American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-03, Issue-08, pp-284-294
www.ajer.org

Research Paper Open Access

Fast and Secure Initial Access Authentication Protocol for Wireless LANs

Sandhya K[1], Nagaraju Rayapati[2]
[1](CSE, Sree Vidynakethan Engineering College, India)
[2](CSE, Sree Vidynakethan Engineering College, India)

ABSTRACT: *Nowadays there is widespread use of WLAN enabled devices, so it is equally important to have efficient initial link setup mechanism. In this paper a fast access authentication process is implemented which is faster than current 802.11i. Through experiments, it is observed that the inefficiency of 802.11i is due to its design from the framework perspective which introduces too many messages. Due to more number of round-trip messages in 802.11i authentication delay is intolerable under some scenarios. To overcome this, an efficient initial access authentication protocol FLAP is proposed which introduces two round-trip messages with authentications and key distribution. Proposed FLAP protocol scheme is more secure than 4-way handshake protocol. Simulations are conducted using different scenarios like Authentication delay, Throughput, Packet Delivery Ratio (PDR), Packet Drops are measured for different scenarios and compared between the 802.11i and FLAP protocol. The results show that the FLAP is more advantageous when WLAN gets crowded.*

Keywords - *WLAN, Authentication delay, 802.11i, Throughput, PDR, Packet drops*

I. INTRODUCTION

Wireless local area networks (WLAN) technology [1], [2] gaining its popularity continuously for its good mobility, high bandwidth, and important flexibility. The portable equipments that support WLAN increase greatly, such as smart phones, laptops, tablet computers, and so on. Users can easily access a variety of network applications through WLAN, for example, face book, twitter, e-mail, and online music and videos. However, security is a serious concern because the wireless medium is open for public access within a certain range.

The 802.11 Task Group proposed the Wired Equivalent Privacy (WEP) to provide secure data communications over wireless links. WEP used to encrypt the data stream and authenticate the wireless devices. However, significant deficiencies have been identified in both the encryption and the authentication mechanisms [3], [4]. To repair the problems in WEP, the Wi-Fi Alliance proposed an authentication mechanism based on EAP/802.1X/RADIUS[5], [6], [7] to replace the poor open system authentication and shared key authentication in WEP. The latest IEEE standard 802.11i [8] was ratified on June 24, 2004 as a solution to securing wireless links. The authentication process combines 802.1X authentication with key management procedures to generate a fresh pairwise key and/or group key, followed by data transmission sessions. Most of the security issues in the WLAN are solved by 802.11i.

However, with the rapid increase of the WLAN and its enabled mobile devices, new scenarios emerge that challenge the current WLAN standards, especially 802.11i. In a WLAN, every time the mobile device enters an Extended Service Set (ESS), it has to do an initial set-up to establish WLAN connectivity which generally includes the discovery and association of an Access Point (AP), along with 802.11i authentication and acquisition of an IP address. This works well when the number of new stations (STAs) in a given time period is small. However, when a large number of users simultaneously enter an ESS, an efficient mechanism that scales well is required to minimize the time STAs spend in the initial link setup, while maintaining a secure authentication. While the setup of the initial connectivity consumes a lot of time, consequently, mobile devices

cannot make fullest use of the WLAN and a lot of services are difficult to carry out, such as:
1. In rush hours, a large amount of passengers enter into a metro station or get off the train simultaneously, their WLAN-enabled terminals try to establish links with the WLAN to get network services.

2. Real-time services are offloaded from 3G to WLAN seamlessly. If the 3G and WLAN are not conducted by a same operator, the pre-authentication cannot be performed, and a fast initial authentication is required to establish a link with the WLAN efficiently.

3. Without a stop, a car or truck in the expressway can complete the payment or exchange the goods information through the WLAN when it passes by a toll station or a weighbridge station.

4. The express train provides network service to passengers through on-board APs, and in the backend the APs keeps the connection with the infrastructure networks along the trail through the beamed antenna using the 802.11.

5. When a user passes by a shop, his WLAN-enabled device can connect the WLAN of the shop and gets an electrical coupon without a stop; and the shop can identify the user and push the appropriate advertisements and electrical coupons.

6. An ambulance can upload vital patient information to the hospital, they are going to (or to any other specialists that need to be consulted) through the APs along the roadway while enroute.

7. All fleets attempt to keep track of all of their vehicles at all times. Widespread Wi-Fi hotspots along roads and throughout urban areas can be used by trucking fleets to quickly link to their home office to not only indicate where they are located, but at the same time to download necessary updates to the driver.

