International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), Nov 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

STUDY OF AUTHENTICATION KEY AGREEMENT PROTOCOL FOR WIRELESS LANs: A-REVIEW

Navjot Sharma[1], Dr. Sandeep Kautish[2]

[1]Research Scholar, Deptt. Of CSE Professor, Guru Kashi University,Talwandi Sabo (India)

[2]Professor, Deptt. Of CSE Professor, Guru Kashi University,Talwandi Sabo (India)

ABSTRACT

A wireless network uses wireless mode of transmission and communication purposes. One of the major threats in a WLAN is its security. This paper gives the details description of a Authentication and Key agreement protocol to provide better security in a Wireless LAN. We have also described the working of this protocol along with its effects against various attacks encountered in a Wireless LAN. It has also been stated in this paper that this protocol provides enough security to handle these attacks and can further be enhanced to provide better security in other wireless networks.

I. INTRODUCTION

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes [1]. Wireless telecommunications networks are generally implemented and administered using radio communication [2]. Some wireless networks have a wired backbone with only the last hop being wireless. Examples are cellular voice and data networks and mobile IP. In others, all links are wireless. One example of such networks is multichip radio networks or ad hoc networks.

Now a days WLANs are being deployed in various installations e.g. homes, educational institutions, airports, military facilities, offices, buildings, coffee shops etc., due to their flexibility, cost-effectiveness, and ease of installation [6][7][8]. This has increased the potential attacks to both in form of active as well as passive attacks to home users, small businesses and the corporate world at different security levels.

Several protocols have been proposed and implemented for secure data transmission and robust mutual authentication for WLANs. Further there are many techniques used for authentication in trusted Wireless LANs where as in case of untrusted Wireless LANs is concerned a protocol named Secure Authenticated Key Agreement (SAKA) provides secure mutual authentication, key establishment and key confirmation over an untrusted network.

There are two kinds of key establishment protocols: Key transport protocols in which a key is created by one entity and securely transmitted to the second entity, and Key agreement protocols in which both parties contribute information which jointly establish the shared key. A key agreement protocol which provides implicit key authentication to both entities is called an authenticated key agreement protocol. A key agreement protocol which provides explicit key authentication to both entities is called an authenticated key agreement with key confirmation [9].

In this paper we shall be studying an efficient three-pass authenticated key establishment protocol that provides secure mutual authentication and key agreement with key confirmation. The SAKA (Secure Authenticated Key Agreement) is based on the challenge and response in the Secret-key setting [9].

This paper consists of 5 sections where Section 2 corresponds to the literature reviewed and section 3 will discuss the desirable properties for key agreement protocols. Section 4 shall be describing the working of SAKA and an analysis of the secure authentication and key agreement protocol shall me made and Section 5 shall be the conclusion and future scope of this study.

II. RELATED WORK

In the year 2007 a new and efficient secure authentication and key agreement (SAKA) protocol was proposed by Pierre E. ABI-CHAR et al, for providing robust authentication and security in untrusted Wireless LANs. It also resisted dictionary attacks mounted by either passive or active networks intruders.[10]

In the year 2013, New Authentication and Key Agreement Protocol for LTE-WLAN Interworking was proposed by Ahmed H.Hassanein et. al, for provide secure 3G-WLAN interworking in the SAE/LTE architecture, Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) is used and analyses vulnerabilities in LTE-WLAN interworking and proposes a new authentication and key agreement protocol based on EAP-AKA. [11]

In the year 2013, also a new Exploration of GSM and UMTS Security Architecture with Aka Protocol was proposed by Jyoti Kataria et. al, focuses on the architecture of GSM and UMTS along with Authentication and Key Agreement protocol description, which shows the encryption process used in the authentication. also gives an introduction to some concepts of UMTS security architecture.[12]

In the year 2014, a new Analysing secure key authentication and key agreement protocol for promising features of IP multimedia subsystem using IP multimedia server-client system was proposed by Bakkiam David Deebak et al, for providing Secure- Key Authentication and Key Agreement protocol (SK AKA) to meet out the standard demands of IMS. It also do Secure- Key Authentication and Key Agreement protocol (SK AKA) to meet out the standard demands of IMS.[13]

In the year 2015, one more a new and efficient secure Performance and security enhanced authentication and key agreement protocol for SAE/LTE network was proposed by Fikadu B.Degefa, et al, An improved approach without adding extra cost so that it can be implemented with in the same environment as the existing security system Evolved Packet System Authentication and Key agreement (AKA).[14]

In the year 2017, to solving large communication overhead issue and strengthening the securities of AKA protocols was proposed by Hung-Yu Chien, for providing Authentication and key agreement (AKA) is a challenge-response-like security protocol that uses symmetric-key cryptography to establish authenticated keys between 2 parties. UMTS-AKA and LTE-AKA. It also resisted drastically reduces the communication overhead and greatly strengthens the security robustness.[15]

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), Nov 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

III. DESIRABLE PROPERTIES FOR KEY AGREEMENT PROTOCOLS.

A number of desirable properties for key agreement protocol are identified on the basis of which most of the protocols can be analysed. They are as follows:

Known-key security: Each run of a key agreement protocol between two entities A and B should produce a unique shared secret key called session key Ks. A protocol should still achieve its goal in the face of an adversary who has learned some other session key.

