

Secure Session Mobility using Hierarchical Authentication Key Management in Next Generation Networks

Muhammad Zubair and Xiangwei Kong

School of Information and Communication Engineering, Dalian University of Technology, Dalian, China

Email: m.zubairpaf@gmail.com, Kongxw@dlut.edu.cn

Saeed Mahfooz

Department of Computer Science, University of Peshawar, Peshawar, Pakistan

Email: saeedmahfooz@upesh.edu.pk

Abstract—In this paper we propose a novel authentication mechanism for session mobility in Next Generation Networks named as Hierarchical Authentication Key Management (HAKM). The design objectives of HAKM are twofold: i) to minimize the authentication latency in NGNs; ii) to provide protection against an assortment of attacks such as denial-of-service attacks, man-in-the-middle attacks, guessing attacks, and capturing node attacks. In order to achieve these objectives, we combine Session Initiation Protocol (SIP) with Hierarchical Mobile IPv6 (HMIPv6) to perform local authentication for session mobility. The concept of group keys and pairwise keys with one way hash function is employed to make HAKM vigorous against the aforesaid attacks. The performance analysis and numerical results demonstrate that HAKM outperforms the existing approaches in terms of latency and protection against the abovementioned attacks.

Index Terms—Next Generation Networks; Hierarchical Authentication Key Management; Session Mobility; Hierarchical Mobile IPv6; Authentication Latency

I. INTRODUCTION

Next Generation Networks (NGNs) offer the availability of a variety of resources through accessing heterogeneous technologies such as Global System for Mobile Communications (GSM), Worldwide Interoperability for Microwave Access (WiMAX), Wireless Local Area Network (WLAN), Code Division Multiple Access (CDMA), Long-Term Evolution (LTE), and so on. The expectations of NGNs users are to obtain Always Best Connected (ABC) services in their mobile devices [1] [2]. In order to achieve this goal, end-to-end communication (real-time and non real-time IP services) needs to be established. Internet Engineering Task Force (IETF) has proposed different protocols to maintain seamless mobility while establishing end-to-end communication. Among these, Mobile Internet Protocol (MIP) is considered as the main protocol for mobility at the network layer [5], whereas Session Initiation Protocol (SIP) at the application layer [3] [4].

MIP has an update version MIPv6 for NGNs which comprises several extensions such as Fast MIPv6, Seamless MIPv6, Hierarchical MIPv6, and Proxy MIPv6. The objective of these protocols is to handle the seamless mobility at the network layer. In order to consider mobility at application layer, SIP has been introduced, which has the potential of session, service, personal and terminal mobility [5] [6]. A number of approaches have been proposed in which SIP is integrated with the network layer mobility protocols such as SIP with FMIPv6, Seamless MIPv6, and HMIPv6 [6-8]. These approaches have tried to provide end-to-end communication by managing both network and session mobility together. A major contribution has made related to QoS in these approaches. However, end-to-end security is still a challenge. Several security mechanisms have been considered such as Internet Key Exchange Version 2 (IKEv2), IPSec, AAA (Authentication, Authorization, and Accounting) model, diameter protocol, Fast authentication during handover in NGN, and so on. These mechanisms are found to be unsuccessful in providing end-to-end security. In IKEv2 the limitations of communication and computational overhead make it inefficient because of cryptographic operations and number of round trips [9]. The IPSec has the lack of end to end security due to termination of IPSec terminal at IP server not at the end point [10]. The existing solutions of AAA model and diameter protocol are using security association between two entities, which is considered not to be feasible during frequent handover in NGNs. It is because the mobile node (MN) cannot be authenticated directly by local AAA (LAAA) as it does not have enough information. The information is acquired from home AAA (HAA) which results severe security holes and latency related issues [11].

In this paper we focus these issues and propose a novel approach called Hierarchical Authentication Key Management (HAKM). Session initiation protocol (SIP) is combined with HMIPv6 in this approach to handle the authentication in hierarchical manner. The main

contributions of our proposed scheme are to reduce the authentication latency and provide defence against denial-of-service attacks, man-in-the-middle attacks, guessing attacks, and capturing node attacks.

The rest of the paper is organized as follows: Section II depicts the related work and its shortcomings, whereas in Section III mobility protocols employed in HAKM are briefly described. The algorithm of HAKM is explained in Section IV, followed by the strength of proposed scheme in Section V. The performance analysis and numerical results are presented in Section VI and VII respectively. Section VIII concludes the paper and outlines the future work.

II. RELATED WORK

International Telecommunication Union (ITU-T) has designed security architecture in its recommendations X.805 for offering end-to-end communication. The architecture presents eight different directions in order to achieve end-to-end security in NGNs. These dimensions include access control, authentication, non-repudiation, communication security, data integrity, data confidentiality, and privacy. Several approaches have been proposed to provide security in NGNs. We summarize the limitations in these existing approaches [12].

A. Internet Key Exchange version 2 (IKEv2)

IKEv2 is a security protocol which has been used in HMIPv6 to offer secure association between mobile node (MN) and mobility anchor point (MAP). The limitation with this protocol is that it has certain communication and computational overhead regarding involvement of cryptographic operations and requirement of number of round trips. Especially, in remote access the use of Extensible Authentication Protocol (EAP) for authentication increases the latency. When there is failure of recovery condition, to re-establish security associations (SAs) is time consuming. Particularly, in the case of IPsec peer because a huge number of SAs need to be re-establishing with different end points. The user interaction for re-authentication through the re-establishment of an IKE SA also affected the usability [9].

B. IPsec

It was developed to offer security in Internet protocols. The limitation with IPsec is that it has complex key computation and management of algorithm. This complexity makes IPsec inefficient in mobile communication because of inadequate resources for calculation and limited lifetimes of battery in mobile devices. Another major problem in IPsec is due to having no support of end-to-end security in its existing commercial products. It is because of the termination of IPsec tunnel at the IPsec server, not at the final communication correspondent [10].

C. TLS/SRTP

Transport Layer Security (TLS) protocol is used to protect SIP signalling [13], which is extensively adopted commercially [10]. The Secure Real-time Transport

Protocol (SRTP) is used to encrypt and authenticate real-time transport protocol (RTP) packets. TLS/SRTP solution has been used to enhance the security in SIP. The limitation with this approach is that when mobile node (MN) moves across different networks, its IP address changes which disconnect the TLS/SRTP sessions. To re-establish the session, delay is occurred due to the exchange of several messages [10] [14] [15]. This greatly affects the performance regarding SIP mobility. Additionally, the responsibility of SRTP was to protect RTP packets only. No solution is there to protect non-RTP packets. Thus, the existing TLS/SRTP solution does not fulfil the security requirements for SIP in NGNs.

