UNIVERSITY OF CINCINNATI

Date: 19-Aug-2009

I, Nidhi Rastogi **,**

hereby submit this original work as part of the requirements for the degree of:

Master of Science

in Computer Science

It is entitled:

A Novel Security Scheme during Vertical Handoff in Integrated Heterogeneous Wireless Networks

Student Signature: _____

This work and its defense approved by:

Committee Chair: *Qing An Zeng, PhD*

Ali Minai, PhD

George Purdy, PhD

A Novel Security Scheme during Vertical Handoff in Integrated Heterogeneous Wireless Networks

A thesis submitted to the

Graduate School of the University of Cincinnati

in partial fulfillment of the requirements for the degree of

Master of Science

Department of Computer Science

College of Engineering

University of Cincinnati

August 2009

by

Nidhi Rastogi

Bachelor of Information Technology

University of Delhi

July 2003

Committee Chair & Thesis Adviser: Dr. Qing-An Zeng

Abstract

In an integrated heterogeneous wireless network (IHWN), a user can connect itself to different types of networks on anytime, anywhere basis. Any of the following networks: cellular networks, WLANs, and ad hoc and sensor networks can constitute an IHWN network. The user is free to roam within networks seamlessly based on his needs and network availability. However, the security concerns associated with the IHWN count for some of the challenges involved in its implementation. These concerns combined with the different security requirements of various constituent wireless networks may have made security a serious issue. Seamless transfer of user's credentials is a major requirement when considering security during vertical handoff between two different types of networks. A security scheme that can fit all types of networks is difficult to propose. However, a reasonable architecture that keeps both security and user convenience into consideration can be designed. The existing security schemes fail to address mobility and scalability requirements. Considering the importance of these aspects in securing a global network, we propose a novel security scheme that uses two different security algorithms depending on the number of vertical handoffs made by the mobile node after the first authentication in the home network. It makes use of existing network elements, such as RADIUS and Diameter protocols and supports scalability, mobility, and secure key exchange. We also introduce a time

factor which is pre-set between the home network and foreign network. It delegates the task of authorizing subsequent requests from mobile node to connect to a different foreign network. Finally, we evaluate the efficiency and scalability of the scheme and prove its superiority over the existing schemes. The simulation results show a significant improvement over messages exchanged during key distribution at the time of vertical handoff. They also show how the scheme provides an excellent solution for delegated authentication. For a fair comparison, we also analyze the existing key distribution schemes and discuss their limitations in supporting the user security needs in current wireless networks.

Dedicated to my Family…

Acknowledgement

I take this opportunity to thank my adviser, Dr. Qing-An Zeng for his incessant support and direction without which this work could not have reached the quality it has now. I am fortunate to have worked under his guidance and develop a research-oriented aptitude that helped me reach technical depths. His availability and honest criticism and nothing less than perfect attitude made me follow a rigorous, yet honest research path. I shall always be indebted to him for helping me grow a sound technical background.

I am thankful to my committee members, Dr. George Purdy and Dr. Ali Minai, for their cooperation.

I am also proud and thankful to the ISSO, University of Cincinnati for their dedication towards helping international students.

I thank my parents, and the true pillar of my strength, my husband, Kanishk Rastogi for his never dying support, motivation and belief in me and also for proof-reading this work.

TABLE OF CONTENTS

List of Figures

List of Tables

1 Introduction

Telecommunications industry has seen exponential growth in the past two decades. Mobile technology has evolved from analog systems in the first generation (1G) to digital systems in the second generation (2G) [17]. The third generation (3G), however, makes use of improved spectral efficiency achieving increased bandwidth and can support mobile multimedia applications [25]. Another set of standards called the IEEE 802.11[56] family carries out the wireless local area network (WLAN) implementation. It covers small areas but provides higher bandwidth. The different types of networks mentioned till this point belong to the infrastructure category. Ad-hoc networks, on the other hand, are self-configuring networks where mobile nodes connect to each other through wireless links. Integrated heterogeneous wireless networks essentially integrate the features of different types of networks [28] and support the complementary characteristics, such as, speed and coverage of its constituent networks like WLAN and cellular.

On the other side, handheld devices have experienced an explosive growth in recent times, with the initial philosophy behind their usage having been changed drastically. Mobile device use is no more limited to making calls and exchanging text. Now, they can also be used for gaming, internet surfing including online banking, and shopping. The users of these devices desire to

use an optimum radio interface available at all times. The nature of underlying supporting network for these scenarios is envisioned to provide ubiquitous high data rate services to users. It is diverse and can comprise the IEEE 802.11 [56]-based WLANs and cellular networks following 3GPP/3GPP2 standards [26]. Security in these integrated heterogeneous wireless systems is a entirely different undertaking from the security of its individual components accounting to the variegated nature of security protocols and access technologies deployed by them. Hence, we are struggling to find one that is appropriate for use by a mobile node for seamless and secure inter-network mobility. The unique yet overlapping attributes of the component networks of the integrated heterogeneous wireless networks pose interesting challenges in the area of security.

1.1 Motivation

The focus of our research is to propose a security scheme for integrated heterogeneous wireless networks (IHWN) comprising WLANs and cellular networks. By definition, in an IHWN, a mobile node can connect itself to different wireless networks providing varying coverage and QoS and co-operating with each other to provide an “always on and everywhere” service. This is feasible if the mobile node is equipped with the appropriate network interfaces [20]. However, it’s a challenge to propose a security scheme for users switching between WLAN and cellular networks with completely different security mechanisms. A major requirement when defining a suitable security

scheme is to be able to implement it seamlessly in the least possible time. By this, we mean that a user transfers its credentials between two different networks during vertical handoff without a glitch and using least number of messages exchanged for authentication as the user moves from one location to another [17].

Technically, WLAN-3G internetworking is supported by the 3GPP specifications [1]. Since cellular networks support GPRS (General Packet Radio Service) [27] and WLAN is IP based, inter-roaming is possible [24]. In the heterogeneous wireless network under consideration, a user with its cellular network as the home operator can roam in WLAN networks with which the mobile service providers have pre-established roaming agreements. The reverse is also true.

Several attempts have been made towards finding an ultimate security solution but they have worked only for a certain network type and up to a limited network scale. According to our analysis of the existing schemes [2]-[7], we are still awaiting a standard state transfer protocol that can facilitate vertical handoff during inter-network roaming and fast security-context transfer in a secure, time-limited way. Some of the existing authentication protocols [2], [3] assume that a trust relationship already exists between the new foreign agent and the previous one. Some [30], [31] also follow a fast authentication mechanism but let the mobile node access only limited resources. Methods like Group Key Agreement (GKA) Protocols in [4], [5], establish a cryptographic key

for a group of nodes in a network. The key is derived from secret-key contributions from each member of the group. In essence, participating group members provide a portion of the final group-key as their contribution. Hence with each addition or removal of a node, a new key is derived and is redistributed by a chosen leader. They are convenient for mobile devices as it supports connectivity with mobility [7]. But they address mainly energy consumption and not the security strength of the group key agreement protocol. Time needed to authenticate a roaming mobile node has not been given its due consideration and research focus. It can be a decisive factor considering the present mobility trends and the huge delay a security algorithm can cause during vertical handoff.

Hence, we need a security solution that can cater to the needs of a mobile node that needs to quickly authenticate itself to networks despite the distance from the home agent or the network it gets connected to. The features of this security architecture should include:

(a) A mutual network-device authentication – both network and supplicant authenticate each other.

(b) A fast, yet secure, authentication mechanism in roaming scenarios – a security scheme that is time considerate without compromising the security of involved parties.

(c) Backward and forward secrecy – contiguous subset of group keys cannot discover preceding or succeeding group keys.

1.2 Our Scheme

In this research, we put forward a novel scheme for secure, seamless and fast mobile node authentication in an integrated heterogeneous wireless network of cellular and WLAN during vertical handoff. Our proposal uses two established and extensively used security algorithms. Extensible Authentication Protocol – Shared Key Exchange (EAP-SKE) [6] and Identity Based Encryption (IBE) [3]. EAP-SKE [6] is used when the mobile node undergoes the first vertical handoff between a cellular and WLAN (or vice-versa) to offer an uninterrupted service with secure and seamless mobility [6]. In this EAP-method, the mobile node uses the same master key as inputs to the EAP [22] and SKE algorithms [6]. However, using IBE [3] for authentications with the successive foreign networks proves less costly in terms of messages exchanged between the network and the supplicant. IBE [3], like EAP-SKE [6], also uses the same master key to generate several session keys for intended recipients. The biggest advantage of using IBE [29] is its ability to simplify the complex public key and certificate management and eliminating any pre-distribution of public-private keys. This is very helpful for a mobile node which is constantly moving away from the home network and needs quick authentication every time it wants to utilize the resources of a foreign network. Requesting for private information from the home agent can get costly each time a user authenticates itself to the foreign agent. IBE

[3] takes advantage of a previous successful session and makes use of the same master key. The amount of time a mobile node shall

1.3 Our Contributions

The main contributions made through this thesis are:

- Identify existing security mechanisms for heterogeneous wireless networks, their shortcomings and limitations. This validates the driving idea behind our research that security becomes weak and slow and expensive when users are mobile and use the same authentication mechanism to connect themselves in every network.
- Propose a new security scheme which addresses the issues not covered by any of the earlier schemes. Our scheme allows a mobile node to travel among different types of networks - WLANs and cellular networks, while securely transferring credentials from one network to another but faster than any of the previous cases [2]-[7], [30], [31]. It makes use of two different algorithms and uses them according to the number of vertical handoffs that the mobile node makes after the initial authentication in the home network. It is advantageous for the node as it need not request for full authentication parameters from the home agent to gain access to resources in the foreign network.

1.4 Thesis Organization

The thesis is organized as follows:

Work related to IHWN security and challenges faced in this field is discussed in Chapter 2. The subsections define relevant cryptographic algorithms and its various types. In Chapter 3, we propose our security scheme and also describe in detail the security protocols it has used. We then present our analysis and simulation results in Chapter 4 followed by a summary of work and future work possible using our scheme in the subsequent Chapter 5.

2 Security Challenges in IHWN

The basic requirements for security in IHWN are similar to the requirements of a homogeneous network, i.e., confidentiality, integrity and non-repudiation. However, the different levels of trust in IHWN necessitate a dissimilar treatment for securing the network and the mobile nodes. In the following section, we present, in detail, the challenges faced in securing an IHWN.

2.1 Security threats in IHWN

An IHWN consists of a variety of mobile nodes and wireless networks. The mobile nodes may belong to either of the following categories: handheld devices, powerful computers, laptops, PDA's, and other wireless modules which attempt to access the wireless infrastructure. The presence of this wide variety of devices and the lack of interoperability of security parameters between access technologies poses a potential security hole [32]. Therefore, efficient security measures need to be implemented in order to avoid risking the stakeholders, most importantly the backbone network. Seamless mobility also introduces time constraints on the vertical handover because a security context transfer includes transferring cryptographic keys, information on algorithms utilized, and the user's information. It is desired that the security context transfer does not add additional overhead in the process of keeping

the communication secure. Thus, at this point, it is important to understand the concept of handover.

