# Fast and Secure Authentication Using Double Token based Scheme for WLANs

Poonam Jindal
(Member IEEE)
ECED, National Institute of Technology
Kurukshetra, India

Brahmjit Singh
(Member IEEE)
ECED, National Institute of Technology
Kurukshetra, India

## ABSTRACT

Authentication can provide security by preventing unauthorized usage and negotiating the credentials for secure communication. Nevertheless, it induces heavy overhead to communications, further deteriorating the quality of service *(QoS).* Analyzing QoS and security impact of authentication, therefore, becomes critical to developing efficient authentication schemes. In this paper, we propose a system model for the analysis of challenge/response authentication in wireless networks. In the proposed double token based fast authentication scheme, one token is generated in the registration phase and second in the authentication phase which provides another layer of security to the authentication scheme. All the keys are exchanged during the registration phase. This makes the security parameters known only to the mobile client (MC), authenticator and authentication server (AS). Attackers would be unable to know the token and other secret keys because they are shared only during the registration phase. This makes the authentication scheme highly secure. The number of key exchanges that takes place during authentication phase is less, which makes the authentication fast as compared to Extensible Authentication Protocol (EAP) authentication where all messages are exchanged during the authentication phase. The proposed scheme results in fast authentication without compromising the security of wireless networks.

## General Terms

Authentication, Encryption, Wireless network security.

## Keywords

EAP, Token based authentication, WLAN

## 1. INTRODUCTION

There has been tremendous growth of wireless communication services over the last decade. The security concerns are becoming more serious with the growth of wireless networks. As more people access critical information and consumers begin to do their business and banking on mobile wireless devices, wireless security has moved to the forefront. Due to open nature of wireless medium there are certain attacks that exist on wireless networks and these can be classified as active and passive attacks [1]. Active attacks are those in which the transmitted data can be modified by an intruder and in passive attacks transmitted data can only be read. Cryptographic primitives such as encryption and authentication are used to secure data over the wireless channel at the expense of QoS due to implementation overheads [2].

Authentication is the way a user is identified prior to being allowed access to the network and network services. Authentication is done on the basis of: something you have, something you know or some you are. The best authentication techniques combine two or more of these mechanisms. Different authentication mechanisms based on these verifications are password based authentication, challenge response authentication and Zero knowledge proofs. Password sniffing, post authentication hijacking, online password guessing, offline dictionary attack, replay attack, denial of service attack, man in the middle attack are the different possible attacks on authentication mechanisms. To overcome these attacks some authentication mechanisms and protocols have been developed.

Wired equivalent privacy (WEP) was the first security protocol, designed to cover the security requirements in wireless environment, and provides authentication, data integrity and privacy as the basis. Due to faulty implementation of RC4 cipher in the WEP protocol, many security flaws were discovered based on known drawbacks of the RC4 cipher. The flaws give rise to a number of attacks, both passive and active, that allow eavesdropping and tampering with the wireless transmissions [3]-[6]. WPA contributes to the increase of wireless communication protection by Wi-Fi standard through increased level of data protection, access control and integrity. This standard is completely compatible with a new IEEE 802.11i standard. It introduces TKIP (Temporal Key Integrity Protocol) group of algorithms created to improve safety mechanisms of WEP and provide strong and safe authentication by using a pre shared key and RADIUS-based 802.1x/EAP standard. EAP is an authentication framework which supports multiple authentication methods. EAP-TLS, EAP-TTLS, PEAP, LEAP, EAP-MD5 are the available EAP authentication methods [7]-[11]. Comparison between different EAP standards is presented in [12]-[14].From the available literature it has been found that wireless devices are facing different attacks such as, attacks in the integrity and attacks on availability of user resources (denial of service attack). To prevent the wireless network from being discovered a strong and secure authentication scheme is required before allowing anyone to access the network. After the completion of authentication phase strong encryption mechanisms must be employed to encrypt all the messages exchanged over wireless network.

To run these cryptographic primitives, the system must consume more power. The encryption and authentication algorithms need processing. For the device, this represents computation overhead, which has direct impact on the power consumption. Some of the security algorithms consume huge amount of power. Beside the computational overhead, encrypting data traffic involves adding extra bytes to the frames. Authentication, on the other hand, involves adding extra messages. Adding extra bytes and extra messages to the original data result in throughput reduction and also increases the wait time.

To secure the wireless communication and the overheads associated with applying encryption and authentication mechanisms represents an important issue. There is a trade-off between security and performance of the wireless network. In this work, we address the issue of flexibility and high speed authentication in WLANs.

EAP authentication is not a secure method of authentication due to the exchange of secret keys during the authentication phase and is prone to several attacks. Keys are exchanged during each session which makes the process slow. To overcome these drawbacks of 802.1x EAP protocol, a strong and fast authentication scheme has been introduced by the author in [15]. Security and speed of fast token based authentication scheme has been analyzed in [16]. It has been found that the token based fast authentication scheme overcomes the tradeoff between security and performance of wireless networks. But several drawbacks have been found in the fast token based authentication scheme.

In this paper, we propose a double token based fast authentication scheme. Performance analysis of the scheme has been reported. From the numerical results it is found that double token based authentication scheme is providing high level of security as compared to EAP based authentication and fast token based authentication. Time taken to complete the authentication phase is less than EAP and is comparable with fast authentication scheme.

