ISSN 2047-3338

EAP-SAM: A Simple Authentication Mechanism for Mutual Authentication in EAP-Enabled WLANs

Suhail Ahmad[1], Ajaz Hussain Mir[2] and Ghulam Rasool Beigh[3]
Electronics and Communication Engineering Department, National Institute of Technology, Srinagar (J&K), India
[1]sa_mir@in.com, [2]ahmir@rediffmail.com, [3]grbegh136@yahoo.com

***Abstract*— Authentication forms an important part of security mechanism by securing the networks from unauthorized access. The time taken by the client to authenticate to the Extensible Authentication Protocol (EAP)-enabled Wireless Local Area Networks (WLANs) will have a significant impact on the real time applications particularly under mobile conditions. Also, the number of messages involved in the authentication will have a significant impact on the energy consumption as the mobile terminal is having limited energy source (battery). In this paper the quantitative analysis of Extensible Authentication Protocols is provided and the security features of these protocols are compared. The protocols compared are EAP-MD5, EAP-TLS, and PEAP. A simple authentication protocol, EAP-Simple Authentication Mechanism (SAM) is proposed in this paper, consisting of reduced number of authentication messages. The reduced number of authentication messages yields the least authentication delay as well as the reduced energy consumption resulting in uninterrupted services for the real time applications.**

***Index Terms*— EAP, EAP-MD5, EAP-TLS, EAP-SAM and PEAP**

I. INTRODUCTION

THE most important thing to consider in a security plan is to understand the properties and behavior of the assets being protected. In any computing infrastructure the most important element is the information. In the modern networks and in high-speed processors, large amounts of information can be moved or accessed over thousands of miles in microseconds or even in nanoseconds. Information in the transit is vulnerable to many attacks. To protect information from these attacks security protocols are employed.

The three goals of security protocols to protect the information are confidentiality, authenticity and Integrity. Confidentiality means hiding the information from the unintended recipient so that only the intended recipient can access it. Integrity refers to protect information from modification during transit so that the intended recipient receives the original copy without being modified. Authentication is a process in which principal proves its identity it claims to be [1]. The principal which wants to authorize itself is sometimes referred to as the prover, while the party to whom proof is submitted for identity verification is called verifier.

This paper is focused about one goal of security protocols i.e., authentication. The authentication mechanisms can be classified into three groups, based on the following three criteria

i). Authentication based on what the principal has, such as a physical hardware which may be a token or a card.
ii). Authentication based on something the principal knows, such as a password or a secret.
iii). Authentication based on something the authentication party is, such as a physical characteristic of the link it is attached to.

The rest of this paper is organized as follows: Next section presents a survey of the related work. In section III we present the comparative study and quantitative analysis of Extensible Authentication Protocols used in WLANs. Section IV gives the design of the proposed protocol, security analysis of it and the performance analysis. Finally, section VI concludes this paper.

II. RELATED WORK

This paper is in continuation of the previous work which was published in [2], in which authentication delay associated with EAP Protocols was evaluated. It was observed in [2] that more complex protocols have greater authentication delay associated with them. The motive of this paper is to propose a highly secure authentication protocol at the same time having least authentication delay and least energy requirements so that the user gets access with least time involved and reduced consumption of battery power. Jyh-Cheng Chen et.al has presented the technical details of the Extensible Authentication Protocol and IEEE 802.1x [3]. They have analyzed and developed an open source implementation of IEEE 802.1x [4] client and various EAP-based authentication mechanisms called WIRE1x [5].

Mishra and Arbaugh have discovered some weaknesses of 802.1x [6]. According to them, the main problems are mutual authentication and key distribution between Access Point (AP) and supplicant. Yen-Chieh Ouyang et.al has proposed a new

scheme to construct a secure channel for regular communication security [7].

Mohammad Abdul Azim et.al has proposed a mutually authenticated key agreement protocol. The protocol employs elliptical curve digital signature algorithm and elliptic curve Diffie-Hellman exchange intended for mutual authentication and key exchange respectively [8].