The IEEE 802.11ai is established to reduce the initial link setup establishment time. The IEEE 802.11i specified authentication process is a bulky time consuming for initial link setup. To explore the 802.11i authentication efficiency, numerous experiments are conducted and observed that 802.11i will become inefficient when WLAN is crowded. Time taken to perform DHCP and channel scan process will also make the initial link setup time even longer. Therefore, 802.11i cannot meet the requirements and it became an obstacle by preventing users from making use of WLAN.

The main reason leading to 802.11i inefficiency is due to its framework perspective which introduces too many messages between the terminals and network. Eleven round-trip messages are designed for EAP-TLS and practically it needs 13 round-trips due to fragmentation in the MAC layer.

To improve the efficiency, an efficient authentication method is implemented which introduces only two round-trip messages to make the authentications and key distributions between mobile Station (STA), Access Point (AP) and Authentication Server (AS). The contributions are as follows:

1. A fast WLAN initial access authentication method FLAP is proposed, and we formally prove that it is more secure than the four-way handshake protocol.

2. We implement FLAP and the measured authentication delay is just 5.3 percent of EAP-TLS. Based on the implementation, we ran thorough simulations with different background traffic and STA numbers. The results indicate that the advantage of our scheme is more salient than EAP-TLS in the crowded network environment. Furthermore, based on the experimental result, we get an authentication delay estimation method for EAP-TLS and FLAP. To the best of our knowledge, we are the first to investigate the authentication delay under different background traffic and STA numbers.

3. From the real-world implementation perspective, we give a simple and practical method which makes the proposal compatible with 802.11i.

Some performance metrics are calculated to measure the performance of a network. Network throughput shows the number of packets delivered per unit time in communication channel. Throughput is measured in bits/sec or bps. Authentication Delay specifies how long time it took to complete the authentication process. It gives ratio of sum of time taken to deliver packets for destination by number of packets received by destination. Packet delivery ratio is defined as the ratio of data packets received by the destinations to those packets sent by the sources. The greater value of packet delivery ratio means the better performance of the

protocol. Packet drops specify the number of packets dropped during the communication. It is measured as the difference of number of packets sent with number of packets received.

Section 2 presents 802.11i and its drawback analysis. Our scheme FLAP is given in Section 3. Section 4 presents some implementation considerations. Section5 shows the performance measures. Security provided by FLAP is given in Section 6 and the paper is concluded in Section 7.

II. 802.11I BACKGROUND

802.11i robust security network association (RSNA) [9] establishment procedure consists of 802.1X authentication and key management (AKM) protocols. Three entities are involved, called the Supplicant (the STA), the authenticator (the AP), and the AS (de facto a RADIUS [7] server).

Generally, a successful authentication means that the supplicant and the authenticator verify each other's identity and generate secret keys for subsequent key derivations. Based on this secret key, the key management protocols compute and distribute usable keys for data communication sessions. Assuming the link between the AS and the authenticator is physically secure, the AS can be implemented either through a separate server or as a single device with Authenticator. The complete handshakes of establishing an RSNA are shown in Fig. 1.

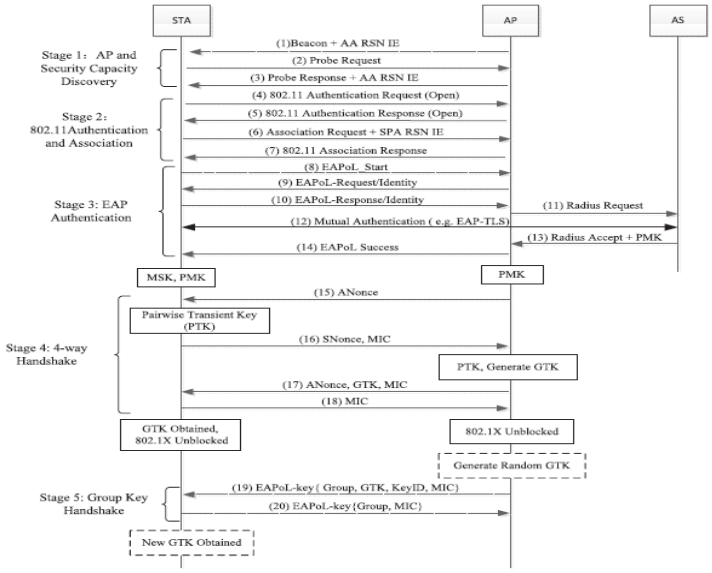

Figure 1: 802.11i 4-Way Handshake

2.1 Drawbacks of 802.11i

A test bed is established to explore the efficiency of 802.11i and EAP-TLS authentication delay is practically measured i.e., 50s, on average if there are 10 STA. Furthermore, we conducted thorough experiments with STA numbers and traffic. The results are shown from which it can be seen that with the average authentication delay of 30 new incoming STAs is 450s. We believe that if the network discovery and DHCP process are taken into account, the initial link setup time will get even longer; such inefficiency is intolerable for some applications.