D. AAA Model and Diameter Protocol

To provide solution for the AAA problem regarding the request which a network receives from mobile node (MN) during its movement in foreign network, IETF has proposed AAA model [16-18] and diameter protocol [19]. Using AAA model four types of security associations (SAs) are used for sharing secret information among two network entities. The MN must provide authentication information to the domain where it using resources while roaming. One of the key challenges related to mobility of MN in conventional authentication mechanism is that MN cannot share secret information with Local AAA (LAAA) because of having no direct security association. The LAAA sends the information to Home AAA (HAAA) server of MN and wait for reply because LAAA does not have enough information to verify the authentication information of MN. This passing of information between foreign and home network makes the authentication inefficient. Additionally, the frequent handover of MN between different domains is resulting the needs of authentication for MN each time. This causes severe problem when distance increases between home network and foreign network [11].

E. Leakage Resilient-Authenticated Key Establishment

LR-AKE scheme is proposed in [20], which is based on the idea of public key infrastructure (PKI). PKI is providing prevention mechanism against all attacks but its heavy cryptographic calculation is not suitable for mobile devices. This limitation makes LR-AKE scheme inefficient in mobile communication [11].

F. Local Authentication Concept for Mobile Networks

A local authentication mechanism for mobile networks has been proposed in [21] to minimize the authentication delay. In this scheme when MN moves to foreign network for the first time, the authentication request must be sent to the HAAA server. If there is a large distance between foreign network and home network server then the delay due to authentication will be long. Moreover, a strong assumption has been made about a secret key which is pre-shared between MN and LAAA. But in AAA model there is no such concept of security association.

G. Authenticated Fast Handover in HMIPv6

A scheme proposed in [22] is based on AAA model, in which there is no security association between MN and mobility anchor point (MAP). Therefore, MAP cannot authenticate MN, and asks AAAH through AAAF (AAA server at foreign network) to generate and send the session key. If the distance is too long and frequent handover is taking place then it will result huge delay. Moreover, on the basis of analysis made in [23] this approach is declared vulnerable to several attacks such as denial of service, malicious mobile node flooding and replay attacks.

H. Fast Authentication during Handover in NGN

The fast authentication mechanism has been proposed in [24] and it has been tried to reduce handover latency, but the limitation of AAA still exists. When the MN moves from one access point to another, the information is sent to AAA server in core network which causes extra delay. Moreover no analysis and numerical results are presented to verify the efficiency of the proposed method.

III. HIERARCHICAL AUTHENTICATION KEY MANAGEMENT

A novel approach Hierarchical Authentication Key Management (HAKM) is proposed to secure session mobility in NGNs. The proposed scheme uses the concept of Combined SIP HMIPv6 [7] as shown in Fig.1, integrating two protocols such as Hierarchical Mobile IPv6 (HMIPv6) and Session Initiation Protocol. The combination is supplemented with QoS managers at both core network and each respective region to handle end-to-end QoS in NGNs. HAKM provides defence against various attacks such as denial of service (DoS) attacks, man-in-the-middle attacks, capturing node attacks, and guessing attacks. Moreover, HAKM manages the authentication mechanism locally in order to reduce delay.

The mobility protocols and QoS manager employed in HAKM are briefly described as follows.

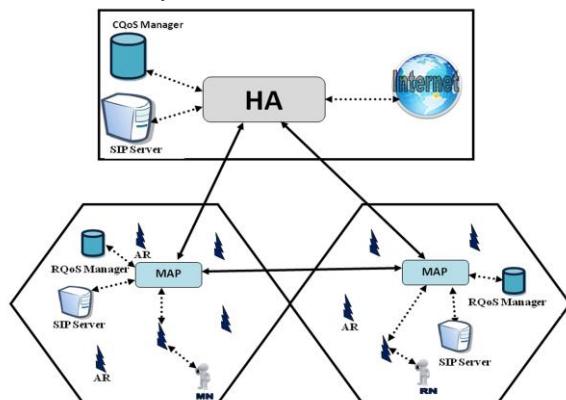


Figure 1. Architecture of HAKM

A. Hierarchical Mobile IPv6 (HMIPv6)

Various mobility protocols such as MIP, MIPv6, Fast MIPv6, HMIPv6, and so on are used in wireless communication to access any network through several radio access methods. The parental mobility protocol is

MIP, and all the other mobility protocols are extensions of MIP [25]. The mobility management protocol used for the next generation of the IP is MIPv6. The limitations in MIPv6 are exchange of messages during frequent handover of MN. If HA is located far away from MN, then these messages are resulting extra delay, signalling overhead, and security issues [26].

In order to resolve these issues, HMIPv6 is used to handle the signals and traffic locally [27]. It has hierarchical structure which reduces the amount of signalling exchange between distinct entities like HA, MAP, MN, and resultant node (RN). HMIPv6 has Mobility Anchor Point (MAP) at each region, which acts as local HA. MAP has been introduced in the updated RFC 5380, which have made HMIPv6 more efficient. Two types of addresses are used in HMIPv6, the first one is regional care of address (RCoA), and the second one is on-link care of Address (LCoA). Each region is represented by RCoA, whereas LCoA is the address of the access router through which MN is connected with MAP [28] [29].

When MN initiates handover within the region, only its LCoA is changed at MAP. The change of LCoA means that MN moving from one access router to another. Both HA and RN are unaware of the local handover. This transparency helps in reducing delay, minimizing signalling overhead, and making the communication secure.

If MN is moving from one region to another, its RCoA is changed and updated at HA. The updated RCoA is then forwarded to RN in order to continue the communication. HA and RN have the knowledge of MN's RCoA only.

B. Session Initiation Protocol (SIP)

SIP is a text based signalling protocol defined by the Internet Engineering Task Force (IETF) [3]. It is an application layer protocol, which can establish and tear down the multimedia sessions. Various entities like user agents, proxy servers, redirect servers, and registrars are used in SIP [29] [30]. User agent means both the ends participate in the communication. Proxy servers can act as both client and server, and its main functionality is routing. It works as an intermediary entity to make the request on behalf of other clients.

The main function of redirect server is to allow proxy servers to direct the SIP session invitation to outside regions. Registrar is a server used to accept REGISTER requests for the registration of one or more IP addresses to a certain SIP URL. It is commonly located with SIP proxies, but it can be placed with redirect server for network scalability [6] [26].

SIP support four types of mobility, these are terminal mobility, personal mobility, session mobility, and service mobility. In order to establish session, the mobility is performed in SIP at following two stages [31].

Pre-call mobility: When MN obtains a new IP address before receiving or making call, it will register itself by sending REGISTER message to SIP server connected with MAP. The registrar in SIP server will register this address.

TABLE I. DESCRIPTION OF NOTATIONS

Notation	Definition	Notation	Definition
RCoA	Regional Care of Address	K_G	Group key between HA and MAP
LCoA	On-Link Care of Address	K_g	Group key between MAP and MN
RK	Region Key for each region	K_{gp}	Group key between Two MAPs'
RSK	Region SubKEY	K_{gl}	Group key between MN and RN
$RN_{HA}, RN_{MAP}, RN_{MN}$	Random Numbers created by HA, MAP and MN	MAC	Message Authentication Code
SK	Sub Key within regions	$H(\cdot)$	A collision-resistant cryptographic hash function
K_{temp}	Temporary session key	\oplus	XOR operator
PK	Pairwise Key	\parallel	A concatenation operator

The INVITE message is sent by RN to SIP server for making session with MN [31] [6]. SIP server in reply forwards the address of MN. RN communicates with MN directly using INVITE message. When the Ok message received from MN, it means the session is established successfully.

