Volume 7, Issue 5, May 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# A Systematic Review of Security Protocols for Ubiquitous Wireless Networks

**Manas Kumar Yogi, L. Yamuna, P. Surayanka**
CSE Department, Pragati Engineering College,
Andhra Pradesh, India

***Abstract— We present in this paper a review of efficient security protocols for ubiquitous wireless networks. Issues pertaining to user privacy ,confidentiality, data integrity are focused upon. Design issues are also considered while implementing robust mobile system architecture so as to eliminate intruders. Then we discuss security protocols like EAP,WEP,802.1x authentication protocol. We also study the comparison between the presented protocols.***

***Keywords— ubiquitous, mobile, security, wireless, authentication***

## I. INTRODUCTION

In modern era wireless networks have emerged as a complex aggregation of network components facilitating multiple options for users to access network , such as WiFi and cellular systems, which have the ability of providing ubiquitous wireless services, anytime, anywhere. Therefore, ubiquitous wireless networks are part of ambient intelligence. The enhanced application of wireless local area networks (WLANs) for attaining of high data transmission speed along with cellular systems for widespread coverage has become a wonderful platform for wireless data communications. For fully supporting the inter connected roaming system for increasing the relevant income along with the resource utilization, needs of full authentication are be deployed so as to realise the potentials of portable devices, in addition to support the mobility of the environments. In the past, WLANs have already exercised an remarkable success rate due to their high data transfer rates and flexible deployment. The users of the mobile systems can access the Internet with a laptop or a portable digital assistant (PDA) with embedded or removable 802.11a/b/g cards with so much of ease , thereby obtaining the services of data communications over the IP backbones. But the issue to be tackled here is that , WLAN systems are incapable of mobility and roaming support functionalities due to local authorization and registration challenges. This drawback is handled by established cellular networks on which many users have depended for ubiquitous access. However, enabling ubiquitous wireless communications introduces many challenges for network management, since a network cannot exercise the functionality of authorization of an unknown user without having the identification of concerned user and history of the mobile user, which may create a security breach in misusing system resources. In specific, as wireless mediums are open in nature and due to high degree of the mobility of roaming terminals, along with the use of IP backbone networks, sensitive data are heavily prone to attacks. As obvious is the fact that security issues can occur in both wired and wireless networks, the prevalent dangers in wireless field are far greater than those present in the networks which use wired medium.

Multiple security risks exists in ubiquitous, wireless networks, few are user identity privacy, data integrity, and confidentiality . In this paper, we have presented the issue of authentication and security protocols for wireless networks. Authentication is evidently a security mechanism, which is so designed that it can protect networks in case a incoming request of fraud nature occurs. In such a scenario the validity of such incoming transmission, a message, or the real identity of the originator is performed. The authentication process involves , verification of the user's credentials. For instance when a mobile component requests a particular service from a network other than its home network , it has to essentially furnish the individual data for authorization and then only it will be able to register its locations to the new network for subsequent service. This mechanism of functional authentication and registration determines a crucial role in protecting the confidentiality and integrity of wireless networks by not accepting a illegal transmission and prevention of intrusions is also established .Therefore, it can be rightly advocated that the robustness of authentication quality has a huge effect on network security as well as the mobility management in wireless data networks. Authentication makes sure that k resources of a network are used by authorized users only and to prevent the usage of resources from any unauthorized activity or damage. Second, authentication also takes care of issues regarding communication of login credentials for secure interactions. As known well, the main work of authentication protocols is to authorize networking access, but it also has important role in contributing on the the quality of operational service, due to the fact that authentication mechanisms load the wireless systems with signalling overhead. Also known is the fact that ,the latency introduced by authentication strategies may enhance loss of packets and in couple of cases may result in reduced wireless system throughput.

 

Authentication as a procedure to authorize mobile users involves two major issues: the design of intended architecture for authentication and authentication protocols. The former is concerned with what entities are needed for authentication and how to distribute them in different networks, while the latter is concerned with signalling messages used for transferring requirements and credentials. Hence, we discuss the background of authentication and design principles for wireless networks in Section 2. Subsequently we introduce an overview of authentication architecture for the combination of 3G and WLAN systems in Section 3.

