Improved Authentication Method for Wireless LAN to Prevent Various Security Attacks

[1]Udita Chudasama, [2]Gayatri S Pandi
[1]Student, [2]HOD PG Dept.
[1]M.E (IT),
[1]L.J Institute of Engineering and Technology,
Ahmedabad, India

Abstract : *Wireless Local Area Network (WLAN) is a system which is designed to connect networks. WLAN security is required as the signals do not have a physical boundary and they are prone to illegitimate access over a network which leads to the vulnerability of data. The security of the transmitted data over a wireless channel aims at protecting the data from unauthorized access so this can be done by providing advanced security mechanisms. Extensible Authentication Protocol (EAP) is a framework which is used in WLANs. The Existing EAP-based authentication protocols include EAP-MD5, EAP-TLS, LEAP and EAP-TTLS and so on. In LEAP, encrypted messages are all encrypted with 8-bit random numbers, which makes them vulnerable to dictionary attacks during data transmission. For the EAP-MD5 protocol, the user name and password are stored as MD5 values in the authentication server, when a new user is created. MD5 only perform one-way authentication and does not guarantee the authentication of the authentication server to the client STA. EAP-TLS (EAP Transport Level Security) is a certificate-based two-way authentication scheme. The attacker forwards the client's authentication information to the legal authentication system, and then forwards the message received from the legal authentication system to the client. Due to this, the transit data can be tampered or forged. To meet these issues, various authentication, encryption, invisibility, and other controlling techniques can be used in WLAN to avoid dictionary attack, replay attack, the man in the middle attack, spoofing and denial of service attack. Only the Authenticated Users should be able to exchange messages in the network. So network security should be achieved initially, by authenticating each and every user.*

Keywords – WLAN, Authentication, Kerberos, Security Attacks.

I. INTRODUCTION

Wireless LAN is much more flexible than wired LAN. As wireless LAN uses radio waves for sending information, data can easily tamper. It is necessary to authenticate users for giving access to resources in WLANs [2]. Wireless networks are inherently insecure. Although many security issues have been addressed, still wireless networks are not as secure as wired networks [1]. Wired networks send data between endpoints A and B, connected by a network cable. Wireless networks broadcast data in every direction to every device that might be listening, within a limited range. Because of the broadcast nature in wireless medium, the data is suspicious to many attacks like replay attack which occurs when an attacker gets information and saves old messages and then tries to resend them later, by pretending itself to be one of the participants [26], or IP spoofing attack in which the attacker sends a packet with the IP source address of a known host instead of its own IP source address to a target host. The target host might accept the packet and act upon it [27], or a MITM attack which occurs when a hacker gets itself inserted in between the communication of a Client and a Server [27], or denial-of-service attack, in which the attacker floods a system's resources so that it cannot respond to services that are requested [27]. The attacker will send too many bogus requests that are not necessary to be responded.

Fig.1 wireless lan architecture [8]

Figure 1 shows the architectural design of a wireless local area network which consists of a router and workstations.

The rest of this paper is organized as Section II with an introduction to the authentication protocol called Kerberos, Section III discusses the work done by different authors on authentication protocols, Section IV comprises of the proposed model and Section V shows the implementation part and Section VI gives the brief conclusion of the proposed scheme.

II. INTRODUCTION TO KERBEROS

Kerberos is an authentication service developed as a part of Project Athena at MIT [1, 11].In an open distributed environment users would like to have access over services which are distributed on servers in a network. In this scenario, the workstation cannot be trusted as the authorized user to authenticate services. Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users [1]. Authentication, Confidentiality, and Authorization are the main goal of Kerberos [3]. Kerberos assumes that each user is trusted but if any malicious user has access over the host that issues tickets for authentication (Key Distribution Centre) then the whole authentication system is at risk [9] [10]. The Kerberos was intended to have 3 components for guarding the network's gate [1]: Authentication, Association, and Audit. The last 2 components were not implemented [1].KERBEROS is designed for two purposes: 1. Security 2. Authentication. When a Client wants to access a Server with Kerberos, the Client must be verified through a trusted third party. This third party is the key distribution centre (KDC). KDC consists of 2 Servers, Authentication Server (AS) and Ticket Granting Server (TGS) [4].

