PERFORMANCE ANALYSIS OF SECURITY MECHANISM DURING HANDOFF IN MOBILE IP

A Thesis by

Anant Shah

Bachelor's of Electronics and Communications Engineering

JBIET, Hyderabad 2005

Submitted to the Department of Electrical and Computer Engineering
and the faculty of the Graduate School of
Wichita State University
in partial fulfillment of
the requirements for the degree of
Master of Science

December 2007

PERFOMANCE ANALYSIS OF SECURITY MECHANISM DURING HANDOFF IN MOBILE IP

I have examined the final copy of this thesis for form and content, and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science with a major in Electrical and Computer Engineering.

_____
Ravi Pendse, Committee Chair

We have read this thesis and recommend its acceptance:

_____
Kamesh Namuduri, Committee Member

_____
Krishna Krishnan, Committee Member

DEDICATION

This thesis is dedicated to my beloved parents, all my family members and friends who have supported and encouraged me throughout my life. Without their support and encouragement this thesis would not be a success.

ACKNOWLEDGEMENTS

My stay at Wichita State University has been learning and fun filled experience. In these two years that I have spent here, I have grown both professional and personally. I am indebted to a number of people for making this possible.

I would like to thank my advisor, Dr. Ravi Pendse, for all his support and valuable guidance over the entire course of my academic career at WSU and for giving me an opportunity to do my Master's thesis under his guidance in the field of Mobile IP. I am thankful to my committee for taking the time to work with me in this endeavor.

I would also like to thank Nagaraja Thanthry, Amarnath Jasti and Vijay Ragothaman and all my friends at the Advanced Networking Research Center (ANRC) at Wichita State University for their help they have given me during this time.

Finally, I am forever indebted to my parents and family for supporting and encouraging me throughout my life to achieve higher goals.

ABSTRACT

With the advent of wireless devices, such as PDA, palmtops, the demand for staying connected to the internet have steadily increased. The traditional TCP/IP stack does not have support for mobility. In order to address these demands, Mobile IP protocol was proposed, which has support for mobility. With Mobile IP protocol, one can stay connected to the internet while they are moving. As the mobile node moves from one network to another, it undergoes handoff in order to register with new network. The traditional Mobile IP protocol does have built in support for security. Hence external security mechanisms such as IPSEC, AAA are used in order to address the security issues during handoff in Mobile IP. These security mechanisms introduce further delay during the handoff.

This thesis focuses on addressing the delay introduced due to security mechanism during handoff in Mobile IP. This research is based on development of algorithm for securing the communication between the mobile node and the home network and also by reducing the delay associated during handoff. The main idea behind this algorithm is to use the key exchange server at the home agent and generate the subset of keys which are then used by different foreign agents to register the mobile node with the home network. In the proposed algorithm, wireless sensor networks are used to detect the movement of mobile node and inform to the respective mobility agents. Then the mobility agents and home network exchange the information and when the mobile node moves to the new network, it registers using the key generated previously. In this research, the effects of various parameters such as burst in traffic, different security mechanism have been studied. All the simulation in this research work was carried out using MATLAB and

different parameters such as registration cost, handoff cost and movement cost have been studied and compared to that of previous proposed schemes.

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont.)

Chapter Page

LIST OF FIGURES

LIST OF FIGURES (Cont.)

LIST OF ACRONYMS

USAF ..... United States Air Force

ARPANET ..... American Research Project Agency Network

TCP ..... Transmission Control Protocol

IP ..... Internet Protocol

NSF ..... National Science Foundation

NSFET ..... National Science Foundation Network

PDA ..... Personal Digital Assistant

IETF ..... Internet Engineer Task Force

HA ..... Home Agent

MN ..... Mobile Node

FA ..... Foreign Agent

IPSEC ..... Internet protocol c

IKE ..... Internet Key Exchange

COA ..... Care of Address

CN ..... Correspondent Node

ICMP ..... Internet Control Message Protocol

NEMO ..... Network Mobility

PAN ..... Personal Area Networks

BET ..... Bi directional Tunnel

WSN ..... Wireless Sensor Network

STUN ..... Scalable Tracking Using Sensor Networks

DES ..... Data Encryption

LIST OF ACRONYMS (Cont.)

AES ..... Advance Encryption Standard

RSA..... Rivest, Shamir and Adleman

NMAD ..... New Mobility Agent Determination

QOS..... Quality Of service

AAA..... Authentication, Authorization, and Accounting

AAAH..... Authentication, Authorization, and Accounting Home

AAAF.....Authentication, Authorization, and Accounting Foreign

ACK ..... Acknowledgement

oFA ..... Old Foreign Agent

nFA .....New Foreign Network

CHAPTER 1

INTRODUCTION

1.1 Background

It all started way back in the 1960's when RAND PAUL BARAN of RAND Corporation was commissioned by the United States Air Force (USAF) to do a study on how they could maintain command and control over their Missiles. He tried many proposals but finally came out with proposal of packet switched network which started the revolution of the 19th century and was the basis for successful implementation of networks [2]. Though American Research Project Agency Network (ARPANET) was using Transmission Control Protocol/Internet Protocol (TCP/IP) [3] for data transmission the speed was very slow and only a limited amount of data could be transferred. In 1984 the National Science Foundation (NSF) created NSFET, a network using Transmission Control Protocol/Internet Protocol (TCP/IP) [2] which was able to transfer the data at rapid rate and was able to connect many super computers, while doing this it connected almost a total of 170 Local Area Network (LAN).For a while the speed at which data was transferring was good but as the number of users increased the speed decreased. In order to cope up with the increasing demand and the need for speed, in 1988 National Science Foundation (NSF) contracted with MERIT, a non-profit group of eleven Michigan University's to build a much faster national network whose speed was T1 (1.44 Mega bytes per second) and which could be used for connecting 16 cities across the United States. After expanding its network by connecting several schools and universities it became the largest 'Internet' in the United States. This was the reason for the closure of the American Research Project Agency Network (ARPANET) [4].

Wireless computing is rapidly developing over the years. This is due to technological advances in wireless data communications devices such as laptops, palmtops and personal digital assistants (PDA's). When mobility and the internet come together, the criteria to stay connected becomes the main focus. Routing packets correctly to a mobile destination is a concern as IP assumes a network to be static and there is no mobility support in a traditional TCP/IP stack [5]. As mobile computing has become a reality, new technologies and protocols have been developed to provide mobile users the services that already exist for non-mobile users. Mobile IP [5] is the solution to overcome the complications faced by IP to support mobility. Standardized by IETF (Internet Engineering Task Force), Mobile IP, enables a node to change its point of attachment to the internet in a manner transparent to applications running on top of the protocol stack. It has three basic entities: Home Agent (HA), Mobile Node (MN) and Foreign Agent (FA).The concept of Mobile IP is further explained in detail in Chapter 2. One downside to the Mobile IP is handoffs which may possible introduce latency and packet loss that are not desired for delay sensitive and real time applications. This can be reduced using registration schemes. In addition security is important while using mobile IP as wireless communication as it is inherently less secure than wired communication. Transmissions are sent "out in the open" where they can be intercepted. In mobile IP, with a traditional security mechanism, such as IPSEC, due to increase in the delay, real time traffic is bound to be effected specifically during hand off.

1.2 Problem Statement.

When the MN is moving from a Home Network to the Foreign Network, MN has to register with the Home Agent in order for it to route a packet properly to the MN. This

process is generally referred to as Handoff and is associated with some latency. Due to this latency, few packets are lost and are highly un-acceptable in the real time scenario. In order to overcome this situation, pre-handoff scheme is used where the movement of Mobile Node is detected and the packets dropped due to hand off are reduced. But while using the pre-handoff mechanism, as the MN is moving from one FA to another, security is an important aspect that needs to be considered.

With Traditional security mechanisms such as IPSec and IKE there will be increases in the delay and also reduces the throughput by 70% when compared to the cases where IKE is used. Also the key negotiation and generation as required by IKE imposes a significant penalty to the throughput. An average of 10 seconds of inactivity periods occurs in each hand-off due to the key generation and TCP's congestion avoidance mechanisms.

The other work around for such issues is the use of key exchange servers at the home network and foreign network, which allows exchange of keys with Mobile Node as well as foreign agent and home agent. With this workaround there is a decrease in the delay but the throughput does not decrease significantly and also few security vulnerabilities arise as the key exchange server may not be legitimate and some one could spoof a packet to get the whole network topology.

Another ID based security mechanism was proposed for reducing the throughput caused by the server model. Based on the public key cryptography, this mechanism guarantees a higher level of security than the basic server mechanism and has reduced registration time compared to the server based mechanism. With this model the delay in the registration process is reduced by 63%.However due to heavy operations of public key cryptography, it takes a bit more time than the basic server method.

1.3 Goals

Security is one of the important feature that needs to be considered. Traditional security mechanisms such as IPSEC do provide basic security but do not prevent attacks such as man in the middle, eaves dropping etc. This thesis focuses on using different security mechanism as opposed to the standard security mechanisms such as IPSEC, to provide a higher level of security while reducing the number of packet loss. The proposed solution should be scalable such that it can be implemented on large scale networks, even on existing Mobile IP infrastructure.

1.4 Organization of Thesis

The organization of the remainder of this thesis is as follows: Chapter 2 provides the overview of Mobile IP and network mobility. It also highlights the previous work done. Chapter 3 describes the use of wireless sensors. A mathematical explanation is provided for the fast-handoff method. Chapter 4 presents an analytical model built for the existing and proposed schemes. Chapter 5 contains simulations to compare the performance of various schemes by varying various parameters. Chapter 6 provides conclusions and future work.

CHAPTER – 2

LITERATURE REVIEW

2.1 Introduction to Mobile IP

Mobile IP [5] provides an efficient and scalable mechanism to move within the internet. Normal routing protocols cannot support mobility since the IPv4 address can identify only the network interface which identifies the physical location of the Mobile Node. But as the Mobile Node moves from one domain to another domain its IP address is changed or renewed. In recent years, the IETF has standardized many protocols to (solve this mobility problem) to support the mobility. Using mobile IP, nodes may change their point of attachment without changing their IP address. This allows the MN to maintain connection with the Home Network even when they are in the FN. Mobile Node is associated with a long term IP address when it is at the home network [6]. As it moves away from home network it is associated with a care-of address (COA) which indicates its current location which enables routing of packets from HA to MN. So, with these two IP addresses and their association, the MN always maintains a connection to the internet. Now the MN is reachable at a fixed IP address irrespective of its current point of attachment. When the MN moves away from its Home Network, a tunnel is created between Home Agent (HA) and Foreign Agent (FA) in order to forward packets from Home Network to Foreign Network [6]. For this Internet Engineering Task Force defines some terminologies i) Home Agent, ii) Foreign Agent and iii) Mobile client, iv)Agent advertisement v) COA, vi) Correspondent Node. Mobile IP refers the Home Agent and Foreign Agent as mobility agents.

Figure 2.1 shows a MN being in HA and is attached to the HA. As the MN moves to a new Network (Foreign Network), the MN registers with its corresponding HA with the new COA. When a CN sends a packet destined to the MN, it is first intercepted by the HA .The HA then encapsulates the existing IP packet with the MN's COA. The MN's COA would then be the destination address and would forward it to the FA. This process of adding the new IP header to the already existing IP header is called tunneling. By default IP in IP tunneling is used, but few other tunneling methods such as GRE and minimal encapsulation can also be used. The FA upon receiving the packet strips of the COA header and passes the packet to the MN with the original IP header as sent by CN. Figure 2.2 shows MN which is in FA is connected via tunnel to the HA.

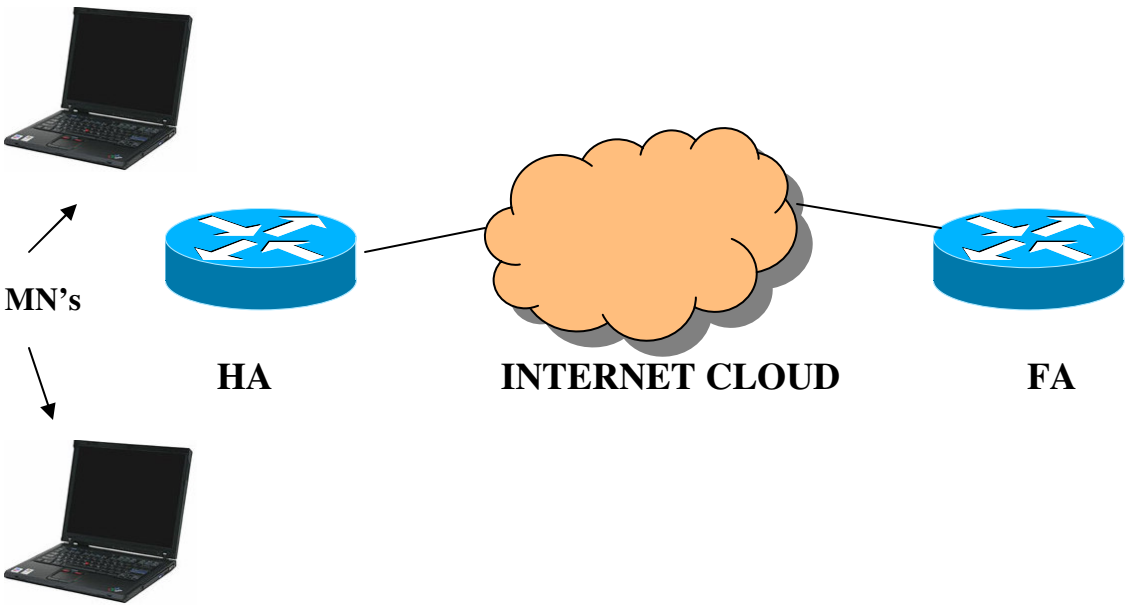

Figure 2.1: Mobile Node in Home Network and attached to the HA.

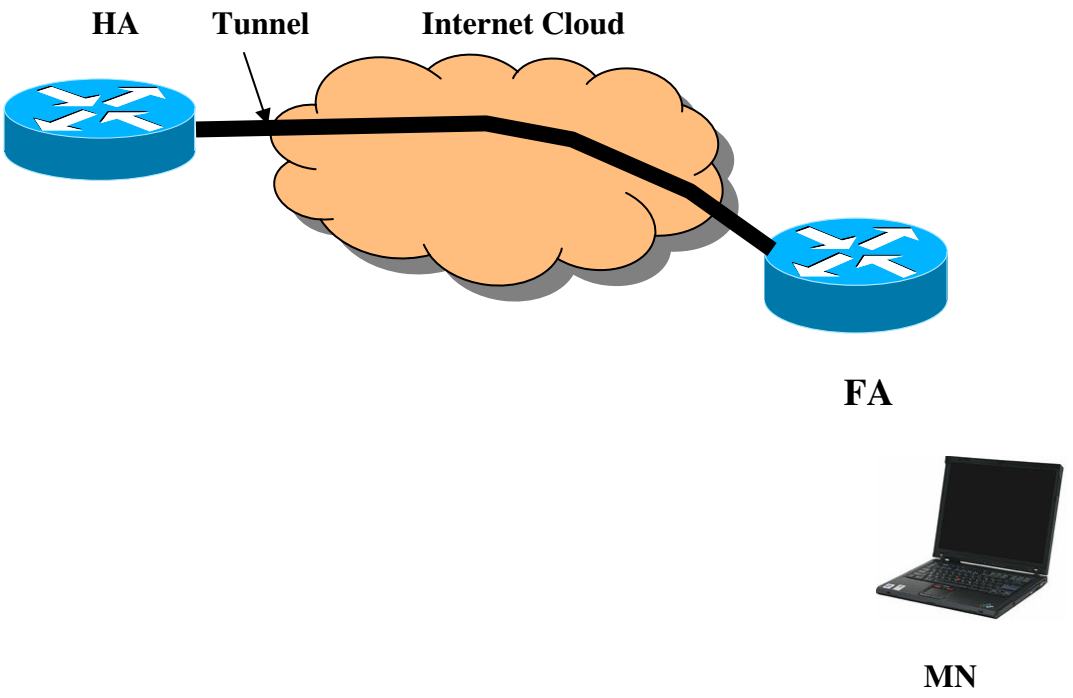

Figure 2.2: Mobile Node in Foreign Network and attached to the FA.

2.1.1 Home Agent [6].

A router on a Mobile Node's home network which delivers datagram's to departed Mobile Nodes and maintains current location information for each. While the Mobile Node is away from home, the Home Agent intercepts packets on the home link destined to the Mobile Node's address, encapsulates them, and tunnels them to the Mobile Node's registered care-of address.

2.1.2 Foreign Agent [6].

A router on a Mobile Mode's visited network which cooperates with the Home Agent to complete the delivery of datagram's to the Mobile Node while it is away from home.

2.1.3 Mobile Node [6].

A host or router that changes its point of attachment from one network or sub network to another, without changing its IP address.

2.1.4 Agent Advertisement [6].

Foreign agents advertise their presence by using a special message, which is constructed by attaching a special extension to a router advertisement.

2.1.5 Care-of Address [6].

An IP address associated with a Mobile Node while visiting a foreign link; the subnet prefix of this IP address is a foreign subnet prefix. Among the multiple care-of addresses that a Mobile Node may have at a time (e.g., with different subnet prefixes), the one registered with the Mobile Node's Home Agent is called its "primary" care-of address.

2.1.6 Mobility security association

A collection of security contexts between a pair of nodes that may be applied to mobile IP protocol messages exchanged between them. Each context indicates an authentication algorithm and mode (as described in the fourth section), a secret (a shared key, or appropriate public/private key pair), and a style of replay protection in use.

2.2 Mechanism in Mobile IP [6].

Mobile IP mechanism can be explained in three steps:

2.2.1 Discovering COA [6].

When the MN moves from its home network to a new network, HA has to know about this movement. HA's and FA's broadcast the agent advertisements at some intervals to publicize their presence or MN solicits for an agent advertisement. This is similar to ICMP router discovery. These agent advertisements are to inform about the special features they can offer to MN and to discover a connection to HA or FA. The MN solicitations are answered by the HA or FA. The MN detects its movement by two methods. First, it depends on the lifetime expiry method. Here, if the MN does not detect any new agent advertisement within the lifetime expiration, it detects that it has moved.

RFC 3344 states: "If advertisements are sent periodically, the nominal interval between the advertisements should be no longer than 1/3 of the advertisement lifetime given in ICMP header. This interval may be shorter than 1/3 also but allows Mobile Node to miss three successive advertisements before deleting the agent from its list of valid agents…"

Secondly, it depends on prefix extensions but here all the mobility agents have to send this extension with their advertisements [7]. When the MN receives an agent advertisement with a new prefix extension, it detects that it has moved to new network. To achieve this, the HA and FA must send their prefix extension in the advertisement or else the algorithm will not work.

In this way MN detects its movement and receives its new COA in the agent advertisement of FA.

2.2.2 Registering COA [6].

After the MN receives a new COA, it has to register this address with HA. This registering is done in two different ways.

- Care-Of-Address (COA).
- Co-located Care-of-Address (CI-COA).

In the case of COA, the MN connects to the HA using the functionality of Foreign Agent. The HA is associated with the MN and the COA till the lifetime expires. This association of HA and MN with COA is called binding. The advantage of COA is that it can be unregistered when it returns to Home Network and this COA can be used by another MN. So all the Mobile Nodes in a foreign network can share the same care-of-address and thus save IP addresses. Here, the MN requests the HA for registration remotely and thus security plays an important role so that no spoofing takes place in between. To ensure that each request is unique, some identification fields change in the registration request packet with each request. When the 'S' bit is set, the MN is requesting not to delete the prior mobility binding(s) which is called simultaneous binding. If 'B' is set, it indicates to the HA to send all the data packets it intercepts within the home network. With the 'D' bit set MN indicates that it is using co-located COA and can decapsulate the packets on its own. If the 'T' bit is set, it requests for reverse tunneling [7] . Type field indicates whether it is a request or reply message. The FA is also responsible for authentication and registering the MN with the HA. Therefore, FA is also needed to employ security mechanisms to identify and deliver data packets.

The other way of registering the care-of-address is using co-located COA. This method is similar to the one above but here each MN is given a unique COA address by the DHCP server within the foreign network. The MN uses this address as long as it stays in the network to communicate with the HA. This co-located address also lets the MN to communicate directly with the corresponding node without the interference of the FA.

But here the Foreign Agent has to provide unique IP address for each MN in that network which is difficult with IPv4. This can be possible with IPv6.

2.2.3 Tunneling the data packets to COA [6[.

After the successful registration process, any packet destined to the MN reaches HA. But the packets have to reach the MN which is in foreign network. A mechanism is needed to correctly route the packets to the MN from corresponding node. Mobile IP provides a tunnel between HA and FA to deliver data packets to COA when the MN is away from HA. Tunneling is used to hide the MN address. When a packet reaches the HA with MN as a destination , HA adds a new IP header called tunnel header in which the source address is HA and destination address is the FA. In this way the HA encapsulates the data packet and sends to the FA. At FA, it decapsulate and sends to the MN. This encapsulation is called IP-within-IP encapsulation which is simple and generally used [8] . Alternatively, minimal encapsulation can be used as long as MN, HA and FA agrees to do so. Minimal encapsulations do not allow data fragmentation as with IP-within-IP encapsulation. The protocol number 55 in the encapsulating IP header field indicates the presence of minimal encapsulation. In this instead of encapsulating the whole packet into another packet, source and destination fields are replaced by encapsulating agent and COA of Mobile Node thereby reducing the header size compared to former method.

