February 2010

Master's Degree Thesis

Kerberos based Authentication for Inter-domain Roaming in Heterogeneous Wireless Network

Graduate School of Chosun University

Department of Information
and Communication Engineering

Anish Prasad Shrestha

February
2010

Master's Degree
Thesis

Kerberos based Authentication for Inter-domain
Roaming in Heterogeneous Wireless Network

Anish Prasad Shrestha

Kerberos based Authentication for Inter-domain Roaming in Heterogeneous Wireless Network

February 25, 2010

Graduate School of Chosun University

Department of Information
and Communication Engineering

Anish Prasad Shrestha

Kerberos based Authentication for Inter-domain Roaming in Heterogeneous Wireless Network

Advisor: Prof. Seung-Jo Han

This thesis is submitted to Chosun University in partial fulfillment of the requirements for a Master's degree

October 2009

Graduate School of Chosun University

Department of Information and Communication Engineering

Anish Prasad Shrestha

Anish Prasad Shrestha's
Master's Degree Thesis Approval

Committee Chairperson Prof. Jong-An Park (인)

Committee Member Prof. Seung-Jo Han (인)

Committee Member Prof. Jae-Young Pyun (인)

November 2009

Graduate School of Chosun University

Table of Contents

List of Figures

List of Tables

Acronyms

3GPP	3rd Generation Partnership Project
AAA	Authentication Authorization and Accounting
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AS	Authentication Server
AP	Access Point
Auth	Authenticator
BS	Base Station
CA	Certificate Authority
DES	Data Encryption Standard
EAP	Extensible Authentication Protocol
GSM	Global System for Mobile communications
HN	Home Network
KAIR	Kerberos based Authentication for Inter-domain Roaming
IMEI	International Mobile Equipment Identity
MAC	Media Access Control
MITM	Man in The Middle
MS	Mobile Station
NAI	Network Access Identifier
niAddr	Network Interface Address
PKI	Public Key Interface
RTT	Round Trip Time
SK	Session Key
SN	Serving Network
TKT	Ticket
TLS	Transport Layer Security
TTP	Trusted Third Party
UMTS	Universal Mobile Telecommunications System
VN	Visiting Network
WWAN	Wireless Wide Area Networks
WPAN	WirelessPersonal Area Networks
WLAN	Wireless Local Area Network

초 록

이종 무선네트워크에서 인터 도메인 로밍을 위한 Kerberos 기반의 인종

Anish Prasad Shrestha
지도 교수: 한 승 조
정보통신공학과
조선대학교 일반대학원

고속 무선 접근이 가지는 유비쿼터스의 강화된 수요는 다른 행정적 도메인에 의해 제공된 다른 무선 기술의 통합을 이끌었다. 모바일 장치가 무선 네트워크의 범위의 출입에 따라, 모바일은 인증될 필요가 있다. 연구는 주로 무선 네트워크의 인증으로 하였다. 기존 프로토콜은 모바일 노드의 인증을 위해 일반적으로 집중되며, 홈 네트워크는 각 인증 과정에 참여합니다. 그것은 홈 네트워크에서 다른 네트워크의 방문을 위한 지속적인 로밍을 위해 요구된다. 또한, RTT(Round Trip Time)결과는 매우 지연된다. 그런 문제를 해결하기 위해 로밍 인터 도메인을 지원하는 새로운 Kerberos 기반의 인증 프로토콜은 제안한다. 제안된 프로토콜은 Kerberos의 강한 특징을 사용한다. 모바일이 이전의 방문했던 네트워크의 로밍 파트너에게 접근을 할 수 있기 위해 토큰의` 발급을 포함한다. 제안한 프로토콜의 실행 환경과 표준 프로토콜와의 비교 분석은 제안한 방법의 우수성을 확인할 수 있게 한다.

ABSTRACT

Kerberos based Authentication for Inter-domain Roaming in Heterogeneous Wireless Network

Anish Prasad Shrestha
Advisor: Prof. Seung-Jo Han,
Department of Information and
Communications Engineering
Graduate School of Chosun University

An increased demand in ubiquitous high speed wireless access has led integration of different wireless technologies provided by different administrative domains creating truly a heterogeneous network. As a mobile device moves in and out of the coverage of one wireless network to another, it needs to be authenticated. The study mainly covers the authentication in wireless network. The existing protocols for authentication of a mobile node are typically centralized, where the home network participates in each authentication process. It requires home network to maintain roaming agreement with all other visiting networks. Moreover, the round trip time results high latency.

A Kerberos based new authentication protocol is presented in this thesis that supports inter-domain roaming to overcome such problems. The proposed protocol adopts the strong features of

Kerberos based on tickets for rigorous mutual authentication and session key establishment along with issuance of token so that the mobile station can have access to not only the roaming partner of home network, but also to the roaming partner of previous visited networks. The performance evaluation and comparative analysis of the proposed protocol is carried out with the already implemented standard protocols and most remarkable research works till date to confirm the solidity of the results presented.

Ⅰ. Introduction

A. Overview

Our perception of communication and network is changed with the evolution of the different wireless access technologies. In the past, it was mainly based on fixed wired access system making the device quite immobile. With the growth of various wireless access technologies and proliferation of mobile devices supporting internet access, it is possible for users to communicate or transfer data independent of their current location or their movement.

The existing wireless technologies can be categorized into three groups based on their coverage range: Wireless Wide Area Networks (WWAN), Wireless Local Area Network (WLAN), and Wireless Personal Area Networks (WPAN). WWAN includes wide coverage area technologies such as cellular networks like Global System for Mobile communications (GSM) and Universal Mobile Telecommunications System (UMTS). WLAN includes 802.11, Hiper LAN and several others. The coverage area of WLAN is normally 300 feet which is extended by using strategically placed wireless Access Points (AP) within a given facility. WPAN are short-range networks, utilizing Bluetooth or Infra-Red technology, and commonly used to

interconnect compatible devices near a central location [1]. A growing number of such wireless technologies and increasing number of wireless providers of different sizes have truly created a heterogeneous wireless network.

With the increased demand in ubiquitous high speed wireless access, the current trend is to integrate different but complementary wireless access technologies and make inter-operation among different administrative domains possible providing almost a global coverage envisioning all IP networks [2]. From a mobile user's perspective, it is highly desirable to have seamless connectivity allowing inter-operation of the different technologies and providers allowing universal access. Maintaining strong security becomes inevitable requirement while integrating different wireless networks. Although a significant effort has been made by the research community to develop defense techniques against security attacks, in the present context, we need security mechanisms that can exploit the basic network architecture of distributed heterogeneous networks.

B. Motivation

A mobile user is always driven by a quest for best service available in the region. For example, we can consider integration of

3rd Generation cellular network and WLAN. A mobile user with dual radio interface supporting both technologies can enjoy high bandwidth in WLAN network and switch to cellular network in absence of WLAN for universal roaming.

As heterogeneous wireless network will consist of wireless networks of multiple technologies operated by multiple service providers, a Mobile Station (MS) must be able to discover and select the best service provider at a given location. As it moves in space and time, it must be able to seamlessly roam from one network to the other in a secure manner, being always connected to the best network. However, in order to maintain security, the first and foremost step is to verify both the MS and the network by performing authentication process prior to any service delivery. Efficient authentication is the primary foundation which helps to achieve what are necessary elements in heterogeneous network security i.e. identification of MS allocation of specific services to MS; and holding them accountable for their actions or collectively known as Authentication Authorization and Accounting (AAA) [3].

For authentication between any two networks, the roaming agreement should exist between them. The work of this thesis is motivated by a vision of exploiting the roaming agreement that exists between the networks in distributed mesh form in a heterogeneous network so that the MS can choose the best service

at any location from multiple options of networks irrespective of their trust relation with the Home Network (HN) of the mobile station to which it is subscribed. The main advantage of such approach is performance because the authentication requires message deliveries no farther than the adjacent networks.

The main factors that restrict seamless global roaming in heterogeneous network are limited trust relationship with other administrative domains and excessive authentication latency. The limited trust relationship confines the mobility range of MS while excessive authentication latency may disrupt the on-going session. The work presented in this thesis focuses on developing an improved authentication approach that do not compromise the security level while overcoming such restrictions.

C. Research Approach and Contributions

A novel Kerberos based authentication protocol is designed suitable for distributed heterogeneous network. The Kerberos protocol is exploited for mutual authentication between the Mobile Station and the Visiting Network (VN) that shares roaming agreement with the MS's home network. The HN grants ticket to the MS and acts as Trusted Third Party (TTP), based on the trust relation it shares with VN and the MS itself. The ticket consists of

Session Key (SK)between the MS and VN as in Kerberos. After successful authentication, MS receives a token from the visited network with which it can roam to another foreign network that shares roaming agreement with previous visited network but not with its home network. The MS presents the token obtained from previous authentication to the roaming partner of previous visited network. However, this time the previous visited network acts as TTP instead of HN and issues the ticket consisting session key between MS and new visiting network. As such, HN is not required in the successive authentication process. As the proposed protocol adapts Kerberos protocol and offers inter-domain authentication for roaming MS, it is referred as Kerberos based Authentication for Inter-domain Roaming (KAIR).

The main contributions of the proposed protocol are summarized as follows

1. Firstly, it extends the mobility range of MS beyond the roaming partners of HN by using previous visited domain as TTP during authentication. As the ticket issuing authority can be shifted from one network to another constituting a chain formation, the mobility range is also extended simultaneously. This feature exploits the trust relationship that exists in basic network architecture of distributed heterogeneous networks.

2. Secondly, it reduces the latency by avoiding Round Trip Time (RTT) to HN in succeeding authentication process once it is successfully authenticated in presence of Home Network. As the HN is usually remote from the VN, the message transfer between two networks offers higher latency and hence, should be avoided if possible. This feature helps to provide seamless connectivity.

D. Thesis Organization

The content of this thesis is organized in modular chapters. Chapter 2 describes some important issues related with authentication and its properties. The major problems for authentication in wireless network are also explained in this chapter. In chapter 3, some of the already implemented standard wireless authentication protocols and other remarkable research works till date are discussed. The proposed KAIR protocol is presented in chapter 4. The following chapter is devoted to carry out comparative analysis and evaluation of KAIR. The last chapter concludes the thesis with wrapping text for the summary of carried research and possible future works.