Handoff or handover is a concept of cellular telecommunications. For a mobile user, handoff provides transition from one base station to another to avoid call termination. Mobile IP (MIP) [42], an IP layer mobility management protocol, helps a mobile node to remain connected to the internet while moving between networks. During this process, the mobile node discovers the neighboring networks, which it wants to communicate with, either by listening to beacon messages, or by periodically probing for the presence of a base station. The beacon message carries the Care of Address (CoA), which will be the address of the node in a foreign network and the signal information. The observed signal information known as Received Signal Strength Indicator (RSSI) is the basic principal behind handoff. When the RSSI for a mobile node falls below a mobile-specified threshold, the mobile node is handed over from the current base station to a new one [9]. Such a handoff can be horizontal or vertical:

i. Horizontal Handoff – It takes place between networks using the same access technology or wireless network interface
ii. Vertical Handoff – It takes place between networks using the different access technologies.

2.2 Existing Schemes

Cryptographic algorithms for key distributions, like identity-based authentication, are considered simple public-key management algorithms that

make use of signatures for authentication. However, they add computational overhead and hence are less efficient. Mobile IPv6 [42] uses symmetric keys and hash functions which, although recommended for mobile environment and data integrity, are hard to manage. In some cases [38], where the network comprises both, WLAN and cellular networks, authentication in the cellular network is based on the information stored in the SIM (Subscriber Identity Module) [39] and the WLAN uses a certification mechanism for authentication. If a mobile node moves from WLAN to cellular, it authenticates itself to the access point in the WLAN by validating its certificate. For this self-authentication, the mobile node should hold the certificates for the relevant CA and all the other CA's which it will eventually contact in the future for other access point connections. At this stage the node is offline, while it is still waiting for mutual authentication with the access point. Hence, it needs the CA certificate before authenticating the access point. As the number of CA grows, it can become very cumbersome for the node to first procure and then hold the information. This scheme [38] proposes to have an always-on connection with the cellular network. However, there are several flaws associated with this scheme. It assumes an "always-available" cellular connection which results in an overhead for the node to stay connected to the two networks simultaneously in a fast moving environment. Deploying certificates in this type of scenario may involve additional cost for subscribing to the certifying authority in addition to the extra time required to obtain such certificates right before the authentication takes place.

Methods like Group Key Agreement (GKA) Protocols [13], and [14], attempt to resolve the security issues by establishing a cryptographic key for a group of nodes in a network. The key is derived from a secret-key contribution from each member of the group. Here, each member calculates part of the group-key and passes it on to a chosen group leader. Hence, with each addition or removal of a node, a new key is first derived by re-calculations and is then re-distributed in the group. The group of nodes is in the form of a logical tree with the root as the leader and the leaves as the nodes. Such mechanism can be convenient for mobile users as it supports connectivity with mobility [15]. But it addresses mainly the energy consumption by various network entities and not the security strength of the group key agreement algorithm. In addition, Forward Secrecy, and DoS attacks are other problems this mechanism fails to address along with guaranteeing a holistic security solution. [33] Goes a step further by solving the regular calculation and distribution of group-key. It proposes a method for designing multicast key management trees that match the network topology. The proposed key management scheme localizes the transmission of keying information and considerably reduces the communication overhead caused by constant key exchange. Their research proposes a handoff scheme for topology-matching key management trees and also considers the heterogeneity of the network. [34] Recommends an adaptive cognitive algorithm to improve security of the network. However, it only caters to the Denial of Service (DoS) attack instead of addressing the overall security.

For key distribution among the group key distribution scenarios described in [13]-[15], [33]-[37], a certificate-based key exchange proves resource demanding for the resource constrained network entities [35]. In [36], the authors propose a data structure which dynamically captures the mobility topology of the network to reduce the authentication time. This theory of proactively transferring security context with the help of the data structure is viable only for mobile nodes that do not change their connectivity to the network to keep a radio link quality. Another scheme [37] on proactive key distribution in heterogeneous networks acknowledges random key pre-distribution to achieve more secure network. This scheme does not consider the cumbersome process of pre-distributing the keys among mobile nodes in order to participate in this scheme. [40] Assumes that the WLAN and cellular networks are offered by the same operator. The likelihood of this scenario is low where one operator provides both converged services and broadband access. [41] Also faces similar shortcomings. It assumes that the operator provides both the services. In principal, it proposes to reduce the roundtrips between the supplicant and the home network by co-locating the MIP [42] and Session Initiation Protocol (SIP) [43] server.

2.3 Encryption Techniques

In this section, we study the notions of established cryptographic algorithms in wireless security.

An encryption scheme enables a message sender to send a message to the receiver in a format difficult to interpret by an adversary. The encryption can be accomplished broadly through two mechanisms:

I. **Symmetric Encryption**: This Encryption uses the same key for both encryption and decryption. Some of the common examples are :
   - **DES** – The Data Encryption Standard based on a symmetric-key algorithm that uses a 56-bit key [45]. Because of the short length of the cipher key, it has been proved to have theoretical attacks and researchers have confirmed comprehensive key search attacks [48].
   - **AES** – The Advances Encryption Standard [46] is one of the most popular algorithms used in symmetric key cryptography. It uses the concept of block cipher adopted by government agencies as an encryption technique for unclassified resources and business dealings.
   - **H-MAC** – Hash-Message Authentication Code [49] authenticates the message and ensures its integrity by digitally signing the message. HMAC's have an input test and a secret key known only to sender and the receiver [50].

II. Asymmetric Encryption: This is the mechanism for secure communication between two parties which use public key for encryption and private key for decryption. The private key is safely stored by the owner while the public key is widely distributed to enable anyone to send encrypted message. The

advantage of this is that asymmetric cryptography is less computationally intensive and requires less bandwidth. But on the flip side, it requires a prior set-up of the private-public pair by a designated authority to which the user must get authorized. Such an authority is called the Certificate Authority (CA). The CA distributes the public key by digitally signing it. Some of the examples of this types of encryption are :

- **RSA** – The RSA algorithm [44] was invented by three researchers, R.L. Rivest, A. Shamir, and L. Adleman and is named after the first alphabet of their last names. It is a public key encryption mechanism and involves key generation which is used for encryption, by involving two large random prime numbers. Its difficulty is based on the complexity of factoring large integers. However, recent advancements in the capability of computation machines, their hardware and factoring techniques have increased the vulnerability of this mechanism [47].
- **IBE** - is also a public-key cryptosystem where any information about the user is a valid public key. In particular, email addresses and dates can be public keys. The IBE [3] email system is based on the first practical Identity-Based Encryption scheme (IBE) [3]. The CA or a trusted third party, called Private Key Generator (PKG), generates the corresponding master key. This master key is used to generate private keys when decryption is required by the user. The security in email system is one of the common uses of this encryption.

- **Diffie Hellman** - is a cryptographic protocol published by Whitfield Diffie and Martin Hellman in 1976 [18]. It allows two parties to jointly establish a shared secret key over an insecure communications channel. This key is used to encrypt message exchange using a symmetric key.

The limited resources make the use of Asymmetric Cryptosystems infeasible because they are computation and memory intensive. This makes algorithms like Diffie-Hellman key agreement and RSA undesirable. Asymmetric cryptosystems cannot be used even to establish session keys because that would leave the nodes vulnerable to Denial of Service attacks [11, 12, 57]. Symmetric key ciphers and hash functions are considered better as they are two to four orders of magnitude faster than digital signatures [11].

However, it is beneficial to make the best of both the worlds. A strategic use of symmetric and asymmetric keys together can also yield good results. We use both these mechanism of data security simultaneously in an integrated heterogeneous wireless network and accomplish a good level of security.

3 Proposed Security Scheme

3.1 Base Algorithms

In this section, we first describe the algorithms which are the foundation of our security scheme. Subsequently, we present an analysis of their strengths and limitations and the justification behind the choice of cryptographic schemes.

3.1.1 Identity Based Encryption (IBE)

[8] Demonstrates that a likely trend in the world of wireless security is the partial use of certificates and identity-based authentication. The concept of identity based cryptography was first introduced by Adi-Shamir in 1984 [29]. It is a type of public-key cryptography that identifies digital signatures where the public key can be any uniquely identifying information of the user. The user's email-id, NAI, address etc. qualify as an acceptable, uniquely user-identifying information. Several issues affecting this cryptographic algorithm, like decrypting a message with no authorization, led to its derivative scheme called basicIdent [19]. BasicIdent [19] is not chosen cipher text secure and hence paved the path for another scheme called FullIdent [18]. We use this idea in our scheme for a seamless localized transfer of security credentials and therefore, fill the gaps left by EAP-SKE [6]. These gaps are described in the section below.

3.1.2 EAP-SKE

Extensible Authentication Protocol [22] is an authentication framework which supports a chosen authentication method based on MD5 [51], AKA [52], PSK [53]. Several EAP-methods [6], [21] and [23] have been proposed with the above mentioned cryptographic protocols as their base cryptographic protocol.

Some of these methods are described below:

- **EAP-MD5**: This EAP method [22] uses Message-Digest algorithm 5 (MD5) [51] hash to authenticate the client. MD5 [51] offers minimal security as it only authenticates client to server and is vulnerable to dictionary attacks. Also, it does not support mutual authentication.
- **EAP-AKA**: Authentication and Key Agreement (AKA) [21] is a mutual authentication and key distribution scheme used in mobile wireless networks like UMTS and CDMA. It is based on the challenge-response authentication in which a party presents a challenge and the other party must provide a valid answer to get access.
- **EAP-PSK**: This method is derived using a Pre-Shared Key (PSK) [23]. It was designed for authentication over insecure networks like public hotspots.
- **EAP-SKE**: This is an EAP [22] implementation of W-SKE [6]. The mechanism provides authentication between the home and foreign agent in a single round-trip-time (RTT) with low latency and key distribution. Comparisons with other EAP-methods [6], [21] and [23] prove that this

protocol is best suited for today's IP networks with roaming clients. The EAP-SKE [6] uses only one roundtrip to mutually authenticate, authorize and generate session keys between the mobile node and the network [6]. As this method has proven to be the best among all the EAP-methods, we choose it as the base security algorithm for our proposed scheme.

However, it assumes that the supplicant is attaching itself to different ASs and re-authenticating every time to the home network. [54] Achieves localized authentication for WLAN roaming using an authentication protocol based on a public-key infrastructure. This scheme was proposed for WLAN interworking but the advantages behind the localization concept spans across all types of networks. We use it in our scheme but in a novel format. A mobile node undergoes full authentication the first time using EAP-SKE [6] and IBE [3] after the mobile device moves into foreign network. The IBE [3] security is used as the local security algorithm for a certain time which is specified by the home network. The foreign agent uses IBE [3] , explained in detail later, for this time frame after which the supplicant must go through the next full authentication.

3.2 Main Idea

We propose a novel security scheme called EAP-SKE-IBE that conforms to the requirements of current networks and devices and also to the requirements of security architecture as set forth in the previous section. Fig. 4.1 gives a high-level

overview of the current network architecture. It depicts a general network where a mobile node can move between base station and access point belonging to a cellular network and WLAN respectively.