Step 1 Client request to AS

Step 2 AS responds a TGT to Client

Step 3 Client send encrypted TGT and service request to TGS

Step 4 TGS sends token to Client

Step 5 Client sends token to File Server

Step 6 File Server decrypts the token

File Server verifies the Client and allows its resources to be used by the Client for a certain period of time according to the token. The token is like a movie ticket, with which a person can go to a theatre to enjoy a certain movie, at a certain time and on a certain day. After that time, which is specified in the ticket, the person cannot use it to watch the movie. Similarly, when the ticket time expires in the message, the whole authentication process will be repeated again. The expiration of the ticket should not be too short because it will affect the network efficiency and also it should not be too long because it can cause a replay attack.

III. RELATED WORK

This section introduces the related work that has been done by the researchers to have a secure communication. Some of the major protocols that are used have been listed as EAP-TLS, LEAP, PGP, EAP-MD5, and EAP-TTLS [7]. In [3] and [5] the author introduces an asymmetric key encryption method which uses public key encryption for data transmission and the receiver uses the corresponding private key for decryption. With unidirectional characteristics and high security, the encryption can avoid password guessing attacks caused by dictionary attacks as much as possible. Aiming at the problem that the request message from Client to the Authentication Server is vulnerable to replay attacks, the protocol uses a combination of the message sequence number and a random number to protect the message. Finally, the protocol introduces a mechanism that uses an irreversible Hash function to encrypt the final authentication result, thereby effectively solving the man-in-the-middle attack. In [9] [10] [12] and [14] there is a discussion on authentication as well as the non-repudiation problem. Authentication implies proof of origin and non-repudiation defines that the originator of the message cannot deny that the message was not originated by him/her. So to achieve this, the mechanism of PGP (Pretty Good Privacy) is introduced. The User uses a key to encrypt detail information and send it to PGP. PGP digitally sign the information and send to KDC. KDC grant a ticket and send it back to PGP. PGP again digitally sign the ticket and send it to User. User decrypts the ticket with his key and requests to access his desired service. In [13] the proposed method provides authentication, confidentiality, integrity, and privacy features to Cloud Service Providers and Cloud Users. In [16], [17] and [18] author identify that the existing scheme: does not provide anonymity of a user during authentication, user has no choice in choosing his password, vulnerable to insider attack, no provision for revocation of lost or stolen smart card, and does provide session key agreement. To remedy these security flaws, author proposed an enhanced authentication scheme, which covers all the identified weaknesses of Wang et al.'s scheme and is more secure and efficient for practical application environment. In [19] [20] and [21] the author proposed EAP method which satisfies the security requirements defined under RFC 4017. They take advantage of the nature of dynamic keys to eliminate the need for session keys and use optimal encryption algorithm AES-128-CBC for message encryption decryption before transmission through an insecure channel. In [15] and [22] the goal of each message in EAP-TLS handshake is to improve the contents of the message and the methods used to protect information. Asymmetric cryptography is faster than symmetric for transferring small sizes of data, like transferring a symmetric secret. The EAP-TLS supports both symmetric and asymmetric methods. The hash algorithm creates value of arbitrary data to a fixed value. Via small change in the message, the hash result is different, so the integrity is satisfied. In [23] the advantage of the nature of dynamic keys is mentioned, to eliminate the need for session keys and use optimal encryption algorithm AES-128-CBC for message encryption decryption before transmission through an insecure channel. In the registration phase, U and AS share credentials for future authentication. The entire registration phase is performed in offline mode. The dynamic key generators are selected such that they are unique. After the registration phase U authenticates with AS and vice versa. After the mutual authentication returns an EAP-Success message, then U can send messages through the authenticated channel. If he/she wants to reconnect, the authenticator checks with the AS whether the shared credentials exist for the particular user in its database. If it exists, then the particular user is forwarded to Authentication phase otherwise the user is directed to the Registration phase. User is able to accomplish the quick re-join authentication process with frequently visited APs. This phase is applicable when a mobile user gets disconnected from the current access point due to some interference and want to connect with the same AP (or Visited APs), then Users are not required to perform full authentication process again. The proposed scheme gives fast mutual authentication capabilities between client and server. So the quick re-join can be done if User gets disconnected. In paper [24]

author point out that Park et al.'s protocol is vulnerable to the dictionary attack upon identity privacy. We propose two schemes with mutual authentication, half-forward secrecy, and lower computation cost and less exchanged messages than Park et al.'s protocol and also identity privacy.

IV. PROPOSED MODEL

For authentication, some of the initial control messages are sent in between the communicating entities. Communicating entities are Client, Access Point (AP) and Key Distribution Centre (KDC) [25]. The initial request message should have the must require fields of the message to be set so that the server would proceed for further authentication only if it can serve the Client with its required service otherwise the request would be discarded and no control message transmission would be done further [25]. Figure 2 shows the authentication steps of proposed system.

