February 2017

Master’s Degree Thesis

Directional Random Routing to Enhance Source-Location Privacy in Wireless Sensor Networks

Graduate School of Chosun University

Department of Computer Engineering

Amod Pudasani

Directional Random Routing to Preserve Source-Location Privacy in Wireless Sensor Networks

무선 센서 네트워크에서 발생원 위치 보안을 개선하기 위한 지향적 랜덤 라우팅

February 24, 2017

Graduate School of Chosun University

Department of Computer Engineering

Amod Pudasaini

Directional Random Routing to Preserve Source-Location Privacy in Wireless Sensor Networks

Advisor: Prof. Seokjoo Shin, Ph.D.

A thesis submitted in partial fulfillment of the requirements for a Master's degree

October 2016

Graduate School of Chosun University

Department of Computer Engineering

Amod Pudasaini

푸다사이니 아모드의 석사학위논문을

인준함

위원장 조선대학교 교수 모 상 만 (인)

위 원 조선대학교 교수 강 문수 (인)

위 원 조선대학교 교수 신 석주 (인)

2016 년 11 월

조선대학교대학원

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Directional Random Routing to Preserve Source-Location Privacy in Wireless Sensor Networks

Amod Pudasaini
Advisor: Prof. Seokjoo Shin, Ph.D.
Department of Computer Engineering
Graduate School of Chosun University

Wireless sensor networks are being deployed in different event monitoring applications and the location of source indicates valuable information like the presence of valuable asset or person, behavior of event etc. Thus, strong location privacy preservation technique is always preferred by sensor system. Although the content is secured with different encryption techniques, open wireless channel allows an adversary to analyze traffic patterns, trace back and locate the source node. To achieve source-location privacy, several techniques based on flooding, random walk and dummy traffic transmission are proposed for WSN. In this thesis, we propose a new routing method that randomly forwards a packet towards the sink such that an adversary will find difficult in tracing the source location.. We evaluate privacy of our proposed method in terms of adversary's success rate. The simulation results shows proposed routing strategy is better in preserving privacy.

요약

무선 센서 네트워크에서 발생원 위치 보안을 개선하기 위한 지향적 랜덤 라우팅

푸다사이니아모드

지도교수: 신석주

조선대학교 컴퓨터공학과

무선 센서 네트워크는 다양한 이벤트 모니터링 어플리케이션에 적용되고 있으며 네트워크에서의 발생원 위치는 이벤트 행위, 사람 혹은 자산의 존재 유무 등과 같은 가치있는 정보를 내포하고 있다. 따라서, 강력한 발생원 위치 보안 기술은 이러한 센서 시스템에서 중요하게 여겨지고 있다. 비록 정보 자체는 다양한 암호화 기술을 활용하여 보호할 수 있지만, 공개된 무선 채널 환경은 공격자가 트래픽 패턴을 분석하고 이를 역추적하여 발생원의 위치를 알아낼 수 있다. 발생원 위치 보안 기술로는 플러딩, 랜덤 워크, 더미 트래픽 전송 과 같은 기법들이 WSN 용으로 제안되어 왔다. 본 연구에서는 패킷을 싱크 노드 쪽으로 랜덤 포워딩 하여 공격자가 발생원의 위치를 추적하기 어렵게 할 수 있는 새로운 라우팅 기법을 제안하였다. 공격자 성공률과 같은 성능 척도를 이용하여 제안 기법의 성능을 평가하였으며 시뮬레이션 결과로부터 제안된 라우팅 기법이 기존 방식에 비해 위치 정보 보안에 더 나은 결과를 도출할 수 있음을 증명하였다.

I. INTRODUCTION

Sensor networks are a networking of hundreds or thousands of small low power, limited memory, and standalone device called nodes capable of monitoring various events which generates useful data and deliver it to sink. Generally, they are deployed in hostile area in number of different applications [1] to monitor various parameters like weather, endangered species, military surveillance, structural failure etc. Now, this information is of primary concern which might be exposed to variety of attacks ranging from eavesdropping to compromise of a node. The mere fact of WSNs deployed in open environment with limited capacity and communication performed through wireless channels possess privacy breaches. Thus, maintaining privacy in wireless sensor networks (WSNs) is quite important job of a network designer.

Privacy of the sensor node can be defined as delivery of event information only for legitimate users such that no other parties can either analyze the traffic patterns and estimate the behavior nor decipher the content. In order to protect the content, various data encryption methods [2] are employed in wireless sensor networks (WSNs) and abundance of research are being carried out in the particular field to protect content information. Compared with data privacy, contextual privacy has not acquired much attention in WSNs environment. However, an adversary may be able to gather valuable information without decrypting the data payload and can analyze the traffic pattern to estimate the behavior of network and locate the source node with contextual information like traffic patterns, transmission speed etc. With the mere fact of sensor networks operating in multi hop fashion the adversary employs backtracking algorithm to trace the source node. Traffic patterns between different hops in WSNs are utilized to infer the location of the source generating the message. Thus, the contextual privacy of transmission pattern needs to be obscured from the attacker and the issue is even more eminent whenever the valuable asset is being monitored. For instance, the endangered species in the wildlife is of prime importance and context associated with the animal is very crucial. From the hunter's perspective, the asset has influential market value and is always in the process to track it. Thus, it is necessary to hide routing information to increase traffic uncertainty from protection against traffic analysis. Based on this principle many authors propose different methods to preserve the traffic pattern that can link to source and sink in the network from adversary.

In the general IP network environment, different privacy preservation techniques related to the protection of context of the user has been proposed through anonymous communication. For the traffic analysis attack Chaum [3] have proposed a mix to cloak the system from attacker performing traffic analysis. Basically, mix transforms the accepted message of fixed length generated from multiple sources. Similarly, onion routing [4] provides user location privacy in the IP networking environment. Tor [5] serves as second generation onion routing popular for providing anonymous communication over internet by relaying the stream of traffic through Tor circuit and hides user's location information. All these systems are computationally powerful and employ complex devices in order to service the privacy of a user. In the context of sensor networking these systems cannot be deployed and rather other obfuscating techniques have been developed. Those methods will be briefly described in the thesis shortly.

A. Research Objective

In the recent years, sensor networks have proved to be center of interest be it for academicians or professionals owing to wide range of applications offered. Generally, sensor networks are found to be applied in various applications like weather monitoring, smart home systems, health inspection, habitat supervision, and defense application. To be more specific, Wireless Sensor Network (WSNs) is a heterogenous mixute of inexpensive miniaturized devices called sensors that are distributed in the application environment. These sensors usually performs sensing, computation and communication. Compared with the legacy wired communication technology WSNs is different in terms of the system cost, flexibility, and deployment complexity. With all these attributes, WSN are like to dominate the world of data communication. One of the key concerns for such a sought-after technology is location privacy of the sensor nodes, the inevitable aspect of wireless sensor networks. Location privacy usually implies the physical location of the data source and the sink. For the sensitive applications like military purposes seeking high degree anonymity, privacy always comes first and it hardly is compromised with other aspects. A meagre failure in protection of the location privacy of source can lead to failure of entire network. Various techniques have been developed and implemented for preserving location privacy of source and most importantly, gathering point of data from all sensor nodes, the sink in WSN applications.