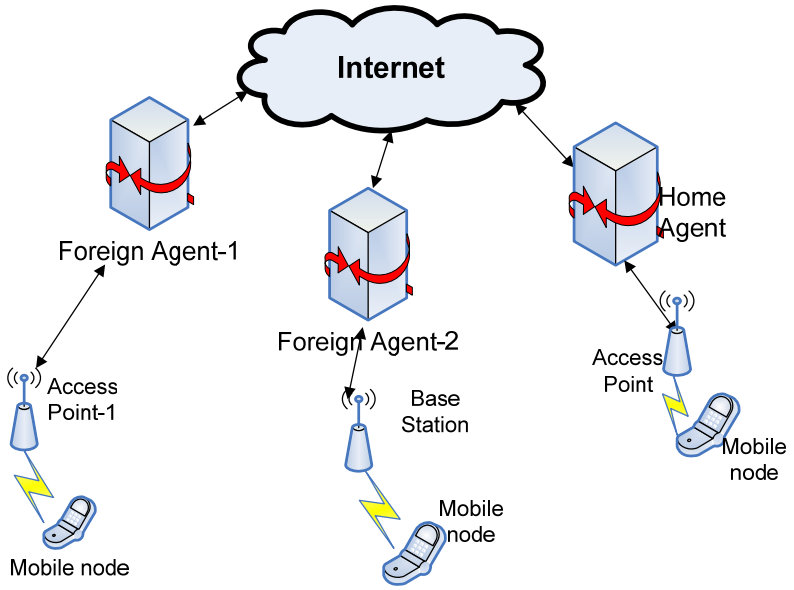


Fig. 3.1 High-level overview of current network architecture

We explain a scenario of a roaming mobile node and also the functioning of our scheme along with it:

When a device comes on a network for the first time, it needs to provide its identity to the network and must go through a full authentication. For the sake of simplicity, we consider this to be a cellular network. Since we understand that this device shall roam between a 3g-WLAN network, we must have a security protocol that can work interchangeably. EAP, as described in Section 2.2, offers a framework along with a 3g security protocol. After making use of the analysis in [6], we came

to the conclusion that EAP-SKE [6] uses only one roundtrip to mutually authenticate, the mobile node and the network. It is also stateless, supports forward secrecy, and supports path authentication. Hence, EAP-SKE [6] is the protocol of choice for authenticating device with the network for the first time.

As the device roams to networks distant from the home network, we are not best positioned to use EAP-SKE [6] as the authentication scheme. EAP-SKE [6] assumes that the supplicant is attaching itself to different access points and re-authenticating every time to the home server irrespective of the distance between the access point and the Mobile Node. Despite its high scope for usability in the networks in question, such an assumption may no longer be valid. Also, this protocol does not support backward secrecy [7] which guarantees that previously used keys must not be discovered by new network entities joining the network. To resolve the aforementioned issues, we introduce the use of identity based encryption (IBE) [3] as a means of authentication in the roaming scenario after the first EAP-SKE [6] exchange has taken place in the home-location. IBE [3] is appealing in roaming scenarios because of its easy to use and does not require a certificates-like infrastructure. This can be accomplished by transferring cached authentication information between adjacent FAs, thereby enabling re-authentication handled locally.

The IBE [3] scheme that we use indistinguishable-against-adaptive-chosen-ID and adaptive- chosen-cipher-text attacks (IND-ID-CCA). In this scheme, the attacker

gathers information, by choosing a cipher text/ plain text and obtaining its decryption/encryption under an unknown key

The novelty of our scheme lies in using two different algorithms with the same device in different scenarios and also the way these two algorithms utilize the same private key and help the device maintain a secure connection even after it has travelled far away from the home network. To accomplish this, we introduce a new attribute in the area of security algorithms called the time factor. This factor should be pre-set by the home network when delegating the task of authenticating the device to the foreign authenticator when handling subsequent authentication requests from the mobile node at the time of roaming. We prove through simulation that if a foreign agent makes the authentication task time-bound and makes use of IBE [3] as the roaming scheme while also informing the home authenticator of the change in care-of-address bound by the associated foreign address, both time and message exchanges can be reduced considerably. We also avoid the long delay which increases as the mobile node moves farther away from the home network. Through simulation of the heterogeneous wireless network deploying the two security algorithms and comparing them, we prove that we can reduce the authentication time by up to ~40% in a roaming scenario. To the best of our knowledge, no one, so far, has used timestamp as a vital security attribute to delegate authentication rights to the foreign network. Neither has anyone used two different protocols with mobile nodes undergoing multiple hops covering different networks.

3.3 Our Security Scheme

We now describe our security scheme in the next section. The flow of messages in the proposed security algorithm is detailed in Fig 3.2.

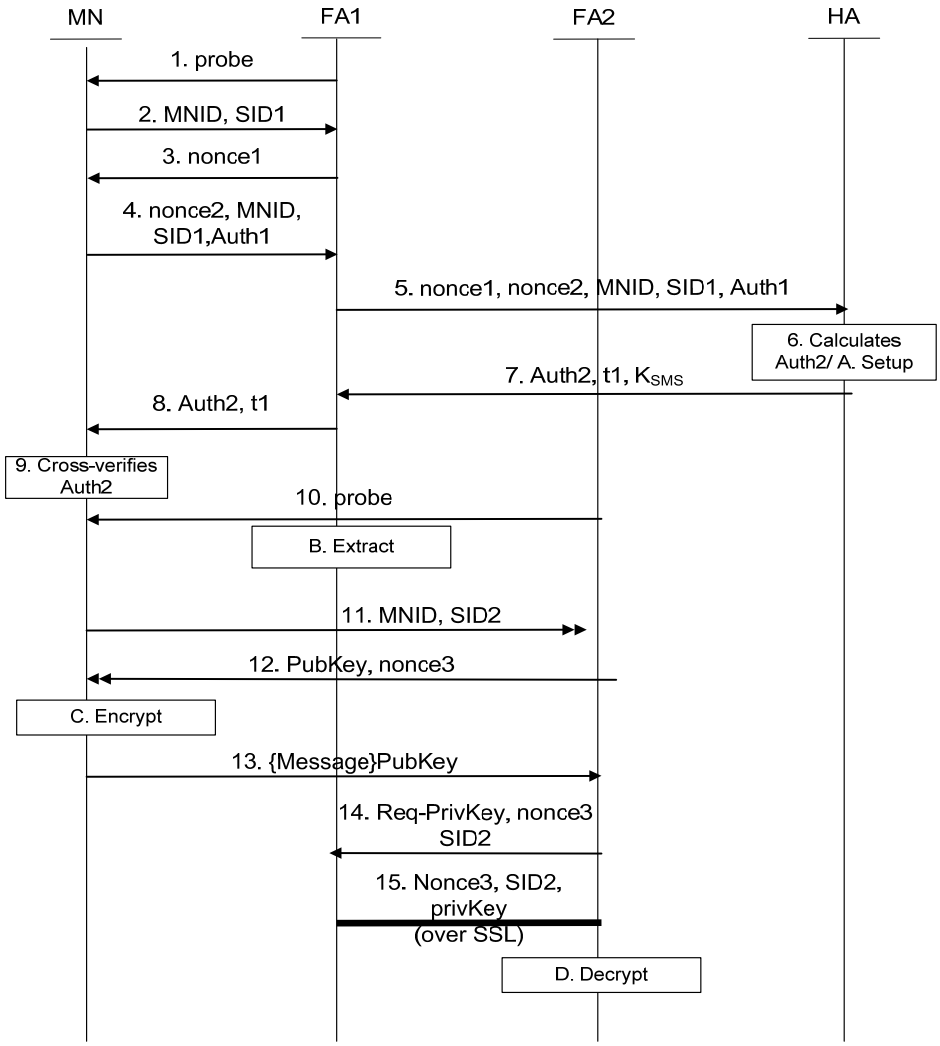


Fig. 3.2 Message flow for EAP-SKE-IBE

Nomenclature of terms used:

MN = Mobile Node

HA = Home Authenticator

FA = Foreign Authenticator

MN ID = Mobile Node identification

NAI = Network Access Identifier

N1, N2 = Nonce

AUTH1 = $MAC_{K\_MN,HA}$(N1|N2|MNID|NAI)

K_{SMS} = $PRF_{K\_MN\text{-}HA}$(AUTH2)

SID = Session ID

The messages are described in detail below:

1. Foreign Agent 1 → MN: {Beacon signals, MN probes}

As the MN moves out of the home network for the first time, it discovers the presence of a foreign agent through broadcasts made by Foreign Agent 1 or probing for the presence of a network meeting the signal threshold. Then, the Foreign Agent 1 issues a request for MN ID.

2. MN → Foreign Agent 1: {MNID, Session-id}

The MN responds with its ID that includes its NAI. The standard syntax for specifying the NAI is "user@realm" where user is the identity of the mobile node and realm identifies an administrative domain within the internet. It also initiates a session-id to keep track of the session with the Foreign Agent 1.

3. Foreign Agent 1 → MN : {nonce1, Session-id }

The Foreign Agent 1 challenges the MN by generating a challenge called nonce1 and sends it to the MN. The nonce is a freshly generated pseudo-random number. Including a nonce accounts for the freshness of every session. The format of the packet in which the nonce value is sent suggests the request for an EAP-SKE [6] authentication scheme as it contains the algorithm to be used for a secure communication.

4. MN → Foreign Agent 1 : {AUTH1, nonce2, MNID, SID1}

The MN generates another challenge called nonce2. It also computes the authenticator called AUTH1 and forwards the two values to Foreign Agent 1. The nonce here assures that the authenticator is fresh for every session as the nonce is used when calculating the authenticator. A MAC algorithm is used by the MN to calculate AUTH1. It uses a unique private key $K_{MN, HA}$ only known to the HOME AGENT and the mobile node.

5. Foreign Agent 1 → HA : {AUTH1, nonce1, nonce2, MNID, SID1}

The Foreign Agent 1 forwards the AUTH1, nonce1, nonce2 and the NAI to the home agent.

6. Home agent calculates AUTH2 and master session key.

The home agent does a look up in the database for a unique private key against the given MNID. It finds the MN-HA key symbolized by K_(MN-SUP, HA). It then compares AUTH1 by calculating one locally and cross-verifies the resulting values. The result is called AUTH2. If the values match, authentication with the MN succeeds; else fails. It also calculates a session key called K_{SMS} for the Mobile Node- Foreign Agent 1 session using the authenticator, AUTH2 and a pseudo random function.

7. HA → Foreign Agent 1: AUTH2, K_{SMS}, time factor

The AUTH2, master session key are then sent to the Foreign Agent 1. This is the usual EAP-SKE [6] mechanism. We introduce the time factor here. Home agent sends a time value in seconds to the Foreign Agent 1 and this time can be a function of the trust between the home agent and the Foreign Agent 1 and the history of mobile nodes roaming in the Foreign Agent 1 network.

8. Foreign Agent 1 → MN : AUTH2, time factor

The Foreign Agent 1 extracts the K_{SMS} and time factor and relays the AUTH2 to the MN. This key is for local message transfer between the Foreign Agent and the mobile node.

