International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-5, June 2014

Analysis and Literature Review of IEEE 802.1x (Authentication) Protocols

Umesh Kumar , Praveen Kumar, Sapna Gambhir

Abstract— This paper gives us detailed study of some of the commonly used EAP authentication protocol. But before understanding these authentication methods we have to understand what EAP is and how EAP work because it's all start with EAP. So our aim in this paper is to provide detailed study of EAP and its architecture. This paper also covers literature review of authentication protocols. EAP is a frame work and it consists of different types of protocols nearly forty but we will study only those protocols which are very common in use and also their advantages and disadvantages.

Index Terms—EAP, MD5, LEAP, TLS, TTLS, PEAP.

I. INTRODUCTION

The IEEE 802.11 standard is most popular standard for WLANs.802.1x protocol known as Port based protocol and proposed by IEEE. Its main task is to solve WLAN user authentication. Authentication is the process of verifying user's identities when they want to use the server resources. There are different types of authentication methods but before study these we have to understand the basic mechanism of its working.

II. EAP OVERVIEW

EAP [1] is stands for Extensible Authentication Protocol. But it is not a protocol it is a frame work on the basis of that different type of protocols are derived and new protocols can easily be added in that frame work. It is defined in RFC 3748 [10]. EAP originally develop for PPP (Point to Point Protocol). EAP is a package agreement between client and server. This can choose any of the protocols present in the EAP frame work. But both sides should used same protocol for authentication and communication. But there is different type of security [3] issues related to EAP protocols. EAP mainly consists of 3 main components as shown in figure 1.

a. Client/Supplicant,
b. AP (Access Point)
c. AS (Authentication Server).

Client/Supplicant: Who wants to join the wireless network.
AP (Access Point): It is a Radio Station that receives the wireless signal and sends these signals to wired network. It serves as a broker between client and server. Initially block the client because it not verified the identity of the client.

Manuscript published on 30 June 2014.
* Correspondence Author (s)
Umesh Kumar*, Assistant Professor, YMCA University of Science and Technology, Faridabad, India.
Praveen Kumar, Research Scholar, YMCA University of Science and Technology, Faridabad, India.
Dr. Sapna Gambhir, Associate Professor, YMCA University of Science and Technology, Faridabad, India.

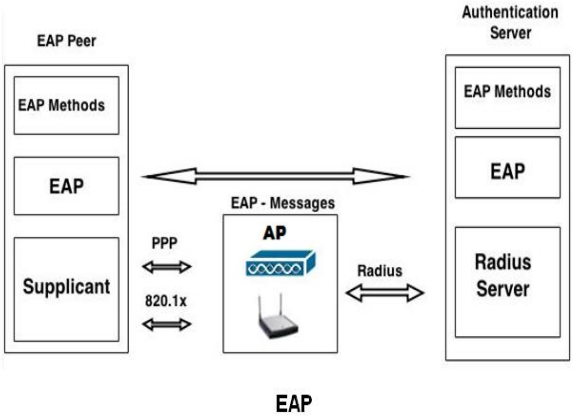

Figure 1

It consists of two logic ports: controlled port and non-controlled port. If the user is certified then controlled port is used but when user is not certified then non-controlled port are used for communication.

AS (Authentication Server): Authentication Server also called RADIUS [2] (Remote Authentication Dial in User Services). It is the remote server where user's account information is store. When any user wants to connect to the server first server checks the existence of that user on server. If the user is certified then authentication server sent the information to access point and establishes a dynamic access control list.

AUTHENTICATION METHODS OF EAP: This section describes commonly used authentication protocols and their properties.