Why is 802.11i so inefficient? From Fig. 1, it can be seen that 802.11i takes multiple round-trip messages to achieve the authentications and key distribution. The number of the message interactions varies for different authentication protocols used, for example, in the design, EAP-TLS has 11 round-trips (not including the scan process) and its implementation takes 13 round-trip messages because in MAC layer one of its messages is fragmented into three. While for each station of a WLAN, it has to compete each other for the wireless channel using the distributed coordinated function (DCF). If the WLAN is crowded, an STA will wait for a long time before it gets the channel to transmit a message. Large numbers of message interactions mean that a lot of time has to be spent to get the channel. As a result, AP cannot efficiently establish links with multiple users at the same time or the dwelling time is not enough to establish the initial link before an STA moves out the coverage of the AP.

The main reason leading to its inefficiency is that 802.11i is designed from the framework perspective which introduces too many extra messages. Rather than being a specific protocol, 802.11i is designed as a uniform framework where different authentication protocols can be incorporated. Compared with the design of a specific authentication protocol, devising a uniform framework will take more factors into consideration to make the framework more general and suitable for most scenarios. First, to achieve backward compatibility, the open system authentication is preserved. Yet, the two messages are useless for the initial link establishment. Second, the EAP authentication is employed; the advantage of which is that it is open and any two-party authentication protocol can be integrated and run within it. Furthermore, to keep the uniformity of the framework, EAP authentication and four-way handshake protocol have to be sequentially executed. That is, only after the EAP phase, can the four-way handshake protocol be performed to realize the mutual authentication between the STA and the AP. But in practice, to some degree the authentication between AP and STA can be performed in parallel with the one between the STA and the AS.

III. PROPOSED SCHEME

From the analysis, we get the goal and guideline for our scheme as follows:

Performance: The new scheme should greatly improve the performance of 802.11i.

Functionality: The least two round-trip messages are used to realize the authentication and key distribution between Station (STA), Access Point (AP), and Authentication Server (AS).

Orientation: The new scheme is just a complement instead of replacement of 802.11i and should be compatible with it.

Scope: Just a new initial access authentication is introduced which should not affect the subsequent procedure of the 802.11i.

Security: The security level of the new scheme is more than the current standard.

According to the drawback analyzed in 802.11i and the design goal outlined above, we get the design idea of new scheme as follows: A specific authentication protocol is designed with the least messages (two messages) which are used to realize the authentication between the STA and the AS, and the four-way handshake protocol messages are integrated rationally to realize the authentication between the STA and the AP.

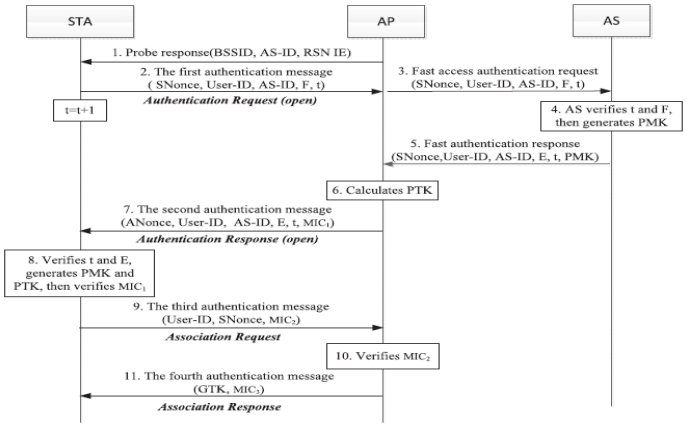

Figure 2: FLAP Scheme

3.1 Protocol Procedure

In the proposed scheme, each STA shares a key k with the AS, and it is also assumed that the link between the AS and the AP is secure. Our scheme is shown in Figure. 2 and its interaction procedure are as follows:

1. Through the proactive scan, the STA gets the WLAN information which includes the BSS identity, the security capacity of the networks and Authentication Server (AS) identity.

2. The first authentication message {SNonce, User-ID, AS-ID, F, t} is sent to the AP from the STA. Where SNonce is the random value generated by STA. User-ID is the user's identity, while AS-ID is the AS identity. And t is a counter; the STA increases its value by 1 once sending a message. Initial t value is 1. F=f (k, t||SNonce||User – ID||AS-ID), where f() is a hash function and || denotes the concatenation.

