols which distribute large amounts of packet traffic in the network, ReRR aims to distribute a reduced amount of packet traffic to ensure long-term SLP protection.
- Create random routing paths with high path diversity by employing a randomization factor (R_{ZF}) and node offset angle (θ) parameters. To achieve the random routing paths, provide three candidate relay nodes (rNs) for each source node (SN) and randomly select one rN based on the values of R_{ZF} and θ. The routing algorithm of ReRR guarantees that a new rN

조선대학교
CHOSUN UNIVERSITY

is selected for each successive packet routing to ensure the routing paths are unpredictable to the adversary. Hence, ReRR ensures adversary obfuscation to achieve high levels of SLP protection.

The ReRR protocol operates in two phases as shown in algorithm 5.1. Phase 1 involves the processes for network configuration while phase 2 includes the mechanisms for packet routing. The network initialization process is done according to the mechanisms explained in section 2.1. The sink node is located at coordinates (0, 0). Distance between any two points in the network is calculated using the Euclidean distance equation in equation (1). After the network initialization process is complete, the θ for all sensor nodes is computed as presented in section 2.1.

The network configuration for the proposed ReRR protocol is shown in Fig. 5.1. The network is divided into four network sections. Each section is separated from other sections by using the section boundaries (*SBs*) as shown in Fig. 5.1. The *SBs* are used to ensure the *rNs* and *SNs* are located in different network sections. This guarantees that the location of any *rN* is safeguarded at a safe distance away from the *SNs*. The location of the *SBs* is determined by the value of section boundary

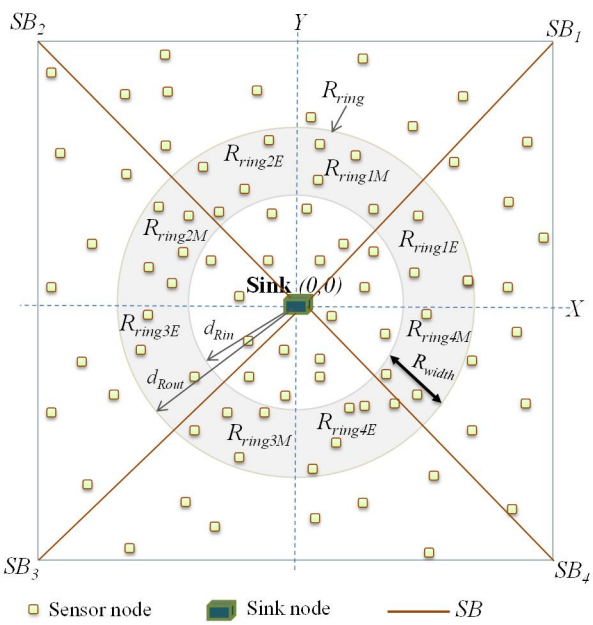


Figure 5.1: Network configuration for the proposed ReRR protocol.

조선대학교
CHOSUN UNIVERSITY

angle (θ_{SB}). The θ_{SB} is the inclination angle formed between a *SB* and the *X*-axis. Table 5.2 shows the θ_{SB} for each *SB*. A relay node ring (R_{ring}) is generated according to Fig. 5.1. R_{width} is the width of the R_{ring} while d_{Rin} is the distance between the sink node and the inner boundary of the R_{ring} and d_{Rout} is the distance between the sink node and the outer boundary of the R_{ring}.

The R_{ring} has four unique sections according to θ of the sensor nodes, as shown in Table 5.3. Thus, the R_{ring} is divided into R_{ring1}, R_{ring2}, R_{ring3}, and R_{ring4}. Each section of the R_{ring} is further divided

Algorithm 5.1: Proposed algorithm for ReRR protocol

Input:
S_{LOC}: Location of sink node;
S_{hop}: Hop count at sink node;
Output:
Routing path to sink node;
Phase 1: Network configuration
network initialization
compute θ
generate *SBs* according to Fig. 5.1 and Table 5.2
generate R_{ring} according to Fig. 5.1
assign nodes into R_{ring} according to Table 5.3
assign nodes into sections of R_{ring} according to Table 5.4
assign d_T
assign nodes into *RRs* according to Table 5.5
Phase 2: Packet routing
sensor node become *SN*
generate R_{ZF}
if ($d_S \geq d_T$) **then**
    select *rN* according to RS1 in Table 5.6
  else
    select *rN* according to RS2 in Table 5.7
  end if
route packet from *SN* to sink node through selected *rN*

Table 5.2: Section boundary angle for each *SB*.

SB	SB_1	SB_2	SB_3	SB_4
θ_{SB}	$\pi/4$	$3\pi/4$	$5\pi/4$	$7\pi/4$

Table 5.3: Assignment of sensor nodes into R_{ring}.

θ	$0° \leq \theta < \pi/2$	$\pi/2 \leq \theta < \pi$	$\pi \leq \theta < 3\pi/2$	$3\pi/2 \leq \theta < 2\pi$
Section of R_{ring}	R_{ring1}	R_{ring2}	R_{ring3}	R_{ring4}

조선대학교
CHOSUN UNIVERSITY

Table 5.4: Assignment of sensor nodes into sections of R_{ring}.

Node location	R_{ring1}		R_{ring2}	
θ	$\theta < \theta_{SB1}$	$\theta \geq \theta_{SB1}$	$\theta < \theta_{SB2}$	$\theta \geq \theta_{SB2}$
Section of R_{ring}	R_{ring1E}	R_{ring1M}	R_{ring2E}	R_{ring2M}
Node location	R_{ring3}		R_{ring4}	
θ	$\theta < \theta_{SB3}$	$\theta \geq \theta_{SB3}$	$\theta < \theta_{SB4}$	$\theta \geq \theta_{SB4}$
Section of R_{ring}	R_{ring3E}	R_{ring3M}	R_{ring4E}	R_{ring4M}

Table 5.5: Assignment of sensor nodes into *RRs*.

θ	$0° \leq \theta < \theta_{SB1}$	$\theta_{SB1} \leq \theta < \pi/2$	$\pi/2 \leq \theta < \theta_{SB2}$	$\theta_{SB2} \leq \theta < \pi$
RR	RR_1	RR_2	RR_3	RR_4
θ	$\pi \leq \theta < \theta_{SB3}$	$\theta_{SB3} \leq \theta < 6\pi/4$	$6\pi/4 \leq \theta < \theta_{SB4}$	$\theta_{SB4} \leq \theta < 2\pi$
RR	RR_5	RR_6	RR_7	RR_8

into two sections according to the θ of the sensor nodes, as shown in Table 5.4 and Fig. 5.1. For example, in R_{ring1}, if θ of a node is $< \theta_{SB1,}$ the sensor node is assigned into R_{ring1E}. Otherwise, node is assigned into R_{ring1M}. The structure of the network configuration and node assignment ensure that during packet routing, any *rN* will be located at least one R_{ring} section away from the *SNs*. The aim is to guarantee that the *SN* location information is not easily leaked to the adversary even after the adversary locates the *rNs*. A threshold hop distance (d_T) is defined. All sensor nodes with $d_S \geq d_T$ are assigned into relay regions (*RR*) based on their θ, as shown in Table 5.5. The d_S is computed by each sensor node during the network initialization process. The algorithm of ReRR protocol is summarized in algorithm 5.1.

To create highly random routing paths and provide high path diversity, the ReRR protocol involves two routing strategies: routing strategy 1 (RS1) and routing strategy 2 (RS2). The choice of a routing strategy for each *SN* is highly dependent on the values of distances d_S and d_T. For each *SN*, if $d_S \geq d_T$, RS1 is employed. Otherwise, RS2 is employed. The *rN* selection process for RS1 is summarized in Table 5.6 while RS2 is summarized in Table 5.7. Both RS1 and RS2 generate three candidate *rNs* for each *SN* and one of the *rNs* is selected based on the value of R_{ZF}. R_{ZF} is a random

조선대학교
CHOSUN UNIVERSITY

number in the range [1, 9]. It is generated by the *SN* after the *SN* detects an asset. The use of R_{ZF} ensures a high probability that a different *rN* is selected for each successive packet and the routing paths are unpredictable to the adversary.

The location of *SNs* with respect to the sink node location and θ are also considered during the *rN* selection process in RS1 and RS2. As an example, if *SN* has $d_S \geq d_T$, then RS1 in Table 5.6 is employed. If the *SN* has *X*-coordinate ≥ 0, *Y*-coordinate ≥ 0, $\theta < \theta_{SB1}$, and $R_{ZF} < 4$, then *rN* is selected from R_{ring2E}. On the other hand, if the same *SN* generates $R_{ZF} > 6$, then a *rN* is selected from R_{ring4E}. When *SN* has $d_S < d_T$, the RS2 in Table 5.7 is employed. If the *SN* has *X*-coordinate < 0, *Y*-coordinate < 0, $\theta \geq \theta_{SB3}$, and $4 \leq R_{ZF} \leq 6$, then *rN* is selected from RR_2. On the other hand, if the same *SN* generates $R_{ZF} > 6$, then *rN* is selected from RR_4. After *rN* is selected, packet routing between the *SN*

Table 5.6: RS1 for selection of *rN* from sections of R_{ring} according to *SN* location, θ, and R_{ZF}.

X* and *Y* coordinates, and θ of *SN		$X \geq 0$ and $Y \geq 0$		$X < 0$ and $Y \geq 0$	
		$\theta < \theta_{SB1}$	$\theta \geq \theta_{SB1}$	$\theta < \theta_{SB2}$	$\theta \geq \theta_{SB2}$
Selection of *rN* from R_{ring}	$R_{ZF} < 4$	R_{ring2E}	R_{ring2M}	R_{ring3E}	R_{ring3M}
	$4 \leq R_{ZF} \leq 6$	R_{ring3E}	R_{ring3M}	R_{ring4E}	R_{ring4M}
	$R_{ZF} > 6$	R_{ring4E}	R_{ring4M}	R_{ring1E}	R_{ring1M}
X* and *Y* coordinates, and θ of *SN		$X < 0$ and $Y < 0$		$X \geq 0$ and $Y < 0$	
		$\theta < \theta_{SB3}$	$\theta \geq \theta_{SB3}$	$\theta < \theta_{SB4}$	$\theta \geq \theta_{SB4}$
Selection of *rN* from R_{ring}	$R_{ZF} < 4$	R_{ring4E}	R_{ring4M}	R_{ring1E}	R_{ring1M}
	$4 \leq R_{ZF} \leq 6$	R_{ring1E}	R_{ring1M}	R_{ring2E}	R_{ring2M}
	$R_{ZF} > 6$	R_{ring2E}	R_{ring2M}	R_{ring3E}	R_{ring3M}

Table 5.7: RS2 for selection of *rN* from *RRs* according to *SN* location, θ, and R_{ZF}.