The literature survey reveals that most of the researchers have proposed the protocols for authentication and key exchange; however the impact of these protocols on the performance of the WLANs has not been considered. This paper proposes a mutual authentication protocol and compares the proposed protocol with the other EAP authentication methods. The proposed protocol EAP-SAM is having least complexity and good security features which are discussed in section IV.

III. QUANTITATIVE ANALYSIS OF EXTENSIBLE AUTHENTICATION PROTOCOLS

The authentication in WLAN's involves three parties that are: the supplicant, which requests for authentication; the authenticator, which grants access; and the authentication server (AS), which verifies supplicant credentials. The EAP [9], is used to carry the credentials required to authenticate the clients. EAP is a flexible protocol as it separates the exchange of messages from the process of authentication by providing an independent exchange layer called EAPoL. By virtue of this feature, it achieves the orthogonal extensibility, which means that the authentication processes can extend i.e., a newer mechanism can be adopted without changing the EAP layer. This feature of EAP has been utilized in proposing the EAP-SAM protocol. The EAP protocol provides a common platform to various authentication methods like EAP-MD5, EAP-TLS, EAP-TTLS, PEAP. The authentication methods which are quantitatively analyzed in this section are EAP-MD5, EAP-TLS and PEAP.

The EAP-MD5 is a Challenge Handshake Authentication Protocol (CHAP). In the EAP-MD5 a random challenge is generated by AP and is sent to the supplicant. The supplicant responds back to the AP with a message, which contains the hash of the challenge using a secret key. The authentication server verifies the hash and as a result of verification either accepts or rejects the authentication request. If accepted, the supplicant gains access to the services provided by the AP otherwise the access is denied. Fig. 1 shows the message exchange of the EAP-MD5 authentication method.

EAP-MD5 is associated only with authentication. Once the authentication is performed, the messages exchanged between AP and Supplicant are transmitted in clear text. It is also a unilateral authentication protocol; which means only the client is authenticated and the server side (authenticator) is not authenticated; therefore, it cannot detect a rogue AP. The advantages of EAP-MD5 are that it requires only lightweight processing which does not involve key determination and also does not require a certificate infrastructure to manage certificates.

The number of messages exchanged between AP and AS in case of EAP-MD5 is 4 and the number of messages transferred between client and AP is 6. Thus the total number of authentication messages are 10, and the round trip times (RTT) involved between AP and AS are 2.

AP-MD5 is confined only to unilateral authentication and there is no support for key derivation which is an important factor of security protocols against attacks. EAP-TLS [10] overcomes limitations of EAP-MD5 by introducing mutual authentication and providing an encrypted transport layer.

EAP-TLS uses digital certificates for authentication and thus requires an infrastructure which will manage the processing of these certificates. EAP-TLS employs selected parts of the TLS protocol that is defined in RFC 2246. The Fig 2 shows the message exchange of EAP-TLS.

