CUSTOMIZED KEY DERIVATION FUNCTION FOR NEW TIME STAMP IDENTITY AUTHENTICATION PROTOCOL ON WIMAX

[1]AHMED AWADALLA, [2]AHMED RADI, [3]ALAA ROHIEM SHEHATA, [4]A. SESAY

[1,4]Department of Electrical Engineering, University of Calgary, Calgary, Alberta, Canada
[2]Department of Geomantic Engineering, University of Calgary, Calgary, Alberta, Canada
[3]Department of Communication Engineering, Military Technical Collage, Cairo, Egypt
E-mail: [1]ahmed.awadalla@ucalgary.ca, [2]ahmed.elboraee@ucalgary.ca, [3]alaa_rohiem@yahoo.co.uk, [4]sesay@ucalgary.ca

Abstract - To be able to achieve the desired level of confidentiality, integrity, and availability for the network system and services, future network security faces various important security issues. Many of these security problems need to be addressed in different modes and for different user types, even in the final security standard of Worldwide Interoperability for Microwave Access (WiMAX), Privacy and Key Management version 2 (PKMv2). In this paper a new technique for securing Wireless Local Area Network (WLAN), especially WiMAX networks using customized encryption and decryption standard algorithms that depend on different Secure Hashing Algorithm (SHA) is proposed and applied in our New Timestamp Identity Authentication Protocol (NTIAP). This technique is based on the addition of a new security level for key generation after the Master Session Key (MSK) expansion. This level helps the user to adapt the complexity of all keys derived between the Subscriber Station (SS), served Base Station (BS) and the expected BS during the handover process. Also, we can use the techniques to overcome most of the effects of attacks in the IEEE 802.16 without degrading service quality. The Customized Key Derivation Function (CKDF) was simulated and tested using a MATLAB simulation tool. A Graphical User Interface (GUI) which is capable of generating all types of keys that the user may use in the serving cell, and the expected one during the handover, is also developed. We used the most optimized techniques published for implementing the transformations used in the WiMAX security, to complete our design for the CKDF with our proposed NTIAP. A fair comparison and verification between the two standard authentication protocols (PKMv1 and PKMv2) and the proposed one (NTIAP) after adding the CKDF, is accomplished using the same sets of data and claims. Results demonstrated that the proposed protocol outperforms both standard ones in terms of higher security level since the new solution is efficient to tackling the various security threats such as replay, man in the middle and Denial of Service (DOS) attacks. The revised authentication protocol is expected to provide better secure platform for IEEE 802.16(e). Also, the new design helps the user to work in different modes of operations and with both fixed and mobile WiMAX.

Index Terms - WiMAX, PKM, PKMv1, PKMv2, Nonce, Timestamp, NTIAP, CKDF, AES, AAA, EAP.

I. INTRODUCTION

WiMAX is a promising technology that provides high data throughput with low delays for various user types and modes of operations. These advantages make WiMAX applicable for both infrastructure purposes and end-client usage. Since WiMAX is presented as a network framework and a last-mile technology, it is believed to be capable of handling a wide range of usage scenario. WiMAX defines Privacy Key Management (PKM) protocol in security sub-layer, which assures the security of connections access in WiMAX channel. Generally, PKM protocols have two goals, one is to provide the authorization process and the other is to secure distribution of keying data from BS to SS/Mobile Station (MS). PKM uses X.509 certificates and symmetric cryptography to secure key exchange between an SS and BS. There are two versions of PKM. The first version, PKMv1, is used in IEEE 802.16-2004 standard. The second version, PKMv2, is considered as an extension to work with the mobile WiMAX IEEE 802.16e [1, 2, and 3]. Various attacks are found in all versions of the PKM protocols which are designed in the security sublayer of IEEE 802.16 Message Authentication Code (MAC) layer. Those typical attacks are included in PKMv1 such as the Man-In-The-Middle (MITM) attack, the simple replay attack, the multiplicity attack. Also, other attacks are included in PKMv2, such as Intel-Nonce Version and the interleaving attack [4]. We propose counter-attack solutions and a NTIAP to resist those attacks [5], and overcome the existing security problems of WiMAX without degrading service quality. NTIAP has potential benefits that can provide enhancements to the overall security and efficiency of the security standards. To increase these features we need to update our system and customize the algorithms used in the standard key derivation function. All PKMv2 key derivations are based on the Dot16 Key Derivation Function (Dot16KDF) which is an Advanced Encryption Standard (AES) Counter Mode Construction (CTR) used to derive an arbitrary amount of keying material from source keying material [6]. These functions use SHA-1 which is a secure hash standard algorithm that gives a 160 bit output irrespective of any input [7]. Within the last decade we have noticed that the vast majority of trusted SHA-1 certificates die out. Currently, there are around 500,000 SHA-1 certificates still around [6]. If the user encounters a SHA-1 certificate, a degraded security indicator would be displayed. For instance, In Google Chrome, all SHA-1 certificates do not show the green padlock in secure connections,