A.EAP-MD5 [1]: MD5 is based on *one-way hash function.* Hash function is nothing but a cryptographic checksum. It takes an arbitrarily long input message and produces a pseudo-random output called hash. One of the advantage of hash is mathematically it is difficult to find the same message which can produce the same hash. MD5 takes arbitrary length input and produces an output of 128-bit which we call **figure print** or **message digest**. In MD5 message is not store in plain text format on server side. When a user creates his/her account on server and type password then server take hash of that password and store it. Next time when user want to login to the server then user have to enter the password. The MD5 protocol that present on client side converts that password into hash value and forward to server. Now server receives the hash from client. It compares the hash values which it gets from client and stored at server and according to that result is out. One of the most important advantages of MD5 is its implementation which is quite easy as compare to other protocols. A simple challenge and response based method is used to check the validity of the user in the network.

But MD5 also suffers different type of disadvantage like in WLAN attacker can easily sniff a client identity and password hash. It also suffers from reply attack. MD5 also does not support mutual authentication. It only checks the client validity not server. There is no session key is used in the complete communication phase. So from the above discuss we can conclude that it is not recommended for authentication method in WLANs.

B. EAP-LEAP [4]: LEAP (Light Weight Extensible Authentication Protocol): LEAP is developed by Cisco to deal the weaknesses of WEP's. It is based on challenge /response model. LEAP consists of following feature:

a. It provide mutual authentication mean both side check for validity.
b. A temporary session key is derived.
c. It has high speed of computation.
d. It is also compatible with existing and well-known authentication methods.

Initially a secret key is shared among client and authentication server. First the client sent the random challenge to server encrypted with pre shared session key. If the server is valid then it has the secret key and by using that it can decrypt the challenge. AS responds to the client. The client decrypt the response of AS and compare it to the challenge response. If response matches the challenge then validity of server is verified. In similar way the validity of client is also check. As both verify each other then mutual authentication is successful. The information exchange between client and server during authentication process on the basis of that a temporary session key is derived. Now both client and the authentication server use the session key to encrypt the communication between client and server. The main advantage of LEAP is mutual authentication and a session key derivation. But there are some disadvantages also like it does not provide client identity protection because identity of client is sent in plain text form. It is also suffer from dictionary attack.

EAP-TLS [6]: TLS (Transport Layer Security) defined in IETF RFC 2710 [5] and developed by Cisco system Netscape communication. TLS is based on Digital certificate. In this we consider a trusted third party which issues certificate to client and server but for that it will charge some amount of money on regular basics. It uses PKI (Public Key Infrastructure) to authenticate both user and server. It consists of two phases:

a. TLS record protocol
b. TLS handshake protocol

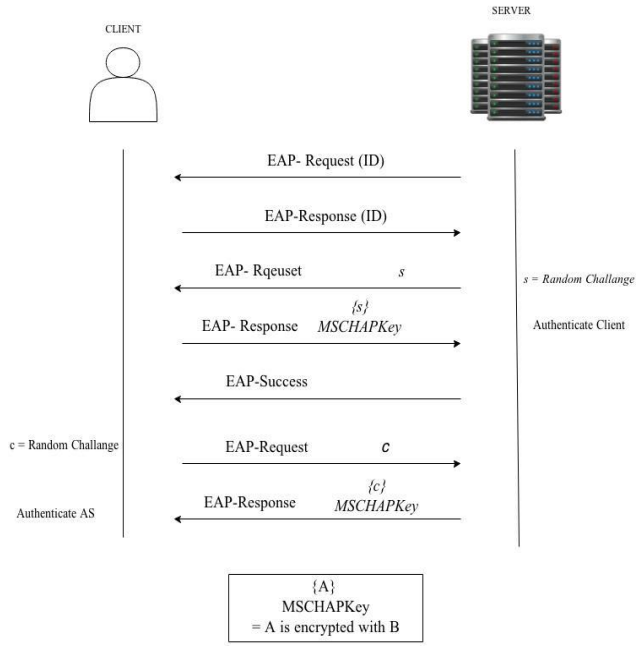

Figure 2

TLS record protocol: The connection is confidential and for data encryption symmetric keys are used. These symmetric keys are unique for each connection and it is based on secret negotiation by using another protocol such as TLS handshake protocol. Many higher level protocols used TLS record protocol for encapsulation.