X* and *Y* coordinates, and θ of *SN		$X \geq 0$ and $Y \geq 0$		$X < 0$ and $Y \geq 0$	
		$\theta < \theta_{SB1}$	$\theta \geq \theta_{SB1}$	$\theta < \theta_{SB2}$	$\theta \geq \theta_{SB2}$
Selection of *rN* from *RRs*	$R_{ZF} < 4$	RR_3	RR_4	RR_5	RR_6
	$4 \leq R_{ZF} \leq 6$	RR_5	RR_6	RR_7	RR_8
	$R_{ZF} > 6$	RR_7	RR_8	RR_1	RR_2
X* and *Y* coordinates, and θ of *SN		$X < 0$ and $Y < 0$		$X \geq 0$ and $Y < 0$	
		$\theta < \theta_{SB3}$	$\theta \geq \theta_{SB3}$	$\theta < \theta_{SB4}$	$\theta \geq \theta_{SB4}$
Selection of *rN* from *RRs*	$R_{ZF} < 4$	RR_7	RR_8	RR_1	RR_2
	$4 \leq R_{ZF} \leq 6$	RR_1	RR_2	RR_3	RR_4
	$R_{ZF} > 6$	RR_3	RR_4	RR_5	RR_6

조선대학교
CHOSUN UNIVERSITY

and *rN* and between the *rN* and the sink node is done by using the directed random-walk routing strategy.

The directed random-walk routing strategy operates as follows. Once a sensor node has a packet to forward, it starts the process of next-hop node selection. The forwarding node computes a set of one-hop neighboring nodes with a shorter hop distance to the destination node than the forwarding node itself. Then, it randomly selects one neighboring node from the set as the next-hop node. The next-hop node becomes the forwarding node and forwards the packet. At the *SN*, the destination node is the selected *rN*. At the *rN*, the destination node is the sink node. To ensure the routing paths for successive packets are diversified, ReRR generates three candidate *rNs* for each *SN* packet forwarding instance and randomly selects *rN* based on the value of the R_{ZF} and θ. Moreover, a new R_{ZF} is generated for each *SN* packet forwarding instance.

The key differences in the routing strategies of the proposed ReRR protocol and the existing DissR and DistrR protocols are summarized in Table 5.8. For the DissR protocol, we assume all sensor nodes with $d_S < d_T$ are located inside the blast ring.

Table 5.8: Key differences in the routing strategies of DissR, DistrR, and ReRR protocols.

Protocol	Routing strategy	
	If *SN* has $d_S < d_T$	**If *SN* has $d_S \geq d_T$**
DissR	• Real packets from the source node are flooded inside the blast ring.	• Real packets and fake packets are distributed in the WSN domain. • Real packets and fake packets are flooded inside the blast ring.
DistrR	• Real packets and large amount of fake packets are distributed in the WSN domain.	• Real packets and large amount of fake packets are distributed in the WSN domain.
Proposed ReRR	• Real packets are transmitted to the sink node through *rNs*, using RS2.	• Real packets are transmitted to the sink node through *rNs*, using RS1.

Some investigations were done to observe the relationship between the size of R_{ring} and the level of SLP protection. Then, we determined an effective R_{ring} size. We assume that an effective R_{ring} size ensures effective number of sensor nodes in the R_{ring} to enable high path diversity and high levels of SLP protection.

Path diversity signifies the presence of route variation where successive packets from a *SN* follow different routing paths that are created between the *SN* and sink node [39], [58], [125]. Hence,

조선대학교
CHOSUN UNIVERSITY

in ReRR, path diversity denotes the existence of many alternative paths between a *SN* and sink node based on the randomly selected *rNs*. We measure the path diversity by counting the number of alternative packet routes that are created between a *SN* and sink node.

Path diversity enables successive packets from a *SN* to follow different routes to the sink node. This has a positive effect on the level of SLP protection by making it more difficult for the adversary to predict the routes for successive packets. Therefore, high path diversity corresponds to high levels of SLP protection. For instance, for a successful back tracing attack, an adversary needs to intercept many packets. If the packets use diversified routing paths, it takes longer for the adversary to detect a great number of packets to intercept. Therefore, the adversary obfuscation effect is increased, the back tracing attack of the adversary becomes complex, and the level of SLP protection is improved.

It is observed that the size of the R_{ring} can be altered to vary the number of sensor nodes inside the R_{ring}. Subsequently, high path diversity and high levels of SLP can be achieved when a large number of sensor nodes is available inside the R_{ring}. This is mainly because when a large number of sensor nodes is available, it generates a larger set of *rNs* for each *SN*. As a result, a greater number of routing paths can be created to improve the path diversity.

Fig. 5.2 shows the average values for path diversity and number of sensor nodes in the R_{ring} for different R_{width} sizes. To obtain the observations in the Fig. 5.2, 2500 sensor nodes were randomly distributed in a target field with side length of 2000 m and d_{Rin} of 300 m. The *ds* of the *SNs* was 35

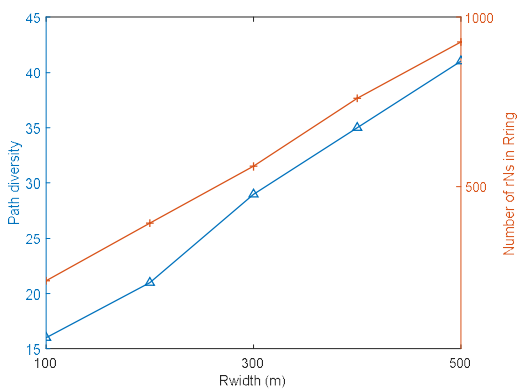


Figure 5.2: Achievable path diversity and number of *rNs* for different R_{width} size.

조선대학교
CHOSUN UNIVERSITY

hops and d_T was set to 25 hops. It is depicted in Fig. 5.2 that a greater number of sensor nodes become available in the R_{ring} and high path diversity is achieved when the size of R_{width} is increased.

In addition, similar to [39], it is observed that path diversity improves with the diversity of the *rNs* in terms of location and randomness. This is due to the fact that the *rNs* in the ReRR protocol appear randomly across the R_{ring} regions. Also, the diversity of the *rNs* in terms of location and randomness tend to increase when the R_{width} is increased.

Although the level of SLP protection improves with the increase in R_{width}, it is important to note that the R_{width} must be regulated to control the communication overhead. When R_{width} is significantly long, the packet routes become longer. Consequently, more energy may be spent to deliver the packets, longer delay may be incurred, and the probability of packet loss events may be increased. Therefore, the network planner must configure the R_{width} according to the application-specific requirements. In this study, it is assumed that the level of SLP protection at R_{width} = 400 m is effectively adequate. Also, it is assumed that the communication overhead at R_{width} = 400 m is acceptable.

5.4. Performance Analysis

This section presents some investigations on the performance of DissR, DistrR, and the proposed ReRR protocol. Various performance metrics were used to evaluate the performance of the protocols. First, the SP and CR were used to measure the level of SLP protection. Then, the energy consumption, energy efficiency, and network lifetime were analyzed. Also, investigations were done to analyze the SLP reliability of the protocols. Thus, a new approach was proposed to measure the safety period reliability and capture ratio reliability of the protocols.

For comparative analysis, the traditional phantom single-path routing (PhanR) protocol was included in the evaluations. In the PhanR protocol, packets are sent from the source nodes to the sink node through less random routing paths. Also, the routing paths are relatively short. Consequently, the adversary is not effectively obfuscated and PhanR achieves low levels of SLP protection [29].

5.4.1. Simulation Environment

조선대학교
CHOSUN UNIVERSITY

The network model in section 2.1 and adversary model in section 2.2 were assumed. Using MATLAB simulation environment, a network with N_{SL} of 2000 was employed and 2500 sensor nodes were randomly distributed. Thus, N_{SN} was 2500. Only one sink node was assumed. The S_{CR} was set to 30 m to ensure multi-hop communications and energy conservation. A cautious adversary was deployed with initial location in the locality of the sink node to ensure maximum probability of packet capture. The A_{HR} was set to 30 m, similar to the S_{CR} to ensure the adversary performs hop-by-hop back tracing attack. The A_{WT} was set to 4 source packets. The d_{Rin} was 300 m and R_{width} was 400 m. The d_T was set to 25 hops. To ensure accuracy of the simulation results, simulations were run for 500 iterations and average values were considered. The network simulation parameters are summarized in Table 5.9.

Table 5.9: Network simulation parameters

Parameter	Value
N_{SL} (m)	2000
N_{SN}	2500
N_{sink}	1
d_{Rin} (m)	300
R_{width} (m)	400
d_T (hops)	25
S_{CR} (m)	30
A_{HR} (m)	30
A_{WT} (source packets)	4
P_{sz} (bit)	1024
SN_{PR} (packet/second)	1
S_{IE} (J)	0.5
Adversary initial location	In the vicinity of sink node

5.4.2. Simulation Results and Discussions

- **SLP Protection**

A) Safety Period

The SP of the protocols was computed to observe the capability of the protocols to provide effective long-term SLP protection. Therefore, the SP was observed at different mission durations (rounds). In the experiments, source nodes were located at a source-sink distance of 35 hops. The results are shown in Fig. 5.3. The results show that the DissR, DistrR, and ReRR protocols achieve significantly

조선대학교
CHOSUN UNIVERSITY

longer SP than the traditional PhanR protocol. Furthermore, the results show that the SP of the ReRR protocol remains high throughout the 900 rounds. On the other hand, the SP of the DissR and DistrR protocols tend to decrease as the number of rounds is increased. Thus, the results indicate that the ReRR protocol is able to achieve effective long-term SLP protection to outperform the DissR and DistrR protocols.

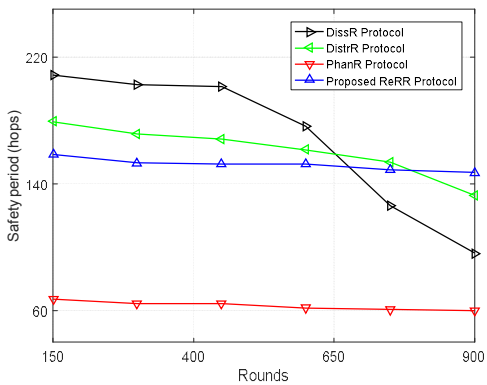


Figure 5.3: Privacy performance of the protocols.

When the number of rounds is low, the DissR protocol is capable of obfuscating the adversary to achieve longer SP than the other protocols because it employs a probabilistic flooding mechanism. It floods both real and fake packets. Therefore, multiple random nodes are selected to broadcast each packet so that the packets arrive at the sink node using multiple random routing paths. As a result, the tracing back attack becomes a complex and time consuming task and longer SP is achieved. Moreover, the cautious adversary is restricted from revisiting the immediate sender nodes. To some extent, the restriction increases the complexity of the adversary back tracing attack when the flooding mechanism is used.

Although the flooding mechanism of DissR helps to improve the SP, it causes short-term SLP protection. As shown in Fig. 5.3, the SP of DissR protocol is significantly reduced at 900 rounds. When both real and fake packets are flooded, a significant amount of sensor nodes energy is consumed to transmit a single packet. Consequently, the sensor nodes drain their energies at a fast rate. At 900 rounds, a significant number of sensor nodes inside the blast ring have exhausted their battery power.

조선대학교
CHOSUN UNIVERSITY

Therefore, fewer sensor nodes are able to participate in the flooding mechanism. As a result, the adversary becomes less obfuscated and the SP is reduced.

