International Journal of Computer Science and Engineering Open Access
Survey Paper Volume-2, Issue-2 E-ISSN: 2347-2693

A Survey on Secure Handover Optimization in Mobile WiMAX Network

Bhanupriya M. Nikhar[1*], Kapil N. Hande[2]

[1*] PG Student, Computer Science and Engineering, RTMNU, India,bhanu.nikhar@gmail.com
[2] Computer Science and Engineering, RTMNU, India,kapilhande@gmail.com

www.ijcaonline.org

Received: 01 Feb 2014 Revised: 16 Feb 2014 Accepted: 22 Feb 2014 Published: 28 Feb 2014

***Abstract*—** GSM, UMTS, WIMAX, and WIFI are different wireless network types, which demands interoperability. Mobile WiMAX is the demanded technology for broadband wireless communication. The challenging aspect is to ensure service continuity for a mobile user when changing different access network. Due to the diversity of mobile networks and services offered by different operators, most users ask for better services without worrying about the technological constraints. Users must have the possibility to migrate from one area to another one without losing connection, knowing that these areas are using different technologies. Most of the Mobile users want quick and seamless service connection, and in mobile WiMAX network handover schemes, the authentication procedure takes long time to execute and thus producing delay in communication. This paper is the review of different handover mechanisms that has been proposed for reducing delay in communication between different users and providing fast and secure authentication schemes to meet the security requirement of users in the network. A pre-authentication based HO schemes for fast and secure HO, are shown to be vulnerable to Denial of Service attacks and Replay attacks. This paper discusses an EAP-based Authentication scheme, an EEP scheme and EAP-TTLS scheme which are proposed to optimize Handover Latency and to overcome above vulnerabilities with much less computational and communicational resources.

***Keywords/Index Term*—** EAP, IEEE 802.16e and Handover

I. INTRODUCTION

WiMAX stands for Worldwide Interoperability for Microwave Access, is a technology for fixed and mobile broadband wireless access systems, intended for allowing high speed internet access for long distances. IEEE 802.16 networks are dedicated to cover a large area. It provides centralized broadband wireless access. It allows transmission though certain obstacles. The main advantage of IEEE 802.16e is its high data rates, built-in support and low cost of deployment for mobility.

WiMAX (Worldwide Interoperability for Microwave Access) has been established as one of the important milestone for broadband wireless communication. When a mobile user moves from one ASN (Access Service Network) to other, MWiMAX system supports handover processes to make a mobile station (MS) find another base station (BS) for establishing a connection when moving out of coverage of current serving BS. The HO occurs when the Mobile station (MS) moves form one base station (BS) to other base station to obtain a higher signal quality and better quality of service. The HO procedure follow the steps like re-authentication, encryption key exchange and network registration need to be implemented, all these steps add delay to the handover process. Therefore, it is very necessary to minimize the handover latency while keeping the whole procedure secure. Handovers are broadly classified into two categories depending on technology: horizontal handovers and vertical handover. Horizontal handovers are homogeneous intra-network inter-cellular, while the vertical ones are heterogeneous inter-network inter-cellular. For example, handovers between multiple WiMAX networks are horizontal handovers and that one in WiMAX and 3G or WLAN are vertical handovers. The WiMAX system defines three types of handover procedures. These are Hard Handover (HHO) is the default handover and two are soft handovers as Macro-Diversity Handover (MDHO) and Fast Base Station Switching (FBSS) Handover, which are the optional procedures.

Hard Handover (HHO):

In this type of handover Mobile Station only communicates with only on Base Station at any time. Hard handover follows the break-before-make strategy as Mobile Station (MS) has to disconnect from serving Base Station (BS) before connecting to target Base Station (BS). The serving Base Station periodically broadcasts neighbour advertisement message MOB_NBR-ADV. The Mobile Station received information through this message about characteristic of neighbouring Base Stations such that number of neighbour Base Stations and their BSIDs. After

Corresponding Author: *Bhanupriya M. Nikhar*

© 2014, IJCSE All Rights Reserved

this the Mobile Station can select appropriate target Base Station for handover. It also performs ranging; association procedures, authentication and registers with target Base Station.