The rest of the paper is organized as follows. EAP authentication and its vulnerabilities are discussed in section 2. Token based fast authentication is discussed in section 3. The proposed double token based authentication scheme is given in section 4. Simulation results are discussed in section 5. Conclusion and future work are outlined in section 6.

## 2. EAP AUTHENTICATION

IEEE 802.1x provides strong authentication mechanisms and has improved the wireless security. This has been achieved by EAP authentication protocol. In EAP authentication the AS request the login name, password and hashing or public/private keys to authenticate MCs or users. EAP authentication is shown in fig. 1.

However the hash functions and digital signatures used in EAP are required in every session. This will slow down the whole process and user has to wait for long time during the authentication phase before he/she gains the complete authorization to access the resources. In figure 1, EAP has three phases: open authentication /association, EAP authentication and encryption. In the authentication phase, public keys, digital signatures used for authentication will be exchanged between the user and the AS in order to complete the mutual authentication process. This exchange of messages adds loss of overheads which make the process slow and user has to wait for long time during the authentication phase. Moreover all secret messages are exchanged during the authentication phase which makes it vulnerable to different attacks like dictionary attacks, (man in the middle) MitM attacks, plaintext attacks, ciphertext attacks. The main cause of these vulnerabilities is the re-use of legacy client authentication protocols that run inside the authenticated tunnel. There is a need to enhance the mutual authentication process security as well as its performance.

## 3. FAST TOKEN BASED AUTHENTICATION

To overcome the limitations of EAP authentication a fast and secure authentication scheme is proposed by authors in [15].

### 3.1 Fast token based authentication and registration phase

A token based registration authentication phase is shown in figure 2. VT is exchanged between user and the AS and later on this token will be used to generate a valid token key (VTK) to encrypt all messages during the authentication phase. To get registered in the wireless network, administrator will issue new user name, password and temporary token (TT) to the MC. By following the steps from 1-6 as shown in figure 1, user will get associated with the authenticator (access point) during the association phase. After the association and open authentication phase there is a registration phase.

The following algorithm can be used for the implementation of authentication registration phase.

1. MC generates a temporary token key (TTK) from TT and media access control (MAC) of the user machine. 128 bits of both TT and MAC are concatenated to generate 256 bits of TTK for encryption.

$$\text{TTK(256bits)} = \text{TT(128 bits)} \parallel \text{MAC(128 bits)}$$

2. Encrypt the pair of UserID and Pwd using the TTK. 128 bits representation of UserID and Pwd are concatenated and encrypted with TTK.

$$[\text{UserID(128 bits)} \parallel \text{Pwd(128 bits)}] \text{ XOR TTK}$$

3. The MC sends the encrypted User ID and Pwd pair and TT, and MAC as a plain text.

$$\text{Encrypted message} \parallel \text{TT} \parallel \text{MAC}$$

4. Server generates TTK from the received TT and MAC pair in the same manner as in step 1.

5. Server decrypts the encrypted UserID and Pwd pair using TTK using XOR.

6. Server generates VT and mapped to MAC value.

7. Server generates asymmetric encryption key ATK (Authentication token key) using RSA method.

8. Server sends VT and the public part of ATK encrypted by TTK to the user.

9. The private key of ATK is always kept in the server and never sent to any user.

10. MC decrypts the encrypted VT and the public key of ATK using TTK.

11. MC generates VTK from VT, date and MAC for future authentication and association.

12. MC sends the messages using ATK for encryption.

### 3.2. Token based fast authentication phase

If the MC or supplicant was registered before and again he/she wants to access the network, he/she has to face the challenge given by the AS to authenticate itself. Steps involved in the authentication phase are explored in figure 3.

1. Once the MC and AP (Access Point) got associated with each other at step 1 and 2,

2. VTK will be generated by MC using the stored VT, MC's MAC address and current date.

3. Authentication request would be sent to AP and forward it to AS at step 4.

4. During the authentication request, user credentials would be encrypted first by using VTK and then by ATK. Also the supplicant's MAC and current date

used to generate VTK would be encrypted by using ATK which is known to MC during the registration phase. On the other end AS will decrypt the request using ATK and extract the date and MAC. Then the AS will check the database to match the VT which is linked to this MAC address. If the user is already registered then its MAC address as well as the VT associated with that MAC will be found. The AS will then generate VTK key to decrypt the user credentials. The date has been used along with the request to avoid the replay attacks.

5. If the user is valid then an accepted authentication message will be delivered to authenticator in step 5.

6. Then in step 6 the authenticator will store the success information in his own database and send this message to MC at step 6.

7. Success association will be done in the step 7 and 8. Association phase is followed by the encryption phase which is same as 802.1x authentication.

## 4. PROPOSED SCHEME

Fast token based authentication scheme discussed in [15] have certain limitations. During the authentication phase the MAC address has been sent in clear and makes the MAC address vulnerable. It has also been observed that the authentication scheme is one step authentication. User is authenticated on the basis of already available data. If the intruder is somehow managed to compromise the scheme or available secure information he/she can authenticate himself by using that particular information. To overcome these limitations a double token based authentication scheme has been proposed.