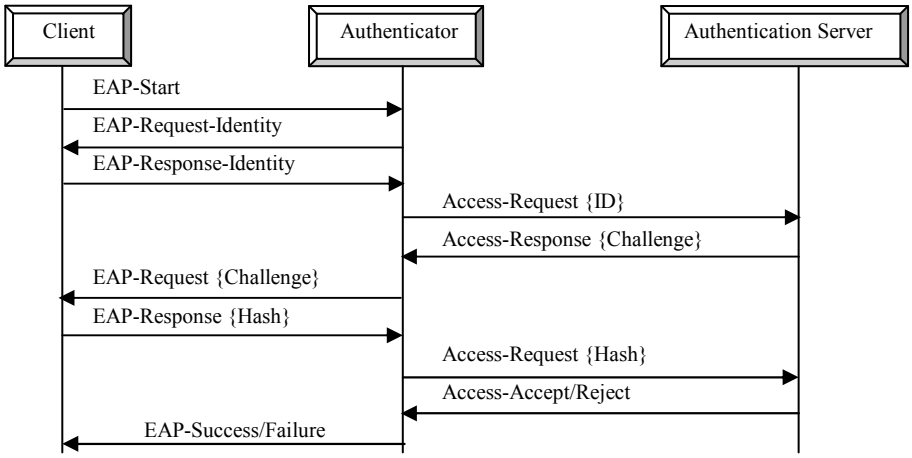

Fig. 1: EAP-MD5 Message Exchange

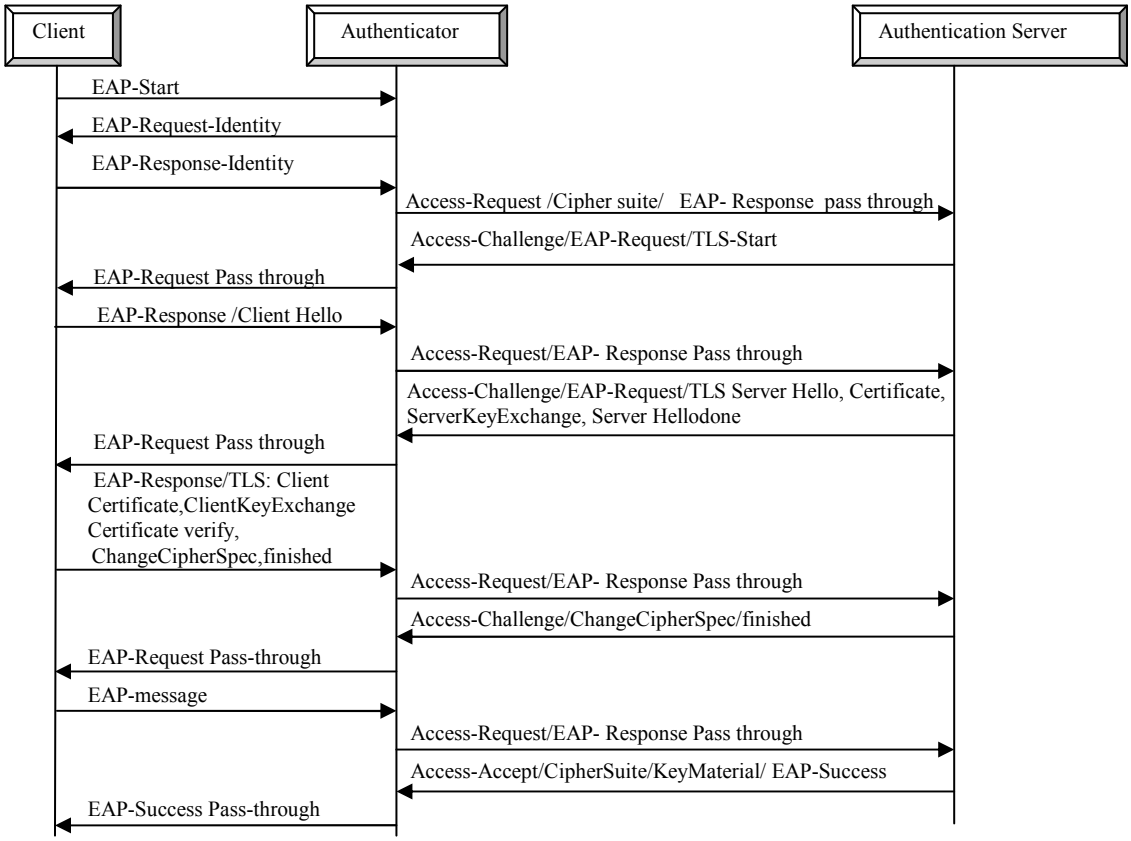

Fig. 2: EAP-TLS Message Exchange

The client initiates the authentication by sending an EAP-Start frame. AP responds back with EAP-Request Identity. The client passes its identity to the AP which in turn passes it to AS. The AS begins the handshake with the EAP-TLS-Start followed by Client hello and Server hello, Server Certificate, Server Key Exchange and Server hello done messages. Once the security parameters from server are transferred to client the client replies with Client Certificate, ClientKeyExchange, Certificate verify, ChangeCipherSpec and finished message. At the Server end if everything goes fine and the client certificate is valid then the authentication was successful and the EAP-Success message is passed to client. The number of messages exchanged between AP and AS in case of EAP-TLS is 8 and between client and AP are 10. Thus, the total authentication involves 18 messages and 4 RTT's between AP and AS.

