SECURE AND EFFICIENT HANDOVER AUTHENTICATION AND DETECTION OF SPOOFING ATTACK

Murugan K[1], Boobalan S[2], Varalakshmi P[3], Nandha Kumar R[4]

[1]*Research Scholar, Department of Computer Technology, Anna University, Tamil Nadu, India*
[2]*PC Scholar, Department of Computer Technology, Anna University, Tamil Nadu, India*
[3]*Assistant Professor, Department of Information Technology, Anna University, Tamil Nadu, India*
[4]*Research Scholar, Department of Computer Technology, Anna University, Tamil Nadu, India*

Abstract

WiMAX comprises of mobile nodes, to provide secure and seamless communication. Handover latency in WiMAX plays a vital role in performance of the system. In this paper we proposed a group manager scheme to reduce the handover latency and security consideration. The Group Manager sends the authentication details of the mobile node to the target Base Station. In order to provide security ,the Group Manager authenticate the Mobile node with base station using light weight RC4 algorithm and then sends it to access service network(ASN). In order to detect the Spoofing attack, an Attack Detection System has been developed using Support Vector Machine which prevents group manager and its mobile nodes from intruders. This approach drastically reduces the number of messages and time taken for authentication and thereby improves the overall efficiency of the network.

Keywords: *mobile WiMAX, Group Manager, Handover, and Authentication.*

----------***----------

1. INTRODUCTION

WIMAX (Worldwide Interoperability for Microwave Access) has been established as one of the most promising solutions for broadband wireless-access technologies due to its high data rate, wide coverage, low cost and built-in support for mobility. However, there are a number of issues which may lead a deployment challenge for the mobile WiMAX networks. Firstly, due to the convenience and mobility of the Mobile Station (MS), the handover request becomes more frequent, which leads to the demand for an effective and fast authentication scheme. There are two authentication methods, RSA and Extensible Authentication Protocol (EAP), in first version of mobile WiMAX standard. The EAP protocol is the only stated authentication method in the next generation mobile WiMAX standard (IEEE 802.16m) [1] because of the flexibility and ability to interact with Authentication, Authorizing and Accounting (AAA) infrastructures. However, a full EAP authentication lasts a considerable time (e.g. an EAP/TLS exchange needs about 8s [2]) which is difficult to support real-time applications, such as video conference, in a handover process. In recent years, many schemes [2-4] have proposed to reduce the handover authentication delay by avoiding the implementation of the EAP authentication. In [5], we also presented a fast handover authentication scheme based on ticket for IEEE 802.16m network. When an MS moves from the service Base Station (BS) to a target BS, it can show its ticket to the target BS and then this BS can authenticate the MS without interacting with any other third party. However, all these schemes have not considered the case of many correlated MSs moving together. For example, users taking the same vehicle such as a bus or a train are always located in the same network and move in the same direction [6]. When correlated MSs Move together in a group and handover from one BS to another at the same time, handover performance could be enhanced if the group information is used. Secondly, because of their intrinsically open nature and the absence of physical protection, wireless networks are vulnerable to spoofing attacks. As a result, an external adversary can easily compromise the MSs Identity privacy due to the sensitive information exchanged in the handover authentication process. What's worse, a global adversary can even trace the MSs Movement route. Therefore, privacy preservation should be paid much more attention to in the handover authentication schemes.

Although the schemes [7, 8] protect the identity information from the adversary, the location privacy is uninvolved and stills a challenge issue. In [9], the location privacy preserving is realized at the cost of the time-consuming cryptography operations on the resource-constraints MS. However, WiMAX network is an unbalance environment, where BS is physically stationary with relatively powerful computing resources while MS is constrained by the computation ability, the storage ability and the battery power. As a result, we should minimize the time-consuming cryptography operations on the resource-constraints MS. With the purpose of a secure and efficient handover process, in this letter, we propose an efficient group-based handover authentication scheme with privacy preservation for mobile WiMAX networks. The main

contributions of this letter involve the following two aspects:
1) Our method transmits all the handover group members' details (security contexts) to the target BS using the encryption scheme during the first MS handover authentication phase. MS sends the authentication details to GM encrypted with RC4 algorithm. Group Manager Aggregates the details received from all MS sends it to the BS.
2) BS receives the authentication details and decrypts it using MD5 algorithm and sends it to the ASN encrypted using MD5. ASN upon receiving the message, decrypts it, verifies the authentication details and sends the response back to BS which in turn sends to GM.