Mid-call mobility: If MN initiates the handover during ongoing session, then mid-call mobility is performed. MN send re-INVITE message to SIP proxy server, which is sent to RN. The RN replies with the 200ok message to continue the session smoothly.

C. QoS Manager

As NGNs are the combinations of heterogeneous networks. Hence, managing this diverse nature of NGNs is a challenging task. Further, if the goal is to enhance security in NGNs, then we have to shell out for this. Therefore, quality of service (QoS) cannot be ignored. For this purpose, the proposed method includes QoS manager, which handles QoS issues like bandwidth management, reservation of resources, and network policies' implementation [6] [7]. Handovers of varied natures are also handled using this module. It makes sure that the resources are provided in advance when MN initiates handover.

In our proposed method, QoS managers are employed at two levels. The first level consists of core QoS (CQoS) manager, which handles QoS issues at the core network. CQoS manager is also responsible to provide resources upon the request made by any regional QoS manger due to shortage of resources in its region.

The second level comprises regional QoS (RQoS) manager, used to manage the QoS issues in their respective regions. RQoS managers of different regions coordinate with one another to establish seamless communication.

IV. HAKM ALGORITHM

The step by step procedure of Hierarchical Authentication key Management is explained in following different phases.

A. Initialization Phase

The Home Agent (HA) creates a key chain of size M before deploying the N Mobility Anchor Points (MAP) at various regions. The size of key chain in HA is greater than key chain in MAP that is $M > N$. Home Agent (HA) selects unique key for each MAP, which is considered to be the region key (RK).

Before making into operational, HA utilizes RK and random number RN in order to create region subkey $RSK = H(RK \oplus RN)$. The HA then uses RSK and random numbers from $R_1 \sim R_n$ to generate a key chain for each MAP.

$$SK_0 = H(RSK_1 \oplus R_1),$$

$$SK_1 = H(RSK_2 \oplus R_2),$$

.

.

.

$$SK_{n-2} = H(RSK_{n-1} \oplus R_{n-1}),$$

$$SK_{n-1} = H(RSK_n \oplus R_n)$$

Each MAP set unique key chain, RSK, and random numbers $R_1 \sim R_n$ from HA. Same hash function $H(\cdot)$ and K_{temp} is used in the hierarchy. The K_{temp} is a temporary session key for all HA, MAP, and MN where as:

$$K_{temp} \neq RK$$

To understand the proposed scheme effectively, various notations are described in Table I.

B. Authentication Phase

In order to authenticate different entities like MAP to HA, Mobile Node (MN) to MAP, and MAP to MAP, following stages are employed in HAKM.

1) Authentication of MAP with HA

i The HA broadcasts message that is "Hello Message" to the entire MAPs' which includes:

$$HAID \parallel \text{Hello Message} \parallel \text{IP address} \parallel \{RN_{HA}\} K_{temp}$$

Where as

HAID = identity number of Home Agent,

IP address = Address of Home Agent,

RN_{HA} = Random Number sent by HA

K_{temp} = temporary session key to encrypt RN_{HA}

ii The MAP receives hello message from HA and creates pairwise key using its Regional Care of Address (RCoA) and RN_{HA} .

$$PK = \{H(RN_{HA} \parallel RCoA)\} K_{temp}$$

MAP replies to HA using response message and pairwise key. The message includes:

$$HAID \parallel \text{response message} \parallel RCoA \parallel \{MAC(PK) \parallel RCoA\} K_{temp}$$

iii When the HA receives response message and RCoA from the MAP, then HA creates pairwise key.

$$PK' = \{H(RN_{HA} \parallel RCoA)\} K_{temp}$$

A condition is checked after creating pairwise key by HA which is $IF (MAC(PK') = MAC(PK))$. If the condition is true then HA confirm that MAP is valid, and if condition is false then HA reject response message.

iv If condition becomes true, then Home Agent (HA) transmit the group key K_G for connection between HA and MAP using pairwise key. Furthermore, the future messages are encrypted by K_G and the format of the new key message is presented below.

HA (ID) || RCoA || { K_G } PK

The flow of MAP authentication with HA is shown in Fig. 2.

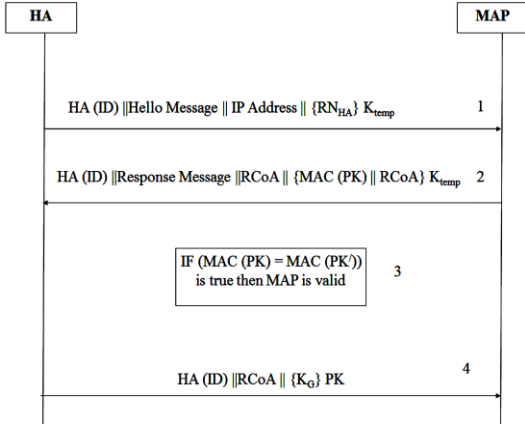


Figure 2. Authentication of MAP with Home Agent (HA)

2) Authentication of MN with MAP

When the MN wants to make a connection with MAP, first it needs to be authenticated to check that whether it is valid or not. Following steps need to be followed to authenticate the MN with MAP.

i Mobility Anchor Point (MAP) broadcasts “hello message” to the Access Routers (ARs) which comprises of:

RCoA || Hello Message || { RN_{MAP} } K_{temp}

ii The Access Routers (ARs) receive hello message from many MAPs, and connect the MN with the MAP having strong signals. A pairwise key is created using its own LCoA and RN_{MAP} transmitted by MAP.

$PK = \{H(RN_{MAP} || LCoA)\} K_{temp}$

Response message is sent to MAP having strong signal in order to authenticate MN with MAP. The message includes:

RCoA || response message || LCoA || {MAC (PK) || LCoA} K_{temp}

iii When MAP receives the response message and LCoA, it creates pairwise key to check that MN is valid or not.

$PK' = \{H(RN_{MAP} || LCoA)\} K_{temp}$

After creating pairwise key, the condition $IF (MAC (PK') = MAC (PK))$ is checked. If it is true the MAP confirms that MN is valid otherwise rejected.

iv When condition is true and to encrypt the succeeding messages, a group key K_g is sent by MAP to MN using pairwise key. The format of new key message is mentioned below.

RCoA || LCoA || { K_g } PK

The flow of MN authentication with MAP is shown in Fig. 3.

3) Authentication between Two MAPs

For the communication between two MAPs, first the authentication should be performed whether the

requesting MAP is valid or not. Suppose MAP1 wants to communicate with MAP2, the authentication is performed using following steps.