The location of the data source and the base station holds a significant importance when it comes to maintaining privacy. Unfortunately, the open nature of a sensor network eases disclosing of privacy resulting from either eavesdropping or analyzing traffic patterns. This can ultimately reveal the location of crucial nodes whose privacy is much anticipated. Adversary may analyze traffic patterns between different communication entities and ultimately track the location of the sensor nodes. Different approaches have been put forward to ensure this; however, it is wise on our part to make rational comparison among all to come up with the best.

- To understand requirement of location based privacy in wireless sensor networks
- To identify different mechanisms withstanding privacy of sensor network in communication
- To compare and contrast different techniques and present possible research issues relevant to privacy
- To propose a new routing method for enhancing source-location privacy in WSN.

To preserve the location privacy, traffic from source needs to have some random behavior while forwarding packets towards sink. We propose a routing based on reference coordinates which makes random forwarding decision and at the same time forwards the packet towards sink. To achieve this, two different pools of reference coordinates are stored on a cache of a node. For forwarding decision, each node randomly selects one of the pools and from the selected pool randomly picks one coordinate. Now, the sensor forwards a packet to one node from its neighbor list which is shortest in distance to the selected reference coordinate. In this way, this method introduces path diversification where each unique packet from source is randomly forwarded towards different sections of the network ultimately making an adversary difficult in tracing source location.

B. Thesis Layout

The remaining of the thesis is organized as follows: In chapter II, privacy in WSN is described with different exixting methods for WSN location privacy. Different existing methods are compared with respect to privacy preservation performance, eachs strategy's advantages and limitations. Also in this chapter, the open issues and challenges in the design of efficient routing strategy has been discussed. The proposed directional routing method is presented in chapter III. In chapter V, the performance of the proposed routing method is evaluated via computer simulation and compared with the phantom single-path routing and gfreedy random walk method. Finally, in chapter VI the thesis is concluded.

II. PRIVACY IN WSN

Privacy in wireless sensor network is divided into two subdivisions : content privacy and contextual privacy. Content deals with payload privacy. We are concerned with contextual privacy rather than content privacy. Contextual privacy is concerned with protection of context associated with the traffic. This includes the measurement of sensed data and the transmission and reception rate of the data from the source and sinks respectively. The figure below shows the categorization of contextual privacy in sensor networks. The context of the sensor environment is further classified into system and user privacy. The system privacy is concerned with obfuscation of traffic generated source and reception from adversary. The time event of the generation of event is also crucial in some applications. The behavior of the user can be inferred from the temporal information in the channel. Thus Protection of time information about the generation is dealt in temporal privacy.

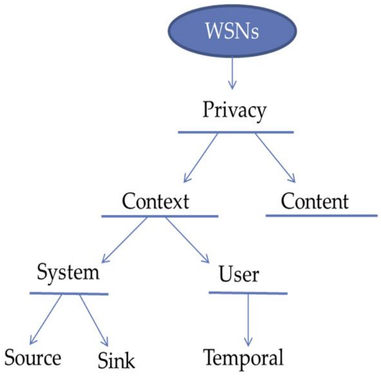


Figure 1. Categorization of privacy in WSNs.

If we consider a scenario in [8] that is WSNs application for for detecting and monitoring an endangered animal where a WSNs is deployed in the forest The panda hunter game here assumes attacker to eavesdrop the channel in order to locate the endangered species. Thus the defender needs to choose a powerful routing strategy in order to preserve the panda. The animal is mobile with change in its location periodically. Radio device attached with the species sends its signal to the receiver node in the vicinity. Now, whenever a sensor node detects an endangered species, it tabulate a report about the animal's location activities and sends the report to the base station. The communication is carried out through a multi-hop routing protocol. An adversary who is a hunter is well equipped with devices such as antenna and spectrum analyzers. Those device can be utilized to capture wireless signals between sensor nodes and measure the angle of arrival of signals. Along the transmission range the signal could be eavesdrop and backtrack the sender.

The adversary would capture wireless communication signals from source node along the transmission path. An adversary can carry out a traffic backtracking attack to locate the source sensor node. It is done by capturing wireless signals for each hop, analyzing their direction, and then identifying the parameters like angle of arrival, signal strengths. Now, it is very much essential to understand the adversary behavior. The adversary can be classified as global adversary and local adversary respectively.

Global adversary has the knowledge of the full topology, as he is economically powerful and owns the certain portions of the network. In the case of local adversary, it has limited knowledge of network. It resides in a single point and moves in the topology to estimate the location of the source node.

Attacker always tries to estimate the location of source node utilizing routing strategy (*R)*. Now, if the estimation error of adversary is high then *R* is considered to be providing excellent privacy. The energy is also considered while designing the various obfuscating techniques. Now, the routing strategy *R* is considered to be powerful in the context of privacy if it is able to disguise the adversary from locating to the source.

Traffic analysis techniques [6] like rate monitoring attack, time correlation attack and content analysis attack are used by adversary. In rate monitoring adversary monitors the rate of transmission and moves closer to node with high sending rate. Attackers statistically analyses the time of packet arrival from different nodes and correlate them in time correlation attack. However, in content analysis attack, adversary gathers maximum information from data headers and payloads.

Now, in order to preserve the location privacy of either source or sink several methods are proposed by researchers. Some of the existing techniques are briefly described below:

A. SOURCE LOCATION PRIVACY

Source node which is generating traffic in WSNs is crucial as it can be compromised to an adversary. This source can be a valuable item thus adversary is alwas interested it to achieve this valuable asset. So, it is important to keep the attacker away from the original source of data generation. For this many routing mechanism has been proposed whose goal is to obfuscate an attacker from tracing the source node in WSN. Different methods based on mechanism of flooding, random walk and fake traffic generation are proposed which serves to preserve context of source.

We review the existing techniques that deal with the preservation of source from adversary extracting information related to traffic in the channel.

1. Flooding

In this mechanism [7] all node is participated in flooding process to deliver the packet to sink. Flooding of packet in all part of network will distribute the traffic, so that it is difficult for an adversary to track the source of data by analyzing network traffic. Nodes check received packed and relay packet to neighboring nodes. Flooding includes baseline flooding, probabilistic flooding.

In the baseline flooding strategy [8], information or event from source node is transmitted to its all corresponding neighbors. As depicted in fig 1, on receiving the packets from a node, neighbor subsequently re broadcast the packet to other nodes in its transmission range. However, every node forwards the same message only once by implementing the cache in the nodes which can remember the packets from its sequence numbers. This technique is used to flood packet all over the network. But, if adversary analyses the traffic, residing near the sink, source can be tracked using back track algorithm. First packet always arrives from the shortest distance to the sink and an adversary can move one hop at a time backward and track the source. With this method, energy consumption of the network is high and adversary can also locate source in a short period of time.Probabilistic flooding [8] is expansion of baseline flooding strategy to overcome energy consumption issue. For mitigating energy consumption, only a subset of nodes is participated in flooding process. Each node calculates the random number x from 0 to 1. If this value of x is less than forwarding Probability Pfwd,(x<Pfwd),then the corresponding packet is forwarded to its neighbors. Forwarding a packet with a predetermined probability makes this scheme energy efficient. However, the problem of shortest path back tracking could not be solved. Also, the randomness in broadcasting a packet is dependent on forwarding probability which consequently reduce delivery ratio.