The rest of the paper is organized as follows. In section II, we briefly explained regarding the literature survey and presented a comparative study of advantage and disadvantages of different handover systems. This is followed in next section III by a brief discussion about the group manager architecture and spoofing attack detection. Section IV with insights to the proposed group manager system's the performance analysis and section V finishes with the conclusion and future work.

2. LITERATURE SURVEY

An efficient and secured protocol is proposed for handover authentication using a system called Handauth [1]. It provides secure authentication and session key establishment. It faces computation overhead and vulnerable attacks since session key is exchanged between mobile nodes and base station. [2] Proposed an pre authentication handover mechanism which in turn suffers with computation overhead since lot of computation happens during initial authentication phase. [3] Proposed an mechanism in which the service Base Station(BS) sends all the handover security context to the target Base Station which results in unwanted transmission of security messages. [4] proposed an efficient protocol called Pair Hand which suffered inherent vulnerable in session key management. [5] Proposed standard mechanism which uses two schemes for efficient handover authentication. First scheme performs authentication using shared key based EAP protocol. Second scheme uses three way handshake process. [6] Proposed an proxy ring signature for EAP protocol which also faced an security issues with spoofing attacks.[7]proposed an improved mobile management process which reduces re-authentication process and IP configuration and supports low handover latency using AAA key based Mobile Agent Identifier. [8] Proposed an intrusion prevention system which is not based on cryptographic functions. It uses spatial correlation of (RSS) Received Signal Strength to detect the spoofing attacks. [9] SVM (Support Vector Machine) was operates mainly on binary classification. Multiclass Classifier has been proposed by several authors by combining several binary classifiers. It results in computationally more expensive to solve multi class problems. Hence, comparisons of these methods have not been done seriously. [10,11]SVM based technique is used for classifying multi spectral image satellite image. Comparison is made between the overall accuracy of conventional image classification method. This paper used SVM for different purpose which is rarely used. [12]IEEE provided a standard 802.11 and 802.11i for WLAN to address the security flaws and vulnerability. But still WLAN suffers from spoofing attacks which results in DoS attacks by launching disassociation messages. [13] MAC addresses of nodes can be easily spoofed and used for DoS attacks. RSS (Received Signal Strength) measurement is used as an important factor for detecting spoofing attacks. But proposed scheme suffers ineffective because they use Single RSS Source. [14] proposed a secure and efficient key management framework (SEKM) for mobile ad hoc networks. SEKM builds PKI using secret sharing scheme with the help of multicast server group. This scheme uses distribution of public key which becomes viable for malfunctioning of networks.

3. PROPOSED SHEME

In this section, the lightweight authentication scheme for handover in mobile based group manager networks is proposed. The mobile nodes are grouped into different groups based on their locality. Figure-1 says that for each group, one group manager selected based on the energy availability. When handover occurs in mobile nodes, authentication is required for efficient functioning of the Mobile networks. For authentication, the mobile nodes have to send their authentication details ASN. For this, mobile nodes send the authentication details to its appropriate Group Manager. Group Manager in turn collects all the messages from its mobile nodes and then aggregates the messages after verifying using enhanced MD5 algorithm. The aggregated message is sent to Base Station for authentication. Base Station sends the authentication request to ASN. ASN, in turn authenticates the details decrypted using MD5 algorithm.

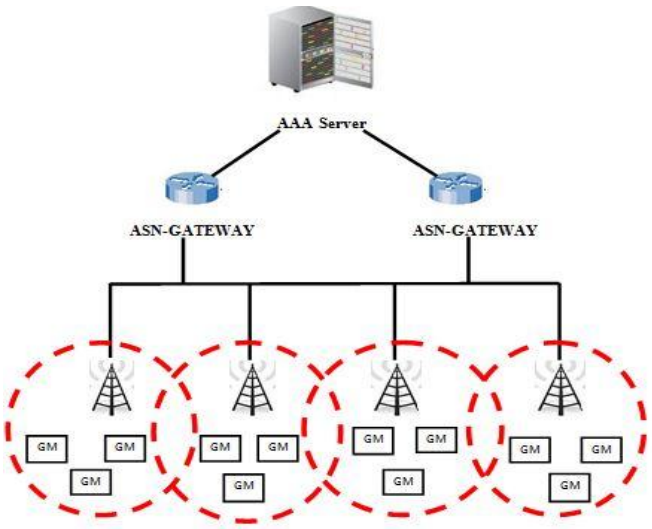

Fig.1. System Architecture

If any discrepancy found while authenticating, the network will be scanned for attacks. This attack detection is achieved using Support Vector Machine concepts. In this system, Spoofing attack is mainly concentrated since mobile networks are more viable to Spoofing attacks more often. In this system the authentication system and attack detection system operates independently. Thus, no extra operation for the authentication server is needed, and the security and the performance are balanced. And the maximum data range of WiMAX networks is found untouched with range reaching up to maximum 40km.