Ⅱ. Background Preliminaries

A. Authentication

Authentication is the act of establishing or confirming something or someone as authentic, that is, claims made by or about the subject are true. This might involve confirming the identity of a person, tracing the origins of an artifact, ensuring that the artifact is what its labeling claims to be, or assuring that a computer program is a trusted one. In network security, authentication normally refers to entity (Device/Network) authentication and message authentication.

Entity authentication is the process whereby one party is assured of identity of second party involved in the process, and that the second has actually participated in it. Either one or both parties may corroborate their identities to each other, providing unilateral or mutual authentication. To conduct entity authentication, a test needs to be conducted of the claim that the device is properly distinguished by means of certain assigned credentials like password, digital certificates or smart cards.

Message authentication ensures and verifies the integrity of the data being communicated. Message authentication is required so that

the receiver of the message can be sure that the information included in the message has been produced by a legitimate source and has not been altered by other parties in transit. A Message Authentication Code (MAC) algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (also known as a message digest). At the other end of communication, a verifier possessing the secret key can detect any changes to the message content by performing the same MAC algorithm.

The research work presented in this thesis is mainly focused in entity authentication.

B. Desirable Properties of Authentication

1. Mutual Authentication

Conventionally for wired networks and even in some wireless networks like GSM, the authentication is unilateral. In such cases, only the client proves its identity to the network, and the authenticity of the network is not verified by the client assuming a trustworthy network. This assumption might be true for some cases, but it is questionable in a multi-access network. A malicious node can exploit the assumption of a trustworthy network by launching a Man in The Middle (MITM)attack in which a malicious node

intercepts and modifies the authentication messages and tricks a client into thinking that the malicious node is actually the legitimate network. Such MITM attack can be prevented if the client and the server both authenticate each other, which is known as mutual authentication. The client-server mutual authentication is a special case of a more generic concept of mutual authentication, where two parties are simply peers and each peer authenticates the other either sequentially or in parallel.

2. Identity Protection

A malicious node should not be able to determine the identity of an authenticating client by eavesdropping to the authentication message. Identity theft can ultimately lead to disclosure of user's location.

3. Resistance to Dictionary and Brute Force Attack

A dictionary attack consists of trying every word in the dictionary as a possible password for an encrypted message. Dictionary attacks are generally far less successful against systems that use pass phrases instead of passwords. Likewise, a brute force attack consists of trying every possible code, combination, or password until the right one is found. A dictionary attack is generally more efficient than a brute force attack, because users typically choose

poor passwords. A malicious node should not be able to decipher the encrypted data by a dictionary attack or perform a brute force attack within a reasonable amount of time.

4. Resistance to Replay Attacks

In a replay attack, a malicious node records the authentication message and plays it back at a later time. In doing so, the malicious node should be able to authenticate itself by simply replaying the previous messages.

5. Key Establishments

A good authentication system should include key establishment as well. Authentication without key establishment is typically not useful. The established keys can be used for encryption and decryption of further message exchanges between two authentication parties.

C. Authentication in Wireless Network

Ubiquitous use of wireless technologies in business and everyday life has introduced new security requirements and challenges. Wireless network not only involves the vulnerabilities that exist in a conventional wired network but also other threats due to

technology's underlying transmission medium, the airwave, which is open to all sorts of unwanted parties. Therefore, communication security solutions that were developed for wired networks in general are not suitable for wireless communications. For a strong security system, a good authentication mechanism is essential as it is the initial process to authorize any mobile terminal. Besides the desirable security properties of authentication mentioned in section II-B, we need to address other few issues required in wireless network.

With a wired network, a system administrator might determine who generated certain traffic based on the physical from which it arrived. By assuming that inbound traffic on a particular port is always coming from a certain source, there is no need to constantly verify where the traffic was coming from. However, with wireless networking, many users can access the network at the same AP or Base Station (BS) depending on technologies making it more difficult to map who did what. It is often desirable, therefore, to allow users to identify who they are before letting them through the BS onto the rest of the network. This prevents unauthorized usage while having the added bonus of being able to track a particular user's activity should the need arise. The major problems during authentication in wireless network are listed below:

- Communication in wireless network is much more vulnerable to

eavesdropping and intercepting attacks,

- Network bandwidth and latency vary greatly,
- Mobile devices often have lower configuration than desktop,
- Mobile devices often depend on limited battery power and computational capacity,
- Users are more frequent to join and leave systems,
- The great amount of number of users and services in the system lead the huge maintenance cost, and
- Mobile devices may be easily stolen and can reveal sensitive information stored within it.

In order to design an efficient wireless authentication mechanism, above enlisted issues must be properly addressed. A good authentication mechanism should involve simple encryption/decryption techniques in an efficient manner with secure key establishment technique. The designed mechanism should be able to precisely identify the wireless device along with the user of the device so that misuse of stolen devices can be avoided.

D. Mobility versus Authentication

In wireless network, mobility is associated with the ability of a user to access services from different locations and devices with

ongoing session without any interruption. Ubiquitous mobility is often expressed in terms of "anywhere, anytime, and any device" connectivity. Mobility is also a service; its realization requires additional support from both part of the network and the user. The use of wireless device raises mobility support requirements. Wireless does not mean mobile. A user can always move within a WiFi cell, but without mobility support he cannot move seamlessly to a neighboring cell [4]. Mobility introduces new technological and security challenges in designing authentication mechanism.

As mobile node moves in and out of coverage area of one network to another, handover process takes place. The mobile node should be able to continue a communication session started at the initial location after reconnecting to the new attachment point. To maintain security, we need to perform an authentication for each handover. The authentication can be categorized into two types i) intra-domain authentication and ii) inter-domain authentication. Handover executed between access networks managed by different authorities is referred to as inter-domain handover; otherwise the mobile node executes an intra-domain handover and is referred to as micro mobility as depicted in Figure 2.1 and 2.2.

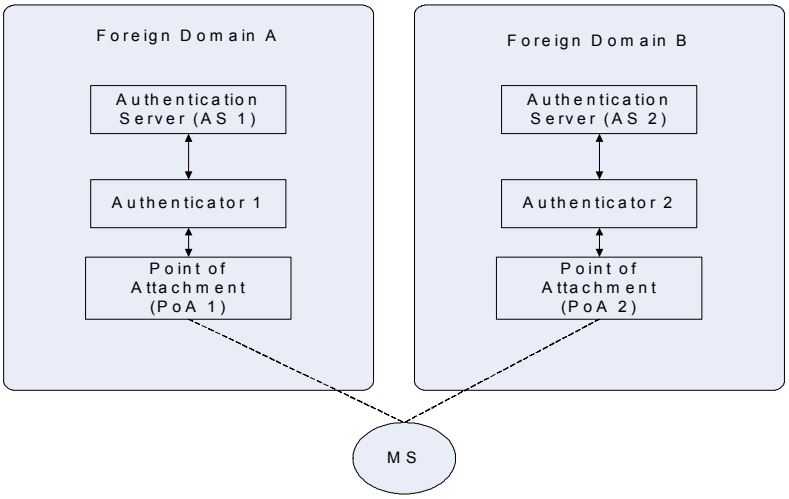

Figure 2.1 Inter-domain handoff

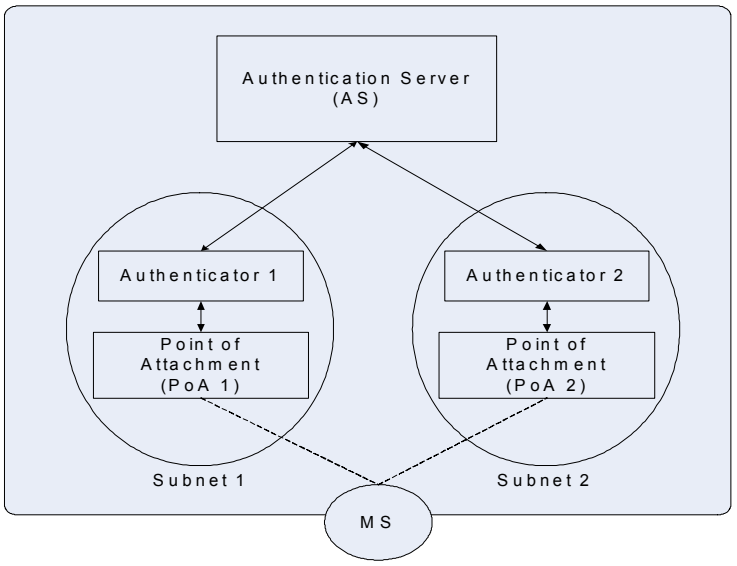

Figure 2.2 Intra-domain handoff

The design of inter-domain authentication is quite complex than intra-domain authentication. Inter-domain handover execution involves numerous entities that bring all threats associated with

them into a process. Many issues are raised by handover preparation and initiation phases. As handover may be both mobile initiated and network initiated, the risk of false handover should be addressed. When choosing a new network of attachment, a mobile node should be able to learn its capabilities and the security level provided.

Most of the existing protocols for inter-domain authentication are based on centralized scheme. For example, for roaming users in GSM, a challenge response mechanism is carried out between the MS and the Authentication Center (AuC) at its home network [5]. In such conventional approach, each time a Mobile Station hand-offs to another foreign network, the home-domain actively participates during authentication as shown in Figure 2.3.