TLS handshake protocol: It main task is to provide connection security. It also allows both client and server to authenticate each other. And also helps to negotiate on both algorithm as well as key used in communication. It has following properties:

a. Client is identified by its public key.
b. Negotiation on shared secret among client and server is always secure.
c. Negotiation should be secure so that no attacker can make any type of change without the permission of both client and server.

EAP-TLS is consider one of the best authentication protocol for WLANs but the used of client certificate make it costly because to get certificate from third party client have to pay.

C. EAP-TTLS [7]: Tunnel Transport Layer Security is developed to overcome the TLS issues the client certification. It similar to TLS but only server requires the certification from third party not client. Tunnel has two advantages first it allows us to use less secure legacy protocol for authentication of client. And also using tunnel the identity of the client is hide. Like other tunneling protocols TTLS also consist two phases:

a. Phase 1: Used server certificate to check the validity of server and establish a symmetric encrypted tunnel.
b. Phase 2: In this phase we verify the client identity by using another protocol but this identity check take place inside the tunnel so that identity of client can be secure. The second protocol to verify the validity of client can be EAP methods or legacy methods like CHAP, MSCHAP, MSCHAPv2, PAP etc.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The main use of tunnel is to protect the authentication methods which validate the client. As the validity of client is verified the tunnel gets collapses. Now its client and server job to establish secure communication by using WEP encryption tunnel. EAP-TTLS provides high security during authentication and all support EAP and other legacy methods for client authentication. Implementation cost of TTLS is less then TLS because client certificate is not used in this protocol.

D.EAP-PEAP [8]: Protected Extensible Authentication Protocol also called as EAP inside EAP. It is also a tunnel approach. Similar to TTLS it also used server certificate to check the validity of the server. TLS based tunnel is used to provide encryption and authentication. Various types of attacks are avoided because the message is encapsulate inside the tunnel. PEAP operates in two phases.

a. First phase client validate server the by its server certificate and then TLS session is negotiated and establish
b. Second phases server validate the client by using only EAP methods not legacy.

In short we can say that when PEAP used in WLANs client validate the server by its certificate then a secure tunnel is formed. Now it's time to validate the client by using by using any of EAP method and these methods are protected by TLS tunnel.

III. LITERATURE REVIEW

After discussing about the IEEE 802.1x Introduction, its working and architecture in this section we are briefing about Literature Survey on the various solutions proposed by Researchers / Authors, and which problems still exists.

Jhy-Cheng Chen and Yu-Ping Wang [11] mentioned implementation of different type of EAP (Extensible authentication Protocol) techniques. Implementing these techniques is quite complex but in this paper it is shown that by the help of WIRE 1x we can do easily. It is an OPEN SOURCE implementation of client side because if client side is strong then communication is more secure. These WIRE 1x easily work with windows and it supports nearly all of the Authentication mechanisms defined in EAP. WIRE 1x also provide secure manner of communication for user who is using WLAN. It is release in worldwide on 18th June 2003. And from that date large no. of people visited and downloads the source code for different EAP techniques. This paper define all components of WIRE 1x. It also defines some of EAP techniques like EAP- MD5 EAP- TLS EAP- TTLS EAP- PEAP and also a comparison table has been derived. It also tell about different open source libraries like WinPcap, Libnet, Openssl.

Bahareh Shojaie, Iman Saberi and Seyyed Morteza Alavi [12] has done study of EAP-TLS to compare two type of Extensible Authentication Protocol – transport layer security (EAP-TLS) so that another technique can be provided by using cryptographic methods. The new technique used Elliptical Curve Digital Signature Algorithm (ECDSA) and SHA-256 to provide very high security and also high performance. It also compare it with the existing EAP-TLS method and show that the new techniques provides strong security, high speed and more efficiency by using same level of memory as compare to EAP-TLS. New methods provide a balance between security and optimized uses of resources and time.

