Increasing the Performance of Vertical Handover Delay for Heterogeneous Wireless Network using BAN Logic & EAP

Kundan P. Dongare[1], Prof. Uma K. Thakur[2] & Dr. Leena H. Patil[3]
[1]M.tech Student, Department of Computer Science & Engineering, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, India.
[2 & 3]Assistant Professor, Department of Computer Science & Engineering, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, India.

Abstract:-*In this era, the rapid development of portable devices and next generation wireless network, user want to connect different wireless technologies like GSM, WiMax, WLAN etc. and excepted to provide QoS services to the network ay anytime anyplace in heterogeneous network. One of the major issue is to support multiple wireless network is compatible with vertical handover. In such heterogeneous network environments, improved vertical handover delay play important role in data transitions in seamless mobility. The most important issue for this type of environments is to ABC (Always Best Connected). In this paper, I present a comprehensive survey of the VERTICAL HANDOVER algorithms to choose best network to fulfil the necessity of these requirement.*

Keywords—*Heterogeneous wireless Network, Next Generation Wireless Network, Vertical Handoff, Horizontal handover*

I. INTRODUCTION

Next-generation wireless networks have been envisioned as all- Internet protocol (IP) based infrastructure with the integration of various wireless access networks such as IEEE 802.11 based WLANs, IEEE 802.16 based wireless metropolitan area networks (WMANs), general packet radio service (GPRS), and universal mobile telecommunications system (UMTS) and each of its own characteristics need to integrates to fulfill the requirement of multimedia services. A key reason behind the mushrooming of heterogeneous wireless access technologies is the performance tradeoffs they exhibit in terms of mobility support, network capacity, coverage area, and transmission power. Hence, a mobile user today can potentially be equipped with multiple wireless interfaces that have access to different wireless networks with high data rate and low cost.

In heterogeneous wireless Network, the main challenging issue is to different wireless technologies is to support vertical handover. In vertical handover the device can switch one network to another in different radio access technologies. Handover is the process of managing active user session when they change their base station terminal to another base station terminal without any disturbing. In heterogeneous wireless Networks are split into two types as horizontal handover (HHO) and vertical handover (VHO). In horizontal handover the device can switching the different access point to another within a same wireless technologies. Hence the horizontal handover is not difficult task to communicate devices within same radio access. In vertical handover, mobile terminal can transferring the connection from different access point to another different wireless technologies access point. There is the challenging issue to connect different network in vertical handover.

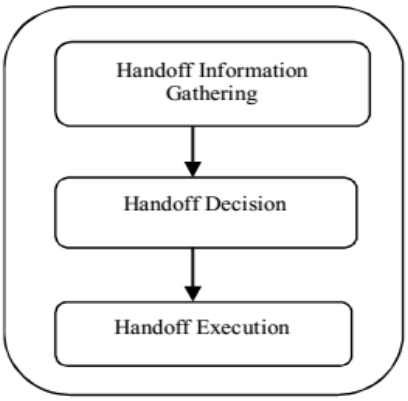

Fig 1: Handoff management process

The handover process has three phases:

• Handover Initiation Phase: It is also called as handover information gathering or system discovery. It is used to gather all the required information to identify the need for the handover and then initiate it.
• Handover Decision: It is also called as network or system selection. It is used to determine whether to do handover and how to perform it by selecting the most suitable network according to the handover selection criteria and also by giving the subsequent instructions to the next phase that is handover execution phase.
• Handover Execution: It is used to select the network according to the handover decision phase. [17]

Vertical Handover algorithms help mobile terminals to choose the best network to connect to among all the available candidates. Here, we only focus on the research efforts and re- cent developments on improving the efficiency of Vertical handover decision process. Vertical

handover decision algorithms, criteria such as cost of services, power consumption and velocity of the mobile terminal may need to be taken into consideration to maximize user satisfaction.