Step 1: The client sends a request message to the AS.

Step 2: After receiving the request packet, the AS sends a Request to the Server, requesting the server to provide the flag information.

Times: Used by the client to request the following time settings in the ticket:

From: The desired start time for the requested ticket.

Till: The requested expiration time for the requested ticket.

Flag: It is the binary bit that is appended by AS to check whether the authentication steps should be completed or not.

Step 3: The server will set the flag to 1 if it is free for that particular time interval or flag will be set to 0 and sent it to the AS.

Step 4: AS returns a ticket-granting ticket, identifying information for the client, and a block encrypted using the encryption key based on the public key of the client. This block includes the session key to be used between the client and the TGS, times specified in step 3 and TGS identifying information. The ticket itself includes the session key, identifying information for the client and the requested time values.

Step 5: client decrypts the message with its own private key to obtain $SK_{C,TGS}$, and uses this key to encrypt the credentials of the client and this package is called Authenticator. The client returns a ticket TGT and Authenticator to TGS; after receiving the request from the client, the TGS decrypts the TGT to obtain the valid time of the $SK_{C,TGS}$, and TGT.

Step 6: The TGS verify the client and its information and send ticket T_V and A_C, encrypted using $K_{C,V}$ to the server (V).

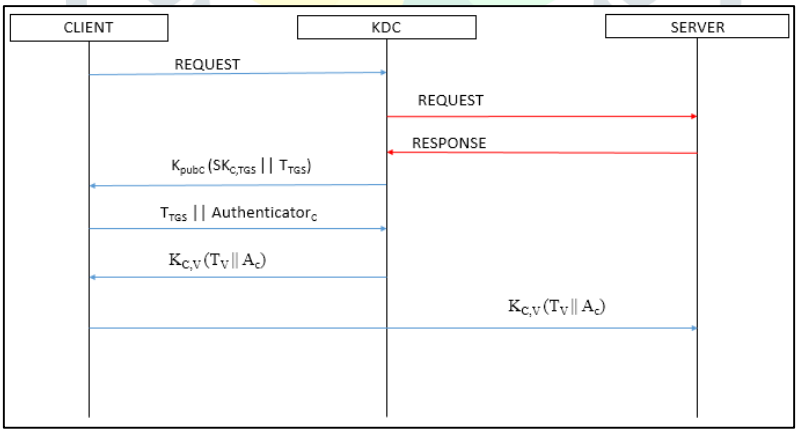
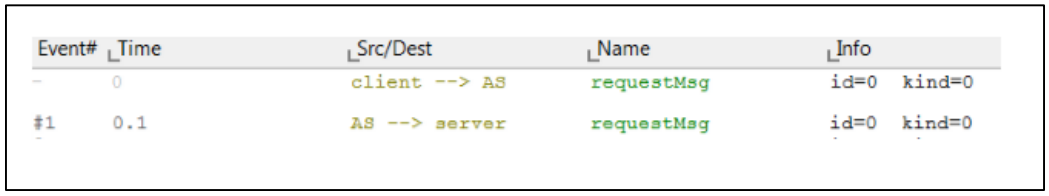


Fig.2 proposed model

The proposed method is used to have a more clear idea that whether the authentication process should be started for the requested server. The method is using Kerberos to authenticate the data on the authentication server and the ticket-granting server over the network. The control messages would be decreased and will only be transferred if the request can be fulfilled and help using a bandwidth constrained network.