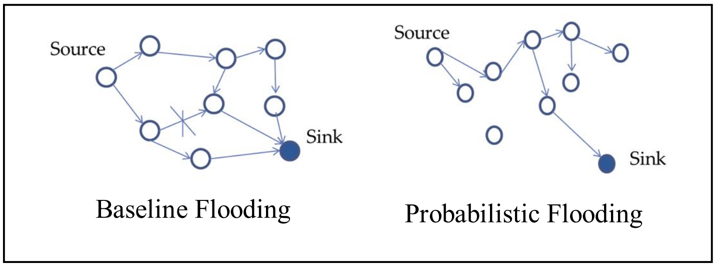


Figure 2. Baselne flooding and Probabilistic flooding

2. Phantom Routing

In random walk [9], the each packet from source is directed to different routes in the network. Each unique packet traverse through different paths in the WSNs. The sink has to capability to reorder the packet to generate the desired message.

As shown in fig 2, in phantom routing, first a packet travel a certain number of hops in random walk fashion where a phantom source is selected, after that it either utilizes single-path or flooding mechanism. In order to hide source location from adversary, first, the node takes a walk value (Dwalk), which is a hop count, and packet is moved randomly until it reaches that hop Count. The node receiving the packet in Dwalk hop is considered as phantom source. Also, to eliminate the possibility of packet to stay around source during random walk, the neighbors of a node is divided near and far set. Now, once the packet is at phantom source either flooding or single-path strategies can be used. The main idea of phantom routing is to entice adversary far from real source. However, the random walk does not make much progress and the source could be easily located. Also, the energy consumption is also high when the flooding technique is used.

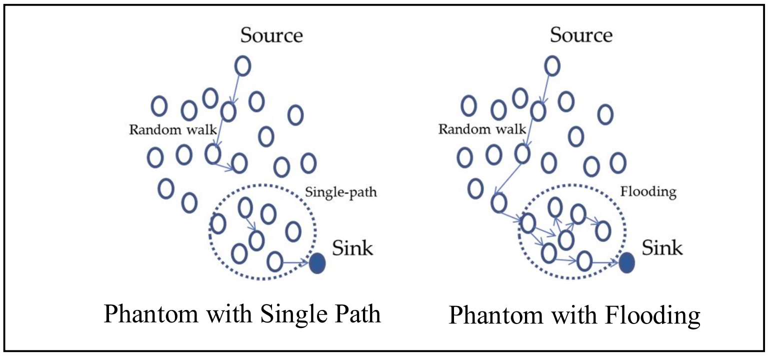


Figure 3. Phantom Routing

3. Greedy Random Walk

In greedy random walk [10], sink and source both participate in random walk for delivery of data. As shown in fig 4, at first, sink chooses h number of hops and randomly select h nodes in backward direction, which acts as receptors. After selecting receptors, source forwards the packet in the fashion of random walk. Each packet is traversed new path and when packet meets one of the receptor, it follows the predetermined path. The method tries to cover all part of network at different times using random walk. The packet might loop for random walk which will degrade network performance.

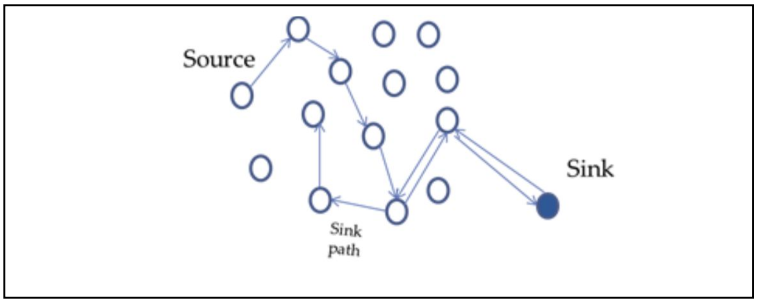


Figure 4. Greedy Random Walk

4. Dummy Data Transmission

Dummy packets [11] are generated by each sensors and flows across the network with pre-determined probability. The objective is to disguise adversary so that actual location will not be revealed. The fake packet is discarded but the actual packet is forwarded towards sink. Intelligent adversary, however, can distinguish the nature of real and dummy traffic.

5. Fake Source Routing

As the name suggests, the behavior of source is simulated [12] by some nodes in the network in order to confuse the adversary. The base station will create fake sources whenever it receives a signal indicating that a sensor wants to send data. The position of simulated sources is assumed to be far in distant with real source but these fake sources will have similar distance to the sink. To achieve it, the size of network should be of considerably large. Both real and fake senders start generating packets at the same instance and with the same traffic pattern. One of the major question of this technique is whether the fake source can precisely simulate the behavior of real data sources or not. Furthermore, such a technique will also incur more energy consumption in WSN environment.

B. Sink Location Privacy

In WSNs environment all data from the sensors nodes arrive at the sink. As required by the application the purpose of the sink is to process the data as. The privacy of the base station or sink is primarily concerned because of the fact that revealing the physical location of a sink to adversary may give lead to disruption of service or loose vital information or might occur other undesirable consequences. The legacy routing protocols could reveal the location as sensor nodes near the base station forward a greater number of data packets compared with other sensor nodes that are far away from the sink .Different methods have been proposed in order to protect the privacy of sink which are discussed below:

1. Multi Parent Routing

Multi parent routing [13] is introduced in order to conceal sink from an adversary that studies parent child information by monitoring rate of traffic. The traffic near the sink has high density than that of the farthest node in the network. An attacker can easily locate the sink if he does rate analysis and move to sink. So, to mitigate this scenario multi routing technique spreads the traffic evenly in the network such that an adversary will be confused from inferring location of base station. The network is divided into subsequent levels. To achieve this, sink initially transmit beacon with level zero. First order node in the transmission range which receives this beacon increase their level and re broad cast them. Now sensors select all neighbors whose value is less than theirs as parent nodes.

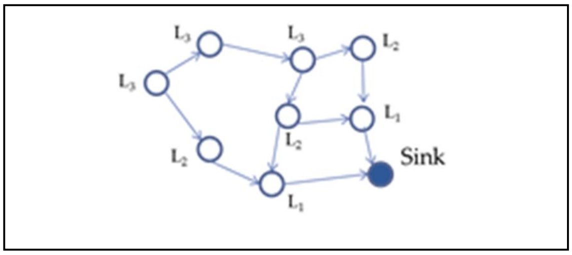


Figure 5. Multi Parent Routing

In the figure, the nodes in the transmission range of sink are found to be in level one (L1). Similarly, higher levels are marked in the network with beacon broadcast. Now, a node identifies its parent node as one with level lower than acquired by itself. Each sensor nodes erase its level value after it finds corresponding parent nodes. For a transmission of packets, nodes select one of its multiple parents in the range to forward the packet towards sink. This technique is similar to the concept of phantom routing, but the goal is to spread out traffic evenly all over network so that adversary intention to track the location of base station shall be failed.