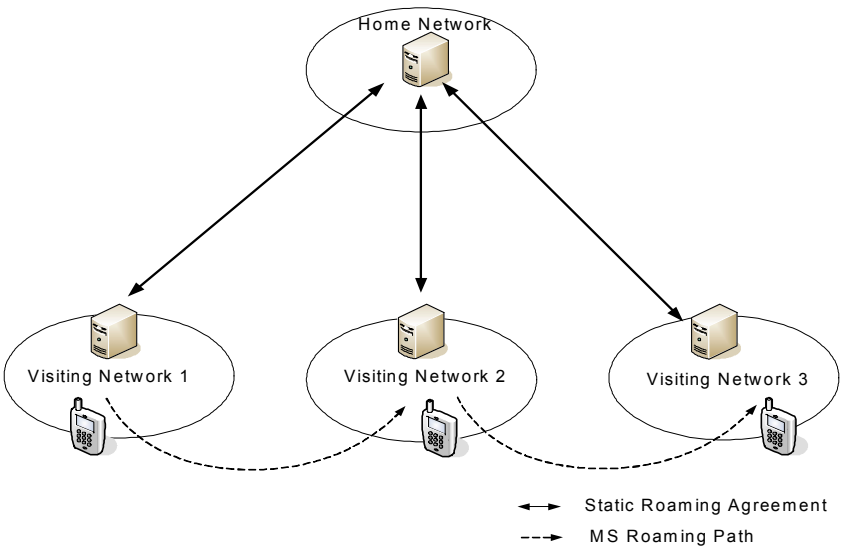

Figure 2.3 Centralized authentication scheme

For inter−domain authentication, a roaming agreement should exist between two administrative domains. The critical problem in centralized scheme is that for N numbers of administrative domain, we need to establish $\frac{N(N-1)}{2}$ roaming agreements amongst the networks. In a true heterogeneous network, there exist several administrative domains of different sizes each providing access to different wireless technologies. The total number of inter−domain roaming agreement to be established in such case would grow tremendously with the increase in number of administrative domains as shown in Figure 2.4. Therefore, maintaining roaming agreement with all the administrative domains is almost infeasible in practical scenario. Moreover, the home network is usually remotely located from visiting networks. As such contacting home network each time for authentication adds up authentication latency. Authentication latency can be typically subjected to computation delay and propagation delay. We do not refer scanning delay here. The RTT between the HN and VN present an overwhelming impact on propagation delay leading to high authentication latency.

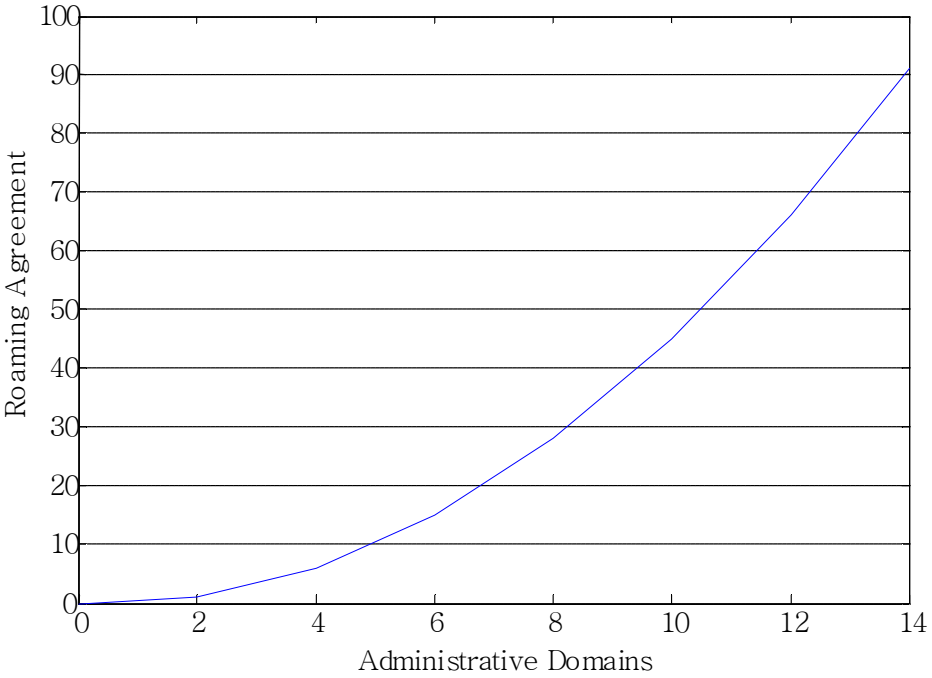

Figure 2.4 No. of Roaming agreements vs. administrative domains

Ⅲ. Related Works

A. Introduction

The authentication protocols developed for wireless network are certain technology specific or meant for a set of technologies (like integrated cellular network and 802.11). Due to emerging heterogeneous network, technology independent protocols are required to be addressed. In this section, we look at some of the already implemented standard protocols for technology specific wireless networks and the recently designed protocols for heterogeneous network.

B. Implemented Protocols

The Extensible Authentication Protocol (EAP) [6] that runs directly over data link layer, originally developed for the use with PPP, has also been applied subsequently to IEEE 802 wired networks, wireless networks such as IEEE 802.11i, IEEE 802.16e as well as IKEv2. EAP is used as encapsulation protocol for upper layer authentication information and allows for various authentication mechanisms so called, EAP methods. Out of more than 40 EAP

methods, we discuss only Transport Layer Security (TLS) [7] and Authentication and key agreement (AKA) protocols [8] to explain about Public Key Interface (PKI) based technology specific protocol and symmetric key based protocol for multiple technology integrated wireless networks like WLAN and UMTS as specified by 3rd Generation Partnership Project (3GPP)[9], respectively.

1. EAP-TLS

TLS, defined in RFC 2716, is considered to be cryptographically strong and promising as it has undergone extensive review. It is based on PKI and uses client and server-side certificates for authentication in 802.11. MS is subscribed to one particular HN, which stores all user related subscription data. HN and MS are both in possession of a public key certificate signed by a Certificate Authority (CA) trusted by both. We consider the roaming scenario for EAP-TLS as in [10, 11]. Upon roaming to a VN, that has a roaming agreement with MS's HN, VN and MS can authenticate each other using EAP-TLS based on the certificates of MS and HN.

Figure 3.1 gives an overview of the EAP-TLS protocol between MS, VN, and HN. VN proxies all EAP messages between MS and HN until the EAP authentication terminate. In case of successful authentication, HN transfers the master session key exchanged during the authentication to VN. From this key, MS and VN can

derive session keys to secure their subsequent communication.

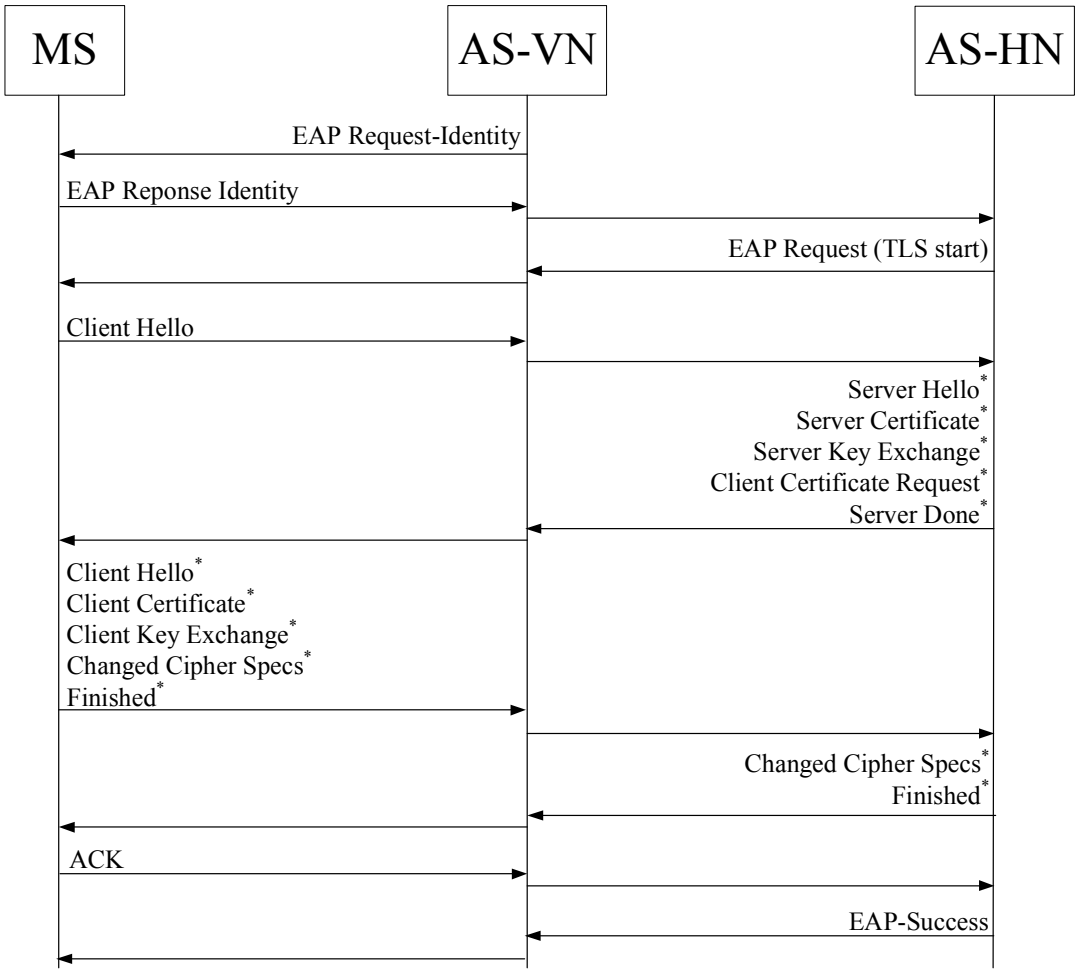

Figure 3.1 Message flow in TLS

The Wi-Fi Alliance has added EAP-TLS to Wi-Fi certified products. Therefore, the implementation of EAP-TLS is pervasive in WLAN world. To exploit the popularity and strong features of TLS, the variants of TLS protocol such as USIM based EAP-TLS [12],

advanced SSL/TLS based authentication [13] and many other protocols are proposed to support interworking of different wireless technologies. Since all of these protocols authenticate by means of digital certificates, they automatically inherit all certificate-related problems. For small devices, storing long digital certificates require higher memory. Similarly, the certificate should be issued by same CA or maintain a chain to the trusted root CA. Moreover, it lacks potential scalability in distributed heterogeneous environment and appears to be expensive as well, particularly for micro-transactions.

2. EAP-AKA

EAP-AKA is another EAP-method popular for interworking 3G-WLAN developed in the 3GPP by Ericsson and Nokia. It provides an opportunity to any application or protocol which can perform EAP authentication to perform UMTS authentication mechanism as well.