2.3 Network Mobility [9].

NEMO is a extension to mobile IP that allows mobility of an entire network as MNs. It is leaf network and does not transmit internet traffic. A mobile router (MR) is implemented in software on a network router such that the network router and entire

network moves while connected to the internet. In this we have bi-directional tunnel between HA and MR to deliver packets to nodes behind the MR. Examples of Network mobility are Personal Area Networks (PANs) and network inside vehicles. Here the QOS degrades since the additional headers due to tunneling.

2.4 Handoff

Handoff occurs each time a MN moves from its old mobile agent domain and associates itself with a new mobile agent (FA) in new domain. Mobile IP handoff delay is divided into two elements; one caused by movement detection and other caused during registration process.

Handoff delay = Movement detection delay + Registration delay…… (2.1)

When mobile IP described handoff first, layer2 (L2) handoff was not considered as it introduces latency. Moreover, the registration process itself is associated with some latency. In real-time, if HA and MN are far away a registration delay causes high transmission delays of about 6-9 ms per 1000 km [10]. If MN has to send data each time it moves to new point of attachment there would be high latency. Handoff latencies affect the service quality of real-time applications for mobile users. .

Many different techniques were proposed to perform fast and smooth handoffs. Some of them are described below. IEEE proposed three methods to reduce the handoff latency [11]. They are Pre-registration handoff, Post-registration handoff and combined registration handoff [12].

2.4.1 Pre-registration Handoff [11].

This method allows L3 handoff initiation before the L2 handoff to a new network. The old FA (oFA), to which the MN is attached solicits or listens to agent advertisement from the new FA (nFA), the network towards which the MN is moving and caches the information when it receives it. Now when the oFA receives a L2 trigger it sends to the MN (network initiation handoff) or the MN solicits for the information (Mobile Node initiated handoff). As soon as the MN receives the agent advertisement it detects that it has moved to new network. Then, it sends the registration request to that nFA with the 'S' bit set to indicate simultaneous binding. The nFA replies to MN through oFA or on its own link if handoff is over.

2.4.2 Post Registration Handoff [11].

This is network initiated handoff. This registration occurs after the layer2 handoff. Here, it defines a source trigger if the L2 trigger occurs at oFA, and a target trigger if L2 trigger occurs at nFA. Here the handoff request and reply messages are exchanged between the mobility agents. After this exchange a bi-directional edge tunnel (BET) is established between oFA and nFA. This tunnel is used to deliver packets from oFA to MN at nFA. Two signals, L2-NHC (Layer 2-Network Handoff Complete) and L2-MHC (Layer 2 –Mobile Handoff Complete) are used to indicate the completion of post-registration process. If the nFA receives a L2-NHC, it must send a router advertisement and if MN receives a L2-MHC, it must send a router solicitation message. In this fashion the mobile IP registration is performed.

2.4.3 Combined handoff [11].

This method first tries the pre-registration handoff when it is successful before the completion of MN's L2 handoff. If pre-registration does not complete before the expiration of the timer on any one of FAs, then post-registration takes over. The start of post-registration depends on the expiration timer on the FAs. The timer is started either at oFA following source trigger or at nFA following the target trigger. The timer should be set to a value that allows forwarding between oFA and nFA to occur before the MN completes the L2 handoff to nFA.

The handoff latency problem can be solved by using micro-mobility, a way to reduce the round trip delay. Cellular IP introduced this concept of micro-mobility. Mobile IP is a good solution for macro-mobility where the frequency is low. Cellular IP interworks with mobile IP to provide wide area mobility [13]. In Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) [14], mobility is kept transparent to MNs. Here the registration process is divided into two sections: one between MN and base station, other is between base station and HA.

2.5 Sensor Networks [15].

With the advancements in micro-electro mechanical systems (MEMS) technology, digital electronics and wireless communication, have enabled the development of low-transmission power, low cost, multifunctional devices that are small in size and can communicate untethered in short distance know as Sensor's. Sensors are devices with low power and have a wide variety of application. Sensor nodes are capable of sensing, data processing and components capable of communicating information. Since these

devices are used in various fields, their design and capabilities generally depend on their application. These devices have a limited amount of storage, computational capabilities and most importantly energy resources. These limitations introduce constraints in the design of MAC protocol.

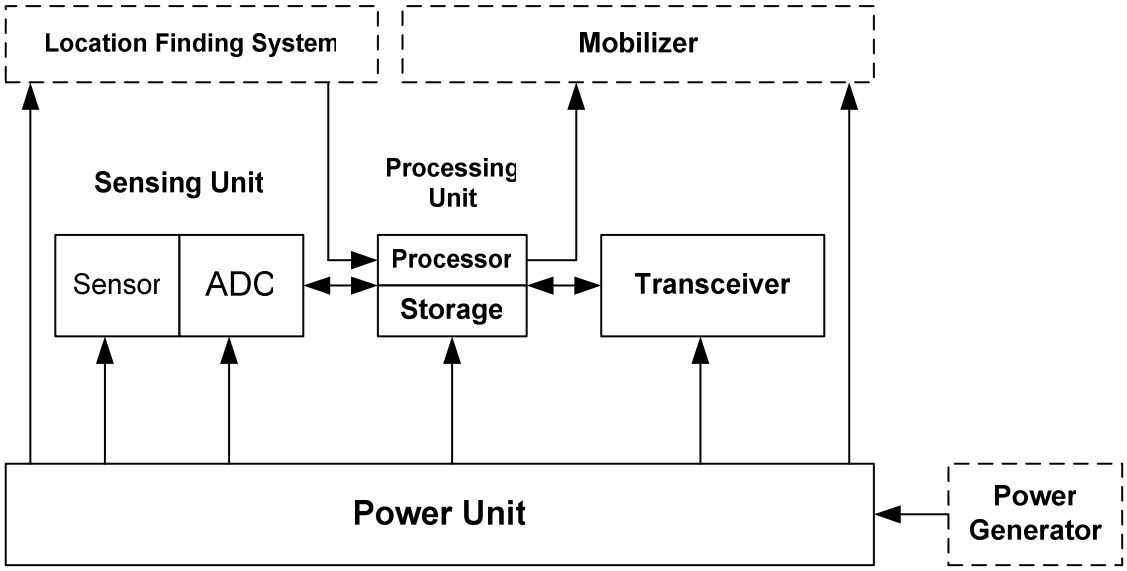

Figure 2.3: Components of Sensor Node.

A sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it .One of the significant advantages of using the sensor nodes is the low power consumption requirement. A sensor network could consist of several different types of sensors such as seismic, low sampling rate, thermal, visual, acoustic and radar which are able to monitor a wide variety of ambient conditions. Sensor networks are different from that of traditional networks and are more prone to failures. As a result the algorithms for sensor networks should be robust, stable and should work in the cases of node failures. A sensor node is

made up of four basic components: a sensing unit, a processing unit, transceiver unit and power unit as shown in the Figure 2.3. Sensor nodes pass the information to the end user through the micro-processors which is fitted onboard. The micro-processors process the information and pass it to the intermediate nodes which then pass the information to the end users [17]. Nodes in the wireless sensor networks synchronize with each other and pass the information successfully to the end user which results in hardly any loss of data.

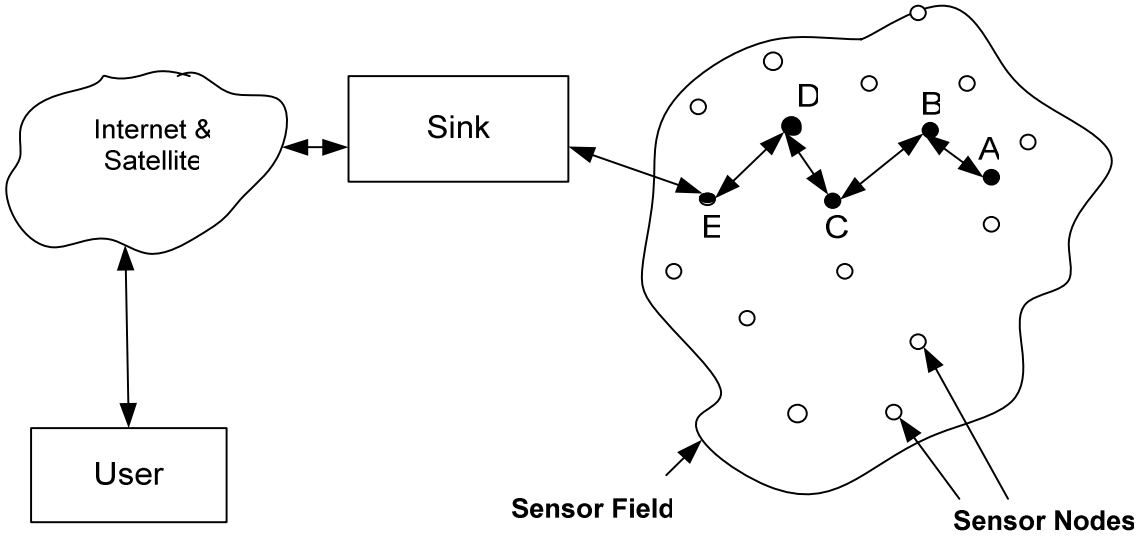

Figure 2.4: Communication architecture of sensor network.

Figure 2.4 shows the communication architecture of the sensor networks. Sensors nodes are usually scattered and are placed in the sensor network depending on their application. The nodes exchange information with each other. The nodes are connected to each other by wireless media such as radio or infrared. The information each node collects is then gathered and is sent to the sink. The sink then passes the information to the user via internet or satellite in appropriate format depending upon the user requirements as well as on the design of the application.

Figure 2.5 shows the protocol stack used by the sink and the sensor nodes. The protocol stack consists of: physical layer, data link layer, network layer, transport layer, application layer, task management plane, mobility management plane, power management plane. Robust modulation, transmission and receiving techniques are needs which are handled by the physical layer. As the Mobile Nodes are mobile, the MAC layer must be aware of power and must be able to minimize the collisions with neighbor's broadcast. The routing data supplied by the transport layer is properly routed by the routing layer. The transport layer is responsible for maintaining the data flow in the sensor networks depending on the application. Depending upon the application, different types of application software can be built and used on the application layer. Depending on the sensing task, few sensors nodes are required to perform the given task. The task management plane balances and schedules the sensing and forwarding task of the sensor nodes. The mobility plane is responsible for mobility management and movement pattern for sensor nodes. The power management plane which combines power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium, and promotes cooperative of sensor networks. It also manages the utilization of power used by the sensor nodes. These sensor nodes can automatically turn off them selves when not in use. As the sensor nodes are inexpensive, they can be deployed in large numbers.

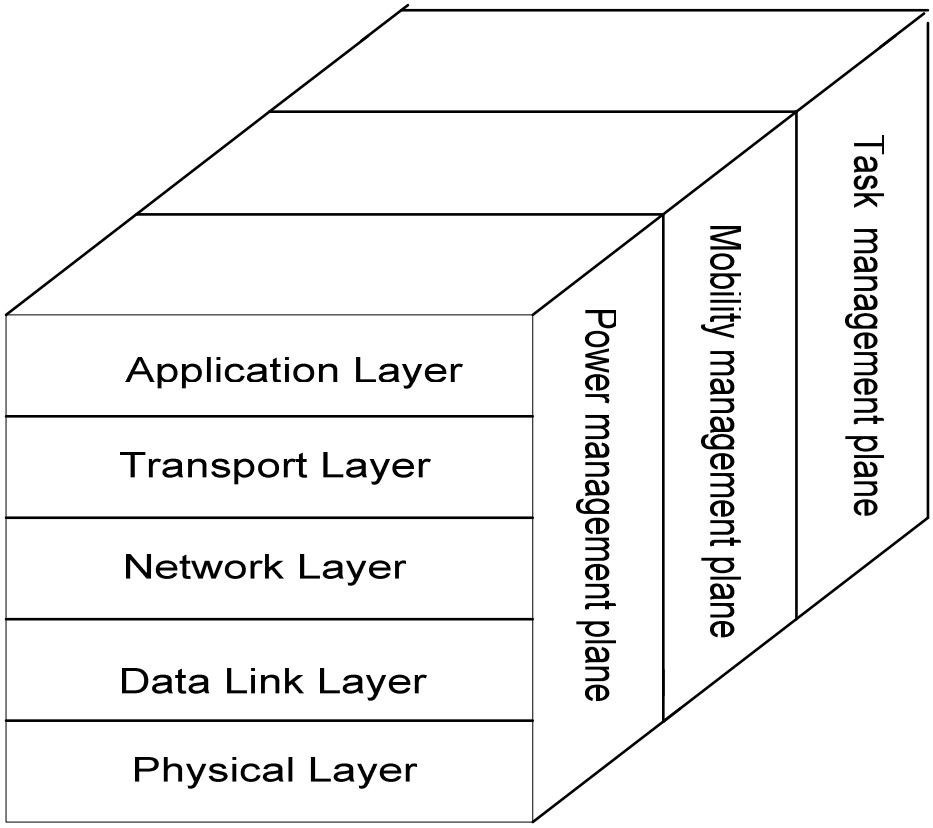

Figure 2.5: Protocol stack of the sensor network

2.5.1 Wireless sensor network [17].

Wireless Sensor Network (WSN) is a network made of numerous small independent sensor nodes. Wireless Sensor Networks can be used in the tracking of objects such as vehicles. Such networks are being used in mobile telephony encompassing military fleet tracking, environmental and commercial areas. Border sensors sense incoming and outgoing objects, while non-border sensors sleep when no movement occurs inside the region. Each application introduces a unique set of goals and requirements and produces a different type of traffic. The small form factor of sensor

nodes imposes severe constraints on the availability of resources, such as power, memory, communication range, and sensing capability. Tracking consists of detecting and monitoring locations of real-world objects, possibly using several types of sensing such as acoustic, seismic, electromagnetic, etc. Figure below shows the architecture for wireless sensor network.

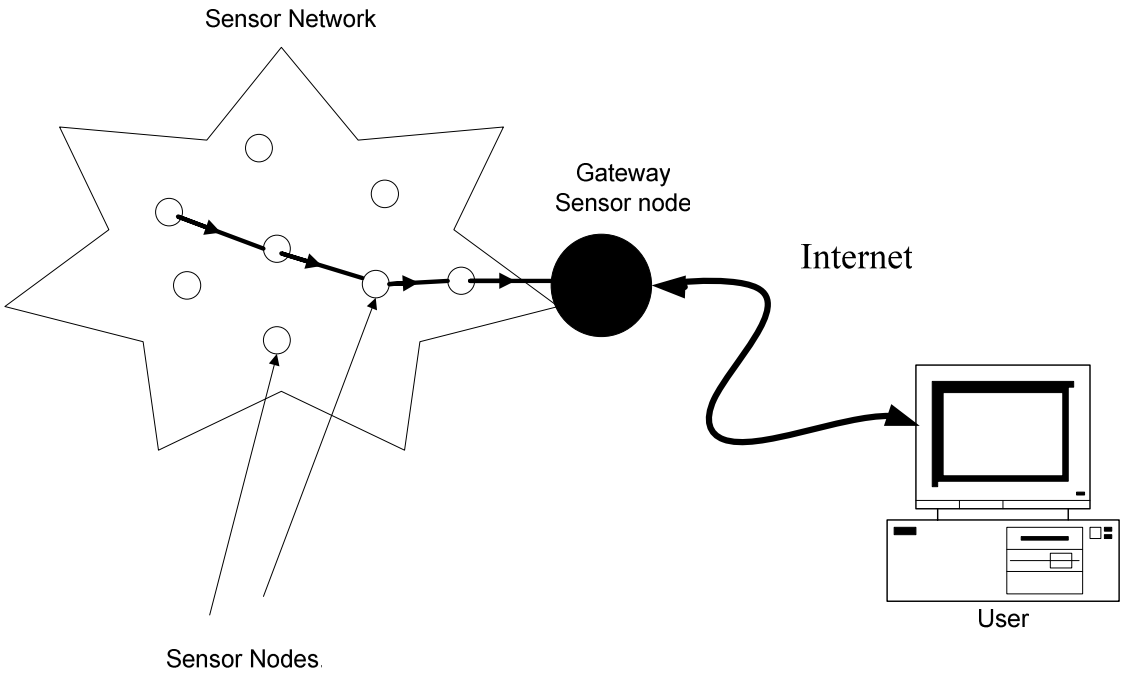

Figure 2.6: Communication architecture of a wireless sensor network

2.6 STUN

In [18], the authors proposed a location tracking architecture know as Scalable Tracking using Sensor Network (STUN). STUN is a hierarchical structure of sensors to track objects. Tracking of objects involve detection and monitoring of Mobile Nodes. In this, sensors are used to inform mobility agents to inform about the movement of Mobile Nodes. STUN is capable of detecting large number of moving objects at once. The STUN is constructed in hierarchical structure assuming that the Mobile Nodes move in predefined manner based on some object's movement patterns [19]. In this pattern, sensors are connected in a tree like structure called hierarchical tree, where all the end

leaf nodes inform movement to intermediate node. The intermediate nodes inform the root node only if it observes a change in the mobile object position. Otherwise, the message is terminated. This reduces the redundant messages. This message pruning in the hierarchy is the key to reduce the communication cost.

Here the detected set of sensor at leaf nodes consist of the objects within the range of detection but the root node's detection set consists of all the objects in the region. The main purpose of maintaining the detected sets is to allow efficient querying.

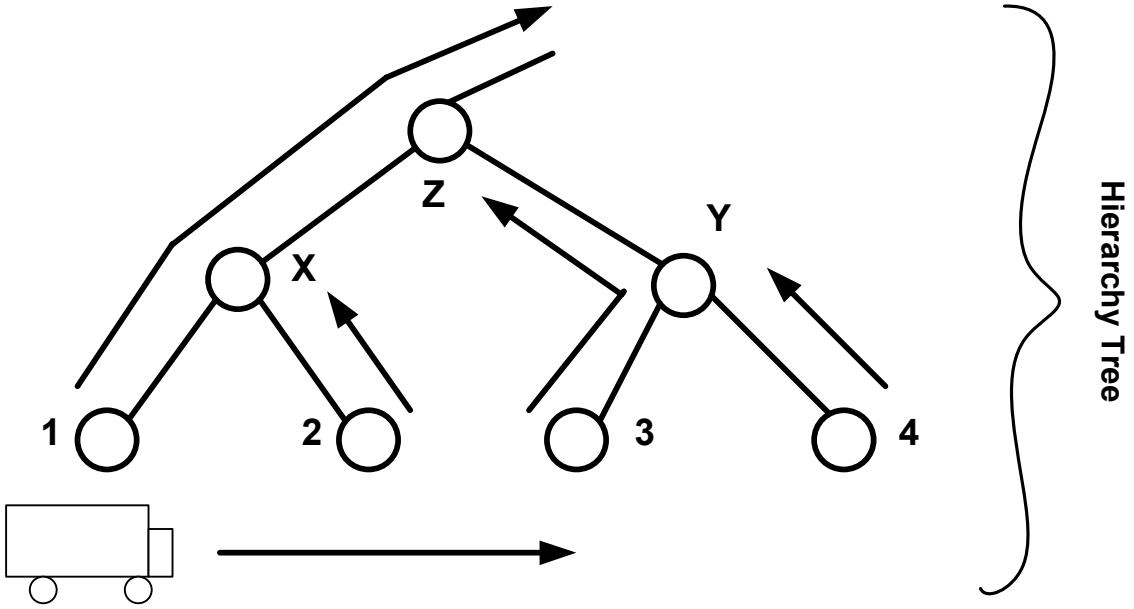

Figure 2.7: Stun Architecture for movement detection

The Figure 2.7 shows the architecture of STUN. As shown in the Figure the sensors are in a tree structure and the Mobile Node is a vehicle. X and Y are intermediate nodes which send messages to root node Z. Nodes 1, 2, 3, and 4 are leaf nodes that detect the Mobile Node movement. These are offspring of root node Z in the hierarchy. As the vehicle moves through the region covered by the sensor nodes, detection messages are generated and are sent to the intermediate nodes in the hierarchy. Node 1 detects the

Mobile Node movement and informs this to X. X will then pass the message to Z which in turn propagates the signal to its root node. X adds this movement of the vehicle to its detection set. Any other message about the movement of the Mobile Node will not be added to the detection set and will not be sent to higher nodes in the hierarchy. Hence, if nodes detect a movement, they send a message to node X. But X does not add it to its detection set. So, by pruning messages, communication cost is reduced. In the same way, as the vehicle moves towards node 3 from node 2, node 3 detects this and informs to its intermediate node Y. Y adds this to its detection set but does not add it when the message comes from node 4. When Z hears from node Y, it prunes the message and does not modify its detected set.