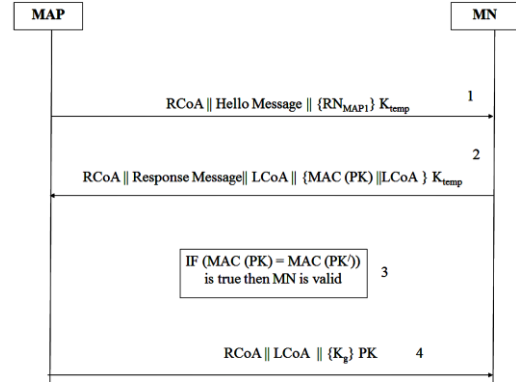


Figure 3. Authentication of MN with MAP

i The MAP1 sends Hello Message to MAP2. The message consist of:

RCoA (MAP1) || Hello Message || RCoA (MAP2) || { RN_{MAP1} } K_{temp}

ii When MAP2 receives message from MAP1, a pairwise key is created by MAP2.

$PK = \{H(RN_{MAP1} || RCoA (MAP2))\} K_{temp}$

In order to reply MAP1, MAP2 sends response message which is consist of:

RCoA (MAP1) || response message || RCoA (MAP2) || {MAC (PK) || RCoA (MAP2)} K_{temp}

iii On arrival of response message and RCoA (MAP2), the MAP1 creates pairwise key for the validity of MAP2.

$PK' = \{H(RN_{MAP1} || RCoA (MAP2))\} K_{temp}$

The condition $IF (MAC (PK') = MAC (PK))$ is checked. If it is true, it means MAP2 is valid and if the condition is false, MAP1 rejects MAP2.

iv When MAP1 confirms that MAP2 is valid, then a group key K_{gp} using pairwise key is sent to MAP2 for future messaging. The new key message includes:

RCoA (MAP1) || RCoA (MAP2) || { K_{gp} } PK

The flow of authentication between two MAPs is shown in Fig. 4.

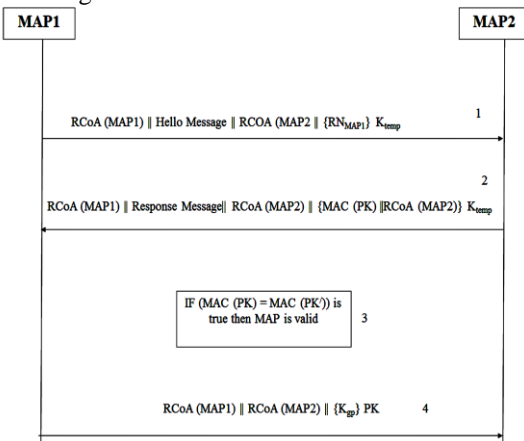


Figure 4. Authentication between two MAPs

C. Secure Session Mobility

In order to establish the session between MN and RN, two types of mobility are focused. At the beginning of a

communication when session is established, it refers to pre-call mobility. During MN movement, if the handover is initiated, then mid-call mobility is applied to maintain the session smoothly.

In both types of mobility security is an important factor to be considered. Our proposed scheme presents an invulnerable mechanism to maintain the security either at the start of session or at the middle of a session.

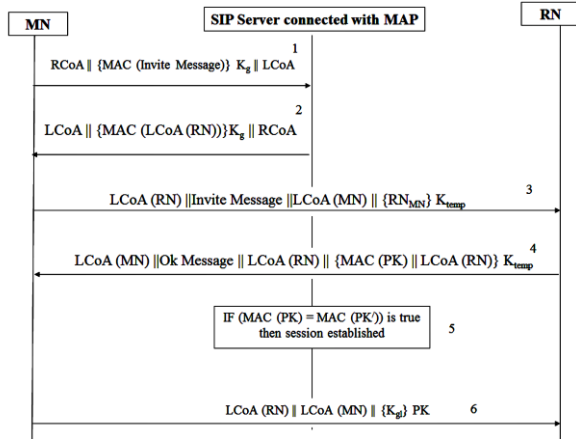


Figure 5. Pre-call mobility authentication

1) Pre-call Mobility Authentication

Here pre-call mobility authentication is considered for the case when MN wants to communicate with RN, and both located at the same region. Following steps need to be performed while establishing secure pre-call mobility.

i MN sends INVITE message to SIP server connected with MAP. The message is encrypted with group key that is K_g . The message includes:

$RCoA || \{MAC (Invite message)\} K_g || LCoA$

Whereas RCoA is the Regional Care of address of MAP to which MN and SIP server are connected. LCoA is on-Link Care of Address of MN.

ii The SIP server sends the address of RN which is also encrypted with K_g . Here the RN belongs to same region, so the LCoA of RN is sent to MN. The message from SIP server to MN includes:

$LCoA || \{MAC (LCoA (RN))\} K_g || RCoA$

iii MN directly communicates with RN by sending INVITE message for establishing session. The message comprises random number RN_{MN} to create pairwise key and checks that whether the RN is valid.

$LCoA (RN) || Invite message || LCoA (MN) || \{RN_{MN}\} K_{temp}$

iv In response to MN INVITE message, RN creates pairwise key that is $PK = \{H (RN_{MN} || LCoA (RN))\} K_{temp}$. RN sends Ok message to MN which includes:

$LCoA (MN) || Ok message || LCoA (RN) || \{MAC (PK) || LCoA (RN)\} K_{temp}$

v When MN receives Ok message, it creates pairwise key using its own random number and LCoA of RN.

$PK' = \{H (RN_{MN} || LCoA (RN))\} K_{temp}$

A condition is checked that is $IF (MAC (PK) = MAC (PK'))$. The result with true indicates that RN is valid node and a secure session is established. The result with false prevents the MN to establish session with invalid node.

vi With the validity of RN and session establishment, MN sends group key K_g encrypted with PK to RN for secure messaging in future. The message consist of:

$LCoA (RN) || LCoA (MN) || \{K_g\} PK$

The flow of authentication in pre-call mobility is shown in Fig. 5.

For the case when RN located outside MN region, the MAP of MN forward the INVITE message to SIP server at Home Agent. SIP server replies with RCoA of RN. The MAP of MN makes the connection with MAP of RN using proper authentication, and forward INVITE message to SIP server at RN region. After receiving LCoA of RN, the MN establishes session and authenticates it using pairwise key. A group key is used for future messaging between RN and MN.

2) Mid-call Mobility Authentication

During ongoing session, when MN initiates handover within same region or from one region to another, a smooth session is established before breaking the previous one. This session establishment during movement refers to mid-call mobility. In order to maintain security during mid-call mobility, following steps are performed.

i MN sends re-INVITE message to RN encrypted with group key K_g . The message includes:

$LCoA (RN) || \{MAC (re-INVITE message)\} K_g || LCoA (MN)$

ii After receiving re-INVITE message, RN sends the following message to continue the smooth communication.

$LCoA (MN) || \{MAC (200ok message)\} K_g || LCoA (RN)$

If any node moving outside of the region during ongoing session, its new RCoA and LCoA is authenticated first and then mid-call mobility is performed.