Macro Diversity Handover (MDHO):
This is an optional scheme so it must be supported by both Mobile Station and Base Station. In this scheme mobile Station and Base Station keeps a list of Base stations which are capable to the MDHO on MS's coverage area. This group of Base Stations is called diversity set or active set. One Base Station among these is defined as anchor Base Station. The Mobile Station can communicate with any Base Station in diversity set for UL and DL traffic. The Base Stations involved in MDHO must share or transfer MAC context including current encryption and authentication keys.

Fast base Station Switching (FBSS):
This scheme is similar to MDHO. Both Mobile Station and Base Station have to support FBSS. The Mobile station and Base Station manage the diversity set but Mobile Station can only communicate with one Base Station i.e. anchor Base Station for all type of traffic. The switching from one anchor BS to other anchor BS is performed without invoking normal HO procedure. As in MDHO, it is required that BSs involved in FBSS share or transfer MAC context.

II. Related Works

Researchers have been working on Handover of IEEE 802.16e broadband wireless network for years and several fast handover schemes had been proposed. To reduce the EAP-based authentication delay during HOs without compromising security requirements, in [1] researchers have followed two approaches, namely the re-authentication and the pre-authentication approaches. Re-authentication approaches intent to reduce the authentication delay by reusing the information exchanged between the MS and the AS in the previous authentication. In [11], the authors proposed a secure pre-authentication that follows the least privilege principle to solve the domino effect and handover protocol guarantees the backward and forward secrecy. But this pre-authentication scheme is not efficient and secure. In [13], an Enhanced EAP based TTLS (Tunnel Transport Layer Security) is proposed to overcome DoS and Replay attacks that occur in an EAP scheme.

In [16], a new fast handover algorithm was proposed which reduces the waste of the wireless channel resources and handover delay. This scheme tries to reduce unnecessary neighbour Base Station scanning & association process. The proposed scheme performs Target Base Station estimation using mean CINR and arrival time differences. In [17], the authors proposed two efficient schemes to enhance the performance of authentication during handover in Mobile WiMAX. The proposed schemes help to avoid the device re-authentication. In the first scheme, whenever Mobile Station first enters the network it is authenticated by AAA through EAP authentication. After that whenever Mobile Station needs to be authenticated by AAA server then instead of standard EAP method used in handover authentication, an efficient shared key-based EAP method is used. In the second scheme, the standard EAP method is skipped and the device authentication is done by SA-TEK three way handshake in PKMv2 process. This scheme is not suitable for implementation because it avoids the standard procedures.

III. Solution/Need/Importance of the Study Problem Statement/Objectives

HHO related issues in WiMAX:
Though the HHO is the mandatory scheme in MWiMAX and the most bandwidth-efficient handover technique in MWiMAX, yet such handover activities are surrounded by serious problems like excessive scanning activity in a somewhat non-optimized scanning interval before finalizing a TBS and prolonged inter-handover connection gaps. There are also several other important issues, such as unwanted network re-entry activities during the handover owing to ping-pong effects, IP connectivity delay during the network re-entry phase, and optimization of handover-based load distribution, needed to be investigated.

Excessive Scanning and Association Activities: The MS can scan some of the NBSs as potential TBS candidates. This may result in unnecessary wastage of channel resources and degrading the overall performance due to redundant scanning of NBSs. Moreover, along with scanning, synchronization, ranging and association activities are also performed one after another during the Network Topology Acquisition Phase (NTAP). Hence, the redundant scanning activity which is followed by synchronization, ranging and association activities proportional to the number of NBSs scanned increases the overall handover delay. A number of measures have been proposed to simplify scanning related procedures during the topology acquisition phase, to minimize the overall delay and enhance the system performance.