2.7 Various Encryption Techniques [27].

We use "security" in many ways in our daily lives ranging from physical security to computer security. Security plays an important role in the world of computer society. When considering computer security, we need to address three important aspects: Confidentiality, Integrity and Availability.

- *Confidentiality [20]* ensures that information is accessible only to those authorized to have access as defined by ISO. Confidentiality is sometimes referred to as secrecy or privacy.
- *Integrity [20]* refers to the where the data can be modified only by authorized personnel or by authorize ways. Data integrity is having assurance that the information has not been altered in transmission, while transmitting from source to destination.

- *Availability [20]* means that the data is accessible to authorize persons at appropriate times. It ensures that information or resources are available when required.

Various security techniques have been designed to address these issues.

2.7.1 Substitution Cipher [27].

The first cipher to develop was the substitution cipher which works on the simple substitution procedure. Various kinds of substitution ciphers are listed below.

2.7.1.1 The Caesar Cipher [27].

The Caesar cipher was the first to use the substitution scheme and plays an important role in history. Julian Caesar was first to use this scheme. In this, each letter is translated to a letter a fixed number of places in the alphabet. The advantages of using this cipher is, it is very easy to perform and is not complicated. The major disadvantage is as it is very simple it was easy to decode. Also its pattern was a major concern.

2.7.1.2 Other Substitutions [27].

In other substitutions, the alphabet is scrambled and each plain letter maps to a unique cipher text. Mathematically the scheme is "Permutation is re-ordering of the elements of sequence". An example for other substitutions cipher is poem code. The disadvantages of these were that they were very easy to break.

2.7.1.3 The Vernam Cipher [27].

The Vernam cipher is a type of one time pad devised by Gilbert Vernam. The cipher is immune to most cryptanalytic attacks. The technique involves using encryption where an arbitrarily long non repeating sequence of numbers is combined with the plain text. The sequence of random numbers is not repeated. As long as the key does not repeat or is not used, the cipher is immune to the attack. The Advantage of using this scheme is, as it uses random number, it was immune to attacks .The disadvantage of this systems is, if the key is re-used, it might be prone to attacks as it could then be very easy to break.

2.7.1.4 Book Ciphers [27].

In this method, the random number is any book, piece of music or other object which the structure can be analyzed. Both the sender and the receiver must access the same object. In this scheme, the key is formed from the letter of the text in the order provided by any book. The flaw of this scheme is neither the key nor the message is evenly distributed.

2.7.2 Transposition Cipher [27].

A transposition is an encryption where the letters of the message are rearranged .In this encryption method, attempt was to make it difficult for the attacker to determine how a message and key are transformed in cipher text. The main goal of this is to confuse the attacker. As transposition rearranges the symbol of message, it is also known as permutation.

2.7.2.1 Columnar Transposition [27].

Columnar Transposition is a re-arrangement of the characters of plain text into columns. The plain text characters are written in rows and are arranged one row after another. This algorithm requires a constant amount of work per character as the cipher involves no additional work beyond arranging the letters and reading them off again. Also, the time needed is proportional to the length of the message. The disadvantage of using this scheme is the storage needed and the delay involved in decrypting the cipher.

2.7.2.2 Other Transpositions [27].

In this, the characteristic patterns of pairs of adjacent letters called diagrams are used as compared with the characteristic letter. Letter pairs such as –re-, - th- -en- , etc appear very frequently. These frequencies of appearance of letter groups are used to match up the plaintext letters that have been divided in cipher text.

2.7.3 Various Encryption Algorithms [27].

Substitutions and transpositions can be considered as the building blocks of encryption. The above mentioned encryption techniques have been trivial. As the encryptions techniques were trivial, they are used for basic encryption and are fairly easy to break. An algorithm is said to be proficient if it can not only encrypt, but must be fairly difficult to break. So the above said techniques are not used any more rather, Standard algorithms are preferred. The algorithms that are popular in the commercial world are DES, AES, RSA, IPSEC etc.

2.7.3.1 Data Encryption standard (DES) [27].

The DES is a system developed by and for the U.S government and was selected as an official FIPS for the United States. DES is a careful and a complex archetypal block cipher algorithm that takes a fixed-length string of plaintext and transforms it through a series of complicated operations into another cipher text string of the same length. The algorithm is ran for total of 16 cycles and hence derives its strength from repeated application techniques, one on top of other. The algorithm begins by encrypting the plain text as block of 64 bits. DES uses a fixed key of length 56 bits to customize the transformation, so that the data can be decrypted only by the users who know the key that was used to encrypt. DES is now considered to be insecure for many applications chiefly due to the 56-bit key size being too small. DES keys have been broken in less than 24 hours [21]. The most practical attack to date is still the brute force approach. To address these issues double and triple DES have been proposed.

2.7.3.2 Double DES

The 56-bit key associated with the DES is no longer considered to be safe. Hence double DES is suggested to address the discomfort of the DES algorithm and to increase the secrecy. The double DES uses a 57 –bit key instead of the 56-bit used by DES. In Double DES, there are two keys instead of one when compared to DES. In theory two encryptions are performed, one on top of another. Hence, the difficulty in breaking the encryption is doubled. But in reality this is not the situation; the keys can be easily found by using a hashing algorithm. Hence, double DES is considered to be more unsafe than regular DES [21].

2.7.3.3 Triple DES [27].

Triple DES is a block cipher formed from the DES cipher by using it three times. TDES was chosen as a simple way to enlarge the key space without a need to switch to a new algorithm. That is, first encrypt with one key, decrypt with second and encrypt with first again [28]. This application of the DES algorithm three times doubles the effectiveness of the key length. The key length of 112 bits is quite strong and is effective against all feasible known attacks.

2.7.3.4 Advance Encryption Scheme (AES) [27].

AES is a block cipher adopted as an encryption standard. AES is fast in both software and hardware, is relatively easy to implement, and requires little memory. The AES algorithm uses one of three cipher strengths: a 128-, 192-, and 256-bit encryption key. Each encryption key size causes the algorithm to behave slightly differently thereby increasing the complexity of the cipher algorithm. This means that AES starts with a key more than double the size of DES key. AES is a substitution-permutation cipher involving *n* rounds that depends on the length [22]. AES is secure enough to protect the classified information up to the top secret level. With this algorithm, it is slightly faster to encrypt and decrypt data protected with 128 bit AES.

2.7.3.5 Rivest, Shamir and Adleman (RSA) [27].

RSA is a public key cryptography. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA involves a public key and a private key. Public key is known by everyone and used to encrypt the data. This encrypted data can only be decrypted using

the private key. The RSA encryption algorithm incorporates results from number theory, combined with the difficulty of determining the prime factors of a target. Using an RSA system, the identity of a sender can be identified as genuine without revealing his private code.

This algorithm uses two keys, one for encryption and the other for decryption[24]. A plaintext message P is encrypted to cipher text C using,

$$C = P^e \bmod n$$

And this is again recovered by

$$P = C^e \bmod n$$

Because of symmetry in modularity arithmetic, encryption and decryption are mutual inverses and commutative. RSA encryption and decryption is quite fast but not for many high speed network applications. Accordingly, it is often used to exchange a secret key.

2.7.4 Diffie-Hellman Algorithm [27].

Diffie-Hellman key exchange is a protocol that allows two groups to jointly establish a shared secret key with each other over an insecure communication channel [27]**.** In this, the two groups may not have any idea about each other. Each party chooses a large prime number and sends a number g raised to the power of the prime to the other [26]**.** The key exchange is very efficient and is considered secure against eavesdroppers if the two numbers are chosen properly. The secrets are discarded at the end of the session. Since the long term private keying material is not disclosed, the key exchange itself trivially achieves the secrecy. The key-exchange process is vulnerable to the man in the middle attack as the key exchange does not provide authentication of the parties. Some method to authenticate the parties is generally needed.

2.7.5 IPSEC [42].

IPSEC or 'Internetworking Protocol Security' is a suite of protocols that seamlessly integrate security features, such as authentication, integrity, and/or confidentiality, into IP. IPSEC was created to provide the access control, data confidentiality, data integrity, data origin authentication, and protection against replay functionality across the internet. It offers security service at the IP layer through Authentication Header (AH) and the Encapsulation Security Payload (ESP) protocols [43]. It is the probable long-term direction for tunnels and secure data transmission in general due to its (intended) interoperability and its evolution toward an internet standard. An IPSec tunnel will only transmit what its configuration specifies. This makes it considerably more complex to use than other types of tunnels. Using IPSec protocols, one can create an encrypted and/or authenticated communication path, depending upon the protocols used, between two peer sides. It has two modes of operation, transport mode and tunnel mode. In transport mode, IP payload is encrypted while the original headers are left intact, whereas in tunnel mode the entire IP packet is encrypted and becomes the payload of new IP packet.

IPSec is a standard for providing common means of authentication, integrity and confidentiality (IP encryption). It presents a way to protect sensitive data that travels across untrustworthy networks. With IPSec, data can be transmitted across a public network without fear of observation, modification, or spoofing. This enables applications such as virtual private networks (VPNs), including intranets and extranets. IPSec allows the creation of a secure tunnel between two security gateways or IPSec compliant routers. Intranets in separate geographic locations can be created across the internet. This concept

is commonly referred to as transferring data from trusted networks across an untrustworthy network.

In this Chapter the author starts with the explanation of working of basic mobile IP and then focuses on the handoff and the types of handoff. Also in this Chapter, the author tries to enlights about various security protocols and various encryption mechanisms.

CHAPTER - 3

Security Mechanism during Handoff in Mobile IP

In this Chapter the author describes the proposed algorithm which addresses the security issues during hand off in mobile IP. The tracking of Mobile Nodes using STUN is described first, then the issues with previous proposed algorithms and the proposed algorithm is described. In later sections the proposed algorithm is explained by considering an example network scenario and a mathematical explanation.

3.1 Using STUN for tracking movement of Mobile Nodes

When MN's starts moving from one network to another, STUN is used for tracking the direction of the MN. Figure 3.1 shows the connectivity between MN's, sensor networks and a mobility agent.

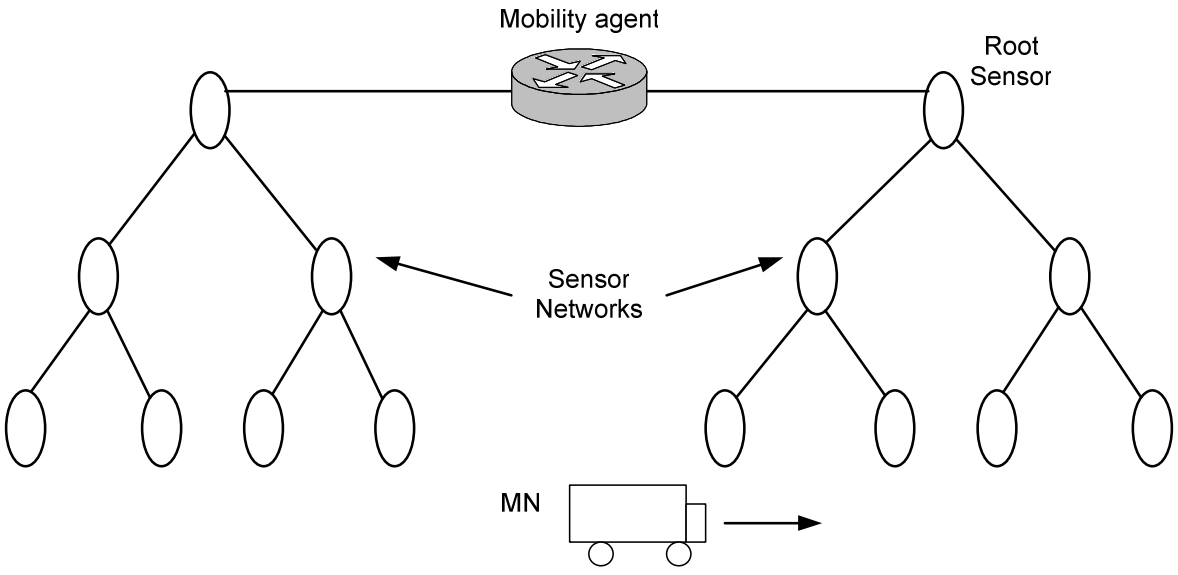

Figure 3.1: Mobile Networks, sensors and mobility agent

The sink, which is the root node or a root sensor, is connected to the mobility agent [19]. The leaf node detects the movement of the MN. The information travels from the leaf node to the root node. The sink (root node) informs the mobility agent about the MN movement. As soon as the mobility agent receives the message from the sink, the pre-registration handoff process is triggered.

Sensor networks are installed at the edge of network boundaries such that they are equidistant from the mobility agents. The connection to the mobility agent may also be through an intermediate router. The Figure 3.2 shows the topology of the sensor networks attached by different mobility agents.

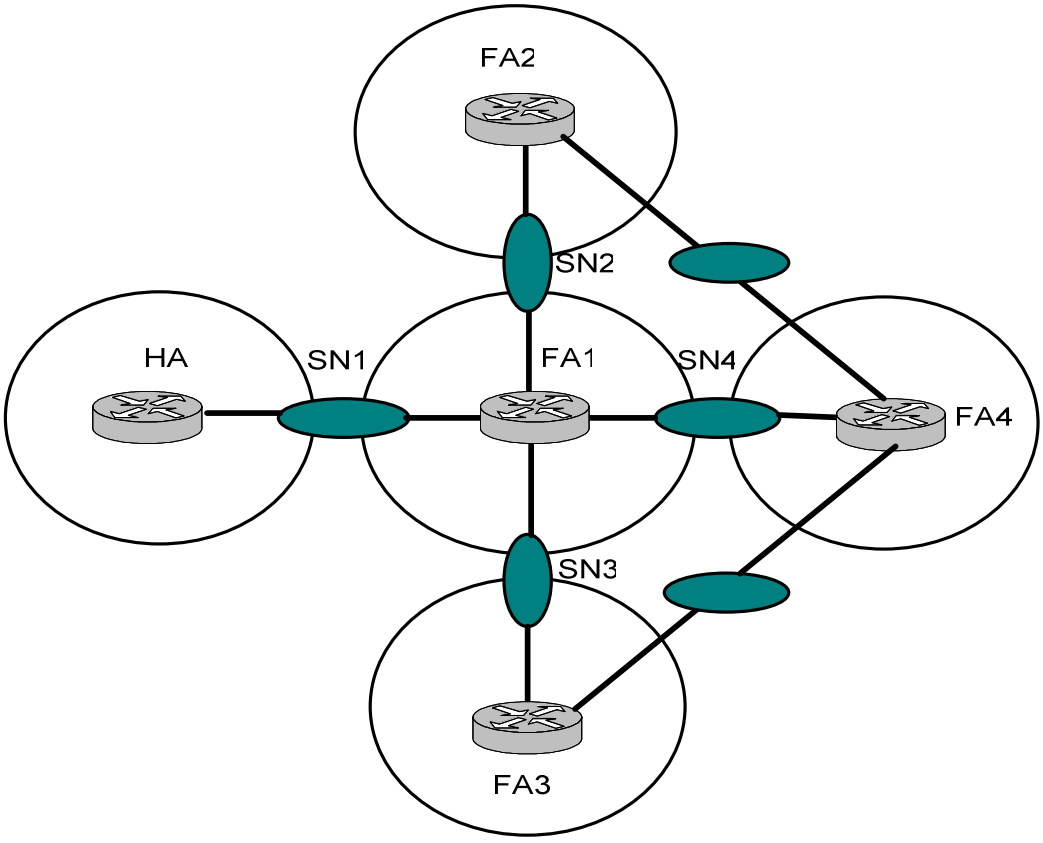

Figure 3.2: STUN used for the proposed scheme

When the network starts, each sensor network gratuitously broadcasts a message that contains the IP address of the mobility agents connected to it. Mobility agents that are not directly connected to the other agents make an entry of the other mobility agents. This information is stored in a table which is called new mobility agent determination table (NMAD) [36].

SN1	HA
SN2	FA2
SN3	FA3
SN4	FA4

Table 3.1: NMAD table at FA1

When the networks comes up, as the sensor networks broadcasts, FA1 is informed about HA, FA2, FA2, FA3 by the sensors SN1, SN2, SN3, SN6 respectively. Based on these advertisements FA1 enters this information in the NMAD table. Similarly the HA is informed about the FA1, FA2, FA3, FA4, by the SN1 and HA stores information in its NMAD table. When the MN starts its movement towards the FA1, SN1 detects it and sends a message to FA1 and HA. As soon as FA1 receives a message from SN1, it understands that the MN is moving towards itself. As soon as this occurs, FA1 trigger the pre-registration handoff. Similarly if the MN is moving from FA1 to FA2, SN3 detects it

and informs both the FA1 and FA2 and the pre-registration handoff is triggered. All mobility agents maintain similar tables and when they hear from a sensor node, the agent looks up in their NMAD table and determines where the MN is moving. After every 5 minutes, the sink sends a hello packet to confirm that it is alive. Also as sensor networks are inexpensive, they can be deployed in large numbers to reduce the point of failure.

3.2 Previous proposed schemes

In this section all the historical research work carried in this field is described. Bahety et al [36] proposed a pre-registration hand off scheme where, when a Mobile Node moves, the sensor nodes detects it and informs the mobility agents associated with it. In this scheme, the QOS was considered and the authors have presented the scheme which improves the QOS in mobile IP when compare to the traditional mobile IP. Results indicate that the performance improves when compared to traditional Mobile IP. In this scheme the authors do not consider the security parameter and its effect on the proposed model.

Dong Hu et al. [29] has discussed the performance of IPSEC for Mobile IP during hand off. In this paper, authors have discussed the performance issues while using traditional security mechanism such as IPSEC on the mobile IP during handoff and have proved them. In this scheme authors believe that even though IPSEC is very flexible and have many options; however it is very complex in nature and confusing in its associated documentations. Also the authors have proved that IPSEC in the upper layers could only prevent leakage of data integrity by using some standard encryption methods but could not prevent such DOS with masquerading attacks.

Jose Caldera et al [35] have discussed the performance of the security protocols such as IPSEC and IKE on Mobile IP in the wireless media. Authors, with the help of simulation have proved that IPSEC protocols over wireless links do not impose a significant penalty whereas the key negotiation and generation as required by IKE imposes a significant penalty to the throughput An average 10 seconds inactivity periods occur in each hand-off due to the key generation and TCP's congestion avoidance mechanisms. In addition, the throughput is reduced by 70% compared to cases where IKE was not used

Dhongai et al [30] have proposed a new authentication method to increase the security during handoff. Here, the authors introduced a AAA server at the foreign agent (AAAF). This reduces the burden of AAAH and AAA networks. In this paper authors have proved that, by using the proposed scheme, the issues which arise with traditional security mechanism such as IPSEC, can be addressed.

3.3 Proposed scheme with an example

As discussed above, various mechanisms have been proposed to not only reduce the hand off delay but also to keep communication secure. While considering the scheme proposed by Dhongai et al [30], various schemes have been proposed by using the AAA. However, the issues while using the AAA foreign are that since the server being in foreign network, we do not have any control over the server. Also, it would be easier for the attacker to attack the AAF, which in itself is a bad design. Also, as described by the authors while using the proposed scheme, the cost would be greater in terms of delay as compared to the previous proposed scheme. In order to overcome these issues, we have

proposed a new scheme in which there would be a key exchange server at the HA as shown in the Figure 3.3.

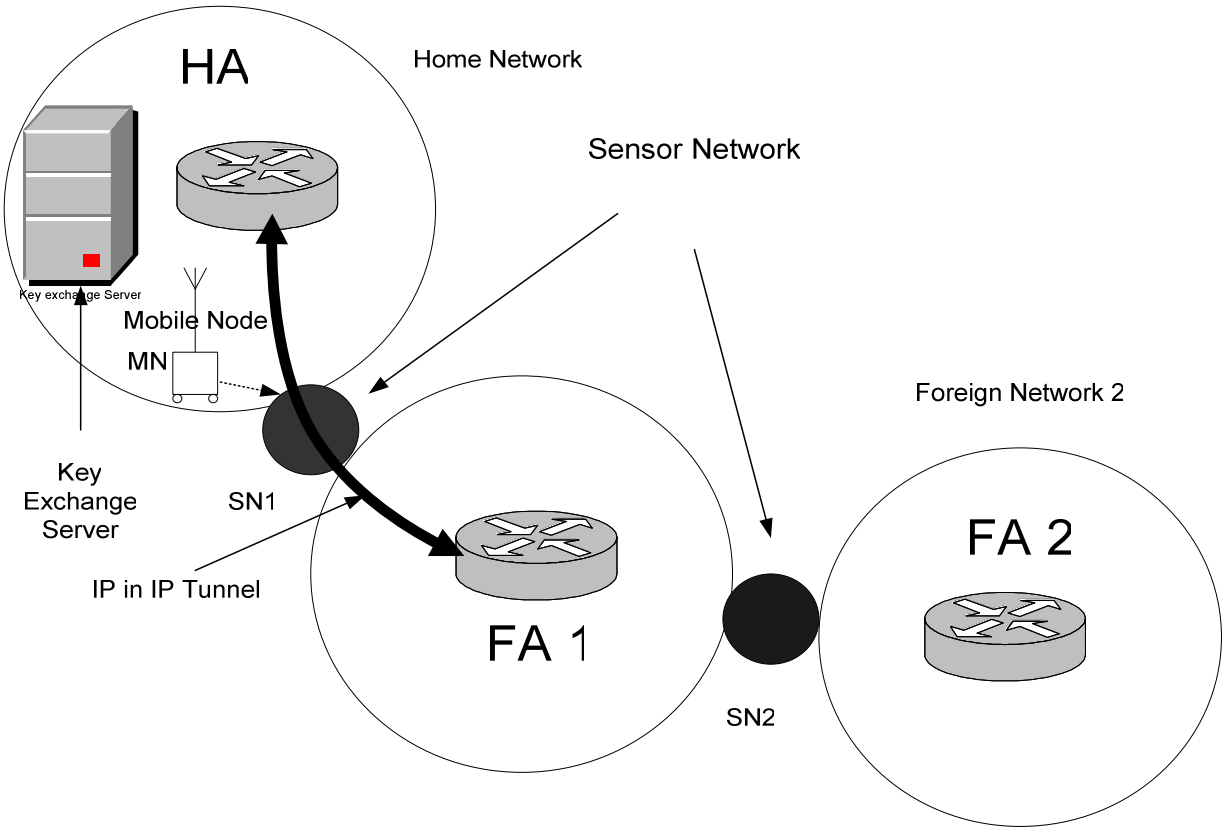

Figure 3.3: Network showing proposed scheme while MN moving from HA to FA1

Consider the network shown in Figure 3.4. As shown in the Figure, MN is the Mobile Node which is currently in the home network and is moving from the home network to a foreign network. FA1 and FA2 are the foreign networks. Below is the procedure for the proposed scheme.