The DistrR protocol distributes a considerable amount of fake packet traffic around the source node, simultaneously with the transmission of real packets. Consequently, the adversary is tackled with multiple packets and finds it difficult to identify the exact immediate sender node of the real packets. Also, the adversary is tricked into back tracing the fake packet routes. As a result, adversary is steered away from the location of the real source node. Therefore, the adversary is obfuscated, the back tracing attack is made more complex, and long SP is achieved. However, similar to DissR, the SP of DistrR is significantly reduced at 900 rounds. The main reason for the reduced SP in DistrR is that, the number of candidate fake packet sources is highly dependent on the amount of the sensor node residual energy. For a sensor node to become a candidate fake packet source, one of the criteria is that the value of the sensor node residual energy must be greater than a threshold value. In our experiments, a threshold value of 0.2 J was assumed. Since DistrR distributes a considerable amount of fake packet traffic in the network, many of the sensor nodes deplete their residual energy. When the number of rounds was increased, the residual energy of some of the sensor nodes became less than the threshold value. As a result, small numbers of fake packet sources were generated. Subsequently, the amount of fake packet traffic was reduced, the adversary became less obfuscated, and the SP was reduced.

To achieve significantly longer SP than the traditional PhanR protocol, the ReRR protocol creates random routing paths with high path diversity by employing the R_{ZF} and θ parameters during the route creation process. Also, to ensure high path diversity, ReRR generates three candidate *rNs* for each source node packet forwarding instance and randomly selects a *rN* based on the value of the R_{ZF} and θ. Therefore, it guarantees that the routing paths for successive packets are unpredictable to the adversary. Moreover, ReRR ensures the *rNs* and source nodes are located at least one R_{ring} section or *RR* away from each other. This ensures that the location of any *rN* is safeguarded at a safe distance away from the source nodes. As a result, the location information of the source nodes is not easily

조선대학교
CHOSUN UNIVERSITY

leaked to the adversary even after the adversary locates a *rN*. The adversary back tracing attack is made more complex. Hence, ReRR achieves significantly longer SP than the PhanR protocol.

To achieve long-term SLP protection, ReRR considers three aspects. (i) Packet transmission and reception are the most energy consuming tasks for the sensor nodes [35], [94]. (ii) Exhaustive energy consumption of the sensor nodes can result in short-term SLP protection [35]. (iii) DissR and DistrR protocols transmit large amounts of packet traffic in the network, resulting in high energy consumption and short-term SLP protection. Therefore, ReRR transmits a reduced amount of packet traffic in the network. Fig. 5.3 shows that beyond 850 rounds the ReRR protocol achieves long SP to outperform the other protocols.

B) Capture Ratio

It is shown in Fig. 5.3 that below 600 rounds, the DissR and DistrR protocols are able to achieve significantly long SP to outperform the ReRR protocol. Therefore, in such conditions, it was interesting to investigate how the SLP performance of the protocols is affected when some of the network parameters are varied. Hence, the CR of the protocols was observed under varied sensor node residual energy, adversary hearing range, and number of sensor nodes.

The SLP performance of the DistrR protocol is affected by the amount of sensor node residual energy [35]. Therefore, we observed the CR of the protocols against varied sensor node residual energy. In the experiments, the threshold value for residual energy was 0.2 J. We observed the residual energy of 90% of the sensor nodes that were located within 6 hops from the source nodes. The source nodes were located at a source-sink distance of 35 hops. The results are shown in Fig. 5.4 (a). The results show that the ReRR protocol is able to achieve significantly lower levels of CR than the PhanR protocol. Furthermore, when the residual energy of the sensor nodes is below the threshold value, the ReRR protocol achieves significantly lower levels of CR than the DistrR protocol. The CR of the DistrR protocol is high below the threshold value mainly because smaller numbers of fake packet sources were generated. Consequently, reduced amounts of fake packet traffic were broadcasted and the adversary became less obfuscated. Therefore, the adversary was able to improve

조선대학교
CHOSUN UNIVERSITY

its attack success rate and high CR was achieved. Fig. 5.4 (a) also shows that DissR achieves lower CR than the other protocols. Moreover, the CR of DissR remains unchanged when the residual energy of the sensor nodes is varied.

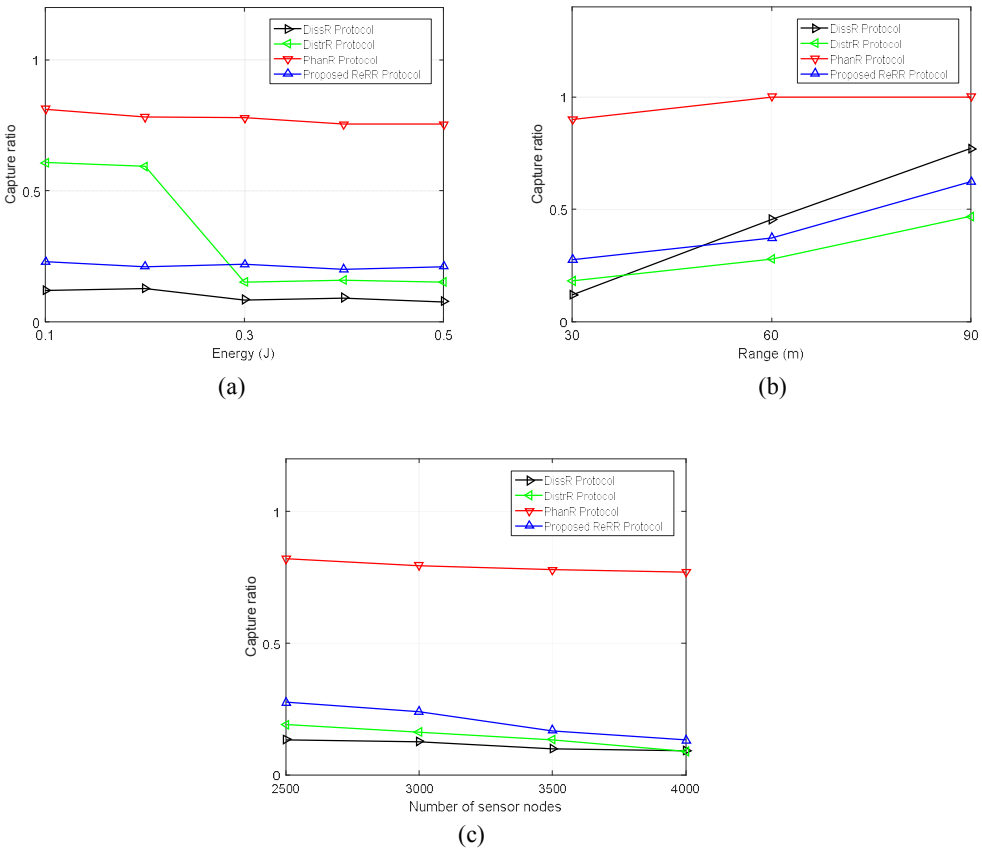


Figure 5.4: Privacy performance of the routing protocols. (a) CR against energy of sensor node. (b) CR against adversary hearing range. (c) CR against number of sensor nodes.

The observations in Fig. 5.4 (a) suggest that when short-term SLP protection is considered, DissR is capable of achieving higher levels of SLP to outperform DistrR and ReRR even when the residual energy of the sensor nodes is varied. On the other hand, ReRR is capable of achieving higher levels of SLP to outperform DistrR when the residual energy of the sensor nodes is below the threshold value. However, DissR and DistrR are less practical when long-term SLP protection is considered, as shown in Fig. 5.3.

조선대학교
CHOSUN UNIVERSITY

In the experiments for the results in Fig. 5.4 (b), CR was observed under varied adversary hearing range. The adversary hearing range was varied between 30 and 90 m. The results show that for all the protocols, the CR increases with the increase in adversary hearing range. This is mainly due to the fact that the adversary becomes more powerful when it has a longer hearing range. The traffic analysis attacks become less complex when the adversary can hear a packet sent from a sensor node which is more than 1 hop distance away.

Fig. 5.4 (b) also shows that when the adversary hearing range is increased, the ReRR protocol is capable of achieving reduced CR to outperform the DissR protocol. The CR of the ReRR increases at a slower rate than the CR of the DissR mainly because the ReRR ensures high path diversity by generating multiple candidate *rNs* for each source node packet forwarding instance. Moreover, the *rNs* and source nodes are located at least one R_{ring} section or *RR* away from each other to ensure the location of any *rN* is safeguarded at a safe distance away from the source nodes. As a result, the routing paths for successive packets are less predictable to the adversary and the location information of the source nodes is not easily leaked to the adversary. On the other hand, DissR isolates the real and fake source nodes and it does not distribute fake packets near the phantom nodes. Consequently, the adversary obfuscation effect between the phantom nodes and source nodes is reduced. Also, the location information of the source nodes is easily leaked to the adversary after the adversary locates a phantom node. Therefore, it becomes easy for the adversary to successfully locate the source nodes and the CR is increased.

Fig. 5.4 (b) also shows that although the CR of DistrR increases with the increase in adversary hearing range, DistrR maintains a low CR to outperform ReRR. DistrR is able to maintain low CR because it employs a different fake packet distribution strategy. Unlike DissR, DistrR does not isolate the real and fake source nodes. Furthermore, DistrR distributes fake packets near the phantom nodes. As a result, the adversary obfuscation effect is increased and low CR is maintained.

The observations in Fig. 5.4 (b) suggest that when short-term SLP protection is considered, DistrR is capable of achieving high levels of SLP to outperform DissR and ReRR even when the adversary hearing range is increased. On the other hand, ReRR is capable of achieving high levels of

조선대학교
CHOSUN UNIVERSITY

SLP to outperform DissR when the adversary hearing range is increased. However, both DissR and DistrR are less practical when long-term SLP protection is considered, as shown in Fig. 5.3.

In the experiments for the results in Fig. 5.4 (c), CR was observed under varied number of sensor nodes. The number of sensor nodes in the network was varied between 2500 and 4000. Fig. 5.4 (c) shows that the CR for the ReRR and DistrR tend to decrease when the number of nodes is increased. In ReRR, CR decreases mainly because the number of *rNs* increases with the increase in number of sensor nodes. When a large number of *rNs* is available, the path diversity can be improved to ensure the routing paths are unpredictable to the adversary and CR is reduced. Furthermore, the number of next-hop neighboring nodes at the source node can be increased with the increase in number of sensor nodes. Consequently, different next-hop node can be selected during the packet forwarding process to improve the path diversity.

As an example, if a source node has j next-hop neighboring nodes with shorter hop distance to *rN*, the probability that the source node will select a particular next-hop neighboring node during the directed random-walk is $1/j$. If *rN* has h next-hop neighboring nodes with shorter hop distance to the sink node, the probability that *rN* will select a particular next-hop neighboring node during the directed random-walk is $1/h$. Also, if u sensor nodes are available as *rNs*, the probability that a node will select a particular sensor node as a *rN* is $1/u$. Thus, there is up to $j \times h \times u$ random routes between a source node and the sink node. Therefore, when the number of sensor nodes is increased, it improves the path diversity and reduces CR. Similarly, in DistrR, when the number of sensor nodes is increased, it increases the probability of a higher number of candidate fake packet sources. When a large number of fake packet sources is generated, large amount of fake packet traffic is broadcasted to obfuscate the adversary. Consequently, the CR is reduced.

Fig. 5.4 (c) also shows that the CR of DissR does not vary very much when the number of sensor nodes is increased. This is due to the fact that DissR employs a probabilistic flooding mechanism and both fake and real packets are flooded with equal probability. When the number of sensor nodes is 4000, the CR of ReRR is approaching the CR of DissR.