Optimizing Scanning Intervals: In the MWiMAX, HHO scenario, scanning of multiple channels is a necessary activity for discovering the NBS. Hence, though it is difficult to avoid scanning process completely, one can try to keep it within limits. During scanning, MWiMAX handover mechanisms temporarily pauses the uplink and downlink of data transfer between the MS and the SBS. These scanning intervals are allocated by the SBS on getting scanning interval allocation requests from the MS. The frequent temporary suspension of data exchange lowers the system throughput, and adds more delays to the overall handover process. Also, QoS requirement may get disrupted. An efficient Adaptive Channel Scanning

© 2014, IJCSE All Rights Reserved

algorithm in a multi-MS oriented MWiMAX environment, relying on the exchange of configuration parameters between the NBSs in order to find out the required scanning time for a MS. Along with optimisation of the allocated scanning intervals for all MSs, the scheme also maintains the QoS of the application traffic in the system. However, utilization of unlimited channel buffers, in order to make the packet loss almost negligible, complicates the problem of channel resource wastage.

Wastage of Ranging Slots: Handovers initiated by either the MS, or the SBS, or even the underlying network is supported by MWiMAX. In case of MS-initiated handovers, when the suitability of the potential candidate NBSs selected by the MS during the NTAP is accepted, the individual BSs allocate ranging slots for the MS, which then selects the new TBS and retains only the ranging slots provided by that BS. The other unused ranging slots add up to the list of resources being wasted during the entire handover process. Such wastage of unwanted resources can be avoided if the SBS can select the new TBS before the allocation of ranging slots. Only that TBS may allocate ranging slots that has been selected, debarring the other NBSs from unnecessarily allocating such slots.

Prolonged Handover Connection Disruption Time (CDT): HHO is a 'break before make' technique, the HHO concept in MWiMAX suffers from a lengthy "inter-handover" CDT that could lead to unwanted hazards like packet losses, call disruptions or even call drops. This occurs in the actual handover phase, when an MS terminates the connection with the SBS and tries to set-up connections with the selected TBS. In MWiMAX, data, voice and multimedia contents are intermixed and each requires different mechanisms for its transmission, particularly during handover. So, such a lengthy CDT may cause serious service disruptions in case of real-time high-speed delay-sensitive voice and streaming multimedia applications in MWiMAX networks. The IEEE MWiMAX group has incorporated the MDHO and FBSS techniques, which are ideal for delay sensitive applications like VoIP.

Network Re-entry Activity due to Ping-Pong Effect: In MWiMAX HHO, when an MS wants to get connected to a new BS, it has to complete the entire network re-entry procedure comprising of the series of security and connection re-establishment processes which is a lengthy process. In a situation where in the middle of an ongoing communication, an MS, that is performing network re-entry procedures with a TBS, wants to come back to the previous SBS due to change in signal strengths, it leads to further delays if the entire re-entry procedure needed to be performed again for the old SBS. Handover overheads caused by unnecessary re-entry procedures resulting from such ping-pong effects may degrade the overall system performance.

MDHO And FBSS Related Issues:
Similar to the HHO, these soft handover techniques also suffer from few drawbacks. Both MDHO and FBSS suffer from performance hindrance challenges, specifically with the accuracy of updates of the active sets during the actual handover phase. Not much work has been done for dealing with these important issues.

Ping-Pong Effects While Updating the AS: In MDHO and FBSS, depending on the signal strengths of the BSs, an MS always maintains an AS of NBSs, comprising of the NBSs with the most powerful signal strength at that particular instance of time. The AS also contains the serving or anchor BS (ABS). The other NBSs remain in the set of probable candidate BSs (candidate set) for the active set. The MS always monitors these BSs to update the AS, depending on a threshold value. The difference between the new threshold value and the existing value should be large enough to trigger the requirements for AS updating as there are always possibilities that due to a very low threshold value difference, NBSs from the candidate set may move in and out of the AS unnecessarily. Such enhanced ping-pong activities would not only make the AS updates meaningless, but also hike the resource consumption in regard to the required signalling, degrading the overall performance. So, efficient methods of determining the right threshold values to update the AS are required to reduce such performance-hampering activities.