Case 1: When MN moving from HA to FA1

1. Initially, MN is in home network and registers with the HA.
2. When network starts up, MN registers with the HA.
3. Then, MN sends a packet to the HA which contains the key.
4. HA then forwards the packet to the key exchange server.
5. The key exchange server upon receiving the packet from the HA, makes the subsets of the keys and sends it back to the HA.
6. The HA then sends an ACK packet back to the MN indicating that the subset of keys is successful.
7. Upon receiving the ACK packet, the MN stores the key in its database.
8. As soon as MN starts moving towards FA1, sensor networks (SN1) detects it and informs both the FA1 and the HA.
9. FA1 triggers the pre-handoff by enquiring HA about the MN's characteristics
10. HA sends the information to FA1 which contains the key as well.
11. The FA1 then sends an ACK packet to the HA, indicating that it has received all the required information. In addition, the ACK packet contains the COA that would be associated with the MN.
12. When MN arrives in the FA1, it sends a solicit message which contains the negotiation packet.
13. The packet is encrypted by the key given by the HA.
14. If MN is successfully able to decrypt the packet, it would then send an ACK packet to the FA1 and negotiate the encryption algorithm.

15. If FA1 does not receive the ACK packet, it confirms the user is not legitimate and informs the same to HA.

Case 2: When MN is moving from FA1 to FA2

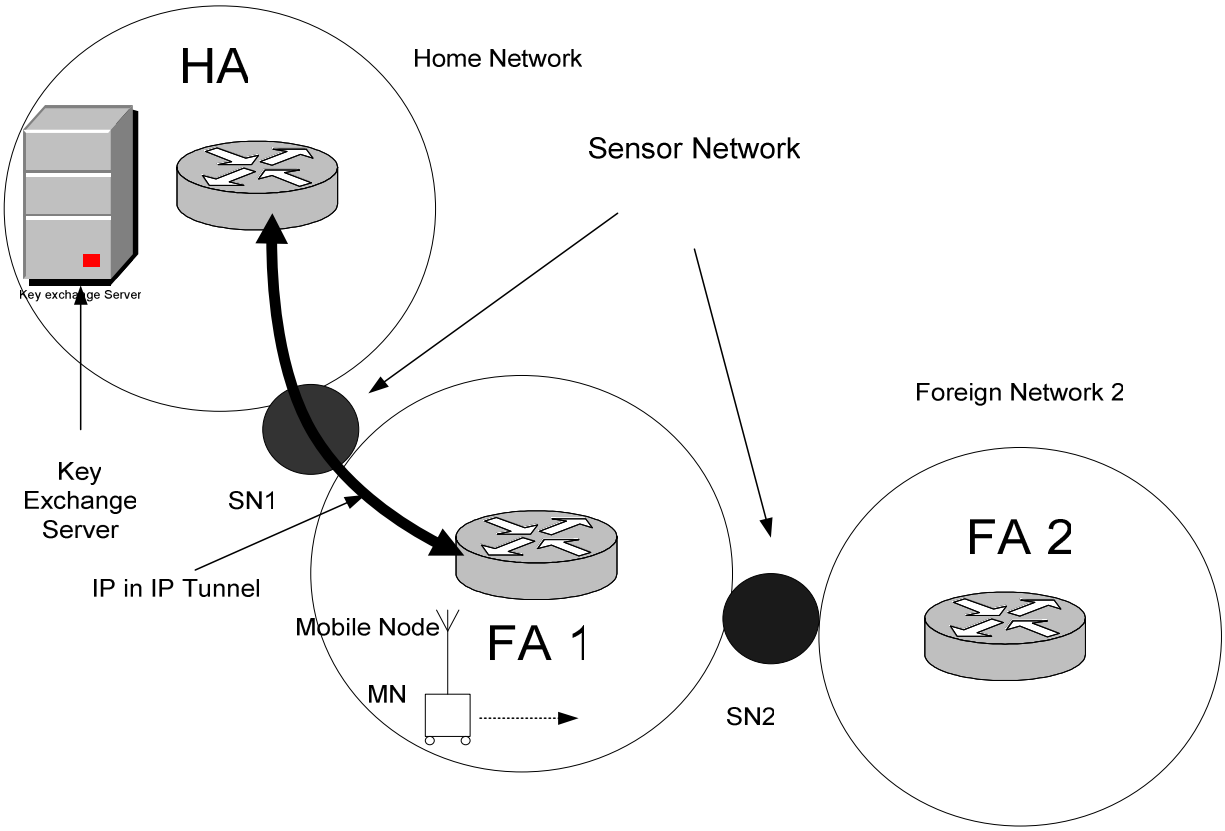

Figure 3.4: Network showing proposed scheme while MN moving from FA1 to FA2

1. As soon as MN starts moving towards FA2, sensor networks (SN2) detects it and informs HA, FA1 and FA2.
2. FA2 triggers the pre-handoff by enquiring HA about the MN characteristics.
3. HA sends the information to the FA2 which contains the key as well.

4. FA2 then sends an ACK packet to the HA, indicating that it has received all the required information. This ACK packet contains the COA that would be associated with the MN.
5. HA creates a simultaneous binding for the MN. Packets intercepted by the HA, will be tunneled to both the foreign networks and as a result there might be duplicate packets for a short duration.
6. When MN arrives in the FA2, FA2 it sends a solicit message which contains the negotiation packet.
7. The packet is encrypted by the key given by the HA.
8. If MN is successfully able to decrypt the packet, it would then send an ACK packet to the FA1 and negotiate the encryption algorithm.
9. MN would send a registration request packet to the FA and FA would send a registration reply on behalf of HA.
10. MN as soon as it receives the registration reply, would force a L2 handoff.
11. FA2 forwards a message to FA1 to delete the reservation for MN.
12. If FA1 does not receive the ACK packet, it confirms the user is not legitimate and informs the same to HA.

Figure 3.5 shows a flow chart of the proposed algorithm. As per the flow chart, first the MN is in HA and exchanges the key with the key exchange server. When MN is moving from one network to another, it would check the authentication and if it is successful, communication will takes place. If not, the MN will not be able to communicate with the HA.

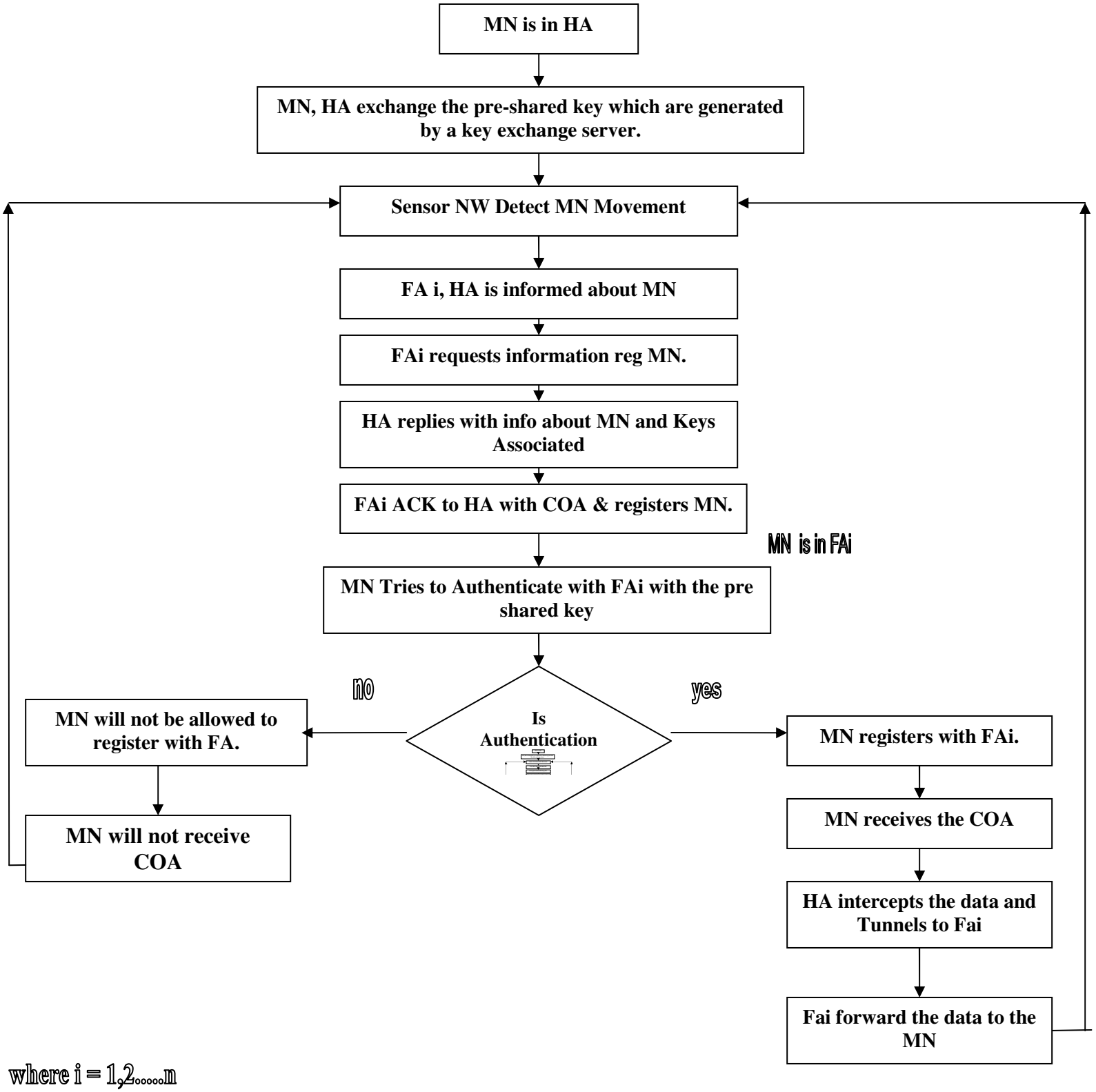

Figure 3.5: Algorithm for the proposed Scheme

3.3.1 Key exchange mechanism

In this section, the key exchange mechanism is described. When MN is in home network, as described earlier, the MN would send a packet to the HA, which contains the key, the MN would be using. HA would forward the key to the key exchange server, which would then create a subset of the key and would return it back to the HA. The HA would then store the subset of the keys, and would send the main key back to the MN, which would then store it in its database. In reality, there might be thousands of MN associated with the HA. If there is no limits on the number of subsets, associated with the key, then the memory requirements would be very high at the HA, to store the keys. Also, if the number of keys increase, the processing power to process the packet at the HA would be very high in terms of cost and delay. Also, not all the keys may be used, which would result in the loss of resources. To address all these issues, we have proposed a mechanism in which the key exchange server would generate only ten subsets of a key. This would greatly decrease the overhead and would increase the performance. The proposed key exchange algorithm is described below.

1. MN sends a packet to the HA with the main key.
2. HA forwards the packets to the key exchange server.
3. Key exchange server creates 10 subsets as per main key and forwards the same to the HA.
4. HA stores the key and then forwards the main key back to the MN.
5. MN then waits for nine handoffs.
6. As soon as it completes nine handoffs, MN sends a packet back to the HA, with the new main key.
7. The HA repeats steps 2 to 4.

8. This continues until the MN is back in HA.

With the proposed scheme, the overhead on the HA is reduced. The only time there would be overhead is when the MN sends the packet with the new key. However, this is far less compared to the actual mechanism. Also as we notice, the resources are not wasted if handoffs are less than nine.

3.3.2 Considering Bursty Traffic

In all the previous proposed schemes, bursty traffic is not considered. In reality, the channel might not be ideal, and the traffic might suffer from bursts loss. Real time traffic might suffer from burst losses and delay which is responsible for the degradation of quality [38]**.** It is very important to restrict these losses to the least possible extent. To restrict it, it is very important to study the factors responsible for it. Also, if the traffic is bursty, it will increase the overhead as the packet which is lost might need to be re transmitted. In the proposed scheme, we have considered the traffic being bursty and have analyzed the overhead caused by it.

To study the overhead caused when traffic is bursty we have considered the semi markov process. A markov chain represents a stochastic process in which the outcome of an event depends on its previous event.. The relationship between the current and previous state of system is expressed using the equation [39]

$$P\{X_n = j | X_{n-1} = i \ , X_{n-2} = i_{n-2} \ \ldots\ldots \ X_0 = i_0\} = P\{ X_n = j | X_{n-1} = i \} \ldots\ldots\ldots\ldots\ldots (3.1)$$

Where X_n represents the state of the process at an instant n.

A markov chain with m possible states includes an initial probability vector **p**(0) of size *m* , a state transition probability matrix [**P**] of size (*m* x *m*) and a limiting state

probability vector **p**(n) of size *m*. The state transition probability vector at an instant time *n* , given the initial state probability vector **p**(0) is given by [38]

$$\mathbf{p}(n) = \mathbf{p}(0) * [\mathbf{P}]^{n} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(3.2)}$$

Since the probability of the chain returning back to the same state immediately is 0 , this markov chain is an embedded markov chain.

In the proposed scheme, this embedded markov chain is considered. Initially the agents are in the equilibrium state which is the state 0. If the state is 0, then they assume that the mobility is still in equilibrium state and there are no packet losses. When the traffic is bursty, and due to this few packets might be dropped. As soon as the packet is dropped, the mobility agent makes the transition to the next state. Eventually the mobility agents would transition back to the equilibrium state. The mobility agents can transition back to the equilibrium state immediately from the next state. Whenever there is a change in the state at the mobility agent, the mobility agent would need to re send the packet. For example, if the mobility agent transitions to state 1 from state 0, it would need to send only 1 packet. If the mobility agent, transitions to sate 3, it cannot directly transition to state 3, it would first transition to state 1 then to state 2 and eventually it will be transitioned to state 3, but it can directly transition back to the state 0 (equilibrium state). Nevertheless it would have to resend 3 packets as it has lost 3 packets while it transitioned to state 3 from state 0, which would increase the overhead. Figure 3.6 shows the probability of the transition states.

In the proposed scheme, we have implemented this and have studies the impact of bursty traffic which is covered in the result section.

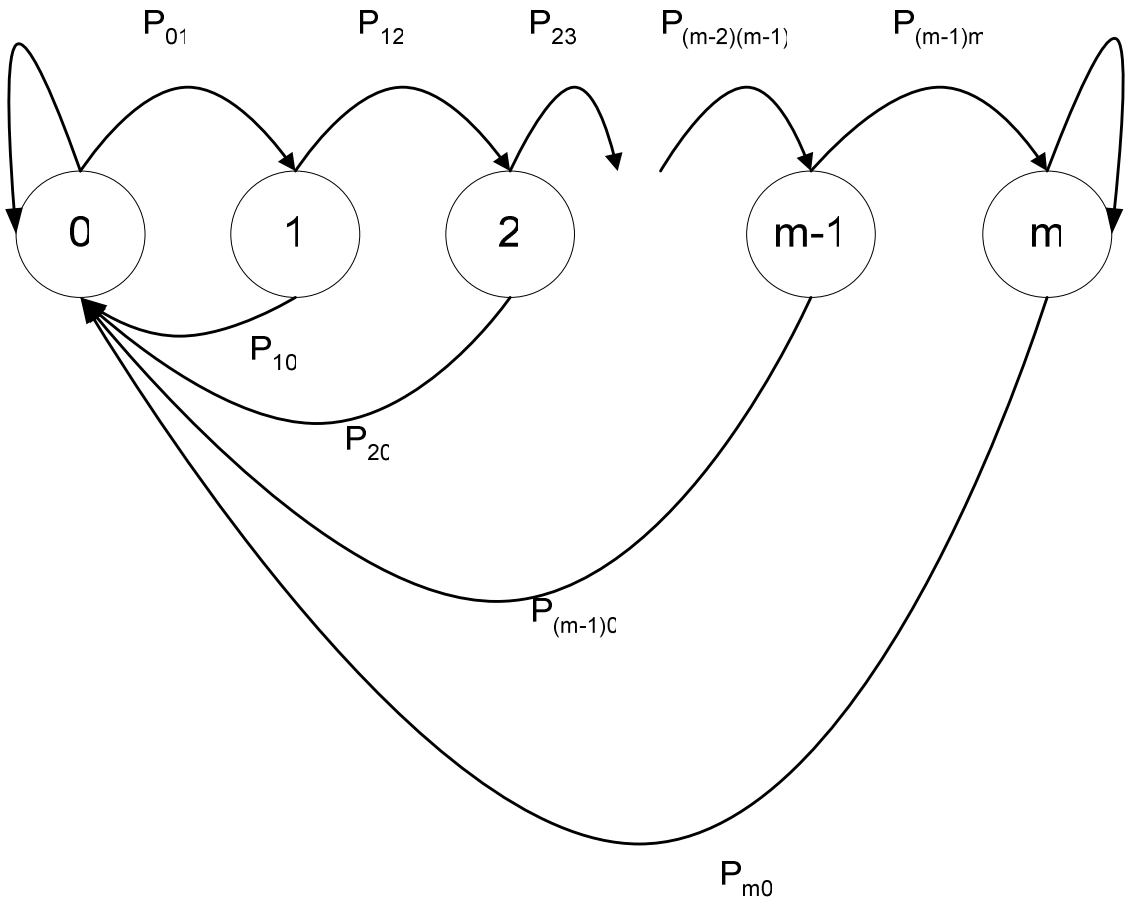

Figure 3.6: Probability of transition from m states to (m-1) state

3.3.3 Mathematical explanation

In this section, the above proposed scheme is described in detail using mathematical equations. Figure 3.7 shows a timing diagram for the traditional Mobile IP. Handoff time can be defined as the time taken by the Mobile Node to move from the old network to a new network. Also, it can be defined as the difference between the last packets received from oFA and the first packet received from the nFA. As described earlier the delay associated with Mobile IP during handoff can be represented as

Handoff delay = movement detection delay + registration delay

3.3.3.1 Handoff cost for traditional Mobile IP

As described in the RFC 3344, the movement detection in traditional Mobile IP occurs when the lifetime expires or by using prefixes. As discussed above, the life time is the amount of time that is stored in the Mobile Node after which it receives the last advertisement. So once the lifetime expires, the Mobile Node thinks that it has moved to another foreign network and starts the handoff process. While using the prefix extension every mobility agent needs to send a prefix in their advertisement. As soon as the Mobile Node receives a prefix other than the one it received initially, it assumes that it has moved to another network and initiates the handoff process. The limitation while using the pre-extension is that all agents must send the extension in their advertisement.

Now, while considering the handoff for traditional Mobile IP, let us assume that the lifetime expiration is used. When the lifetime expires, the MN detects that it has moved to another network since it did not receive any new advertisement from the old mobility agent. Considering the worst case scenario, where the MN has just received the advertisement from the old mobility agent (oFA) before it moved to the new mobility agent (nFA). Let $T_{lifetime}$ be the total lifetime of the last advertisement received. Let T_1 be the time it received the last advertisement from the oFA. Using the movement detection algorithm of traditional Mobile IP as described by the RFC 3344 , the time taken by the MN to realize that is has moved to another network would be $T_{lifetime} + T_1$. After it knows it has moved, the MN would try to force a L2 handoff. As in traditional Mobile IP, a MN cannot associate itself with two mobility agents; MN would try to force a L2 handoff with the previous mobility agent so as to register with the nFA.