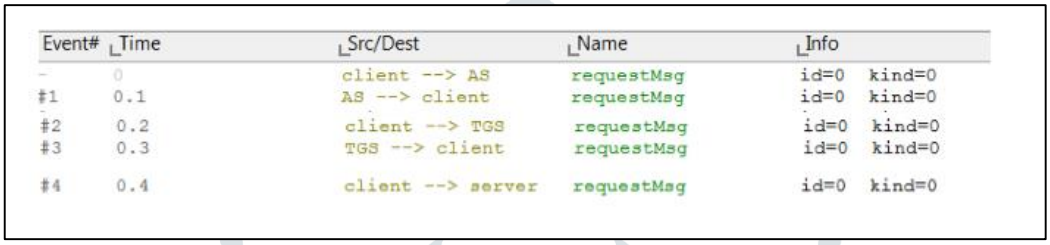
V. IMPLEMENTATION

The proposed system has been developed to check the feasibility of the authentication mechanism in WLAN to work faster than the traditional mechanism of authentication in WLAN. The hosts are dynamic in nature and they want the network to behave fast and respond fast. The control message transfers between client, KDC and server is done to authenticate the client to the server. Our system is simulated in Omnet++ environment to authenticate the client and allow it to access the resources from server. We have simulated the work on an ideal environment for the testing purpose. The code is written using the C++. The simulated experiment in figure 3 shows the number of control messages transferred between clients to server in traditional scenario does not change if the server is busy. The authentication steps will be carried out at first and then if the server is busy then it may not respond and maybe the client will again follow the authentication steps to get the access. The working of proposed method is much faster than the traditional approach only when the server is busy with another client in the network.



Event#	Time	Src/Dest	Name	Info
–	0	client --> AS	requestMsg	id=0 kind=0
#1	0.1	AS --> server	requestMsg	id=0 kind=0

Fig.3 proposed work scenario



Event#	Time	Src/Dest	Name	Info
–	0	client --> AS	requestMsg	id=0 kind=0
#1	0.1	AS --> client	requestMsg	id=0 kind=0
#2	0.2	client --> TGS	requestMsg	id=0 kind=0
#3	0.3	TGS --> client	requestMsg	id=0 kind=0
#4	0.4	client --> server	requestMsg	id=0 kind=0

Fig.4 traditional work scenario

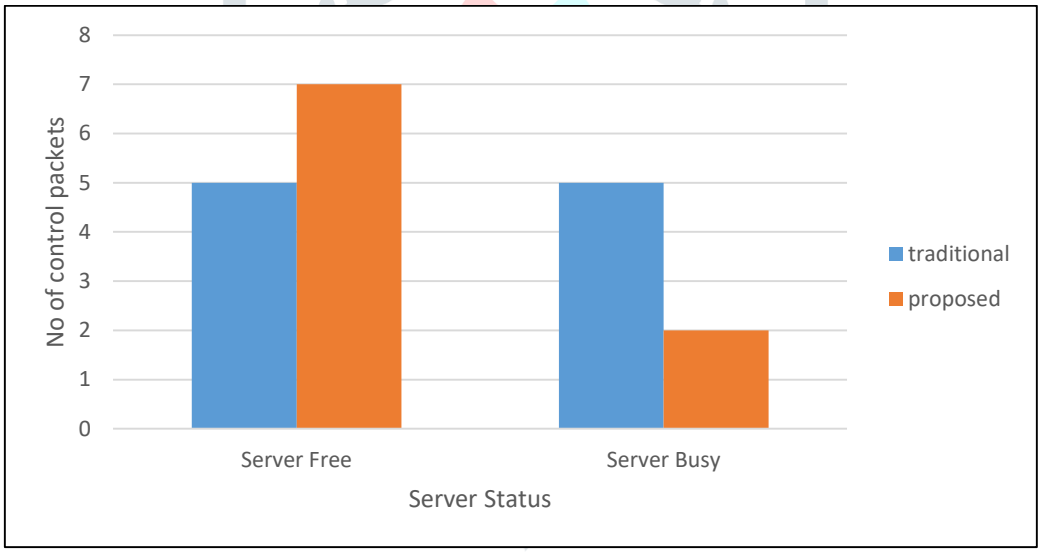


Fig.5 result analysis

In Figure 5, a graph is described having server status (ideal or busy) on X-axis and the number of control message transfer for authentication on Y-axis. The traditional approach has the same number of messages (5 messages) for whether the server is busy or not but the proposed method have little more control message (7 messages) transfer, when server is ideal and much less control messages (2 messages) transfer, when server is busy.

VI. CONCLUSION

The proposed technique try to ensure that the authentication steps may reduce the number of control message transfer. This proposed technique is providing the security to user identity. The main purpose of this technique is to decrease the amount of bandwidth utilization that happens due to control message transfer. The existing authentication method does not have fast reconnect and also have recursive authentication process for each and every service from the same server. And due to these, the control message transfer traffic is increased in a bandwidth constraint network. The computational cost of the messages that are being transferred should be reduced.