The observations in Fig. 5.4 (c) suggest that when short-term SLP protection is considered,

조선대학교
CHOSUN UNIVERSITY

DistrR and DissR are capable of achieving high levels of SLP to outperform ReRR. Furthermore, the SLP protection of DistrR and ReRR improves with the increase in number of sensor nodes. Moreover, when the number of sensor nodes is increased, the level of SLP protection in ReRR tends to approach the level of SLP protection in DissR. However, DissR and DistrR are less practical when long-term SLP protection is considered, as shown in Fig. 5.3.

- **Energy Consumption and Network Lifetime**

A) Energy consumption

Fig. 5.5 shows the energy consumption of the protocols. In the experiments, source nodes were assumed at different source-sink distances. Packets were sent from each source node to the sink node and the energy consumption per sensor node was computed. For the DissR protocol, the boundary of the blast ring was assumed at 400 m from the sink node. The results in Fig. 5.5 show that in the near-sink regions, the ReRR protocol incurs lower energy consumption than the DissR and DistrR protocols. ReRR incurs low energy consumption mainly because it distributes a reduced amount of packet traffic in the near-sink regions. In the case of DissR, both real and fake packets are flooded when the source nodes are located outside the blast ring. Therefore, DissR incurs the highest energy consumption in the near-sink regions. The DistrR protocol generates a significant amount of fake packet traffic throughout the network domain, depending on the location of the source nodes and phantom nodes. Based on the distribution of the fake packet traffic, DistrR is able to trick the

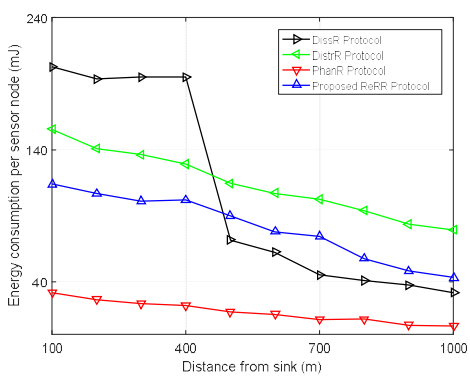


Figure 5.5: Energy consumption of the protocols.

조선대학교
CHOSUN UNIVERSITY

adversary into back tracing the fake packet routes. Therefore, the adversary is steered away from the location of the real source nodes. Although this process ensures high levels of SLP protection in DistrR, it has a negative effect on the energy consumption performance. Consequently, DistrR incurs high energy consumption.

Fig. 5.5 also shows that the DissR protocol achieves unbalanced energy distribution. It shows that DissR incurs significantly lower energy consumption in the regions away from the sink node. The unbalanced energy distribution in DissR is due to the fact that the packet flooding mechanism is employed inside the blast ring regions. Outside the blast ring, the energy consumption of DissR is significantly reduced because the protocol distributes only one fake packet for each real packet.

In the energy-constrained WSNs, unbalanced energy distribution can seriously affect the operation of the network, resulting in inefficient energy consumption and limited network lifetime [21], [23], [35], [117]. Investigations on the energy efficiency and network lifetime performance are presented below.

B) Energy Efficiency

The energy ratio (ER) parameter was used to measure the energy efficiency of the protocols. ER is the ratio of the energy that is used in 600 rounds to the total energy. High ER corresponds to low energy efficiency.

Based on Fig. 5.5, the protocols incur significantly higher energy consumption in the near-sink regions (hotspot regions) than in the away from sink node regions (non-hotspot regions). Therefore, the ER was computed for hotspot regions and non-hotspot regions as shown in Fig. 5.6. If the ds of a sensor node was < 25 hops, the sensor node was considered to be located in hotspot regions. Otherwise, sensor node was in non-hotspot regions.

Fig. 5.6 shows the ER of the protocols at varied source packet rate. It shows that the ER of all the protocols tend to increase with the increase in source packet rate. Fig. 5.6 (a) shows that in the hotspot regions, the ReRR protocol incurs lower ER than the DissR and DistrR protocols while Fig. 5.6 (b) shows that the ReRR protocol has lower ER than the DistrR protocol in the non-hotspot

조선대학교
CHOSUN UNIVERSITY

regions. Furthermore, the Fig. 5.6 shows that the ER of the ReRR protocol increases at a slower rate that the ER of the DissR and DistrR protocols. In the hotspot regions, the ER of DissR increases at a fast rate mainly because DissR floods a large amount of packet traffic. Therefore, when the packet rate is increased, more packets are generated per second and the ER is increased. Similarly, the ER of DistrR increases at a fast rate mainly because DistrR distributes large amount of fake packet traffic throughout the WSN domain.

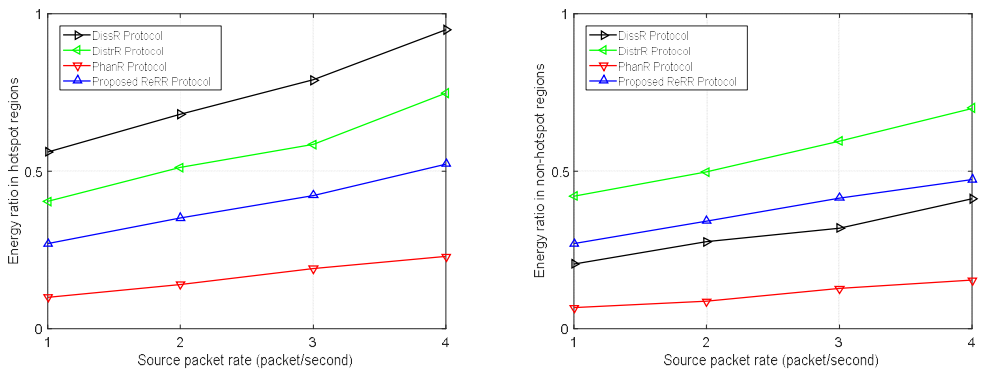


Figure 5.6: Energy efficiency of the protocols. (a) Energy ratio in hotspot regions. (b) Energy ratio in non-hotspot regions.

It was shown in [32], [35], [83] that high energy consumption of the sensor nodes in the hotspot regions can have a significant impact on the network lifetime. To maximize the network lifetime, the energy consumption and ER of the sensor nodes in the hotspot regions must be minimized [35]. Investigations on the network lifetime of the protocols are presented below.

C) Network Lifetime

To analyze the network lifetime of the protocols, the network lifetime model in section 2.4 was assumed. The network lifetime was observed under varied source packet rate. Fig. 5.7 shows the results of the network lifetime analysis. The results show that the ReRR protocol achieves significantly long network lifetime to outperform the DissR and DistrR protocols. ReRR achieves significantly long network lifetime because it guarantees reduced ER in the hotspot regions. On the other hand, the DissR and DistrR protocols achieve limited network lifetime mainly due to the high

조선대학교
CHOSUN UNIVERSITY

ER in the hotspot regions as shown in Fig. 5.6 (a). The results also show that the network lifetime is affected by the source packet rate. When the packet rate is increased, more packets are generated per second, the ER is increased, and the network lifetime is reduced. At the source packet rate of 5 packets/second, the network lifetime of DissR is significantly reduced because DissR floods a large amount of packet traffic in the hotspot regions. Hence, high packet rate increases the ER and reduces the network lifetime.

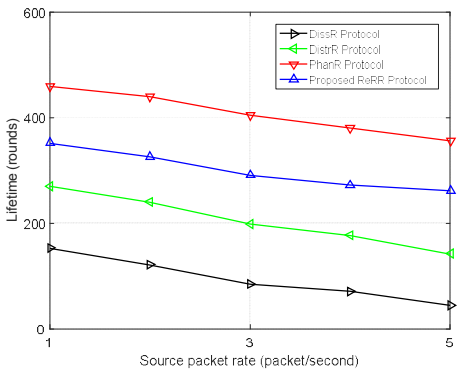


Figure 5.7: Network lifetime of the protocols.

- **SLP Reliability**

The investigations and analysis results above have shown the SLP protection capability of the protocols in terms of SP and CR. Although some of the protocols are capable of achieving high levels of SLP protection, they may not be reliable in long-term monitoring due to their high energy consumption, high ER, and reduced network lifetime. Therefore, it is important to investigate the SLP reliability of the protocols. Moreover, since there are many factors influencing the functioning of WSNs, it is essential to obtain its working ability at any time [7], [126]. Also, it is important to quantify the degree to which the performance can meet the application-specific requirements [67].

According to [66]-[68], a reliability index for a WSN should quantitatively assess the ability of the network to perform its intended function. Although the SP and CR parameters are able to measure the magnitude of the SLP protection, they do not take into consideration the application-specific requirements for achieving the intended SLP protection. Thus, the SP and CR metrics fail to reflect

조선대학교
CHOSUN UNIVERSITY

whether or not the SLP protection can be maintained for a given period of time, such as a specified mission duration. Therefore, we propose a novel approach to analyze the SLP reliability of the SLP protocols using equations (18), (19), (20).

In the equations, γ represents the SLP metric which is being analyzed. For example, γ may represent SP or CR. Two main values of γ are considered, the achieved γ (γ_{Ach}) and the application-specific required γ (γ_{Req}). The γ_{Ach} is the magnitude of γ that is achieved by the protocols. The γ_{Req} is according to the application-specific requirements. For example, some applications such as monitoring of endangered animals may specify a minimum γ_{Req} in terms of SP as 140 hops, throughout the mission duration. Meaning that throughout the mission duration, the protocols must guarantee that the achieved SP is greater than or equal to 140 hops.

In the equation (18), the γ realiability (R_γ) is computed. When $e^{\Delta\gamma} \geq 1$, the R_γ becomes 1 to indicate that the γ_{Req} is achieved and SLP reliability is guaranteed. Otherwise, the R_γ becomes 0 to indicate that the γ_{Req} is not achieved and the SLP reliability is not guaranteed.

$$R_\gamma = \begin{cases} 1, & if \ \ e^{\Delta\gamma} \geq 1 \\ 0, & otherwise. \end{cases} \tag{18}$$

where Δ_γ is the difference between the γ_{Ach} and the γ_{Req}. Equation (19) is used to compute the Δ_γ.

$$\Delta_\gamma = \frac{\gamma_{Ach} - \gamma_{Req}}{\gamma_{Ave}} \tag{19}$$

where γ_{Ave} is the average of the γ_{Ach} and γ_{Req}. Equation (20) is used to compute the γ_{Ave}.

$$\gamma_{Ave} = \frac{\gamma_{Ach} + \gamma_{Req}}{2} \tag{20}$$

Therefore, we define the SLP reliability as the probability that the achieved level of SLP protection is greater than or equal to the minimum required level of SLP protection. In this study, we measure the SLP reliability in terms of safety period reliability (R_{SP}) and capture ratio reliability (R_{CR}). The R_{SP} and R_{CR} of the protocols are investigated below.