2. Fractal Propagation

Although traffic is spread in multi parent routing nature of shortest path delivery might be undesirable in a way to preserve sink location privacy. To mitigate such phenomenon fractal propagation technique [14] was proposed. In fractal propagation technique, first the source nodes forward the packet and transmit it towards sink. While this transmission takes place the neighboring nodes generates fake packet and broadcast it. The fake packet then travels a given number of the hops. Activity of packet transmission is increased in the network area which tends to deceive the adversary.

When a sensor node overhears packet from its neighbor it starts generating fake packet with pre-determined probability distribution and selects system parameter *K*. The fake packet is randomly forwarded to neighboring node with value of a parameter *K*. Now this neighbor decrease value of *K* by one and again selects one of neighbor randomly. The fake packet travels in the network until the value of system parameter is zero. This technique works with the assumption that normal node can distinguish the fake packet and real packets while the adversary cannot distinguish between the two packets. For this, node has to use encryption key to distinguish between fake and real traffic and act accordingly. And assume tha an adversary will be unable to do so because he doesn't own an encryption key. Fractal propagation can be used with multi parent routing and random walk for making communication flow in the network to be somewhat like a fracture of the structure. As new packets are introduced in the network implementing the fractal propagation requires extra energy consumption .

3. Location Privacy Routing

Location privacy routing protocol (LPR) [15], introduce irregularity in routing paths and forwarding direction of packet does not always point towards receiver. The concept of this technique is to divide neighboring nodes of each sensor into closer and further list. All the nodes that are farther from sink is considered as farthest list and all sensors nodes closer to sink falls in closer list. Distance between two sensor nodes is measured either in hop distance or by Euclidean distance. The node selects to forward a packet to farther list with probability P and closer list with 1-P. With low P more from closer list are choosen and the routing path is reduced but fails in providing strong privacy. In Contrarst with this, high P allows farther list to be selected by nodes. This will enhance the privacy but latency is increased tremendously. Thus there is a tradeoff between privacy and other network performance with different values of P in LPR technique. To boost the privacy, fake packet can be further injected along with the original packet transmission. Involvement of packet in the network will increase network overhead. Size of the network and the division of two lists are quite crucial in maintaining privacy using this method. Energy requirement of the network gets increased while location of sink is being preserved. The probability factor is important parameter and should be well selected for balance performance of this technique.

C. Comparison and Discussion of Privacy Preserving Methods

In this section, a detailed comparison of the privacy preserving methods designed for WSNs is discussed. In Table 1, the source and sink location privacy reviewed in the previous section are compared with respect to performance, advantages and limitations.The comparison of routing methods is evaluated on the basis of privacy preservation, energy consumption, delay of packet delivery.

As packet is flooded all over network, energy consumption in baseline flooding is increased tremendously. Compared with baseline flooding probabilistic flooding and phantom routing seems to consume less energy. It is because of the fact that, in probabilistic flooding the brodcasting nature of a packet is depended on the forwarding probability. And in phantom random walk with single-path consumes less energy. The result from [6] shows the reduction of energy consumption while using phantom routing instead of flooding. The greedy random walk seems to consume no extra energy in the application because it does not use flooding mechanism. The energy requirement is reduced compared to other source location privacy preservation techniques. To state about methods employed for sink-location privacy, an introduction of fake packet in fractal propagation and LPR increase energy requirement while in multi parent there is no extra energy overhead is involved.

Delay for baseline flooding is low delay because the message arrives to the sink from the shortest path. The same holds in the case of multi parent routing. All other methods have high delay as they involves in diverting packet to other part of network before delivering it to sink.

The uncertainty of data delivery for probability flooding is because packet transmission is dependent on the forwarding probability. Also, phantom routing using probabilistic flooding shows same behavior. In greedy the delivery of message is depended on the intersection of two random walk, one from the source and other from the sink side. In the sink privacy techniques data delivery is guaranteed.

Privacy preservation of the source node is fair in the case of baseline flooding. The data arrives to the sink from shortest path and the adversary easily backtrack the source node.

With introduction of forwarding probability in probabilistic flooding the energy is reduced but the level of privacy remains same as of baseline flooding. This is because of the same reason of shortest path delivery of packet to sink make an adversary easily trace back location of source node. Now, with introduction of random walk followed by flooding in the phantom routing the adversary performing backtracks is only able to track to phantom source. Two way random walk increase the privacy preservation capability in greedy random walk method. Fake traffic has satisfactory performance as intelligent adversary can distinguish between fake and real traffic.

In the case of sink privacy preservation, mufti parent routing serves fair performance. Compared with Multi parent routing technique other two are good at preserving source location privacy

Table 1. Comparison of the location preserving methods for WSNs.

Privacy Techniques		**Privacy Performance**	**Advantages**	**Limitations**
Suorce-Location Preservation	Baseline and Probabilistic Flooding [8]	• Source is located in short time	• Easy implementation • Data delivery is guaranteed in baseline flooding.	• Consumes high energy due with minimum privacy preservation
	Phantom Routing [8]	• Outperforms flooding based privacy preservation technique • Adversary is enticed to new phantom source which increases traceback time	• Phantom source entice attacker away from source	• Random walk tends to stay around source. •Source is traced in short time period.
	Greedy random walk [10]	• Better performance than Flooding and Phantom routing	• An adversary is highly distracted compared with other methods	•Data arrival depends on intersection of two random walk
	Dummy Data [11]	• Privacy preservation is better when mixed with other strategy.	• Obfucation due to dummy traffic	• Intelligent adversary can distinguish traffic High energy consumption

Table 1. ***Continued.***

Privacy Techniques		Privacy Performance	Advantages	Limitations
Sink-Location Preservation	Multi Parent Routing [13]	• Energy consumtion is minimum on extra communication	• It guarentees data delivery with no extra delay	• Privacy preservation is fair
	Fractal Propagation [14]	• Better than multi parent	• Packet activity is increased to disguise adversary	• Requires to encrypt fake data each time Extra energy requirement
	Location Privacy Routing [15]	• For low forwardingProbability-low latency with reduced privacy • For high forwardingProbability-high latency with increased privacy	• Forwarding packet has irregularity which is good for privacy	•Depends on size of network and two lists.

D. Open Issues and Challenges

There are many challenges prevailed in the field of location privacy preservation techniques in WSNs. In this section we are going to discuss on the possible challenges and open issues for location privacy schemes for WSNs:

1. Network performance enhancement

The existing techniques if found to have huge tradeoff between privacy and network performance. Almost all methods introduce some techniques that increase network latency in order to preserve privacy. Optimum solution that could help gain both benefits is still another part of the story. This could be the future step to develop the techniques that could give best performance in both side of interest.

2. Energy Reduction

Although some techniques seems to reduce energy while providing privacy of the sink or the source location but it is not promising. It is necessary to understand that energy is one of the crucial factors in wireless sensor networks. So, designing the energy efficient privacy techniques will always be acknowledged by large number of applications.