Perfect forward secrecy: If long-term private keys of one or more entities are compromised, the secrecy of previous session keys established by honest entities is not affected.

Key-compromise impersonation: Suppose that A's long- term private key is disclosed. Clearly an adversary that knows this value can now impersonate A, since it is precisely this value that identifies A. However, it may be desirable that this loss does not enable an adversary to impersonate other entities to A.

Unknown key-share: Entity A cannot be coerced into sharing a key with entity B without A's knowledge, i.e., when A believes the key is shared with some entity C = B, and B (correctly) believes the key is shared with A.

Key control: No other entity should be able to force the session key to a preselected value. [8]

In addition to this the identification protocol must also possess the properties related to the performance which are as listed below:

Computational efficiency: this includes the number of operations required to execute a protocol. In order to achieve this property, the protocol should have the minimum number of operation as possible.

Communication efficiency: This includes the number of passes (message exchanges) and the bandwidth required (total number of bits transmitted).

IV. THE WORKING & ANALYSIS OF SECURE AKA

In actual, a key agreement protocol involves two or more parties or persons for communication. Each person or a party is meant for sending and receiving the signals as well as data, each run of a protocol is call a session, each step within a session will be termed as flow.

4.1 Description of the protocol

Authentication and key agreement protocol consists of three flows, defined as follow:

Within the first flow, Bob chooses a random challenge ub,

where $1 \leq ab \leq n - 1$, then he computes:

$$bb = \alpha^{ub} + b_s \qquad (1)$$

and finally he sends b_b to Alice.

Within the second flow, Alice chooses a random challenge u_a,

where $1 \leq ua \leq n - 1$, then Alice computes: (2)

$$ba = \alpha^{ua} \qquad (3)$$

computes b_s and computes K, where

$$K = [b_b - b_s]^{ua} \qquad (4)$$

Also Alice computes K_h where

$$K_h = MAC_K(b_s||K) \quad (5)$$

and computes:

$$Y1 = MAC_{Kh}(ID(Alice)||bb||ba) \quad (6)$$

Finally he sends Y1 and b_a to Bob.

Within the third flow, Bob computes:

$$K = [b_a]^{u}{}_{b} = \alpha^{u}{}_{a}{}^{u}{}_{b} \quad (7)$$

and Bob computes K_h where

$$K_h = MAC_K(b_s||K) \quad (8)$$

Also Bob computes:

$$Y' 1 = MAC_{Kh}(ID(Alice)||b_b||_{ba}) \quad (9)$$

Bob can then verify the value of Y ′ 1 by checking that (Y ′ 1 == Y1) If so, Bob authenticates Alice. Furthermore, if Y ′ 1 and Y1 are equal, Bob can be confirmed that Alice has actually established the same shared K_h with him because the value of K_h used in MAC is derived from the shared key K. Then Bob computes:

$$Y2 = MAC_{Kh}(ID(Bob)||b_a) \quad (10)$$

and finally he sends Y2 to Alice.

In order to authenticate Bob, Alice will compute:

$$Y' 2 = MAC_{Kh}(ID(Bob)||b_a) \quad (11)$$

and then Alice will verify the value of Y2 by checking that (Y ′2 == Y2), if so, if they match, then Alice authenticates Bob and Alice can be confirmed that Bob has actually established the same shared K with her.

Finally, Alice and Bob agree on the common session key Ks where

$$K_s = MA_{CKh}(ID(Alice)||ID(Bob)||K) \quad (12)$$

Both sides will agree on the session Key Ks if all steps are executed correctly. Once the protocol run completes successfully, both parties may use Ks to encrypt subsequent session traffic in order to create a confidential communication channel.

4.2 Performance Analysis

Some attacks like man-n-the-middle attack, active attack and passive attack have been considered for the analysing the effect of the protocol on such attacks and the assumptions considered for the analysis are :

a) Shared Key: assumption is made that the secret key K_H is known only by Alice and Bob.

b) Random Challenges u_a and u_b: we assume that Alice and Bob both have perfect random number generators which they used to determine their challenges. Therefore, there is only a very small probability that the same challenge occurs by chance in two different sessions.

c) MAC Security: we assume that the message authentication code is very secure. Therefore, the probability that Oscar, the adversary, can correctly compute MACk is almost negligible.

The protocol will ensure the security of the network if it satisfies the following properties.