A) Safety Period Reliability

Safety period reliability (R_{SP}) is the probability that the achieved SP is greater than or equal to the

조선대학교
CHOSUN UNIVERSITY

minimum required SP. Based on equations (18), (19), (20), the R_{SP} was computed using equation (21).

$$R_{SP} = \begin{cases} 1, & if \ \ e^{\Delta SP} \geq 1 \\ 0, & otherwise. \end{cases} \tag{21}$$

In the experiments, R_{SP} was observed for the mission duration of 1200 rounds. It was assumed that the minimum required SP was 140 hops. Fig. 5.8 shows the R_{SP} of the DissR, DistrR, PhanR and ReRR protocols. It is shown that the DissR and DistrR protocols are capable of achieveing R_{SP} but only for few rounds. Beyond 900 rounds, both DissR and DistrR do not provide R_{SP}. The proposed ReRR protocol is capable of providing R_{SP} for more than 1000 rounds mainly because ReRR has lower ER and higher energy efficiency than DissR and DistrR. The traditional PhanR protocol does not provide the required R_{SP} mainly because it employs a simple routing algorithm that is not effective at obfuscating the adversary. The achieved SP of PhanR was below the required SP.

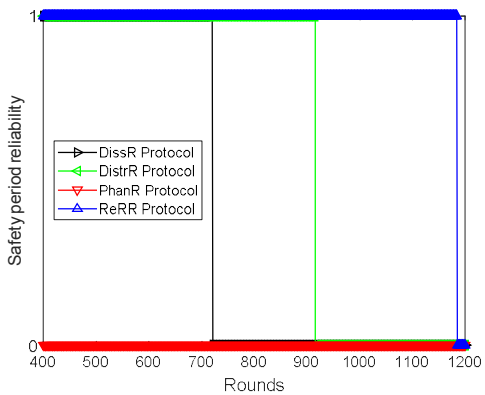


Figure 5.8: Safety period reliability of the protocols.

B) Capture Ratio Reliability

Capture ratio reliability (R_{CR}) is the probability that the achieved CR is less than or equal to the maximum required CR. Based on equations (18), (19), (20), the R_{CR} was computed using equation (22).

$$R_{CR} = \begin{cases} 1, & if \ \ e^{\Delta CR} \geq 1 \\ 0, & otherwise. \end{cases} \tag{22}$$

조선대학교
CHOSUN UNIVERSITY

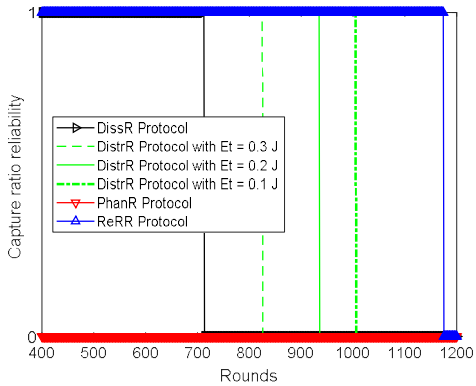


Figure 5.9: Capture ratio reliability of the protocols.

In the experiments, R_{CR} was observed for the mission duration of 1200 rounds. It was assumed that the maximum required CR was 0.3. Fig. 5.9 shows the R_{CR} of the DissR, DistrR, PhanR and ReRR protocols. It is shown that, similar to the R_{SP} performance, the ReRR protocol provides R_{CR} for longer durations to outperform the DissR and DistrR protocols. The proposed ReRR protocol is capable of providing R_{CR} for more than 1000 rounds mainly because ReRR has lower ER and higher energy efficiency than DissR and DistrR. Furthermore, as it was shown in Fig. 5.4 that the CR of DistrR can be affected by the amount of sensor node residual energy and the threshold value for residual energy, it was interesting to observe the R_{CR} of DistrR when the threshold value for residual energy (Et) is varied. Therefore, the Et was varied between 0.1 and 0.3 J. It is shown in Fig. 5.9 that DistrR provides R_{CR} for longer durations when the Et is reduced.

5.4.3. Limitations and Open Issues

Although the proposed ReRR protocol achieves reduced energy consumption in the near-sink regions to outperform the DissR and DistrR protocols, ReRR has significantly higher energy consumption than the traditional PhanR protocol. To ensure a more flexible energy management and improve the suitability of ReRR for IoT, techniques such as integration of distributed energy resources (DERs) [33] may be considered. It is important to improve the suitability of the protocols for energy-constrained IoT sensors because sensor-based IoT communication is a popular use case in the anticipated 6G and beyond wireless technology [127]. The integration of DERs into ReRR protocol

조선대학교
CHOSUN UNIVERSITY

remains an open issue and it will be considered in our future work. Also, energy-harvesting WSNs (EH-WSNs) are becoming increasingly popular and have the potential to overcome the battery power constraints in IoT sensors. In [128], it was presented that reinforcement learning frameworks enable delay sensitive EH-WSNs for deployment in a range of IoT applications. Hence, EH-WSNs may be considered to improve the suitability of the protocols for IoT applications. Furthermore, due to the location configuration of the relay regions, ReRR may incur reduced packet delivery reliability. Therefore, in our future work, we will analyze the performance of ReRR in terms of EED and PDR.

5.5. Remarks

One of the main challenges in designing and developing WSNs and SLP routing protocols is satisfying their strict reliability requirements. Therefore, this article considers the techniques for achieving reliable SLP protection in monitoring WSNs. Limitations of two fake packet-based SLP protocols are identified. A new protocol, namely ReRR protocol, is proposed to address the limitations of the fake packet-based protocols. To achieve high levels of SLP protection, the ReRR protocol provides multiple candidate relay nodes for each source node and randomly selects one relay node based on the value of the randomization factor and node offset angles. Furthermore, ReRR generates multiple relay ring sections and relay regions between source nodes and relay nodes. As a result, the location of any relay node is safeguarded. The network configuration of ReRR guarantees that the location information of the source nodes is not leaked to the adversary even after the adversary locates a relay node. Moreover, the routing paths for successive packets have high path diversity. Therefore, the adversary is effectively obfuscated and strong SLP protection is achieved.

It is observed that exhaustive energy consumption and unbalance energy distribution result in less reliable SLP protection. Therefore, unlike the fake packet-based protocols, ReRR ensures improved energy efficiency and reliable SLP protection. Analysis results demonstrate the superiority of the ReRR protocol. Moreover, a new approach is presented to measure the SLP reliability of the protocols. It is demonstrated through experimental evaluation that the proposed ReRR protocol is capable of satisfying the reliability requirements to outperform the fake packet-based protocols.

조선대학교
CHOSUN UNIVERSITY

Chapter 6

Conclusion and Future Work

SLP is a significant challenge in WSNs for IoT when safety-critical monitoring applications are considered. Therefore, this work presents some investigations and new findings on the topic of SLP protection. It is observed that many state-of-the-art SLP protocols provide high levels of SLP protection at the expense of high transmission cost. For example, fake packet-based SLP protocols provide high levels of SLP protection at the expense of increased communication cost and network overhead. Often, the protocols are energy-inefficient, they incur limited network lifetime, and have high probability of packet collision events which result in reduced PDR and increased EED. Therefore, in this work, series of experiments are conducted to evaluate the performance of various fake packet-based SLP protocols. Different from previous studies, this work presents comprehensive experimental analysis under varied network parameters and configurations. Subsequently, based on the observations, some recommendations are presented to address the limitations of the SLP protocols. Furthermore, realizing the shortcomings of the existing SLP protocols, several new SLP protocols are developed. The proposed protocols present improved performance to outperform some of the existing SLP protocols in terms of SLP protection and/or transmission cost.

A PhaP protocol is developed to address the limitations of the existing ProbR protocol. Simulation results show that PhaP achives high levels of SLP protection and reduced energy consumption in the near-sink regions to outperfm the ProbR protocol. A PhaT protocol is devised to address the limitations of the existing TreeR protocol. It is demonstrated that PhaT achieves improved energy consumption, PDR, and EED to outperfm the TreeR protocol. Angle-Strat protocol is proposed to address the limitations of the existing Strat-R protocol. Similarly, Angle-Proxy protocol is proposed to address the limitations of the existing Proxy-R protocol. It is observed that the Angle-Strat and Angle-Proxy protocols achieve improved energy consumption, PDR, and EED. The ReRR protocol is developed to address the limitations of the existing DissR and DistrR protocols. It is established that ReRR outperforms the DissR and DistrR in terms of long-term SLP protection,

조선대학교
CHOSUN UNIVERSITY

energy efficiency, and network lifetime. In addition, novel approaches are proposed to realize the SLP reliability of the protocols.

Recent studies show that DERs are becoming increasingly popular in IoT to deal with the energy and environmental challenges. Therefore, future work should explore the mechanisms of DERs to improve the performance of SLP protocols. In particular, DERs may be deployed to improve the availability of effective number of fake source, relay, or phantom nodes for long mission durations. Furthermore, this work focused solely on measuring the SLP reliability of the ReRR protocol. Therefore, future work should evaluate the packet delivery reliability of ReRR. Also, since this is the first work to measure the SLP reliability, more work is required to measure the SLP reliability of other state-of-the-art SLP protocols.

조선대학교
CHOSUN UNIVERSITY

REFERENCES

1. D. Thomas, R. Shankaran, M. Orgun, and S. Mukhopadhyay, "A secure barrier coverage scheduling framework for wsn-based iot applications," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 622–634, June 2021.
2. S. Hriez, S. Almajali, H. Elgala, M. Ayyash, and H. B. Salameh, "A novel trust-aware and energy-aware clustering method that uses stochastic fractal search in iot-enabled wireless sensor networks," *IEEE Systems Journal*, early access, August 2021, doi: 10.1109/JSYST.2021.3065323.
3. R. K. Lenka, A. K. Rath, and S. Sharma, "Building reliable routing infrastructure for green iot network," *IEEE Access*, vol. 7, pp. 129892–129909, September 2019.
4. J. Lin, P. R. Chelliah, M. Hsu, and J. Hou, "Efficient fault-tolerant routing in iot wireless sensor networks based on bipartite-flow graph modeling," *IEEE Access*, vol. 7, pp. 14022–14034, February 2019.
5. S. Kumar, and V. K. Chaurasiya, "A strategy for elimination of data redundancy in internet of things (iot) based wireless sensor network (wsn)," *IEEE Systems Journal*, vol. 13, no. 2, pp. 1650–1657, June 2019.
6. H. Kharrufa, H. A. A. Al-Kashoash, and A. H. Kemp, "RPL-based routing protocols in iot applications: A review," *IEEE Sensors Journal*, vol. 19, no. 15, pp. 5952–5967, August 2019.
7. L. Xing, "Reliability in internet of things: Current status and future perspectives," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6704–6721, August 2020.
8. A. M. Khedr, W. Osamy, A. Salim, and S. Abbas, "A novel association rule-based data mining approach for internet of things based wireless sensor networks," *IEEE Access*, vol. 8, pp. 151574–151588, August 2020.
9. C. Lyu, X. Zhang, Z. Liu, and C. Chi, "Selective authentication based geographic opportunistic routing in wireless sensor networks for internet of things against dos attacks," *IEEE Access*, vol. 7, pp. 31068–31082, March 2019.
10. M. Shakeri, A. Sadeghi-Niaraki, S-M. Choi, and S. M. R. Islam, "Performance analysis of iot-based health and environment wsn deployment," *Sensors*, vol. 20, p. 5923, October 2020.