For 3G systems such as UMTS, mobile services are secured by a subscriber identity module (SIM). A SIM includes subscriber-related information, consisting of its identity, authentication key, and encryption key. The subscriber identity and authentication key are used for authorization of mobile access. In UMTS, authentication is in place by a shared secret key between the SIM on a mobile device and an authentication center (AuC). This mechanism follows a challenge/response protocol combined with a sequence-number-based protocol for network authentication derived from ISO/IEC 9798-4. In UMTS, authentication is generally done with the help of the registration functionality ,a activity for user validation for the relevant records in a centralized database which contains home location register (HLR); AuC, call origination, a process of originating an outgoing call; and call termination, a process of receiving an incoming call. Therefore, security architecture and authentication functions are embedded in 3G systems. In other words, there are no separate protocols or architectures for authentication in 3G systems, which is one of the features of centralized cellular systems.

For distributed or localized wireless systems, Mobile IP is advocated by the international committee, IETF .It is a protocol working at network layer to provide macromobility in WLAN systems, which is considered as a networking protocol by 3GPP2 for 3G cellular systems. In Mobile IP, each mobile node is associated with a home agent (HA) which behaves as a router for the mobile node and keeps all the information of this mobile node. If a mobile node moves out the coverage of a home agent, then it needs to contact a local agent, a so-called foreign agent (FA). However, the basic Mobile IP does not provide security protection on the communication links from an FA to an HA and from an FA to a mobile node (MN). In today's technological world Mobile IP having features of authorization, authentication and accounting (AAA) standard is designed to offer secure communications on these corresponding two links.

Current research efforts are extensively been carried out to reduce handoff latency. We should observe that authentication in wireless networks force us to think regarding new challenges and design considerations. These design considerations, which are the main techniques for developing new and efficient technologies instead of using already existing technologies, can be presented as follows.

First, in a non homogeneous wireless networks, there will be numerous mobile users roaming in the network areas with dissimilar technical specifications, formats of signals, authorization of identity details, network protocols etc. The area of coverage for each network ranges from few meters in WLANs to few of kilometres in 3G systems, of course which depends on the design and architecture of that specific network. The components of an autonomous network, are the authentication server (AS), which acts as a centralized server for authentication purpose inside the area of the coverage of the network, as shown in Figure 1, where an access router (AR) acts as an a radio network subsystem (RNS) in UMTS or an access point (AP) in WLAN. Related to each mobile node, the device which is always used by the mobile user, consists of a permanent authentication relationship with the AS in its home network to which a already the mobile user is subscribed to a pack of services. Authentication servers have a fair amount of trust on each other due to the underlying principle of security associations (SAs), which are defined as a one-way relationship between a sender and a receiver for security services conforming to standard in IP security(IPSec).The Authentication architecture, which has ability to connects authentication servers, has a huge effect on the operational performance of authentication techniques and protocols for such non homogeneous environments, due to the reason that user credentials are typically sent through the authentication architecture; thereby making , it an important design issue in 3G/WLAN integration.

Second, ambient intelligence requires every device be involved with pervasive computing with sufficient security functions. For protection of information secrecy, data integrity, and availability of resource for the users, security architecture and protocols are essential. Information secrecy refers to prevention of disclosure of information which is improper; data integrity is related to the undesired modification of data; and resource availability means prevention of denial-of-service attacks that generally put inside useless packets into the network on purpose so as to block legitimate traffic of the network. During an authentication process, especially for interdomain roaming, a mobile node negotiates cryptography algorithms with an authentication server and obtains keys for subsequent data transmission. Additionally, authentication can reduce the attack of denial of service. Advanced authentication protocols can use security associations for individual connection link and so as to enable encryption of the data through the full session of data delivery. Also ,the involved encryption and decryption algorithms need robust processing and computation powers, which should ideally be looked upon for battery-operated portable machines. Mobile IP is developed for mobility of the terminal over the Internet, so it facilitates roaming in WLAN, i. e., mobile terminals can move from one subnet to another without communication interruption. Mobile IP is of huge importance due to the reason that it is the basis for the 3G/WLAN integration. Therefore, we focus on the authentication architectures that are related to Mobile IP networks since roaming capability is one of the most important features in ambient intelligence applications. In this paper, we introduce three architectures proposed recently.