When the mobile node moves away into a different foreign network, the new foreign network, Foreign Agent 2, does not need to contact the home agent and retrieve session keys after mutually authenticating with the mobile node.

Instead, the previous foreign agent serves as the authentication centre for the MN until the time; time factor granted by the home agent expires. It keeps track of the time to check if it is nearing expiration after which, if the mobile node wants to move to another foreign network, it will have to request EAP-SKE [6] full-authentication from the home agent. The time format specifies the date and time till which the foreign agent can act on behalf of the home agent.

The Foreign Agent 1 makes use of an IBE-based algorithm which is considered the best approach for simplifying public key cryptography. IBE [3] uses the MNID as the public key, enabling data to be protected without the need for certificates. Protection is provided by the Foreign Agent 1 which acts as the key server that controls the mapping of MNID to decryption key. This keeps the MN from distributing public key certificates. Also, the recipient does not need to be ready with both public and private keys.

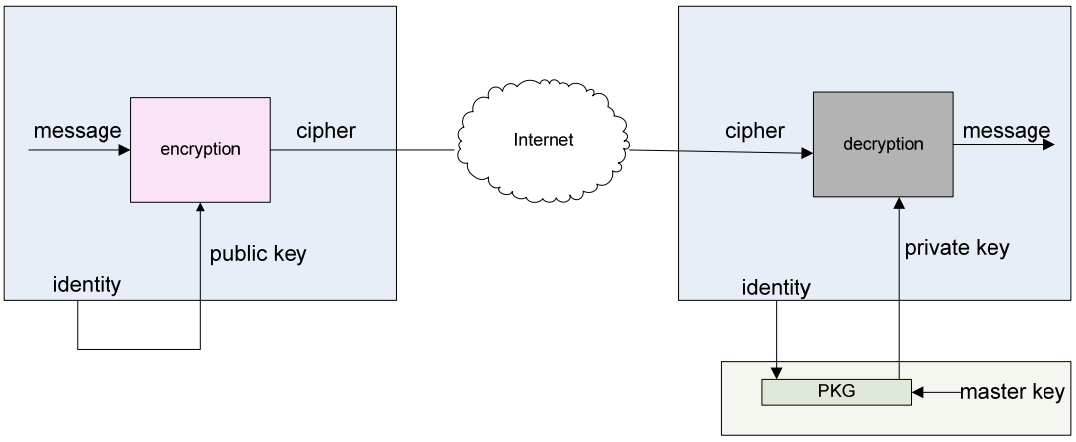


Fig. 3.3 Working of an Identity Based Encryption Scheme.

In IBE [3], a sender can create public key for the receiver who does not have to be ready with a private key for decrypting the message.

Similar to the IBE [3] mechanism, the various phases are accomplished as follows:

A. **Setup phase**: The home agent acts as the Private Key Generator (PKG). The K_{SMS} calculated by the home agent is used as the master key and is the input to the extraction phase implemented by the Foreign Agent 1. As described in [8], the setup algorithm takes some security parameters, k, and two hash functions G and H as inputs and gives system parameters, params and a master key as output.

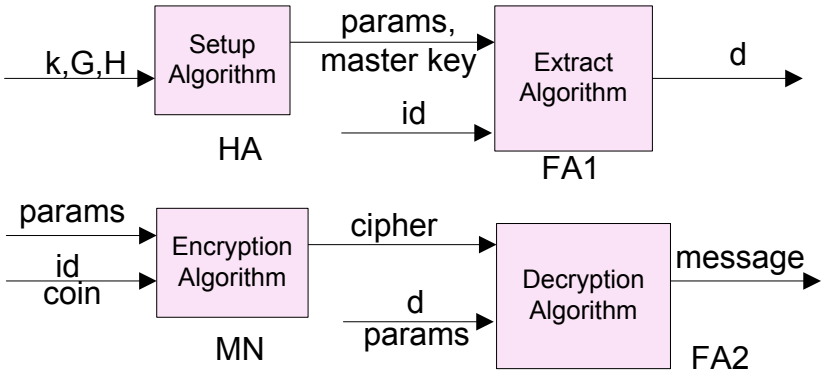


Fig. 3.4 Phases of IBE.

B. **Extraction Phase**: This is executed by the foreign agent; it takes the params, master-key, $K_{SMS,}$ the public key which is the ID of the mobile node and the COIN (k) as input parameters. The output of this phase is the private keys, d which are stored in Foreign Agent 1's database next to the respective MNID. COIN (k) is the coin flipping space.

C. **Encryption Phase**: The MN encrypts the message using its ID, params, and COIN(k)

D. **Decryption Phase**: When a new foreign agent requests for the key to decrypt messages sent by the mobile node, it contacts the Foreign Agent 1 for the private key for that session with the mobile node.

9. The mobile node validates the home agent by comparing the value AUTH2. It then locally generates the master session key, K_{SMS}.

10. Foreign Agent 2 → MN: {Beacon signals, MN probes}

    The MN moves to another network and discovers signals stronger than the current one. It discovers the presence of Foreign Agent 2 through broadcasts or by sending a request to join the network to Foreign Agent 2.

11. MN→ Foreign Agent 1→ Foreign Agent 2: {MNID, SID2}

    The MN sends its id to Foreign Agent 1 which, in turn, relays it to the Foreign Agent 2 and marks the session with another id called SID2.

12. Foreign Agent 1→MN: {Public Key, nonce3}

    The Foreign Agent 1 sends a public key to the MN using which it can encrypt the messages.

13. MN→ Foreign Agent 2: {{Message}Public Key}

    Using the Public Key from the previous step, MN encrypts the messages and sends them to Foreign Agent 2.

14. Foreign Agent 2→ Foreign Agent 1: {Req-Private Key, nonce3, SID2}

    Foreign Agent 2 extracts the current NAI and requests for a private key.

15. Foreign Agent 1→ Foreign Agent 2 : {nonce3, SID2, Private Key(over SSL)}

    Foreign Agent 1 then sends a private key corresponding to that session and public key over an encrypted channel. We use SSL for this purpose as it is the most widely used security protocol for transport.

    The Foreign Agent 1 finally informs the home agent of the change in care-of-address (CoA).

4 Simulation and Implementation

In this chapter, we first describe a vertical handoff in a wireless network and then the implement our proposed security scheme on the same.

4.1 Wireless Network implementing Vertical Handoff

4.1.1 Simulation

Simulating a vertical handoff in an integrated heterogeneous wireless network was paramount to our work as we needed a flawlessly working wireless network base for the security simulations. It helps achieve closest possible results when proving our theory and making a comparison between existing and our scheme.

We followed the Basic Resource Management (BRM) scheme during vertical handoff as proposed in [16]. In this scheme, an active mobile user in an integrated wireless network changes wireless interface from a lower to a higher bandwidth network when the higher bandwidth network becomes available or the mobile node receives poor connectivity. The BRM network comprises more than two networks with different bandwidths and coverage. We do not treat different types of traffic separately and cover only non-real time traffic for our scheme. The blocking probabilities of originating calls and handoff calls under different offered traffic load are evaluated and the results of our simulation are verified with theirs. The flow charts in Fig 5.3 for originating calls and Fig 5.4 for incoming calls explain the algorithm followed to simulate vertical handoff as described in [16]. The calls

initiated within the network are called originating calls while the calls that continue as the node moves within networks while staying connected is called incoming calls. Our simulation helps us determine whether the vertical handoff mechanism is performing correctly by checking our graphs against the graphs in [16]. We use the same performance measure, i.e. blocking probability, as in [16] to study the system behavior and validate its implementation. Blocking probability, by definition, is the probability of a call dropping when it is requested from a server but none is available as all are busy with the existing traffic. For a new call, we derive the blocking probability under different traffic loads. The heterogeneous network system considered in this research comprises a cellular network and a wlan with mobile nodes moving within networks with varying speeds. The entire network is divided into cells. Cells representing the cellular network have radius 800m and contain smaller WLAN cells with radius 80-160m. The system parameters are given in table 4.1

#	**Parameter**	**Value**
1	Average number of mobiles in each cellular cell	4 Mobile Nodes
2	Average number of mobiles in each WLAN cell	4 Mobile Nodes
3	Average call arrival rate of each mobile	1-10 calls/minute
4	Average service rate of each cellular cell channel	120 secs
5	Average service rate of each WLAN cell channel	120 secs
6	Average moving speed	10m/s

Table 4.1 System parameters for vertical handoff

We model our system in a large 10x10 hexagonal grid of cellular network with each cell sized 800 meters in radius and a WLAN radius, a randomly chosen integer ranging between 80-160 meters. A cellular network can have clusters of WLAN networks with integer value ranging between 1-5 cells. Our simulation system is shown in Fig 4.2.