Bakytbek Eshmurzaev and Gokhan Dalkilic [13] mentioned important concept of WLAN i.e. authentication. EAP consist of different type of methods for authentication. But shared key and Certificate based methods provide more security to user. This paper mainly concentrate on EAP-FAST because others methods like TLS uses shared secret keys other than certificate due to which performance of EAP-FAST (Flexible Authentication via Secure Tunneling) is greater the other EAP technique. In this other EAP technique like EAP-TLS, EAP-PEAP, EAP-TTLS are also study. In this also EAP-FAST is validate using different scenarios of EAP-FAST protocol using AVISPA model checker.

Khidir M. Ali and Ali Al-khalifah [14] shows that Extensible Authentication Protocol (EAP) supports variety of upper layer authentication layer protocols each have some advantage and disadvantage. This paper gives an overview of most commonly used EAP authentication methods. The main advantage of this is that by help of this comparative study we can choose technique which is more reliable for communication and which one is worse. Also explain these techniques in details so that user can easily understand these techniques. And at last a comparison table is drawn using different properties. Techniques are MD5, LEAP, TLS, TTLS, PEAP, and FAST.

Shyamala Kumari and M. Deepa Rani [15] has shown that user password have tendency to be stolen and different type of attacks on that can be made. 1st thing is that password chosen by the user is a weak one. So that it can easily be remember and small in length and 2nd is reuse that same password at different sites. Due to which an attacker can launch steal his password by different methods like key loggers, malware and phishing. This paper uses secrete pass-phrase which not cross the network not even authentication phase due to which it is resistance from replay attack and also no secret information is store on any system neither client nor server. Security of the system is hash based such that hash function is non invert. Such function should be tractable to compute in forward direction but also infeasible to invert. In this technique mobile and SMS service is used to avoid stealing password and also password reuse attack. The main advantage is that registration phase and login phase consume less time.

Albert Fernandez-Mir, Jordi Castella-Roca and Alexandre Viejo [16] talks about new technology Radio Frequency Identification (RFID) which is used to identify a remote object by its radio waves. It is used in many applications and it also reduces the huge cost of production processes. It also provides a secure mechanism to prevent attacker to misusing the information. In this technique the server uses the concept of tags. Tags are present both side but more tags are at server side and also management of tags is done at server side so due to which there should be synchronization between client and server must be there. In this a comparison table is also there to compare this technique to other technique. It has two main advantages

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

(a) improves scalability at server side
(b) level of resistance to resynchronization attacks can be configured.

Jing-Wei Zhou and Sheng-Ju Sang [17] shows that in recent year large number of application are developed for WLAN. But different types of issues related to security are also coming in WLAN. To provide security we need a secure authentication protocol like PEAP. This paper mainly talks about Protected Extensible Authentication Protocol (PEAP). It also talks little about EAP-MD5, EAP-TLS and EAP-TTLS. But its main concern on PEAP how its authentication process take place what are the defects in EAP-PEAP and how we can improve PEAP so it can overcome through these defects.

P. Bachan and Brahmjit Singh [18] proposed a new authentication protocol. As the popularity of IEEE802.11 WLAN standard goes up authentication becomes more and more important. To provide security a new protocol re-authentication protocol in introduced. It provides consistent method independent and low latency to WLAN. The main work is to compare it with EAP-TLS and calculate the security cost of it with different speed. In this analysis of physical layer authentication algorithm to find its channel probing, hypothesis testing and compare it with the proposed protocol. And after that an enhanced physical layer schema which worked with moderate terminal mobility is given. In this whole process MATLAB tool is used. It works efficiently in to avoid spoofing attack.

Kenneth G. Paterson and Douglas Stebila [19] shows that to minimize the damage cause by spyware attack, phishing security sensitive industry considers One Time Password (OTP). The main advantage is that the different password is sent every time by server to client to login to server. OTP can only be used once due to which it avoided reply attack. In this paper a new thing is use OTE derived password authentication key exchange by which mutual authentication, session key is achieved. In this also a new technique to generate OTP is used and securely deliver to client a session key is derived that give security to protocol. This protocol is called Password Authentication key Exchange (PAKE).