3. Preserving mobility of sink

In the scenario of application where sink might be mobile it can be thought of providing privacy in itself. However, nodes need to be aware of its new location in order to forward data. So, this can be challenging for improving the privacy of the sink when it is moving constantly in the network.

4. Exact Simulation of Source

It is also interesting and challenging to simulate the exact behavior of source by some nodes in the network. This can increase the energy and memory requirement but could achieve high degree of anonymity in the sensor network location privacy schemes.

III. DIRECTIONAL RANDOM ROUTING METHOD

A. Network model and assumptions

Two-dimensional coordinate system is adopted as the network model. Every node is assumed to have knowledge of their location which could be obtained either via Global Positioning System (GPS) or some triangulation algorithms. Also, each node has memory to store its neighboring table and reference coordinates. The reference coordinates are list of coordinates which is unique for each node and it is utilized whenever a node has to take packet forwarding decision. With respect to sink a particular node could be at any one of the four different positions: Left-Down, Left-Up, Right-Down, RightUp. As shown in table 2 and table 3, there will be two sets of reference coordinates, where first set consists of nine reference coordinates and second set has five reference coordinates. Depending on node position, every node will have its two sets of reference coordinates. We also introduce a constant value called Directivity factor (D_f) which is used in our routing algorithm to randomly choose one of the sets of reference coordinates while making a decision of forwarding a packet. Appropriate value of D_f is found through simulation that will ensure delivery of a packet and provides a strong location privacy for the source node.

Table 2. List of reference coordinates for a node at different position in the network when random number>D_f

Left –Down	Left-Up	Right-Down	Right-Up
(X,y_i)	(X,y_i)	(X_i,Y)	(X+N,y_i)
(X,[y_i+(Y+N)]/2])	(x,[y_i+Y]/2)	([x_i+X]/2,Y)	(X+N,[y_i+Y]/2)
(x_i,Y)	(x_i,Y+N)	(X+N,y_i)	(x_i,Y+N)
([x_i+(X+N)]/2],Y)	([x_i+(X+N)]/2],Y+N)	(X+N,[y_i+(Y+N)]/2])	([x_i+X]/2],Y+N)
(X,Y+N)	(X,Y)	(X,Y)	(X,Y+N)
(X+N/2,Y+N)	(X+N/2,Y)	(X,Y+N/2)	(X,Y+N/2)
(X+N,Y+N)	(X+N,Y+N)	(X,Y+N)	(X,Y)
(X+N,Y+N/2)	(X+N,Y+N/2)	(X+N/2,Y+N)	(X+N/2,Y)
(X+N,Y)	(X+N,Y)	(X+N,Y+N)	(X+N,Y+N)

Table 3. List of reference coordinates for a node at different position in the network when random number<D_f

Left –Down	Left-Up	Right-Down	Right-Up
(xi,Y+N)	(xi,Y)	(X,yi)	(X,yi)
([xi+(X+N)]/2],Y+N)	(X+N,[yi+Y]/2)	(x,[yi+(Y+N)]/2)	(X, [yi+Y]/2)
(X+N,Y+N)	(X+N,Y+N)	(X,Y+N)	(X, Y)
(X+N, ([yi+(Y+N)]/2])	([xi+(X+N)]/2],Y)	([xi+X]/2,Y+N)	([xi+X]/2,Y)
(X+N,yi)	(X+N,yi)	(xi,Y+N)	(xi,Y)

(x_i,y_i)= X- position and Y- Position of a node
N=network Size
(X,Y)= initial potition

B. Routing Strategy

At first, sink broadcasts its location information to every node in the network. Then each node will prepare its two sets of reference coordinates based on its position with respect to sink. This might be referred as the initialization phase. After that, the routing step will ensure packet to travel different paths at different times. Initially, on receiving the packet, node will generate random number between 0 and 1. This number is then compared with D_f. After the random number is compared with D_f, one of the reference set is selected. If the random number is greater than D_f than first set is selected otherwise second reference set is selected. Now, as each selected set has either nine or five reference coordinates the node randomly selects one of the reference coordinate from the selected set. Then from neighbor table, node with shortest in distance to selected reference coordinate is computed. At end, the packet is forwarded towards this node which is in shortest distance to selected reference coordinated. For instance, as shown in fig 5, if we take arbitrary value of random number to be 0.3 and D_f as 0.4, then second set with five reference coordinates will be selected. In this way, our proposed routing method will introduce random forwarding of packet for enhancing the source-location privacy in WSNs.

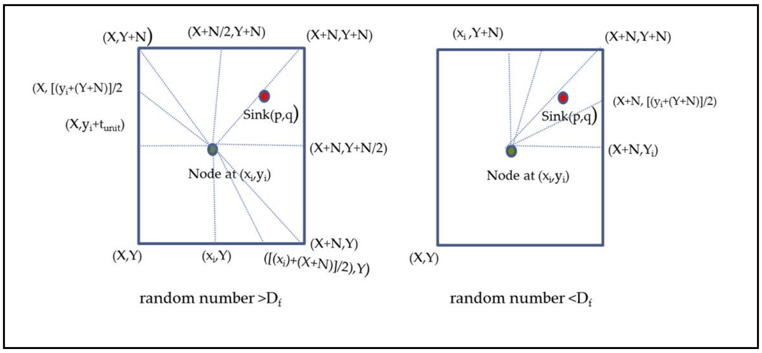


Figure 6. Reference coordinates of node (xi,yi) at left-down position when random number is compared with D_f