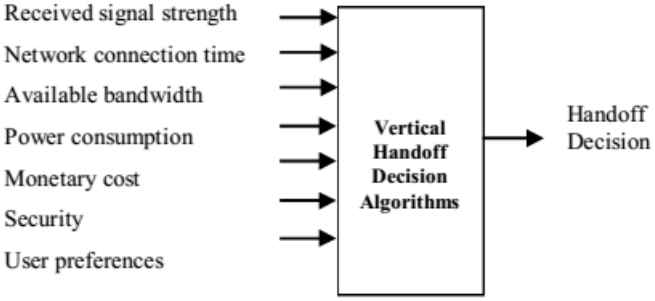

Fig 2: Parameters used for making Vertical Handover decisions

• Received signal strength: handover decision is a handover initiation phase in homogeneous environment.

RSS is the traditional handover decision criteria in almost all existing horizontal handover algorithms. RSS is also an important decision criteria in the VHD algorithms. Received signal strength (RSS) is the most widely used criterion because it is easy to measure and is directly related to the service quality. There is a close relationship between the RSS readings and the distance from the mobile terminal to its point of attachment. Majority of existing horizontal handover algorithms use RSS as the main decision criterion, and RSS is an important criterion for VHD algorithms as well.

Network connection time: It is referred to as the duration that a mobile terminal remains connected to a point of attachment. Determination of the network connection time is very essential for selecting the right moment to initiate a handover so that the satisfactory level of service quality could be maintained.

• Available bandwidth: It is a measurement of available or consumed data communication resources expressed in bits per second. It is a good indicator of traffic conditions in the access network and is especially important for delay-sensitive applications.

• Power consumption: If a MT's battery is low it becomes a critical issue, in such case it would be preferable to handover to a PoA which would help extending valuable battery life.

• Monetary cost: For different networks, there would be different charging policies, therefore, in some situations the cost of a network service should be taken into consideration in making handover decisions.

• Security: For some applications, confidentiality or integrity of the transmitted data can be critical. For this reason, a network with higher security level may be chosen over another one which would provide lower level of data security.

• User preferences: A user's personal preference towards an access network could lead to the selection of one type of network over the other candidates.

II. LITERATURE SURVEY

(1) "Feasibility of SDN-based Vertical Handover between Bluetooth and Wi-Fi" by Eiji Kamioka , Toan Nguyen-Duc [6]

In This Survey, the author suggest the low rang wireless Technology instead of high speed connectivity, people need longer battery life to survive in case of natural disasters such as fire, earthquake or tsunami. There are several ways to conserve battery power, such as dimming the brightness of the display screen and disabling certain applications. Besides, using only one wireless technology such as Wi-Fi, 4G LTE or Bluetooth for communication also helps to reduce the power consumption. This is because each wireless technology commonly constantly seeks for a good connection, thus, it continuously consumes the power of the battery.

Among the technologies, Bluetooth is a potential one because it provides directly and wirelessly connection among mobile devices at a low cost and with little energy consumption. The technology typically transmits data via low-power radio waves between 2.402 GHz and 2.480 GHz. The weak signals, i.e., 1mW, help to avoid interfering with other systems; however, it limits the communication range of a Bluetooth device to about 10 meters. The communication range can be extended if there are more mobile devices joining the network. When the number of the devices is small, they must use another technology, i.e., Wi-Fi, for a longer distance communication.

The author executed a handover procedure at Data Link layer, aiming to make use of all wireless interfaces at the same time. The approach is useful to gain a higher throughput; however, it does not focus on saving the power as the system turns on both wireless interfaces at the same time. For handover between Bluetooth and Wi-Fi, in, the authors proposed virtual interface architecture as a solution to the vertical handover problem. With the similar approach, in, the author tried to evaluate the performance of the vertical handover by simulating the procedure.

Even though there are several studies that consider the vertical handover between Bluetooth and Wi-Fi, the behaviour of the vertical handover when two nodes are communicating directly via Bluetooth connection has not been well described. Specifically, when the Bluetooth connection is going to be lost, if only one node switches the connection

to Wi-Fi, the connection between them will be terminated.

Drawback: The Wi-Fi technology consumes more power than Bluetooth and commonly requires a network infrastructure such as an access point (AP) to provide wireless connection for mobile devices. When there is no network infrastructure, Wi-Fi network still works in an adhoc manner, however, the network only allows point-to point communication.