There are number of drawbacks with the EAP-TLS which are need for client certificate, user identity protection, and protocol efficiency [11]. To overcome these limitations new methods called tunneled versions of EAP are used, one of which is PEAP.

PEAP [12] overcomes the limitations of EAP-TLS, by securing the open exchanges, and adds flexibility by facilitating any of the EAP mechanisms over the secure channel. Certificates are required only for servers. It uses TLS and extends the authentication beyond finished message so that the client is authenticated and key is derived. The client authentication can use any of the legacy EAP methods which satisfy the policy of organization. Fig. 3 shows the message exchange of PEAP. It involves two phases: phase 1 performs the server authentication and tunnel establishment and in phase 2 the client is authenticated using any of the legacy-protocols and the key is derived. There are certain drawbacks associated with PEAP which include, certificate infrastructure required for servers, more number of authentication messages.

The number of messages exchanged between AP and AS in case of PEAP-MSCHAP is 12 messages and the messages exchanged between client and AP are 14. Thus, the total authentication involves 26 messages and 6 RTT's between AP and AS.

Thus the messages involved in PEAP authentication and key derivation are very high as compared with other protocols.

IV. PROPOSED PROTOCOL: EAP-SAM

The design of proposed protocol is simple as compared to the other protocols discussed earlier in this paper and does not require CA, so we have named the protocol as EAP-Simple Authentication Mechanism (EAP-SAM). EAP-SAM also involves three entities which are, supplicant, AP and AS. AS generates a secure key and delivers it to supplicant and AP.

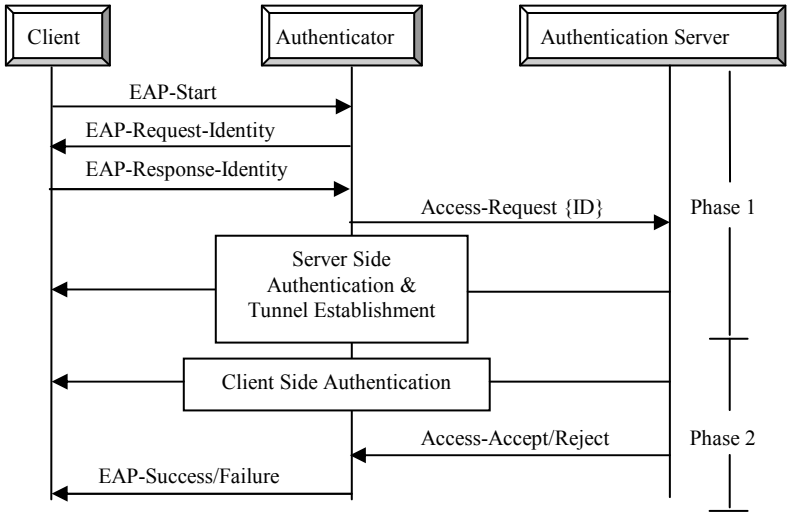

Fig. 3: PEAP Message Exchange

In the proposed mechanism, we assume that the AS and client shares the secret key K_c and AS and AP shares another secret key K_a. The message exchange in EAP-SAM is shown in fig. 4 and consists of the following steps

Step 1: Like other authentication mechanisms, the client sends an EAPoL-start frame to the authenticator.

Step 2: The AP requests the ID of the client.

Step 3: The client responds by sending its ID to the AP.

Step 4: The AP encapsulates the ID of the client in the RADIUS/DIAMETER format and sends it to AS. After receiving the client's ID, the AS will check the client's ID, if it is valid then it will generate the session key $K_{c,a}$ and the associated lifetime of the key and starts constructing message-5. If client ID is not valid the Access-Reject is passed to the AP.

Step 5: The AS will generate message-5 containing session key having format as shown below and sends it to the client

message-5 = E_{Ka} [TS1, LT1, $K_{c,a}$, E_{Kc} (H1, LT1, $K_{c,a}$,TS1)]

Where LT1 = Lifetime of session key.