and instead display the same icon as an unsecured HTTP connection [7]. Recently most security standards went through the "SHA-2 Transition" since SHA-2 remained unbreakable against the main well-defined attacks. It involved re-issuing thousands of existing certificates so that new files could be created and signed with SHA-2. The SHA-2 comprises four algorithms, namely, SHA-224, SHA-256, SHA-384, and SHA-512. SHA-224 and SHA-256 have several commonalities [8, 15]. Likewise, SHA-384 and SHA512 have several commonalities. These aforementioned SHAs algorithms are one-way hash functions that process a message to produce a message digest. In this paper the proposed CKDF enhanced and modified the standard KDF used in the standard PKMv2 in WiMAX technology using SHA-2 family to improve the security and meet these requirements to overcome theoretical drawbacks in SHA1 [9,10,11, and 15].

II. WIMAX STANDARD PROTOCOLS AND RELATED WORK

Security sublayer of WiMAX 802.16 consists of two component protocols, namely the encapsulation protocol and key management. As already mentioned in [2, 12, and 14], PKMv1 is a subset of PKMv2 regarding its function. Additionally, PKMv2 supports mutual authentication which will be explained in this section in details. Usually, the SS to BS mutual authentication can occur in one of two modes of operation. The first mode is only mutual authentication while the second is a mutual authentication followed by an Extendable Authentication Protocol (EAP) as shown in Fig.1 where three messages are illustrated as follows [13]:

Step 1: SS _ BS (PKMv2 Rivest–Shamir–Adleman (RSA)-Request message): This message immediately follows an authentication information message. By sending this message to the BS, the MS applies for the MSK.

Step 2: BS _ SS (PKMv2 RSA-Reply message): Upon receipt of the previous message, the BS performs the following actions: attests the identity of the client SS, generates a MSK, encapsulates the MSK using the SS's public key and sends it back to the SS using this message.

Step 3: SS _ BS (PKMv2 RSA-Acknowledgement message): This message follows a PKMv2 RSA then accepts/rejects the received message. By this message, the SS demonstrates to the BS that it is alive.

At the initial entry, the SS and the AS mutually authenticate each other via the EAP-based authentication method. The AS is an Authorization Authentication Accounting (AAA) Diameter or RADIUS server. The product of the EAP exchange is a 512-bit MSK, known to both the AS and the SS. After that, the MSK is securely transferred from the AS to the authenticator, i.e. the BS. Due to migration of the mobile subscribers, the handover gets into account by conditional changes in the radio channel or by cell capacity considerations. During this handover process, the SS has to accomplish the authentication procedure every time during the handover from one BS to another. Based on that, the time variability and the unpredictability of the channel become more acute and the main challenge arises from the need to handover sessions from one cell to another as the user moves across their coverage boundaries. During this handover process, it is still necessary to provide session continuity and to offer the previously negotiated end-to-end Quality of Service (QoS) and security levels [61]. The additional latency introduced by the handover process is an issue which needs to be tackled to minimize the impact of authentication procedure for the user who falls in the handover process very frequently. Thus, some additional measures are needed to get an effective service by involving the key-caching mechanisms (i.e. increasing the processing time and therefore reduces authentication cost).