In double token based authentication one token is exchanged during the registration phase and second token is exchanged during the authentication phase. If the intruder is able to compromise one token he will have to face the challenge of computing the second token. Every time the valid token (VT) is changed the intruder will not be able to find the VT, hence providing an extra layer of security. As most of the key exchanges are performed in registration phase and very few messages are exchanged during the authentication phase, it makes the scheme secure and fast as well.

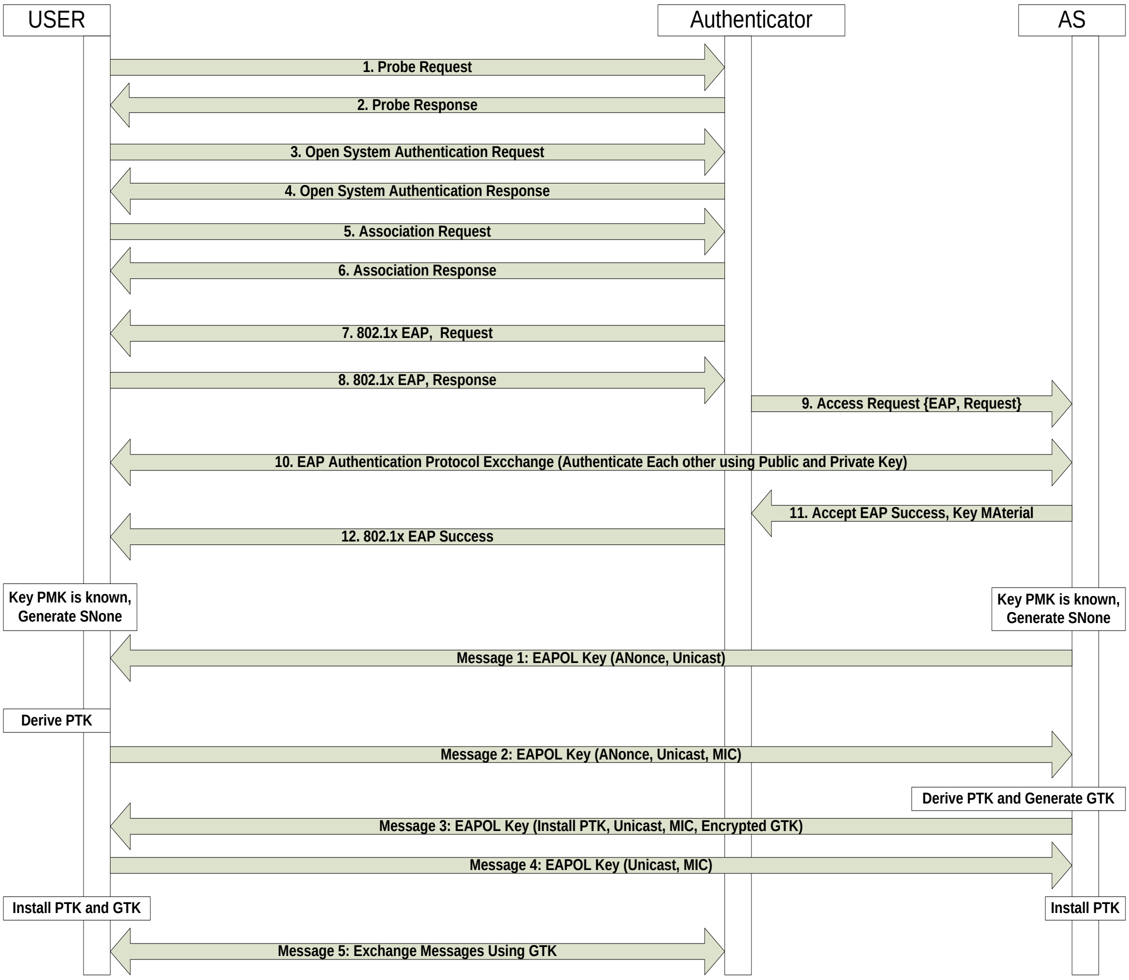
USER
Authenticator
AS
1. Probe Request
2. Probe Response
3. Open System Authentication Request
4. Open System Authentication Response
5. Association Request
6. Association Response
7. 802.1x EAP, Request
8. 802.1x EAP, Response
9. Access Request {EAP, Request}
10. EAP Authentication Protocol Excchange (Authenticate Each other using Public and Private Key)
11. Accept EAP Success, Key MAterial
12. 802.1x EAP Success
Key PMK is known, Generate SNone
Key PMK is known, Generate SNone
Message 1: EAPOL Key (ANonce, Unicast)
Derive PTK
Message 2: EAPOL Key (ANonce, Unicast, MIC)
Derive PTK and Generate GTK
Message 3: EAPOL Key (Install PTK, Unicast, MIC, Encrypted GTK)
Message 4: EAPOL Key (Unicast, MIC)
Install PTK and GTK
Install PTK
Message 5: Exchange Messages Using GTK