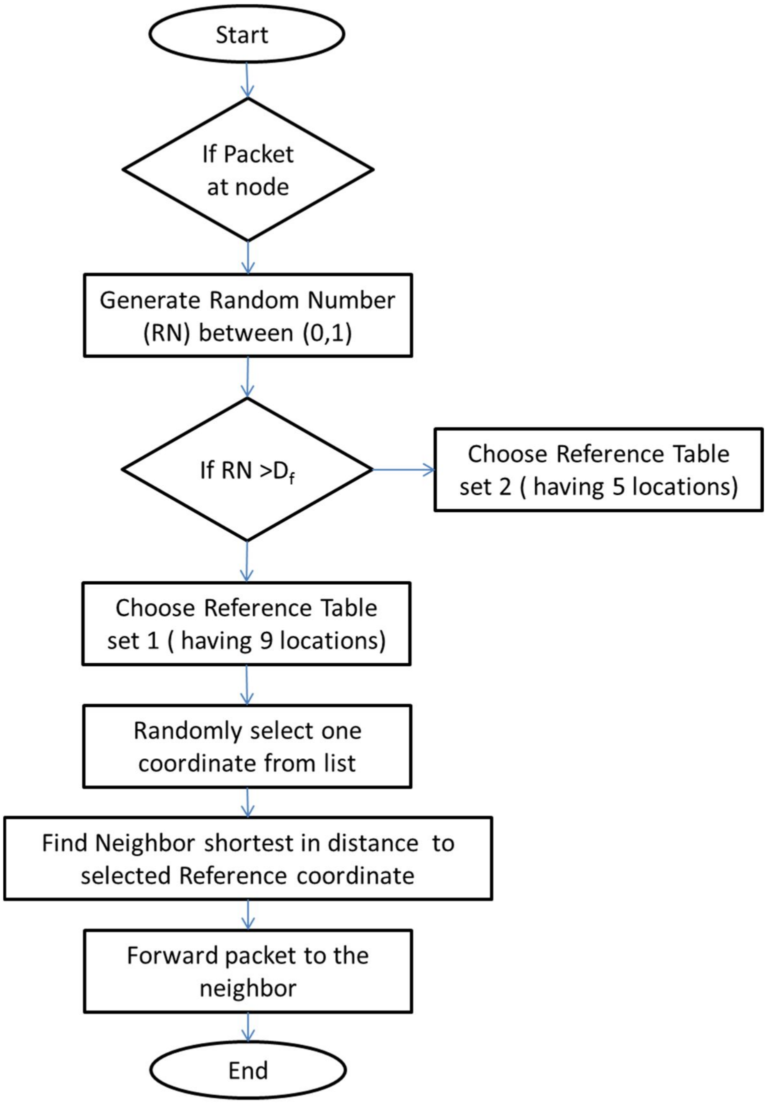

Start
If Packet at node
Generate Random Number (RN) between (0,1)
If RN >D_f
Choose Reference Table set 2 (having 5 locations)
Choose Reference Table set 1 (having 9 locations)
Randomly select one coordinate from list
Find Neighbor shortest in distance to selected Reference coordinate
Forward packet to the neighbor
End

Figure7. Flowchart showing directional random routing process

C. Adversary Strategy

An adversary is assumed to be residing in the vicinity of the sink.It is also assumed that it will have knowledge of routing strategy and is equipped with required wireless devices. The adversary is considered to have unlimited power and large amount of memory. Transmission range of an adversary is assumed to be same as that of a sensor node. Backtracking algorithm for the adversary given below is implemented.

Algorithm for An Adversary

```
Adversary_Location=Sink
While  (Adversary_Location != Source_Location)
    Listen_at (Adversary_Location);
   end
Listen_at(Adversary_location)
{
     If (message_arrived)
        Find immediate sender location;
        Adversary_Location= immediate sender location;
    End
 }
```

Figure 8. Algorithm for an Backtracking Adversary

IV. PERFROMANCE EVALUATION

This chapter is focused on the performance evaluation of the proposed routing strategy is evaluated via computer simulation and compared with the Phantom single-path routing and greedy random walk method.

A. Simulation Environment

To evaluate our proposed scheme, simulation has been carried out in MATLAB. For the network area of 50x50 meters, 200 nodes were deployed randomly. Communication between Source and Sink is via multiple sensor nodes in a multi hop fashion. The packets from the source are generated every second and the simulation is carried out for 100Sec with 50 numbers of iterations. For performance evaluation, whole network is divided into four quadrants and the position of sink is kept constant at first quadrant while the source is varied in all four quadrants. The value of D_f for our proposed method is varied from 0.2 to 0.9. Two different existing schemes were implemented in same simulation model discussed above and compared with our proposed method. We found that, for our proposed method the value of D_f greater than 0.6 ensures the delivery of packets at the sink and as D_f value 0.6 ensures higher privacy so we used this value for comparison. Similarly, for greedy routing we used different receptors values and using less number of receptors the packets tends to loop around the network. In our network conditions using 20 receptors all the packets were successfully delivered to the sink. So, this value was considered for comparison purpose. For phantom routing, as performance trends for privacy holds almost same for different variations of phantom routing methods, we implemented Phantom single path routing with directed walk (Dwalk) 20. This value was considered on the basis of scale of the network and performance between different Dwalk values.

The proposed method is compared using the performance matrices; Average delivery time, Average number of transmission, Success rate of adversary, Attack time for successful attack.

The network parameters used in the simulation are summarized in the Table 3.

Table 4. Simulation parameters.

Parameter	Value
Network Size (Meters)	50x50
Number of Nodes	200
Transmission Range	5
Packet rate	1 packet/sec
Simulation Time	100 sec
Number of Iteration	50
Directivity factor	0.6-0.9

B. Smulation Results and Discussion

1. Average delivery time

The average delivery time measures the delay for delivering a packet from source to sink. Phantom single path delivers the packet in very short period of time because the packets from phantom source use single path route and delivered quickly. The delay of greedy is higher compared with proposed method.

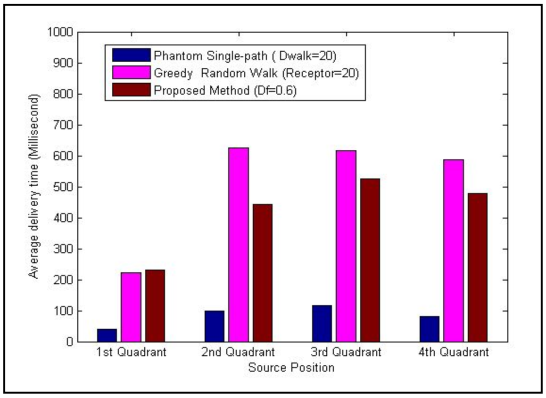


Figure 9. Average delivery time of proposed method, phantom single path routing and greedy routing

2. Average number of transmission

This metric measure the number of transmissions required to deliver a packet. It gives the number of hops the packet travel for reaching destination which is directly related with energy consumption of the network. The energy requirement of proposed scheme is very higher than other two schemes.

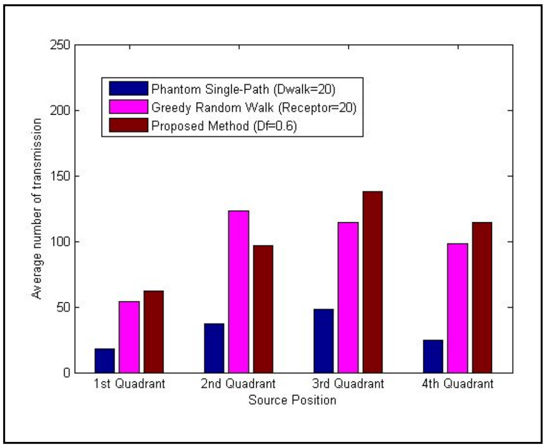


Figure 10. Average number of transmission of proposed method, phantom single path routing and greedy routing

3. Success rate of adversary

It measures the rate of source traceability. It is number of times successfully locating source in the simulation iterations. So, higher the success rate of an adversary we consider lower privacy the routing strategy provides. The phantom routing strategy seems to provide poor source location privacy in all sections of the network.

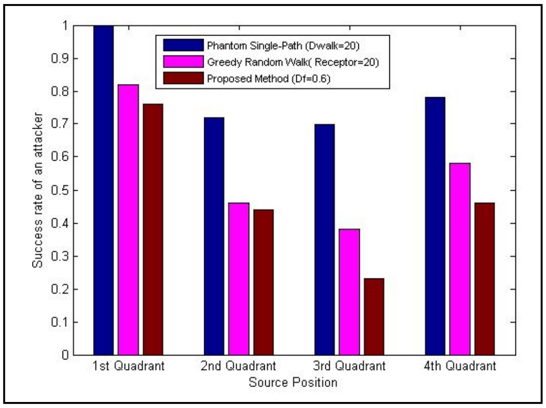


Figure 11. Success rate of proposed method, phantom single path routing and greedy routing

4. Attack time for successful attack

It mesures the time reqired for locating source when there is successful attack. The trace time for proposed scheme is higher when the source is located at second, third and fourth quadrant. As sink is kept constant at first quadrant, the time for locating source is considerably low for all three routing methods.