The AKA achieves authentication between the MS and the VLR and generates the key to encrypt messages and verify the integrity of messages. Figure 3.2 depicts the message exchange in the AKA. It is based upon symmetric keys and runs typically on a UMTS Subscriber Identity Module (USIM). It comprises of two phases:

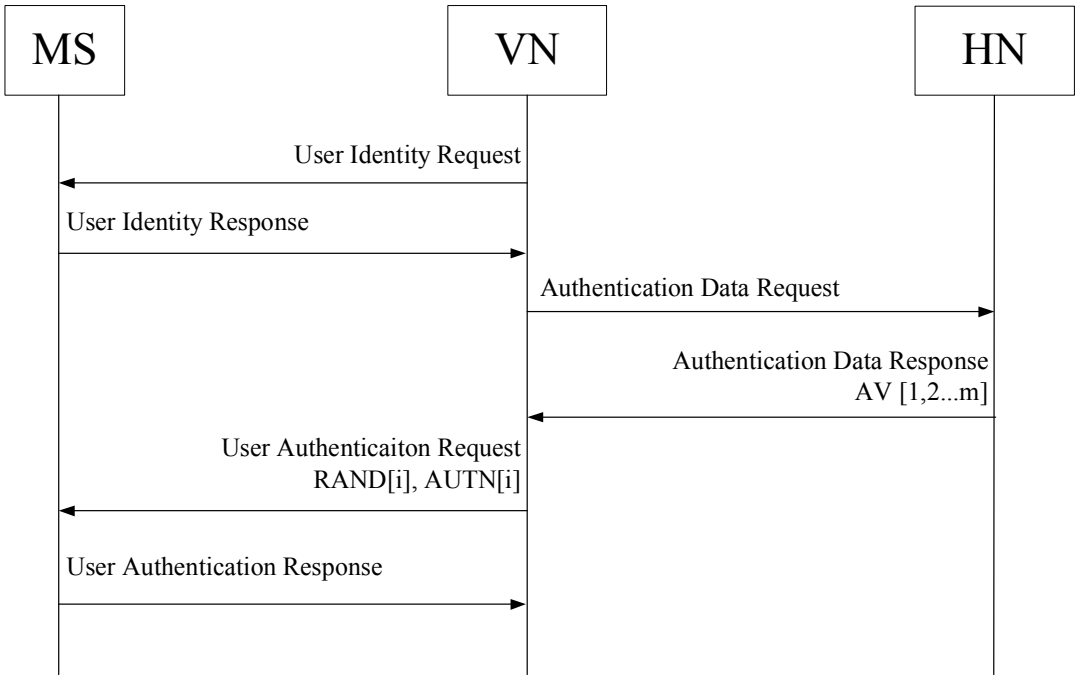

Figure 3.2 Message flow in AKA

a. Distribution of Authentication Vectors (AVs) set from the HN to Serving Network (SN): The elements of AV are calculated by a function of two components: K, a secret key shared between the MS and the HLR and second, a random number selected by the HLR. The AV consists of five components: RAND, XRES, CK, IK, and AUTN. XRES is the expected response from the MS in the sixth message, if the MS is a valid user. CK and IK are, respectively, the keys for the cipher and for message integrity. AUTN is authentication token.

b. Authentication and key agreement procedure between the MS and the SN:

The VLR selects one authentication vector (AV[i]) out of m AVs and sends RAND[i] and AUTN[i] to the MS. The MS generate XRES and CK, IK. First, the MS checks AUTN[i] and (SQN). The MS and the HLR retain the same sequence number (SQN) to prevent a replay attack on the AV. The sequence number is supposed to increase every time the AV is refreshed. The MS produces a response RES[i] and sends the response to the VLR. The VLR compares the received RES[i] with XRES[i]. If they match, the VLR considers the MS as valid, and authentication is successful. After successful authentication, the two keys, CK and IK are available to encrypt and authenticate messages of user data.

However, the AKA has been shown to have critical vulnerabilities such as a lack of vigorous mutual authentication that could lead to re-directive attack [14]. Moreover, performance consideration in resource-constrained environment of a mobile device is another serious concern.

C. Proactive Solutions

The proactive methods are normally used for intra-domain authentication. However, recently this approach is suggested for inter-domain authentication also. In proactive approach, the MS is authenticated to neighboring networks before handover takes place.

1. Shadow Registration

A shadow registration method is proposed in [15]. The concept is to establish the security association between MS and the Authentication Server (AS) in neighboring networks so that after hand off, the registration process is processed locally within that particular domain without contacting home network. As this method operates like the shadow as one walks, it is referred as shadow registration. However, the major backdrop of this approach lies in the fact that, for the pre-establishment of security association, HN needs to be contacted by local network to inform about neighboring network.

2. Media-Independent Pre-Authentication

A Media-Independent Pre-Authentication (MPA) is proposed in [16]. It is MS assisted pre-configuration and pre-authentication method that is executed to a target network before the actual

handoff. It can be used to enhance the performance of existing mobility protocols by proactively performing layer 3 and layer 4 associations and bindings before the actual handoff takes place, thereby saving time for these operations that usually only take place after the layer 2 association. It comprises of four procedures. The first procedure is referred to as pre-authentication, the second procedure is referred to as pre-configuration, the combination of the third and fourth procedures are referred to as secure proactive handover. It requires long time to discover and select multiple candidate networks to connect, and initiate pre-authentication and pre-configuration procedures with the candidate network. So, it is suitable only where an accurate prediction of movement can be made easily.

D. Ticket/Token based Solutions

The ticket/token based solution appears to be most feasible solution based on the distributed nature of heterogeneous network.

1. Proof Token

A proof token based authentication protocol is proposed in [17] which exploit the features of EAP-TLS. The MS carries with it a certificate issued by its home domain's CA and proof-tokens which

are similar to certificates, but are issued by previous visited domain's CA after successful authentications in that particular domain. It supports establishment of spontaneous roaming agreement between pair of domains that do not already have a direct roaming agreement. It differs from EAP-TLS in that instead of the MS presenting a fixed X.509 certificate issued by a root CA, it presents a proof token issued by a foreign domain it has recently visited and with which the current domain also has roaming relations with. Another differing point is that the AAA server carries with it a number of roaming-certificates instead of a single certificate issued by a root CA. To find out which proof token to use, the MS sends a list of all visited domain name. The AAA server chooses a common domain between MS's visited domain list and its roaming partner domain list, and sends the corresponding roaming-certificate. The rest of the message exchange is same as EAP-TLS. Although this mechanism seems promising, yet analysis needs to be carried out in terms of latency and efficiency as it involves asymmetric encryptions as in TLS.

2. Fast re-Authentication Protocol (FAP)

In [18], a Fast re-Authentication Protocol (FAP) is proposed for inter-domain roaming which eliminated the need of communication between the target and home network for credentials verification and

uses short living lightweight re-authentication ticket. It consists of two sub-protocols: ticket acquisition and fast re-authentication. The former is executed when the user is attached to the network and requires inter-domain communication, and the latter is executed during handover and localizes the authentication process in the target domain. However, to generate authentication tickets, the authentication server should have access to results of different authentication methods, which may have been used for the last authentication. Moreover, the MS needs to update the information about future possible roaming partners frequently as the lifetime is very short.

Ⅳ. KAIR: Kerberos based Authentication for Inter-Domain Roaming

A. Implemented Standards

The proposed solution KAIR is based on distributed scheme as shown in Figure 4.1 unlike centralized scheme explained in section II-D. Due to the distributed nature, KAIR can take advantage of dispersed uneven trust relationship that exists in heterogeneous network. It eliminates the participation of home network in every successive authentication process.

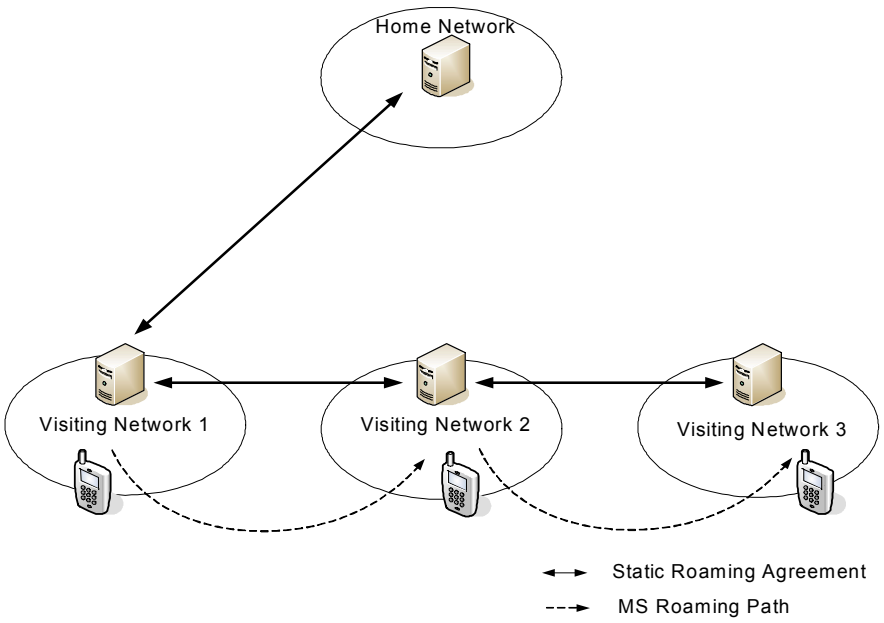

Figure 4.1 Distributed authentication scheme

The mobile network can authenticate itself in roaming partner network of previous visited network and roam seamlessly. The HN grants ticket to the MS and acts as TTP, based on the trust relation it shares with VN and the MS itself. The ticket consists of session key between the MS and VN as in Kerberos. After successful authentication, MS receives a token from the visited network with which it can roam to another foreign network that shares roaming agreement with previous visited network but not with its home network. The MS presents the token obtained from previous authentication to the roaming partner of previous visited network. However, this time the previous visited network acts as TTP instead of home network and issues the ticket consisting session key between MS and new visiting network.

B. Kerberos

Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography [19]. It was developed at the Massachusetts Institute of Technology as part of Project Athena in the mid-1980s and uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. Since Kerberos is a lightweight protocol based

on inexpensive symmetric key cryptography, it is more adaptable for small devices with low computational power.