Inaccurate AS Updating based on the BSs' Signal Strengths: The FBSS and MDHO rely on the 'signal strength' of the NBSs as the sole basis for updating the AS. They take into account neither the path followed by the MS, nor the mobility of the MS. Relying only on signal strengths does not always result in optimum performance, especially in regard to channel and resource wastages. Though the signal strengths of such NBSs may be strong enough to be included in the AS, they might not fall into MS's movement trajectory. Automatically such BSs would pop out of the AS after some time, when the MS moves further away from them, resulting in frequent and unnecessary updating of the AS. Thus, in terms of channel usage, inclusion of such NBSs is a complete waste.

Inaccurate AS Updating based on Absolute Threshold Values: In the MDHO and the FBSS, the MS updates the AS based on the absolute H ADD and H DELETE threshold values contained in the DCDs broadcasted by the BSs. At any instant, all the NBSs in the AS having CINR value less than H DELETE threshold are removed from set and those, from the candidate set (CS), with CINR values more than H ADD threshold are added to the AS. However, in reality, with the load of a cell changing at every moment, relative threshold values instead of an absolute one seem to be more realistic for accurate updating of the AS.

© 2014, IJCSE All Rights Reserved

IV. HYPOTHESIS

Research hypotheses are the specific testable predictions made about the independent and dependent variables in the study. Usually the literature review has given background material that justifies the particular hypotheses that are to be tested. Hypotheses are couched in terms of the particular independent and dependent variables that are going to be used in the study.

V. METHODOLOGY

A pre-authentication-based handover scheme for mobile WiMAX networks aims to achieve fast and secure inter-ASN handovers. However, it is shown to be vulnerable to Denial of Service (DoS) and replay attacks. In order to maintain high level security for the mobile users, the mobile station MS and the target BS (tBS) or target access service network gateway (tASN) have to authenticate each other the MS is granted access to the mobile WiMAX network using the Extensible Authentication Protocol (EAP). EAP-based Authentication uses a backend authentication server (AS) which allows an authentication method to be selected. The flexibility makes the EAP-based authentication to be popular choice for the authentication for HOs in mobile WiMAX systems. To reduce the EAP-based authentication delay during HOs without compromising security requirements, two approaches have been followed as re-authentication and pre-authentication approaches. Re-authentication approaches intent to reduce the authentication delay by reusing the information exchanged between the MS and the AS in the previous 'authentication'. In EAP-Based re-authentication protocol (ERP) a MS and AS uses the extended master session key (EMSK) derived from previous EAP authentication for the master session key (MSK) derivation. A fast and secure EAP-Based pre-authentication scheme is proposed to face the challenges in the design of efficient and robust authentication protocols for HOs, symmetric key cryptography is used to secure the pre-authentication message exchange with low demand of computational resources.

EAP-based authentication uses a backend authentication server (AS) such as an authentication, authorization, and accounting (AAA) server, which allows users to choose an authentication method. In order to reduce the handover latency, mobile WiMAX supports handover optimization, allowing users to reduce handover latency by reusing key materials from previous authentication.

Re-Authentication Approach

Re-authentication can avoid a full EAP-based authentication in handover by reusing the information exchanged between the MS and the AS in the previous authentication. The HOKEY working group has proposed the EAP re-authentication protocol (ERP) which allows a MS and the AS to use the extended master session key (EMSK) from previous EAP authentication for master session key (MSK) derivation. Thus, instead of carrying out a full EAP authentication, the MS and the AS will only need a single round trip to exchange the ERP messages.

Pre-Authentication Approach

By pre-authentication techniques, a MS and the AS pre-compute the shared secret keys before a handover. Thus, the handover delay could be effectively reduced to the same amount of the time used by a 3-way handshake, resulting in the shortest authentication signalling delay. The main advantage of the pre-authentication is that the cryptographic material will not be reused, hence it becomes more secure.