H1 = MAC (K_c, [$K_{c,a}$,TS1, LT1]).

E_K = Encryption using key (k).

Step 6: The AP will decrypt message-5 and passes portion of message-5 encrypted with K_c to the client adding $E_{Kc,a}$ (TS1) to it as

message-6 = $E_{Kc,a}$ (TS1) || E_{Kc} (H1, LT1, $K_{c,a}$, TS1)

After receiving message-6 the client will decrypt the portion of the message encrypted with K_c and also will compute the hash on the received message and will compare it with the received hash. If the two are same then the message is accepted otherwise it will be discarded. After obtaining $k_{c,a}$ it will decrypt first portion of message-6 to obtain TS1 which is same as in the second portion of the message-6, this confirms that the AP is having the same session key as that of the client. After message-6, since both the AP and the client are having the shared secret then the 4-way handshake takes place.

The number of messages exchanged between client and AP in case of EAP-SAM is 4 and the number of messages between AP and AS is 2. Thus, the total authentication involves 6 messages and 1 RTT between AP and AS.

A. Security Analysis of Proposed Protocol: EAP-SAM

EAP-SAM has number of advantages which include the following

Reduced number of authentication messages: The key establishment methods are used to set up keys between communicating entities. Methods of symmetric key establishment can be grouped into three categories: Key transport, Key agreement and Manual key establishment. In key transport, a key server (or AS) generates the key and then delivers it to the AP and the Client. On the other hand, in key agreement, the server and the client exchange parameters. The exchanged parameters are then processed through a common procedure to derive the key. The authentication methods like EAP-TLS, PEAP correspond to this scheme. The strength of the key agreement approach is that the authentication entities can contribute to the key generation. However, this contribution of authentication entities requires additional processing which causes an increased authentication delay. This extra processing is not required in the key transport technique, which simplifies the entire authentication. In case of manual key establishment, the keys are installed on the communicating entities manually. The proposed scheme belongs to the key transport category. In WLAN, the client can be a PDA having limited computational and storing capability and can be very sensitive to the authentication delays, hence using EAP-SAM can be a good solution in such cases.

Defense against Rogue AP attacks: In the proposed protocol the attacker cannot gain access to the message exchanged between the AS and the AP as it is encrypted by the K_a, which is only known to the legitimate AP and the AS. So, rogue AP will not be able to intercept the communication.

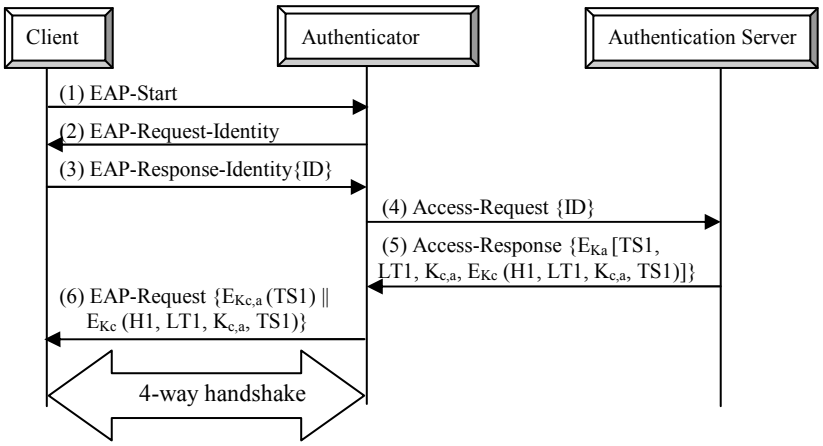

Fig. 4: EAP-SAM Message Exchange

Withstanding Message Integrity attacks: In EAP-SAM the AS computes the hash over the various fields sent to the client, any intruder gaining access to the message can change its contents but due to the hash the client will be able to detect the modifications. So, our proposed scheme withstands the message integrity attacks as well.