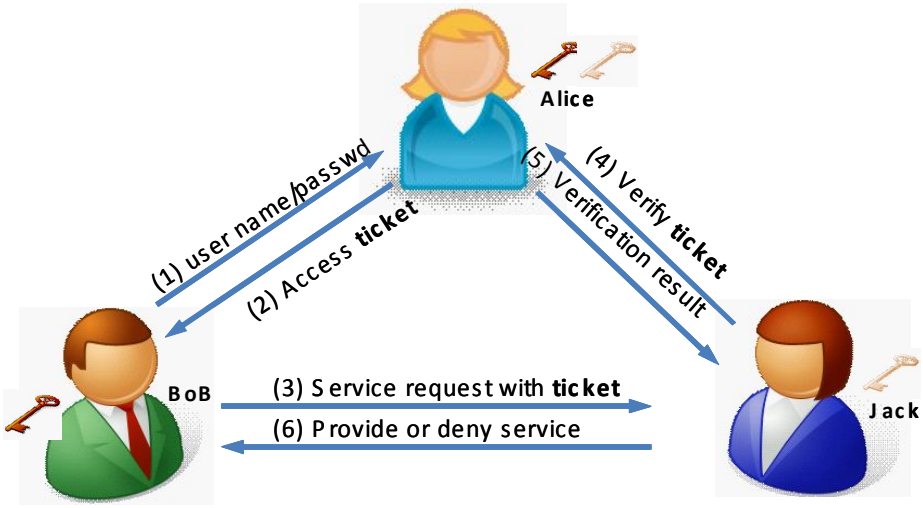

Figure 4.2 Kerberos operation

The basic idea of Kerberos can be explained based on Figure 4.2. Alice shares a unique secret key with both Bob and Jack. Bob sends its username and password to Alice. Alice verifies the password and grants a ticket to Bob. The ticket is encrypted by the secret key shared between Alice and Jack. Then, Bob presents the ticket to Jack to access service. Jack verifies the ticket with the secret key that is shares with Alice. After the verification of ticket, Jack provides the service to Bob. In summary, Alice acts as a TTP between Bob and Jack. Bob and Jack both do not share any trust relationship. Alice creates that trust relationship between them.

C. Assumptions

The few assumptions considered in the proposed protocol are described in this section.

1. The MS and its home network share a secret key K_m of 128 bits. This secret key is provided by HN at the time of subscription to MS. The MS can roam from one non-home network to another. To distinguish these visited networks, we will presume the one which MS visits at first and shares roaming agreement with the HN as the first visiting network (VN_1).
2. VN_1 and HN shares a secret key K_v of 128 bits. The secret key is established during the roaming agreement between the two networks. After successful authentication in VN_1, MS enters another visiting network close to VN_1 geographically. We call this network the second visiting network (VN_2). VN_2 shares roaming agreement with VN_1 but not with HN.
3. VN_1 and VN_2 shares secret key K_r, established during the roaming agreement between VN_1 and VN_2, which is also 128 bits. The roaming agreement should establish strong trust relationship between the domains.
4. MS initiates authentication in VN_1 and moves to VN_2, another wireless administrative domain, with ongoing session. We refer

the authentication in VN_1 as initial authentication and authentication in VN_2 as re-authentication.

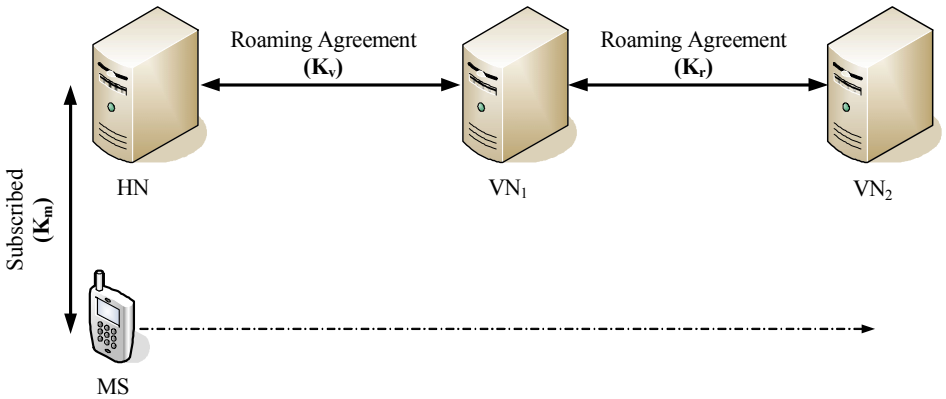

Figure 4.3 Assumed roaming scenario

D. Initial Authentication

During the initial authentication, MS is in VN_1, the roaming partner of HN. To perform mutual authentication between MS and VN_1, HN acts as TTP as shown in Figure 4.4. HN issues the ticket just like Kerberos server and assists in establishing session key between MS and VN_1. VN_1 grants a token to MS after the successful authentication for further authentication in other domains which are its roaming partner. The authentication comprises of seven steps as follow:

Step1: The presence of MS is perceived during scanning phase by the VN_1 within its coverage area and thereforth a request is sent for identification of the MS.

Step 2: The MS responds with its identity which is in NAI (Network Access Identifier) format of 72 bytes [20] indicating its home network to which it is subscribed for routing purposes.

Step 3: Upon receiving the address of the home network of MS, VN_1 sends the authentication request to the HN including the identity of MS.

Step 4: The HN confirms the identity of MS and if valid, responds back to MS with message (4−1)) comprising four parameters − a session key (SK_1), the identity of the visiting network (VN_1ID), a ticket (TKT) and its lifetime. The entire parameters are encrypted with secret key K_m. The ticket consists of session key between MS and VN_1, its lifetime, MS's network interface address (niAddr) and identity of MS, all encrypted by the secret key (K_v) shared between VN_1 and HN. niAddr could be International Mobile Equipment Identity(IMEI) for cellular phones or Media Access Control (MAC) address assigned to network interface cards for computers and so on depending on the devices.

$$E_{Km}\ \{SK_1||VN_1ID||TKT||lifetime\} \qquad (4\text{-}1)$$

$$TKT = E_{Kv}\ \{ID||SK_1||\ niAddr\ ||lifetime\} \qquad (4\text{-}2)$$

Step 5: As the fourth message is encrypted by the secret key K_m that is possessed by only MS and HN, VN_1 cannot decrypt it and simply relays the same message to the MS.

Step 6: The MS decrypts and retrieves the ticket TKT along with session key SK_1, VN_1ID, and lifetime. The MS checks the VN_1ID to confirm if the HN received the authentication request from the same VN as the MS has requested. The MS generates authenticator (Auth) as

$$Auth = E_{SK1}\ \{ID||\ niAddr\ ||nonce\} \qquad (4\text{-}3)$$

It then sends TKT and Auth to VN_1.

Step 7: The VN_1 decrypts the TKT with secret key K_v and retrieves the session key SK_1. It also decrypts Auth using SK_1 and recovers identity of MS and nonce. The Auth ensures that the ticket is being presented by the same client to whom it was issued. The recovered nonce is increased by unit value which is then again encrypted by

the same session key. VN_1 also generates a token to verify MS has been successfully authenticated. The incremented nonce and token are sent back to the MS.

The MS decrypts the message sent by the VN_1. After the verification of nonce, establishment of proper session key between them is realized.

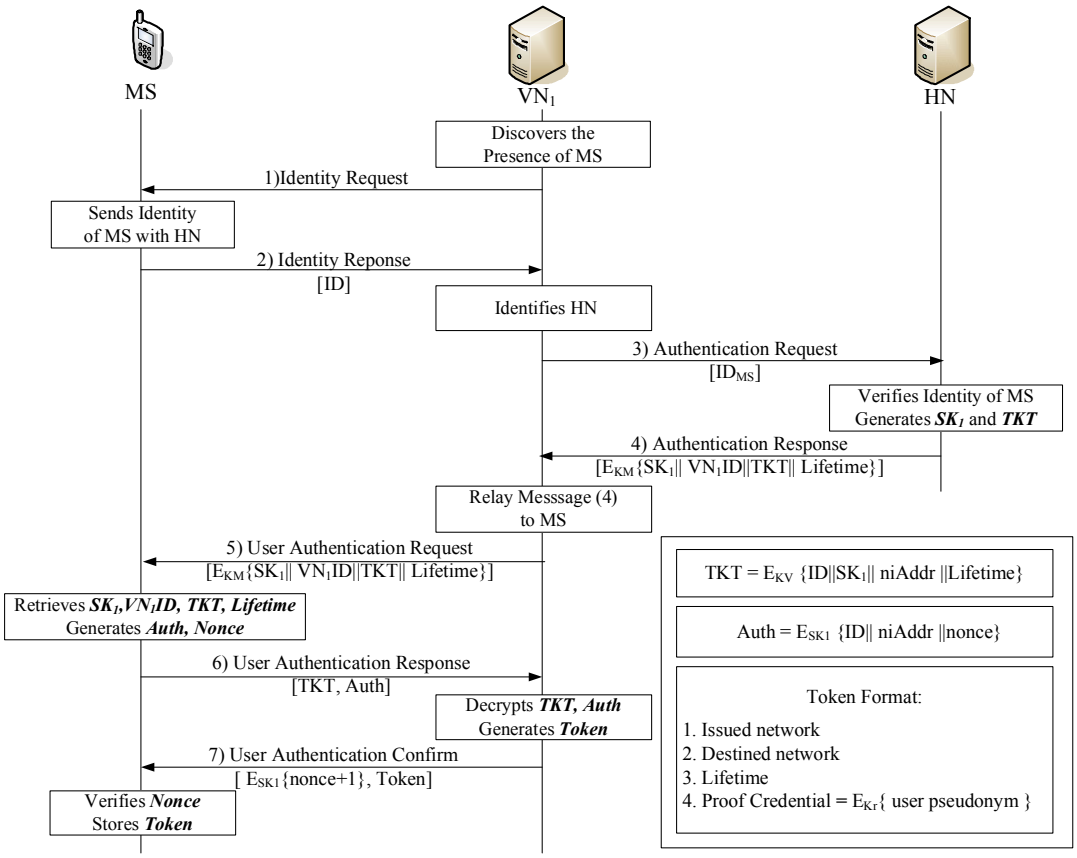

Figure 4.4 Initial authentication in VN_1

E. Token Format

The token issued by the first visiting network consists of:

1) Issued network: represents the name of the network which has provided the token (VN_1).
2) Destined network: represents the name of the roaming partner network (VN_2) of the token issuing network.
3) Lifetime: determines the end of the token validity period. The lifetime could be set from few hours to days as per our requirement.
4) Proof Credential: consists of anonymous identity (user pseudonym) provided by the token issuing network (VN_1) to the MS after successful authentication in its domain. The user pseudonym is encrypted by secret key K_r shared by issuing network and destined network.

$$\text{Proof Credential} = E_{Kr}\{\text{ user pseudonym }\} \qquad (4\text{-}4)$$

F. Re-authentication

When the MS enters VN_2, the roaming partner of VN_1 that shares no trust relations with the HN, VN_1 acts as TTP. The MS presents the token received from VN_1 to authenticate itself in VN_2. The

authentication takes place as shown in Figure 4.5.