조선대학교
CHOSUN UNIVERSITY

11. G. Han, H. Wang, X. Miao, L. Liu, J. Jiang, and Y. Peng, "A dynamic multipath scheme for protecting source-location privacy using multiple sinks in wsns intended for iiot," *IEEE Transactions On Industrial Informatics*, vol. 16, no. 8, pp. 5527–5538, August 2020.
12. G. Han, H. Wang, M. Guizani, S. Chan, and W. Zhang, "KCLP: A k-means cluster-based location privacy protection scheme in wsns for iot," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 84–90, December 2018.
13. G. Han, H. Wang, J. Jiang, W. Zhang, and S. Chan, "CASLP: A confused arc-based source location privacy protection scheme in wsns for iot," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 42–47, September 2018.
14. N. A. M. Alduais, J. Abdullah, and A. Jamil, "RDCM: An efficient real-time data collection model for iot/wsn edge with multivariate sensors," *IEEE Access*, vol. 7, pp. 89063–89082, July 2019.
15. S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion detection protocols in wireless sensor networks integrated to internet of things deployment: Survey and future challenges," *IEEE Access*, vol. 8, pp. 3343–3363, January 2020.
16. M. A. Al-Jarrah, M. A. Yaseen, A. Al-Dweik, O. A. Dobre, and E. Alsusa, "Decision fusion for iot-based wireless sensor networks," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1313–1326, February 2020.
17. I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, First quarter 2020.
18. O. J. Pandey, and R. M. Hegde, "Low-latency and energy-balanced data transmission over cognitive small world wsn," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7719–7733, August 2018.
19. X. Liu, and J. Wu, "A method for energy balance and data transmission optimal routing in wireless sensor networks," *Sensors*, vol. 19, p. 3017, July 2019.
20. M. Adil, et al, "An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment," *IEEE Access*, vol. 8, pp. 163209–163224, September 2020.
21. I. Khan, and D. Singh, "Energy balance node selection algorithm for heterogeneous wireless

조선대학교
CHOSUN UNIVERSITY

sensor networks," *ETRI Journal*, vol. 40, no. 5, pp. 604–612, October 2018.

22. X. Fu, Y. Yang, and O. Postolache, "Sustainable multipath routing protocol for multi-sink wireless sensor networks in harsh environments," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 1, pp. 168–181, March 2021.
23. L. Tang, Z. Lu, and B. Fan, "Energy efficient and reliable routing algorithm for wireless sensors networks," *Applied Sciences*, vol. 10, p. 1885, March 2020.
24. W. Tan, K. Xu, and D. Wang, "An anti-tracking source-location privacy protection protocol in wsns based on path extension," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 461– 471, October 2014.
25. K. Haseeb, et al, "Secret sharing-based energy-aware and multi-hop routing protocol for iot based wsns," *IEEE Access*, vol. 7, pp. 79980– 79988, July 2019.
26. F. Wang, et al, "To reduce delay, energy consumption and collision through optimization duty-cycle and size of forwarding node set in wsns," *IEEE Access*, vol. 7, pp. 55983–56015, May 2019.
27. M. Asiri, T. Sheltami, L. Al-Awami, and A. Yasar, "A novel approach for efficient management of data lifespan of iot devices," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4566–4574, May 2020.
28. J. Jiang, G. Han, H. Wang, and M. Guizani, "A survey on location privacy protection in wireless sensor networks," *Journal of Network and Computer Applications*, vol.125, pp. 93–114, January 2019.
29. L. C. Mutalemwa and S. Shin, "Secure routing protocols for source node privacy protection in multi-hop communication wireless networks," *Energies*, vol. 13, p. 292, January 2020.
30. M. Kamarei, A. Patooghy, A. Alsharif, and V. Hakami, "SiMple: A unified single and multi-path routing algorithm for wireless sensor networks with source location privacy," *IEEE Access*, vol. 8, pp. 33818–33829, February 2020.
31. G. Han, X. Miao, H. Wang, M. Guizani, and W. Zhang, "CPSLP: A cloud-based scheme for protecting source location privacy in wireless sensor networks using multi-sinks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2739–2750, March 2019.
32. J. Long, M. Dong, K. Ota, and A. Liu, "Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks," *IEEE*

조선대학교
CHOSUN UNIVERSITY

Access, vol. 2, pp. 633–651, July 2014.

33. Z. Xiong, H. Wang, L. Zhang, T. Fan, and J. Shen, "A ring-based routing scheme for distributed energy resources management in iiot," *IEEE Access*, vol. 8, pp. 167490–167503, September 2020.
34. W. Chen, M. Zhang, G. Hu, X. Tang, and A.K. Sangaiah, "Constrained random routing mechanism for source privacy protection in WSNs," *IEEE Access*, vol. 5, pp. 23171–23181, November 2017.
35. L. C. Mutalemwa and S. Shin, "Comprehensive performance analysis of privacy protection protocols utilizing fake packet injection techniques" *IEEE Access*, vol. 8, pp. 76935–76950, April 2020.
36. L. C. Mutalemwa and S. Shin, "Routing Schemes for source location privacy in wireless sensor networks: A survey," *J. Korean Inst. Commun. Inf. Sci*., vol. 43, no. 9, pp. 1429–1445, September 2018.
37. M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 15, no. 3, pp. 1238–1280, 2013.
38. A. Bushnag, A. Abuzneid, and A. Mahmood, "Source anonymity against global adversary in wsns using dummy packet injections: A survey," *Electronics*, vol. 7, no. 10, p. 250, 2018.
39. Q. Wang, J. Zhan, X. Ouyang, and Y. Ren, "SPS and DPS: Two new grid-based source location privacy protection schemes in wireless sensor networks," *Sensors*, vol. 19, p. 2074, May 2019.
40. L. C. Mutalemwa and S. Shin, "Strategic location-based random routing for source location privacy in wireless sensor networks," *Sensors*, vol. 18, no. 7, p. 2291, 2018.
41. M. Bradbury, A. Jhumka, and M.Leeke, "Hybrid online protocols for source location privacy in wireless sensor networks," *J. Parallel Distrib. Comput.*, vol. 115, pp. 67–81, 2018.
42. Z. Hong, R. Wang, S. Ji, and R. Beyah, "Attacker location evaluation-based fake source scheduling for source location privacy in cyber-physical systems," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1337–1350, May 2019.
43. N. Jan and S. Khan, *Energy-Efficient Source Location Privacy Protection For Network Lifetime Maximization Against Local Eavesdropper In Wireless Sensor Network (EeSP)*. Hoboken, NJ, USA: Wiley, August 2019, pp. 1–16.

조선대학교
CHOSUN UNIVERSITY

44. P. K. Roy, J. P. Singh, P. Kumar, and M. Singh, "Source location privacy using fake source and phantom routing (fsapr) technique in wireless sensor networks," *Procedia Comput. Sci.*, vol. 57, pp. 936–941, 2014.
45. C. Gu, M. Bradbury, and A. Jhumka, "Phantom walkabouts: A customisable source location privacy aware routing protocol for wireless sensor networks," *Concurrency Computat Pract Exper.*, vol. 31, p. 5304. 2019.
46. I. Tomić, and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910–1923, December 2017.
47. H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, "A review of iot sensing applications and challenges using rfid and wireless sensor networks," *Sensors*, vol. 20, p. 2495, April 2020.
48. F. Deng, P. Zuo, K. Wen, X. Wu, and Y. He, "Low delay technology research of transmission line tower monitoring network integrating wsn and rfid," *IEEE Access*, vol. 7, pp. 111065–111073, August 2019.
49. D. De Donno, L. Catarinucci, and L. Tarricone, "Ultralong-range rfid-based wake-up radios for wireless sensor networks," *IEEE Sensors Journal*, vol. 14, no. 11, pp. 4016–4017, November 2014.
50. S. S. Anjum *et al.*, "Energy management in rfid-sensor networks: taxonomy and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 250–266, February 2019.
51. H. Shen, Z. Li, L. Yu, and C. Qiu, "Efficient data collection for large-scale mobile monitoring applications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 6, pp. 1424–1436, June 2014.
52. H. Saghlatoon, R. Mirzavand, M. M. Honari, and P. Mousavi, "Sensor antenna transmitter system for material detection in wireless-sensor-node applications," *IEEE Sensors Journal*, vol. 18, no. 21, pp. 8812–8819, 1 November 2018.
53. M. Cai, and S. Mirrabbasi, "A self-sustained smart monitoring platform for capacitive de-ionization cell in wireless sensor network," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 5, pp. 4164–4172, May 2021.
54. M. N. M. Bhutta, and M. Ahmad, "Secure identification, traceability and real-time tracking of

조선대학교
CHOSUN UNIVERSITY

agricultural food supply during transportation using internet of things," *IEEE Access*, vol. 9, pp. 65660–65675, 2021.

55. H. Saghlatoon, R. Mirzavand, and P. Mousavi, "Fixed-frequency low-loss dielectric material sensing transmitter," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 4, pp. 3517–3526, April 2021.
56. N. Wang, J. Fu, J. Li, and B. K. Bhargava, "Source-location privacy protection based on anonymity cloud in wireless sensor networks," *IEEE Transactions On Information Forensics And Security*, vol. 15, pp. 100–114, 2020.
57. J. Kirton, M. Bradbury, and A. Jhumka, "Source location privacy-aware data aggregation scheduling for wireless sensor networks," in *Proc. 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, Atlanta, USA, June 2017, pp. 2200–2205.
58. L. C. Mutalemwa and S. Shin, "Achieving source location privacy protection in monitoring wireless sensor networks through proxy node routing," *Sensors*, vol. 19, no. 5, p. 1037, 2019.
59. C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *Proc. 2nd ACM Workshop Security Ad Hoc Sensor Networks*, October 2004, pp. 88–93.
60. S. Gupta, and B. Prince, "Preserving privacy of source location using random walk: A survey," in *Proc. 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology*, May 2016, pp. 2047–2051.
61. N. Jan, A. Al-Bayatti, N. Alalwan, and A. Alzahrani, "An enhanced source location privacy based on data dissemination in wireless sensor networks (delp)," *Sensors*, vol. 19, no. 9, p. 2050, 2019.
62. H. Wang, G. Han, W. Zhang, M. Guizani, and S. Chan, "A probabilistic source location privacy protection scheme in wireless sensor networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 5917–5927, June 2019.
63. Y. Wang, L. Liu, and W. Gao, "An efficient source location privacy protection algorithm based on circular trap for wireless sensor networks," *Symmetry*, vol. 11, p. 632, 2019.
64. M. Bradbury, and A. Jhumka, "A near-optimal source location privacy scheme for wireless sensor networks," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, Sydney, Australia, August 2017, pp. 409–416.