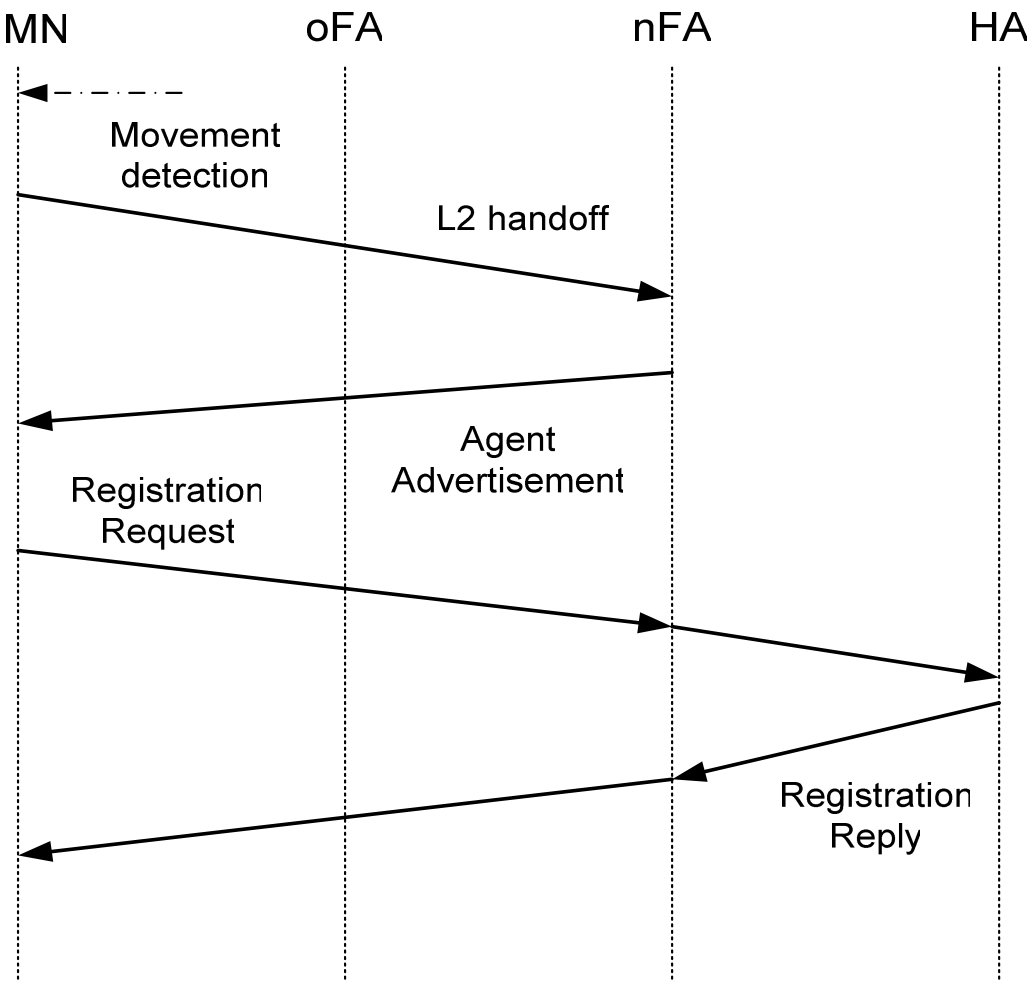

Figure 3.7: Timing diagram during handoff for the Traditional Mobile IP

Hence, the MN would break the L2 handoff with the oFA which causes a L2 handoff delay which is L2 delay. Once it performs the L2 handoff with the oFA, MN would try to register itself with the nFA from which it had received advertisements or would try to discover an agent by performing agent solicitation. Let the time taken by this process be T_3.Then, the MN would send a registration request packet to the FA in order to register itself with the HA. Let the time taken be $T_{(MN\text{-}FA).}$ The packet is then forwarded to the HA by the FA. Let the time taken be $T_{(FA\text{-}HA).}$ HA sends a registration reply to the FA. Let this time taken be $T_{(HA\text{-}FA).}$ The packet is forwarded to the MN. Let it

be $T_{(FA-MN).}$ Hence, the total time taken by the traditional Mobile IP to perform a handoff would be

$$T_{Handoff} = T_{lifetime} + L2\ delay + T3 + T_{(MN-FA)} + T_{(FA-HA)} + T_{(HA-FA)} + T_{(FA-MN)} \ldots\ldots (3.3)$$

During the handoff time, as there is no communication between the MN and the HA, all the packets destined to the MN are lost. Hence the $T_{Handoff}$ would be the total time during which packets are lost.

3.3.3.2 Handoff cost while using the wireless senor network

In the scheme proposed by Bahety et al [36], by using the wireless sensor network, the handoff cost is significantly reduced. The Figure 3.8 shows the timing diagram of the proposed mechanism by Bahety et al [36]

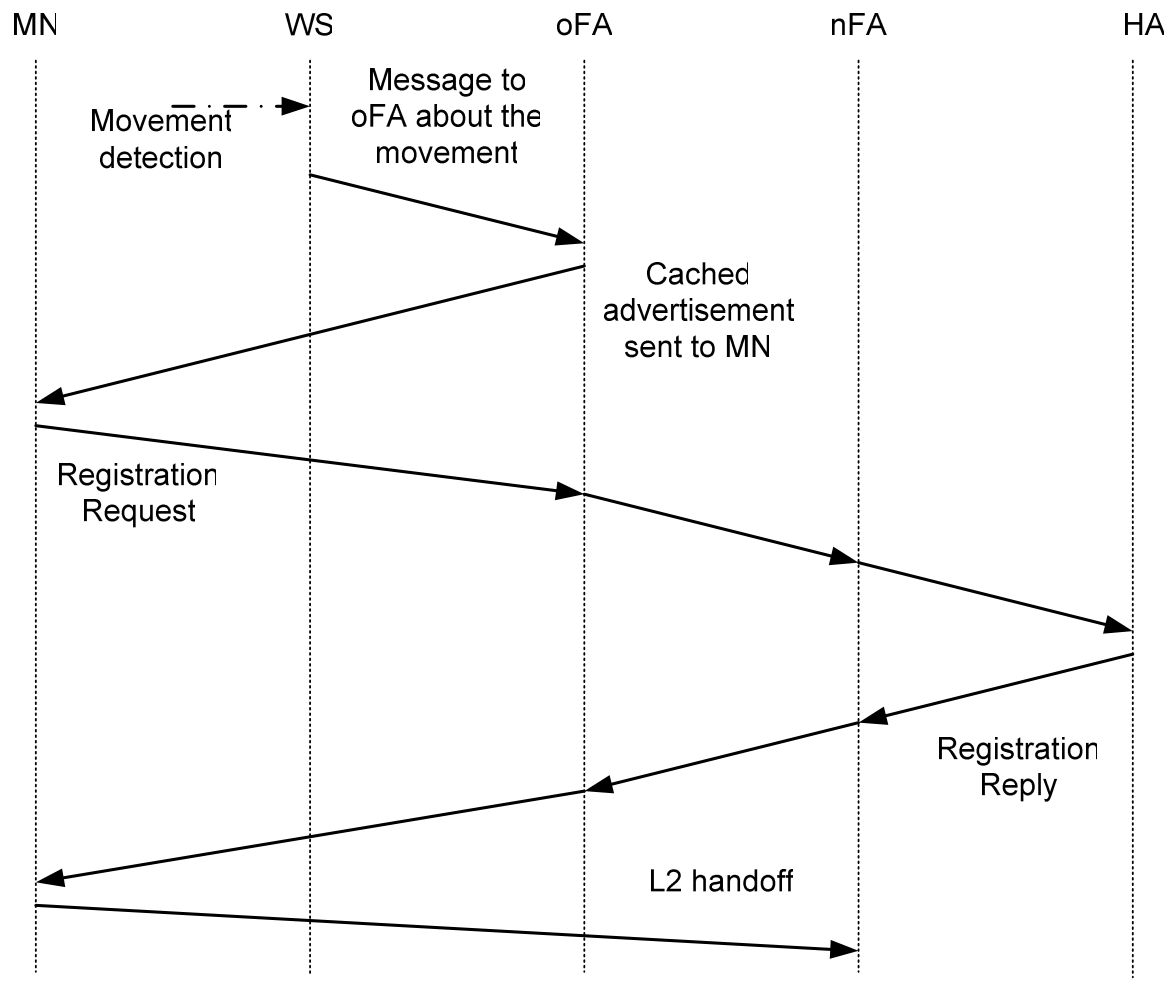

Figure 3.8: Timing diagram during handoff by using WSN.

In this method, the wireless sensors which are present at the edge of the network perform movement detection**.** As described earlier, it uses the STUN method to detect the movement of the MN and informs the mobility agents regarding the same. The wireless sensors can be installed in such a way that the L3 handoff process completes before L2 handoff takes place, assuming that the wireless cells do not overlap. Let X be a certain non-zero time taken by the wireless sensor network to detect that mobile network is moving in a particular direction. The WSN then informs the FA about the detection of the movement of MN. Let this time be $T1_{WS\text{-}FA}$. At this point the FA sends a cached agent

advertisement to the MN that begins the registration process. Let the time taken be T3. During the cached registration process the oFA would solicit on behalf of the nFA. As soon as the MN receives this new agent advertisement it would believe that it has moved to an nFA. The MN sends registration a request to the FA which is then forwarded to HA. Let the time taken be $T1_{MN\text{-}FA}$ and $T1_{FA\text{-}HA}$ respectively. The nFA receives a registration reply from the HA and forwards it to the MN. Let the time taken be $T1_{HA\text{-}FA}$ and $T1_{FA\text{-}MN}$ respectively. As soon as MN receives the registration reply, it tries to force a L2 handoff. Since the MN will receive the packets during the L3 handoff from oFA , the total handoff delay would be

$$T_{(WS)Handoff} = L2_{delay.} \quad \text{..... (3.4)}$$

Here $T_{(WS)Handoff}$ is the total handoff latency using the WSN during which the packets would get lost. Also an optimum distance at which WSN should be installed is calculated. The total time taken for detection and L3 handoff is

$$T_{Detection} = X + T1_{MN\text{-}FA} + T1_{FA\text{-}HA} + T1_{WS\text{-}FA} + T1_{HA\text{-}FA} + T1_{FA\text{-}MN} \quad \text{..... (3.5)}$$

Also the distance D at which the wireless sensor networks should be installed is given by

$$D = T_{Detection} * u \text{ meters} \quad \text{..... (3.6)}$$

3.3.3.3 Handoff mechanism using AAAF server

The above discussed mechanism does not consider security parameters. There are few other schemes proposed in which it was discussed how security protocols such as

IPSEC fail to provide security and are prone to attacks. In the above proposed mechanism a AAA server is used. The AAA server is placed at both the HA and the FA. The timing diagram for the proposed scheme is shown in the Figure 3.9 **[30].** In this scheme, there are 2 AAA servers. The AAA servers are used to address the issue faced by traditional security mechanisms such as IPSEC. The proposed scheme is based on IP/AAA model and is as follows

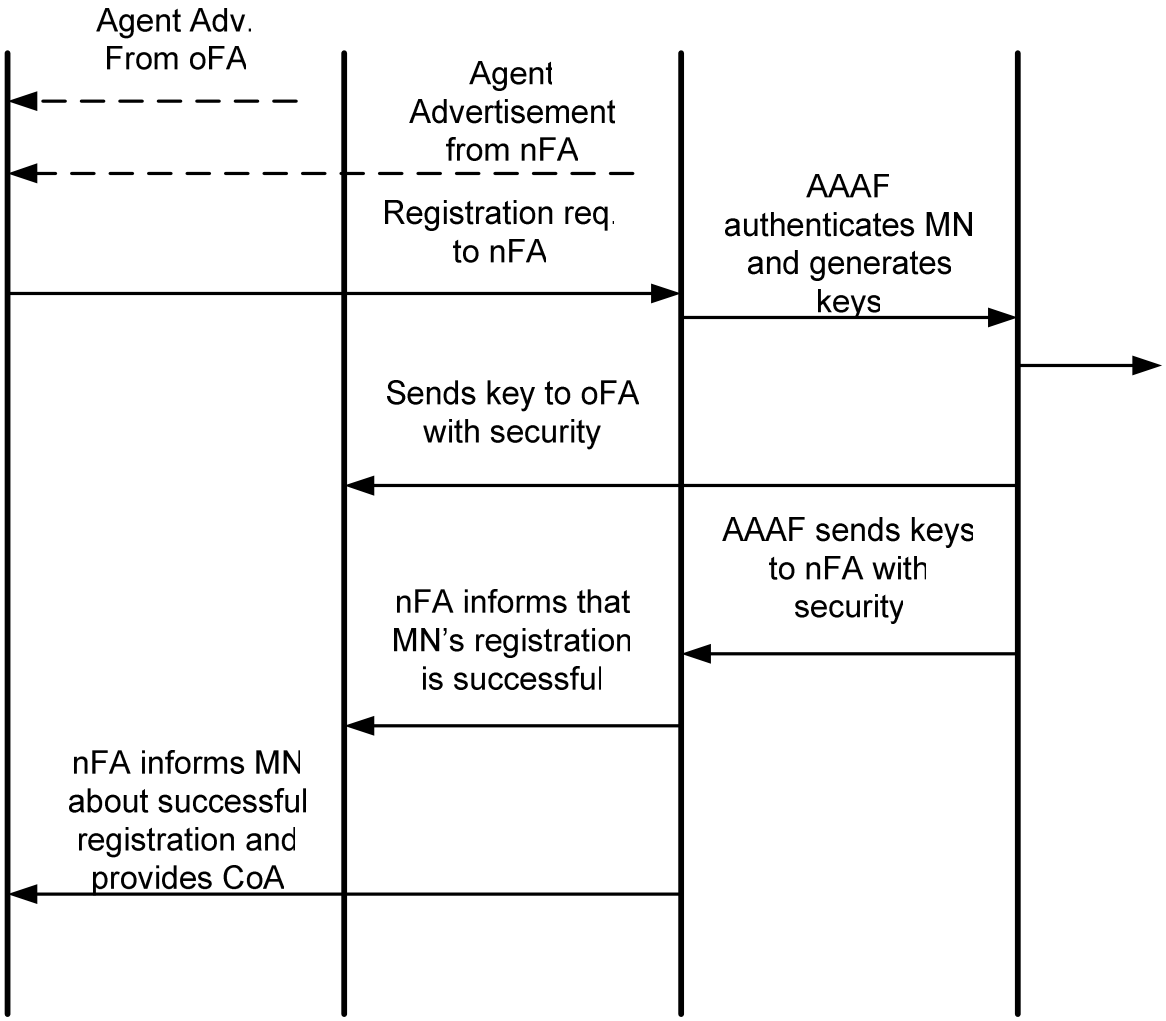

Figure 3.9: Timing diagram during handoff for the scheme using AAAF

When the MN is in HA, it will obtain authentication from the AAAH. When the MN moves from HA to the foreign network, the AAAH sends the MN information to the AAAF and assigns that AAAF can authenticate MN. AAAH generates a new temporary key between AAAF and MN as MN already obtained authentication from AAAH. Let this time be $T_{(AAAF-MN)}$. The AAA servers distribute the keys between the MN and the mobility agents till the keys expire. AAAH distributes the session key $K_{(MN-HA)}$ between the HA and the MN. Let the time taken be $T_{(AAAF-HA)}$. AAAF distributes the foreign keys $K_{(MN-FA)}$ between MN and FA $K_{(FA-HA)}$ between the HA and FA. If oFA and nFA are in some domain, the same AAAF, there exists only one security association. Let this time taken be $T_{(AAAF-NFA)}$ between AAAF and nFA and $T_{(AAAF-OFA)}$. MN then registers with the NFA and the registration request and the registration reply are routed through the oFA , since MN is not connected to the nFA prior to the L2 handoff. Hence the total handoff time would be

$$T_{(Handoff)} = T_{(AAAF-MN)} + K_{(MN-HA)} + T_{(AAAF-HA)} + K_{(MN-FA)} + K_{(FA-HA)} + T_{(AAAF-NFA)} + T_{(AAAF-OFA)} + X \quad \text{..... (3.7)}$$

Where X is the key exchange mechanism between MN and AAAH. Also when the nFA and oFA are in different domains, it would add more overhead as the AAAH would have to communicate with AAAF at both the oFA and nFA.

3.3.3.4 Mathematical analysis for the proposed model

As seen in the previous proposed model, by using the wireless sensor networks, the handoff delay can be reduced and also by using the AAA server, the issues by using

the traditional security mechanisms such as IPSEC can be addressed. But as seen above by using the AAA server, it not only adds delay, it still does not completely eliminate security threats. In order to address these issues, the scheme is proposed.

Figure 3.10 shows the timing diagram of the proposed scheme during handoff. The Figure 3.10 shows the timing diagram when the MN is in HA and is moving from HA to FA1 and Figure 3.11 shows the timing diagram when MN is moving from FA1 to FA2.

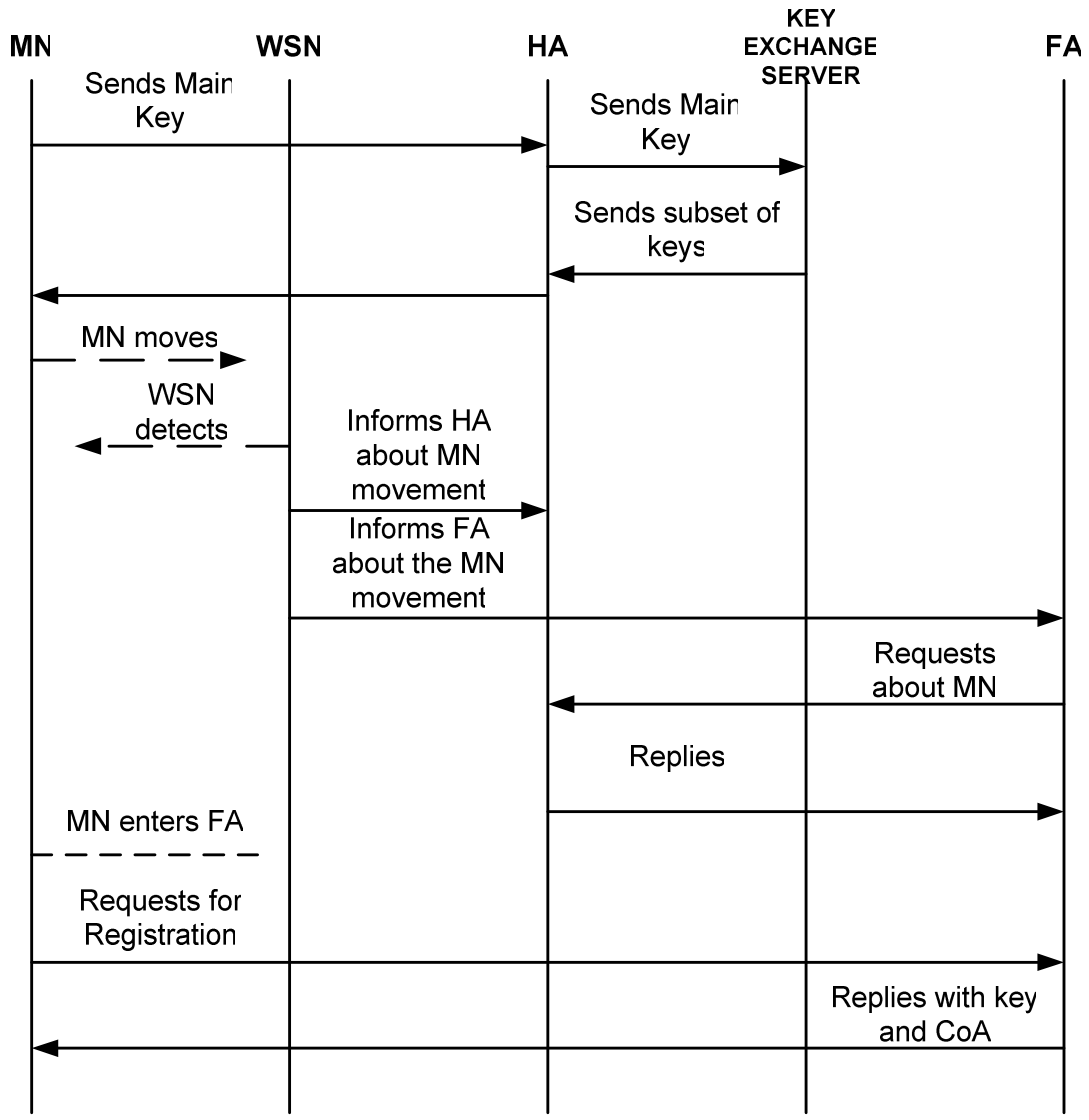

Figure 3.10: Timing diagram during handoff for the proposed scheme when MN is in home network