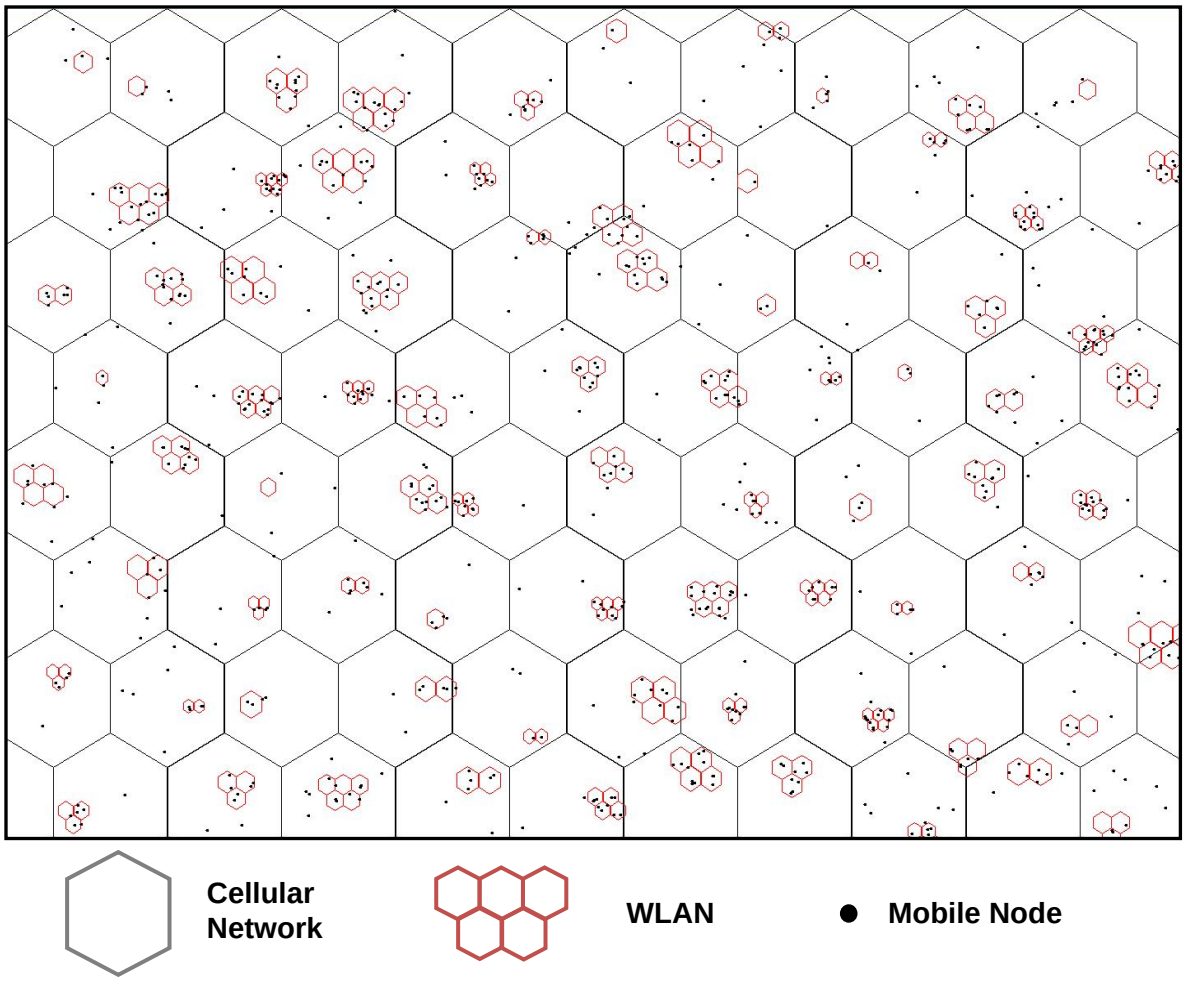


Fig 4.1 Snapshot of simulation work

The large cells depict cellular network and the smaller ones are wlan. The black dots are the moving wireless nodes using resources from one network or the other. The number of arrivals in the queuing system in a given time interval [0,t] assumes Poisson distributed arrivals with different arrival rates with mean values is given in table 4.1. Using the concepts and formulae studied in [17], we verify our graphs and then build our security algorithm on top of that. Fig 4.4 a, b, and c and Fig 4.5 a, b and c present the graphs for blocking probability during vertical handoff for cases such as – moving node in a cellular and wlan network, and static node in a cellular and wlan network.

Java is used as the language to create the simulation environment. Java is an object-oriented programming language with a number of features that make the language well suited for our use. It is portable, platform-independent and has a rich set of APIs which make coding an easier task. Graphical User Interface (GUI) support has helped us visualize the simulation and helped in debugging.

A short description of the flowcharts is as follows:

For originating calls: When an originating call is generated, it checks for bandwidth availability in the cellular network. If there is enough bandwidth the call is accepted by the cellular network. Otherwise, the originating call checks the availability for wlan network. If there is a free channel available, the call is accepted by the wlan network. Else, the call is blocked.

For incoming calls: When an ongoing call in a cellular network completes its ongoing communication and moves to another network, the occupied bandwidth becomes available. The now free bandwidth is reallocated to an ongoing call in the wlan network based on Last-In-First-Out basis.

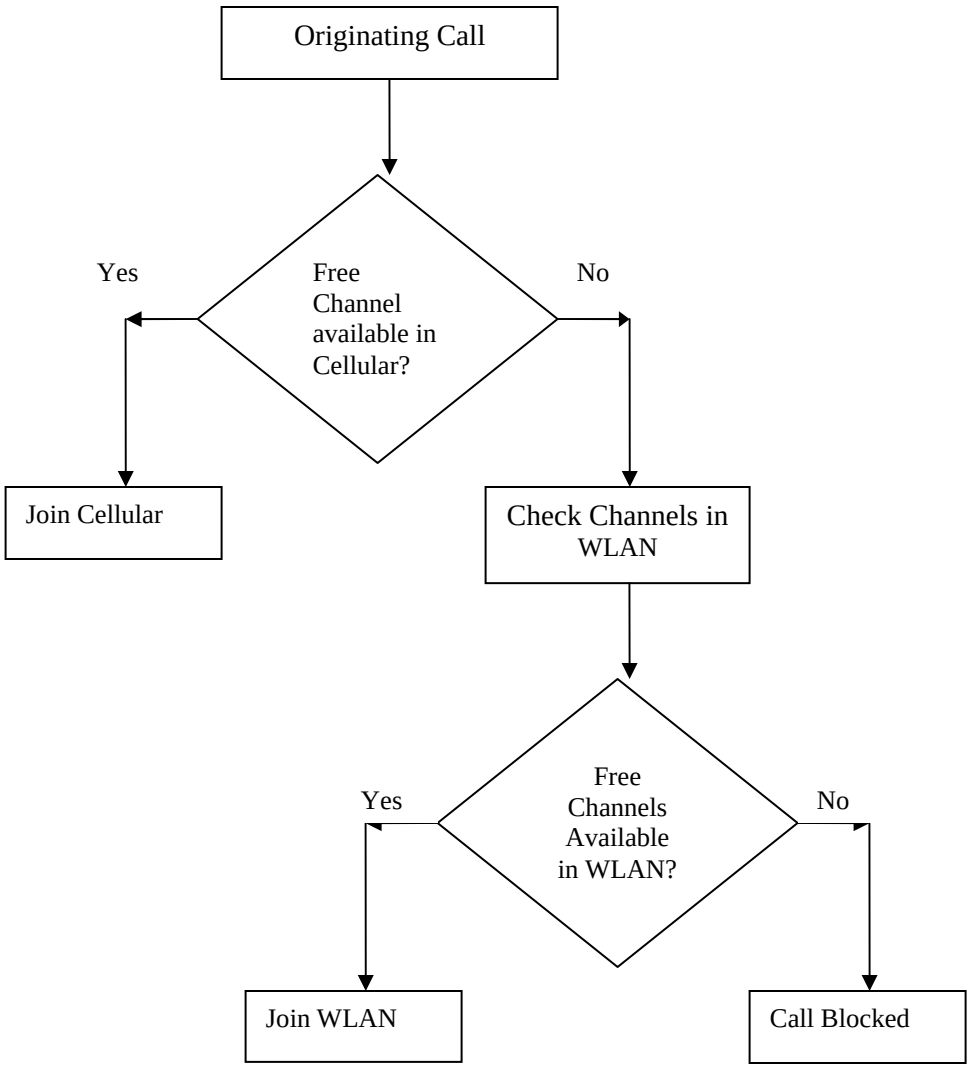


Fig 4.2: Flowchart for Originating calls during vertical handoff

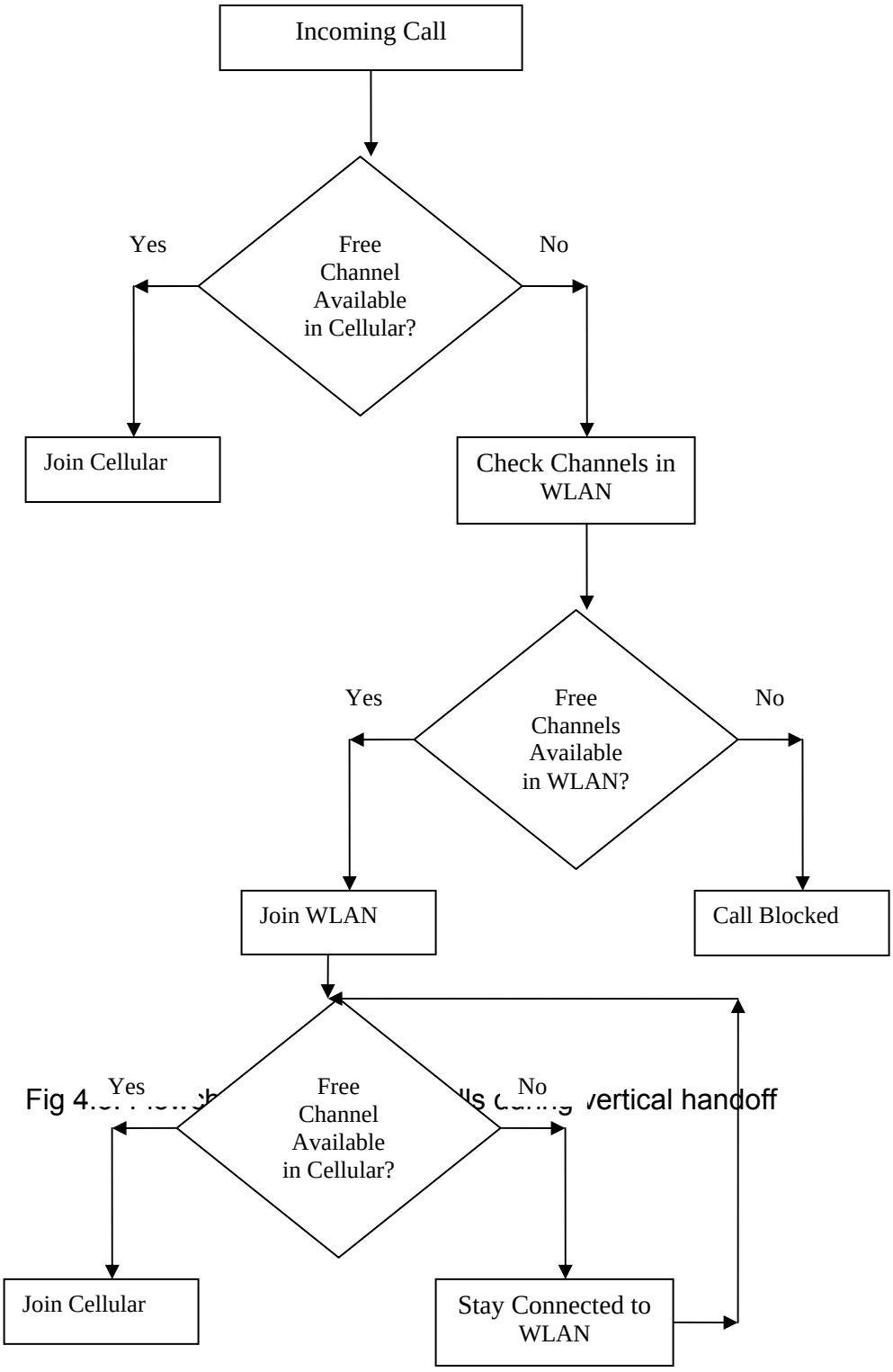
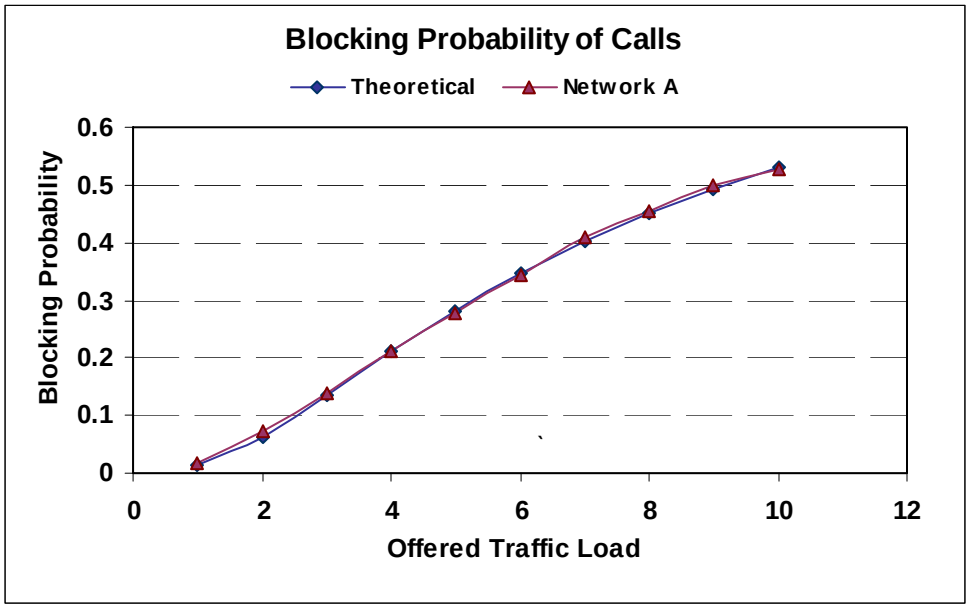
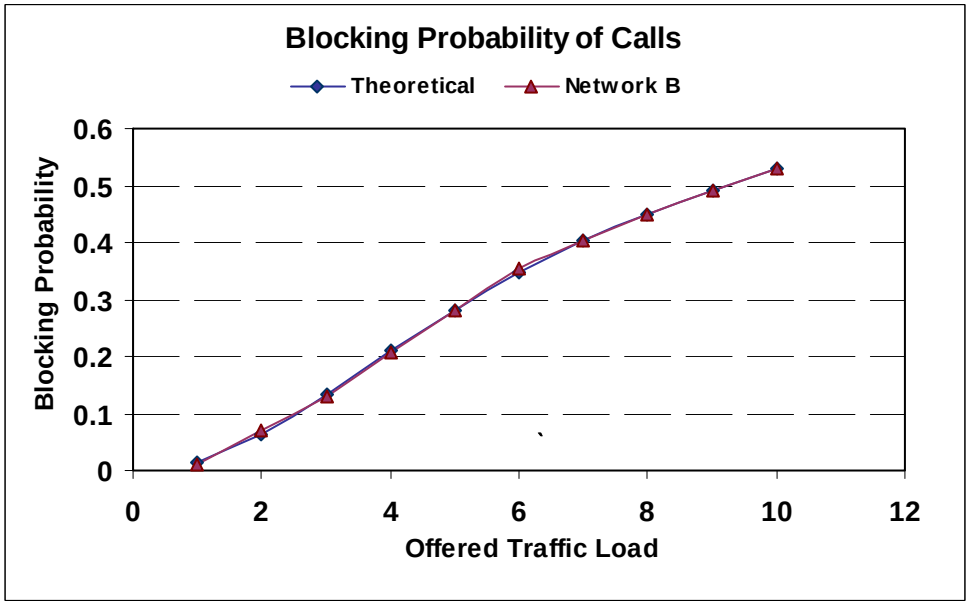