Handover Procedure

In fig. 1 describes the basic HO operations. The HO is always started from the hBS to a tBS with a decision for an MS to handover. It can be triggered by a request from the MS or the hBS through MOB_MSHO_REQ or MOB_BSHO_REQ messages respectively. If MS intends to HO then the hBS will have to send the HO notification messages to the possible tBSs over the backbone network. If the hBS receives the HO notification responses from the tBSs, it selects a suitable tBS for the MS's HO to occur according to the response message whether to accept or to reject, and sends an HO confirmation message to the tBS that has been selected for HO. Thereafter, the MS is informed by the hBS about the selected tBS by sending the MOB_BSHO-RSP message in the case of MS-initiated HO or the MOB_BSHO-REQ in the case of BS-initiated HO. Upon receiving this message, the MS makes its final HO decision and has to send an MOB_HO-IND message to start the HO. After that, the hBS sets a timer to disconnect the MS. The MS will start the synchronization and ranging process with the tBS and proceed with the network re-entry procedure, which includes basic capability negotiation, authentication and registration. At the end of a successful HO, the MS can start receiving service from the new hBS.

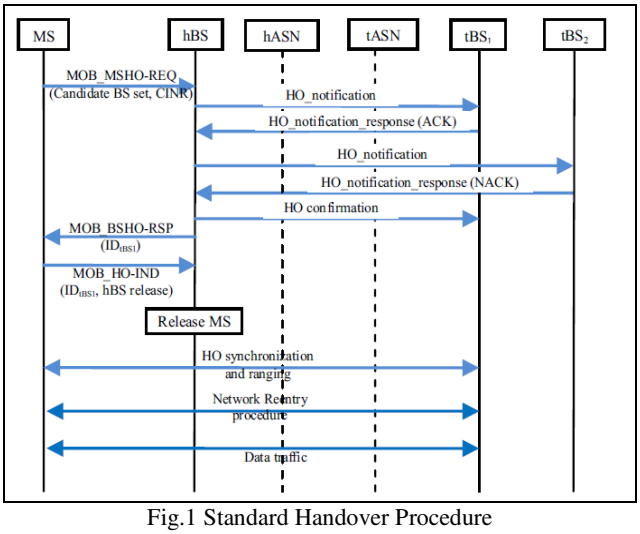

Fig.1 Standard Handover Procedure

© 2014, IJCSE All Rights Reserved

The Pre-Authentication Scheme

The Procedure for the pre-authentication scheme is as follows.

Step 0: A MS when joins a sector of a WiMAX network, it performs a full EAP authentication with the AS. As a result, a MSK is distributed to the hASN. The MS and the AS also share a secret EMSK, and this secret key will not be revealed to any other entity. A pre-authentication integrity key (PIK) and a pre-authentication encryption key (PEK) are derived from the MSK and EMSK respectively using the Dot16KDF function,

PEK = Dot16KDF (EMSK, "PEK", 128)

PIK = Dot16KDF (MSK, "PIK", 160)

The PEK is only known by the MS and the AS and is used to encrypt secret keying materials. The PIK is known by the MS, the hASN and the AS. It is used to calculate the Hash based Message Authentication Code (HMAC) to protect the integrity of the pre-authentication messages.

Step 1: a pre-master secret (PMS) and a nonce NMS is generated randomly when the MS initiates a pre-authentication session. The PMS is encrypted using the PEK. The MS constructs the PREAUTH_REQ message and is consisting of a unique 16-bit sequence number (SN) concatenated with the encrypted PMS, the NMS, the IDMS and the HMAC calculated from the PIK. The SN is incremented whenever the MS initiates a new preauthentication session to prevent replay attacks. The MS, the hASN and the AS all maintain a record of the SN in the last PREAUTH_REQ message received from the MS. The MS sends the PREAUTH_REQ message to the hASN. The hASN will first check whether the message is fresh message or is a replayed message by checking whether the received SN is greater than the last SN received from the MS. Next, it verifies the origin authentication and the integrity of the message by calculating the HMAC using the PIK and compares it with the HMAC in the message. After that, it relays the message to the AS.

Step 2: Upon receiving the PREAUTH_REQ message, the AS checks the freshness, the origin authentication and the integrity of the message following the same steps as the hASN did. If the message is genuine, the AS decrypts the cipher text using the PEK to obtain the PMS. It will then generate a nonce NAS, concatenate it with the SN, the cipher text obtained from encrypting (PMS+1) using the PEK and the IDMS, attach the corresponding HMAC and send it back to the hASN as the PREAUTH_RSP message. Similar to the step 1, the hASN will verify the message and relay it to the MS. The MS can verify the correctness of the received message and keep a record of the NAS. By decrypting the cipher text using the PEK, it can confirm whether the AS has obtained the correct PMS.