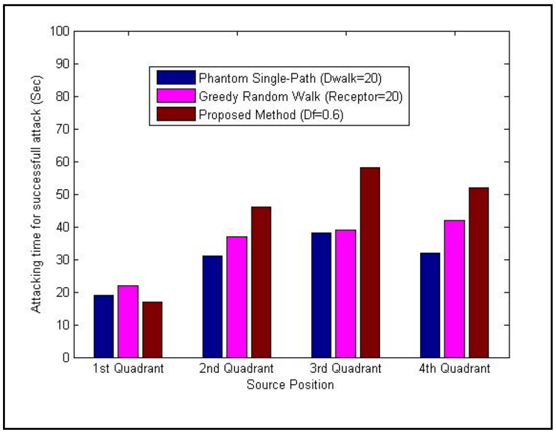


Figure 12. Attack time for successful attack of proposed method, phantom single path routing and greedy routing

V. CONCLUSION

In this thesis we highlighted several existing methods for preserving location privacy in sensor networks. From the study, it was found that uncertaiity in routing will make an attacker's task difficult in tracing the source. The exising methods for source location privacy could preserve the privacy but the trace back time was miimum. We proposed a source-location privacy preserving routing technique for WSNs. Using the two sets of reference coordinates the packets are randomly transmitted and ensured to be converged towards the sink. Also, we implemented the adversary which eavesdrop and back tracks packet in the sensor network. We evaluated the proposed method and compared it with phantom single-path routing and greedy random walk routing. From the simulation result energy consumption of phantom single-path routing was found less amongst all. However, we observed that, success rate of attacker for phantom single-path routing is quite high in all four quadrants of the network and our proposed routing method has lower success rate of attacker. Similarly, except the first quadrant attack time for successful attack for proposed method is higher with above 40 second at other three quadrants. Thus, the proposed method can provide better privacy than other two schemes. In the near future, powerful adversary modeling and stringent energy requirement will be considered for our proposed routing strategy.

APPENDIX

1. Performance of proposed Directional Random Routing

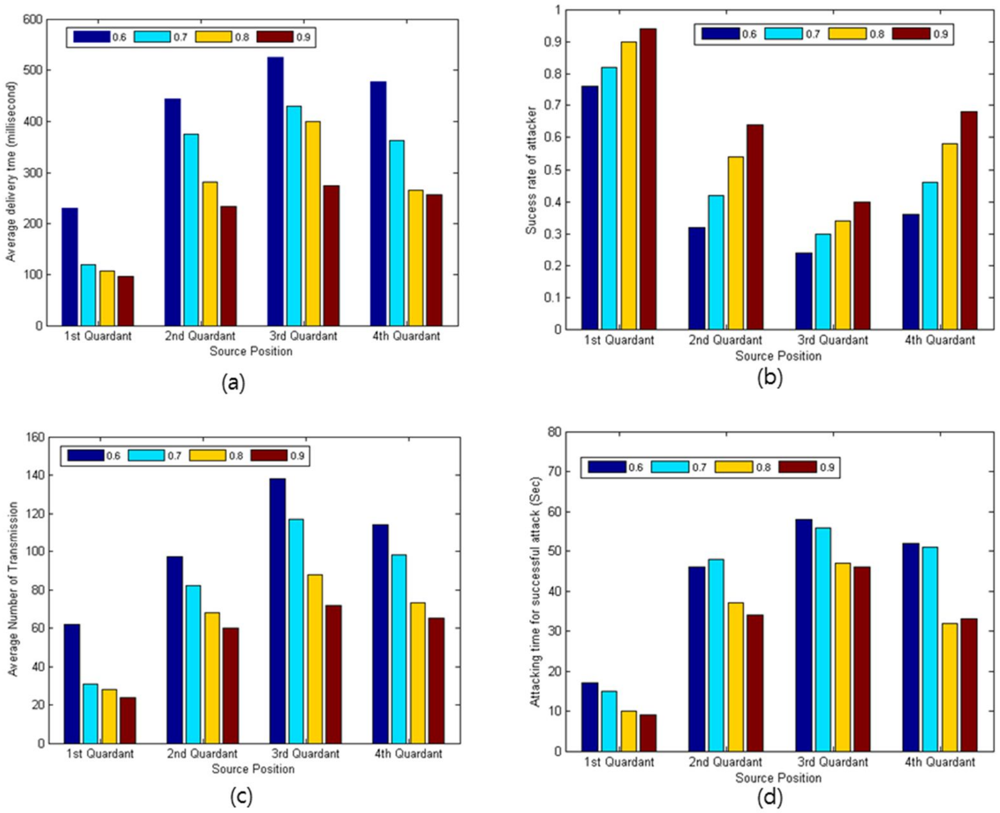
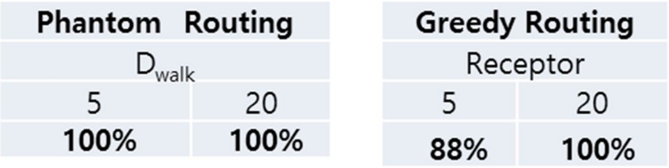


Figure 13. Performance of proposed random routing with different D_f values: (a) average delivery time; (b) Success rate of an attacker; (c) average number of transmission; (d) average time for successful attack

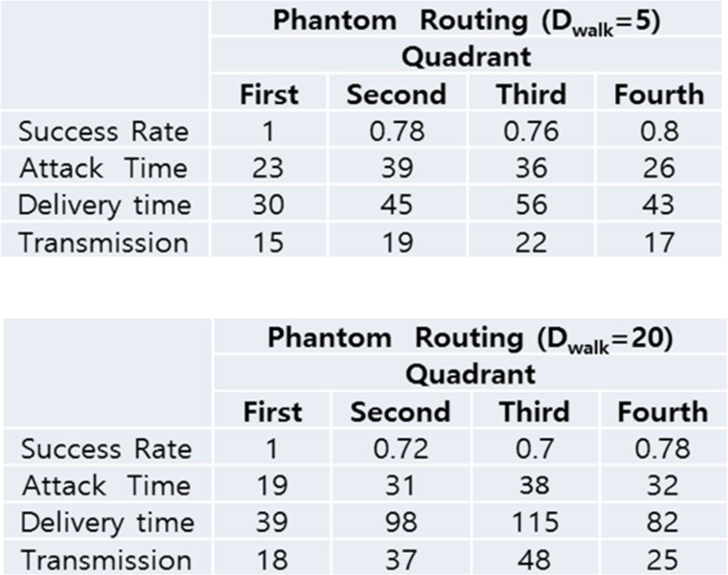
2. Total percentage of packet received at sink for two different schemes