3.1 Group Manager and Authentication

In this section, our enhanced lightweight authentication system for Mobile Networks is proposed. Our proposed system has four different phases such as Group Manager Formation, authentication and aggregation, authentication by ASN nodes, intrusion detection for achieving efficient handover and intrusion detection. Initially the network is assumed to have as many nodes as possible.

Initial Authentication Phase:

a) Group Managers formed using LEACH Algorithm.

b) Mobile nodes encrypt the data using RC4 with hash value.

c) Mobile node sends the authentication request to Group Manager.

d) Group Manager receives the request, decrypts it and validates using calculated key based on packet transmission time, packet processing time, transmission delay.

e) Mobile Node during handover,
Compute the key($K^t_j \leftarrow F(t_l,IV)$)
Encrypt data using K^t_j.
Forward the data.
Group Manager receives the data.
Calculate Tick Window Size.
While (count<=tick window size)
{
Compute key k_j
If (k_k==k_j)
Forward the packet to destination Else
Continue
}
If (count>tick window size)
Discard the packet. //Destination:
Receive the packet
While (count<=tick window size)
{
Compute key k_j
If (k_k==k_j)
Decrypt data and read it Else
Continue
}
If (count>tick window size)
Discard the packet.

The number of groups in the network may change dynamically. The nodes choose their Group Manager based on their energy. The nodes during handover send their authentication data directly to the Group Manager which in turn sends it to the base station after aggregating all data it received. For group manager formation, LEACH (Low-Energy Adaptive Clustering Hierarchy).

LEACH has two phases: the set-up phase and the steady-state. I) The Set-Up Phase-Where Group Managers are chosen based on the energy. II) The Steady-State-where the Group Manager is maintained and data is transmitted between nodes. RC4 algorithm is used for checking the integrity between mobile node and group manager. Then it aggregates the data and sends the aggregated one using MD5 based encryption. RC4 algorithm is one of the most efficient, lightweight and requires less energy consumption and computation. In RC4, the key generation and state array swapping is done on both the ends. Generally, RC4 algorithm uses a static key and a state array for the key array generation. In this system, time is used as the key. So the key is changing dynamically without any need for frequent transmission. Receiving end gets the time of the sender using the packet transmission time and decrypts the received data to get the original message. Since it is dynamic, there is less chance for any intruder attack. Also mostly in all dynamic keying systems, a lot of energy is required for the transmission of the key. In this system, there is no need for any explicit key transmission. This results in the saving of more energy and overhead in the system. . In RC4, key is dynamically changing but without explicit transmission. So, it will be less difficult to the attack and take preventive measures.

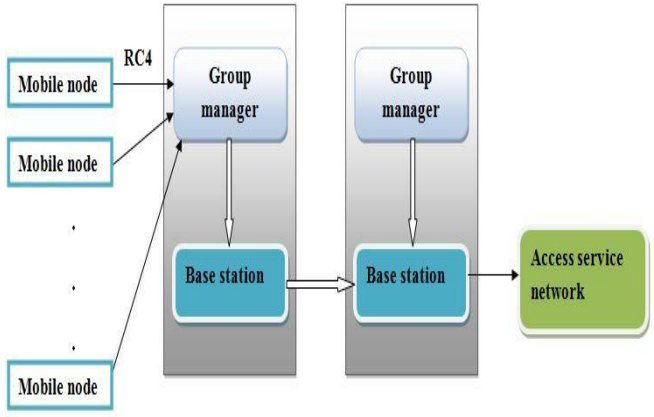

Fig.2. Group Manager

After this, Group Manager will receive the message and create hash for the message. Group Manager will collect the data sent by the nodes in its group. Group Manager reduces the resource utilization effectively by aggregating all the data send by its mobile nodes. This is by means of calculating mean, median, number of data, maximum and minimum values. Finally these data are encrypted finally and send to the Base Station. The hashing algorithm is implemented on both sides. So, a Group Manager will create a hash for each authentication request and send it along with authentication details to base station. The aggregation is done by maintaining an audit log for each Group Manager. The audit log contains Group Manager ID followed by the data it receives.

Handover Authentication Phase:

Suppose consider that Handover happens for mobile node leaving BS1 to BS2 through GM2.

a) MN sends the encrypted authentication request to GM2.

b) GM2 in turn, validates the request and forward it to BS2 for authentication.

c) BS2 receives the request and send it to ASN for authentication. ASN verifies the mobile node details like initial authentication phase and send the response back to the BS2 which in turn sends the response back to the GM2.