**Fig 1. Eap authentication**

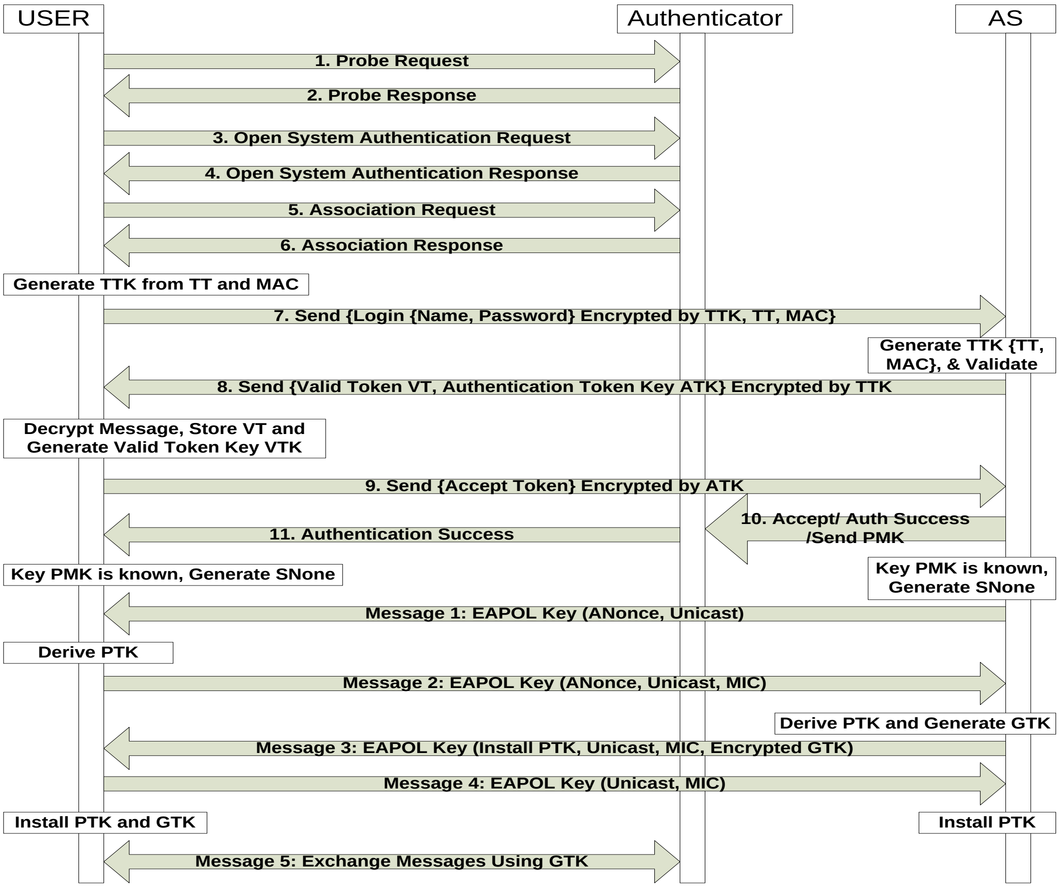
USER
Authenticator
AS
1. Probe Request
2. Probe Response
3. Open System Authentication Request
4. Open System Authentication Response
5. Association Request
6. Association Response
Generate TTK from TT and MAC
7. Send {Login {Name, Password} Encrypted by TTK, TT, MAC}
Generate TTK {TT, MAC}, & Validate
8. Send {Valid Token VT, Authentication Token Key ATK} Encrypted by TTK
Decrypt Message, Store VT and Generate Valid Token Key VTK
9. Send {Accept Token} Encrypted by ATK
10. Accept/ Auth Success /Send PMK
11. Authentication Success
Key PMK is known, Generate SNone
Key PMK is known, Generate SNone
Message 1: EAPOL Key (ANonce, Unicast)
Derive PTK
Message 2: EAPOL Key (ANonce, Unicast, MIC)
Derive PTK and Generate GTK
Message 3: EAPOL Key (Install PTK, Unicast, MIC, Encrypted GTK)
Message 4: EAPOL Key (Unicast, MIC)
Install PTK and GTK
Install PTK
Message 5: Exchange Messages Using GTK