조선대학교
CHOSUN UNIVERSITY

65. A. Thomason, M. Leeke, M. Bradbury, and A. Jhumka, "Evaluating the impact of broadcast rates and collisions on fake source protocols for source location privacy," in *Proc. 12th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, July 2013, pp. 667–674.
66. S. Chakraborty, N. K. Goyal, S. Mahapatra, and S. Soh, "Minimal path-based reliability model for wireless sensor networks with multistate nodes," *IEEE Transactions On Reliability*, vol. 69, no. 1, pp. 382–400, March 2020.
67. S. Xiang, and J. Yang, "Reliability evaluation and reliability-based optimal design for wireless sensor networks," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1752–1763, June 2020.
68. W. Sun, et al, "End-to-end data delivery reliability model for estimating and optimizing the link quality of industrial wsns," *IEEE Transactions On Automation Science And Engineering*, vol. 15, no. 3, pp. 1127–1137, July 2018.
69. A. E. Zonouz, L. Xing, V. M. Vokkarane, and Y. Sun, "Reliability-oriented single-path routing protocols in wireless sensor networks," *IEEE Sensors Journal*, vol. 14, no. 11, pp. 4059–4068, November 2014.
70. Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of sourcelocation privacy schemes for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 7, pp. 1302–1311, July 2012.
71. P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Proc. 25th IEEE Int. Conf. Distrib. Comput. Syst.*, November 2005, pp. 599–608.
72. H. Chen and W. Lou, "On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks," *Pervas. Mobile Comput.*, vol. 16, part A, pp. 36–50, 2015.
73. Y. Liu, J.-S. Fu, and Z. Zhang, "K-nearest neighbors tracking in wireless sensor networks with coverage holes," *Pers. Ubiquitous Comput.*, vol. 20, no. 3, pp. 431–446, June 2016.
74. H. Chen and W. Lou, "From nowhere to somewhere: Protecting end-toend location privacy in wireless sensor networks," in *Proc. Int. Perform. Comput. Commun. Conf.*, December 2010, pp. 1–8.
75. M. M. E. A. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1805-1818, Oct. 2012.

조선대학교
CHOSUN UNIVERSITY

76. A. Jhumka, M. Bradbury, and M. Leeke, "Towards understanding source location privacy in wireless sensor networks through fake sources," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, June 2012, pp. 760–768.
77. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, January 2000, pp. 1–10.
78. T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand, and A. H. Gandomi, "I-SEP: An improved routing protocol for heterogeneous wsn for iot-based environmental monitoring," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 710–717, January 2020.
79. R. Manjula and D. Raja, "A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in wsns," *Pervasive Mobile Comput.*, vol. 44, pp. 58–73, February 2018.
80. A. Liu, X. Jin, G. Cui, and Z. Chen, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network," *Inf. Sci.*, vol. 230, pp. 197–226, May 2013.
81. R. Yarinezhada and A. Sarabib, "Reducing delay and energy consumption in wireless sensor networks by making virtual grid infrastructure and using mobile sink," *Int. J. Electron. Commun.*, vol. 84, pp. 144–152, February 2018.
82. N. Alaouil, J. P. Cances, and V. Meghdadi, "Energy consumption in wireless sensor networks for network coding structure and arq protocol," in *Proc. 1st Int. Conf. Electr. Inf. Technol.*, March 2015, pp. 317–321.
83. C. Huang, M. Ma, Y. Liu, and A. Liu, "Preserving source location privacy for energy harvesting wsns," *Sensors*, vol. 17, no. 4, p. 724, 2017.
84. X. Liu, A. Liu, T. Wang, K. Ota, M. Dong, Y. Liu, and Z. Cai, "Adaptive data and verified message disjoint security routing for gathering big data in energy harvesting networks," *J. Parallel Distrib. Comput.*, vol. 135, pp. 140–155, January 2020.
85. S. Misra, S. K. Roy, A. Roy, M. S. Obaidat, and A. Jha, "MEGAN: Multipurpose energy-efficient, adaptable, and low-cost wireless sensor node for the Internet of Things," *IEEE Syst. J.*, vol. 14, no. 1, pp. 144–151, March 2020.
86. A. Jhumka, M. Bradbury, and M. Leeke, "Fake source-based source location privacy in wireless sensor networks," *Concurrency Comput., Pract. Exper.*, vol. 27, no. 12, pp. 2999–3020, August

조선대학교
CHOSUN UNIVERSITY

2015.

87. M. Bradbury, M. Leeke, and A. Jhumka, “A dynamic fake source algorithm for source location privacy in wireless sensor networks,” in *Proc. IEEE Trustcom/BigDataSE/ISPA*, August 2015, pp. 531–538.
88. J. Ren, Y. Li, and T. Li, “Routing-based source-location privacy in wireless sensor networks,” in *Proc. IEEE Int. Conf. Commun.*, June 2009, pp. 1–5.
89. X. Luo, X. Ji, and M.-S. Park, ‘‘Location privacy against traffic analysis attacks in wireless sensor networks,’’ in *Proc. Int. Conf. Inf. Sci. Appl. (ICISA)*, April 2010, pp. 1–6.
90. A. Bushnag, A. Abuzneid, and A. Mahmood, “Source anonymity in wsns against global adversary utilizing low transmission rates with delay constraints,” *Sensors*, vol. 16, no. 7, p. 957, 2016.
91. R. Lu, X. Lin, H. Zhu, and X. Shen, “TESP2: Timed efficient source privacy preservation scheme for wireless sensor networks,” in *Proc. IEEE Int. Conf. Commun.*, May 2010, pp. 1–6.
92. S. Kokalj-Filipovic, F. Le Fessant, and P. Spasojevic, “The quality of source location protection in globally attacked sensor networks,” in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PERCOM Workshops)*, March 2011, pp. 44–49.
93. C. Gu, M. Bradbury, A. Jhumka, and M. Leeke, “Assessing the performance of phantom routing on source location privacy in wireless sensor networks,” in *Proc. IEEE 21st Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, November 2015, pp. 99–108.
94. L. C. Mutalemwa and S. Shin, “Regulating the packet transmission cost of source location privacy routing schemes in event monitoring wireless networks,” *IEEE Access*, vol. 7, pp. 140169–140181, 2019.
95. F. Engmann, F. A. Katsriku, J.-D. Abdulai, K. S. Adu-Manu, and F. K. Banaseka, “Prolonging the lifetime of wireless sensor networks: A review of current techniques,” *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–23, August 2018.
96. T. He, K.-W. Chin, S. Soh, and C. Yang, “On optimizing max min rate in rechargeable wireless sensor networks with energy sharing,” *IEEE Trans. Sustain. Comput.*, vol. 5, no. 1, pp. 107–120, January 2020.
97. A. Boukerche, Q. Wu, and P. Sun, “Efficient green protocols for sustainable wireless sensor networks,” *IEEE Trans. Sustain. Comput.*, vol. 5, no. 1, pp. 61–80, January 2020.

조선대학교
CHOSUN UNIVERSITY

98. J. Tang, A. Liu, J. Zhang, N. Xiong, Z. Zeng, and T. Wang, "A trust-based secure routing scheme using the traceback approach for energy-harvesting wireless sensor networks," *Sensors*, vol. 18, no. 3, p. 751, 2018.

99. H. Wang, G. Han, C. Zhu, S. Chan, and W. Zhang, "TCSLP: A trace cost based source location privacy protection scheme in wsns for smart cities," *Future Generation Computer Systems*, vol. 107, pp. 965–974, June 2020.

100. A. Jhumka, M. Leeke, and S. Shrestha, "On the use of fake sources for source location privacy: Trade-offs between energy and privacy," *The Computer Journal*, vol. 54, no. 6, pp. 860–874, June 2011.

101. W. Wang, L. Chen, and J. Wang, "A source-location privacy protocol in wsn based on locational angle," in *Proc. 2008 IEEE International Conference on Communications*, May 2008, pp. 1630–1634.

102. R. Manjula and R. Datta, "An energy-efficient routing technique for privacy preservation of assets monitored with wsn," in *Proc. 2014 IEEE Students' Technology Symposium*, March 2014, pp. 325–330.

103. P. Kumar, J. P. Singh, P. Vishnoi, and M. P. Singh, "Source location privacy using multiple-phantom nodes in wsn," in *Proc. TENCON 2015 - 2015 IEEE Region 10 Conference*, November 2015, pp. 1-6.

104. L. Zhang, "A self-adjusting directed random walk approach for enhancing source-location privacy in sensor network routing," in *Proc. 2006 International Conference on Wireless communications and Mobile Computing*, July 2006, pp. 33–38.

105. J. Huang, *et al.*, "A source-location privacy protection strategy via pseudo normal distribution-based phantom routing in WSNs," in *Proc. 30th Annual ACM Symposium on Applied Computing*, April 2015, pp. 688–694.

106. M. F. Khan, E. A. Felemban, S. Qaisar, and S. Ali, "Performance analysis on packet delivery ratio and end-to-end delay of different network topologies in wireless sensor networks (wsns)," in *Proc. 2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks*, December 2013, pp. 324–329.

107. D. Fotue, H. Labiod, and T. Engel, "Controlled data collection of mini-sinks for maximizing packet delivery ratio and throughput using multiple paths in wireless sensor networks," in

조선대학교
CHOSUN UNIVERSITY

Proc. 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications, September 2012, pp. 758–764.

108. Y. Yang, M. I. Fonoage, and M. Cardei, "Improving network lifetime with mobile wireless sensor networks," *Comput. Commun.*, vol. 33, no. 4, pp. 409–419, 2010.
109. H. Wang, G. Han, L. Zhou, J. A. Ansere, and W. Zhang, "A source location privacy protection scheme based on ring-loop routing for the IoT," *Comput. Netw.*, vol. 148, pp. 142–150, January 2019.
110. A. Liu, X. Wu, Z. Chen, and W. Gui, "Research on the energy hole problem based on unequal cluster-radius for wireless sensor networks," *Comput. Commun.*, vol. 33, no. 3, pp. 302–321, 2010.
111. A. Liu, D. Zhang, P. Zhang, G. Cui, and Z. Chen, "On mitigating hotspots to maximize network lifetime in multi-hop wireless sensor network with guaranteed transport delay and reliability," *Peer-to-Peer Netw. Appl.*, vol. 7, no. 3, pp. 255–273, 2014.
112. J. Ren, Y. Zhang, K. Zhang, A. Liu, J. Chen, and X. S. Shen, "Lifetime and energy hole evolution analysis in data-gathering wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 2, pp. 788–800, April 2016.
113. P. Spachos, D. Toumpakaris, and D. Hatzinakos, "Angle-based dynamic routing scheme for source location privacy in wireless sensor networks," in *Proc. 79th IEEE Veh. Technol. Conf. (VTC Spring)*, May 2014, pp. 1–5.
114. S. Gupta, P. Kumar, J. P. Singh, and M. P. Singh, "Privacy preservation of source location using phantom nodes," in *Information Technology: New Generations*, vol. 448. Cham, Switzerland: Springer, 2016, pp. 247–256.
115. Y. Li and J. Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in *Proc. IEEE INFOCOM*, March 2010, pp. 1–9.
116. Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 4, pp. 829–835, April 2006.
117. J. Zhang, J. Tang, and F. Wang, "Cooperative relay selection for load balancing with mobility in hierarchical wsns: A multi-armed bandit approach," *IEEE Access*, vol. 8, pp. 18110–18122, January 2020.