(2) "Knapsack - TOPSIS Technique for Vertical Handover in Heterogeneous Wireless Network" by E. M. Malathy, Vijayalakshmi Muthuswamy[10]

The literature reveals that parameters such as signal strength, bandwidth, and power consumption influence the network characteristics that have direct impact on the design of the handover decision algorithm. Therefore, selection of parameters for the decision phase is critical for the performance evaluation of the algorithm.
The literature survey that there is no evidence in the past which employed dynamic programming with the Knapsack problem approach to handle various QoS traffic classes for vertical handover problem. The proposed handoff decision strategy is designed for network-controlled handoff, which erratically removes the limitation of mobile-controlled handoff. This situation motivates the division of the network into zones, and computation of the ranking score by TOPSIS method offers a deviation of the decision variable towards the ideal solution.

The proposed schemes adds repository to keep all set of policies governing the decision rules and network makes smart choice to choose the candidate network through MADM method such as TOPSIS. Moreover, TOPSIS alone is unreliable for performing handover in a heterogeneous environment. To adopt traffic load balance in determination of optimal VHO triggers, dynamic programming steers the correct mobile user with optimal handover through mobile IP functionality.

This paper adds QoS-aware decisions to improve efficiency by reducing unnecessary handover and removing centralized estimation of the network via estimation of the decision using a dynamic approach in the handover scheme. To achieve an optimal solution, recursive dynamic programming construction is derived, which uses stage-wise analysis of the mobile nodes connected to the point of attachment/base stations.

Drawback: The TOPSIS Method Spilt the network services into zone wise service and gives the QoS. According to that there are more working load is applied to zonal Network server hence the quality of services may degrade and handover may be delay.

(3) "Vertical handoff based on QOS Parameters in Heterogeneous Network" by Richa, Shelej Khera [17]

Handoff scheme for management the data loss in mobile communication has been proposed. The author has performed number of studies dealt with handoff management in mobile communication systems and some of these studies presented handoff schemes to manage this important process in cellular network. The existing schemes use relative signal strength (RSS) measurements.

In author's Work, a new proposed handoff scheme had been presented depending not only on the RSS measurements but also used the threshold distance and neighbouring BSS power margins in order to improve the handoff management process.

The author explained the handoff mechanism in terms of cost effectiveness and handoff should be feasible means it should be implemented on proper time during call in mobile communication. They explained that Heterogeneous networks with different Wireless technologies increase the availability of Internet services (i.e., cloud services). They presented a feasible handoff management solution (CSH-MU) with embedded vertical handoff decision algorithm (VHDA) based on RSS and power consumption for mobile phones with restricted system resources (e.g., limited access to decision metrics, battery life).

The author has been assimilated the knowledge about Vertical handoff and different distance based schemes for improvement in vertical handoff. They explained the core concept to implement the data transfer rate vertical handoff in 4G wireless heterogeneous networks. They explained that the Wireless Heterogeneous Networks are integrated within fourth generation recently. The 4G wireless communication system should assure a few of QoS related facilities such as offering high data rates, seamless mobility, strong RSS. When accomplishment and requisite of a user is acknowledged the system get succeed in handoff and seamless connectivity.

Vertical handover can be implemented by taking the techniques used in Wi-Fi (Wireless Fidelity) & WiMAX (Worldwide Interoperability for Microwave Access). They explained that if a mobile station velocity is high and its movement pattern is irregular, unnecessary handovers likely occur more frequently, and then a seamless handover algorithm between heterogeneous wireless networks is required.

The author has explained the vertical handoff in mobile networks having different networks and implemented in VANET. They explained That In Vehicular ad hoc network (VANET), vehicular users (VUs) are capable of connecting to different access networks for interacting both safety related information and user application related information. In the overlapped area of heterogeneous networks, VUs are allowed to perform vertical handoff between various access networks. As the performance of vertical handoff plays an important role in guaranteeing user quality of service (QoS) and achieving system performance enhancement, it should be examined and evaluated thoroughly.

