Fast Initial Authentication and Secure Wireless Local Area Network Protocol

Komalpreet Kaur[1], Gurmeet Kaur[2]

[1]*Department of Electronics and Communication Engineering, Punjabi University, Patiala, India*

[2]*Department of Electronics and Communication Engineering, Punjabi University, Patiala, India*

[1]shining4ever12@gmail.com

[2]farishta02@yahoo.co.in

***Abstract*- Speed of the connection establishment and communication in wireless local area networks is a very important aspect to be considered along with achieving faster authentication of the communicating nodes to make the overall system efficient. While few standards developed by IEEE were easy to implement and had minimum hardware and software requirements but did not provide much desired security, others provided a secure environment to carry out the data transmission but took ample time to provide initial authentication services. In this paper a new method, FALAN-AKA, i.e. fast wireless local area network authentication and key agreement has been proposed which provides minimal delay in the initial authentication and provides the security of data by encrypting it.**

***Keywords*- Wireless local area network, fast initial authentication, advanced encryption standard.**

I. INTRODUCTION

With an increase in the desire of using latest technologies and internet facilities, there has been seen a trend in shifting from wired to wireless connections. In this light, wireless local area network has gained much popularity due to the convenience and flexibility with which it can be used [1]. Since data transmission in wireless networks takes place through the air so it is susceptible to various external threats and intrusions by various attackers [2]. Thus carrying out secure data transfer and simultaneously achieving the fast authentication of users has become an important task. Various IEEE standards have evolved along with security and authentication protocols to carry out safe and fast transmission of data in a wireless network but each with its own limitations of being hacked or interrupted due to simultaneous developments in sophisticated attacking techniques [3]. In this work, a new method i.e. FALAN-AKA has been proposed which provides less delay in initial authentication of the user compared to the present delay provided by FLAP and also ensures secure transmission of the data by suitably encrypting it using AES. The proposed strategy has been statistically analyzed to validate its performance and the work has been taken to the next step by comparing the values with FLAP and computing its efficiency over FLAP in terms of the resource usage [4]. The methodology of the proposed method is provided in section II and the results are given in section III. Finally, the conclusion and the future scope has been discussed in the section IV.

II. METHODOLOGY OF FALAN-AKA

The proposed model has been offered to protect the voice data and user data in the wireless network and environments. The key scheme has been designed to be used on the point-to-point architecture using the centralized base transceiver station (AP) node. The access point ensures its security by using the authentication scheme between the wireless nodes and access point. The design of the proposed solution has been prepared to mitigate the threats from the wireless WLAN network. The security of the pre-setup and post-setup phases has been covered under this system design by using the amalgamation of the cryptography methods along with the random generator key table production. The multi-column key pairing is utilized to scramble the key data up to the highly secure manner. The Advanced Encryption Standard (AES) has been utilized for the purpose of cryptography of the key data during transfers [5]. The major aim of this thesis is to protect the WLAN network against the passive attacks which includes replication, replay and session hijacking attacks, which are launched to snoop the information from the active data channel.

For authentication purpose, we are using a table with 5 columns and multiple rows in which the first 3 columns (i.e. a, b, c) are used for query key generation and the last 2 columns (i.e. d, e) are used for reply key building. For each row i.e. for the corresponding values of a, b and c variables, which are used in query key generation, system takes random values each time. Same is done for variables d and e.

Query key generation

$$\mathrm{Qk} = round\ (\log 10\ (sin\ (\mathrm{a}) * \cos(\mathrm{b}) * \tan(\mathrm{c})) * 887000 + (\mathrm{a} * \mathrm{b} * \mathrm{c}))$$

Reply key generation

$$\mathrm{Rk} = round\ (\log 10\ \left(\sin(d)\, , a\ tan2(d, e) * \frac{180}{\pi}\right) * 347100)$$

2.1 Main Key Generation Policy

Algorithm: Key Scheme Algorithm Sequence for Function Calling

CASE 1: When wireless node initiates the data transmission to access point:

1. Wireless node initializes the setup phase, and request access point to complete the call.
2. The access point initializes the authentication process.