 

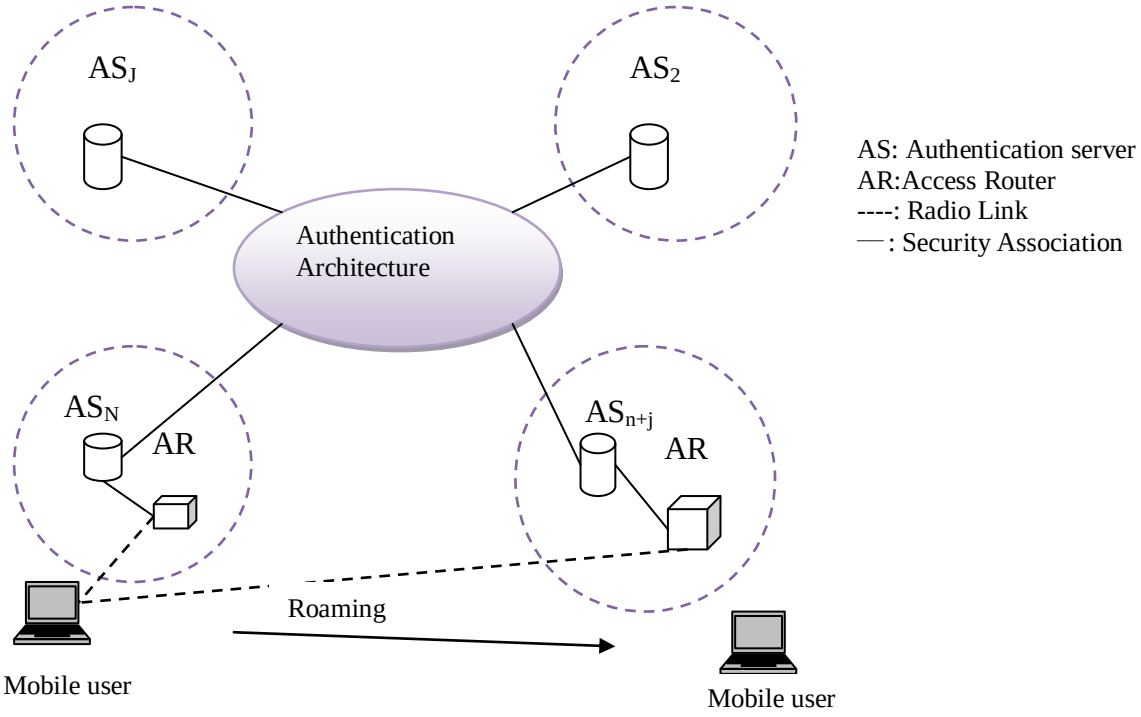


Figure 1. System architecture of authentication in wireless networks

## II. AUTHENTICATION ARCHITECTURE FOR INTERWORKING 3G/WLAN

### *1. Mobile IP with AAA Extensions*

In the simple Mobile IP architecture, authentication extension (AE) is given the functionality of registration of messages, which consists of a security parameter index (SPI) and an authenticator, which is computed by the usage of a keyed hash function. It is built in a way which provides entity authentication, which protects home agent (HA) and mobile nodes (MNs) when intruder wants to perform replay attacks, either by timestamping provision or by random number generation. AE does not provide data protection between a foreign agent (FA) and MNs. This protocol has been designed with assumption that security associations (SAs) between FAs and HAs have been already arranged . This assumption needs a tremendous work to control a large networking environmental setup, and in case of scaling up of networks it may not be of so much effect. To enhance the strength of relay protection, Mobile IPv4 challenge/response extensions (MICRE) have been also developed.

This protocol is having the ability of replay protection for all messages which are exchanged with the Mobile IP protocol .It operates by implementing two new types of message extensions: first one is the principle of creation of challenge extension for FA advertisement messages and secondly by creating mobile challenge response extension for trustful registration of messages. So in case a MN wants to undergo an authentication by itself, it has to send an authentication request message along with the challenge value obtained from the FA advertisement. After the checking of the challenge value, the FA can stop the intended attack from an MN.

The checking of a challenge value is always dependant on the security relation between the MN and its HA, but it has to be noted that the security association between the FA and the MN may or may not exist. A secure scalable authentication (SSA) is having the single objective of provision to develop Mobile IP with a robust, extendable authentication technique which is based on public- key cryptography. Consider a scenario where an MN moves close to an FA, it obtains an advertisement having the authentication extension and certificate extension which are being broadcasted by the FA. Now the MN retrieves and validates the certificate with the help of a public key issued by a competent and valid certificate authority. Subsequently, the MN makes usage of the public key of an FA to verify the digital signature in the FA authentication extension created by the FA's private key. Then, the MN will obtain the secret key of the FA; thereby making , the communication between the MN and the FA will be protected.