**Fig. 2. Token-Based Fast Authentication Registration phase in WLAN**

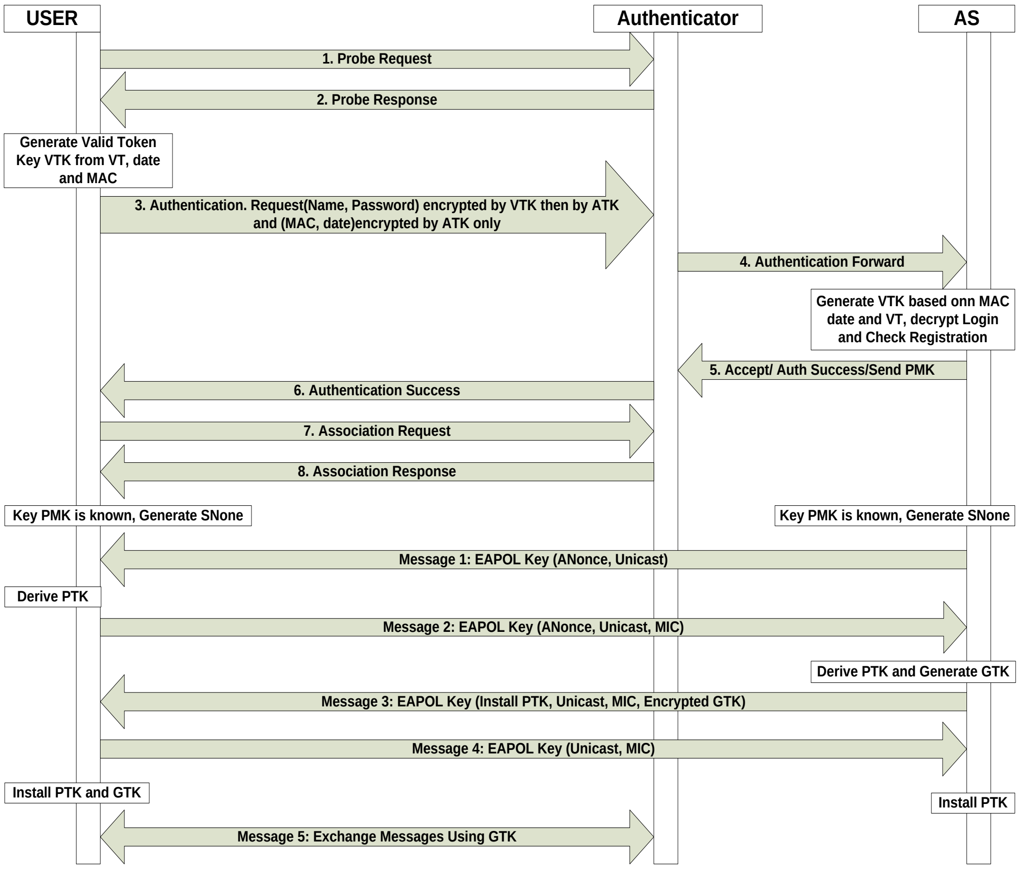
USER
Authenticator
AS
1. Probe Request
2. Probe Response
Generate Valid Token Key VTK from VT, date and MAC
3. Authentication. Request(Name, Password) encrypted by VTK then by ATK and (MAC, date)encrypted by ATK only
4. Authentication Forward
Generate VTK based onn MAC date and VT, decrypt Login and Check Registration
5. Accept/ Auth Success/Send PMK
6. Authentication Success
7. Association Request
8. Association Response
Key PMK is known, Generate SNone
Key PMK is known, Generate SNone
Message 1: EAPOL Key (ANonce, Unicast)
Derive PTK
Message 2: EAPOL Key (ANonce, Unicast, MIC)
Derive PTK and Generate GTK
Message 3: EAPOL Key (Install PTK, Unicast, MIC, Encrypted GTK)
Message 4: EAPOL Key (Unicast, MIC)
Install PTK and GTK
Install PTK
Message 5: Exchange Messages Using GTK