CASE 2: When the wireless node initiates the data transmission to another wireless node:

1. The access point receives the setup call for the wireless node.
2. The access point requests the mobile station and verifies the ready state.
3. When wireless node replies with the ready state, access point initializes the authentication process.

Flow chart representation of the main algorithm has been shown in fig 2.1 and has been explained below it.

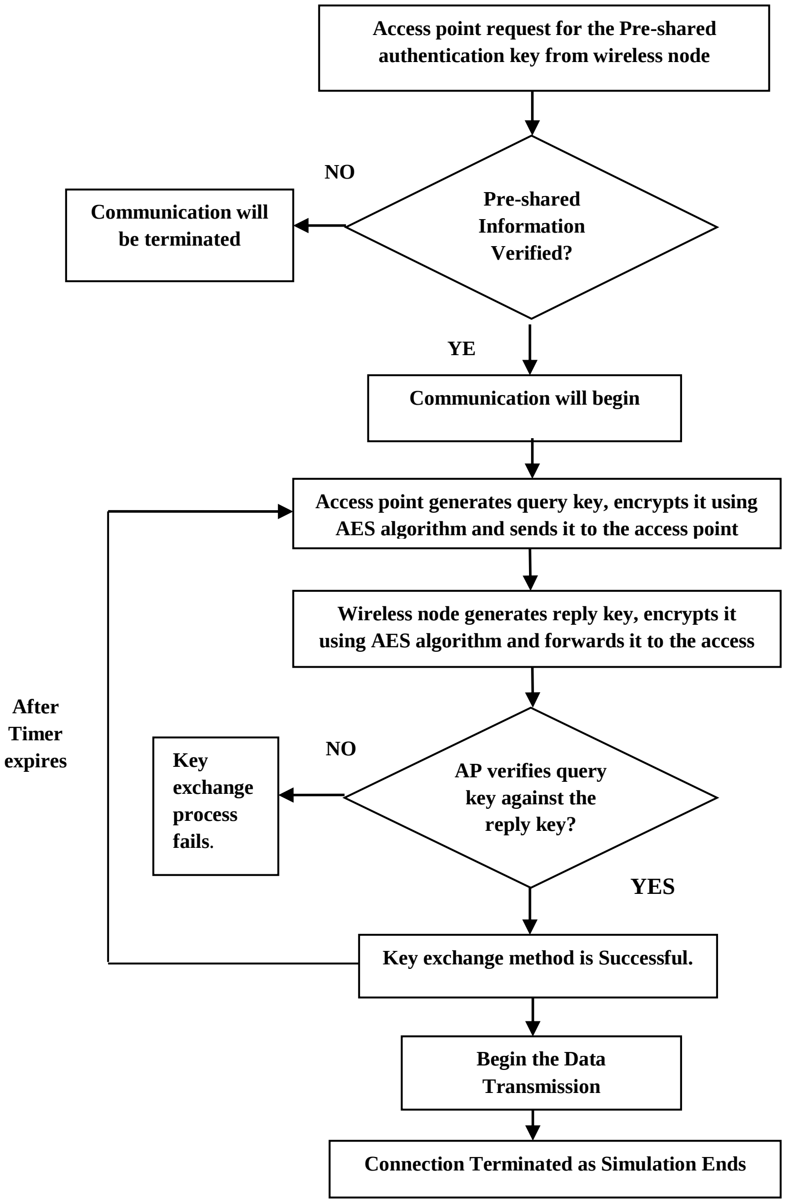
Access point request for the Pre-shared authentication key from wireless node
NO
Pre-shared Information Verified?
Communication will be terminated
YE
Communication will begin
Access point generates query key, encrypts it using AES algorithm and sends it to the access point
Wireless node generates reply key, encrypts it using AES algorithm and forwards it to the access
After Timer expires
NO
AP verifies query key against the reply key?
Key exchange process fails.
YES
Key exchange method is Successful.
Begin the Data Transmission
Connection Terminated as Simulation Ends

Fig. 2.1 Proposed key exchange based authentication scheme algorithm.