REFERENCES

[1] Cryptography and network security by William Stallings 6th Edition.
[2] Forouzan, B. A. (2010). TCP-IP PROTOCOL SUIT. (4th Ed.). New York, NY: McGraw-Hill.
[3] Yi Ma, Hongyun Ning "The Improvement of Wireless LAN Security Authentication Mechanism Based on Kerberos" 2018 International Conference on Electronics Technology pp. 392-397
[4] Jindal P, Singh B. Security-Performance Tradeoffs in a Class of Wireless Network Scenarios [M]. Plenum Press, 2017.
[5] Liu Y, Jin Z, Wang Y. Survey on Security Scheme and Attacking Methods of WPA/WPA2[C]// International Conference on Wireless Communications NETWORKING and Mobile Computing. IEEE, 2010:1-4.
[6] Xin Gong Wang. Research on the 802.1x Authentication Mechanism and Existing Defects[J]. Applied Mechanics and Materials, 2012, 1927(192).
[7] Shojaie B, Saberi I, Salleh M. Enhancing EAP-TLS authentication protocol for IEEE 802.11i [J]. Wireless Networks, 2017, 23(5):1-18.
[8] https://www.indiamart.com/proddetail/networking-amc-service-15281468055.html Accessed on 30/11/2018.
[9] Moin A. Khorajiya, Gardas Naresh Kumar "A Security based Architecture using Kerberos and PGP" ACM 2016.
[10] JithraAdikari "Efficient Non-Repudiation for Techno- Information Environment" First International Conference on Industrial and Information Systems, ICIIS 2006, 8 - 11 August 2006, Sri Lanka.
[11] MIT Kerberos Team, Kerberos: The Network Authentication Protocol DOI=http://web.mit.edu/kerberos/
[12] Neel N. Shah, Gardas Naresh Kumar, Jigar A. Raval., "Web-Based Framework for Data Confidentiality in Removable Media ensuring safe cyberspace" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 5, May 2015.
[13] Subhash Chandra Patel, Ravi Shankar Singh, Sumit Jaiswal.," Secure and Privacy Enhanced Authentication Framework for Cloud Computing" IEEE Sponsored Second International Conference on Electronics and CommunicationSystems (ICECS '2015).
[14] Bahareh Shojaie, Iman Saberi, Mazleena Salleh "Enhancing EAP-TLS authentication protocol for IEEE 802.11i" Springer 2016.
[15] Liao, Y.-P., & Wang, S.-S. (2009). A secure dynamic ID-based remote user authentication scheme for a multi-server environment. Computer Standards & Interfaces, 31(1), 24–29.
[16] Khan, M. K., Kim, S. K., & Alghathbar, K. S. (2011). Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'. Computer Communications, 34(3), 305–309.
[17] Narmadha, R., Malarkan, S., & Ramesh, C. (2011). Performance analysis of signaling cost on EAP-TLS authentication protocol based on cryptography. International Journal of Computer Applications, 33(7), 18–23.
[18] Saberi, I., Shojaie, B., & Salleh, M. (2011). Enhanced key expansion for AES-256 by using even-odd method. In 2nd international conference on research and innovation in information systems –2011 (ICRIIS'11) (pp. 5), IEEE, Kuala Lumpur.
[19] Biswanath Dey, SS Vishnu, Om Satyam Swarnkar "An efficient dynamic key based EAP authentication framework for future IEEE 802.1x Wireless LANs" 2018 Association for Computing Machinery.
[20] H. Hwang, G. Jung, K. Sohn, and S. Park, "A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using 802.1X and EAP," Proc. Int'l Conf. Information Systems Security, pp. 164-170, 2008.
[21] Amit Kumar, Dr. Hari Om "A Secure, Efficient and Lightweight User Authentication Scheme For Wireless LAN" IEEE 2016
[22] Y.M. Park and S.K. Park, "Two Factor Authenticated Key Exchange (TAKE) Protocol in Public wireless LANs," IEICE Trans. Comm., vol. E87-B, no. 5, pp. 1382-1385, 2004.
[23] E.J. Yoon and K.Y. Yoo, "An Optimized Two Factor Authenticated Key Exchange Protocol in PWLANs," Proc. Sixth Int'l Conf. Computational Science (ICCS '06), pp. 1000-1007, 2006.
[24] W.S. Juang and J.L. Wu, "Two Efficient Two-Factor Authenticated Key Exchange Protocols in Public Wireless LANs," Computers and Electrical Eng., vol. 35, no. 1, pp. 33-40, 2009.
[25] Udita Chudasama, Gayatri Jain "Review on possible attacks for authentication protocol" JASC journal, vol. V, issue XII, December 2018.
[26] Mohan V. Pawar, Anuradha J "Network Security and Types of Attacks in Network" science direct 2015 pp. 503 – 506
[27] https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/ 18/10/2018 12:38 pm