3. AP sends the fast access authentication request message {SNonce, User-ID, AS-ID, F, t} to the AS.

4. A counter is also set in the AS for each user and its initial value is also set as 1. Upon receiving the fast access authentication request message, the AS gets its current t value according to the User-ID and compares it with the received one. If the received t value is less than the current t value in the AS, the authentication of the STA fails and the current t value of the AS will keep unchanged. Otherwise, the AS will further verify F according to the received t and the key k. If correct, the authentication of the STA by the AS succeeds, and the AS increases the received t value by one and sets it as its current t value. Thereafter, AS computes Pair wise Master Key (PMK).

$$PMK= h (k, ``FLAP\ PMK''||t||User –ID||AS\text{-}ID)$$

Where h is a hash function and "FLAP PMK" is a constant string.

5. The AS sends the authentication response message {SNonce, User-ID, AS-ID, E, t, PMK} to AP. Where E = f(k, t||SNonce||AS-ID||User-ID).

6. After receiving the message 5, the AP generates its own random value ANonce and computes the PTK.

PTK = PRF-X (PMK, "Pairwise key expansion"|| Min (AA, SPA) || Max (AA, SPA) || Min (ANonce, SNonce) ||Max (ANonce, SNonce))

Where PRF-X is Pseudo random function. AA is MAC address of AP; SPA is MAC address of STA. "Pair wise key expansion" is a constant string. Min( ) means getting the minimum value; Max ( ) means getting the maximum value; the derivation of the PTK here is exactly same as that of 802.11i. If the AS coexists with the AP, there is no need of message interactions between the AS and the AP, and the related operations are performed by the AP.

7. The AP sends to STA the second authentication message {ANonce, User-ID, AS-ID, E, t, MIC1}, where MIC1 is the message authentication code computed on this message by the AP using the PTK, and t is the current value of the AS.

8. After receiving the message, the STA will compare the received t value with its current t value, and if equal the STA will validate E. If correct, the authentication of the AS will pass. Thereafter, the STA will compute the PMK and PTK, using the same method as that of the AS and AP. At the same time, the STA will verify the MIC1 taking use of the PTK. If valid, the STA authenticates the AP successfully.

9. The STA sends the third authentication message {User-ID, SNonce, MIC2}, where MIC2 is the message authentication code computed on this message by the STA using the PTK. Meanwhile, the STA also indicates that whether the group temporal key GTK is required or not. Furthermore, this message carries the necessary RSN IE parameters to complete the association.

10. After receiving the message, the AP verifies the MIC2. If correct, it means that the STA generates the same PTK and the AP authenticates the STA successfully. So far, the networks side completes the authentication of the STA, and the AP installs the derived PTK. In addition, the AP registers the STA in the distributed system to complete the association operation. If the MIC2 is verified invalid or in a given time the third authentication message is not received, the AP will delete the STA's authentication information and deauthenticate it. Meanwhile, the authentication failure message will be sent to the AS which will in turn delete the authentication information of the STA and rollback its t value.

11. The AP sends the STA the fourth authentication message {GTK, MIC3}, where the GTK is encrypted using the PTK. Upon receiving this message, the STA verifies the MIC3. If correct, the STA decrypts and gets the GTK and other related information. At the same time, the STA installs the PTK and GTK.

IV. IMPLEMENTATION

The proposed scheme does not intend to replace 802.11i; instead, it is oriented as a complement of the current standard for some special applications. Thus, a method has to be provided to enable the new scheme to be compatible and coexist with 802.11i. Before the standard 802.11i, when a user makes the initial authentication, he can choose the open system authentication or WEP. Referring to this method, we also provide the user two options, including 802.11i and the proposed scheme.

Specially, a new AKM Suite Selector [9] is added to the 802.11i AKM Suite List in the 802.11i RSN IE. The authentication request is extended and new authentication algorithm identification is added that is to add dot11AuthenticationAlgorithm [9] value denoted by "FLAP." In such a way, totally there are three optional values, including the existing "Open System" and "Shared Key". Meanwhile, a new IE is added which encapsulates the message field of the proposed scheme.

When the networks support the FLAP and the STA prefers to the new scheme, the STA will set the dot11AuthenticationAlgorithm as "FLAP" in the first authentication message, and add its corresponding information element into the frame body. After the AP receives the message, it will first check the dot11AuthenticationAlgorithm and if it is "Open System," it will reply with authentication response (Open). In such a way, WLAN will run 802.11i as usual. If "FLAP," then the AP will forward the message to the AS. To enable the radius server to understand the message, we can still use the EAP over- radius format to transmit the message. Consequently, the AP needs to perform the EAP encapsulation of the first authentication message received, specifically, to extract the information element and encapsulate it into EAP message. And then send the EAP message to the AS through the radius message. To enable the AS to recognize the protocol, the new scheme has to be implemented in the AS and a new value "FLAP-method" is added into the type field of the EAP message to identify the scheme, and the rest fields are put into the following type-data field correspondingly. After the AS receives the fast access authentication request, it will first check the type field in the EAP message, and if it is "FLAP-method" the AS will execute the new scheme.