III.THE PROPOSED SCHEME

In this Paper, a velocity-adaptive handover scheme is proposed to reduce the HO delay and the waste of the wireless network resource. In WiMAX system, the Received Signal Strength Indicator (RSSI) is typically used as a measure of signal quality. And as soon as the RSSI form the current serving BS is lower than a threshold and the RSSI from a potential target BS reaches a threshold, HO is executed. The most important factor to initiate HO is the received signal strength and MS mobility. However, the IEEE802.16e standard considers only the former.

In our scheme, the HO threshold is set variably according to the MS's velocity, which can reduce the HO delay and wireless network resource waste. The IEEE 802.16 standard of the Worldwide Interoperability for Microwave Access (Wi MAX) aims to provide broadband wireless access for Metropolitan Area Networks (MAN) and offers all packet-switched services for fixed, nomadic, portable, and mobile accesses. The first specification, IEEE 802.16-2004 [I], also called Fixed WiMAX, was ratified by IEEE in 2004 and was extended by the development of IEEE 802.16e [2], also called Mobile WiMAX, which supports mobility so mobile stations can handover between base stations while communicating, as well as supporting some other functions including multicast. In Mobile WiMAX, there are three possible approaches specified to implement handover (HO).

Hard handover (HHO), Macro Diversity Handover (MDHO), and Fast Base Stations Switching (FBSS). IEEE 802.16e supports two different mechanisms for authentication: the mobile station (MS) and the base station (BS) may use RSA-based authentication or Extensible Authentication Protocol (EAP)-based authentication. EAPbased authentication uses a backend infrastructure, such as the AAA (Authentication, Authorization, and Accounting) architecture. Due to the flexibility and ability to interact with AAA infrastructures, it is very likely that EAP will become the de facto authentication method for 802.16e access control [3].

I Propose a fast and secure EAP-based pre-authentication scheme for the inter- ASN HOs. 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 resource. It can overcome the above mentioned drawbacks by allowing the MS to exchange the secret keys with the AS instead of the neighbour ASNs (nASNs). Moreover, the proposed scheme can meet the security requirements of an authentication protocol. The exchange of secret keying materials guarantees high level of the security, which can be proved by the BAN logic. The proposed scheme follows pre-authentication approach to effectively reduce the HO authentication delay in the duration of the SA-TEK 3-way handshake. The proposed scheme is described in below Fig. The procedure of the proposed scheme is as
follows.

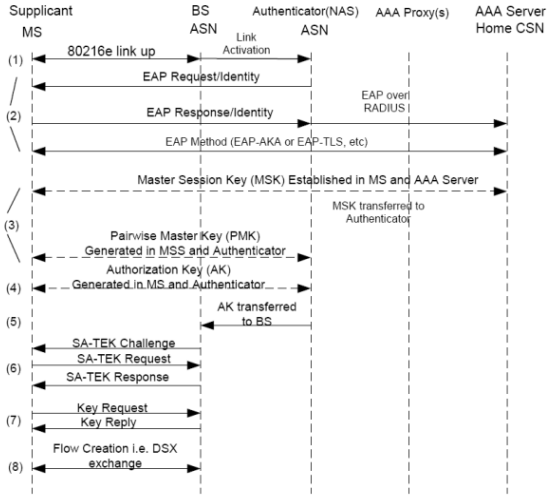

Figure of Proposed Scheme

A. Procedure of Implementation

Step 0: In the first time when a MS 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, which 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, which is specified in [1].

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: The MS initiates a pre-authentication session by randomly generates a pre-master secret (PMS) and a nonce NMS. The PMS is encrypted using the PEK. The MS constructs the PREAUTH_REQ message 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 pre authentication 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.