**Fig. 3. Token based fast only authentication phase**

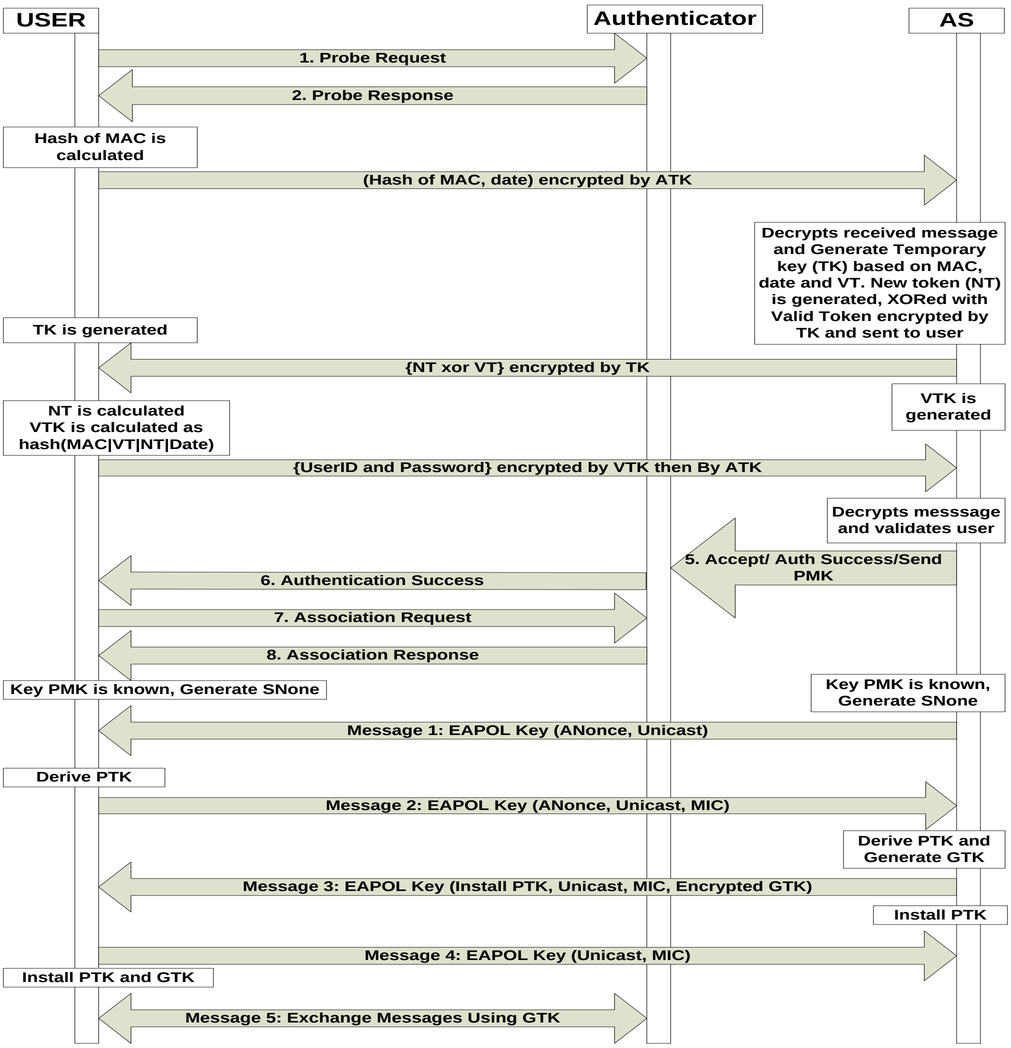
USER
Authenticator
AS
1. Probe Request
2. Probe Response
Hash of MAC is calculated
(Hash of MAC, date) encrypted by ATK
Decrypts received message and Generate Temporary key (TK) based on MAC, date and VT. New token (NT) is generated, XORed with Valid Token encrypted by TK and sent to user
TK is generated
{NT xor VT} encrypted by TK
NT is calculated VTK is calculated as hash(MAC|VT|NT|Date)
VTK is generated
{UserID and Password} encrypted by VTK then By ATK
Decrypts messsage and validates user
5. Accept/ Auth Success/Send PMK
6. Authentication Success
7. Association Request
8. Association Response
Key PMK is known, Generate SNone
Key PMK is known, Generate SNone
Message 1: EAPOL Key (ANonce, Unicast)
Derive PTK
Message 2: EAPOL Key (ANonce, Unicast, MIC)
Derive PTK and Generate GTK
Message 3: EAPOL Key (Install PTK, Unicast, MIC, Encrypted GTK)
Install PTK
Message 4: EAPOL Key (Unicast, MIC)
Install PTK and GTK
Message 5: Exchange Messages Using GTK

**Fig.4. Double token based fast authentication**

## 4.1 Double token based fast authentication scheme

In double token based authentication scheme, the steps involved in association and registration authentication phase are same as proposed in [15]. Only authentication phase has been modified in the proposed scheme. Steps involved in only authentication phase are shown in figure 4. As mentioned in section 3, if the MC or supplicant has already been registered before and again he/she wants to access the network, he/she has to face the challenge given by the AS to authenticate itself as shown in fig. 4. It shows that once the MC and AP get associated with each other at step 1 and 2, both will follow the following steps to complete the authentication.

1. SM (Start Message) is generated and sent by MC to AS.

$$SM = E([Hash(MAC) \| Date], ATK)$$

2. AS receives SM and decrypts to generate the TK (temporary token).

$$TK = Hash(MAC \| Date \| VT)$$

3. A new token (NT) (any 128 bits random number generated by AS) is generated and XORed with VT and send to user after encrypting by TK.

$$E(NT\ XOR\ VT, TK)$$

4. In the mean time, user generates the TK.

5. NT is calculated at user end by decrypting the received message.

6. VTK is generated at both ends by hash value of $MAC \| VT \| NT \| date$.

7. User ID and passwords are shared by dual encryption; first by VTK (symmetric) and then by ATK (Asymmetric), with this authentication is completed and acceptance message is sent to user.

8. NT is stored by replacing VT for future communication.

The date has been used along with the request to avoid the replay attacks. If the user is valid then an accepted authentication message will be delivered to authenticator. Then in step 6 the authenticator will store the success information in its own database and send this message to MC at step 6. Success association will be done in the step 7 and 8. Association phase is followed by the encryption phase which is same as 802.1x authentication.

# 5. PERFORMANCE ANALYSIS OF DOUBLE TOKEN BASED AUTHENTICATION SCHEME

Fast and secure authentication is a critical issue in wireless networks. If authentication is not secure then the system will be vulnerable to several attacks. Any intruder can get the secret keys and access the information. On the other side if the authentication process is slow, it will make the user to wait for long time before he/she will get the full access to the network. Therefore security and speed of the authentication scheme is a critical issue in the wireless networks. The strength of our proposed framework has been analyzed in terms of security and performance in terms of time consumed in the authentication phase.

## 5.1 Security analysis

Mutual authentication is performed between the supplicant and AS in double token based scheme. In the present scheme it has been obtained, since all the secret information has been exchanged in the registration authentication phase and no secret keys are exchanged during the authentication phase, the intruder will not be able to discover the key. Two tokens are generated in the scheme and intruder will not get the full access without the knowledge of both tokens. Keys generated during the authentication phase are dependent on both keys used in the registration phase and the keys used in the authentication phase. Registration of the user with the AS is done everytime the user wants to communicate but in registration phase the registration was user dependent and in authentication phase the registration is server dependent. Different attacks to which the proposed scheme resists are:

**1.** *Password guessing attack*. Since the password is not sent in clear, rather encrypted passwords are transmitted during the registration phase, it makes the password guessing attack very hard and moreover no passwords are exchanged during the only authentication phase.