V. STRENGTH OF HAKM AGAINST ATTACKS

The security can be breached by an outsider node which has lack of knowledge about the Keys in the key chain or about pairwise keys. It can be a node, which is captured by an attacker and act as an internal node.

Our proposed scheme focuses the possible attacks that can be made by an attacker. These attacks are discussed here such as denial of service (DoS) attacks, man-in-the-middle attacks, capturing node attacks, and guessing attacks.

A. Denial of Service (DoS) Attacks

The common attacks which are considered in networks are denial of service attacks in which the malicious entity makes a service unavailable to the intended users. The attackers can make the services unavailable such as occupying the network available bandwidth, CPU power consumption, occupying memory in the server, and network equipments without proper authorization.

In our proposed scheme, defence mechanism is presented against DoS. It is due to the use of MAC and one-way hash function in which the HA, MAP, MN and RN exchange messages without expecting any acknowledgment. If an attacker tries to stop the message

from reaching to the nodes, the HA, MAP, and MN are unaware of this.

B. Man-in-the-Middle Attacks

Man-in-the-middle attacks are considered as a category of eavesdropping in which the malicious entity establishes autonomous connection with the nodes and takes over the control to handle all the messages between MN and RN. Both MN and RN think that they are directly communicating with one another through a private connection. However, in real an attacker makes them fool and controlled all their details.

The proposed scheme uses pairwise keys and group keys between all the entities like HA, MAP, MN, and RN in a hierarchical manner. Therefore, if malicious entity has no knowledge about the pairwise keys or group keys, it still cannot make this attack. An attacker cannot eavesdrop and even cannot make changes in the message. Thus, man-in-the-middle attack does not have any influence on NGNs using this scheme.

C. Capturing Node Attacks

As NGNs are mixture of heterogeneous networks, preventing this type of attack is very difficult. The attacker can try to obtain some material of the K_{temp} and pairwise key from any node using the capturing node attacks. In our proposed scheme the K_{temp} is only used to create pairwise key in each hierarchy and then discarded. Different pairwise keys are used in each hierarchy. Therefore based on characteristics of pairwise keys, if the adversary captured any node and try to obtain its internal material and harm other nodes, it cannot be happened.

D. Guessing Attacks

Guessing attacks are considered an important attack in any security system. Suppose that a malicious entity can get data or information related to keys in NGNs. The key can also be guessed using public information. In our proposed scheme, the key at each hierarchy is changed at regular intervals. Furthermore, different group keys and pairwise keys are used at each hierarchy to encrypt messages, so guessing attack cannot infect this system.

VI. PERFORMANCE ANALYSIS OF HAKM

A. Analytical Authenticated Mobility Models

The hexagonal structure shown in Fig. 6 is used for our authenticated mobility models. The structure shows an example of MAP region which is composed of cells surrounded by circles of cells. Every region consists of C circles of the same size. The inner most cell at the centre is represented by "0" surrounded by circle having cell denoted by "1". Similarly the no "2" represents cells in circle 2 and it is also assumed that each cell is managed by one access router. The total number of cells up to circle C in a MAP region is represented in following equation.

$$N(C) = \sum_{c=1}^C 6c + 1 = 3C(C+1) + 1 \quad (1)$$

Two types of mobility models such as fluid-flow and random-walk models [32] [33] are used for the analysis of HAKM. Fluid-flow model is suitable for the users moving with erratic speed, high mobility, and changing of directions. Whereas, random-walk model is appropriate for mobility of pedestrian users having small geographical area such as residential area or campus.

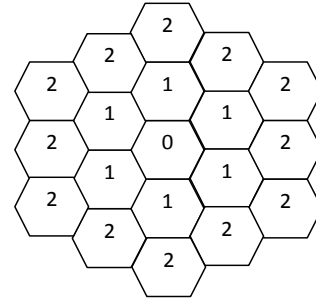


Figure 6. Mobility models structure

1) Fluid-flow Model

The MN roaming within a MAP region is spread in the range of $(0, 2\pi)$ using fluid-flow model. Let S be the average speed of MN (m/s), r the cell radius, d the density of the user in a cell, P_a , P_b the perimeters of cell and MAP region with N circles, and C_a , C_b represent region crossing rates. These are represented in (2) and (3).

$$C_a = \frac{d \times S \times P_a}{\pi} = \frac{d \times S \times (6r)}{\pi} \quad (2)$$

$$C_b = \frac{d \times S \times P_b}{\pi} = \frac{d \times S \times (12C + 6)r}{\pi} \quad (3)$$

2) Random-walk Model

In random-walk model the upcoming position of MN is calculated by its preceding position in addition with the value of random variable drawn from an arbitrary distribution. It is assumed that the current position of MN in a cell of circle "c", the probability of moving ahead to another cell of circle "c+1" or backward to a cell of circle "c-1" are represented in (3) and (4).

$$P^+(c) = \frac{1}{3} + \frac{1}{6c} \quad (4)$$

$$P^-(c) = \frac{1}{3} - \frac{1}{6c} \quad (5)$$

The probability of MN staying in current cell and moving to another cell is assumed k and $1-k$ respectively. $P_{c, c+1} = (1-k)$ if $c = 0$,

$$P_{c, c+1} = (1-k) \times \left[\frac{1}{3} + \frac{1}{6c} \right] \text{ if } 1 \leq c \leq C \quad (6)$$

$$P_{c, c-1} = (1-k) \times \left[\frac{1}{3} - \frac{1}{6c} \right] \text{ if } 1 \leq c \leq C \quad (7)$$

TABLE II. DELAYS COMPARISON

Protocols	MR & CoA Config.	Authentication Delay	BU delay	Packet Delay	Total Delay
MIPv6	$T_{(MR \& NAC)}$	$3(T_{MH} + T_{HR})$	$2(T_{MH} + T_{HR})$	$(T_{MH} + T_{HR})$	$T_{(MR \& NAC)} + 6T_{MH} + 6T_{HR}$
FMIPv6	$T_{(MR \& NAC)}$	$3(T_{MH} + T_{HR})$	-	$T_{MH} + 2T_{HR}$	$T_{(MR \& NAC)} + 4T_{MH} + 5T_{HR}$
SMIPv6	$T_{(MR \& NAC)}$	$3(T_{MH} + T_{HR})$	T_{MR}	T_{MR}	$T_{(MR \& NAC)} + 3T_{MH} + 3T_{HR} + 2T_{MR}$
HAKM	$T_{(MR \& NAC)}$	$T_{MM} + T_{MR}$	T_{MM}	$T_{MM} + T_{MR}$	$T_{(MR \& NAC)} + 2T_{MR} + 3T_{MM}$

Equations (6) and (7) represent the transition probability from the state c to $c+1$ or $c-1$.