To proceed as above, the STA has to first get to know whether the networks support the fast access authentication or not. In the scan phase, AP will broadcast whether the new scheme is applicable or not in the RSN IE. Only when both the AS and the AP support FLAP, can the AP claim the WLAN supports this method. To implement the proposed scheme, the AP has to be updated. From the implementation perspective, the reasons to adopt the four message interactions are as follows:

1) The message framework of authentication (open) and association are reused. Consequently, the new scheme just needs to modify the contents of the four messages instead of its framework.

2) The message contents of the four-way handshake are reused. The four messages between the STA and the AP in the proposed scheme are similar to the four-way handshake. Therefore, the implementation of the new scheme can be achieved through the appropriate modification of the contents of the four-way handshake. Thus, the new scheme is easy to implement.

3) The state machine of the STA in 802.11i can be maintained unchanged.

Its initial state is "State 1: Unauthenticated, Unassociated." After the successful mutual authentication with the AS, the STA enters into the "State 2: Authenticated, Unassociated." When the protocol completes successfully, the STA enters into "State 3: Authenticated, Associated." This accords with the specification of 802.11i.

V. PERFORMANCE ANALYSIS

5.1 Compatibility Analysis

From above section, it can be seen that the proposed scheme can be compatible with 802.11i. And the new scheme provides users another choice in addition to 802.11i. FLAP scheme will be executed only when both the STA and the network support the fast initial access authentication. If the new scheme is not supported on both sides, 802.11i can be used instead. In addition, our scheme is involved only in the initial access authentication and the resulting outputs are the PMK and PTK which are same as those of 802.11i, therefore, the subsequent procedure (e.g., the update of the PTK) of 802.11i will not be affected. In such a way, FLAP can achieve nearly full compatibility with the current standard.

5.2 Security Analysis

If the hash function f() and h() is secure, our scheme FLAP can achieve mutual authentications among the STA, AP and AS, and generates a secure key PTK. Furthermore, the FLAP is more secure than the four-way handshake protocol.

5.3 Performance Analysis

According to the implementation consideration, we implement the proposed scheme. A test bed is established whose topology is shown in Figure. 3.

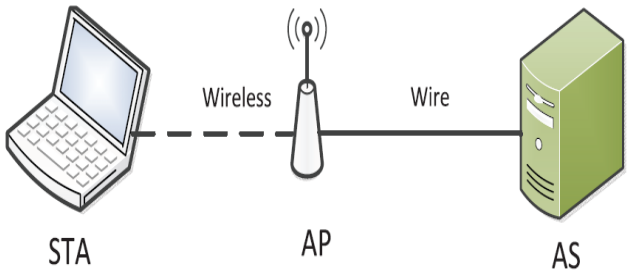

Figure 3: Test bed Topology

In this paper, simulation is done for the concept as the number of stations increases authentication delay increases, it consume lot of time in authentication process. And here along with the authentication delay some other parameters are also considered like throughput, packet delivery ratio and packet drops. These parameters are also equally important to say the protocol is efficient.

The authentication delay is made up of two components and they are process delay and communication delay. The former mainly consists of computation time, packet encapsulation and decapsulation time. The communication delay is the time spent to transmit messages over the wireless and the wire. In a WLAN, all the STAs have to compete with each other using CSMA/CA [1] to get the wireless channel, which costs considerable time. Comparing with the time spent in the wireless, the time in the wire is negligible because the bandwidth is very high and APs do not need to compete for the wire channel.

When a new STA is added (the original STA number is assumed to be n, and then now there are n + 1 STAs in total), for each of the original n STAs, its process time basically will not increase (we assume that the AS's computation capacity is enormous and it can handle authentications in parallel), while the communication delay gets longer because one more STA comes to compete for the channel with it. Consequently, for each of the original n STAs, the addition of one STA results in the increase of its communication delay. It is assumed that the average authentication delay is D when the STA number is n and the extra average communication delay resulting from one additional STA is delta, then for each of the original n STAs, the new average authentication delay is D þ delta. For the new incoming STA, its authentication delay also approximates to that of the rest n STAs. Therefore, the average authentication delay of the n + 1 STAs will also be D + delta.

