International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:6, 2015

Secured Session Based Profile Caching for E-Learning Systems Using WiMAX Networks

R. Chithra, B. Kalaavathi

***Abstract*—**E-Learning enables the users to learn at anywhere at any time. In E-Learning systems, authenticating the E-Learning user has security issues. The usage of appropriate communication networks for providing the internet connectivity for E-learning is another challenge. WiMAX networks provide Broadband Wireless Access through the Multicast Broadcast Service so these networks can be most suitable for E-Learning applications. The authentication of E-Learning user is vulnerable to session hijacking problems. The repeated authentication of users can be done to overcome these issues. In this paper, session based Profile Caching Authentication is proposed. In this scheme, the credentials of E-Learning users can be cached at authentication server during the initial authentication through the appropriate subscriber station. The proposed cache based authentication scheme performs fast authentication by using cached user profile. Thus, the proposed authentication protocol reduces the delay in repeated authentication to enhance the security in E-Learning.

***Keywords*—**Authentication, E-Learning, WiMAX, Security, Profile caching.

I. Introduction

WiMAX enables wireless broadband access with better quality of service. The broadcast multicast feature of WiMAX [1], [2] enables the E-Learning users to use to service of these networks. In WiMAX, the E-Learning users are connected to the WiMAX base station. The Access Service Network has a group of Base station. These base stations are controlled by the Access Service Network Gateway. The Connectivity Service Network consists of Authentication Authorization Accounting (AAA) server and it enables internet connectivity suitable for connecting with the E-Learning server for E-learning.

The Extensible Authentication protocol uses Privacy Key Management Protocol to carry over the authentication messages. In the initial ranging process, the subscriber station of E-learning user establishes Primary Management Connection with the base station. The Users must be authenticated by the AAA server. It uses the Privacy Key Management Protocol (PKM) for the secure distribution of authentication key (AK) between the communication network and the E-Learning user.

The authentication protocols such as PKM v1 and PKM v2 is used for authenticating the users in WiMAX. The message exchange using PKM v1 and PKM v2 protocol [3] in WiMAX is susceptible to attacks such as Rouge base station attack, Man in the Middle attack, Replay attack, Denial of Service attack [8]. The Extensible Authentication Protocol using PKMv2 for E-Learning is susceptible to security issues [6], [7].

The open source E-Learning system such as MOODLE is insecure in session management, authentication, and confidentiality. This leads to security problems such as Session hijacking, Man in the Middle attack. In Session Hijacking, a malicious user after acquiring the user login credentials can use the services of the user using another browser in the same system or in different system. To ensure security in E-Learning, the users of WiMAX based E-Learning system are requested to perform repeated authentication. The Secured Session Based Authentication protocol [9] overcomes the security issues in authentication; this protocol requires full authentication procedure to be followed during each repeated authentication process to overcome the session hijacking problem. Using this protocol each user has to request for authentication by forwarding authentication messages during each re-authentication process.

The proposed scheme overcomes security issues in E-Learning with reduced delay using profile caching at the authentication server. In this scheme, the user profile credentials after the successful initial authentication are cached at AAA server to enable faster authentication. The following section represents the architecture of the proposed system.

II. Existing Authentication Protocols

A. Authentication Using PKM v1

The WiMAX base station accepts the subscriber station information and uses the Privacy Key Management Protocol for authentication. The subscriber station uses X.509 digital certificates during initial communication with the Base Station (BS). In IEEE 802.16d, the base station authenticates the subscriber station using the Privacy Key Management Protocol (PKM v1) [4]. The message exchange in PKM v1 is represented as:

- Message1: SS → BS:Cert(SS.Manufacturer)
- Message2:SS → BS:Cert(SS) | Capabilities | BCID
- Message3:BS → SS:KU_{ss}(AK) | SeqNo | Lifetime | SAIDList

where Cert(SS, Manufacturer) is the X.509 certificate of SS's manufacturer, and Cert(SS) is Subscriber Station's X.509

R.Chithra, Assistant Professor is with the Information Technology Department, KS Rangasamy College of Technology, Namakkal, Tamil Nadu, India (e-mail: chithra@ksrct.ac.in).

Dr. B. Kalaavathi, Professor and Head, is with the Department of Computer Science and Engineering, KSR Institute for Engineering and Technology, Namakkal, Tamil Nadu, India.

certificate. BCID is the Basic Connection Identifier of Subscriber Station. KU_{ss} (AK) is the Authentication Key Encrypted with public key of subscriber station. SeqNo is the sequence number of Authentication Key and Lifetime specifies the life time of the Authentication Key. SAID List is the list of security association for which the subscriber station is to be authenticated.