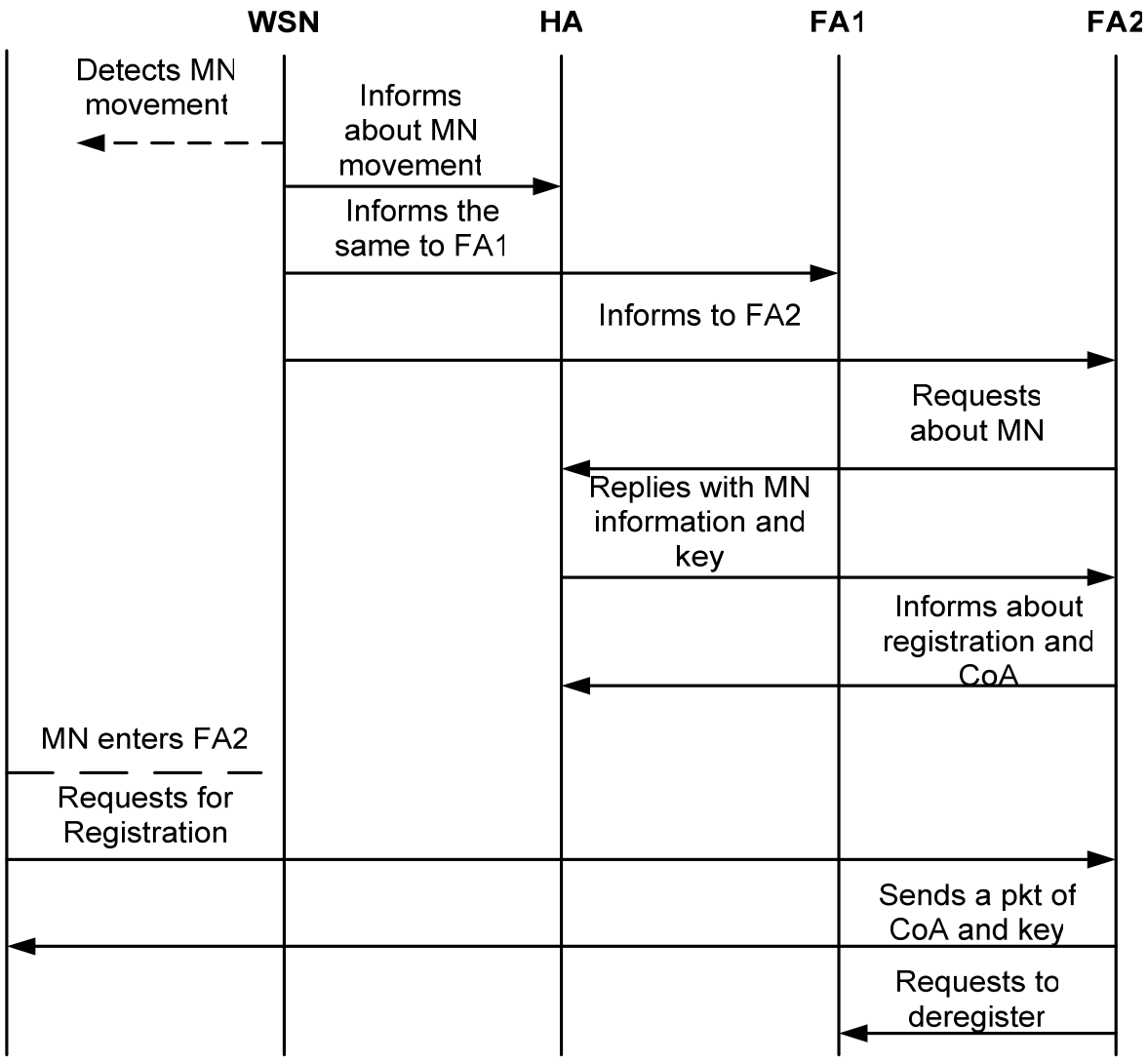

Figure 3.11: Timing diagram during handoff for the proposed scheme when MN is moving from FA1 to FA2.

When the network starts up MN is in Home Network. MN sends a packet to the HA. The packet that is sent contains the key. HA then forwards the packet to the key exchange server. The key exchange server generates a key which is forwarded to HA and then HA forwards the key to the MN, where HA a store the subsets of the keys and MN has the main key. Let the time taken to generate the keys be T_K (ms). As the MN moves towards

FA1, sensor networks detect its movement. Let this time be T_d (ms). The sensor networks report MN's movement to both the HA and FA. Let the time taken be T_i (ms). Now the FA requests information about MN from HA. Consider this time to be $T_{(Fi-Hi)}$ (ms).HA replies to FA about MN and the keys associated with it. Let the time taken here be $T_{(Hi-Fi)}$ (ms). FA acknowledges to HA about registration of MN and the associated CoA. Let the time here be $T_{(FA1-HA1)}$ (ms). As MN moves into FN, it requests registration with FA. Consider here the time be $T_{(MN-FA)}$ (ms). FA sends a packet to MN with key and the CoA. MN receives the packet with CoA and the key associated. Let the time taken for this be $T_{(FA-MN)}$ (ms) + $T_{(MN-FA)}$ (ms).HA intercepts all the packets destined to MN and delivers to MN via FA. If FA finds that MN is not legitimate, it does not receive COA and will not be allowed to register with HA. Now the MN moves from FA1 to FA2. When MN is moving from FA1 to FA2, the Wireless Sensor Network detects the MN movement. Let the time taken be T_{d1} (ms). The sensor network reports MN's movement to HA, FA1, FA2. Let the time taken be T_{i1} (ms). FA2 requests information about MN to HA. Let the time taken be $T_{(FA2-HA)}$ (ms).HA replies with the information about MN to FA2 and the key associated with it. Let the time taken be $T_{(HA-FA2)}$ (ms).FA2 acknowledges to HA .Let the time taken be $T_{(FA2i-HA)}$ (ms).The registration and exchange of keys occurs between FA2 and MN. Let the time taken be $X=T_{(MN-FA)} +T_{(FA-MN)} + T_{(MN2-FA)}$ (ms). Next, FA2 requests FA1 to delete the entry of MN and perform the L2 handoff, which would cause a L2 delay. Also considering the traffic being bursty, the mobility agent would have to re-transmit the packets. Let this time taken be T_R. Hence Total hand off time before 9^{th} movement and after 10^{th} movement using proposed Mobile IP is

$$\text{Total Time} = T_{\text{Lifetime}} + T_{d1} + T_{i1} + T_{(FA2\text{-}HA)} + T_{(HA\text{-}FA2)} + T_{(FA2i\text{-}HA)} + X + L2 \text{ delay} + T_R \quad \text{(3.8)}$$

Also as per the proposed algorithm, the MN would send an extra packet to the HA, after every 9 movement, this would add more delay. Let the time be Tp. Also, considering the traffic being bursty, the mobility agent would have to re-transmit the packets. Let this time taken be T_R . Total Hand off time for the 1st, 10th, 20th …. Movement using proposed Mobile IP is

$$\text{Total Time} = T_{\text{Lifetime}} + T_{d1} + T_{i1} + T_{(FA2\text{-}HA)} + T_{(HA\text{-}FA2)} + T_{(FA2i\text{-}HA)} + X + L2 \text{ delay} + T_K + T_R + Tp \quad \text{(3.9)}$$

CHAPTER 4

MATHEMATICAL ANALYSIS

In this Chapter the authors would discuss the analytical model for the proposed scheme with supported equations. A simulation model is described and various parameters such as registration cost, handoff cost and movement cost have been estimated. In the last section the overhead cost associated with the proposed model is described.

4.1 Simulation model

As described in Chapter 2, the handoff cost is the sum of the movement cost and the registration cost. Registration cost is defined as the time taken by the MN to register with the HA and the movement cost is defined as the time taken by the MN to force a L2 handoff. In [36], authors have used a similar model for the proposed scheme, but have not taken any security parameters into consideration. Also bursts in the traffic are not considered. In the proposed scheme all the parameters are considered.

In the proposed scheme for analyzing purpose, let us assume that equal sized non overlapping hexagonal cells are considered where each cell represents the movement area of the MN as shown in Figure 4.1 Each cell will have a mobility agent and the area represents the coverage area for the mobility agent. Whenever a MN moves (cross) from one cell to another, a handoff will occur. As described earlier, when the handoff occurs, the MN will not be receiving any packets. During the handoff time the packets would not be reaching the MN, but would be stored in a buffer of the mobility agent.

. As shown in the Figure 4.3, each ring represents a separate domain. MN while moving in the same domain has to perform handoff as each cell has a separate mobility

agent. As a result, when a MN moves from one cell to another, regardless of the domain, handoff will occur. Considering the Figure 4.1, each cell represents a mobility agent, and all the cells in the ring represent a domain. As seen in the Figure each cell is surrounded by the ring of cells. The number of cells surrounded by the cell is 6. Hence the number of cells in the ring i is given by 6i.where i varies from 1 to n. The value shown in each cell describes the distance between the cells from the centre. The number of cells that are within a distance d from any cell is given by [41] 3d (d+1) +1.

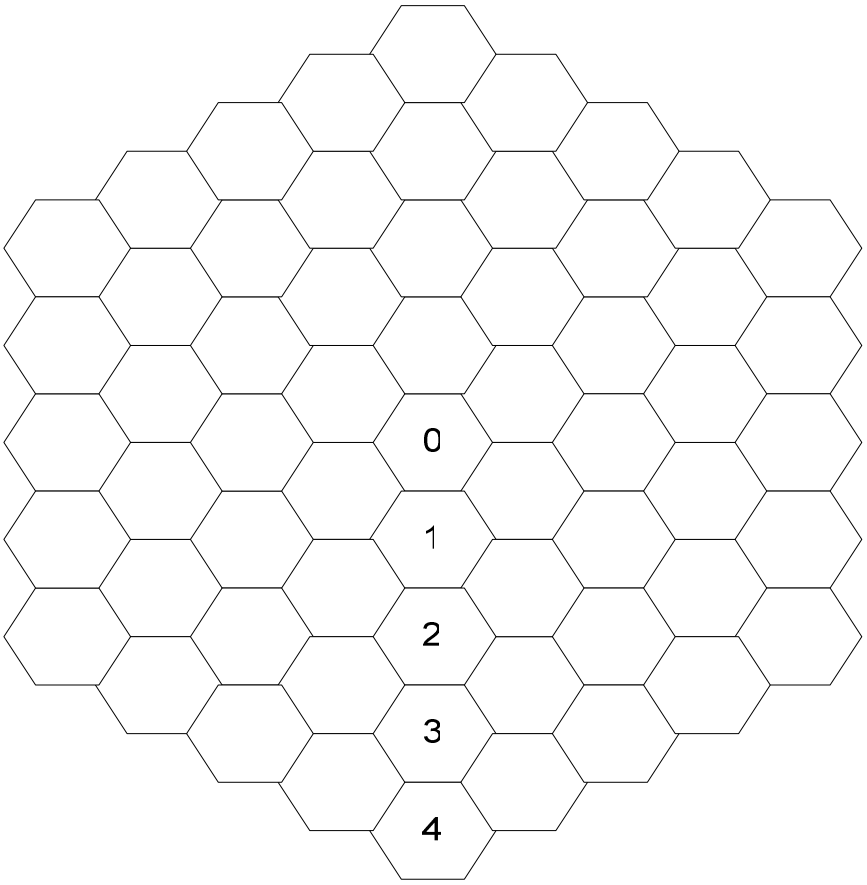

Figure 4.1: Mobile Networks, sensors and mobility agent

To reach a particular cell (mobility agent associated with the cell), the MN has to undergo *n* movements and hence has to perform *n* number of handoffs. Hence, for each movement, the MN has to perform a handoff at each cell to reach the destination cell. Let HA be at a distance k from the first FA. Each cell is at a distance i from the center. The distance between the HA and the FA is described by the using the random walk mobility model.

While studying the different mobility management features such as registration, paging, handoff and database approach, mobility models play an important role. Traces and synthesis are two types of mobility patterns that are present. Traces are the mobility patterns that are observed in the real life, whereas synthesis model attempt to represent the MN without the use of traces. There are 7 different types of mobility models [40]. Random Walk Mobility Model, Random Waypoint Mobility Model, Random Direction Mobility Model, Gauss-Markov Mobility Model, A Probabilistic Version of the Random Walk Mobility Model and City Section Mobility Model.

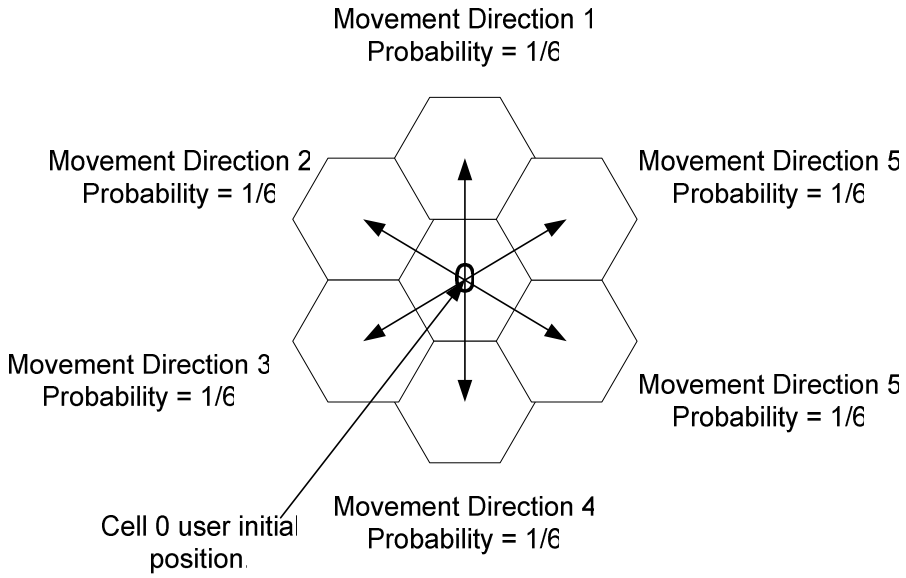

Figure 4.2: The probability of MN moving to the next cell

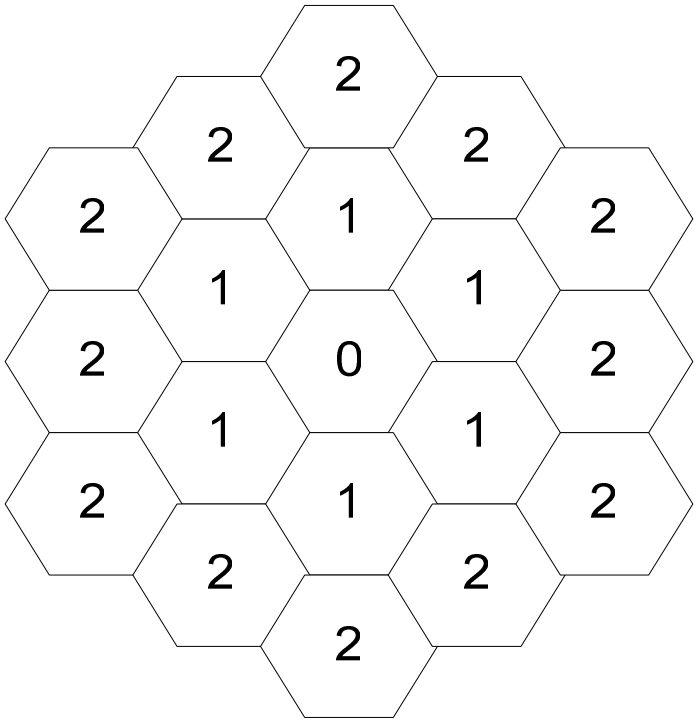

Figure 4.3: Each ring consisting for 6i cells and each Ring is in same domain

In the proposed scheme, a 2d random walk mobility model is considered. Let L^n be matrix in which each element $L^n{}_{i,j}$ is the probability of MN moving to the new mobility agent at a distance i cell after n^{th} movement. As shown in the Figure 4.2, the MN movement is restricted to move in one of the six directions. Hence the probability at which the MN may move to the neighboring cell is equal to 1/6 in each direction. Also, as shown in the Figure 4.3, each ring i consists of 6i cells. So a MN can move into any one of the cells, within the same domain or can move in another domain. The probability distribution of the distance traveled by the MN is shown in the Figure 4.2

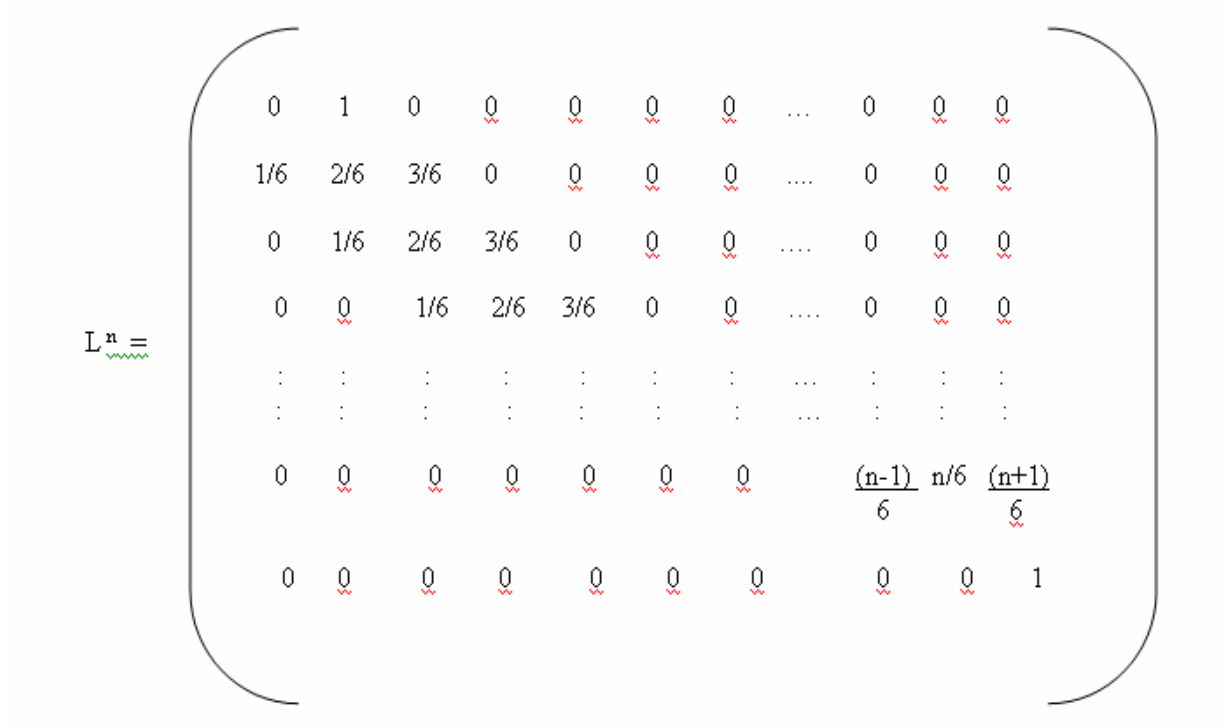

Figure 4.4: Probability Matrix using the Random Walk Mobility model

4.2 Registration Cost

As described earlier, registration cost is the sum of movement cost and the handoff cost. The registration cost at the mobility agents is the sum of processing the registration messages and transmitting the messages over wireless channels. For analyzing purposes, it is assumed that costs for processing the messages at the mobility agents are constant. Let the cost be denoted by $C_{p.}$ The transmission cost is directly proportional to the distance between the mobility agents that is the difference between the HA, FA and MN. Let the distance between the mobility agents be $\delta_{t.}$ In the proposed scheme as all the mobility agents are at equidistant, δ_t is assumed to be constant. The messages are transmitted over wireless links. The cost of transmitting the messages over wireless links is always higher than that of the wired links. Let this cost be 'w' times higher than the wired links. Hence, the total transmission cost between the mobility

agents is $w\,\delta_t$. Let T_{hf} denote the transmission cost between the HA and the FA and T_{fm} be the transmission cost between the mobility agent and the HA. Figure below shows the message flow for the registration process for the traditional Mobile IP. The registration cost per movement of traditional Mobile IP is

$$2\,T_{fm} + C_p \quad \text{when MN returns home} \qquad (4.1)$$

$$\text{and} \quad 2\,T_{hf} + 3Cp + 2\,T_{fm} \text{ for all the other cases} \qquad (4.2)$$

The registration cost of traditional Mobile IP for d movements is calculated. Let us assume that $d^h_{i,j}$ denotes the distance between the HA and the FA in the cell with-ordinates (i , j) , and $C_{i,j,mh}$ denotes the cost for MN to register with the HA from cell (i , j). Hence $C_{i,j,mh}$

$$= 2w\delta_t + C_p + H_p \quad \text{for } d^h_{i,j} = 0 \qquad (4.3)$$

$$= 2(d^h_{i,j} + w)\delta_t + 3C_p + H_p \quad \text{for } d^h_{i,j} \neq 0 \qquad (4.4)$$

Hence, the average registration cost for the traditional Mobile IP for d movements is given by

$$\frac{1}{d} \sum_{n=1}^{d} \sum_{i,j} L^n_{i,j} * C_{i,j,mh} \qquad (4.5)$$

When wireless sensor networks are used, the pre-registration message is sent and received through the oFA, hence there would be additional processing costs and the transmitting cost. Hence the average registration cost for the Mobile IP with WSN for d movements is given by

$$\frac{1}{d}\sum_{n=1}^{d}\sum_{i,j} L_{i,j}^{n} * \acute{C}_{i,j,mh} \quad \ldots\ldots (4.6)$$

Where $\acute{C}_{i,j,mh} = 2w\delta_t + C_p + H_p$ for $d^h_{i,j} = 0$……………………..…. (4.7)

$= 2(d_{sen\&fa} + w)\delta_t + 2C_p + H_p$ for $d^h_{i,j} \neq 0$ …..….…… (4.8)

The Average registration cost for the proposed is explained using the Figure 4.5. In the proposed scheme, the wireless sensor networks is placed in-between the mobility agents, thus the processing cost would be greater than that of the traditional Mobile IP. In the proposed scheme, when the MN is initially at the HA, it has to undergo key exchange process which would add more overhead. Also the WSN is placed in such a way that the distance between the mobility agents and the WSN is same. Also, as stated earlier, once the MN starts moving after 9 handoffs, MN would send a packet to the HA to generate a new key as the original subsets of keys are limited to 9, hence after every 9 handoffs it would have to generate a new key which would result in higher registration cost. Let the nFA be indexed by (i , j) . Then the cost between the WSN and the mobility agent (nfa) is denoted as $d_{sen\&fa.}$ Hence the cost $\hat{C}_{i,j,mh}$ can be calculated as

$=2w\delta_t + C_p + H_p + K_g$ for $d^h_{i,j} = 0$………………………………...…. (4.9)

$=4*delta+2*C_p+H_p+4*(w+C_p) + K_s$ for $d^h_{i,j} \neq 0, 1 \leq d^h_{i,j} = 10$…........(4.10)

$= 4*delta+2*C_p+ H_p+4*(w+ C_p) + K_s+K_e+K_d$ for $d^h_{i,j} \neq 0, d^h_{i,j} = 1$.(4.11)

Where K_e is the key exchange process and K_d is the time taken to generate the process.