We vary the number of new incoming STAs that concurrently authenticate with the WLAN from 1 to 40. We simulated 10, 20, 30 and 40 nodes. The authentication delay simulation result for 802.11i EAP-TLS and proposed protocol are as show below:

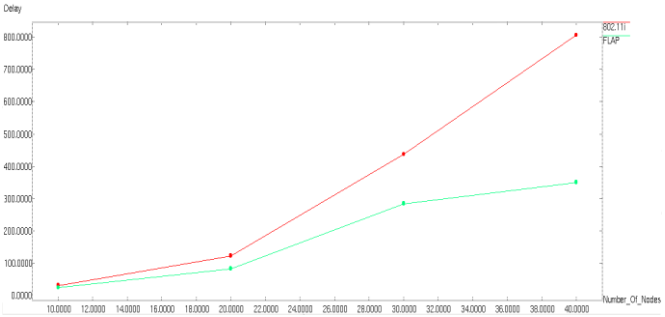

Figure 4: Authentication Delay simulation of 802.11i and FLAP

Furthermore, we notice that in Fig. 4, when the STA number is less than 10 the delay increases slowly, while the delay increases quickly (nearly linearly) when there are more than 10 STAs. This is because an additional STA does not affect the communication delay too much when the node number is small, but when the number gets large, the affect becomes considerable. This result accords with that of [11] which uses a Markov chain to analyze the WLAN performance. We found that when the STA number was greater than 10, the model was much closer to the practical situation. Based on the analysis model proposed in [11], [10] reaches the conclusion that WLAN access delay increases nearly linearly with the number of STAs.

Throughput is the number of packets/bytes received by source per unit time. It is an important metric for analysing network protocols. The throughput comparison between EAP-TLS and FLAP schemes are shown in below figure:

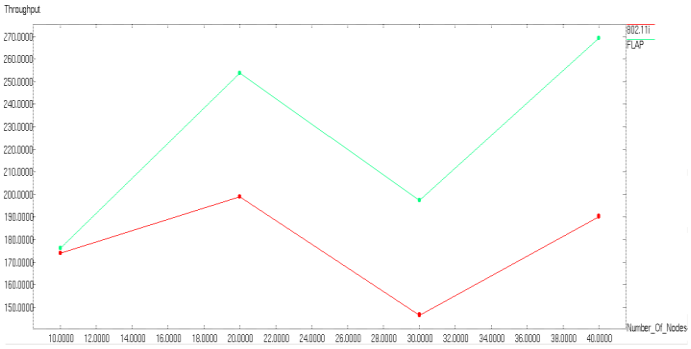

Figure 5: Throughput comparison between 802.11i and FLAP

From the above graph it is clear that throughput is efficient in FLAP than EAP-TLS 802.11i. When the number of STA is 10 the throughput values of both the protocols are approximately similar. As the number of STA increases to 30 then the values are 256 for FLAP and 198 for EAP-TLS. Throughput is measured in kbps.

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those packets sent by the sources. The PDR for 10, 20, 30 and 40 number of STA for both 802.11i and FLAP are shown as below:

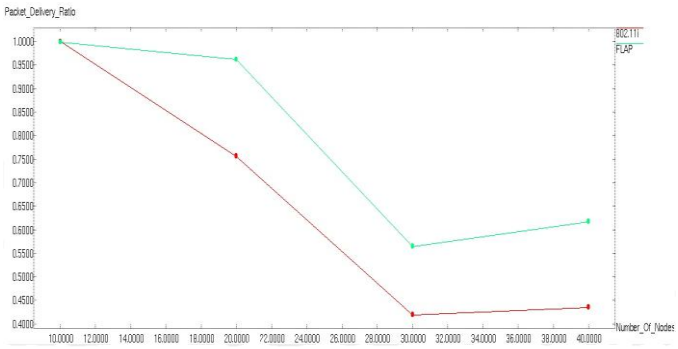

Figure 6: PDR comparison between 802.11i and FLAP

Above graph shows that the PDR for both EAP-TLS and FLAP schemes is same when there is 10 number of STA i.e., 1. When the number of STA increases to 40 then PDR of FLAP is 0.68 where as for EAP-TLS is 0.43. The greater value of packet delivery ratio means the better performance of the protocol.

And finally Packet Drops are considered and compared between both the existing and proposed schemes. Packet Drops show the total numbers of packets those drops during the transmission from source to destination. The below figure shows, the simulation results of packet drops for both protocols.