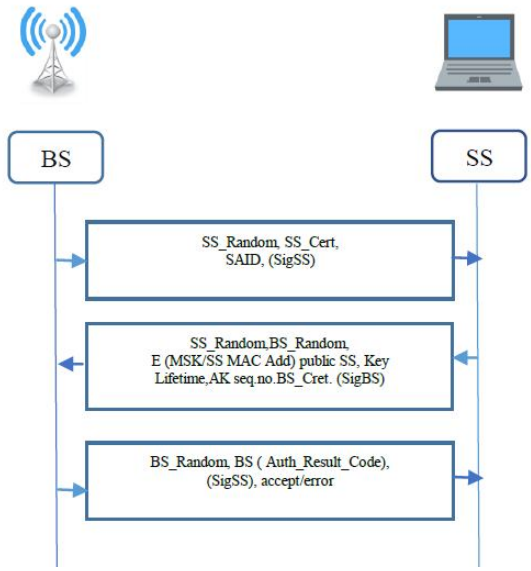


Fig. 1 WiMAX Mutual Authentication

Regarding the KDF, it is handled by the RSA-based authorization which, consequently, produces the EAP-based MSK [6, 13]. A complete map of the 802.16e key hierarchy is depicted in Fig.2 where the EAP-based authentication process yields the MSK that is given by Access Service Network (ASN) to BS by secured transmission and is transmitted to SS as seen earlier. MSK leads to the generation of other keys done independently in SS and BS [6, 7].

The procedure for Dot16KDF is shows as follows [7]:

```
Dot16KDF (key, a string, keylength)
{
result = null;
Kin = Truncate (key, 160);
for (i=0; i <1= int ((keylength-1) /160); i++)
{
result = result | SHA-1 (i| a string | keylength | Kin);
```

}
return Truncate (result, keylength);
}
Various standard keys generated in PKMv2 are:

1) Master Session Key (MSK-512 bits): This key is generated by the ASN and sent to BS through a secured channel. BS sends this key to SS after authenticating SS. The simulation work generates MSK by hashing MS_Random, BS_Random, MS_MAC, and BS_MAC using SHA-1.
2) Pairwise Master Key (PMK 160bits): MSK is truncated in such a way that the first 160 bits are derived as PMK.
3) Authorization Key (AK 160 bits): This is derived by Dot16KDF (PMK, MS MAC Address |BSID| "AK", 160)
4) Integrated Key (HMAC mode Key 448bits): This is derived by Dot16KDF ((AK, MS MAC Address |BSID| "HMAC_KEYS+KEK", 448)
5) Uplink Key (HMAC_KEY_U 160 bits): Integrated key is truncated in such a way that the first 160 bits are derived as HMAC_KEY_U.
6) Downlink Key (HMAC_KEY_U 160 bits): Integrated key is truncated in such a way that the second 160 bits, i.e. 161th bit to 320th bit, are derived as HMAC_KEY_U.
7) Key Encryption Key (KEK 128 bits): The remaining part of the integrated key, i.e. 321th bit to 448th bit, are termed as KEK.
8) Traffic Encryption key (TEK): TEKs are used to encrypt data transmission between the BS and SS. TEKs are generated by BS randomly. TEK encrypted with triple-DES (Use 128 bits KEK), RSA (Use SSs public key), and AES (Use 128 bits KEK).

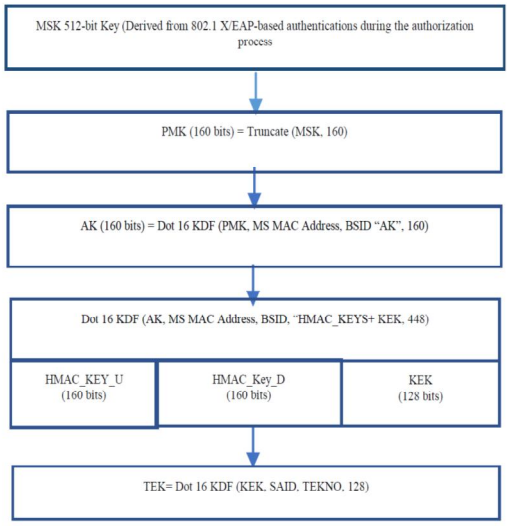


Fig. 2 Standard Key Derivation Function in PKMv2

III. THE PROPOSED AUTHENTICATION PROTOCOL

As discussed in [1, 2, 3, and 4], the existing standard protocols are still vulnerable to replay, Denial Of Service (DOS), and MITM attacks when analyzed using Scyther tool [5]. Some solutions are introduced to solve those attacks in our design [5]. To prevent both MITM attack and replay attack we add timestamp. There is only one main problem with timestamp where it requires time synchronization between MS and BS. In wireless communication, time synchronization is considered to be difficult (particularly under mobility). However, in IEEE 802.16e it is assumed that the synchronization is done between MS and BS [13]. Our proposed authentication protocol improves the WiMAX mutual authentication by increasing the authentication strength between SS and BS using timestamp. Authentication Server (AS) appears as trusted third party to authenticate the BS to SS and solve the main problem of rogue BS [5]. Also, to enhance the timing and communication overhead during the handover, we use a new idea through the scenario to enhance the security and efficiency of the network as shown in the following figure and messages: The following messages describes the enhancements in the standard authentication protocols included some modifications to improve the service performance [5].