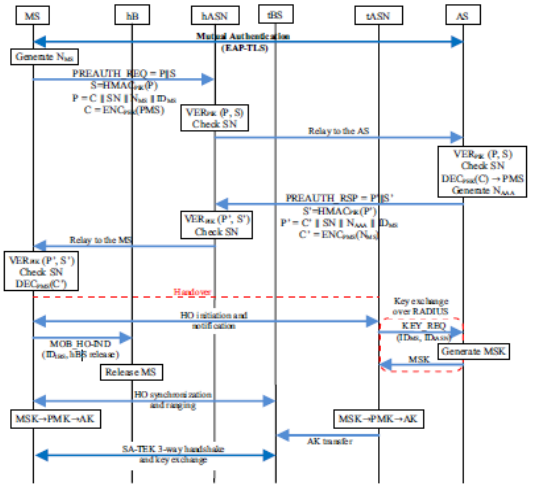

Figure 3: The proposed Pre-authentication Scheme

Notation	Definition
ENCx	Encrypt *X* using *K*
DECK (X)	Decrypt *X* using *K*
HMACK (X)	Generate HMAC for message *X* using *K*
VERK (X,S)	Verify *X* with the corresponding HMAC (S) using *K*
IDA	Identifier of A
NA	Nonce generated by A
X‖Y	Concatenation of *X* and *Y*

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)

More information on the TLS-PRF-X function can be found in [12]. Not only the MSK but also the EMSK and the initialization vector (IV) can be derived after the preauthentication process. The MSK will be protected by using the shared secrets between the AS and the tASN and sent back over the RADIUS. Meanwhile, the MS can derive the MSK using the similar formula. After above 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.

B. EFFICIENCY OF PROPOSED WORK

By the Proposed scheme, the EAP authentication procedure between HO AND tANS

has been migrated into pre-authentication process. The analysis result is summarized in fig 4. In the table, m denotes the average number of neighbour BSs. It is assumed that the number of BSs in the diversity set is also same as the number of neighbour BSs, m.

The communication property represents the number of communication exchanges for authentication and key distribution. Typically, the communication cost is the most important factor to evaluate the efficiency of a protocol. In this analysis, communications for the common message exchanges such as for the initial authentication exchanges between the MS and the serving BS are not included. The computation property represents secret keys that each entity is supposed to generate in each scheme. The MSK and TEK are not derived from other keying materials so that they are not included in the analysis.

The memory requirement property represents the secret keys that each entity should maintain. In the IEEE 802.16e, there are two kinds of TEK per SA at a given time, one is an old TEK and the other is a new TEK whose life times are overlapped for a seamless secure connection. In addition, the TEK can be created and revoked dynamically for the dynamic SA associated with the dynamic service flow management. However, TEKs for the dynamic SAs are not included in the analysis for simplicity. The backward/forward secrecy represents that whether each scheme satisfies the backward and forward secrecy, and resists the domino effect.

In the proposed hard handover scheme, the MS should generate and store m PMKs and m AKs during the preauthentication phase; whereas, the MS is required to generate and store only the current PMK and AK related to the serving BS in the IEEE 802.16e hard handover scheme. Upon a handover, however, the re-authentication phase in the proposed hard handover scheme requires only 3-way handshake since the PMK is delivered to the target BS and the AK is already shared in the pre-authentication phase before handover. Thus, the most time-consuming process of EAP-based authentication is eliminated during the handover process. Likewise, in the proposed soft handover scheme for FBSS, the MS is required to generate and store m PMKs, m AKs, and m TEKs. The communication cost for a key distribution in the proposed scheme is almost same as the IEEE 802.16e soft handover schemes. The Key Request and Key Reply message in the IEEE 802.16e soft handover schemes are replaced by the 3-way handshake, which one more message needs exchange per BS in the diversity set. Since the 3-way handshake does not execute at a significantly higher frequency than the TEK distribution, the additional communication cost seems trivial.

The IEEE 802.16e soft handover schemes cannot guarantee the backward or forward secrecy due to the domino effect resulted from the share of the same key. In contrast, the proposed soft handover scheme for FBSS satisfies the backward and forward secrecy due to the independent key management among the BSs in the diversity set.

The following are the graphs which can shows differences network using our scheme before and after.