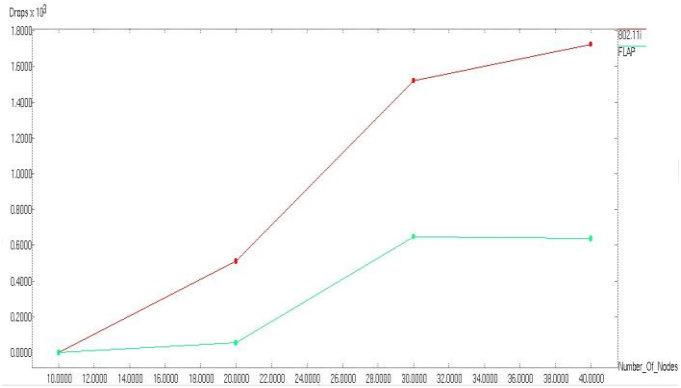

Figure 7: Packet drops comparison of 802.11i and FLAP

By considering the results of all these parameters we can say that FLAP is more efficient in many scenarios than 802.11i EAP-TLS.

- EAP-TLS is inefficient; especially when the incoming STAs number increases dramatically or the WLAN is crowded. For example, when there are 40 number of STA the average authentication is 820s.

  Taking into account the scan and DHCP process, the initial link setup time will get even longer. With this performance, the offloading of real applications from 3G to WLAN cannot be realized for certain. In addition, let us image such a scenario where the radius of a WLAN is assumed to be 100 m and a car with the speed of 45 km/h passes through the WLAN. It will take the car up to 16 s, which is not quite enough for the onboard STA to establish the initial link if there is background traffic or the WLAN is crowded.

- Our scheme has salient advantage over the EAP-TLS, especially when the WLAN is crowded. With the new incoming STAs number increases, the authentication delay difference between EAP-TLS and our scheme gets bigger and bigger.

The below table shows the performance analysis results of our two protocols based on some performance metric such as number of nodes, authentication delay, throughput, PDR and packet drop:

Table 1: Performance Results of 802.11i and FLAP

Number of Nodes	Existing 802.11i values				Proposed FLAP values			
	Delay	Through put	PDR	Drops	Delay	Through put	PDR	Drops
10	29.49	173.89	1	0	23.12	176.08	0.99	0
20	122.4	198.90	0.75	512	82.73	253.59	0.96	53
30	436.8	146.56	0.41	1521	283.8	197.43	0.56	648
40	807.1	190.18	0.43	1724	350.0	269.10	0.61	638

Simulation result analysis: There are three factors that contribute to the salient advantage of our protocol over EAP-TLS.

1) Rather than being an authentication framework, our proposal is a specific authentication protocol. Therefore, some messages in the 802.11i can be eliminated, such as the open authentication request/response messages. Meanwhile, some messages in the 802.11i are integrated, for example, the identity information in our protocol is sent with other authentication information, while 802.11i employs two independent messages to carry this information.

Furthermore, the authentication between the STA and the AS is incorporated skilfully with the four-way handshake, without introducing extra messages. To realize the integration, the AS has to authenticate the STA successfully after receiving the first message (the fast access authentication request). Otherwise, the AP cannot get PMK or generate PTK before it generates the second message, and it cannot proceed to the four-way handshake. While, in the design of the two-message authentication protocol between the AS and the STA, how to ensure the freshness of the fast authentication request is a crucial problem. In our scheme, a loose counter t is utilized which is unnecessarily strictly synchronous. In such a method, the authentication between the STA and the AS can be integrated with the four-way handshake without introducing extra messages. Through the efforts mentioned above, our proposal just needs two roundtrip message interactions while 802.11i has 13 roundtrip messages. By means of reducing message exchanges, the time to spend in competing for the wireless channel is greatly cut down, especially when the WLAN is crowded.

2) The symmetric cryptographic algorithm is utilized in our scheme while EAP-TLS employs the asymmetric algorithm; therefore, the computation delay of EAP-TLS is much longer than ours.

3) The data amount of EAP-TLS is 14,341 bytes (from the EAPoL-Response/ identity to the end of four-way handshake) wherein the transmission of public key certificates is a major contributor, and ours is just 1,129 bytes.

VI. SECURITY IN FLAP

In our scheme, there is no strict synchronization requirement for the t values in the STA and the AS. We just require that the t value in the STA is no less than the one maintained by the AS. Therefore, it does not have a high demand for the system.