Step 1: The identity of MS is requested by VN_2.

Step 2: MS passes on the token provided to it by the VN_1 from previous authentication process.

Step 3: The VN_2 validates the token and decrypts the proof credentials by using secret key K_r. It then sends authentication request by passing on user pseudonym to the VN_1 which it had assigned to the MS.

Step 4: The VN_1 verifies the user pseudonym and if valid, generates the ticket which consists of new session key (SK_2) between MS and VN_2 encrypted by secret key K_r. VN_1 also derives another key K_{MV} which we refer as extended roaming key. It is also of 128 bits long. This key is derived by pseudorandom function (PRF) from parameters including previous session key (SK_1); nonce and the MS's network interface address (niAddr).

$$K_{MV} = PRF\ [SK_1 \ ||\ nonce\ ||\ niAddr] \qquad (4\text{-}5)$$

The MS can derive the extended roaming key before authentication start to reduce authentication latency. VN_2 sends back ticket, session key, and lifetime along with the identity of new

visiting network (VN_2) encrypted by the extended roaming key K_{MV}. The rest of the steps (5, 6, and 7) continue as described in section III- B except that this time Auth comprises of parameters as shown in (4-6)

$$Auth = E_{SK2} \{proof\ credential \parallel niAddr \parallel nonce\} \qquad (4\text{-}6)$$

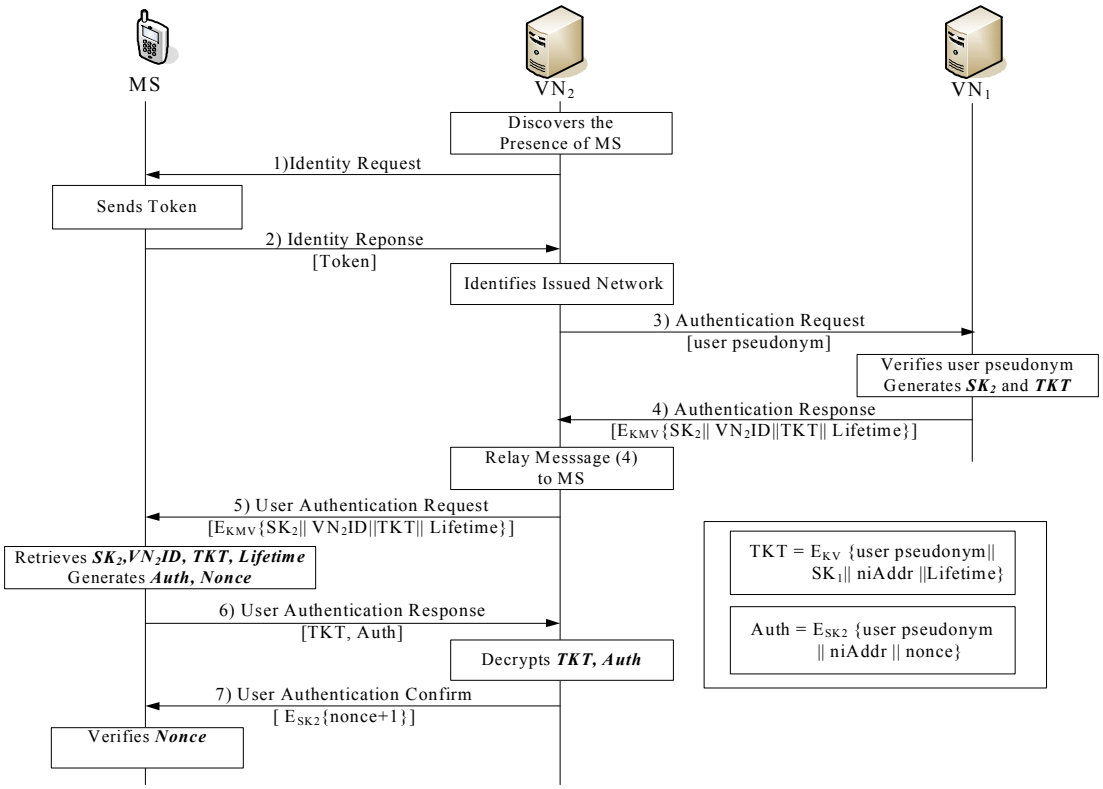

Figure 4.5 Re-authentication in VN_2

V. Analysis and Evaluation of KAIR

A. Security Analysis

1. Mutual Authentication

Since TTP is deployed during authentication, both the MS and visiting network are certain that they are communicating with their authentic counterparts. Based on the trust shared with TTP, the authenticating entities confirm that both of them share the same session key. The visiting network retrieves session key from TKT sent by MS. The TKT is encrypted by the secret shared key between VN and TTP which assures that the MS cannot modify it. This confirms that the MS is authentic. Similarly, the MS authenticates visiting network using nonce. The nonce is sent embedded within the authenticator and encrypted with the same session key. The VN would require the secret key shared with TTP to decrypt the TKT. The encryption of incremented nonce with the same session key ensures the VN also possesses the correct session key.

2. Key Derivation and Delivery

The key distribution among the authenticating entities can be

divided into the key derivation and key delivery schemes. KAIR protocol involves one key derivation scheme and one key delivery scheme. The session key is always generated by TTP and it is delivered to authenticating parties using secure encryption method based on key delivery scheme. This avoids the computational overhead to client and also reduces the resources required to derive the key. On the other hand, the extended roaming key K_{MV} is based on key derivation scheme. K_{MV} is derived mutually by TTP and the client using common one-way pseudorandom functions based on the parameters like earlier session key between them, nonce and niAddr. The key derivation scheme is used because it provides the opportunity for client to contribute in generating the secret key while it is in alien network that is not trusted by HN. The key itself is not required to be transmitted in the alien network.

3. Identity Protection

The original identity of the client is hidden in the new visiting network that does not share any roaming agreement with the home network of MS. To achieve this, user pseudonym is deployed which has no logical relationship with the original identity of the client. The client pseudonym is assigned by the first visited network that shares roaming agreement with HN, while issuing the token. The first visited network, however needs to keep the record of client

pseudonym in its database.

4. Man in the Middle Attack

An unwanted party could impersonate in the visiting network. The threat from such attack is avoided by assuring the identity of visited network provided by TTP in step 4 and 5. TTP sends the identity of visiting network encrypted by secret key shared between MS and TTP. Thus, MS can always compare the received identity of the VN with the one which it receives from beacon signal at scanning phase before it enters to the visiting network. If the two identities do not match each other, the client can be aware of illegitimate entities in the VN. Moreover, the MS can also validate the incremented nonce send by the VN. If somehow it differs from the one sent by the MS or does not receive any nonce at all, it can be aware of false party acting as an entity of visiting network.

5. Compromised Tickets and Tokens

If somehow a ticket or token is compromised, it is still difficult to counterfeit. In order to exploit the use of compromised ticket, one should present authenticator as well. To generate authenticator, niAddr and Identity of MS is required which are specific as per the device and the user of device. Similarly, for exploiting stolen token one should have knowledge of previous session key to derive secret

key K_{MV}. Without deriving the secret key K_{MV} one cannot decrypt the further message. Besides that, the token has its own lifetime for validity which limits the damage.

6. Brute Force Attack

In order to prevent brute-force attack, no authentication ticket should have a lifetime longer than the expected time required to crack the encryption of the ticket. However, we use 128-bits key Advanced Encryption Standard (AES) which would require years and years to crack even with the latest computing devices, unlike Data Encryption Standard (DES) in actual Kerberos. Hence, the KAIR is safe from brute force attack. We need to set the lifetime ticket only to avoid replay attack.

B. Comparative Analysis

In this section, The proposed protocol is analyzed with other protocols discussed in chapter III. These protocols are compared based on seven features as shown in Table 5-1. Besides MPA and Shadow registration, all the protocols are reactive i.e. authentication takes place after handoff. Although implementing proactive method in inter-domain method may be simple, but for inter-domain authentication it requires accurate predictive mechanism which could

be difficult to design. A pre-authentication in inter-domain requires sufficient time, thus prediction should be made properly about next visiting network. Encryption key is another important parameter as it affects in the computational load. The use of complex asymmetric key cryptography in TLS and Proof token methods results high computational load. AKA utilizes pre-shared key in USIM while the shadow registration and MPA does not specify whether to use public key or pre-shared secret key. The key choice is optional in FAP due to which the computational load is variable. KAIR involves symmetric encryption i.e. AES which simple but seure at the same time.

All the protocols support mutual authentication except the shadow registration. However, although AKA provides mutual authentication, it is still vulnerable to false base station attack. Similarly, the EAP-TLS is designed to support only WLAN technology where as the AKA supports integrated WLAN and cellular network. The rest of the protocols are designed purely for heterogeneous network. During the successive authentication in other visiting networks, TLS, AKA, MPA and shadow registration requires to contact HN resulting higher latency. KAIR, Proof-token and FAP uses token received from previous successful authentication in successive authentication.

To implement any kind of protocols, some kind of inter-domain trust is required. The MPA requires only the MS to have trust

relation with the network it is trying to connect; instead of the current network. In case of FAP, Proof-token and KAIR, the networks are required to have a trust relationship with neighboring adjacent networks. Whereas in case of AKA and shadow registration, HN should have direct trust relationship with the visiting networks. TLS is based on digital certificates. Thus, these certificates should be issued by same or should have chain to a trusted root CA. Overall, KAIR is satisfactory in terms of all the features enlisted in Table 5-1.