Bayalagmaa Davaanaym , Young Sil Lee , HoolJaeLee , SangGon Lee and Hyo Teak Lim [20] OTP is one of the best concepts for authentication method to check the validity of the client. But the main thing which is important is that algorithm which is used to generate OTP. If it is secure then guessing the next password by looking previous series of password is not possible. Which make him more secure. In this paper to generate OTP Ping Pong-128 stream cipher method is used. Ping Pong is a strong stream cipher function which generates temporary OTP. Ping Pong used two mutually clocking memory bit LFSRs which are length 127 and 129 bit and second single memory bit. In this paper both algorithm and its implementation are given.

Thomas Guillet , Rim Moalla , Ahmed Serhrouchni and Abdelatif Obaid [21] mentioned that security of information store in system is becoming more and more important because large and different types of attack are occurring every day. Present methods of authentication are challenge and response based because in this format information is sent in plain text format. In this paper a new protocol based on HMAC One time password (HOTP) reduces the SIP handshake without changing the signaling. It is challenge and response based. The proposed protocol provides same security as it provided by response and challenge based protocols. It is more popular in Voice over IP protocol (VoIP).

Wen-Bin Hsieh and Jenq-Shiou Leu [22] shows that OTP is one of the secure method for authentication but the main problem arise is which method or algorithm is used to generate OTP. In this paper a new way of OTP generation is given in which time and location of a person is used to generate OTP. It increases the security as the it restrict the validity of OTP in certain time period but also geometric location so that security is provided if user is not at its location then another algorithm is proposed is used to avoid such type of situation. In this paper also a comparison table is drawn to compare the proposed protocol and how it is better than the pre existing protocol.

LI Tong Liang and JIN Zhi Gang [23] said that to secure information authentication is very important term. This paper gives a new authentication schema based on the hashing and it is also economically very good. In this scheme user have to remember a random number that number is also the part of username and password. Every time a random number make this schema difficult for attacker and also hide the identity of the user. It also supports the mutual authentication by mutual authentication the freshness is maintained. In this schema the hashing is done every time rather than plain text. It also defends many type of attacks by which other techniques suffer. A session key is also derived for communication by exchange of a random number. This session key increases the security of this schema.

Anjani K. Rai, Shivendu Mishra and Vimal Kumar [24] discusses that worldwide interoperability for micro wave access (WiMAX) is wireless technology for MAN (metropolitan area network). 802.16e support EAP. In EAP methods EAP-TLS is one of the best method and also secure. But the main drawback is that it requires certification from 3rd party to both client and server. Getting certification from 3rd party is quite costly it is not one time but client and server have to pay some amount after a fix interval of time. This paper provides detail study of some of the common techniques of EAP like EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP. Detailed experiment and observation are conducted to examine the protocols in term of disk usage, computation time and data transmission time. The analysis shows that the identity-based key exchange maintain similar security level as the other protocols, while conveying better performance. Paper main concern on EAP-TLS and on the basis of that it proposed a new protocol and also draws a table which shows comparison between EAP given above techniques and the proposed one. The proposed protocol work using Diffie-Hellman and for hashing SHA-1 is used. The proposed protocol overcomes the drawbacks of EAP-TLS and it is also cost effective.

Myeonggil Choi and Nguyen Thang [25] proposed and implemented a new protocol which is combination of OTP and TLS/SSL. A multi hop mesh network is extension of wireless mesh network by ad hoc network. TLS is used to authenticate the server and make a tunnel for secure communication.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Also hashing is used to generate the OTP. By the help of OTP we can secure our system from different type of attacks like reply attack, dictionary attack and brute force attack. In this paper also the new concept PANA (Protocol for Carrying Authentication and network Access) is introduce and also detail study about it. This proposed and implemented protocol can be used in many mesh networks in real world with less cost and simplicity. In this protocol to generate OTP we can used different type of technique like Hash based, Time synchronization, Developing challenge based OTP, list of password printed on paper.