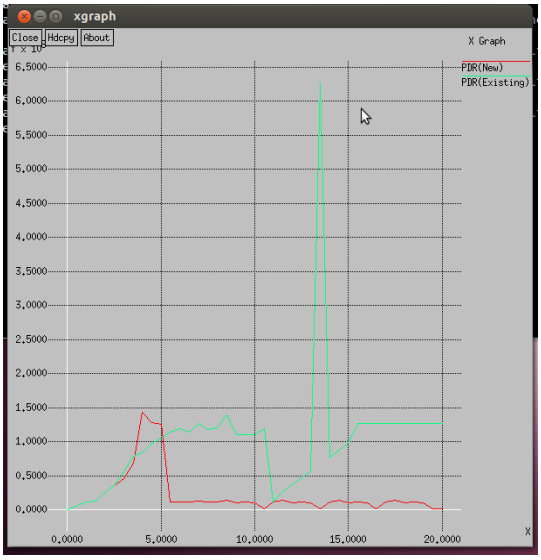

Fig. A PDR (Packet drop ration which is based on packet send from one node to another)

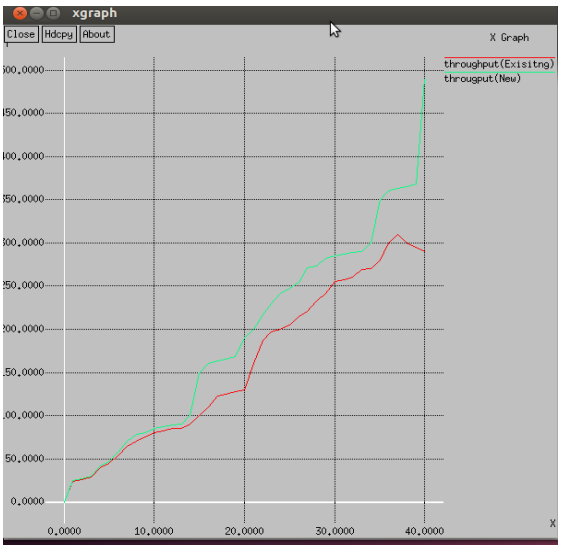

Fig. Throughput graphs defines the rate of successful message delivery over a communication channel

VI. CONCLUSION

A method should be proposed to reduce handover latency and to minimize the handover delay by minimizing unnecessary scans to find target

Base Station and also prevents resource wastage. Secure data transfer is important in Mobile WiMAX, 3G or 4Gnetwork therefore some improvements are needed in handover procedure to make secure and efficient data transfer. In this paper, we analysed different security aspects of hand over schemes defined for IEEE 802.l6e as well as their vulnerabilities. Afterwards, we used the Scyther tool to formally verify the handover security of the IEEE 802.16 standard. This verification showed some flaws in the used standard. For example, some messages which carry sensitive information without any authentication were found. If they are forged this can be dangerous for the system operation. In addition, the IEEE 802.l6e specification does not define a pre-authentication scheme.

Although we believe that this pre-authentication handover scheme would be of high value for a more secured protocol. Therefore, we formally verified the proposed pre-authentication handover scheme and proved that it is opposing the domino effect. Finally, we proposed changes on the pre-authentication protocol and verified that using Scyther tool, such proposed changes will increase the security of Mobile WiMAX significantly. In this paper, two efficient schemes are proposed to accelerate handover authentication in Mobile WiMAX. These two schemes need less modification on current WiMAX architecture. The proposed schemes are efficient and are as secure as the standard one. In the future, we will demonstrate the improvement by some simulations.