Assuming $\pi_{c,c}$ is a steady-state probability of state c inside a MAP region of C circles. The $\pi_{c,c}$ is represented in (8) using the transition probabilities.

$$\pi_{c,c} = \pi_{0,c} \prod_{i=0}^{c-1} \frac{P_{i,i+1}}{P_{i+1,i}} \quad (8)$$

As Markov chain property states that the summation of all the steady-state probabilities is equal to 1, so the $\pi_{0,c}$ is represented as:

$$\pi_{0,c} = \frac{1}{1 + \sum_{c=1}^C \prod_{i=0}^{c-1} \frac{P_{i,i+1}}{P_{i+1,i}}} \quad (9)$$

B. Latency Analysis

The performance of the HAKM is compared with the authentication mechanism in MIPv6, Fast MIPv6, and SMIPv6. In Fig. 1, the architecture of proposed approach is shown, in which MN wants to communicate with RN. The delay between MN and HA, HA and resultant node, MN and MAP, MAP to MAP, access routers, and MAP to RN is represented by T_{MH} , T_{HR} , T_{MM} , T_{M-M} , T_{ArAr} and T_{MR} respectively.

When handover is initiated the following steps are performed for the successful communication between MN and RN.

Movement recognition (MR) and new CoA configuration ($T_{(MR \& NAC)}$)

Authentication (T_A)

Binding Update (T_{BU})

Packet Delivery (T_{PD})

The total delay is the sum of the time durations for the above four steps.

$$T_D = T_{(MR \& NAC)} + T_A + T_{BU} + T_{PD} \quad (10)$$

3) Latency in MIPv6

The MN in MIPv6 discovers its movement through router solicitation or router advertisement when it enters new subnet. The new CoA is configured by MN using prefix information in router advertisement. For the verification of unique new CoA, Duplicate Address Detection (DAD) is used. The delay for detecting movement and new CoA gaining is represented in following formula.

$$T_{(MR \& NAC)} = T_S + T_{RAdv} + T_{DAD}$$

Where, T_S represent delay for router solicitation

T_{RAdv} represent delay for router advertisement

T_{DAD} represent delay for DAD.

When new CoA is configured, then authentication is performed which at least 1.5 round trip delay needs between the MN and RN [6]. The total delay for authentication is represented as follows.

$$T_A = 3(T_{MH} + T_{HR})$$

The delay for BU request and reply is shown below.

$$T_{BU} = 2(T_{MH} + T_{HR})$$

After authentication and BU, the delay for Packet delivery is:

$$T_{PD} = (T_{MH} + T_{HR})$$

Thus, the total delay from start of the handover to the successfully delivery of packet is represented as follows.

$$T_D = T_{(MR \& NAC)} + 3(T_{MH} + T_{HR}) + 2(T_{MH} + T_{HR}) + (T_{MH} + T_{HR}) \quad (11)$$

$$T_D = T_{(MR \& NAC)} + 6(T_{MH} + T_{HR})$$

4) Latency in FMIPv6

The delays for movement detection, CoA configuration, and authentication are same like in MIPv6. But the delays for binding updates and packet delivery are different which are computed below.

During the handover procedure there is no BU procedure in FMIPv6, so it is not considered. The delay for delivery of packets to new location of MN is increased as compared to MIPv6 and HMIPv6. The reason is packet is forwarded to AR1 firstly and then again relays to AR2 during the movement of MN from AR1 to AR1. Hence the delay for packet delivery is expressed below.

$$T_{PD} = T_{MH} + T_{HR} + T_{ArAr}$$

If HA is aggregator router, then T_{ArAr} is:

$$T_{ArAr} = T_{HR}$$

$$T_{PD} = T_{MH} + T_{HR} + T_{HR}$$

Therefore,

$$T_D = T_{(MR \& NAC)} + 3(T_{MH} + T_{HR}) + T_{MH} + T_{HR} + T_{HR} \quad (12)$$

$$T_D = T_{(MR \& NAC)} + 4T_{MH} + 5T_{HR}$$

5) Latency in SMIPv6

In SMIPv6, the MN detects its movement using router solicitation or router advertisement when it predicts to enter into new subnet. The MN then configures its new CoA, employs DAD to automatically generate unique addresses and remove the requirement of validating uniqueness of new addresses. The delays for movement detection and new CoA are calculated as:

$$T_{(MR \& NAC)} = T_S + T_{RAdv} + T_{DAD}$$

The authentication latency is represented as:

$$T_A = 3(T_{MH} + T_{HR})$$

The delay for BU is calculated as:

$$T_{BU} = T_{MR}$$

The delay for packet delivery is computed as:

$$T_{PD} = T_{MR}$$

The total delay is represented in following equation.

$$T_D = T_{(MR \& NAC)} + 3(T_{MH} + T_{HR}) + T_{MR} + T_{MR} \quad (13)$$

$$T_D = T_{(MR \& NAC)} + 3T_{MH} + 3T_{HR} + 2T_{MR}$$

6) Latency in HAKM

In our proposed approach HMIPv6 is used which manages the authentication and traffic locally, and delay is reduced to handsome amount. The delays for detection of movement, CoA configuration and packet delivery are same like MIPv6, but the delays for authentication and binding updates are different which are calculated below.

As the authentication is handled locally, so the problem of round trip delay is resolved in HMIPv6. Thus, the delay for authentication is expressed as:

$$T_A = T_{MM} + T_{MR}$$

As the MN moves and its mobility is handled locally, so the BU delay is significantly reduced which is represented below.

$$T_{BU} = T_{MM}$$

The delay for packet delivery is expressed as:

$$T_{PD} = T_{MM} + T_{MR}$$

Therefore, the total calculated delay in proposed method is shown as follows.

$$T_D = T_{(MR \& NAC)} + T_{MM} + T_{MR} + T_{MM} + T_{MR} \quad (14)$$

$$T_D = T_{(MR \& NAC)} + 2T_{MR} + 3T_{MM}$$

The comparison in Table II demonstrates that the delay calculated in HAKM is greatly reduced which makes it efficient as compared to MIPv6, FMIPv6, and SMIPv6.

VII. NUMERICAL ILLUSTRATIONS

In this section we present the numerical results of HAKM and its comparison with MIPv6, FMIPv6, and SMIPv6. The OPNET simulation tool is used to obtain numerical results. NGNs environment is deployed consisting of heterogeneous networks such as core network, WiMAX, TDMA based network, WLAN and simple voice network. The common parameters set for the simulation are shown in Table III.

TABLE III. SIMULATION PARAMETERS

Network size	2000m*2000m
Wired bandwidth	1Gb/s
Wireless link bandwidth	100Mb/s
Packet size	1 Kb
Moving speed	5-45m/s, 10-90m/s for fast moving devices
Packet rate	150 packets/s
Processing time (t_{proc})	5 ms
handover latency of layer 2 (t_{L2})	10 ms
Simulation time	400s

In our proposed scheme each region comprises of MAP, RQoS manager, SIP server, and also equipped with HAKM mechanism. The mobility and authentication is handled locally which reduce the latency to great extent. Moreover attacks like denial-of-service attacks, man-in-the-middle attacks, guessing attacks, and capturing node attacks are performed to check the strength of HAKM. The results demonstrate that the proposed scheme

strongly protects the communication between MN and RN against the above mentioned attacks.