In the fundamental architecture developed and which is shown in Figure 2(a), each local AAA server (AAAL) is built in such a way that it shares security association with a home AAA server (AAAH) of a roaming MN in the current area, in a way that the AAAL can transmit MN's credentials securely. This setup, faces a drawback , it can result in a quadratic rise in the count of trust relationships, as the number of AAA authorities (AAAL and AAAH) maximises . This issue has been pointed out by the IETF roaming working group. A possible solution to this problem is to use intermediate entities to avoid excessive relationships of trust among every couple of administrative areas.

One example with multiple layers of intermediate brokers is shown in Figure 2(b). In this model, integrity or privacy of data between the home and non home area may be obtained by either hop-by-hop security associations or end-to-end security relationships which are implemented with the help of the broker infrastructure. A intermediate entity acts as a proxy between two administrative areas, which have security associations with the intermediate entity , and has the ability of relaying AAA messages from as well as to end users.

 

***2.*** Another security protocol, the Diameter protocol, advocated by the IETF, is as a pragmatic solution for AAA in Mobile IP networks. A Diameter server essentially acts as an authority center, which is made responsible to authenticate, authorize, and gather accounting information for Mobile IPv4 service offered to a mobile node. The Diameter base protocol basically provides an AAA framework for mobile applications, like a network access or IP mobility, and work in both the local AAA and roaming situations. In recent years, Diameter protocol is being applied as a even more robust successor to the popularly-deployed RADIUS protocol for authentication, authorization, and accounting. Security is increased between AR and either HA or MNs during AAA and the registration process. With these inherent benefits, the Diameter protocol is all set to become the most efficient authentication mechanism for operation of Mobile IP networks.

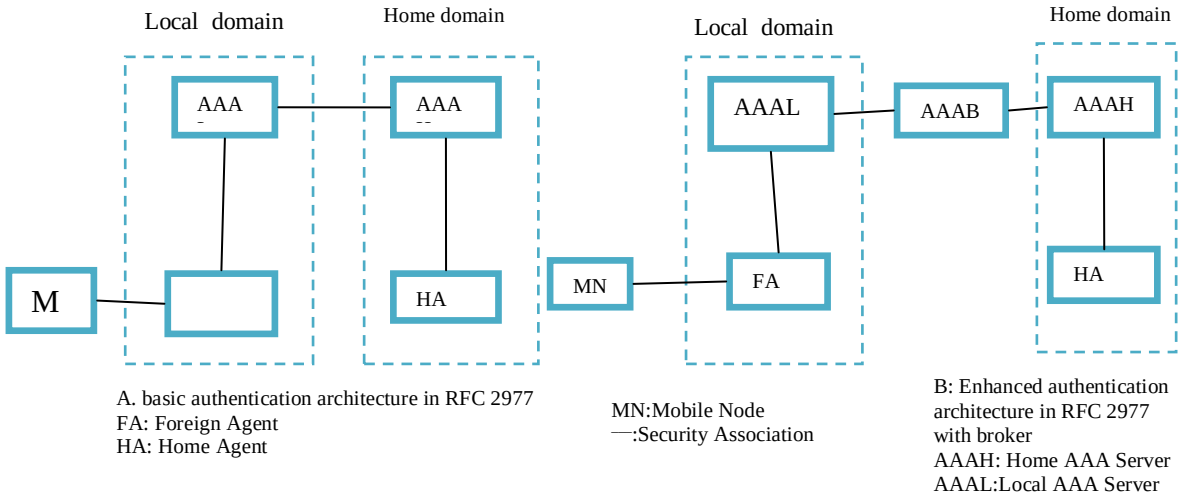


Figure 2. Authentication, authorization, and accounting in mobile IP networks.