$K_e = 2*(w+ C_p)+2* C_p +2*delta+2*H_p+K_d$………………. (4.12)

Also as described earlier, when the traffic is bursty, due to the burst ness in traffic few packets may be dropped. Hence the mobility agents would have to re-transmit the dropped packets which itself costs more delay. Let the nFA is indexed by (i , j) . Then the cost between the WSN and the mobility agent (nFA) is denoted by $d_{sen\&fa.}$ Hence the cost $\hat{C}_{i,j,mh}$ can be calculated as

$$=2w\delta_{t} + C_p + H_p \text{ for } d^h_{i,j} = 0 \quad (4.13)$$

$$=4*delta+2*C_p+H_p+4*(w+C_p) + K_s + R_p, \text{ for } 1 \leq d^h_{i,j} \leq 10 \quad (4.14)$$

$$=4*delta+2*C_p+ H_p+4*(w+ C_p) + K_s+K_e+ R_p \text{ for } d^h_{i,j}= 11 \quad (4.15)$$

Where Ke is the Key Generation Process and R_p is the cost for re-transmission.

$$Ke == 2*(w+ C_p)+2* C_p +2*delta+2*H_p+K_d \quad (4.16)$$

$$R_p = 2w\delta_{t} + 2C_p + H_p \text{ (for 1 state)} \quad (4.17)$$

Hence the average registration cost for the proposed scheme for d movements is given by

$$\frac{1}{d} \sum_{n=1}^{d} \sum_{i,j} L^n_{i,j} * \hat{C}_{i,j,mh} \quad (4.18)$$

4.3 Movement Cost

Movement detection is used to identify whether the MN has moved from one network to another. A MN when crosses a network boundary does not realize it has moved from one network to another, it realizes only when the lifetime expires or the prefix is different from the one it received initially as described earlier. In the proposed scheme, it is assumed that the MN uses the lifetime expiry method. Assuming that the MN receives an advertisement from the mobility agents of a lifetime of L seconds.

Considering the worst case scenario, where the MN has just received an advertisement when it is about to move to the new network. Hence the MN may stop receiving the packets due to the handoff as soon as it receives the last advertisement. The MN will then take L seconds to perform the movement detection. However considering the best case scenario, the MN may stop receiving advertisement packets in the old network from the mobility agent immediately after the lifetime of the last advertisement expires. The MN may then prefer to perform a L2 handoff as soon as it breaks the association with the old mobility agent.

However, the MN cannot register with the new mobility agent and will have to wait until the old advertisement expires to register with the new mobility agent. As soon as the old advertisement expires, the MN can register with the new mobility agent. During this phase the MN will not be receiving any packets. But in the case of wireless sensor networks, the movement of MN is detected and before the MN moves to the old mobility agent, the old mobility agent does a proxy for the new mobility agent. In the proposed scheme, the WSN detects the movement but does not proxy. It triggers the handoff initiation, and as soon as MN crosses the boundary, it advertises and the registration process is started. As MN movement is detected, the cost for detection is just the L2 delay when compared to the cost of delay associated with the traditional Mobile IP.

The movement detection cost can thus be considered as a discrete random variable with a uniform distribution between n and n+1. Let Cn denote the cost of the delay, a random variable as the MN moves a mobility agent. The average cost for movement detection for a traditional Mobile IP delay can be calculated as

$$\sum \sum L^n{}_{i,j} * M^n{}_{i,j,f} \ldots\ldots\ldots\ldots(4.18)$$

In the scenario where, WSN are used for movement detection, the movement delay cost is equal to L2 handoff delay. Let M` be the value of the L2 delay. Now the movement detection delay cost is

$$\sum \sum L^n{}_{i,j} * M` \ldots\ldots\ldots\ldots(4.20)$$

In the proposed scheme, as WSN are used to perform the movement detection of the MN, the movement detection cost would be equal to the L2 handoff delay. P_{nj} is the probability of the mobility node being in the nth level after j movements and is given by

$$\mathbf{P}_{n,j} = \mathbf{P}_{(n-1)(j-1)} * \mathbf{L}_{(n-1)n} + \mathbf{P}_{n(j-1)} * \mathbf{L}_{(n)n} + \mathbf{P}_{(n+1)(j-1)} * \mathbf{L}_{(n+1)n} \ldots\ldots\ldots\ldots(4.21)$$

Let C_n be the cost of the movement to n^{th} level. Hence the movement detection cost for the proposed network is

$$\sum_{n=1}^{n+1} P_{n,j} * C_n \ldots\ldots\ldots\ldots(4.22)$$

4.4 Handoff Cost

The Handoff cost is the sum of the registration cost and the movement cost. As described earlier, the handoff is the process where, the MN, when it moves from one network to another, needs to register with the HA and hence the handoff occurs. Hence when MN moves from one network to another it is known as movement cost, and when MN registers with the HA it is known as the registration cost.

The handoff cost is not as same as handoff delay, later is described in 4.5. As calculated in the previous sections, the registration cost and the movement cost, the handoff cost in case of traditional Mobile IP can be calculated as

$$\frac{1}{d}\sum_{n=1}^{d}\sum_{i,j} L_{i,j}^{n} * C_{i,j,mh} + \sum\sum \boldsymbol{L}^{n}_{i,j} * M^{n}_{i,j,f} \quad \text{.....(4.23)}$$

Similarly the Handoff cost in the case of Mobile IP with the WSN can be calculated as

$$\frac{1}{d}\sum_{n=1}^{d}\sum_{i,j} L_{i,j}^{n} * \acute{C}_{i,j,mh} + \sum\sum \boldsymbol{L}^{n}_{i,j} * M` \quad \text{.....(4.24)}$$

Also the handoff cost for the proposed scheme can be given by the equation

$$\frac{1}{d}\sum_{n=1}^{d}\sum_{i,j} L_{i,j}^{n} * C_{i,j,mh} + \sum_{n=1}^{n+1} P_{n,j} * Cn \quad \text{.....(4.25)}$$

4.5 Handoff Delay

Assuming that the MN has open traffic session during the handoff, Handoff delay can be defined as is the time difference between receiving the last packet from oFA and the first packet from the nFA. In the case of traditional Mobile IP, it is the sum of movement detection delay, registration delay and the L2 delay. Hence

For **Traditional Mobile IP:**

$$C_{i,j,mh} + M^{n}_{i,j,f} + M` \text{ …..(4.26)}$$

But for the **proposed method it** is equal to L2 delay i.e $M`$

CHAPTER 5

RESULTS

In this Chapter the author focuses on the simulations for various parameters that were carried out for the proposed scheme. The various parameters that are calculated are then compared with that of the traditional Mobile IP and the previous proposed schemes such as WSN. All the Simulations were carried out using MATLAB based on the analytical model described in Chapter 4. The Various parameters that are calculated and compared are the basic cost at the mobility agents, the registration cost, the movement cost and the handoff cost.

5.1 Simulation

In this research work, various parameters such as registration cost, movement cost and handoff cost has been compared to that of the previous proposed techniques. Also various scenarios such as bursty traffic and key length which results in further overhead are compared to enlighten their importance.

For the simulation purpose, the hexagonal random walk mobility model is considered, where movement area of MN is considered within the 20 hexagonal rings. The HA is always assumed to be at the centre of the hexagonal model and the rings that are associated with the next level are considered to be the FA1, FA2,…FAn respectively where FA1, is the FA next to the HA and FA2 is at two hops away from HA and FAn is at the ‘n’ distance away from HA. The MN is always assumed to start from the HA and then move towards different foreign agent. Consider an example where MN is at cell 0 initially (which is the HA) and if MN makes 20 movements it may reach cell 20, if it

moves in one direction. Assuming the random walk mobility model, the MN may not take single direction always and may move to a different FA. All the costs are calculated considering using the random walk mobility model.

The simulations are run for different cases in which, first varying the length of the key that needs to be generated is calculated and is proved that the key length increases the overhead associated with the registration cost. Secondly the scenario for bursty traffic is calculated where it is shown that the burst in traffic can result in packet loss and which results in increases in the cost when compared to the traditional mobile IP. Finally the processing cost (Cp) and the delta are varied and the registration cost, movement cost and handoff cost are calculated and compared to that of the previous proposed schemes.

5.2 Comparison off basic cost

First the basic cost associated with the proposed scheme is compared. The basic cost is the cost for the MN to register with the HA with respect to each FA.

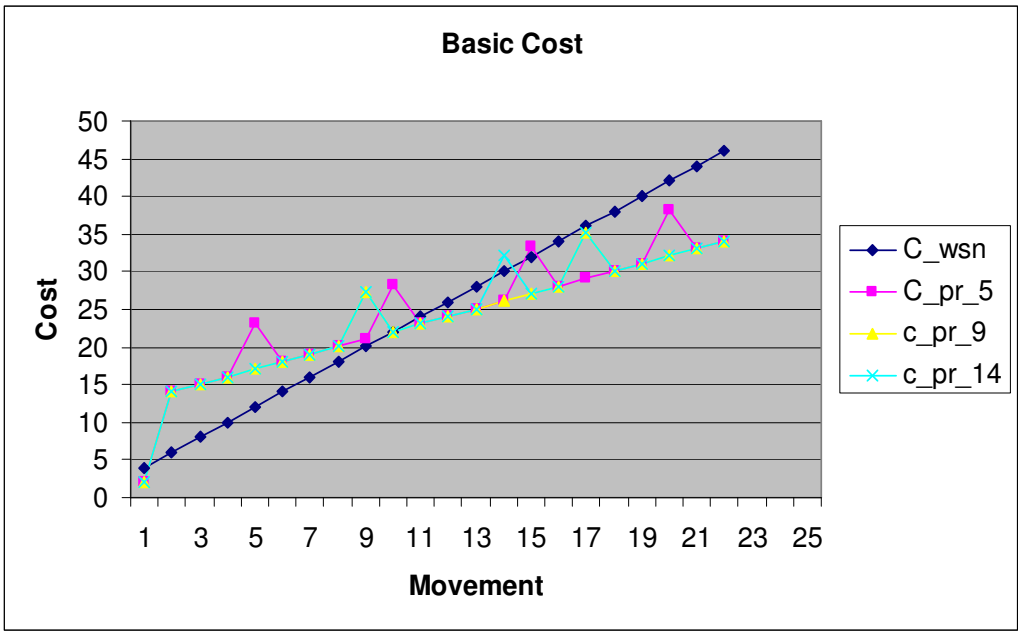

Figure 5.1 Basic cost for the proposed mechanism without probability and bursty traffic

Figure 5.1 shows the basic cost associated with each FA. Initially the MN is at the HA and it starts moving towards the different FA. As seen in the Figure the cell 21 is the maximum cell the MN can reach. As described in Chapter 4, as the MN moves, it would have to generate the new keys once the old keys expire. As seen in the Figure the cost while generating the keys is high when compared to the normal cost associated. Hence this signifies that generating the keys causes the over head. As shown in the Figure, the basic cost for the proposed scheme is higher when compared to that of the previous proposed scheme. The above cost is calculated without considering the random walk mobility model and also the bursty traffic is not considered.

As mentioned above the basic cost is cost associated for the MN to register to the HA from each FA. This cost is calculated without using the random walk probability model. The basic cost is calculated for the Bursty traffic. Figure 5.2 shows the basic cost when the traffic is bursty.

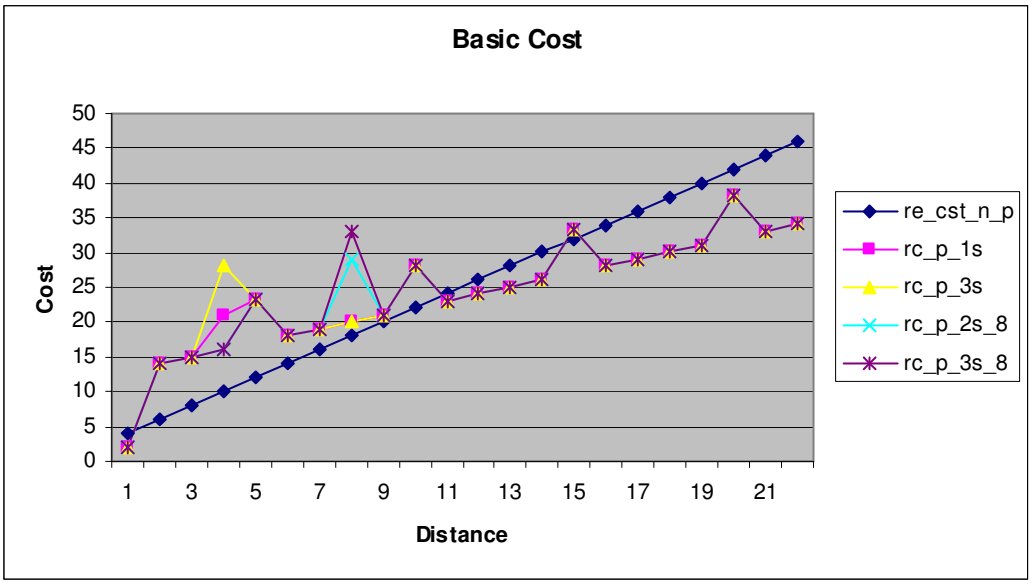

Figure 5.2: Basic cost for the proposed mechanism without probability and with bursty traffic

As shown in the Figure, the basic cost for different states is calculated and is compared to that of the previous proposed scheme. As seen in the Figure above when the traffic is bursty there might be packet loss and the mobility agents might have to re-transmit the packet which increases the overhead.

Also the above cost is calculated assuming that basic encryption system such as Ciphers and DES is used, but when the level of encryption technique increases, the processing cost at the mobility agents and the home agent increases. Hence basic cost is calculated by varying the processing cost to observe the increase in the overhead associated with increase in the level of encryption. Figure 5.3 shows the basic cost when the processing cost is increase and random walk mobility model is not considered and also the traffic is not considered to be bursty. As seen from the Figure 5.3, the basic cost increases while compared to the basic cost associated with basic encryption scheme. Hence as the encryption level increase, the cost increases this increases the overhead.

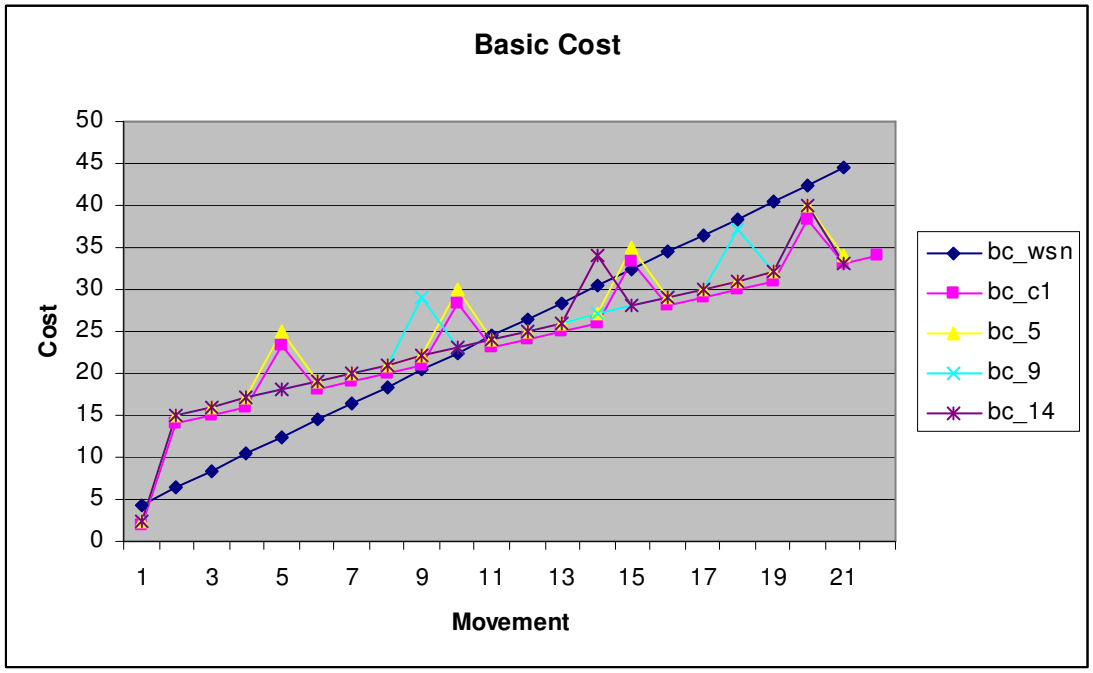

Figure 5.3: Basic cost for the proposed mechanism for higher security encryption without probability and bursty traffic

5.3 Comparison of registration cost

The registration cost is the cost required for the MN to register with the HA, from the respective FA. As described in Chapter 4 the registration cost is the combination of basic cost with the random walk mobility model. Registration cost for various scenarios have been calculated. Figure 5.4 shows the registration cost associated with each movement of the MN. As seen in the Figure the registration cost increases when compared to the previous proposed schemes. Also the registration cost is calculated for different set of keys.

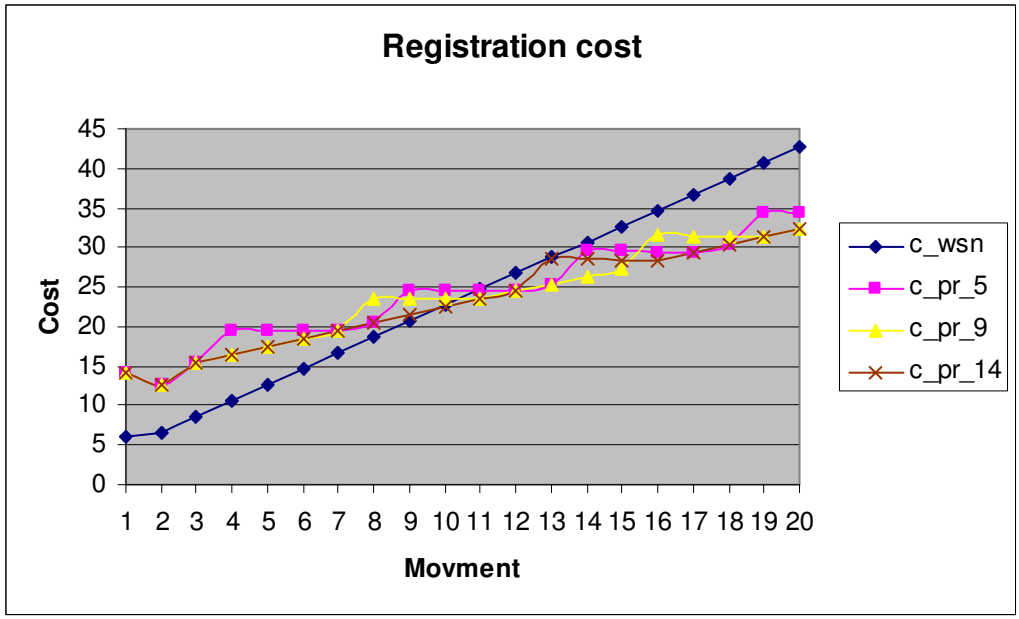

Figure 5.4: Registration cost for the proposed mechanism with probability and without bursty traffic

As seen in the Figure the registration cost increase when compared to the previous proposed schemes. Here the random walk mobility model is considered and hence the registration cost varies depending on the probability of it being in the respective FA.

Hence the registration cost associated with each movement depending upon the probability of it being in the respective FA is calculated. The above registration cost is calculated without the bursty traffic.