Figs. 7, 8, and 9 demonstrate the relationship between authentication latency and average velocity of user for MAP region. The results in Figs. 7 and 8 are using random-walk model. The stay of MN in current region results the lower latency and less likely to move between regions. In Fig. 7 the authentication latency is obtained for handover within region.

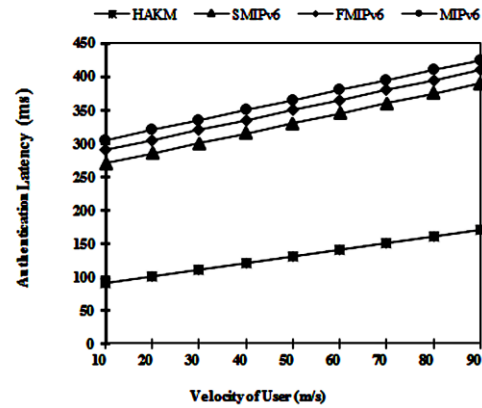


Figure 7. Authentication latency during handover within region

Fig. 8 shows the authentication latency when the MN moves from one region to another. The results reveal that HAKM is quite efficient and having less latency as compared to MIPv6, FMIPv6, and SMIPv6.

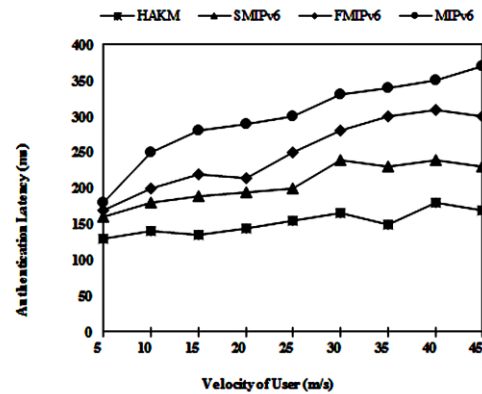


Figure 8. Authentication latency during handover from one region to another

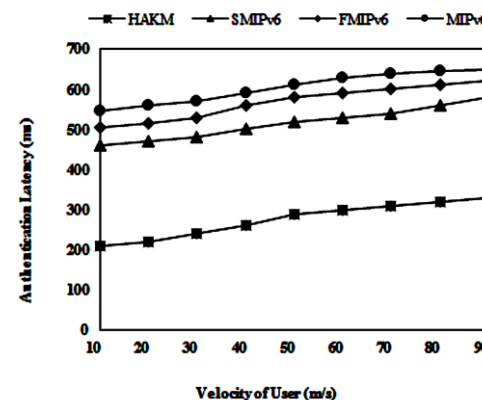


Figure 9. Authentication latency during fast movement

In Fig. 9, the authentication latency is shown for fast moving device such as vehicular. Fluid-flow model is used, in which the lower velocity is resulting a lower cell/region crossing rate and less delay. The result shows that by increasing the speed the authentication latency is increased. Variation in results is because of increasing and decreasing the speed of vehicular device. Our proposed mechanism results seem outstanding in fast moving device as compared to MIPv6, FMIPv6, and SMIPv6.

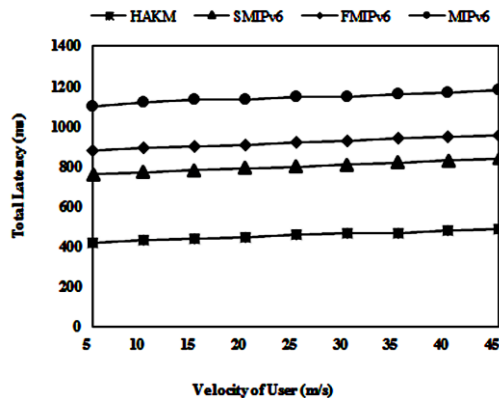


Figure 10. Overall latency

The sum of all the latencies that is $T_D = T_{(MR \& NAC)} + T_A + T_{BU} + T_{PD}$ is shown in Fig. 10. The result shows the latency for our proposed approach which lies between 400 to 500ms and it is quietly reduced as compared to MIPv6, FMIPv6, and SMIPv6. It is verified that by handling the authentication, signal, and traffic locally the latency is reduced to handsome amount.

VIII. CONCLUSIONS AND FUTURE WORK

In this paper we proposed a novel Hierarchical Authentication Key Management to handle the security locally during session mobility. Combination of SIP with HMIPv6 is employed to manage the authentication in hierarchical order. The target objectives of HAKM are reducing the latency and defence against the attacks including denial-of-service attacks, man-in-the-middle attacks, guessing attacks, and capturing node attacks. The efficiency of proposed approach is compared with MIPv6, FMIPv6, and SMIPv6. Two types of mobility models such as fluid-flow model and random walk model are used for the performance analysis. Numerical results are obtained based on mathematical analysis which verified that HAKM is quite efficient.

Further study will be carried out to evaluate the performance of HAKM approach in terms of processing cost and packet loss. The target will be to make our approach more efficient.

REFERENCES

[1] Dong-Hoon, S., et al., "Distributed mobility management for efficient video delivery over all-IP mobile networks: Competing approaches," *IEEE. Network*, 27(2), pp. 28-33, 2013.

[2] E. Gustafsson and A. Jonsson, "Always best connected," *IEEE Wireless Communications Magazine*, 10, pp. 49-55, 2003.

[3] J. Rosenberg, et al, "SIP: Session Initiation Protocol," *IETF RFC 3261*, 2002.

[4] W. Wu, N. Banerjee, K. Basu and S. K. Das, "SIP-based Vertical Handoff between WWANs and WLANs," *IEEE Wireless Communications Magazine*, 12(3), pp. 66-72, 2005.

[5] C. Perkins, Ed, D. Johnson, and J. Arkko, "Mobility Support in IPv6," *RFC 6275*, 2011.

[6] Nursimloo, D. S. Chan, H. A. "Integrating fast mobile IPv6 and SIP in 4G network for real-time mobility," Jointly held with the *IEEE 7th Malaysia International Conference on Communication*, 13th *IEEE International Conference on Networks*, 2, pp. 16-18, 2005.

[7] Zubair, M., Mahfooz, S., Khan, A., ur Rehman, W., "Providing end to end QoS in NGNs using combined SIP HMIPv6 (CSH)," *IEEE International Conference on Computer Networks and Information Technology (ICCNIT'11)*, pp. 113 – 118, 2011.

[8] Faisal, S., "Performance Analysis of 4G networks," *Department of Electrical Engineering School of Engineering Bleking Institute of Technology SE-37 79 Karlskrona, Sweden*, 2010.

[9] Y. Sheffer, H. Tschofenig, "Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption," *RFC 5723, Internet Engineering Task Force (IETF)*, 2010.