Fig 4.3: Flowch[illegible]ls during vertical handoff

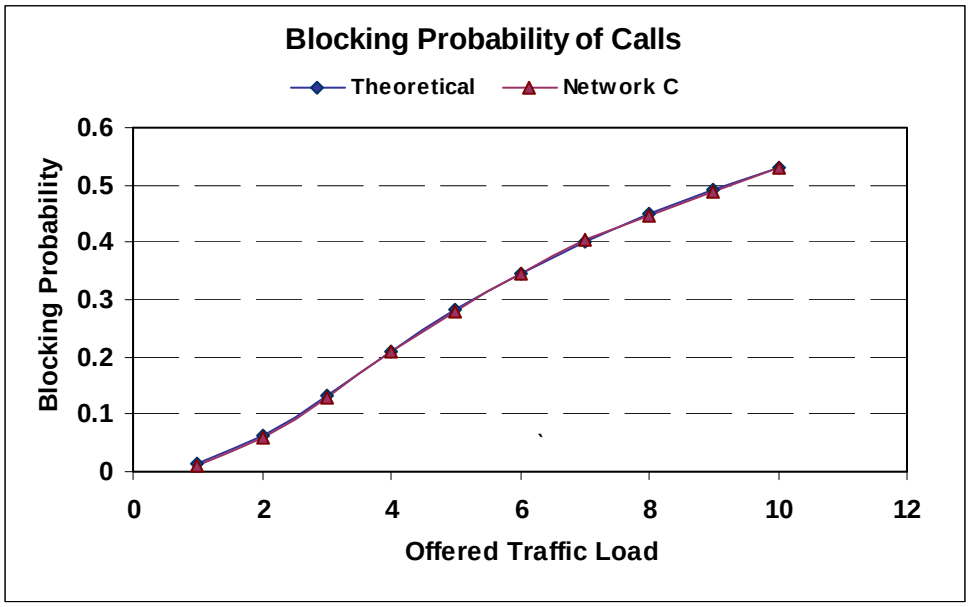
4.1.1.1 Simulation Validation



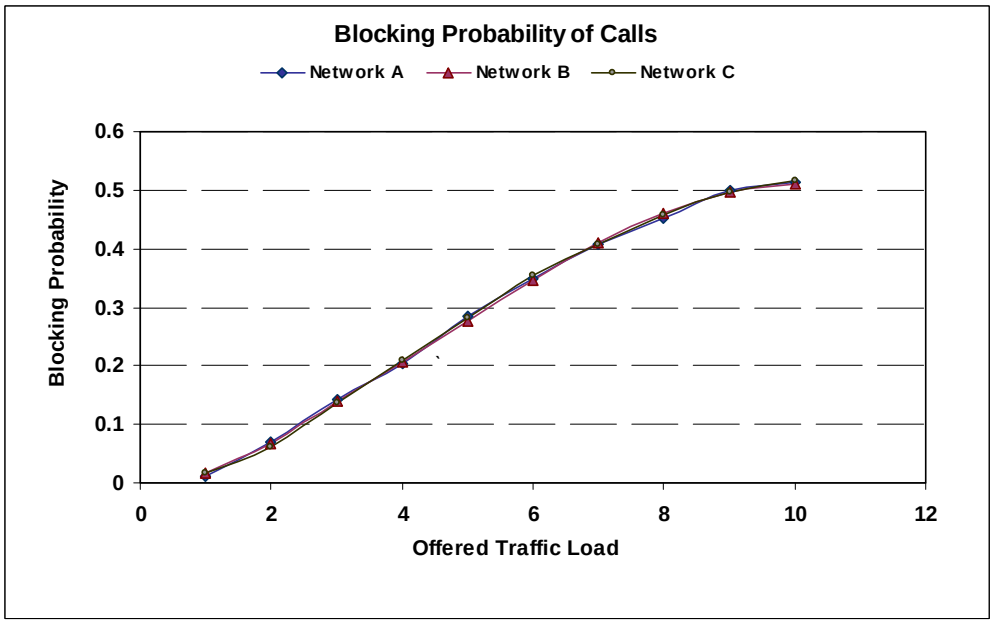
(a)



(b)

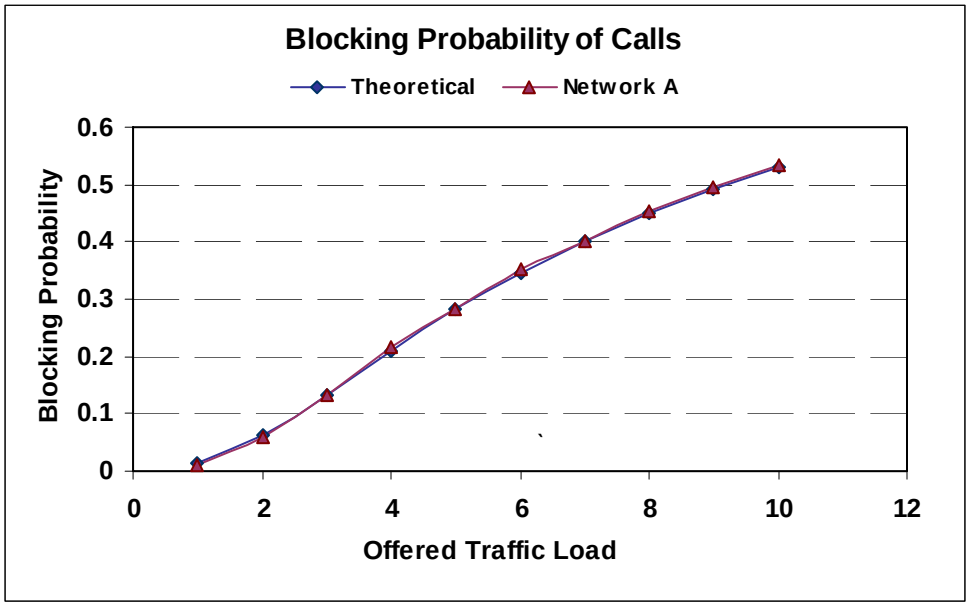


(c)

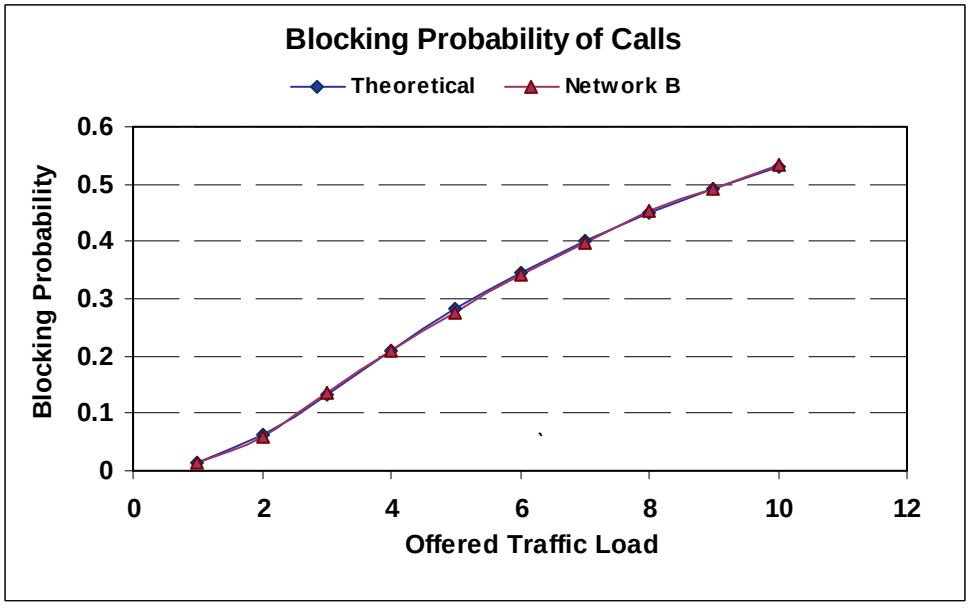


(d)