Message 1: SS - BS: Cert (SS) (Auth Req message) | TS (Time Stamp)
Message 2: SS - BS: Cert (SS) | Capabilities | BCID | TS
Message 3: BS - SS: KUSS (AK) | Seq No | Lifetime | SAID List BSID
Message 4: BS - AS: BSID | SSID | KUss
Message 5: SS - AS: E (KRss, [SSID | BSID])
Message 6: AS - SS: E (KUss, [Confirmation Message])
Message 7: SS - BS: E (Further Communication)
Message 8: BS – MTSO E (SS credentials)
Message 9: MTSO – BS E (Conformation Message)
Message 10: MTSO – All BSs in the same cluster E (SS Credentials)
Message 11: BSs – MTSO E (Confirmation Message)
Message 12: SS – TBS Cert (SS) (Auth Req message) | TS
Message 13: TBS – SS E (KUss, [confirmation Message, BSID, ASID]

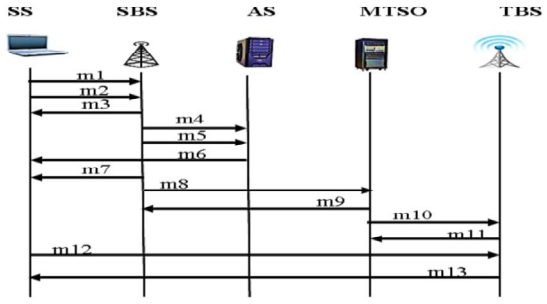


Fig. 3 NTIAP messages

IV. ANALYSIS OF THE PROPOSED CKDF DESIGN

In our enhanced new authentication protocol, the overall security for the entire system starting with the KDFs needed to be enhanced. This could be applied by performing two changes. The first one is related to

changing the hash function used in the standard DOT16KDF while the second change is regarding the hash function used to generate the Master Session Key (MSK), which is generated by the AS. To be more specific, these changes/enhancements include changing the derivation of the DOT16KDF and generate the MSK that depends on SHA-1 to make it able to work with different types of hash functions, as new features, such as; SHA-1, SHA-224, SHA-256, SHA-384, and SHA-256. Thus, the bit-length now is not fixed anymore as it directly depends on the hash function type. These different hash functions are used to generate the MSK. Such new features help us to increase the security for the messages travelling between the MS and BS since a larger bit hash can provide more security due to having more than and possible combination. The possible number of unique hashes can be expressed as the number of possible values raised to the number of bits. For SHA-256 as example, there are 2^{256} possible combinations, and so on with other hash functions. Briefly, the larger the number of possible hashes, the smaller the chance that two values will create the same hash. There are technically an infinite number of possible inputs [9, 10, and 11], yet a limited number of outputs. So, eventually, every hashing algorithm, including a secure one, produces a collision. SHA-1 was deemed insecure due to both its size and construction. The proposed generation keys schedule is shown in Fig. 4.