***3. Authentication Servers and Proxy***

For operational compatibility of 3G/WLAN, the main consideration is how to identify a valid user and how to validate a user's credentials, which are maintained through servers handling authentication. The concept of 3G authentication server is proposed as a new operational element in 3G systems, which acts as a gateway between WLANs and 3G systems to support interworking. The AAA server has ability to terminate all AAA signalling from WLANs and can also block the route to other components in 3G systems. In such case, an AAA server is also termed as AAA Proxy. The same role is played by WLAN AAA proxy in WLANs , which can route AAA messages to 3G servers. WLANs are identified based on network address identifier (NAI) which is part of an access request sent by mobile nodes. A similar logic that uses a security gateway (SGW) in the place of authentication proxies to combine IP mobility and security management together is shown in Figure below. IPSec tunnel mode is activated between the SGW and its MNs by which the SGW sets up an SA for each MN in its network. The MN has a single SA between itself and the SGW in its home network, whether the MN is in its home subnet or it roams to a foreign subnet. The HA takes care of only the Mobile IP registration and forwarding packets to an MN's care of address (CoA). The MN is being secured by the IPSec tunnel which lies between the SGW and an MN. During the time period in which the MN is roaming, there does not exist a window of clear data transmission over wireless links, also there is no requirement to re-establish an IPSec tunnel between the SGW and an MN. So we can say that, this scheme provides a secure communication link between a roaming MN and its HA without the need of the participation of foreign networks.

***4. AAA and Inter-Domain Roaming***

The main aim of Mobile IP with AAA extension is to provide mobility for inter-domain roaming. So,when a mobile user moves out of the coverage of its home network, the network address, which was previously assigned, like an IP session which was active, is now rendered useless. However, a permanent IP address is the key to Mobile IP, so that irrespective of an MN's current location, the data packets can be forwarded to its permanent IP address. So, inter domain roaming becomes a issue for Mobile IP users. So, to elegantly handle such challenges, a common architecture for handling inter-system terminal mobility has been developed with the Mobile IP authentication architecture, as shown in figure below . In this architecture, mobility support is combined with AAA properties by careful design of signalling messages.Before an FA verifies the registration of a visiting node, it interacts with a foreign AAA server with an access request message. Therefore, the AAA functions are completed along with the registration. As designed in the architecture no separate signalling is required for authentication and registration, the number of packets exchanged is reduced. In, two architectures for 802.11 and 3G networks ,two kinds of integration are proposed: tightly-coupled and loosely-coupled interworking. In a tightly coupled architecture, the 802.11 network would provide functions in 3G; so that the 802.11 does not show all information for the 3G networks and it acts as either a packet control function (PCF) in CDMA2000, or as a serving GPRS support node (SGSN) to the wireless network.

As a result, two domains would share the same authentication server for billing and accounting. In case if we dont want to use a common authentication mechanism, based on UMTS SIM (or USIM) for 3G or removable user identity

 

module (R-UIM) cards for authentication on WLANs, a loosely coupled architecture can be considered for usage in which two domains exist and users can use their individual authentication solutions best suitable to them.