N. Asokan, Valtteri Niemi, Kaisa Nyberg [26] this paper shows that when a client authentication protocol is tunneled within another Protocol, it is necessary for each end point to show that it has participated in both protocols within the authentication exchange. If this is not verified then the tunneled authentication protocol is susceptible to a Man-in-the-Middle attack. Paper also shown that the required demonstration can be provided in an implicit or explicit way in a form of a cryptographic binding between the tunnel protocol and the authentication protocol. In our proposals the binding facility is execute in the outer tunnel protocol. It requires the authentication protocol to provide some secret key values for the use of the binding. This approach is preferred since it requires minimal or no changes to the EAP protocols. It allows for exile and secure usage of an authentication protocol in multiple authentication environments without the authentication protocol being aware of the specific environment. The cryptographic binding proposed in this paper does not reduce the security of the tunneled protocols in any case. If the inner authentication protocol is a weak authentication protocol based on a weak client secret, the tunnel must be constructed based on server authentication, and the client should not use the same secret in environments Otherwise, the protocol is vulnerable to dictionary attacks, with or without cryptographic binding. Strong authentication methods are not vulnerable to dictionary attacks, and hence should not be restricted to tunneled environments only.

Mark Vandenwauver, Rene Govaerts, Joos Vandewalle [27] this paper explains authentication methods used in different aspects. Like how authentication is done in UNIX. What are the different types of attacks that can be occurs in UNIX. It also defines different type of biometric methods those can be used for authentication like fingerprints, retina, hand geometry, face recognition and also there drawbacks or issues that can be occurs in these authentication protocols. There is another section which called dynamic password which also defines different types of authentication methods which used in network for authentication like time based, challenge-reposed based etc. In this two authentication protocols Kerberos and Sesame explain in detail and also comparison is done between them.

Kristin S. Fuglerud and Oystein Dale [28] proposed a secure and accessible multi mode authentication method for visually impaired that uses a one-time-password. Client plug earphone on mobile phone which allows people who are functional impairment mean unable to view things. As user receive the password by SMS the application install in mobile read the OTP and by help of earphone he can listen the password and then type in the space provided for password. Proposed protocol works well for visually impaired people. Survey is also done to find what the difficulty can face when we implement this authentication method in our real life.

Kwang-Hyun Back, Sean W. Smith and David Kotz [29] described eight desire properties for WLAN authentication protocols. Study of different type of EAP authentication protocols: LEAP, Kerberos, EAP-TLS, Green pass, ID-based cryptographic authentication, EAP-TTLS and PEAP. Paper finds that LEAP, Kerberos are not sufficiently secure due to dictionary attack. EAP-SRP and ID-based privacy lack current implementation for WLANs. EAP-TLS provide strong security if the network are not concern with delegation and identity privacy. Moreover these protocols overcome some of the difficulty of the authentication the client in EAP-TLS (that is, requiring the client to possess certificate issued by CAs and AS trusts). The most important advantage of this paper is it is simple and easy to understand. In this paper protocols are explain by the help of flow diagram between client and server.

Razieh Mokhtarnameh, nithiapidary Muthuvelu, Sin Ban Ho and Ian Chai [30] presented a comparison between SSL, SSH and ID-based key agreement protocols in their authentication and key exchange protocol. Find their security and complexities. SSL is slower than other terms of data transmission time and mutual authentication. While SSL is strong in secure communication on the internet. SSH has less complexity but vulnerable to MITM attack. It is important to understand the capabilities and performance of the existing key exchange protocol in our application. Detailed experiment and observation are conducted to examine the protocols in term of disk usage, computation time and data transmission time. The through study shows that the identity-based key exchange maintain similar security level as the other protocols, while conveying better performance.