Step 3: A HO begins with a decision for the MS to handover from the hBS to a tBS. Following the standard HO procedure, after receiving the HO notification response messages from the potential tBSs, the hBS chooses one tBS and sends a HO confirmation to that tBS over the backbone.

The message will go through the tASN. As it is informed that it is selected for the HO, the tASN will send a message of KEY_REQ over the RADIUS to the AS containing the IDMS and IDtASN to the AS. The AS will derive the MSK in a way similar to that of the EAP-TLS key derivation in :

Master_secret = TLS-PRF-48(PMS, "master secret", NMS‖NAS‖IDtASN)

Key_Material=TLS-PRF-128 (Master_secret, "client EAP encryption", NMS‖NAS‖IDtASN)

MSK = Key_Material(0,63)

After all these steps the MS and the tASN can share the same MSK, compute the AK and continue with the SA-TEK 3-way handshake as specified by the IEEE 802.16e standard.

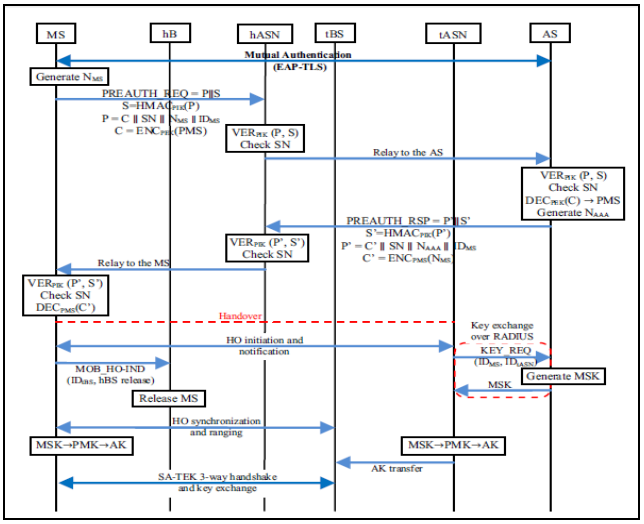

Fig. 2 the Pre-Authentication scheme

EAP-TLS Based Authentication Scheme:

The procedure of the EAP Transport Layer Security (EAP-TLS) based authentication as shown in Fig. 3. This is one of the EAP-based authentication approaches that can provide strong mutual authentication. It has been selected as one of

© 2014, IJCSE All Rights Reserved

the options of the authentication scheme between the MS and the AS by the WiMAX forum. The first step in the procedure is that, the MS issues a link-up requesting message to the BS. The EAP message to the authenticator in the ASN is then relayed by the BS. From there, the EAP message is carried to the AS over the RADIUS. After the authentication process, the MSK that is generated by the AS and MS, will be transferred to the authenticator in the ASN. The MSK is used for both the authenticator and the MS to generate PMK and authorization key (AK). The AK which is used for the SA-TEK 3-way handshake and key exchange is transferred to the hBS. At the end of the authentication, the traffic encryption key is shared between both the MS and the BS for the data encryption. The proposed scheme is designed based on the EAP-TLS authentication.