Trust relationship between the AP and client: In our proposed scheme we are having three network entities; Authentication Server, AP and Client. Both AS and AP and AS and Client trust each other as these are sharing a secret k_a and k_c respectively, and then using these secret keys a trustworthy relationship can be established between client and AP. This is achieved when AS generates a secure key and delivers it to AP and Client. AP and Client authenticate each other with the key obtained from AS.

Defense against Replay attacks: An attacker can use a previously sent message by the AS to the client to gain access but in EAP-SAM time stamps (TS1) and lifetimes (LT1) prevent such forgeries.

In EAP-SAM protocol the only limitation is that the AP has to perform additional processing which is due to the symmetric encryption and decryption. However, these processing delays are very small and can be easily tolerated as compared to parameter processing in key agreement.

B. Numerical Analysis

Table 1 shows the comparison of the EAP-SAM protocol with the other Extensible Authentication Protocols discussed in the previous section. The comparison is on the basis of total number of messages associated with each protocol and the round trip times (RTTs) involved between AP and AS. The RTT is considered because the AS can be located remotely. To compare the results, we treated the expected cost of message delivery between the client and AP as one unit since it involves only one hop. Accordingly, the expected cost of message delivery between AP and the AS, is treated to 'n' units, as the server can be located remotely involving multiple hops to achieve centralized control. Let us assume the delivery cost associated with EAP-MD5, EAP-TLS, PEAP-MSCHAP and EAP-SAM is C1, C2, C3 and C4 respectively. The values of C1, C2, C3 and C4 can be computed by adapting the number of messages from table 1 as:

$$C1 = 6 + 4n \quad (1)$$

$$C2 = 10 + 8n \quad (2)$$

$$C3 = 14 + 12n \quad (3)$$

$$C4 = 4 + 2n \quad (4)$$

TABLE 1:
NUMBER OF MESSAGES EXCHANGED IN EACH AUTHENTICATION METHOD

EAP Method	EAP-MD5	EAP-TLS	PEAP	EAP-SAM
Between client and AP	6	10	14	4
Between AP and AS	4	8	12	2
Total messages involved in Authentication	10	18	26	6
RTT's between AP and AS	2 RTTs	4 RTTs	6 RTTs	1 RTTs

Fig. 5 plots these equations using five values of n (=0, 1, 2, 3, 4), n = 0 means that the AS and the AP are co-located. It is quite clear from the plot that the cost associated with PEAP is greater as compared to the other three which is quiet obvious due to complexity of the tunneled protocols. Our proposed design, EAP-SAM being the simplest of the four is having lower slope and higher security features. Thus, our protocol being the most simple will introduce least authentication delay while the other authentication protocol being more complex will have greater delay associated with them [2].

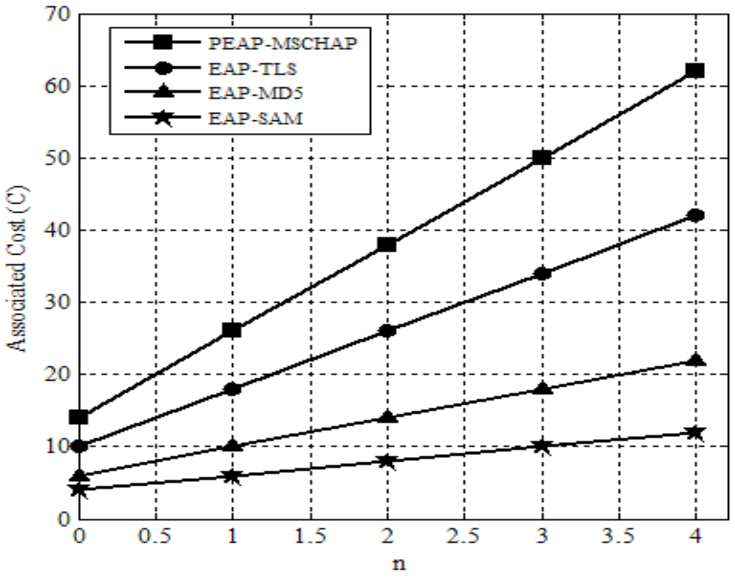

Fig. 5: Comparison of associated cost with each protocol

V. CONCLUSION

The authentication is an important issue in securing WLANs from session hijacking and unauthorized access. To safeguard WLANs from attackers authentication protocols are used. These authentication protocols act as filters to check the legitimate users but at the same time they have a direct impact on the user satisfaction as the user has to wait authentication to complete to get granted access. The authentication delay will also have an impact on Quality of Service in case of the time sensitive application like real-time applications. To reduce this delay the number of messages involved and the computation complexity in the authentication protocol should be less, but at the same time should be secure enough to protect WLANs from the attackers.