**2.** *MAC address spoofing Attack*. MAC address is not sent in clear. First the hash of MAC is calculated and then encrypted with ATK. This step makes MAC address spoofing attack almost impossible.

**3.** *Replay Attack*. Current date has been used during the authentication phase which also resolves the security issue, the replay attack. If the intruder intercepts the message and will try to resend the message later he/she will be discovered.

**4.** *Impersonation Attack*. An attacker cannot impersonate the user. Only the person who knows the VT and can generate the second token will be authenticated.

**5.** *Man-in-the-middle attack (MITM*). If an attacker succeeded in guessing a password or MAC address spoofing he/she will not be able to attempt a MITM attack. This malicious attempt will not work without the knowledge of VT.

**6.** *Denial-of-service attack*. Denial of service attack cannot work in our framework. Suppose intruder is able to guess the NT. He cannot change the NT without the knowledge of old token and that is shared only during the registration phase.

From the above analysis it has been observed that the security of double token based authentication scheme is enhanced as compared to fast token based authentication and EAP based authentication. Here no secret messages are exchanged in clear and no secret information is exchanged during the authentication phase. First challenge, the intruder has to face is the hash of MAC, then he is required to find the VT, and the third layer of security is NT.

## 5.2 Speed analysis

It has been mentioned that all keys are exchanged during the registration phase in the token based scheme. Unlike the EAP authentication [8], there is no need to send public/private keys, hashes, digital signatures during every session of authentication. With this the overheads incurred during the authentication phase are reduced and makes the mechanism fast. Now the MC has not to wait so long for the authentication phase to complete. As compared to fast token based authentication scheme, the number of message exchanges are increased which enhances the security of the proposed double token based authentication scheme but slightly increases the time consumed during the authentication phase.

We have configured the proposed system model to obtain numerical results using MatLab for three authentication schemes: EAP authentication, Token based authentication and double token based authentication. Time consumed by the 802.1x EAP to complete the mutual authentication between the AS and the MC is 0.5919 seconds. Time consumed in only authentication phase (when user is already registered with AS) for fast token based authentication scheme is 0.2325 seconds. Time consumed in only authentication phase for double token based authentication scheme is 0.3911. From the obtained numerical values it is observed that time consumed in only authentication phase for double token based authentication scheme is more than fast token based authentication and this is due to the increased number of message exchanges to enhance the security of the scheme. Time consumed in registration authentication phase for both token based and double token based authentication schemes is same i.e. 0.4537 seconds. Speed analysis of double token based fast token based authentication in authentication registration phase and in only authentication phase is shown in fig.5.

The comparison of EAP 802.1x authentications, token based fast authentication and double token based fast authentication in only authentication phase is shown is fig.6. From the numerical results it is found that time taken to complete the authentication phase is highest in EAP authentication and lowest in token based fast authentication. Numerical values for the comparison of speed in EAP authentication, token based authentication and double token based authentication in only authentication phase are shown in table 1.

Performance analysis of EAP authentication, token based authentication, and double token based authentication showed that double token based authentication scheme provides a very high level of security to the wireless networks as compared to EAP authentication and token based fast authentication along with the improved performance of the network in terms of speed as compared to EAP authentication and comparable performance with fast token based authentication.

# 6. CONCLUSION

In this paper, we have proposed a double token based fast authentication algorithm with enhanced security and better tradeoff between security and performance of WLANs. First layer of security is achieved using TT which is issued to MC by AS. All the secret keys are exchanged between MC and AS during the registration phase, no one will, therefore, be able to understand the keys and will be unable to decrypt the message used for authentication. This makes the authentication scheme highly secure. Second layer of security is provided using the hash of MAC during the authentication phase and third layer of security is provided by computing the NT every time in the authentication phase. Performance analysis has been done in terms of security and authentication time and is compared with the two different authentication schemes. Because the number of key exchanges during the authentication phase is less, this makes the authentication process fast as compared to 802.1x where all keys (public/private keys, DS, hash) are exchanged during the authentication phase in every session between the MC and AS. This shows that the proposed double token based authentication technique provides a fast authentication scheme with an enhanced security.

**Table 1. Speed Analysis of Authentication Schemes**

| Type of authentication | Completion Time (sec.) | Speed Analysis |
|---|---|---|
| EAP 802.1x | 0.5919 | Slow |
| Registration authentication phase for token based authentication | 0.4537 | Fast |
| Token based authentication in only authentication phase | 0.2325 | Very fast |
| Double token based authentication in only authentication phase | 0..3911 | Faster than EAP but Slower than fast token based |