Table 5.1 Comparison of different authentication protocols

	Hand off	Encryption Key	Computational load	Mutual Authentication	Inter-Technology Roaming	Round Trip to HN in successive authentication	Inter-domain Trust required
TLS	Reactive	Public Key	Relatively High	Yes	No	Yes	Certificate based
AKA	Reactive	Secret Key	Low	Yes	Cellular/ WLAN	Yes	Full
FAP	Reactive	Any	Variable	Yes	Yes	No	Partial
Proof-Token	Reactive	Public key	High	Yes	Yes	No	Partial
MPA	Proactive	Not Defined	Not Defined	Yes	Yes	Yes	Not required
Shadow Registration	Proactive	Not defined	Not Defined	No	Yes	Yes	Full
KAIR	Reactive	Secret Key	Relatively Low	Yes	Yes	No	Partial

C. Performance Evaluation

The authentication process introduces overhead in communication and influences QOS metrics. Hence, it is necessary to maintain the authentication latency to minimum. The authentication latency of KAIR protocol is compared with already implemented standard protocols like the EAP-TLS and AKA. Since the rest of the protocols are still under research and exact specifications are unavailable to implement under designed testbed, they are limited to comparative analysis only.

1. Simulation Methodology and Testbed

Based on the specifications of each protocol, the number of messages sent and received by the MS, home network and visiting network are computed along with the length of each message in bytes. The computational speeds of cryptographic algorithms are obtained using a tool called Crypto++ [21]. The test is carried out running on the Intel Core 2.2.1 GHz processor under Windows XP SP1.

The protocols are implemented in OPNET simulator [22]. Four scenarios are designed each one for the implementation of TLS, AKA and KAIR (initial and re-authentication) protocols. The roaming scenario for TLS is set up similar as explained in [10, 11].

TLS is set up similar as explained in [10, 11]. Three networks are set up namely home_network, visiting_network_1 and visiting_network_2 as shown in Figure 5.1. 802.11b environment is set up in visiting_network_1 where as UMTS network is set up in visiting_network_2 as depicted in Fig. 7 and 8 respectively. The network configuration is shown in Figure 5.3 and 5.4 respectively. The home_network is set up geographically far from visiting_network_1 where as the roaming partner of visiting_network_1 i.e. visiting_network_2 is set up close to it. KAIR initial authentication occurs in visiting_network_1 and re-authentication in visiting_network_2. For KAIR, Advanced Encryption Standard (AES) is chosen for encryption and decryption. In KAIR, the length of session key, ticket and token is 16 bytes, 102 bytes and 222 bytes respectively. The lifetime and nonce length are 6 bytes and 8 bytes respectively.

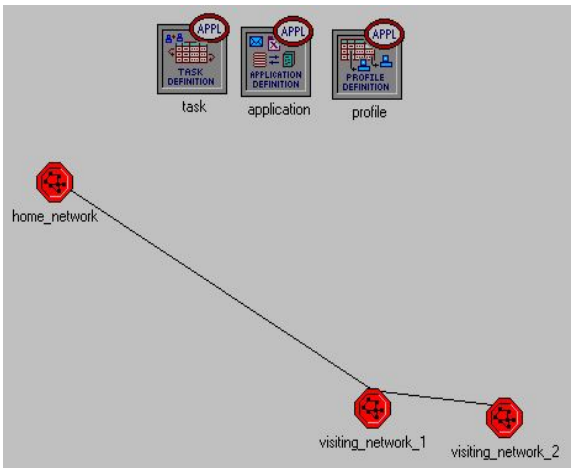

Figure 5.1 Simulation testbed

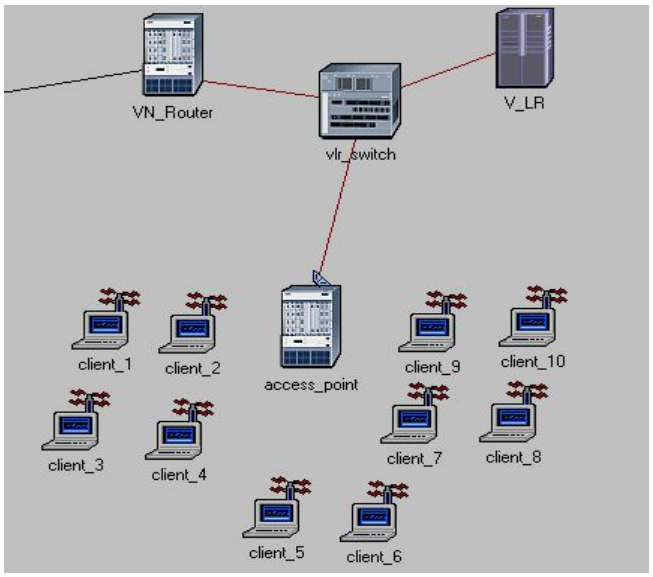

Figure 5.2 802.11b configuration

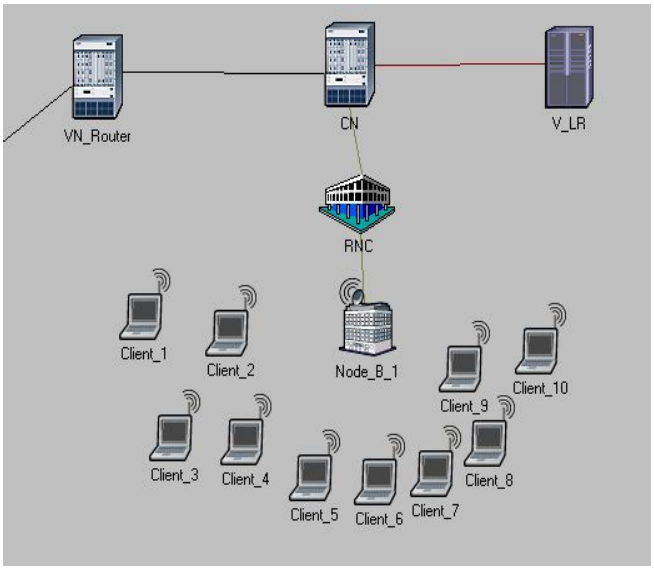

Figure 5.3 UMTS configuration

In the first experiment, the RTT between HN and VN is set around 200 ms. The RTT between visiting_network_1 and

visiting_network_2 is set around 20 ms. The number of MS in the VN is varied from 1 to 35 with interval of 5. As such, each scenario is simulated 8 times. The authentication delay for each MS

Table 5.2: Simulation parameters

Physical Characteristic	Direct Sequence
Transport protocol	UDP
Data rate	11 Mbps
Bandwidth	22 MHz
Transmit power	0.001 W
Short retry limit	7
Long retry limit	4

is recorded for all 8 simulations of each scenario. Then the average authentication is calculated. Likewise, in the second experiment, we set 20 MS in the network and the RTT is varied from 100 to 500ms with an interval of 50ms. As in the first experiment, multiple simulations for each scenario is run and average authentication delay is recorded.

2. Results

Experimental results show the authentication delay of standard authentication protocols and the proposed protocol. Figure 5.4

illustrates the average authentication latency for different number of MS. It can be seen that the latency provided by KAIR is least. During experiment, it was found that the round trip time between VN and HN has an overwhelming impact on the authentication delay compared to that of the latency caused by the necessary cryptographic computations. Since TLS involved multiple round trips to HN and involved complex cryptography and sharing of certificates with the mandatory chain to a trusted common root CA, it presented the highest delay. In case of AKA, the transmission of multiple sets of authentication vectors from HN to VN led relatively extra delay compared to the proposed protocol.