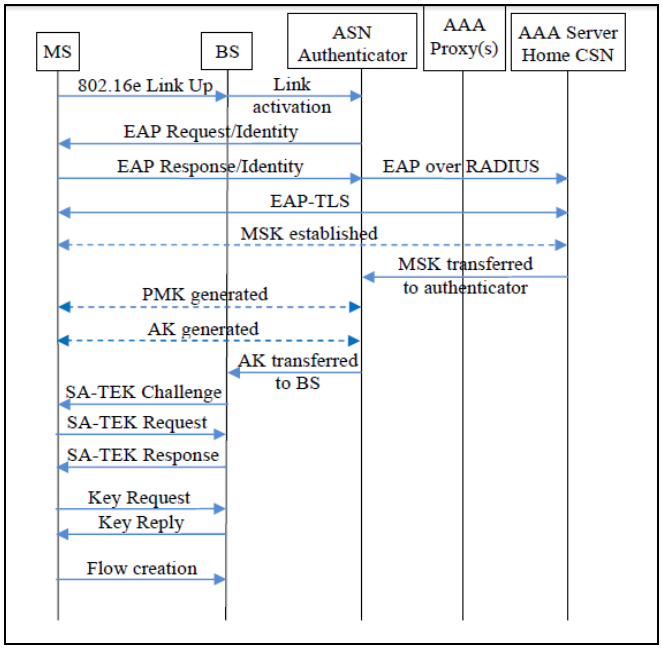

Fig. 3 EAP-TLS Based Authentication

The procedure of EAP-TLS-based authentication is shown in Fig.3. The EAP authentication is executed between a MS and the BS in the Privacy Key Management version 2 (PKMv2) security protocol specified by the IEEE 802.16e standard. Firstly, the MS issues a link-up request message to the BS. The BS then relays an EAP message to the authenticator in the ASN. From there, the EAP message is carried to the AS over RADIUS. After the authentication process, the MS and the AS generate a MSK, which will be transferred to the authenticator in the ASN. The MSK is used for both the authenticator and the MS to generate a pair-wise master key (PMK) and an AK. The AK is transferred to the hBS, which is used for the SA-TEK 3-way handshake and key exchange. At the end of the authentication, both the MS and the BS share the TEK for the data encryption.

VI. Result & Discussion

By the pre-authentication scheme, the EAP authentication in the HO procedure has been migrated to the pre-authentication phase. During a HO, there is a MSK exchange between the tASN and the AS which is performed in parallel of the period when the MS is working on a HO synchronization and ranging with the tBS. The recommended setting for a ranging duration in a HO is around 20ms and it is longer than the time required for the MSK key exchange process, which requires less than 10ms. The transmission time of MSK key exchange messages is relatively short because, the average round trip propagation delay between the tASN and the AS is 4ms. Thus, the additional key exchange will not introduce any extra delay to the HO latency. As the result, the delay of network re-entry process during the HO is significantly reduced to the duration of the SA-TEK 3-way handshake and the registration.

Another enhancement compared to the EAP-TLS authentication is that the scheme has made use of symmetric key cryptography to protect the pre-authentication message exchange, which requires much less time and computational resource compared to the heavy public key operations such as certificates verifications, signature signing and verifications involved in the EAP-TLS authentication process. This scheme has allowed the MS to exchange keying materials with the AS and allow the AS to distribute the MSK to the tASN upon the confirmation of a HO, thus, it overcomes the main drawback of the pre- authentication approach, which is that the MS wastes unnecessary power for the key exchange with other ASNs that they may never roam to.

VII. Conclusion

A Pre-authentication scheme has been proposed to reduce the authentication delay in the HO process for the mobile WiMAX networks. Symmetric keys have been used for the encryption of the secret key, the origin authentication and the integrity protection of the pre-authentication messages. Secure data transfer is important in Mobile WiMAX network therefore some improvements are needed in handover procedure to make secure and efficient data transfer.

The scheme that can reduce the HO delay with much less computational resource by allowing the MS and the AS to exchange the secret key used for the HO authentication session before the HO happens is needed to be implemented. So it should result in, the MS does not need to perform EAP authentication with the AS and can proceed with the SA-TEK 3-way handshake straight away.

© 2014, IJCSE All Rights Reserved

VIII. SCOPE FOR FURTHER RESEARCH

Thus, the Pre-authentication scheme that will remove the above vulnerabilities of the mentioned pre-authentication scheme should be proposed and should provide fast and secure authentication for user moving from one station to other and should reduce the communication delay in between two. The resulting scheme can be compared with the existing one to let to know which method is secured and lead to a smaller delay. NS2 would be used to implement the proposed protocol and simulate a WiMAX Network. NS2 simulation would be used to measure the effectiveness of the proposed solution.

ACKNOWLEDGMENT

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression, "One of us (R. B. G.) thanks . . ." Instead, try "R. B. G. thanks". Put applicable sponsor acknowledgments here; DO NOT place them on the first page of your paper or as a footnote.