When the traffic is bursty, the registration cost increases as the mobility agents need to re-transmit the packets. Figure 5.5 shows the registration cost associated when the traffic is bursty.

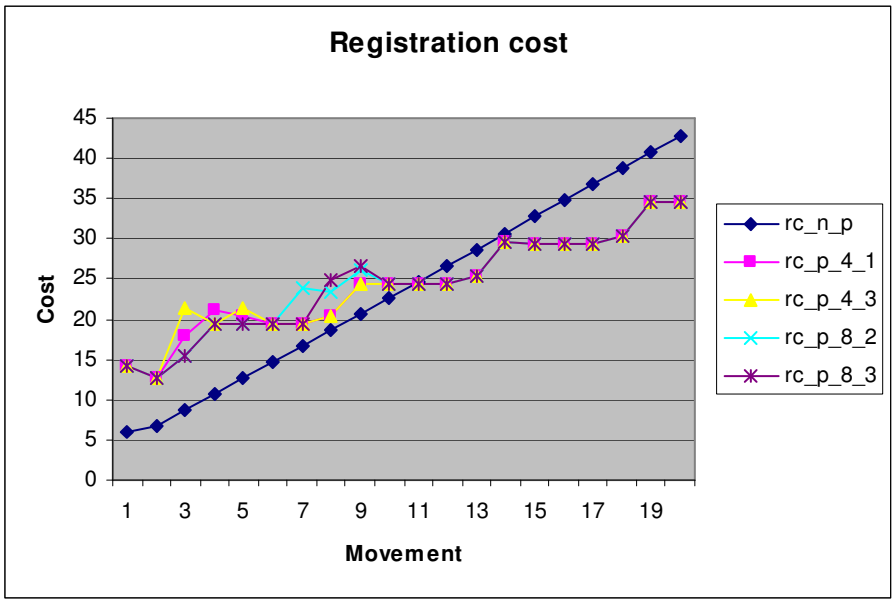

Figure 5.5: Registration cost for the proposed mechanism with probability and bursty traffic

The burst in the traffic at different movements have been observed and is found that when the traffic is bursty depending on the state, the mobility agents have to retransmit the packets, which increases the registration cost. As shown in the Figure 5.5, at the 5th movement when the traffic is bursty there is an increase in the registration cost. Also the bursty in traffic at 8th movement is observed. The above registration cost is calculated for basic security mechanism .As the level of encryption increases the

registration cost increase. Figure 5.6 shows the registration cost when the higher levels of security mechanism used.

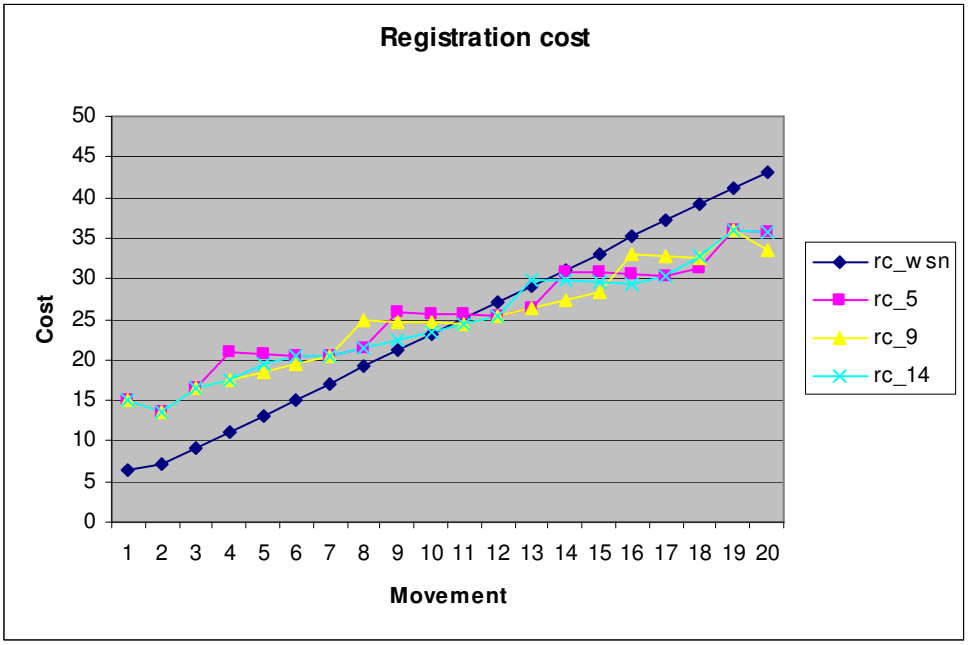

Figure 5.5: Registration cost for the proposed mechanism for higher encryption level and with probability and bursty traffic

5.4 Comparison of movement cost

As described earlier movement cost is the cost taken by the MN to detect that it has moved to a different FA. For the proposed scheme the movement cost associated with each movement is calculated. The movement cost for the proposed scheme is the product of the probability of it being in that particular FA after the n^{th} movement and the Cost associated with the each level. Here the cost associated with each level is the L2 delay and hence is constant for each level. Hence for simulation purpose, the delay is assumed to be constant and is assumed to be a value of 0.5. All the results were calculated for two values of the L2 delay. Figure 5.7 shows the movement cost between the proposed

scheme and the previous proposed scheme. As seen in the Figure, when the MN modes makes the first movement , it movement cost is highest as the MN will certainly move to the FA1, but as the movement increases , depending on the probability of the MN being in the cell , the movement cost is calculated. For example, after first movement the MN cannot be in level 3 or 4 , it can reach only level 2 , hence the probability is one , but after 5 movement , the MN could be in any cell starting from 1 to 5 , hence all the probabilities are considered and the movement cost is considered.

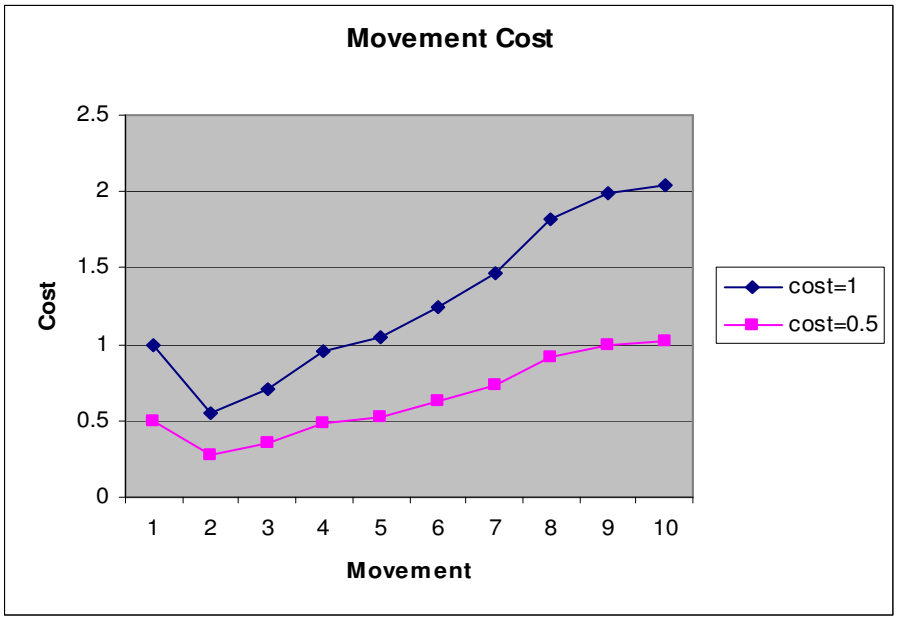

Figure 5.5: Movement cost for the proposed mechanism

From Figure 5.7 it can be concluded that the movement cost is 1 after the first movement and there by varies depending on the probabilities. As for the proposed scheme, the WSN is considered, the l2 delay is same as the previous proposed schemes,

but in the previous proposed schemes, the probabilities have not been considered and the movement cost is just the l2 delay.

5.5 Comparison of handoff cost

As described in Chapter 4, the handoff cost is the sum of registration cost and movement cost. Registration cost is always higher in the proposed method due to extra messages that need to be transmitted during the key exchange and also due to the burst ness in traffic. Movement detection cost could be same or lower when compared to the previous proposed method. If we do not consider the probability the movement cost is equal to the movement delay which is the same as the previous proposed schemes. But in the proposed scheme as the probability of the MN being in different mobility agent is considered, the movement cost remains to be lower than the previous proposed scheme. Also in the proposed scheme, the movement cost is considered for the scenario where the detection and the advertisements synchronize.

Also reducing the lifetime of the advertisements can reduce the handoff cost, but the overhead increases. Also if the wireless sensor networks are not placed properly, then the movement cost could increase as there would be increase in the delay, which might result in higher packet drops. Hence the placing of WSN also plays a crucial role.

The handoff cost for different scenarios has been calculated and is compared to that of the previous proposed schemes. Figure 5.8 shows the handoff cost for the case where the basic encryption scheme is used and the probability is not considered. As the registration cost if higher for the proposed scheme, the handoff cost is more when compared to that of the previous proposed schemes. The handoff cost is calculated for the

scenario where the length of the key is assumed to be of 14. As the length of the key varies, the registration cost varies according to it.

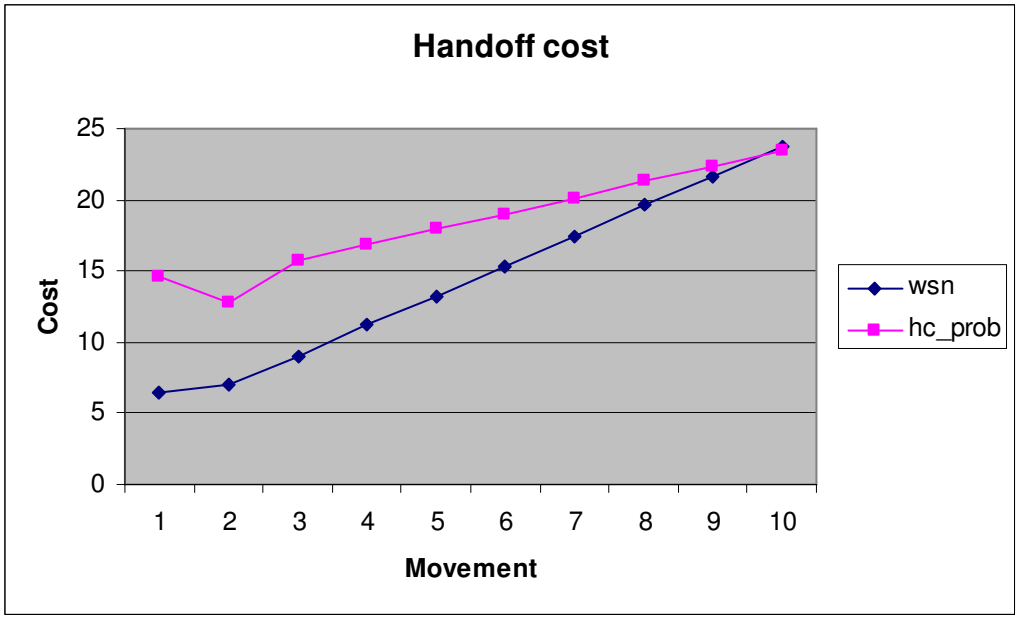

Figure 5.8: Handoff cost for the proposed mechanism with probability and without bursty traffic

The above calculated handoff cost is without considering the bursty traffic. In practical this might not be the issue as some times, the traffic could be bursty eventually results in dropping the packets. The mobility agent's needs to re send the dropped packets which results in the overhead .Figure 5.9 shows the handoff calculated when the traffic is bursty at 8^{th} movement and is compared to that of the previous proposed schemes. From the Figure it indicates that when the traffic is bursty the registration cost increases due to the overhead associated while re transmitting the packets. For the simulation purpose the processing power is considered to be 0.01 as it is constant and few other parameters such

as delta and the L2 delay are assumed to be constant. Depending on the network scenarios, these parameters can be changed.

Also the above two scenarios have been calculated while considering the encryption level to be basic. Increasing the encryption level would increase in the registration cost as the processing cost at the mobility agents increase.

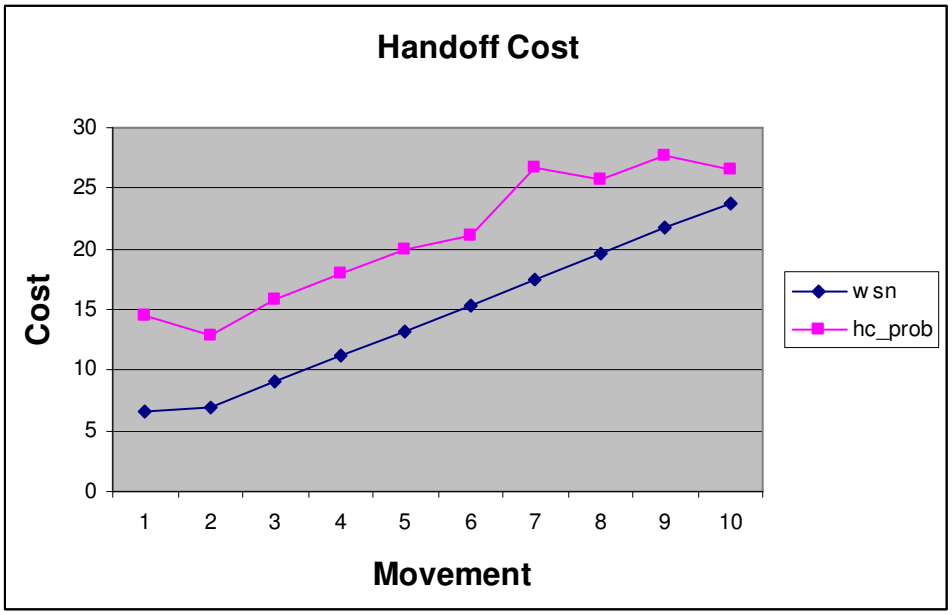

Figure 5.9: Handoff cost for the proposed mechanism with probability and with bursty traffic

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Conclusion

With the advancements in wireless technologies and mobility and demand for mobile internet, has led to a new protocol called Mobile IP which supports mobility. One of the reason for Mobile IP to accomplish lots of importance is while using Mobile IP one can stay connected to the internet even while they are. Mobile IP provides a global mobility solution and is the only protocol supports macro mobility. While mobile IP provides mobility, it does not support quality of service and also security is one of the major concern while using the mobile IP. As there is no built is support for mobility, a external security protocol needs to be applied in order to make the communication secure. Due to this, there could be overhead which would result in degradation of quality of service, which is not acceptable for real time traffic. Various security mechanism have already been proposed for making the communication more secure , while trying to minimize the handoff associated with it .Due to such issues , mobile IP is yet to undergo large scale deployment.

In this research a novel idea is proposed for making the communication more secure while minimizing the latency during handoff. Key exchange server is placed at the home agent and the subsets of keys are generated by using the key provided by the Mobile Node. These keys are provided to the mobility agents which results in more secure communication. While varying the length of the key the overhead associated with the registration cost is studied and is found that the registration cost increases with the length of the keys. Wireless sensor networks are installed at the edge of the network

boundaries of the mobility agents, hence reducing the latency during the handoff. In this research, the handoff costs associated with different encryption level are studied. Also the burst ness in traffic which is one of the important factors for a real time application is considered and their effect on the registration cost has been studied. Mobility agents are informed in advance regarding the characteristics of the Mobile Nodes, so that the mobility agent can reserve the bandwidth and hence could reduce the packet loss which improves the quality of service.

An analytical model is formed to study and compare the performance of the proposed scheme with that of the previous proposed schemes. While using the proposed scheme, the registration cost increases which is due to the overhead associated with the key exchange mechanism. Various scenarios have been considered and various parameters affecting the registration have been studied. Also with the proposed scheme, the handoff delay decreases when compared to the traditional Mobile IP. Also the cost of deployment is far less when compared to the previous proposed schemes, as with wireless sensor networks which are in placed are not expensive.

6.2 Future work

In the proposed scheme, the quality of service which is one of the important factors for real time traffic is not considered. Also an method to minimize the overhead associated with various encryption algorithms can also be an area of research. The WSN can be made more secure due to which there could be increase in the overhead and the performance can be studied. Also the overhead associated while the mobility agents communicate wirelessly can be studied.

REFERENCES

LIST OF REFERENCES

[1] http://www.davesite.com/webstation/net-history.shtml

[2] http://en.wikipedia.org/wiki/Defense_Advanced_Research_Projects_Agency

[3] BBN and the Defense Advanced Research Projects Agency by Dr. Richard and E Schantz.

[4] DARPA, "Internet Protocol" RFC 791, IETF, September 1981.

[5] C. Perkins "IP Mobility Support for IPv4" RFC 3344, IEFT, August 2002.

[6] Mobile IP Charles E. Perkins, Sun Microsystems, IEEE Communications Magazine, May 1997.

[7] C. Perkins, "Minimal Encapsulation within IP," RFC 2004, May 1996.

[8] S. Hanks *et al.*, "Generic Routing Encapsulation (GRE)," RFC 1701, Oct. 1994.

[9] RFC 3963 - Network Mobility (NEMO) Basic Support Protocol.

[10] Integrating Voice and Data Networks by Scott Keagy.

[11] Low Latency Handoff Mechanisms and their implementation in an IEEE 802.11 Network by C. Blondiaa, O. Casalsb, Ll. Cerdàb, N. Van den Wijngaerta, G. Willemsa, P. De Cleyna.

[12] K. El. Malki, "Low latency handoffs in mobile IPv4", draft-ietf-mobileip-lowlatency-handoff's-v4-07.txt, IEFT, October 2003.

[13] An Enhanced Handoff Mechanism for Cellular IP by Kyung-ah Kim, Jong-deok Kim , Chong-kwon Kim and Jae-yoon Park.

[14] HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-Area Wireless Networks T. La Porta S. Thuel K. Varadhan S. Y. Wang and R. Ramjee.

[15] A Survey on Sensor Networks by Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci.

[16] http://wwwcsif.cs.ucdavis.edu/~bharathi/sensor/snw.html.

[17] http://en.wikipedia.org/wiki/Sensor_network.

[18] Efficient Location Tracking Using Sensor Networks by H. T. Kung and D. Vlah

[19] H. T. Kung , D. Vlah “Efficient Location Tracking Using Sensor Networks” proceedings of 2003 IEEE wireless communications and networking conference (WCNC).

[20] http://en.wikipedia.org/wiki/CIA_Triad.

[21] http://everything2.com/index.pl?node_id=1265123.

[22] http://www.bitzipper.com/aes-encryption.html.

[23] http://en.wikipedia.org/wiki/RSA.

[24] http://www.cs.utexas.edu/~plaxton/c/337/05f/slides/Cryptography-3.pdf.

[25] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[26] http://en.wikipedia.org/wiki/Diffie-Hellman.

[27] Security in Computing, by Charles P. Pfleeger , Shari Lawrence Pfleeger.

[28] http://en.wikipedia.org/wiki/Triple_DES

[29] Security research on mobile IP network handover by Dong Hu and Dong Zhou.

[30] An authentication method on security association for mobile IP fast handoff by Donghai Shi and Chaojing Tang.

[31] Design and implementation of a secure Mobile IP protocol by Mufti and M. Khanum, A.

[32] ID-Based Secure Session Key Exchange Scheme to Reduce Registration Delay with AAA in Mobile IP Networks by Kwang Cheol Jeong1, Hyunseung Choo1, and Sang Yong Ha2.

[33] IDentification Key Based AAA Mechanism in Mobile IP Networks by Hoseong Jeon1, Hyunseung Choo1, and Jai-Ho Oh2.

[34] Secure Session Key Exchange for Mobile IP Low Latency Handoffs by Hyun Gon Kim1, Doo Ho Choi1, and Dae Young Kim2.

[35] Performance Analysis of IPSec and IKE For Mobile IP on Wireless Environments by Jose Caldera Dionisio , De-Niz and Junichi Nakagawa.

[36] Scalable QoS provisioning for mobile networks using wireless sensors Bahety, V.; Pendse, R.

[37] Enhanced mobility support for mobile devices using sensor networks Narayanaswamy, Vishwanath, Thanthry, Nagaraja and Pendse, Ravindra

[38] Model and Analysis of Burst Loses in VOIP using the semi-markov process by Murali Krishna Kadiyala , Ravi Pendse.

[39] R. Nelson, Probability stochastic processes and Queuing Theory : Mathematics of computer performance and Analysis . Springer-Verlag Series. 1995

[40] A Survey of Mobility Models for Ad Hoc Network Research by Tracy Camp, Jeff Boleng and Vanessa Davies.

[41] A 2D Random Walk Mobility Model for Location Management Studies in Wireless Networks by Kuo Hsing Chiang, and Nirmala Shenoy.

[42] http://www.cisco.com/Uniivercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt4/scipsec.htm

[43] ”All-in-One Cisco(r) CCIE(tm) Lab Study Guide,”Stephen Hutnik, Michael Satterlee, Osborne/McGraw-Hill; 2nd Bk&Cdr edition (May 29, 2001)

[44] www.mathworks.com.

[45] http://www.mathworks.com/access/helpdesk/help/techdoc/matlab.html.