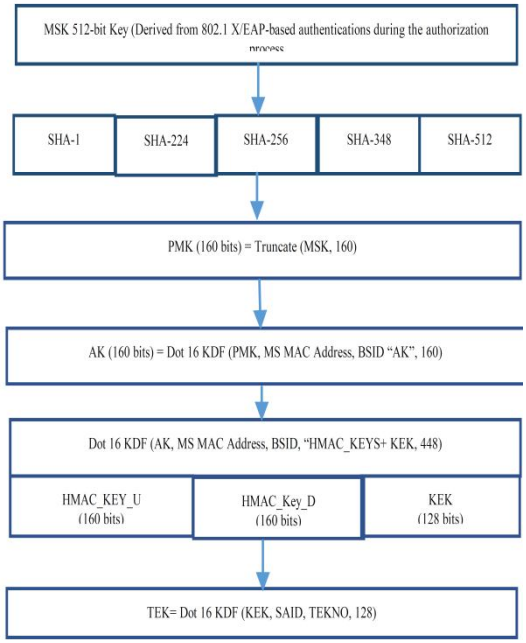


Fig. 4 CKDF for NTIAP

Fig. 4 highlights the detailed step-by-step of the new proposed technique used to enhance the security of the data transferred between the SS's and BS's. As mentioned before, this could be achieved by generating the keys used in the WiMAX network using the different types of standard hash functions (SHA-160, SHA-224, SHA-256, SHA-384, SHA-512) instead of the unique SHA-1 which is the standard hash function used in the standard protocol PKMv2. The first key is the selection of the type of hash function we need to use in our key derivation.

Firstly, the AS generates the MSK and sends it to the BS. Based on that, the BS generates the AK and sends it to the SS. Finally, the SS generates the integrated key to derive uplink key, downlink key, KEK and the TEK. All the keys derived in our simulation is in hexadecimal. It is known that SHA-1 and SHA-2 input block size depends on which algorithm is used [9]. In this stage the message is padded into a block size, namely chunk. The input block size of SHA-1, SHA-224 and SHA-256 is equal to 512-bits divided into 16 words of 32-bit (i.e. W[0-15]). While the input block size of SHA-384 and SHA-512 is equal to 1024-bits divided into 16 words of 64-bit (i.e. W[0-15]). Then the extension of W[0-15] depends on the algorithm used. Table I highlights a fair comparison between different hash functions.

TABLE I. Hash Function Comparison [10]

Algorithms	Rounds and W	Block Size (bits)	Output Size (bits)	Max Message Size (bits)
SHA-1	80	512	160	(2^64)-1
SHA-224	64	512	224	(2^64)-1
SHA-256	64	512	256	(2^64)-1
SHA-348	80	1024	348	(2^128)-1
SHA-512	80	1024	512	(2^128)-1

V. SIMULATION MODEL FOR CKDF

The proposed model for the enhanced CKDF was simulated using a MATLAB simulation tool and the simulation results are shown in Fig. 5. The components used in this implementation are: User's inputs; the details of the user are acquired and processed through a MATLAB GUI. Database; here we consider the standard MY- SQL database which acts as the AS in our Proposed method. Let us discuss the results with two subscriber cases. First case; when the subscriber is newly entering the network (new user) and second case is when the user is re-entering the network (old user).

1st case: New subscriber:

Subscriber enters the network randomly and his validity is checked corresponding to its existing MAC addresses pre-stored in the database. If not matched, then the user is affirmed as an "Unauthorized User". On the other hand, if the user is affirmed as an "Authorized User", then the MSK is generated by the AS and sent to the BS. After that, the BS sends it to the SS and derives the PMK from the MSK and,

consequently derives the AK from PMK. Moreover, AK is stored in the database against the corresponding MAC address. Then all other keys needed for the data transmission between the BS and SS derived, as shown in Fig. 4, using different standard hash functions (SHA-160, SHA-224, SHA-256, SHA-384, SHA-512) instead of using the unique SHA-1 used in the standard PKMv2. Thus, the user could have the ability to generate all possible keys used in the served cell or the next expected one during the handover process.

2nd case: Old Subscriber:

When the user re-enters the network, a request is sent from the SS to the BS. After that, the BS checks the validity of SS, authenticates it and declares him as the old user. If the SS is known to enter within its caching time, compressed AK is directly delivered bypassing all the steps aforementioned in Fig. 4 using different standard hash functions (SHA-160, SHA-224, SHA-256, SHA-384, SHA-512) instead of using the unique SHA-1 used in the standard PKMv2. Finally, the SS decompresses and derives AK. As mentioned in Section IV, the SS generates the integrated key to derive different keys (such as the uplink key, downlink key, KEK and the TEK). Thus, a GUI is needed to clarify such a generation, to the network designer, based on the selected hash function In the GUI for the proposed new CKDF used in WiMAX authentication, a dropdown menu on the upper left hand-side allows the designer to select a certain hash function, for instance SHA160, SHA224 and SHA512. The following step is the key generation which could easily be achieved by pressing the bottoms on the left hand-side of the GUI, as shown in Fig. 5. A window to the right hand-side of each key generated displays the required time needed to generate each key, depending on the platform used. Hence, the designer can calculate the processing time to derive all keys.