Man in the middle attack (or active attack): Suppose that an attacker, Oscar, intercepts α^{ub} and replaces it with α^{ub1}, Oscar then receives Y1 and α^{ua} from Alice. He would like to replace α^{ua} with α^{ua2}, as before. However, this means that he must also replace Y_1 by Y_o where Y_o $MAC_{Kh}(ID(Alice)||b_b||\alpha^{ua2})$, but unfortunately for Oscar, he

can not compute the MAC_{Kh} on the string Yo because he does not know the MAC algorithm that it is used neither the value of K, K_H and Kh. Oscar cannot computes the value of K because he does not know the value of b_s, so he will not be able to compute K_h. Therefore the SAKA (v1 or v2) protocol thwarts the man in-the-middle attack.

Passive attack: Suppose that Oscar the attacker performa passive attack, then the session will terminate with both parties accepting. That is, Bob and Alice successfully identify themselves to each other, and they both compute the session key. So, Oscar, the adversary, cannot compute any information about the common shared session key Ks by assuming the intractability of the Decision Diffie-Hellman problem and by assuming that the MAC is very secure. In addition, to the fact that the key K_h used by MAC is a combination of K_H and K. Therefore the SAKA (v1 orv2) protocol resists against the passive attack.

Known-key attack: In this attack, an adversary will capture the session key from an eavesdropped session. In our proposed protocol, (v1 or v2), the client and the server both generates new α^{ua} and α^{ub} every new session and in addition the key K_h is generated with every new session also. Thus SAKA (v1 or v2) protocol is secure against known key attacks assuming that the Decision Diffie-Hellman problem is intractable.

V. CONCLUSION AND FUTURE SCOPE

In this paper we have reviewed the authentication and key agreement protocol for Wireless LANs. The working of the protocol along with its description is clearly stated. SAKA being a secure key agreement protocol still have some flaws, more importantly the major limitation of this protocol is that its computation cost as well as its communication cost in terms of rounds can further be reduced. Apart from this, the described protocol can also be enhanced for providing better security in WLANs, which shall also be the future scope of this review article.

REFERENCES

[1.] "*A New Clustering Algorithm for Wireless Sensor Networks"* (PDF).

[2.] *"Getting to Know Wireless Networks and Technology"*. informit.com. Retrieved 16 September 2016.

[3.] "*What you will want next and the really smart house*," Newsweek, May 30, 1999.

[4.] S. Ramanathan and M. Steenstrup, "A *survey of routing techniques for mobile communication networks*," Mobile Networks and Appl., vol. 1, no. 2, pp. 89–104, 1996.

[5.] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standard 802.11–1997, IEEE Computer Society LAN MAN Standards Committee, Ed., 1997.

[6.] Fayssal S., Salim H., and Youssif A.-N., "*Anomaly-Based Behaviour Analysis of Wireless Network Security*", In *Proc. of* Mobile and Ubiquitous System: Networking and Services, (Philadelphia, PA), pp. 1–8, 2007.

[7.] Laeeq K., "*Security Challenges & Preventions in Wireless Communications*", IJSER, vol. 2, issue 5, pp. 1–8, 2011.

[8.] Sagiraju P. K., Gali P., Akopian D., and Raju G. V. S., "*Enhancing Security in Wireless Networks Using Positioning Techniques*", In *Proc. of* IEEE-SoSE'07 (San Antonio, Texas, USA), pp. 07–15, 2007.

[9.] A. Menezes, P. Oorschot, and S. Vanstone, "*Handbook of Apllied Cryptography*", CRC Press, 2nd edition, 1996.

[10.] Pierre E. ABI-CHAR, Abdallah MHAMED, "*A Secure Authenticated Key Agreement Protocol For Wireless Security*", pp. 01-06, 2007.

[11.] A.Hassanein, A. Hafez, "*New Authentication and Key Agreement Protocol for LTE-WLAN Interworking*", pp.01-05, 2013.

[12.] J. Kataria, Dr. A. Bansal**, "***Exploration of GSMand UMTSSecurity Architecture with Aka Protocol*", pp.01-03, 2013.

[13.] B. David & R. Muthaiah, "*Analyzing secure key authentication and key agreement protocol for promising features of IP multimedia subsystem using IP multimedia server-client systems",* pp. 01-33, 2014

[14.] Fikadu B. Degefa, Donghoon Lee, Jiye Kim, "*Performance and security enhanced authentication and key agreement protocol for SAE/LTE network*", pp.01-19,2015.

[15.] Hung-Yu Chien, "*An effective approach to solving large communication overhead issue and strengthening the securities of AKA protocols*", pp.01-12, 2017.

[16.] Abdrabou MA, Elbayoumy ADE, EI-Wanis EA, "*LTE authentication protocol (EPS-AKA) weaknesses solution*", 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS'15), 12-14 Dec.

[17.] Aminmoghadam E, Mirghadri A., "*A forward secure PKI-based UMTS-AKA with tunneling authentication*". 2015 Third International Conference on Digital Information, Networking, and Wireless Communications (DINWC), 3-5 Feb. 2015.

[18.] Mun,K.Han,K.Kim,3GWLAN Interworking security analysis and new authentication and key agreement based on EAP-AK, in Proceedings of Wireless Telecommunications Symposium(WTS), 2009, pp.1–8.