In the message 2, any node can intercept message from subscriber station and this message is replayed to Base Station. This type of attack is known as replay attack. The replay attack may result in making the Base Station denying the service to subscriber station known as Denial of Service attack. In the message 3, the information about the base station is not available so any node can pretend as base station and forwards message to subscriber station resulting in Rogue Base Station Attack. So the message 2 and message 3 of the PKM v1 protocol is vulnerable to security problems. This protocol must be improved for E-Learning applications.

B. Authentication Using PKM v2

Mobile WiMAX (IEEE 802.16e) uses the PKM v2 protocol. Even though this protocol is an improved version of PKM v1 [4], [5] this is also susceptible to security problems such as replay attack, interleaving attack. The rouge base station attack in PKM v1 is overcome in PKM v2 where the certificate of base station along with its signature is transmitted in the message. However, the message from the base station may be intercepted by the malicious node and replay it to the subscriber station for gathering the information about the subscriber station which results in replay attack and interleaving attack. Therefore, the PKM v2 is insecure in providing authentication.

The message exchange in PKM v2 is represented as:

- Message1:SS → BS:Cert(SS.Manufacturer)
- Message2:SS → BS:NS|Cert(SS)|Capabilities| BCID
- Message3:BS → SS:NS|NB|KUSS(preAK,SSID) |Lifetime|SeqNo|SAIDList|AAID|Cert(BS)|SIGBS
- Message4:SS → BS: NB|SSAddr|AK(NB | SSAddr)

When PKM v2 protocol is used for authentication, the base station may deny the access to E-learning users. So improvement in PKM v2 is needed to overcome the security problems.

C. Session Based Authentication Protocol

The Session based Authentication Protocol uses the user credential along with session information is utilized during authentication of the users. The message exchange during the initial authentication of the user is represented as:

- Message1:E_{SS} → BS:Ns| MAC_Es
- Message2:E_{SS} → BS: U_ID|SS_D|Ts $\oplus$ N_S |Cert(E_{SS})| Capabilities| BCID
- Message3:BS → E_{SS}:Ts $\oplus$ N_B|KU_{SS}(AK, SSID)|PMK| Lifetime| SeqNo| SAIDList| AAID

The initial message named message 1 contains the nonce, MAC address of the Subscriber Station and it is then forwarded to the base station. Once the device is recognized, then the information about the E-Learning users is forwarded to the base station in the successive message with user identity, type of the service needed, and duration of the session. This message is then forwarded to the authentication server through the ASN gateway. In order to provide the mutual authentication between the user and the authentication entity, the nonce and the timestamp in the message are coded. Thus if the user and the base station knows either the nonce or the timestamp the other entity can verify that the message is from the legitimate entity. Thus, the proposed protocol ensures the security of the message and it is free from security attacks. On successful authentication the authentication key AK, along with its lifetime, Pairwise Master Session Key (PMSK) is exchanged and also stored in the subscriber and the base station.

III. Proposed System Architecture

The proposed WiMAX based E-Learning system consists of E-Learning user accessing the E-Learning Server through the Base Station (BS).The group of base stations are controlled by Access Service Network (ASN) Gateway. The ASN consists of collection of ASN gateway. The ASN provides the radio access, Multicast and Broadcast Control to users connected in the network. The Connectivity Service Network (CSN) consists of Home Agent, AAA proxy/servers, user databases. The Access Service Network is connected with the CSN. Before accessing the services of the E-Learning system, the users must be authenticated by the Authentication Authorization Accounting (AAA) Server.

During the initial authentication through the association request, the user credentials such as user name, nature of the service, MAC address of the subscriber station are forwarded to the Access Service Network Gateway using the Session based Profile Cache enabled Authentication Protocol. The CSN provides Remote Authentication Dial-In User Service (RADIUS) protocol. The RADIUS acts as a client / server protocol to enable the authentication server responsible for remote E-Learning users Authentication, Authorization and Accounting services by conveying message between ASN and CSN in WiMAX.

After successful initial authentication the attributes such as authentication key, Session key, Session duration, Session Identity are returned to E-Learning user. These attributes can be cached at the Authentication server along with the user name and password for the current session. The caching of credentials can carried out at the authentication server until the session expires.

To improve the security of the E-Learning system, the users of the system are requested to perform repeated authentication process at predetermined time period throughout the session. Thus, when the same user requests for re-authentication, the user credentials can be verified with cache and a new session key can be forwarded to the user without requiring additional delay during re-authentication. Fig. 1 represents the architecture of the proposed system.

During the repeated authentication process, the user session key and the authentication key are cached at the Authentication server along with the user profile are utilized to

verify the user identity. Thus, the subsequent authentication of E-Learning users is enabled at a rapid rate. The proposed cache enabled authentication scheme is presented in the following section.