Swati Sukhija and Shilpi Gupta [31] described different protocols for securing Wireless LAN. WEP is not able to provide security against various attacks and threats. Then WPA was come into picture which is a temporary solution to the security faults identified in WEP. But it is still prone to various attacks like Beck-tews, ChopChop etc. Thus WPA2 was introduced providing an enhancement over WPA. WPA2 provide strong encryption by using block cipher AES but it is still vulnerable to attack due to sharing of GTK among clients and transmission of unencrypted control and management frames. Also WPA2 does not support legacy hardware unlike WPA.

IV. CONCLUSION AND PROPOSED WORK

We know that the popularity of wireless network is increasing. So our first aim is to provide security against attackers to secure the network. And authentication is one of the most important phases to secure network. In this paper we have discuss EAP (Extensible Authentication Protocol) frame work which consist of different type of protocols there are nearly 40 authentication protocol in this. We also discuss some of those protocols like EAP-MD5, EAP-LEAP, EAP-TLS, EAP-TTLS and EAP-PEAP. We discuss these because these are commonly used protocol in communication according to their requirement.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

And at last we carried out some conclusion that all of above EAP-TLS is one of the strongest protocol among all of them and some protocol use its advantage in there communication phase like TTLS and PEAP. They used server certificate to check the validity of the server. But any protocol in itself is not complete. In our proposed work we will provide a more secure authentication approach that will be based on OTP considering how to send this OTP to the user in a more secure way so that attacker or intruder will not be able to access that.

REFERENCES

[1] Jyh-Cheng and Yu-Ping Wang "Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience" IEEE DEC 2005 ISSN 0163-6804/05.

[2] C.Rigney, et al, "Remote Authentication Dial User Service (RADIUS)," IETF RFC, June 2000.

[3] Samuel Sotillo "Extensible Authentication Protocol (EAP) Security Issues" Dept. of Technology System East Carolina University.

[4] Kshitij R.Mawale, Dhananjay M.Dakhane and Ravindra L.Pardhi "Authentication Methods for WiFi Networks" IJAIEM Vol. 2, Issue 3 ISSN 2319-4847 March 2013.

[5] B. Aboba and D. Simon "PPP EAP TLS Authentication Protocol" IETF RFC 2716, October 1999.

[6] Bahareh Shojaie, Iman Saberi, Mazleena Salleh, Mahan Niknafskermani and Seyyed Morteza Alavi "Improving EAP-TLS Performance Using Cryptographic Methods" International conference on computer & Information Science 2012.

[7] Khidir M.Ali and Ali Al-Khalifah "A Comparative Study of Authentication Methods for Wi-Fi Networks" 3rd ICCICSN November 2011.

[8] Bakytbek Eshmurzaev and Gokhan Dalkilic "Analysis of EAP-FAST Protocol" 34th int. Conf. on Information Technology Interfaces Cavtat, Croatia 2012

[9] Kwang-Hyun Baek, Sean W. Smith, David Kotz "A Survey of WPA and 802.11i RSN Authentication Protocols" Dartmouth Collage Computer Science TR2004-524 November 2004.

[10] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, Ed "Extensible Authentication Protocol (EAP) " IETF RFC 3748 June 2004

[11] Jyh-Chen and Yu-Ping Wang "Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience " IEEE Dec 2005 ISSN 0163-6804/05.

[12] Bahareh Shojaie, Iman Saberi , Mazleena Salleh "Improving EAP-TLS Performance Using Cryptographic Methods " International Conference on Computer & Information Science 2012.

[13] Bakytbek Eshmurzaev and Gokhan Dalkilic "Analysis of EAP-FAST Protocol " 34th Int. Conf. on Information Technology Interfaces Cavtat , Croatia June 2012.

[14] Khidir M. Ali and Ali Al-Khalifah "A Comparative Study of Authentication Methods For Wi-Fi Networks " 3rd International Conference on Computational Intelligence communication System and Network 2011.