REFERENCES

[1]. T. N. Nguyen and M. Ma, "An Pre-authentication Protocol With Symmetric Key For Secure Handover in Mobile WiMAX Network". IEEE ICC-communication and information system security Symposium-**2012**.

[2]. A. Fu, S. Lan, B. Huang, Z. Zhu and Y. Zhang, "A Novel Group-Based Handover Authentication Scheme With Privacy Preservation for Mobile WiMAX Networks". IEEE Communication letter, vol. **16**, no. **11**, November **2012**.

[3]. M. Shurman, M. F. Al-Mistarihi and S. Naseer, "Hard Handover Optimization in Mobile WiMAX Networks", presented at the 5th International Conference on Communications, Computers and Application, Istanbul, Turkey, Oct. **2012**.

[4]. Caiyong Hao, Hongali Liu, Jie Zhan, "A velocity-Adaptive handover scheme for mobile WiMAX", International Journal of Communication, Network and System Sciences, vol. **2**, no. **9**.

[5]. E. Ahmed, B. Askwith and M. Merabti, "Handover Optimization for Real-Time Application in Mobile WiMAX/IEEE 802.16e" UK. ISBN: 978-**1-902560-24-3, 2010** pp. **2-3**.

[6]. A. Pontes, D. Silva, J. Jailton., K. Dias, "Handover Management in Integrated WLAN And Mobile WiMAX Networks" IEEE Wireless Communications, October **2008**, pp. **88-90**.

[7]. T. Nguyen and M. Ma, "Enhanced EAP-Based Pre-Authentication for Fast and Secure Inter-ASN Handovers in Mobile WiMAX Networks", IEEE Transactions on Wireless Communications, Vol. **11**, No**. 6**, pp. **2173-2175**, June **2012**.

[8]. A. Taha, A. Hamid and S. Tahar, "Formal Analysis of the Handover Schemes in Mobile WiMAX Networks" **2009** © IEEE.**978-1-4244-3474**, pp. **2-4**.

[9]. Y. Benkaouz, B. Angoma and M. Erradi, "Performance Analysis of WiFi/WiMAX Vertical Handover based on Media Independent Handover" in Networking and Distributed Systems Research Group, **2012** © IEEE. **978-1-4673-1520**.

[10]. T. Issariyakul and E. Hossain, Introduction to Network Simulator NS2. New York: Springer, **2008**.

[11]. J.Hur, H.Shim, P.Kim, H.Yoon and N-O.Song, "Security Considerations for Handover Schemes in Mobile WiMAX Networks," Proc. of Int'l Conf. on Wireless Comm. And Networking, **2008**.

[12]. S. More and D. K. Mishra, "4G Revolution: WiMAX Technology" in Department of Computer Science and Engineering, **2012** © IEEE. **978-1-473-2590**.

[13]. Subhashini S., "Active EAP Protocol for Secure Inter ASN Handover in Mobile WiMAX Networks", IJREAT International Journal of Research in Engineering & Advanced Technology, vol. **1**, no. **2**, April-May, **2013.**

[14]. G. Zorn (2010, 09 December **2010**). RADIUS Attributes for IEEE 802.16 Privacy Key Management Version 1(PKMv1) Protocol Support.[RFC 5904]. Available: http://www.rfc-editor.org/rfc/rfc5904.txt

[15]. Y. Ye, Q. Yi, and H. Sharif, "Performance analysis if IEEE 802.16e handover with RSA-based authentication", in ICC 2010-2010 IEEE International Conference on Communications, **23-27** May **2010**, Piscataway, NJ, USA, 2010, p.**5** pp.

[16]. Lee D.H., Kyamekya K., Umondi J.P., "Fast Handover Algorithm for IEEE 802.16e Broadband Wireless Access System", ISWPC **2006**.

[17]. H-M.Sun, S-Y.Chang, Y-H.Lin and S-Y.Chiou, "Efficient Authentication Schemes for Handover in Mobile WiMAX," Proc. of 8th Int'l Conf. on Syst. Design and Applications, **2008**.

© 2014, IJCSE All Rights Reserved