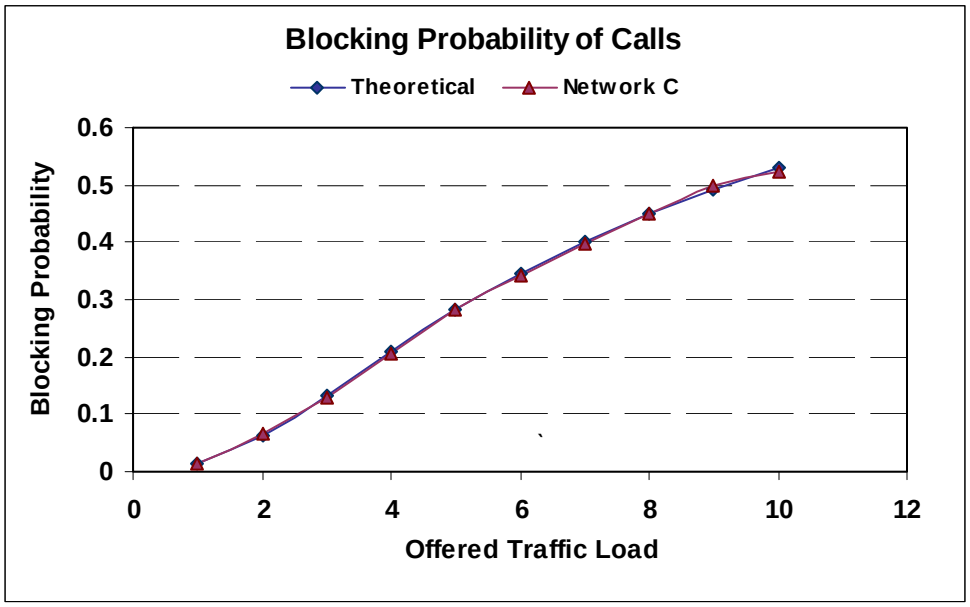
Fig 4.4 - Cellular network with static mobile nodes (a, b, c) and moving mobile nodes (d)


Blocking Probability of Calls
Theoretical
Network A
Blocking Probability
0.6
0.5
0.4
0.3
0.2
0.1
0
0
2
4
6
8
10
12
Offered Traffic Load

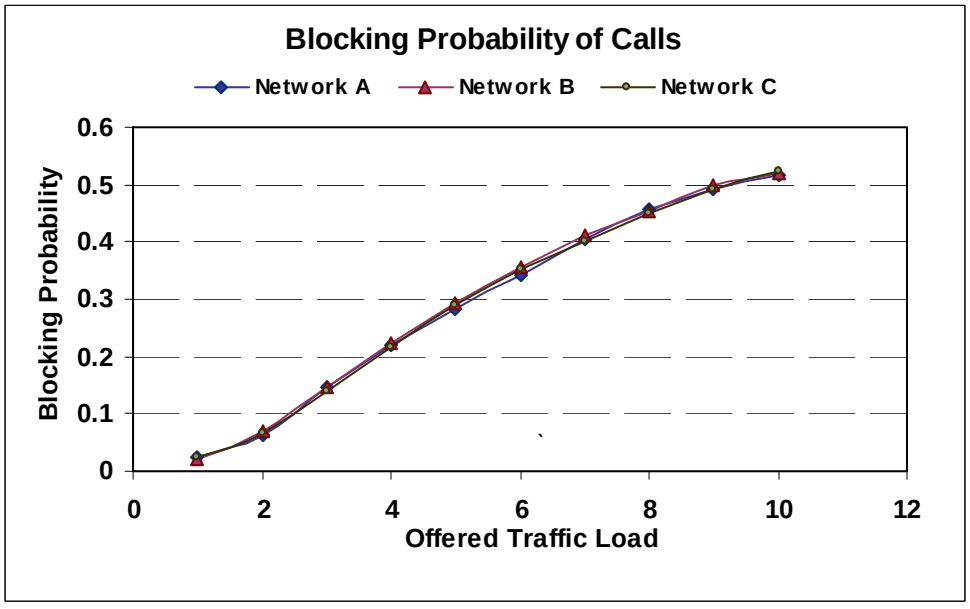
(a)


Blocking Probability of Calls
Theoretical
Network B
Blocking Probability
0.6
0.5
0.4
0.3
0.2
0.1
0
0
2
4
6
8
10
12
Offered Traffic Load

(b)



(c)



(d)

Fig 4.5 - WLAN network with static mobile nodes (a, b, c) and moving mobile nodes (d)

In Figures 4.5 and 4.6, we show that the simulated BRM scheme achieve the same simulation results as in [16] in the blocking probability of calls. The Fig 4.5 and Fig 4.6 show graphs for three cellular and WLAN networks with very close graphical results, hence validating our simulation. As all the networks are measured against theoretical results, it gives us confidence on the implementation of the wireless network.

4.1.2 EAP-SKE-IBE Secure Scheme

We now describe the simulation procedure for our security scheme and implement it on the simulated wireless network. The scheme is then experimented with the latency difference between EAP-SKE [6] and EAP-SKE-IBE as the number of handoff increases. These values determine the time delegated to Foreign Agent to act as the authenticator for MN after it has undergone full-authentication using EAP-SKE [6] with the home agent. EAP-SKE-IBE provides improved authentication results by reducing time taken for session key distribution. The key idea behind our approach is that a localized authentication can guarantee that the overhead associated with the authentication time can be reduced. It can also minimize the impact on the authenticating network's roaming user caused by the delay in accessing the home network. Further, it prevents the occurrence of a situation of a home network's unavailability and as a result, loss of connectivity to the mobile node.

4.1.2.1 Results and Analysis

The top curve in the Figure 5.6 is the vertical handoff delay for WLAN-Cellular using EAP-SKE where the values for handoff delay are around 4 – 10.31 seconds. The delay for EAP-SKE-IBE is much less than in EAP-SKE. This can be attributed to the fact that when the Mobile node moves between the WLAN and Cellular networks, each handoff request requires AAA authentication which consumes considerable amount of time. An EAP-SKE-IBE using mobile node also goes through these steps but with a difference that it still maintains connectivity through its Foreign AAA. Hence the AAA authentications do not add to the handoff delay in case of EAP-SKE-IBE.

It can also be noted from the results presented below that the difference between the handoff times is not significantly high initially but with increase in the traffic on the network the performance of EAP-SKE vertical handoff degrades fast. This is mainly due to the additional communication and signaling between network entities viz. FAAA, HAAA and mobile node etc. for location update and registration. With increasing load this communication takes longer time to traverse through the network.

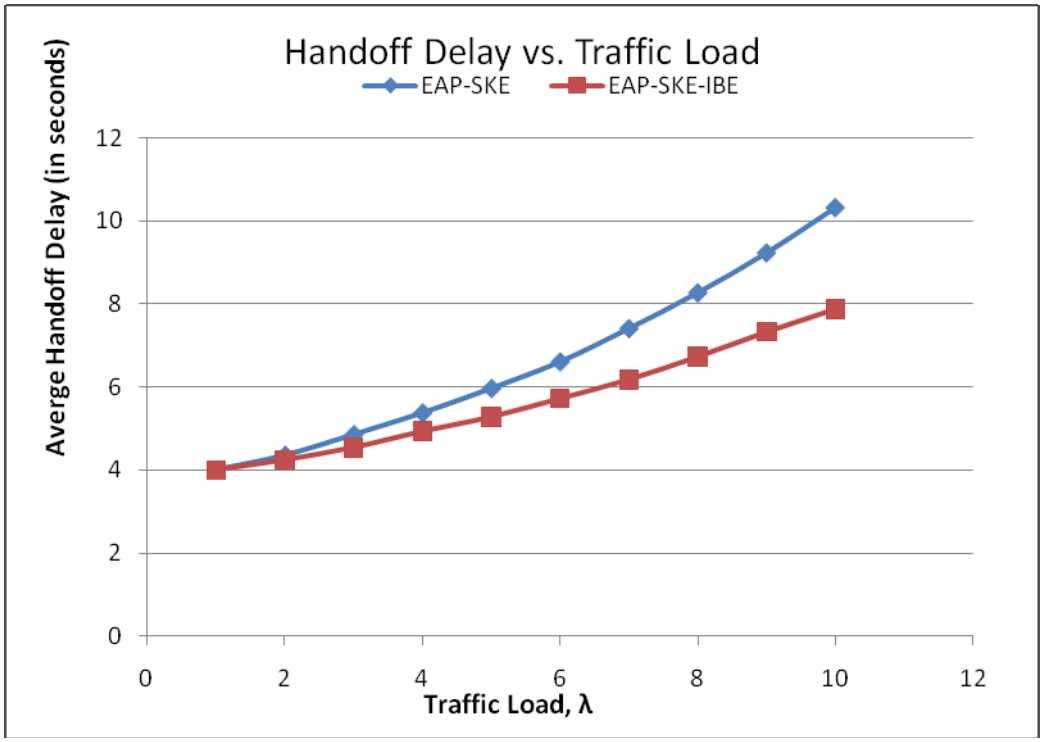


Figure 5.6 Vertical Handoff Delay vs Traffic Load comparison for EAP-SKE-IBE and EAP-SKE

5 Summary

5.1 Conclusion

This research presented an efficient authentication protocol that uses two security mechanisms depending on the location of the user. It enhanced an existing scheme, EAP-SKE [6] authentication, by utilizing a localized distribution of keys by means of the identity-based-encryption (IBE) [3]. EAP-SKE [6] was used for the first vertical handoff between two heterogeneous networks when the mobile node undergoes full authentication with the home network. The IBE [3] later provided IND-ID-CCA security and hence made the localized security context transfer secure. In normal scenarios, once the user moves to the neighboring network after undergoing multiple vertical handoffs, it would need to go through full authentication for every inter-system handoff. To overcome the latency that comes with repeated communications with the home network, we introduced our scheme which uses the time factor between the home and foreign domains and delegates the authentication task from the home agent to the foreign agent for localized authentication. The foreign agent then sent out private keys for every new connection while the time designated by the home network lasts. Once the time period expired and the foreign agent could no more authorize the mobile node, the mobile node went through full authentication. After this step, a new foreign agent was again delegated following the same process.

We initially tried to identify the main risks an IHWN network is exposed to and then developed a security protocol to address those issues. We used a performance comparison between an existing scheme, EAP-SKE, and our scheme, EAP-SKE-IBE to prove its efficiency and scalability. Results proved that our scheme, depending on the amount of time it runs, could reduce the total time taken for handoff by up to 40%.

Our protocol is more efficient than all previously known ones since it considerably reduces the number of messages transferred and hence optimizes the computational time.

5.2 Future Work

Although, we have tried to understand the burning security problems in IHWN and have proposed a solution to address them, there certainly is scope for future work. Some of them are discussed below:

1. If enough research time is spent in pursuing this, the IHWN can include other type of networks like ad-hoc, sensor etc. As the number and type of networks increase, so will the complexity of implementing a security algorithm that will cater to the entire different network individually and as a group.
2. In this work, we proved through simulation that as the time factor increases, the latency in security context transfer decreases. However, the algorithm may break after a certain point. This can be quantified by further simulations.

3. This work can also be extended for different types of data including real-time and results can be compared with non-real time.
4. IBE [3] was used as the security mechanism for localized security context transfer. Other suitable algorithms can be used and their efficiency can be verified by extending this work.
5. This work mainly focuses on reducing the latency in security context transfer during vertical handoff. The security threats it can prevent can be analyzed in the future work.
6. We simulated this work under certain defined parameters for the integrated heterogeneous wireless network, assuming the simulations can be scaled later.
7. Machine-to-Machine (M2M) [55] is a fledgling network technology and has great scope of growth in the future. It collaborates with the present standardized technologies, like TCP/IP, WLANs, cellular technologies, and wired networks. Little to no work has been done in securing the communication between this type of network and other existing one's. Using our algorithm in this area has a promising future.