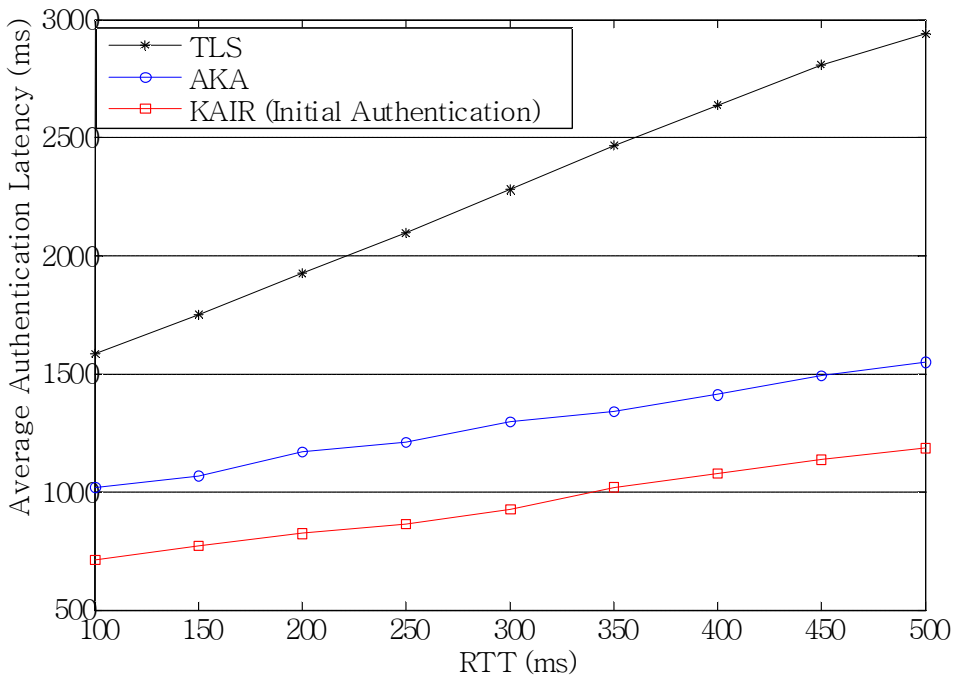

Figure 5.4 Average authentication latency vs. No. of MS

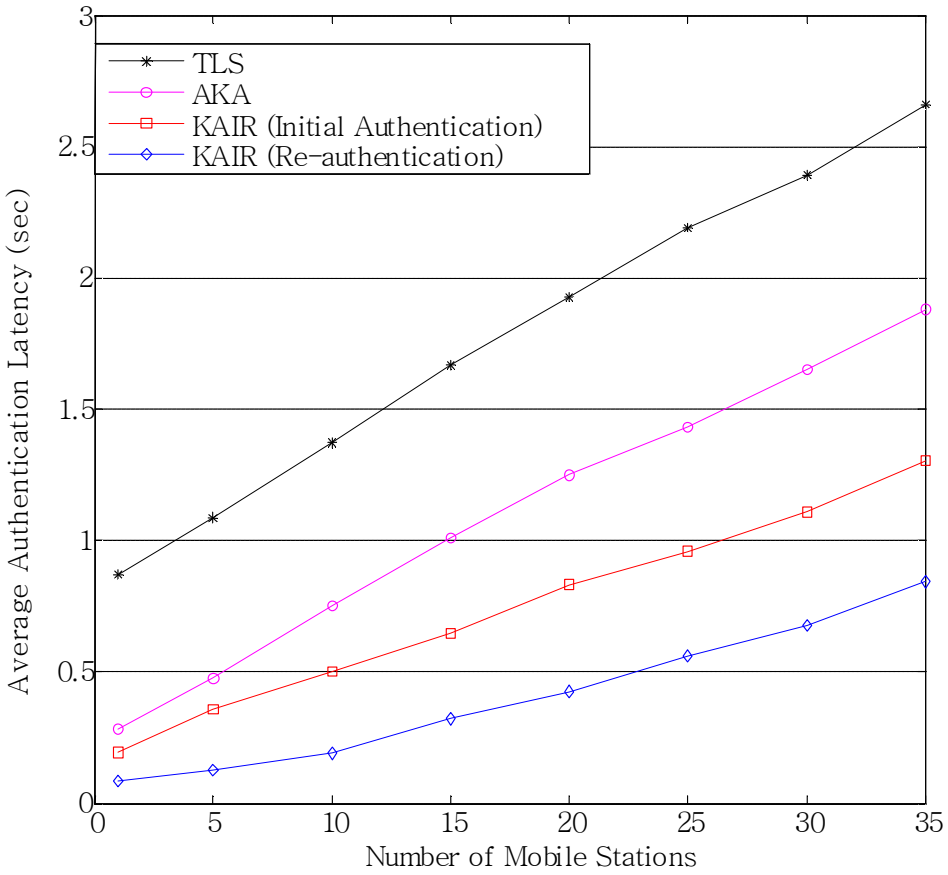

Figure 5.5 Average authentication latency vs. RTT

As the RTT between HN and VN was very critical in determining the latency, we check the average authentication latency in terms of RTT in Figure 5.5. Latency is drastically increased in TLS with increasing RTT where as it gradually increased in case of AKA and KAIR. On analyzing the results of two experiments, it can be seen that the average authentication delay for KAIR is least.

Ⅵ. Conclusion and Future Works

In conclusion, a TTP based authentication protocol is proposed based on Kerberos suitable for inter-domain roaming in distributed heterogeneous network. The use of token helps to improve the mobility range in wide heterogeneous network in a secure manner. The ticket issuing authority is achieved by a visiting network once the client and the visiting network mutually authenticate themselves in presence of home network's participation. The ticket issuance authority can be moved from one network to another constituting a chain formation. The main advantage of such approach is performance because the authentication requires message deliveries no farther than the adjacent networks. If a MS has tokens of few domains that it has visited recently, it can use the token provided by such domains to authenticate in most of the other domains it wants to visit. The simulation results and analysis demonstrate that our protocol is secure and offers lower latency.

The proposed solution does not include the authorization and accounting issues while roaming in foreign networks that do not share any roaming agreement with home network of MS. To solve such problems, policy based authorizing and billing can be used. Managing such policy completely lies in the hand of home network

and informs about the policy to its roaming partner. As such, the previous visited network grants token to the MS based on such policies only. In future, such policy based management will be focused to provide complete authentication, authorization and accounting.

References

1. W. Stallings, "Wireless Communications & Networks", Second edition, 2nd edition, Pearson Education International, 2005.
2. J. C. Chen and T. Zhang, "IP-Based Next-Generation Wireless Networks", John Wiley & Sons, Inc., Publication, 2004.
3. C. D. Laat, G. Gross, L. Gommans, J. Vollbrecht, and D. Spence, "Generic AAA Architecture" IETF RFC 2930, Aug. 2000.
4. A. R. Prasad and N. R. Prasad, "802.11 WLANs and IP Networking: Security, QOS, and Mobility", Artech House Publication, 2005.
5. H. Haverinen and J. Salowey, "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)," IETF Internet Draft, Apr. 2004.
6. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," IETF RFC 3748, Jun. 2004.
7. B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol", IETF RFC 2716, Oct. 1999.
8. J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", IETF RFC 4187, Jan. 2006.
9. <http://www.3gpp.org/>
10. J. Cordasco, U. Meyer, and S. Wetzel, "Implementation and Performance Evaluation of EAP-TLS-KS," in proc. Securecomm and Workshop, pp. 45-56, Aug. 2006.

11. B. Vaidya, Y. J. Kim, E. K. Kim, and S. J. Han, "Investigating Authentication Mechanism for Wireless Mobile Network," Springer LNCS 4159, pp. 902- 911, Sept. 2006.
12. Y. Tseng, "USIM-based EAP-TLS Authentication Protocol for Wireless Local Area Networks," Comput. Stand. Interfaces 31, pp. 128-136, Jan. 2009.
13. G. Kambourakis, A. Rouskas, G. Kormentzas, and S. Gritzalis, "Advanced SSL/TLS-based Authentication for Secure WLAN-3G Interworking," Communications, IEEE Proceedings, Vol. 151, Issue: 5, pp. 501- 506, Oct. 2004.
14. M. Zhang and Y. Fang, "Security Analysis and Enhancement of 3GPP Authentication and Key Agreement Protocol," IEEE Transactions on Wireless Communication,Vol.4, No.2, pp.734-742, Mar. 2005.
15. T. T. Kwon, M. Gerla, and S. Das, "Mobility Management for VOIP Service: Mobile IP vs. SIP," IEEE Wireless Communication Magazine, pp. 66-75, Oct. 2002.
16. A. Dutta, "A Framework of Media-Independent Pre-Authentication (MPA) for Interdomain Handover Optimization," IETF draft, draft-ohbamobopts-mpa-framework-05.txt, July 2007.
17. S. R. Tuladhar, C. E. Caicedo, and J. B. D. Joshi, "Inter-domain Authentication for Seamless Roaming in Heterogeneous Wireless Networks," in proc. IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, pp. 249-255, Jun. 2008.
18. M. Komarova, M. Riguidel, and A. Hecker, "Fast re-Authentication

Protocol for Inter-Domain Roaming," in proc. IEEE PIMRC'07, pp. 146-151, Sept. 2007.

19. J. Kohl and C. Neuman, "The Kerberos Network Authentication Service (V5)," IETF RFC 1510, Sept. 1993.
20. B. Aboba, M. Beadles, J. Arkko, and P. Eronen, The Network Access Identifier, IETF RFC 4282 Dec. 2005.
21. < http://www.cryptopp.com/>
22. < http://www.opnet.com/>

Acknowledgement

This thesis arose in part out of two years of coursework and research that has been done since I joined Computer Network and Information Security (CNIS) lab. It is a pleasure to convey my gratitude to all who contributed during the research and making of this theis in my humble acknowledgment.

In the first place, I would like to record my profound gratitude to my supervisor Prof. Seung-Jo Han, whose encouragement, personal guidance; invaluable support and useful suggestion from the initial to the final level enabled me to develop an understanding of the subject.

I heartily thank to committee members, Prof. Jong-An Park and Prof. Jae-Young Pyun for their detailed review, constructive criticism and excellent advice to overcome my doubts during the preparation of this thesis.

I gratefully acknowledge Dr. Binod Vaidya for his relentless support from the beginning of this research work. His creativity and dedication has triggered and nourished my intellectual maturity that I will benefit from, for a long time to come.

I also like to express my special thanks to Dr. Sang-Duck Lee, Rakesh Shrestha, Roja Kiran Basukala, Keong Yong Han, Jong-Yeop Sung, Kyu-Jin Park and all my lab mates for their support and

making my stay at Korea memorable.

I am as ever, especially indebted to my parents, my brothers Suchit, Kewal, Amit and sister Anna along with all the family members for their support throughout my life.

The financial support of IITA is greatly acknowledged.

저작물 이용 허락서

학 과	정보통신공학과	학 번	20087737	과 정	석사
성 명	한글: 애니쉬 프라사드 쉬레스타 영문: Anish Prasad Shrestha				
주 소	광주광역시 동구 서석동 조선대학교 전자정보공과대학 817호				
연락처	E-mail : anishpshrestha@yahoo.com				
논문 제목	한글 이종 무선네트워크에서 인터 도메인 로밍을 위한 Kerberos 기반의 인종 영문 Kerberos based Authentication for Inter-domain Roaming in Heterogeneous Wireless Network				

본인이 저작한 위의 저작물에 대하여 다음과 같은 조건 아래 조선대학교가 저작물을 이용할 수 있도록 허락하고 동의합니다.

- 다 음 -

1. 저작물의 DB구축 및 인터넷을 포함한 정보통신망에의 공개를 위한 저작물의 복제, 기억장치에의 저장, 전송 등을 허락함.
2. 위의 목적을 위하여 필요한 범위 내에서의 편집과 형식상의 변경을 허락함. 다만, 저작물의 내용변경은 금지함.
3. 배포·전송된 저작물의 영리적 목적을 위한 복제, 저장, 전송 등은 금지함.
4. 저작물에 대한 이용기간은 5년으로 하고, 기간종료 3개월 이내에 별도의 의사 표시가 없을 경우에는 저작물의 이용기간을 계속 연장함.
5. 해당 저작물의 저작권을 타인에게 양도하거나 출판을 허락을 하였을 경우에는 1개월 이내에 대학에 이를 통보함.
6. 조선대학교는 저작물 이용의 허락 이후 해당 저작물로 인하여 발생하는 타인에 의한 권리침해에 대하여 일체의 법적 책임을 지지 않음.
7. 소속 대학의 협정기관에 저작물의 제공 및 인터넷 등 정보통신망을 이용한 저작물의 전송·출력을 허락함.

동의여부 : 동의(○) 반대( )

2010년 2월 25일

저작자: Anish Prasad Shrestha (인)

조선대학교 총장 귀하