조선대학교
CHOSUN UNIVERSITY

118. S. Lata, S. Mehfuz, S. Urooj, and F. Alrowais, "Fuzzy clustering algorithm for enhancing reliability and network lifetime of wireless sensor networks," *IEEE Access*, vol. 8, pp. 66013–66024, April 2020.
119. I. Al-Anbagi, M. Erol-Kantarci, and H. T. Mouftah, "A survey on cross-layer quality-of-service approaches in wsns for delay and reliability-aware applications," *IEEE Communication Surveys & Tutorials*, vo. 18, no. 1, pp. 525–552, First Quarter 2016.
120. Y. Duan, W. Li, X. Fu, Y. Luo, and L. Yang, "A methodology for reliability of wsn based on software defined network in adaptive industrial environment," *IEEE/CAA Journal Of Automatica Sinica*, vol. 5, no. 1, pp. 74–82, January 2018.
121. M. T. Lazarescu, "Design of a wsn platform for long-term environmental monitoring for iot applications," *IEEE Journal On Emerging And Selected Topics In Circuits And Systems*, vol. 3, no. 1, pp. 45–54, March 2013.
122. K. Islam, W. Shen, and X. Wang, "Wireless sensor network reliability and security in factory automation: A survey," *IEEE Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews*, vol. 42, no. 6, pp. 1243–1256, November 2012.
123. J. Long, M. Dong, K. Ota, A. Liu and S. Hai, "Reliability guaranteed efficient data gathering in wireless sensor networks," in *IEEE Access*, vol. 3, pp. 430–444, May 2015.
124. N. Wang, and J. Zeng, "All-direction random routing for source-location privacy protecting against parasitic sensor networks," *Sensors*, vol. 17, 614, 2017.
125. R. A. Shaikh, et al, "Achieving network level privacy in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 1447–1472, February 2010.
126. H. Feng and J. Dong, "Reliability analysis for wsn based on a modular k-out-of-n system," *Journal of Systems Engineering and Electronics*, vol. 28, no. 2, pp. 407–412, April 2017.
127. S. R. Pokhrel, S. Verma, S. Garg, A. K. Sharma, and J. Choi, "An efficient clustering framework for massive sensor networking in industrial internet of things," *IEEE Trans. Ind. Inf.*, vol. 17, no. 7, pp. 4917–4924, July 2021.
128. H. Al-Tous and I. Barhumi, "Reinforcement learning framework for delay sensitive energy harvesting wireless sensor networks," *IEEE Sensors J.*, vol. 21, no. 5, pp. 7103–7113, March 2021.

조선대학교
CHOSUN UNIVERSITY

ACKNOWLEDGMENTS

By the grace of GOD, I have made it. I give all the glory to JESUS, and I am joyful in GOD my Savior.

The past four years have been the most productive. I have learned a lot and published some interesting work. Also, I became a mother to my daughter, Evelyn. Thanks to my entire family for loving and supporting me through it all. Happiness, Irene, Benson, and Nelson have been very supportive and enthusiastic about my PhD course. My mother, Odina Mutalemwa supported me as I ventured through both motherhood and PhD studies. I am profoundly grateful. My father, Charles K. Mutalemwa provided me with a strong educational foundation. Then, he taught me about perseverance and kept me motivated throughout my PhD endeavors. I am so grateful.

My fellow PhD student, Ijaz has been friendly and supportive. We had many fruitful discussions during my time in the Wireless Comminication and Network Lab. Together with Lam and Bih Lii, we made a group of good friends who worked hard while having fun and enjoying the Korean culture.

With gratitude, I would like to acknowledge the immense work of my advisor and supervisor, Professor Seokjoo Shin. He provided me with the necessary guidance and support that made it all possible. Also, I appreciate the constructive comments from my dissertation committee chair, Professor Sangman Moh and the other committee members, Professor Kang, Professor Choi, and Professor Lee. Finally, I am thankful to the BK21 for providing the financial support.

Lilian C. Mutalemwa

조선대학교
CHOSUN UNIVERSITY

PUBLICATIONS

Parts of this dissertation were published by the author in the following:

1. L. C. Mutalemwa and S. Shin, "Novel approaches to realize the reliability of location privacy protocols in monitoring wireless networks," *IEEE Access*, vol. 9, pp. 104820–104836, July 2021.
2. L. C. Mutalemwa and S. Shin, "Comprehensive performance analysis of privacy protection protocols utilizing fake packet injection techniques," *IEEE Access*, vol. 8, pp. 76935–76950, April 2020.
3. L. C. Mutalemwa and S. Shin, "Secure routing protocols for source node privacy protection in multi-hop communication wireless networks," *Energies*, vol. 13, p. 292, January 2020.
4. L. C. Mutalemwa and S. Shin, "Regulating the packet transmission cost of source location privacy routing schemes in event monitoring wireless networks," *IEEE Access*, vol.7, pp. 140169 –140181, September 2019.

Also, the author has published the following:

JOURNAL PUBLICATIONS

1. L. C. Mutalemwa and S. Shin, "A classification of the enabling techniques for low latency and reliable communications in 5g and beyond: Ai-enabled edge caching," *IEEE Access*, vol. 8, pp. 205502–205533, November 2020.
2. L. C. Mutalemwa and S. Shin, "Achieving source location privacy protection in monitoring wireless sensor networks through proxy node routing," *Sensors*, vol.19, no.5, p. 1037, 2019.
3. L. C. Mutalemwa and S. Shin, "Routing schemes for source location privacy in wireless sensor networks: A survey," *The Journal of Korean Institute of Communications and Information Sciences*, vol.43, no.9, pp. 1429–1445, September 2018.
4. L. C. Mutalemwa and S. Shin, "Strategic location-based random routing for source location privacy in wireless sensor networks," *Sensors*, vol.18, no.7, p. 2291, 2018.

조선대학교
CHOSUN UNIVERSITY

CONFERENCE PUBLICATIONS

1. L. C. Mutalemwa and S. Shin, "On the performance of source location privacy protocols under varied sensor node residual energy," in *Proc. 12th International Conference on Information and Communication Technology Convergence (ICTC2021)*, Jeju Island, South Korea, October 20–21, 2021, pp. 237–240.

2. L. C. Mutalemwa and S. Shin, "On the performance gains of decentralized edge caching schemes in 5g and beyond," *in Proc. 2nd Korea Artificial Intelligence Conference*, Jeju Island, South Korea, September 29-October 1, 2021, pp. 199–202.

3. L. C. Mutalemwa and S. Shin, "Ultra-reliable low-latency communications in 5g and beyond: challenges and research opportunities," *in Proc. 2021 Summer Workshop on Computer Communications (SWCC2021)*, Online, August 25, 2021, pp. 36–41.

4. L. C. Mutalemwa and S. Shin, "Achieving location privacy and flexible energy management in industrial internet of things," *in Proc. 2021 Summer Workshop on Computer Communications (SWCC2021)*, Online, August 25, 2021, pp. 32–35.

5. L. C. Mutalemwa and S. Shin, "The impact of energy-inefficient communications on location privacy protection in monitoring wireless networks," in *Proc. 12th International Conference on Ubiquitous and Future Networks (ICUFN)*, Jeju Island, South Korea, August 17-20, 2021, pp. 289–294.
6. L. C. Mutalemwa and S. Shin, "On the performance of source location privacy protocols with multiple source nodes in wsns," in *Proc. The Korean Institute of Communications and Information Sciences (KICS) Summer Conference 2021*, South Korea, June 16–18, 2021.
7. L. C. Mutalemwa and S. Shin, "A study on reinforcement learning techniques for deterministic ultra-low latency in 5g and beyond," in *Proc. 2021 Korean Society for Next-Generation Computing Society Spring Conference*, Gwangju, South Korea, May 13-15, 2021.
8. L. C. Mutalemwa and S. Shin, "Achieving bounded ultra-low latency in 5g and beyond: Challenges and future research directions," in *Proc. The Korean Institute of Communications and Information Sciences (KICS) Winter Conference 2021*, Pyeongchang, South Korea, February 3–5, 2021, pp. 38–41.
9. L. C. Mutalemwa and S. Shin, "Energy balancing and source node privacy protection in event monitoring wireless networks," in *Proc. 35th International Conference on*

조선대학교
CHOSUN UNIVERSITY

Information Networking (ICOIN 2021), Jeju Island, South Korea, January 13–16, 2021, pp. 792–797.

10. L. C. Mutalemwa and S. Shin, "On the performance gains of federated learning edge caching in vehicular internet of things," in *Proc. 1st Korea Artificial Intelligence Conference*, Online, December 16–18, 2020, pp. 136–138.
11. L. C. Mutalemwa and S. Shin, "Improving the packet delivery reliability and privacy protection in monitoring wireless networks," in *Proc. 2020 International Conference on Information and Communication Technology Convergence (ICTC2020)*, Jeju Island, South Korea, October 21–23, 2020, pp. 1083–1088.
12. L. C. Mutalemwa and S. Shin, "Experimental comparison of traffic analysis adversaries in event monitoring wireless networks," in *Proc. 9th International Conference on Smart Media and Applications*, Jeju, South Korea, September 17–19, 2020, pp. 44–49.
13. L. C. Mutalemwa and S. Shin, "Experiments on traffic analysis adversaries against source location privacy routing protocols," in *Proc. Summer Workshop on Computer Communications*, Online, August 27, 2020, pp. 27–29.
14. L. C. Mutalemwa and S. Shin, "Investigating the packet delivery reliability of source location privacy protocols in wsns," in *Proc. The Korean Institute of Communications and Information Sciences (KICS) Summer Conference 2020*, Pyeongchang, South Korea, August 12–14, 2020, pp. 621–623.
15. L. C. Mutalemwa and S. Shin, "Caching solutions and content response latency in information-centric internet of things: A survey," in *Proc. Korean Smart Media Society 2020 Spring Conference*, Gwangju, South Korea, May 22–23, 2020, pp. 243–246.
16. L. C. Mutalemwa M. Kang, and S. Shin, "Controlling the communication overhead of source location privacy protocols in multi-hop communication wireless networks," in *Proc. 2nd International Conference on Artificial Intelligence in Information and Communication (ICAIIC 2020)*, Fukuoka, Japan, February 19–21, 2020, pp. 55–59.
17. L. C. Mutalemwa and S. Shin, "Investigating the energy efficiency of privacy protection protocols with fake packet sources," in *Proc. The Korean Institute of Communications and Information Sciences (KICS) Winter Conference 2020*, Gangneung-si, South Korea, February 5–7, 2020.

조선대학교
CHOSUN UNIVERSITY

18. L. C. Mutalemwa and S. Shin, “Investigating the influence of routing scheme algorithms on the source location privacy protection and network lifetime,” in *Proc. 10th International Conference on ICT Convergence (ICTC 2019)*, Jeju Island, Korea, October 16–18, 2019, pp. 1188–1191.
19. L. C. Mutalemwa, J. Seok, and S. Shin, “Experimental evaluation of source location privacy routing schemes and energy consumption performance,” in *Proc. 2019 19th International Symposium on Communications and Information Technologies (ISCIT)*, Ho Chi Minh City, Vietnam, September 25–27, 2019, pp. 86–90.
20. L. C. Mutalemwa and S. Shin, “A credible and energy-efficient source location privacy scheme for monitoring wireless networks,” in *Proc. The Korean Institute of Communications and Information Sciences (KICS) Summer Conference 2019*, Jeju Island, Korea, June 19–21, 2019, pp. 375–378.
21. L. C. Mutalemwa and S. Shin, “Realizing source location privacy in wireless sensor networks through agent node routing,” in *Proc. 9th International Conference on ICT Convergence (ICTC 2018)*, Jeju Island, Korea, October 17–19, 2018, pp. 1283–1285.
22. L. C. Mutalemwa and S. Shin, “A new diversional routing scheme to preserve source location privacy in wireless sensor networks,” in *Proc. 3rd International Conference on Next Generation Computing*, Kaohsiung, Taiwan, December 2017, pp. 260–262.