After a certain amount of time, it will collect the data from the log and perform aggregation of collected data. The aggregated data is encrypted using the hash generated by MD5 in the group manager. Base Station after receiving the data, compares the generated hash value with the received hash to verify the integrity of the authentication request message. Since extended MD5 algorithm for authentication is used between Group Manager and Base Station, an intruder can comprise the system and capture the authentication details of normal node.

3.2. Attack Detection Using Group Manager

A support vector machine (SVM) is a concept for a set of related supervised learning methods that analyze data and recognize patterns, used for classification and regression analysis. The standard SVM takes a set of input data and predicts, for each given input, which of two possible classes forms the input, making the SVM a non-probabilistic binary linear classifier. Given a set of training examples, each marked as belonging to one of two categories, an SVM training algorithm builds a model that assigns new examples into one category or the other. Support Vector Machine uses support vectors determined from training samples for classification. In this experiment, the support vector rules, which are critical for classification, are obtained by analyzing the data from the training samples. In our experiment, support vector machine is used to classify the malicious node from the normal node. The Malicious node may cause several attacks such as Spoofing attack, Authentication attack and so on. The support vector machine concept is used in both Group Manager and Base Station since there may be the possibility of attacks when the data is being sent from mobile nodes to its appropriate Group Managers or from Group Manager to Base Station.

In mobile networks, the nodes can send abnormal data thereby enabling the base station to malfunction. For example, consider a scenario where the mobile nodes in networks send the authentication details. The malicious node may interrupt the request message and capture the authentication details and use it for Spoofing attacks. If the intruder continuously sends malicious data, then most of Group Manager's energy will reduce considerably by raising an alarm and in minimal time the node will run out of energy. In order to overcome this type of attacks, Intrusion detection module with Support Vector Machine Concept, processes the packet being sent by group nodes or group manager. If packet fails to satisfy the predetermined rules, it will be marked as abnormal data and the packet will be dropped. Generally in RC4 algorithm, keys are generated dynamically in both ends of transmission without any need for key exchange. Using this property in Support Vector Machine, Sender sends the encrypted message along with the key. So that if any changes occur in encrypted data or key, extended RC4 algorithm will find the key based on packet processing time, packet transmission time and delay.

Intrusion Detection:

Step 1: Generate the set of training features for group manager and base station

Step 2: Train the nodes with the set of features generated for intrusion detection.

Step 3: Receive the packet. Check whether the node is in malicious list or not.

If found,

Discard the packet.
Else
Process the received packet.

If Found matching with the set of trained features,

Discard the packet; add the node to malicious list
Else
Forward the packet towards the destination.

If the calculated key varies from the received key for more number of occurrences, the node will be classified as

malicious. In this case, the Base Station can easily ignore the packet sent by the malicious nodes. To experiment our proposed scheme, an test has been conducted using 1000 mobile nodes in which 50 nodes are used for generating spoofing attacks in different interval of time. Our scheme detected those attacks at various and removed malfunctioning nodes from the network thereby preventing further attack from the malicious nodes.

4. RESULTS AND DISCUSSION

Graph in Fig 4 shows the number of successful Handover Authentication with group manager and without using group manager scheme. It is evident that with the introduction of Group Manager, the number of successful authentication for a mobile nodes increases gradually. Since group of requests are aggregated and send to Base Station for authentication, the network bandwidth is utilized efficiently in the given thereby increasing the probability of successful authentication.

Fig.3. Final Group Manager and data transmission

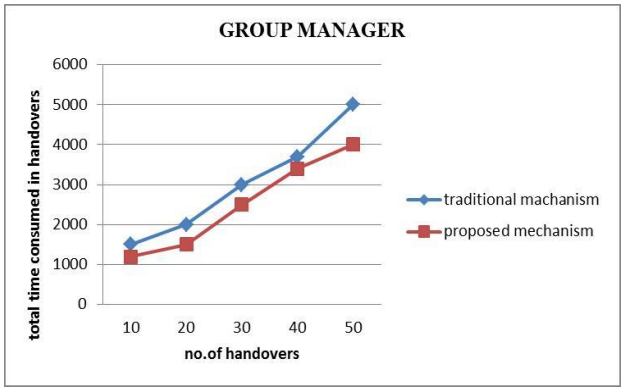

Chart -1:No. of HO authentication with GM and without GM

Fig 5 shows the increment in throughout of an system using Group Manager and without Group Manager. From fig 4, it is evident that the number of successful handover authentication increases with the introduction of Group Manager Scheme. This in turn increases the throughput of system.