Proposed Profile Cache Based Authentication Scheme

The AAA server performs the functions of authenticating the E-Learning users by verifying the identity of users. The server also supports the permitted services through the authorization. The time period through which the E-Learning user uses the service of the network is also accounted in the server. The accounting of user can be either user based or flow based. In user based accounting, the user accessing various services are accounted with a single record. In the flow based accounting, each user data record represents the data regarding the various flow of each user, so every user can have different accounting record.

The caching of E-Learning user information includes authentication Key, session ID and session duration represented by session life, Session key at the authentication server is carried out until the users session expires. The users requesting for re-authentication forwards the Session Identity, the authentication key, Session Key to authentication server along with user name, password, MAC address of the subscriber station. The authentication server verifies these attribute of the E-Learning user and allows the user to proceed the session with new session key. The new session key is replaced with the existing session key at the server. Thus, the caching of user keys at the authentication server helps the E-Learning users to perform repeated authentication with reduced delay.

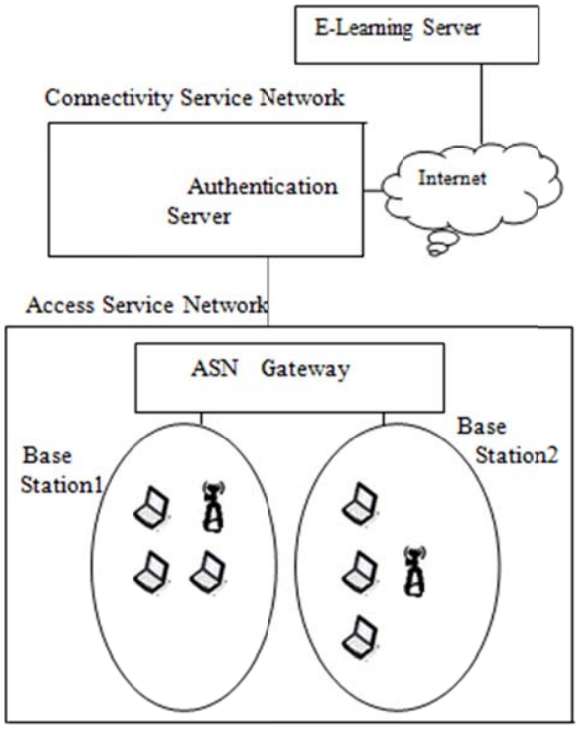

Fig. 1 Architecture of the Proposed E-Learning System

The proposed session based authentication scheme is represented in the following algorithm

Session Based Profile Cache Authentication Algorithm

Precondition: The initial authentication requests contains Timestamp Ts, Nonce Ns, MAC address, User name and password and the re-authentication requests contains Session Key(SK), Session Identity, Session duration (SK_{life}), Authentication Key (AuK).

Begin
1 For all users with association request
2 If initial authentication request from $user_i$
Verify user identity with Ts
3 If valid user
3.1 Generate and forward AuK, SK, TEK to $user_i$
3.2 Cache U_ID, Auk, SK, SID, SK_{life} at CSN
4. If not a valid user
Reject $user_i$ request
5 If association request from existing $user_i$
5.1 Compare U_ID, AuK, SK with the cache AuK, SK
6 If valid user
6.1 Generate SK_{new} and forward to $user_i$
6.2 Update SK_{new} in the cache
End If
End If
End

Initially before accessing the services of the E-Learning system, the identities of the E-Learning users must be verified. The users request for association with server by sending authentication request. The authentication server in CSN verifies the credentials of the user followed by caching and forwarding of the session key (SK), authentication key (AuK) to the user for using the E-Learning services. After the expiry of predetermined time, the same user is forced for re-authentication. The authentication server verifies the session key(SK) and the authentication key (AuK) in the re association request with cached credentials. The authentication server generates the SK_{new} using the attributes available in the association request. The E-Learning users provided with the new session key are now allowed to prolong the session. Thus caching of the E-Learning user keys at the CSN reduces the re-authentication time even when the same user is forced for re-authentication.

IV. Performance Evaluation

The proposed system is simulated using NS3 simulator. The simulation is performed by varying the number of base station used for E-Learning. The number of message exchanges during the re-authentication is considered to evaluate the performance of the system.

Let S(α) represent the communication cost for authentication, C(γ) represent the processing cost at the cache available at the authentication server and n represents the number of users logging for the current session. Then the cost of re-authentication (T) during each session is represented as:

$$T = \sum_{i=1}^{n} S(\alpha) + C(\gamma) \quad (1)$$

In (1), the number of users logging for the current session can be varied depending upon the nature of the service provided by the E-Learning system.