V. 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) 1.Topside E. Mathonsi, Okuthe P. Kogeda "Handoff Delay Reduction Model for Heterogeneous Wireless Networks" Tshwane University of Technology, Private Bag X680, Pretoria 0001, South Africa. Copyright © 2016
12) Khosrow Ramezani1, Elankayer Sithirasenan, (Member, IEEE), and KAILE SU, (Member, IEEE) "Formal Security Analysis of EAP-ERP Using Casper" Received December 8, 2015, accepted December 28, 2015, date of publication January 12, 2016, date of current version March 3, 2016.
13) Ola Salman Sarah, Abdallah Imad, H. Elhajj Ali, Chehab Ayman Kayssi "Identity-Based Authentication Scheme for the Internet of Things". Department Electrical and Computer Engineering American University of Beirut Beirut 1107 2020, Lebanon 978-1-5090-0679-3/16/$31.00 ©2016 IEEE
14) 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-2015.
15) Amali Chinnappan , Ramachandran Balasubramanian "Complexity–consistency trade-off in multi-attribute decision making for vertical handover in heterogeneous wireless networks". Electronics and Communication Engineering, SRM University, Chennai, India. IET Netw., 2016, Vol. 5, Iss. 1, pp. 13–21 & The Institution of Engineering and Technology 2016
16) Eiji Kamioka , Toan Nguyen-Duc "Feasibility of SDN-based Vertical Handover between Bluetooth and Wi-Fi". Graduate School of Engineering and Science Shibaura Institute of Technology Tokyo, Japan. 978-1-4673-6547-5/15/$31.00 ©2015 IEEE
17) Ivan Demydov, Marian Seliuchenko, Mykola Beshley, Mykola Brych "Mobility Management and Vertical Handover Decision in an Always Best Connected Heterogeneous Network". Tc Department, Lviv Polytechnic National University, UKRAINE. CADSM 2015, 24-27 February, 2015.
18) Avinash K S, Arijit Ukil, Jaydip Sen "Vertical Handoff in Heterogeneous Wireless Networks"Innovation Lab, Kolkata Tata Consultancy Services Limited, Kolkata, India
19) 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.
20) 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.
21) 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.
22) 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.
23) 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.
24) 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.

25) 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.
26) T. Issariyakul and E. Hossain, *Introduction to Network Simulator NS2*. New York: Springer, 2008.
27) M. Kassar, B. Kervella, and G. Pujolle, "An overview of vertical handover decision strategies in heterogeneous wireless networks," *Comput. Commun.*, vol. 31, no. 10, pp. 2607–2620, Jun. 2008.
28) F. Akyildiz, J. McNair, J. S. M. Ho, and H. Uzunalioglu, "Mobility management in next-generation wireless systems," *Proc. IEEE*, vol. 87, no. 8, pp. 1347–1384, 1999.
29) F. Zhu and J. McNair, "Multiservice Vertical Handoff Decision Algorithms," *EURASIP J. Wirel. Commun. Netw.*, vol. 2006, no. 1, pp. 1–13, Jul. 2006.
30) J.-M. Kang, J. Strassner, S. Seo, and J. W.-K. Hong, "Autonomic personalized handover decisions for mobile services in heterogeneous wireless networks," *Comput. Networks*, vol. 55, no. 7, pp. 1520–1532, May 2011.
31) N. Nasser, A. Hasswa, and H. Hassanein, "Handoffs in fourth generation heterogeneous networks," *IEEE Commun. Mag.*, vol. 44, no. 10, pp. 96–103, Oct. 2006.
32) J. H. R. H. F. V. Nishith D. Tripathi, "Handoff in Cellular Systems."
33) F. Akyildiz and W. Wang, "A dynamic location management scheme for next-generation multitier PCS systems," *IEEE Trans. Wirel. Commun.*, vol. 1, no. 1, pp. 178–189, 2002.
34) N. Mani and Y. A. Cekercioglu, "A Traveling Distance Prediction Based Method to Minimize Unnecessary Handovers from Cellular Networks to WLANs," *IEEE Commun. Lett.*, vol. 12, no. 1, pp. 14–16, Jan. 2008.
35) H. Zahran, B. Liang, and A. Saleh, "Signal threshold adaptation for vertical handoff in heterogeneous wireless networks," *Mob. Networks Appl.*, vol. 11, no. 4, pp. 625–640, May 2006.
36) S. Mohanty and I. F. Akyildiz, "A Cross-Layer (Layer 2 + 3) Handoff Management Protocol for Next-Generation Wireless Systems," *IEEE Trans. Mob. Comput.*, vol. 5, no. 10, pp. 1347–1360, Oct. 2006.
37) M. D. Austin and G. L. Stuber, "Velocity adaptive handoff algorithms for microcellular systems," in *Proceedings of 2nd IEEE International Conference on Universal Personal Communications*, 1993, vol. 2, pp. 793–797.
38) L. Hua, M. H. Kabir, and T. Sato, "Velocity adaptive vertical handoff on multi-frequency system," in *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2009, pp. 773–777.