In addition, when the environment (e.g., the system failure) results in an asynchronization of the t values, an 802.11i authentication is executed and after the successful authentication both parties send the other the t value that it finally used and the bigger one is chosen as the new synchronized t value. It should be noticed that even the new synchronized t value is smaller than the last t value used before (this situation will happen when both the STA and the AS lose their t values), it will not do harm to the security of the scheme. Because under this circumstance the attacker can just replay the used fast authentication request but cannot get the PMK, which disables it to launch the third authentication message. Furthermore, it can not disturb the synchronization of the t values between the STA and the AS, because if the attacker cannot proceed the scheme, the AS's t value will be rolled back upon receiving the failure message from the AP (refer to the Step (10)). That is, the AS will not update its t value if FLAP cannot be completed fully. In such a way, the t values get synchronized again. From this procedure, it can be seen that AS's rollback of its t value is necessary in the Step (10) if the AP does not authenticate the STA successfully, otherwise, in the resynchronization process if an attacker replays a fast authentication request, the AS's t value will get bigger than the STA's, resulting that the legal STA cannot proceed the authentication.

In 802.11i, only after the successful authentication can the STA' IP address acquisition is executed. But in our scheme, the IP address acquisition can be performed in parallel with the FLAP. If the legacy DHCP [12] is employed to get the IP address, then each of its four messages can be carried by the corresponding message in our protocol as a new field. If the address is allocated with DHCP Rapid Commit Option [13], then its two messages can be carried through the first two messages of our scheme. But in either case, only when the AP authenticates the STA successfully (that is, after the message 9), can the allocated IP address is delivered to the STA.

VII. CONCLUSION

With the rapid increase of the WLAN-enabled devices, the current WLAN security standard IEEE 802.11i is challenged for its low efficiency. In this paper, we first demonstrate its inefficiency through experiments, and then point out that the essential reason leading to such inefficiency is the fact that 802.11i is designed from the framework perspective which introduces too many message interactions. To overcome this drawback and meet the requirement of new applications, an efficient initial access authentication protocol FLAP is proposed, which takes just two roundtrip messages between the client and the networks to complete the authentications and key distribution between the STA, AP, and AS. Analysis indicates that our scheme is more secure than the four-way handshake protocol. Furthermore, simulations are done in different scenarios using different number of nodes like 10, 20, 30 and 40. Delay, Throughput, PDR and Packet drops are compared between 802.11i and FLAP. Results indicate that with the STA number increases, our scheme has more salient advantage over EAP-TLS.

REFERENCES

[1] IEEE 802.11, "Information Technology-Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Equirements-Part 11: Wireless LAN Medium Access Control and Physical Layer Specifications," IEEE Standard, 2007.

[2] IEEE 802.11b, "Higher-Speed Physical Layer Extension in the 2.4 GHz Band, Supplement to IEEE Standard for Information Technology-Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks- Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Standard, Sept. 1999.

[3] W.A. Arbaugh, N. Shankar, and J. Wang, "Your 802.11 Network Has No Clothes," Proc. IEEE First Int'l Conf. Wireless LANs and Home Networks (ICWLHN '01), pp. 131-144, 2001.

[4] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," Proc. ACM MObiCOM, pp. 180-189, 2001.

[5] B. Aboba, L. Blunk, J. Vollbrecht, and J. Carlson, "Extensible Authentication Protocol (EAP)," RFC 3748, June 2004.

[6] IEEE 802.1X, "IEEE Standard for Local and Metropolitan Area Networks-Port-Based Network Access Control,"IEEE Standard, June 2001.

[7] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial in User Service (RADIUS)," RFC 2865, June 2000.

[8] X. Li, J. Ma, and Y. Shen, "An efficient WLAN Initial Authentication Protocol," Proc. IEEE Global Comm. Conf. (Globecom '12), 2012.

[9] IEEE P802.11i, "Medium Access Control (MAC) Security Enhancements, Amendment 6 to IEEE Standard for Information Technology-Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks- Specific Requirements -Part11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications,"IEEE Standard, Apr. 2004.

[10] P. Chatzimisios, A. Boucouvalas, and V. Vitsas, "Packet Delay Analysis of IEEE 802.11 MAC Protocol," Electronics Letters, vol. 39, no. 18, pp. 1358-1359, 2003.

[11] G. Bianchi, "Performance Analysis of the IEEE802.11 Distributed Coordination Function," IEEE J. Selected Areas in Comm., vol. 18, no. 3, pp. 535-547, Mar. 2000.

[12] R. Droms, "Dynamic Host Configuration Protocol," RFC 2131, 1997.

[13] S. Park, P. Kim, and B. Volz, "Rapid Commit Option for the Dynamic Host Configuration Protocol Version 4 (DHCPv4)," IETF RFC 4039, 2005.

[14] C. He and J.C. Mitchell, "Analysis of the 802.11 i 4-WayHandshake," Proc. Third ACM Workshop Wireless Security (Wisec'04), pp. 43-50, 2004.