We have proposed an authentication protocol having minimum number of message exchanges between authentication entities and less computational complexity. The total number of authentication messages involved in our proposed scheme EAP-SAM is 6 which are very less as compared to the most secure tunneled authentication protocol PEAP which involves 26 messages. The delay involved in authentication is reduced significantly in EAP-SAM as it requires only one RTT between AP and the AS whereas PEAP involves six RTTs, EAP-TLS involves four RTTs and EAP-MD5 involves two RTTs. EAP-SAM is also having good security features like defense against Rogue AP attacks, withstanding message integrity attacks, defense against the replay attacks and the mutual trust relationship between client and AP.

REFERENCES

[1] Bernard Menezes, "*Network Security and Cryptography*", CENGAGE learning 2010.

[2] Suhail Ahmad, Ajaz Hussain Mir, Ghulam Rasool Beigh "Latency evaluation of Extensible Authentication Protocols in WLANs", 5th International Conference on Advanced Networks and Telecommunication Systems (ANTS), 18-21 Dec-2011.

[3] Jyu-Cheng Chen and Yu-Ping Wang, "Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience", IEEE Radio Communications, Dec 2005.

[4] W.-K. Chen IEEE Standard for local and metropolitan area networks, "Port-based Network Access Control", IEEE Std. 802.1x, 2001 Edition (R2004).

[5] Wire1x software, [Online]. Available: http://wire.cs.nthu.edu.tw/wire1x/

[6] A. Mishra and W. A. Arbaugh, "An initial Security Analysis of the IEEE 802.1x standard", Dept. of Computer Science University of Maryland, Feb 6, 2002, CS-TR-43228.

[7] Yen-Chieh Ouyang, Reay-Lin Chang and Ji-Hau Chiu, "A New Security Key Exchange Channel for 802.11 WLANs", Int. Carnahan Conference on Security Technology, IEEE 2003.

[8] Mohammad Abdul Azim and Abbas Jamalipour, "An Efficient Elliptical Curve Cryptography based Authenticated Key Agreement Protocol for Wireless LAN Security", IEEE 2005.

[9] L. Blunk, J. Volbrecht, RFC 3748, "Extensible Authentication Protocol (EAP)" IETF Website [online]. Available: http://www.ietf.org/rfc/rfc3748.txt

[10] D. Simon, B. Aboba, R. Hurst, RFC 5216, "The EAP-TLS Authentication Protocol" March 2008

[11] Madjid Nakhjiri and Mahsa Nakhjiri's, *" AAA and Network Security for Mobile Access"*, WILEY 2006.

[12] A. Palekar et al., "Protected EAP Protocol (PEAP), version 2" IETF internet Draft, Oct. 2004, [Online]. Available: draft-josefsson-ppext-eap-tls-eap-10.txt.

Suhail Ahmad received the B.E degree in Computer Science Engineering from the Kashmir University, India, in 2008, the M. Tech degree in Communication and Information Technology from National Institute of Technology, Srinagar, India, in 2011.His research interests include Network Security, Wireless Networks and Computer Networks.

Ajaz Hussain Mir is Professor and Head of Electronics and Communication Department, National Institute of Technology, Srinagar, India. He received the PhD and M. Tech degree from IIT-Delhi. His main research interests include Network Security, Computer Networks and Image Processing.

Ghulam Rasool Beigh is Assistant Professor in National Institute of Technology, Srinagar, India. He received the M. Tech and B. Tech degree from National Institute of Technology, Srinagar, India. His main research interests are Cognitive radio, Network Security and Computer Networks.