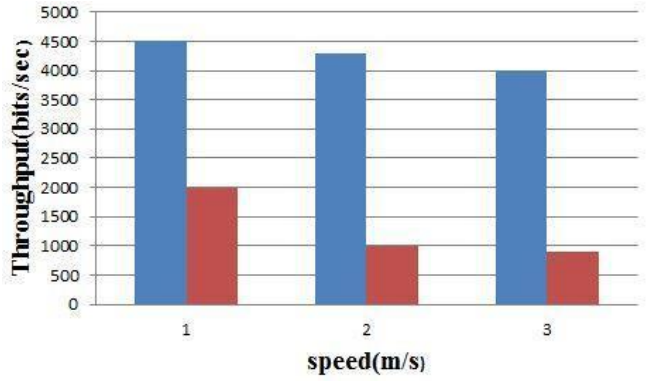

Chart-2: Throughput of an mobile network with and without Group Manager

Table 1 gives an overview of the comparison of handover solutions for group manager . Thereafter, the table will be clarified in the discussion, with an explanation of the choices made. In this scheme , high scaliblity is achieved , since if more number of requests are placed for an group manager, it can be shared between adjacent group nodes which falls inside the data transmission range of overloaded group manager. Thus, the failure of group manager is minimized as much as possible.

Table -1: overview of the comparison of handover solutions for group manager

	HO Latency	**Complexity**	**Dropped Pkt**	**Duration of Event**	**Scalability**
Without GM	High	High	High	Medium	Medium
With GM	Low	Medium	Low	Low	High

5. CONCLUSIONS

In this letter, we have proposed an efficient group-based handover authentication scheme for mobile WiMAX networks. The key idea of our scheme is that all the handover group members' security contexts are transmitted to the target BS through GM by aggregating the multiple requests. In order to overcome the vulnerability in the authentication process in handovers under the spoofing attacks and to improve the efficiency, SVM based intrusion detection system is used.

REFERENCES

[1] Daojing He, Jiajun Bu, Sammy Chan and Chun Chen, "Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks" IEEE Transactions On Computers, Vol. 62, No. 3,

March 2013

[2] Sze Ling Yeo, Wun-She Yap, Joseph K. Liu, and Matt Henricksen," Comments on "Analysis and Improvement of a Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions", IEEE Communications Letters, Vol. 17, No. 8, August 2013

[3] Thuy Ngoc Nguyen and Maode Ma "Enhanced EAP-Based Pre-Authentication for Fast and Secure Inter-ASN Handovers in Mobile WiMAX Networks," IEEE Transactions On Wireless Comm, Vol. 11, No. 6, June 2012

[4] Daojing He, Student Member, IEEE, Chun Chen, Member, IEEE, Sammy Chan, Member, IEEE, and Jiajun Bu, Member, IEEE, "Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions" IEEE Transactions On Wireless Communications, Vol. 11, No. 1, January 2012

[5] Daojing He, Chun Chen, Sammy Chan, and Jiajun Bu," Analysis and Improvement of a Secure and Efficient Handover Authentication for Wireless Networks" IEEE Communications Letters, Vol. 16, No. 8, August 2012

[6] Chia-Mu Yu, Yao-Tung Tsou,"Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks" IEEE Transactions On Information Forensics And Security, Vol. 8, No. 5, May 2013

[7] Jie Yang and Jerry Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks" IEEE Trans.On Parallel And Distributed Systems, Vol. 24, No. 1, January 2013

[8] Y. Chen, W. Trappe, and R.P. Martin, "Detecting and Localizing Wireless Spoofing Attacks," Proc. Ann. IEEE Comm. Soc. Conf.Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), May 2012.

[9] V. Franc and V. Hlava´c, "Multi-Class Support Vector Machine," Proc. Int'l Conf. Pattern Recognition (ICPR), vol. 16, pp. 236-239,2002.

[10] C. Hsu and C. Lin, "A Comparison of Methods for Multiclass Support Vector Machines," IEEE Trans.Networks, vol. 13, no. 2, pp. 415-425, Mar. 2002.

[11] N. Cristianini and J. Shawe-Taylor, An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods". Cambridge Univ. Press, 2000.

[12] F. Guo and T. Chiueh, "Sequence Number-Based MAC Address Spoof Detection", Proc. Eighth IntConf. Recent Adv in ID, pp. 309-329, 2006

[13] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," Proc. IEEE INFOCOM, Apr. 2008.

[14] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," Proc.IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS), 2005.