Phantom Routing		Greedy Routing	
D_{walk}		Receptor	
5	20	5	20
100%	**100%**	**88%**	**100%**

Figure 14. Total packet received at sink with differernt D_{walk} and receptor value for phantom single path and greddy routing respectively

3. PerformancePhantom single-path

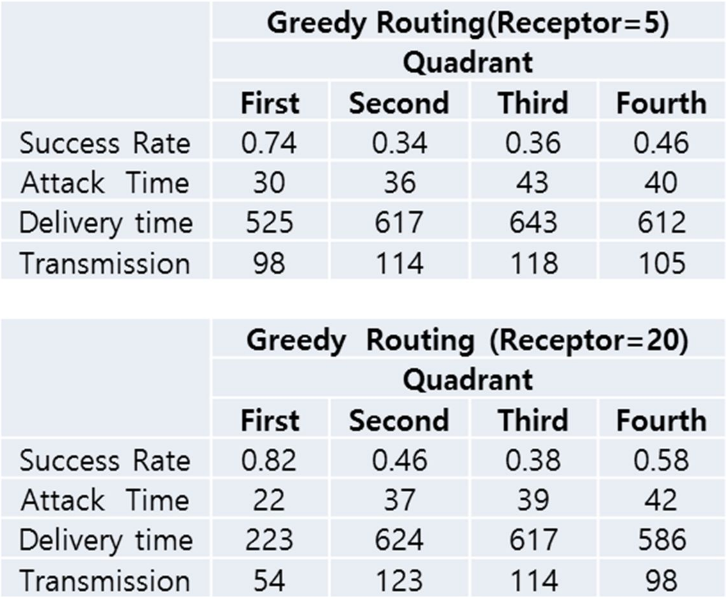


	Phantom Routing (D_{walk}=5)			
	Quadrant			
	First	Second	Third	Fourth
Success Rate	1	0.78	0.76	0.8
Attack Time	23	39	36	26
Delivery time	30	45	56	43
Transmission	15	19	22	17

	Phantom Routing (D_{walk}=20)			
	Quadrant			
	First	Second	Third	Fourth
Success Rate	1	0.72	0.7	0.78
Attack Time	19	31	38	32
Delivery time	39	98	115	82
Transmission	18	37	48	25

Figure 15. Performance of phantom single-path routing with different D_{walk} values

4. Performance of Greedy Routing



	Greedy Routing(Receptor=5)			
	Quadrant			
	First	Second	Third	Fourth
Success Rate	0.74	0.34	0.36	0.46
Attack Time	30	36	43	40
Delivery time	525	617	643	612
Transmission	98	114	118	105

	Greedy Routing (Receptor=20)			
	Quadrant			
	First	Second	Third	Fourth
Success Rate	0.82	0.46	0.38	0.58
Attack Time	22	37	39	42
Delivery time	223	624	617	586
Transmission	54	123	114	98

Figure 16. Performance of proposed greedy routing with different receptor values

BIBLIOGRAPHY

[1] Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol.38, no. 4, pp. 393-422, 2002.

[2] Ramesh, P. S., F. EMILY MANOZ PRIYA, and B. SANTHI. "Review on security protocols in wireless sensor networks," Journal of Theoretical and Applied Information Technology, vol. 38, no. 1, 2012.

[3] David L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Communication of the ACM, vol. 24, no. 2, pp. 84-90, 1981.

[4] Paul F. Syverson, Michael G. Reed, and David M. Goldschlag, "Onion routing access configurations," In DARPA Information Survivability Conference and Exposition, pp. 34–40, 2000.

[5] Roger Dingledine, Paul Syverson, and Nick Mathewson, "Tor: The second-generation onion route," In Proceedings of the 13th USENIX Security Symposium, 2004.

[6] Jing Deng, Richard Han, and Shivakant Mishra, " Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks," International Conference on Dependable Systems and Networks, pp. 637-646, 2004.

[7] Zaho Cheng, and Wendi B. Heinzelman. "Flooding strategy for target discovery in wireless networks," Wireless Networks, vol. 11, no..5, pp. 607-618, 2005.

[8] Pandurang Kamat, Yanyong Zhang, Wade Trappe, and Celal Ozturk, "Enhancing source-location privacy in sensor network routing," 25th IEEE International Conference on Distributed Computing Systems, pp. 599-608, 2005.

[9] Yingpei Zeng, Jiannong Cao, Shigeng Zhang, Shanqing Guo, and Li Xie, "Random-walk based approach to detect clone attacks in wireless sensor

networks," Selected Areas in Communications, vol. 28, no. 5, pp. 677-691, 2010.

[10] Yong Xi, Loren Schwiebert, and Weisong Shi, "Preserving source location privacy in monitoring-based wireless sensor networks," 20th International Parallel and Distributed Processing Symposium, 2006.

[11] Celal Ozturk, Yanyong Zhang, and Wade Trappe, "Source location privacy in energy-constrained sensor network routing," 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 88-93, 2004.

[12] Kiran Mehta, Donggang Liu, and Matthew Wright. "Location privacy in sensor networks against a global eavesdropper". In IEEE International Conference on Network Protocols, pp. 31-323, 2007.

[13] Jing Deng, Richard Han, and Shivakant Mishra, " Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks," Pervasive Mob. Computing, vol.2 no.2, pp. 159–186, 2006.

[14] Jing Deng, Richard Han, and Shivakant Mishra. "Countermeasures against traffic analysis attacks in wireless sensor networks," Security and Privacy for Emerging Areas in Communications Networks, 2005.

[15] Ying Jian, Shigang Chen, Zhang Zhang, and Liang Zhang, "Protecting receiver-location privacy in wireless sensor networks," 25th IEEE International Conference on Computer Communications, pp. 1955-1963, 2007.

ACKNOWLEDGEMENT

The two years of masters in Computer Engineering is on the brink of completion. It would not have been possible without the immense support of people from different avenue. First of all, I am thankful to my respected brother Dr.Subodh Pudasini for introducing me to WHYNET Lab. I will always be grateful for his advice and support since my childhood days. Simillarly, I would like to thank my advisor Profesor Shin Seokjoo for giving me the wonderful platform at chosun university. Under his guidance and support, I could learn different dimensions of research techniques. I will always be motivated by his immense capability in logiacal thinking. During my tenure at WHYNET Lab, his constructive comments were always helpful for carrying out the research works efficiently.

Along with him, I would like to thank Prof. Sangman Moh and Prof Moonsoo Kang for their expertise as a commite chairs to reviw my thesis and giving some valuable comments.

I would also like to remember the international Office of Chosun University which acted as a bridge during my initial days and ushered me to sweetly accommodate in the University environment. The refreshment cultural tour organized by them will always come in my mind. I would also like to thank The Graduate School and Department of Computer Engineering , Chosun University for letting me pursue my masters degree..

The friendly environment at Chosun University was amazing. I could make friends from different nation and culture. The list is long, I am indebt to all the senior brothers ans sisters from Nepal. Especially, I would like to remember my friends Kishor,Debesh,Sumeet.

Lastly, I want to thank my family members for their infinite love and affection.

Amod Pudasaini