[15] C. Shyamala Kumari and M. Deepa Rani "Hacking Resistance Protocol For Securing Passwords Using Personal Device " IEEE Dec 2012 ISSN 978-1-4673-4603-0/12.

[16] Albert Fernandez-Mir, Jordi Castella-Roca and Alexandre Viejo "Secure and Scalable RFID Authentication Protocol " Springer-Verlag Heidelberg 2011.

[17] Jing-Wei Zhou and Sheng-Ju Sang "Analysis and Improvements of PEAP Protocol in WLAN "International Symposium on Information Technology in Medicine and Education 2012.

[18] P. Bachan and Brahmjit Singh "Performance Evaluation of Authentication Protocols for IEEE802.11 Standard " Int'I Conf. on Computer & Communication Technology [ICCCT' 10] 2010.

[19] Kenneth G. Paterson and Douglas Stebila "One-Time-Password-Authentication Key Exchange" Springer-Verlag Berlin Heidelberg 2010.

[20] Bayalagmaa Davaanaym , Young Sil Lee , Hoonjae Lee , SangGon Lee and Ho Teak Lim "A Ping Pong Based One-Time-Passwords Authentication System " 5th International Joint Conference on INC, IMC and IDC 2009.

[21] Thomas Guillet, Rim Moalla , Ahmed Serhrouchni , Abdelatif Obaid "SIP Authentication Based on HOTP " IEEE 2009 ISSN 978-1-4244-4657-5/09.

[22] Wen-Bin Hsieh and Jenq-Shiou Leu "Design of a Time and Location Based One-Time Password Authentication Scheme" IEEE 2011 ISSN 978-1-4577-9538-2/11.

[23] LI TongLiang and JIN ZhiGang "A New Low Cost One Time ID and Password Authentication Protocol Using Popular Removable Strong Devices " 2nd international conf. on Intelligent Networks and Intelligent System 2009.

[24] Anjali K. Rai, Shivendu Mishra and Vimal Kumar "Strong Password Based EAP-TLS Authentication Protocol for WiMAX" International Journal on Computer Science and Engineering Vol. 02,No. 08, 2010, 2736-2741.

[25] Myeonggil Choi, Nguyen Manh Thang "An Exensible Authentication Protocol with Transport Layer Security and One Time Password in Multi Hop Mesh Network" Recent Researches in Business Administration, Finance and Product Management ISSN: 978-960-474-265-3.

[26] N. Asokan, Vaitteri Niemi, Kaisa Nyberg "Man-in-the Middle in Tunneled Authentication Protocols" Nokia Research Centre , Finland, November 2002.

[27] Mark Vandenwauver, Rene Govaerts and Joos Vandewalle "Overview of Authentication Protocols" Katholieke Universiteit Leuven, Belgium.

[28] Secure and Inclusive Authentication with a Talking Mobile One-Time-Password Client "Kristin S. Fuglerud and Oystein Dale" IEEE ISSN 1540-7993/11 March 2011.

[29] Kwang-Hyun Baek, Sean W. Smith, David Kotz "A Survey of WP A and 802.11i RSN Authentication Protocols" Dartmouth College Computer Science Technial Report TR2004-524 November 2004.

[30] Shuhua Wu and Yuefei Zhu "Improved Two-Factor Authenticated Key Exchange Protocol" The International Arab Journal of Information Technology, Vol. 8, No. 4, October 2011

[31] Swati ukhija and Shilpi Gupta "Wireless Network Security Protocols A Comparative Study" International Journal of Engineering Technology and Advance Engineering ISSN: 2250-2459, Vol. 2, Issue 1, January 2012.

Mr. Umesh Kumar, Assist. Prof., YMCA University of Science and Technology, Faridabad, India.
Research Area: Wireless Security

Mr. Praveen Kumar, Research Scholar, YMCA University of Science and Technology, Faridabad, India.
Research Area: Wireless Security

Dr. Sapna Gambhir, Asso. Prof., YMCA University of Science and Technology,Faridabad, India.
Research Area: Wireless