MAIN ALGORITHM:

1. The access point infuses the multi-column keys to prepare the query key.
2. The query key is encrypted using the AES algorithm.

3. The query key is forwarded to the mobile station.
4. The station prepares the reply key by verifying the query key column data and marks the reply key rows.
5. The reply key is prepared by infusing the multiple keys information in the marked columns.
6. The reply key is encrypted using the AES algorithm.
7. The reply key is forwarded towards the access point.
8. The access point verifies the query key against the reply and prepares the decision.
9. If the verification decision is successful.
10. The call setup is complete and call is forwarded to the target station.
11. Time counter (Tc) is initialized.
12. Else,
13. The call is dropped and the wireless node is informed about the authentication failure.
14. When the timer (Tc) expires, the exchange process is repeated.
15. If key verification is successful.
16. The channel stays intact.
17. Otherwise,
18. The call is terminated.

III. RESULTS AND DISCUSSION

Following assumptions have been made in obtaining the results:

- Transmission delay due to traffic jam is zero.
- Channel assignment is automatic.
- Local processing delay is also assumed to be zero.
- AP option: (Enable/ Disable)
- wireless nodes: (Enable/ Disable)
- Number of scenarios:2
- Number of nodes: 50, 100

MATLAB has been used to implement the proposed model. The performance parameters in terms of key generation time and authentication delay time have been evaluated as the primary analysis factors which elaborate the performance of the proposed scheme in the terms of fast speed and network performance. The projected resource usage parameter provides additional insight in to the network performance. The results obtained for all above stated parameters from the simulation of wireless network and AP are given below.

3.1 Scenario with 50 wireless nodes to the access points.

Key generation time: Lower value of key generation time indicates faster authentication of the node in the wireless network thus efficient communication setup.

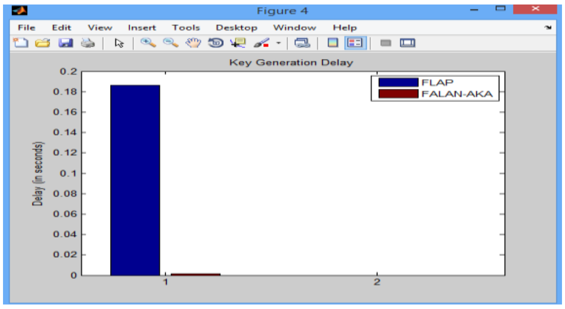

Figure 3.1 Key generation time.

Authentication delay: The authentication delay arises due to the time taken for the whole process of key generation, key transfer and key verification. Thus minimum the authentication time well is the working of whole WLAN system.

Projected resources: The high performance is indicated by the lower value of the projected resources computed from the simulation environment and higher value indicates the lower performance.

The comparison of the evaluated results has been performed over the results obtained from the existing and proposed models for 50 wireless nodes and is presented in tabular form as shown below.

. Table 3.1 Key Generation Time (in seconds) based comparison.

FLAP	0.1861
FALAN-AKA	0.0017

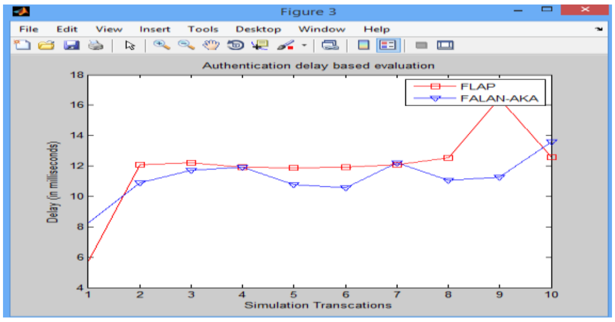

Figure 3.2 Authentication delay based graph.