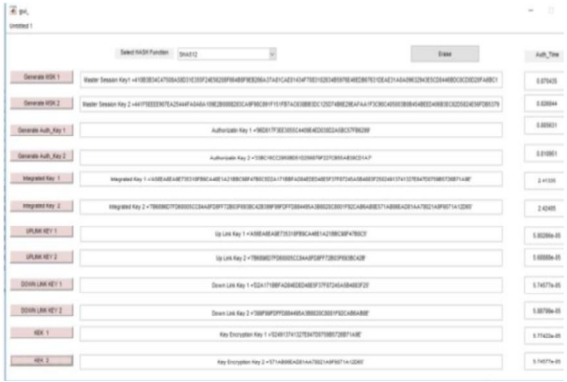


Fig. 5 Matlab GUI for CKDF used in NTIAP using SHA-1 and SHA-2

VI. RESULTS AND DISCUSSION

As mentioned in the previous sections the new authentication protocol NTIAP changes certain parameters in the network design when applied. We notice that we have some advantages and some disadvantages in the new proposed design. The main disadvantages that appeared during the simulations include: time delay, communication overhead, and the hardware description. Firstly, the time delay is increased a little bit since the added messages in the protocol became a part of the messages queue of the simulation, which means it is going to affect the overall time of the authentication process. The time delay also appeared after changing the main hash function algorithm SHA-1 used in the standard protocols to the different hash functions such as: (SHA-224, SHA-256-SHA-384-SHA-512). Secondly, the communication overhead increased since the newly suggested protocol added messages and functions which increased the number of iterations and computations needed to complete the authentication process. Finally we gained more hardware by adding new servers for the mutual authentication process in the network. Also the additional inserted messages caused an increase in the storage overhead. Regarding the advantages we mentioned that the proposed protocol outperforms both of the aforementioned standard ones in terms of higher security level since the new solution is efficient in tackling the various security threats such as replay, man in the middle and Denial of Service attacks. It also, solved the main problem in the communication network which was the rogue BS. Moreover, it helps the network designer to work with all modes of operations such as: (PTP, PMP, Mesh mode). The new design also helps the user to work in both fixed and mobile WiMAX. Last but not least, adding the new features in the CKDF increased the system ability and efficiency to overcome the main network threats.

Table II. Comparison between ntiap and standard protocols

Specs.	PKMv1	PKMv2	Proposed Design
Communication overhead	3 messages	4 messages	7 messages for fixed 13 messages for mobile
Storage overhead	4*160 bits	8*160 bits	10*160 bits
Computational overhead	4 times encryption	8 times encryption	10 times encryption
Mutual Authentication	No Mutual Authentication	With Mutual Authentication	With Mutual Authentication
Modes of operations	PTP, PMP, MESH	PTP, PMP	PTP, PMP, MESH
Mobility	Fixed	Fixed and Mobile	Fixed and Mobile
Security level	Low	High	High
Resiliency of attacks	Replay and MITM attacks	Prevent Replay and MITM Attacks	Prevent Replay and MITM Attacks
KDF	standard SHA-1	standard SHA-1	CUSTOMIZED SHA1 & SHA2

CONCLUSION AND FUTURE WORK

In this paper, we used the most optimized techniques published for implementing different hash functions used in the WiMAX security to propose a novel NTIAP authentication protocol to overcome most of the effects of attacks in the IEEE 802.16. A new key derivation function scenario, namely CKDF, was proposed and applied to the WiMAX network depending on replacing the fixed standard hash function, SHA-160 used in PKMv2, by other customized hash functions, such as (SHA-160, SHA-224, SHA256, SHA-384, and SHA-512), to enhance the security for the overall system. A MATLAB-based GUI was proposed to generate all keys needed by the user in the served cell and the next expected one during the handover process to enable the designer to calculate the processing time required to derive all keys. A fair comparison between the PKMv1, PKMv2 (as standard protocols) and the proposed NTIAP (after adding the CKDF feature). Results demonstrated that the proposed protocol outperforms both aforementioned standard ones in terms of higher security level since the new solution is efficient in tackling the various security threats such as replay, man in the middle and Denial of Service attacks. However, a noticeable increase in communication, storage and computational overheads related to the proposed NTIAP which could be considered as demerits for the proposed algorithm. The revised authentication protocol is expected to provide better secure platform for IEEE 802.16(e). Also, the new design helps the user to work in different modes of operations and with both fixed and mobile WiMAX. For future work we plan to verify the proposed algorithms using standard verification tools such as Scyther tool and implement the proposed design using a network simulator to assure the performance of the new algorithms without degrading the service quality and to prevent our communication system from the expected attacks.