6 Bibliography

[1] 3gpp technical specification,"*3gpp system to wlan inter-working; System description*," TS 23.234 v.6.1.0, June 2004.

[2] J. Loughney, M. Nakhjiri, C. Perkins and R. Koodli, "Context transfer protocol (CXTP)," *RFC 4067 (Experimental), Internet Engineering Task Force*, July 2005.

[3] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in the proceedings of *Crypto '2001*, vol. 2139 of LNCS, pp. 213-229, 2001.

[4] J. C. M. Teo, C. H. Tan and J. M. Ng, "Authenticated Group Key Agreement against DoS in Heterogeneous Wireless Networks," in the proceedings *of IEEE Wireless Communications and Networking Conference*, pp. 3563-3568, March 2007.

[5] J. C. M. Teo, C. H. Tan and J. M. Ng, "Low-power group key agreement for heterogeneous wireless networks," in the proceedings of the *2006 international conference on Wireless communications and mobile computing*, vol. 1, pp. 226 – 236, 2006.

[6] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel and S. Miller,"Efficient authentication and key distribution in wireless IP networks," in the proceedings of *IEEE Wireless Communications*, vol.10, pp. 52-61, Dec. 2003.

[7] W. Diffie, P. Oorschot and M. Wiener , "Authentication and Authenticated Key Exchanges," *Designs, Codes and Cryptography*, pp. 107-125, 1992.

[8] P. Yang, T. Kitagawa, G. Hanaoka, R. Zhang, K. Matsuura and H. Imai, "Applying Fujisaki-Okamoto to Identity-Based Encryption," in *Applied Algebra,*

Algebraic Algorithms and Error-Correcting Codes -16, LNCS 3857, Vol. 3857, pp 183-192, 2006.

[9] P. Nicopolitidis, M. S. Obaidat, G. I. Papadimitriou and A. S. Pomportsis, *Wireless Networks*, First Edition, John Wiley & Sons, 2003

[10] D. K. Kim and D. K. Sung,"Characterization of Soft Handoff in CDMA Systems," in the proceedings of *IEEE Transactions on Vehicular Technology*, Vol. 48, No. 4, pp. 1195-1202, July 1999.

[11] M. Stemm and R. H. Katz,"Vertical handoffs in wireless overlay networks," *Mobile Networks and Applications 3*, Vol. 3, pp. 335–350, 1998.

[12] M. D. Yacoub, "Wireless technology: Protocols, Standards and Techniques," First Edition, CRC Press LLC, 2002.

[13] C. W. Lee, L. M. Chen, M. C. Chen and Y. S. Sun, "A Framework of Handoffs in Wireless Overlay Networks Based on Mobile IPv6," in the proceedings of *IEEE Journal on Selected Areas in Communications*, Vol. 23, pp. 2118 - 2128, November 2005.

[14] A. Hasswa, N. Nasser and H. Hassanein, "Generic Vertical Handoff Decision Function for Heterogeneous Wireless Networks," *Wireless and Optical Communications Networks,* pp. 239-243, March 2005.

[15] Z. Yan, H. Zhou, H. Zhang, J. Guan and S. Zhang, "An Adaptive Multi-criteria Vertical Handover Framework for Heterogeneous Networks," *The International Conference on Mobile Technology, Applications & Systems*, September, 2008.

[16] W. Shen and Q-A. Zeng, "Two Novel Resource Management Schemes for

Integrated Wireless Networks," *Journal of Networks,* Vol. 2, Pages 78-86, September 2007.

[17] D. P. Agrawal and Q-A. Zeng, "Introduction to Wireless and Mobile Systems," *2nd Edition, published by Thomson*, 498 pages, ISBN 0534-49303-3, 2006.

[18] J. Jeong and Z. J. Haas, "An integrated security framework for open wireless networking architecture," in the proceedings of *IEEE Wireless Communications*, Vol. 14, pp. 10-18, April 2007.

[19] K. G. Paterson and S. Srinivasan,"Security and Anonymity of Identity-Based Encryption with Multiple Trusted Authorities," *Lecture Notes in Computer Science*, Vol. 5209, 2008

[20] W. Shen and Q-A. Zeng, "A Novel Decision Strategy of Vertical Handoff in Overlay Wireless Networks," in the proceedings of *Fifth IEEE International Symposium on Network Computing and Applications*, p.227-230, July 2006

[21] J. Arkko and H. Haverinen,"Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," *RFC 4187, IETF*, January 2006.

[22] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz , "Extensible Authentication Protocol(EAP)," *RFC 3748, IETF*, June 2004.

[23] F. Bersani and H. Tschofenig,"The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method," *RFC 4764, IETF*, January 2007.

[24] S. Bhavsar,“Wlan-cellular integration for mobile data networks,” *CNSR 2003 Conference*, pp.126-127, May 2003.

[25] M.M. Matalgah,, J. Qaddour, A. Sharma, K. Sheikh ,“Throughput and spectral efficiency analysis in 3G FDD WCDMA cellular systems,” Proceedings of the *IEEE Global Telecommunications Conference*, Vol. 6, pp. 3423 – 3426, Dec. 2003.

[26] 3GPP TR 22.934,“Feasibility study on 3GPP system to wireless local are network (WLAN) networking,” v.1.0.0.0, Release 6, Feb. 2002.

[27] A. K. Salkintzis, C. Fors and R. Pazhyannur,"WLAN-GPRS Integration for Next-Generation Mobile Data Networks," in the proceedings of *IEEE Wireless Communications*, pp. 12-124, Oct 2002

[28] E. Wu, Y. Huang and J. Chiang,"Dynamic Adaptive Routing for Heterogeneous Wireless Network,” issued in the proceedings of *IEEE Globecom 2001*, Vol. 6, pp. 3608-3612, November 2001.

[29] A. Shamir, “Identity-based cryptosystems and signature schemes", in *Advances in Cryptology, Lecture Notes in Computer Science*, Vol. 196, pp. 47-53, 1984.

[30] M. S. Bargh, R. J. Hulsebosch, E. H. Eertink, A. Prasad, H. Wang and P. Schoo, “Fast authentication methods for handovers between IEEE 802.11 wireless LANs ,” in proceedings of the *2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, pp. 51-60, 2004.

[31] Jahan Hassan, Harsha Sirisena and Björn Landfeldt," Trust-Based Fast Authentication for Multiowner Wireless Networks," in the proceedings of *IEEE Transactions on Mobile Computing*, Vol. 7, pp. 247-261, 2008.

[32] Y. Park and T. Park, "A Survey of Security Threats on 4G Networks," in the proceedings of *IEEE GLOBECOM Workshop on Security and Privacy in 4G Networks,* pp. 1-6, Nov. 2007.

[33] Y. Sun, W. Trappe and K. J. R. Liu, "A Scalable Multicast Key Management Scheme for Heterogeneous Wireless Networks", in the proceedings of *IEEE/ACM Transactions on Networking*, vol. 12, pp. 653-666, August 2004.

[34] R. Muraleedharan and L. A. Osadciw, "Increasing QoS and security in 4G networks using cognitive intelligence," in the proceedings of *IEEE Globecom Workshops*, pp. 1-6, November 2007.

[35] Y. Zhang, "Handbook of Research on Wireless Security," *Published by Idea Group Inc (IGI)*, 2008.

[36] A. Mishra, M. Shin, W. Arbaugh, I. Lee, and K. Jang, "Proactive Key Distribution to support fast and secure roaming", in the proceedings of *IEEE 802.11 Working Group, IEEE 802.11-03/084r1-I*, Vol. 43, pp. 665 – 676, January 2003.

[37] S. Hussain, F. Kausar, A. Masood, "An efficient key distribution scheme for heterogeneous sensor networks," in the proceedings of *International Conference On Communications And Mobile Computing*, pp. 388 – 392, Hawaii, USA, November 2007.

[38] H. Chen, M. Zivkovic, and D.-J. Plas, “Transparent end-user authentication across heterogeneous wireless networks,” in the *proceedings of the 58th IEEE Vehicular Technology Conference (VTC '03)*,Vol. 3, pp. 2088–2092, Orlando, USA, October 2003.

[39] 3rd Generation Partnership Project, "3GPP TS 23.048 Security Mechanisms for the (U)SIM application toolkit; Stage 2(Release 5)," *3GPP*, September, 2002.

[40] Z. Fu and J. C. Strassner, “Access Control and Authentication for Converged Wireless Networks,” in the proceedings of *Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, pp. 1-8, San Jose, CA, July 2006.

[41] P. Xu, J. Liao, X. Wen and X. Zhu, “Optimized Integrated Registration Procedure of Mobile IP and SIP with AAA Operations,” in the proceedings of the *20th International Conference on Advanced Information Networking and Applications*, Vol. 1, pp. 926-931, April 2006.

[42] C. Perkins, “IP Mobility Support for IPv4,” *RFC 3344*, August 2002.

[43] H. Schulzrinne and E. Wedlund, “Application-layer mobility using SIP,” in the proceedings of the *SIGMOBILE Mobile Computing and Communications Review*, Vol. 4, pp. 47-57, July 2000.

[44] R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, “ in the proceeding of the *Communications of the ACM*, Vol. 27, pp. 120–126, February 1978.

[45] “Data Encryption Standard (DES),” Federal Information Processing Standard Publication 46-2, December 1993.

[46] “Specification for the Advanced Encryption Standard (AES),” *Federal Information Processing Standards Publication 197*, November 2001.

[47] M. J. B. Robshaw, “Security estimates for 512-bit RSA, ” in the proceedings of *the WESCON'95 Conference Record*, pp. 409–412, November 1995.

[48] Y. Xiao, B. Sun and H. Chen, “Performance Analysis of Advanced Encryption Standard (AES), ” in the proceedings of the *IEEE GLOBECOM ’06* , pp. 1 – 5, November 2006.

[49] The Keyed-Hash Message Authentication Code (HMAC), *Federal Information Processing Standards Publication 198*, March 2002.

[50] H. E. Michail, A. P. Kakarountas, A. Milidonis, and C.E. Goutis, "Efficient Implementation of the Keyed-Hash Message Authentication Code (HMAC) using the SHA-1 Hash Function," in the proceedings of the *IEEE International Conference on Electronics, Circuits and Systems* (ICECS 2004), pp. 567-570, December 2004.

[51] R. Rivest, “IP The MD5 Message-Digest Algorithm,” *RFC 1321*, April 1992.

[52] R. Rivest, “IP Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA),” *RFC 3310*, September 2002.

[53] P. Eronen and H. Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", *RFC 4279*, December 2005.

[54] M. Long, C.-H. Wu, and J. D. Irwin, “Localized authentication for wireless LAN Internetwork roaming, ” in the p*roceedings of IEEE Wireless Communications and Networking Conference*, Atlanta, GA USA, March 2004.

[55] G. Lawton, “Machine-to-Machine Technology Gears Up for Growth”, *Computer*, Vol. 37, pp. 12-15, September 2004.

[56] “Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications (PHY)”, *IEEE Std. 802.11*, June 1997.