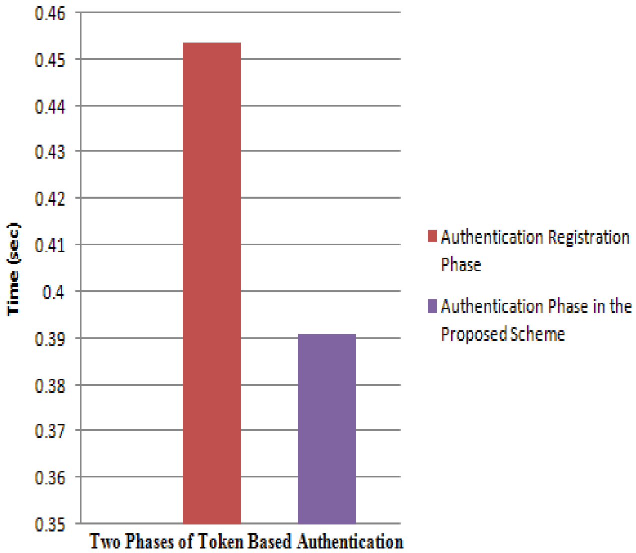

**Fig 5. Time consumed in registration phase and fast authentication phase**

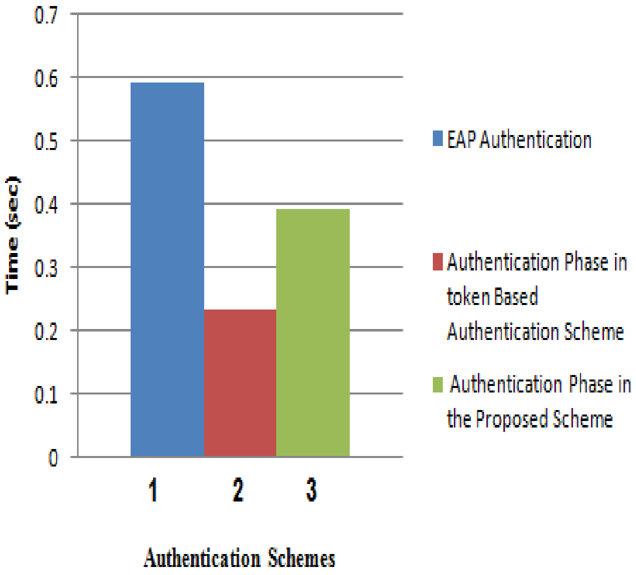

**Fig 6.Comparison of speed in EAP authentication and fast authentication process**

## 7. References

[1] Russ Housley, William Arbaugh, “Security Problems in 802.11- Based Networks”. Communications of the ACM, Vol.46, No. 5, May 2003, pp 31-34.G.

[2] William Stallings, “Cryptography and Network Security, Principles and Practices,” 4rth Edition, Prentice Hall 2007.

[3] Fluhrer, S.; & Shamir, A. “Weaknesses in Key Schedule Algorithm of RC4”. Workshop on Selected Areas of Cryptography, 2001.

[4] Arbaugh, W.A.; & Shankar, N. “Your Wireless Network Has No Clothes”. First International Conference on Wireless LANs, Singapore, March 2001, pp. 131-44.

[5] Borisov, N.; & Wagner, D. “Intercepting Mobile Communications: The Insecurity of 802.11”. International Conference on Mobile Computing and Networking, July 2001, pp. 180-89.

[6] Allam Mousa, Ahmad Hamad, “Evaluation of RC4 Algorithm for Data Encryption”. International Journal of Computer Science and Applications, Vol. 3, No.2, June 2006, pp 44-56.

[7] LAN MAN Standards of the IEEE Computer Society, “Wireless LAN Medium Access Control and Physical Layer Specifications, Medium Access Control Security Enhancement”.IEEE Standard 802.11i, 2004.

[8] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, Extensible Authentication Protocol (EAP), Ed., RFC 3748, Internet Society, Jun. 2004.

[9] K. M. Ali and T. J. Owens, "Selection of an EAP authentication method for a WLAN," International Journal of Information and Computer Security, vol. 1, no. 1/2, pp. 210-233, 2007.

[10] P. Funk and S. Blake-Wilson, “EAP Tunneled TLS Authentication Protocol Version 1 (EAP-TTLSv1)”, The Internet Society, Mar. 2006.

[11] V. Kamath, A. Palekar, and M. Wodrich, Microsoft’s PEAP version 0 (Implementation in Windows XP SP1), The Internet Society, Oct. 2002.

[12] B. Brown, "802.11: The Security Differences Between b and i". Potentials IEEE, Vol. 22, Issue 4, Oct-Nov 2003, pp 23-27.

[13] H. Altunbasak, H. Owan, "Alternative Pair Wise Key Exchange Protocol for Robust Security Networks (IEEE 802.11i) in Wireless LANs". Proceedings Southeast Conference, IEEE, 26-29 March, pp 77-8.

[14] M. Arunesh, A. W. Arbaugh, "An Initial Analysis of the IEEE 802.1X Standard". Department of Computer Science, University of Maryland, CS-TR4328, 2002, pp 1-12.

[15] Ghassan Kbar, "Wireless Network Token Based Fast Authentication" International Conference on Telecommunications, 2010, pp227-233.

[16] Poonam Jindal, Brahmjit Singh "Performance Evaluation of Token Based Authentication Scheme for WLANs" Conference on Advancements in Communication & Computing Systems "COMMUNE CACCS-2012, held at I.T.S. Engineering College. Gr. NOIDA on March 24-25, 2012, pp 68-75.