[10] Liang Zhang, Miyajima, H., Hayashi, H., "An effective SIP security solution for heterogeneous mobile networks," *IEEE International Conference on Communications, (ICC '09)*, pp. 1 – 5, 2009.

[11] Chuang, M. -C. and J. -F. Lee, "A lightweight mutual authentication mechanism for network mobility in IEEE 802. 16e wireless networks," *Comput. Netw.*, 55(16), pp. 3796-3809, 2011.

[12] Atay, S. ; Masera, M., "Challenges for the security analysis of Next Generation Networks," *Information Security Technical Report*, 16, pp. 3-11, 2011.

[13] Xie, Q., "A new authenticated key agreement for session initiation protocol," *International Journal of Communication Systems*, 25(1), pp. 47-54, 2012.

[14] N. Modadugu and E. Rescorla, "The Design and Implementation of Datagram TLS," *In Proceedings of NDSS*, 2004.

[15] Thuy Ngoc Nguyen and Maode Ma., "Enhanced EAP-Based Pre-Authentication for Fast and Secure Inter-ASN Handovers in Mobile WiMAX Networks," *IEEE Transactions on Wireless Communications* 11(6), pp. 2173-2181, 2012.

[16] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence, "Generic AAA architecture," *RFC 2903*, 2000.

[17] S. Glass, T. Hiller, S. Jacobs, C. Perkins, "Mobile IP authentication, authorization, and accounting requirements," *RFC 2977*, 2000.

[18] C. Perkins, "Mobile IP joins forces with AAA," *IEEE Personal Communications*, 7(4), pp. 59–61, 2000.

[19] P. Calhoun, T. Johansson, C. Perkins, T. Hiller, "Diameter Mobile IPv4 application," in: P. McCann (Ed.), *RFC4004*, 2005.

[20] H. Fathi, S. Shin, K. Kobara, S. Chakraborty, H. Imai, R. Prasad, "LR-AKE-based AAA for network mobility (NEMO) over wireless links," *IEEE Journal on Selected Areas in Communications (JSAC)*, 24 (9), pp. 1725–1737, 2006.

[21] Donghai Shi, Chaojing Tang, "A fast handoff scheme based on local authentication in mobile network," *Sixth*

IEEE International Conference on ITS Telecommunications Proceedings (ITST), pp. 1025–1028, 2006.

- [22] Kang, H. -S. and C. -S. Park, "Authenticated Fast Handover Scheme in the Hierarchical Mobile IPv6," *Information Security Applications, Springer Berlin / Heidelberg*, pp. 211-224, 2007.
- [23] Ilsun You, Sakurai, K., Hori, Y., "Comments on Kang-Park's Security Scheme for Fast Handover in Hierarchical Mobile ipv6," *Fourth international conference on frontier of computer science and technology (Fcst '09)*, pp. 351 – 355, 2009.
- [24] Ganti, Srinivas, Ambudkar, Bhavna, "Fast Authentication during Handover in NGN," *International Conference on Communication Systems and Network Technologies (CSNT '12)*, pp. 362 – 365, 2012.
- [25] Jong-Hyoun, L., et al., "Comparative Handover Performance Analysis of IPv6 Mobility Management Protocols," *Industrial Electronics, IEEE Transactions on*, 60(3), pp. 1077-1088, 2013.
- [26] Jie Zhang, Henry C. B. Chan and Victor C. M. Leung, A, "SIP-Based Seamless-Handoff (S-SIP) Scheme for Heterogeneous Mobile Networks," *IEEE Wireless Communications and working Conference, (WCNC '07)*, pp. 3946 – 3950, 2007.
- [27] H. Soliman, C. Castelluccia, K. Elmalki, L. Bellier., "Hierarchical Mobile Ipv6 (HMIPv6) Mobility Management," *RFC 5380*, 2008.
- [28] Thierry Gayraud, Olivier Alphand, Pascal Berthou, Cedric Baudion and Laurence Duquerroy, "Mobility Architectures for DVB-S/RCS Satellite networks," *2th Ka band Broadband Communications Conference, Naples: Italie*, 2006.
- [29] Yen-Wen Lin and Ta-He Huang, "SIP-Based Handoff in 4G Mobile Network," *IEEE Wireless Communications and Networking Conference, (WCNC '07)*, pp. 1-15, 2007.
- [30] El-Mohsen, O. A.; Saleh, H. A. M.; Elramly, S., "SIP-Based Handoff Scheme in Next Generation Wireless Networks," *2012 6th International Conference on Services and Technologies (NGMAST)*, pp. 131-136, 2012.
- [31] Hasanul Ferdous, Sazzadur Rahman, Kamrul Islam, "Comparative Analysis of Mobility Support in Mobile IP and SIP," *World Academy of Science, Engineering and Technology* 9, 2005.
- [32] I. F. Akyildiz and W. Wang, "A dynamic location management scheme for next-generation multiuser PCS systems," *IEEE Transactions on Wireless Communications*, 1(1), pp. 178-189, 2002.
- [33] Li Jun Zhang, Samuel Pierre, "Evaluating the Performance of Fast Handover for Hierarchical mipv6 in Cellular Networks," *Journal of Networks*, 3(6), pp. 36-43, 2008.



Muhammad Zubair has done his Bachelor and Master Degree in Computer Science from University of Peshawar, Pakistan in 2005 and 2007 respectively. In Feb 2006, he joined Pakistan Air Force (Fazaia) Degree College, Peshawar as an instructor in computer science. He was promoted as a lecturer in 2007. In 2009, he was assigned with the responsibilities of Head of Computer Science Department in the college. He was also working as a visiting lecturer in Department of Computer Science, University of Peshawar, teaching to undergraduates and post graduates. He was awarded as a master trainer in Pakistan by Intel. Currently, he is a PhD student at Dalian University of Technology (DUT), Dalian, China. He is reviewer of Computer Communications, IEEE Symposium on Wireless Technology & Applications (ISWTA). He is also member of Doctor Association in School of Information and Communication Engineering, DUT. His research interest lies in wireless communication system; particularly focusing on topics related to all aspects of mobility, QoS and security in Next Generation Networks.



Dr. Xiangwei Kong is currently a professor and director of Research Center of Multimedia Information Processing and Security of Dalian University of Technology, China. During 2006–2007, she was a visiting scholar of Purdue University, USA. Prof. Kong is a member of signal processing society of IEEE. From 2004–2009, she is a vice director of multimedia information security branch of Chinese Institute of Electronics, China. Her research contributions encompass aspects of multimedia information security, digital watermarking, digital image forensics, image and signal processing, and wireless networks.



Dr. Saeed Mahfooz has done his Ph.D. from Liverpool John Moore University, Liverpool, UK in Distributed Multimedia Systems in 2001. He started his teaching career in 1990 which spans around 22 years. He is also heading the Computer Networks Research Group at Department of Computer Science, University of Peshawar. His research interest includes QoS Architectures, QoS Routing, Network Protocols, IPv6, Cloud Computing, Wireless Networks, MANETs, future Internet architecture and Next Generation Networks.