Fig. 2 represents the latency in authenticating the E-Leaning user. When the number of user request increases the latency of re-authentication is high in EAP based authentication. However, in the proposed cache based authentication the profiles of users requesting for re-authentication is compared with the profiles cached in the authentication server. When profile entries matches the user is re-authenticated by providing new session key SK_{new} to proceed with the existing session.

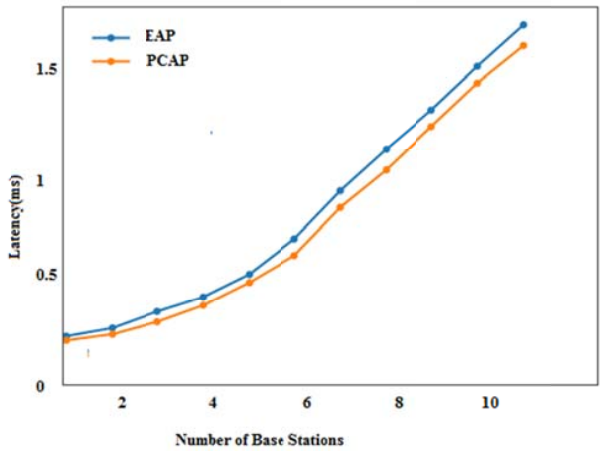

Fig. 2 Authentication Latency

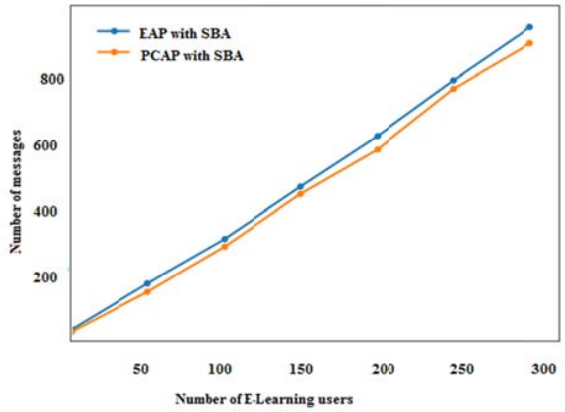

Fig. 3 Authentication Cost

Fig. 3 represents the number of message exchanges during the authentication process. It can be noted that even when the load on the system increases by increasing the number of user request for re-authentication, the proposed cache based re-authentication scheme does not degrade the performance of the system. However, the cost of caching the user profiles at the authentication server will affect the performance of the system. Based on the time needed to process the authentication request at the authentication server, the cost needed to authenticate an E-Learning user can be identified with (1). Even though same number of message exchanges is exchanged in the proposed scheme, the security in E-Learning during authentication is enhanced in the proposed protocol by performing re-authentication with reduced computation cost.

V. Conclusion

The Session Based Profile Caching Authentication Protocol for E-Learning application using the WiMAX networks is proposed in this research paper. The proposed protocol enhances the security in E-Learning without affecting the services of E-Learning server. Even though caching the user profile, the cache memory requirement is more the security in E-Learning system is enhanced with this protocol. The proposed protocol can be enhanced by minimizing the number of messages exchanges during each re-authentication process.

References

[1] IEEE 802.16 Working Group, "IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems," IEEE Standard 802.16-2004, October 2004.
[2] IEEE 802.16 Working Group, "IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands," IEEE Standard 802.16e-2005, February 2006.
[3] Noudjoud Kahya, Naara Ghoualmi, Pascal Lafourcade, Key Management Protocol in WiMAX Revisited, Springer, 2012.
[4] Fuden Tshering, Anjali Sharma, A Review of Privacy and Key Management Protocol in IEEE 802.16e, International Journal of Computer Applications, 2011.
[5] Perularaja Rengaraju, Chung-Horng Lung, Yi Qu, Anand Srinivasan, Analysis on Mobile WiMAX Security, IEEETIC-STH, Information Assurance in Security and Privacy, 2009.
[6] Felician Alecu, Paul Pocatilu, Sergiu Capisizu, WiMAX Security Issues in E- Learning System, Journal of Mobile Embedded and Distributed Systems,2010.
[7] Paul Pocatilu, Using WiMAX Technology for E-Learning Solutions, Economics of Knowledge, Vol.2 (3), 2010.
[8] R. Chithra, Dr. B. Kalaavathi, "Survey of Key Management Algorithms in WiMAX" International Journal of Mathematical, Computational, Natural and Physical Engineering, World Academy of Science, Engineering and Technology, Vol:8, No:9, 2014.
[9] Chithra Rajagopal and Kalaavathi Bhuvaneshwaran, "Secured Session Based Authentication Protocol for E-Learning using WiMAX networks", International Journal of Advancements in Computing Technology, 2015.