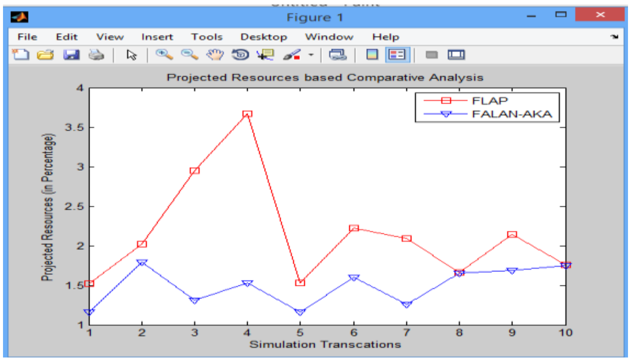

Figure 3.3 Projected resources usage.

Key generation time for FLAP was found to be higher than the proposed system FALAN-AKA with 0.1861 seconds taken compared to the 0.0017 seconds taken by the later system.

Table 3.2 Authentication delay (in seconds) based comparison.

Key Index	FLAP	FALAN-AKA
1	0.0058	0.0083
2	0.0121	0.0109
3	0.0122	0.0117
4	0.0119	0.0119
5	0.0119	0.0108
6	0.0119	0.0106
7	0.0121	0.0121
8	0.0125	0.0110
9	0.0164	0.0113
10	0.0126	0.0136

From the above table it is evident that out of 10 iterations, FALAN-AKA has performed better than FLAP for 8 iterations with less value of authentication delay in seconds, thus, indicating higher efficiency of the proposed protocol over the existing one.

The resource usage has been less for FALAN-AKA as compared to FLAP for 9 simulations out of 10, which were carried out. This lesser use of resources in percentage indicates the better efficiency of the proposed protocol over the given simulation scenario of wireless network.

The experiment was carried out for 100 nodes as well and results were recorded and compared for both the methods. The comparative analysis for both the scenarios i.e. with 50 and 100 nodes has been described in the tabular form for better understanding.

Table 3.3 Projected resources based comparison.

Key Index	FLAP	FALAN-AKA
1	1.5190	1.1602
2	2.0256	1.7969
3	2.9551	1.3086
4	3.6708	1.5273
5	1.5339	1.1641
6	2.2227	1.6016
7	2.0946	1.2617
8	1.6605	1.6563
9	2.1445	1.6914
10	1.7599	1.7500

Table 3.4 Key generation time (in sec.) based comparison between FLAP and FALAN-AKA.

Key Generation time	S1:N50		S2:N100	
Model	FLAP	FALAN-AKA	FLAP	FALAN-AKA
Time	0.1861	0.0017	0.1871	0.0019

As can be seen from the above table, when the number of nodes was increased to 100, FLAP took 0.1871 seconds, which was slightly higher than the scenario when only 50 nodes were taken. However, this time was more than the time taken by FALAN-AKA for same key table generation, which was 0.0019 seconds only. Thus our model achieves faster initial authentication.

Table 3.5 Authentication delay (in sec) based comparison between FLAP and FALAN-AKA.

Authentication delay	S1:N50		S2:N100	
Model	FLAP	FALAN-AKA	FLAP	FALAN-AKA
Average	0.0119	0.0112	0.0117	0.0096
Minimum	0.0058	0.0083	0.0050	0.0068
Maximum	0.0164	0.0136	0.0145	0.0124

From the above table, it can be seen that when the number of nodes was taken to be 50, the average time taken by FLAP was 0.0119 seconds while FALAN-AKA took only 0.0112 seconds for the initial authentication process, thus showing an improvement by 5.88%. When the number of nodes was increased to 100, FALAN-AKA performed better by showing an improvement of 17.94% as the average authentication delay taken by it was 0.0096 seconds as compared to 0.0117 seconds taken by FLAP. Thus the proposed technique is efficient than the existing one.

Table 3.6 Projected resources comparison between FLAP and FALAN-AKA.