REFERENCES

[1] Jinpeng Jiang, Hangyan Mao, Rumeng Shao, and Yuanmin Xu, “Formal Verification and Improvement of the PKMv3 Protocol Using CSP,” IEEE International Conference on Computer Software & Applications, pp. 682-687, 2018.

[2] T. Han, N. Zhang, K. Liu, B. Tang, and Y. Liu, “Analysis of mobile WiMAX security: Vulnerabilities and solutions,” in IEEE 5th International conference on Mobile Adhoc and Sensor Systems, MASS 2008, 29 September – 2 October 2008, Atlanta, Georgia, USA, 2008, pp, 828-833

[3] A K. Rai, S. Mishra, and P N. Tripathi. “An Improved Secure Authentication Protocol for WiMAX with Formal Verification”. In Communications in Computer & Information Science, 2011, 191:407-416.

[4] Vinod Kumar Jatav, Vrijendra Singh, "Mobile WiMAX network security threats and solutions: A survey", Computer and Communication Technology (ICCCT) 2014 International Conference on, pp. 135-140, 2014.

[5] Ahmed Mohamed El-Amin, Salah El-Agooz, Alaa El-Din Rohiem Shehata and Essam Abd-Elwanees Amer “ Design, Verification and Implementation of Enhanced PKM WiMAX Authentication Protocol”. International Journal of Computer Science and Telecommunications, volume 4, issue 3, March 2013.

[6] Alina Olteanu, A. Yang Xiao Yan Zhang.”Optimization between AES Security and performances for IEEE 802.15.3 WPAN”, IEEE transaction on wireless communications, Vol.8, 2009.

[7] Ip Hsieh, Shang Juh Kao, “Handoff optimization in 802.11 wireless networks”, EURASIP Journal on Wireless Communications and Networking 2011.

[8] Kuran, M.S,Gur. G,Tugcu.T, “Applications of the cross layer paradigm for improving the performance of WiMAX”, IEEE Transactions on Wireless Communications, vol: 17, 2010 , pp 86 -95.

[9] A.Kakarountas, A.Miliadonis, and C.Coutis H.Michail,"Efficient implentation of the keyed-hash message authentication code (HMAC) using the SHA-1 hash Function," in 11th IEEE International Conference on Asia South Pacific Design Automation (ASP-DAC'04), 2004, pp. 567-570.

[10] Safaa S. Omran and Laith F. Jumma “Design of SHA-1 & SHA-2 MIPS Processor Using FPGA”, Annual conference on Trends in Information & Communication Technology Applications- (NTICT 2017).

[11] Kadek Dwi Budi Utama, and M.Rizqia Al-Ghazali Q.,” Digital Signatuire Using MAC Address based AES-128 and SHA-2 256- bit”, International Seminar on Application for Technology of Information and Communication (iSemantic),2017.

[12] Prabhat Kumar Panda, and Sudipta Chattopadhyay,” Enhanced Security Scheme with Mutual Authentication for WiMAX System” IEEE- 40222 8th ICCCNT 2017, IIT, Delhi, India, July 3-5, 2017.

[13] Fan Yang, “Analysis and Application of EAP_AKA for IEEE Standard 802.16e.” IEEE 7th International Conference on Wireless Communications, Networking and Mobile computing. Wuhan, China, 2011.

[14] Fan Yang, “Comparative Analysis on TEK Exchange between PKMv1 and PKMv2 for WiMAX”, IEEE 7th International Conference on Wireless Communications, Networking and Mobile computing. Wuhan, China, 2011.

[15] Wanzhong Sun, Hongpeng Guo, Huilei He, and Zibin Dai,”Design and Optimized Implementation of the SHA-2(256, 348, 512) Hash Algorithms. IEEE 7th International Conference on ASIC, Guilin, China, 2007.

★★★