Projected resources	S1:N50		S2:N100	
Model	FLAP	FALAN-AKA	FLAP	FALAN-AKA
Average	2.1587	1.4918	2.4352	1.6297
Minimum	1.5190	1.1602	1.4357	1.3516
Maximum	3.6708	1.7969	3.9065	1.9414

The utilization of the resources, measured in the form of projected resources has been recorded significantly lower than existing model. For scenario 1 i.e. when the number of nodes was taken to be 50, average resource usage by FLAP was 2.1587 percentage points while for FALAN-AKA, the value was 1.4918. When the number of nodes increased to 100, resource usage by respective models also increased but in that scenario too, FALAN-AKA had less value i.e. 1.6297 than that of FLAP which used 2.4352 percent of resources. Thus the lower resource utilization clearly indicates the robustness of the proposed model.

IV. CONCLUSION AND FUTURE SCOPE

The proposed model named FALAN-AKA has been compared against the existing model of FLAP over the standard WLAN simulation scenario with similar structure and environment. The proposed model of FALAN-AKA has been described efficient and effective while evaluated on the basis of the key generation time, authentication delay and projected resources. The better results of the proposed algorithm compared to the existing one suggest that it is efficient in the terms of the time taken for initial authentication process, which if less, can speed up the communication process.

FUTURE SCOPE

The appropriate future enhancement of the proposed model may lie in the following:

- Enhancement of the message level encryption for the insurance of the data security.
- The performance evaluation of the proposed model can be determined in the various aspects, scenarios and network platforms.

REFERENCES

[1] Yong Yu, Qun Wang and Yan Jiang, "Research on security of the WLAN campus network", In International Conference on E-Health, Digital Ecosystem and Technologies, vol. 3, pp. 175-178, 2010.

[2] Mohammad O. Pervaiz, Mihaela Cardei and Jie Wu, "Security in Wireless Local Area Network", Department of Computer Science and Engineering, Florida Atlantic University.

[3] LAN MAN Standards Committee of the IEEE Computer Society, "Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Standard 802.11, 1999, Edition 1999.

[4] Xinghua Li, Fenye Bao, Shuxin Li, and Jianfeng Ma, "FLAP: An Efficient WLAN Initial Access Authentication Protocol, IEEE Transactions on parallel and distributed systems, vol. 25, no. 2, February 2014.

[5] Joan Daernen and Vincent Rijrnen, " AES; Advanced Encryption Standard", Springer, 2001.

[6] Md Waliullah, ABM Moniruzzaman and Md. Sadekur Rahman, "An experimental study analysis of security attacks at IEEE 802.11 Wireless Local Area Network Network", International Journal of Future Generation Communication and Networking, vol. 8, no. 1, pp. 9-18, 2015.

[7] Saurabh Jha and Shabir Ali, "Mobile agent based architecture to prevent session hijacking attacks in IEEE 802.11 WLAN, " In 5th International Conference on Computer and Communication Technology, pp. 227-232, 2014.

[8] Vikas Kumar, Sandip Chakraborty, Ferdous A Barbhuiya and Sukumar Nandi, "Detection of stealth man-in-the-middle attack in wireless LAN, " In 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, vol. 8, no. 12, pp. 290-295, 2012.

[9] R.L. Martin, "The future of wireless applications", International Topical Symposium, pp. 3-4, 1995.

[10] Chander Dhawan, "Unique Applications and Opportunities in Wireless Computing in Developing Countries", International Conference on Personal Wireless Communications, vol. 4, pp. 297- 301, 1997.

[11] Anand R. Prasad, Neeli R. Prasad, AD Kamerman, Henri Moelard and Albert Eikelenboom, "Performance Evaluation, System Design and Network Deployment of IEEE 802.11", Wireless Personal Communications, vol. 19, pp. 57-79, 2001.

[12] Larry Korba, "Security system for wireless local area network", IEEE Computer Society, vol. 9, pp. 1550-1554.

[13] LAN MAN Standards Committee of the IEEE Computer Society, "Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Standard 802.11, 1999, Edition 1999, Revised 2003.