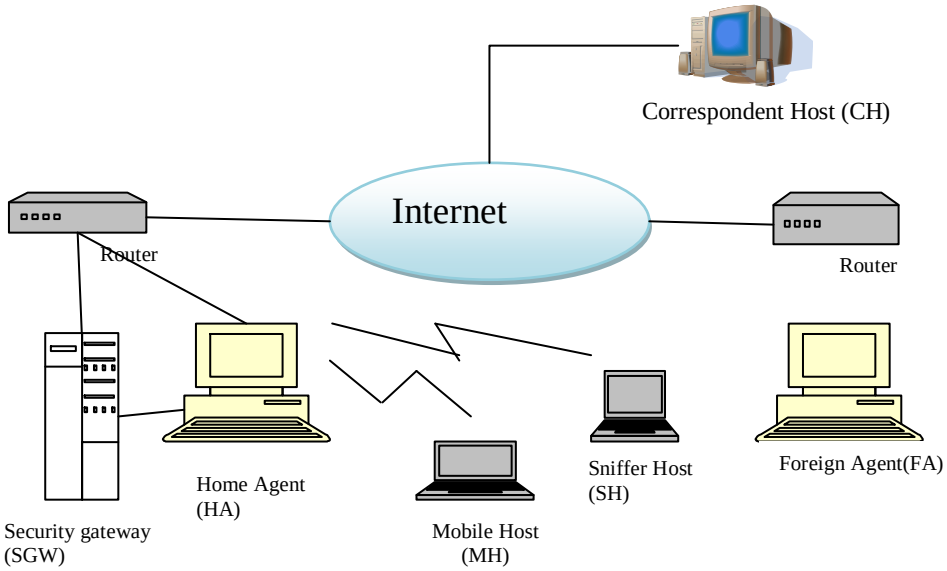


Figure 3. Integration of IP mobility and security mechanism

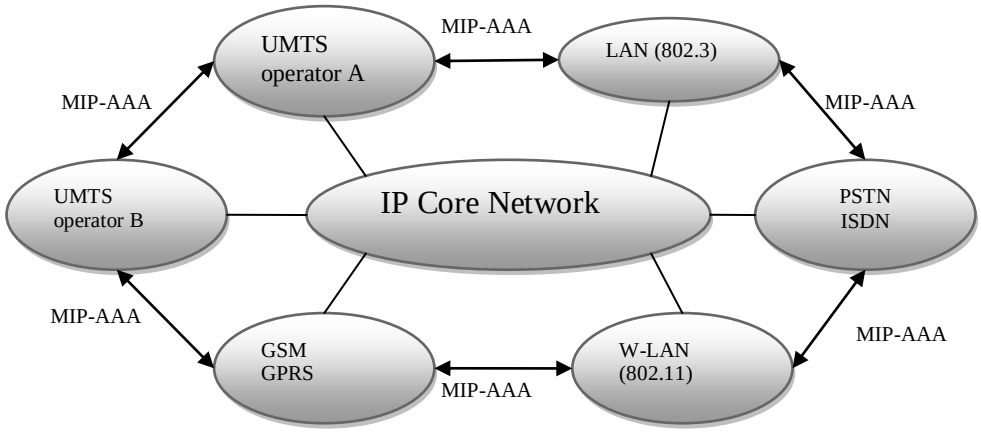


Figure 4. Mobility support in heterogeneous networks.

## III. AUTHENTICATION IN WIRELESS SECURITY PROTOCOLS

In the previous section, we presented authentication architectures for integrated wireless networks. For each architecture, it is also important to design corresponding protocols that deliever messages and credentials in architecture. In this section, we introduce several commonly used security protocols. Both UMTS and Mobile IP are designed to provide wireless services in mobile environments, especially for intra- and intersystem roaming. Although these technologies are going to be mature, their commercial deployment is still in the preliminary stage. WLAN technology and WLAN industry for nomadic roaming, which started in the mid 1980s, are experiencing a tremendous growth due to the large bandwidth made possible by the IEEE 802.11 standard. Considering that the Internet access is dominant in WLAN systems, many wireless security protocols are designed to protect link-level data without mobility support.

### *1. Wired Equivalent Privacy 802.11 LANs*

Wired equivalent privacy (WEP) protocol is a built-in security feature of 802.11standards such as 802.11a/b/g. WEP protocol is designed to protect link-level data during wireless transmission, i.e., only the wireless portion of connections, between clients and access points; but, it does not provide end-to-end security. In particular, the WEP algorithm prevents unauthorized access to a wireless network by relying on a secret key shared between mobile stations and an access point. The WEP secret key encrypts packets before they are transmitted. Also, the WEP uses integrity check to prevent packets from being modified in transit. Most installations use a single WEP key between the mobile stations and access points, even though multi-WEP key techniques can enhance security.

### *2. Extensible Authentication Protocol and its Variants*

Extensible authentication protocol (EAP) is the mechanism that is used between a client and an authenticator. Standard 802.1x can use EAP protocol as a transport mechanism for exchanging messages. The 802.1x standard specifies encapsulation methods for transmitting EAP messages so they can be carried over different media type. EAP is a framework for providing centralized authentication and dynamic key distribution, and it is a general protocol supporting

 

multiple authentication methods, such as token cards, Kerberos certificates, public-key authentication, etc. EAP enables wireless client adapters that may support different authentication types to communicate with different back-end servers, such as remote authentication dial-in user service (RADIUS). When used with 802.1x, it provides end-to-end authentication when a wireless client that associates with an AP cannot gain access to the network until the user performs a network logon. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server, such as RADIUS. The server asks the AP for proof of identity, which the AP obtains from the user and then sends back to the server to complete the authentication. EAP performs mutual authentication, so each side is required to prove its identity to the other, using its certificate and private key. When both client and server authenticate each other, resulting in stronger security, EAP protects against man-in-the-middle and sniffing attacks.

### *3. 802.1x Authentication Protocol*

Standard 802.1x provides network login capabilities between PCs and edge networking entities such as an access point. It offers an architectural framework for implementing various authentication schemes. Standard 802.1x itself does not provide encryption, and it is not an alternative to WEP, 3DES, AES, or any other cipher. Therefore, 802.1x is focused only on authentication and key management, and it can be used in combination with any ciphers. Also, 802.1x is not a single authentication method; rather, it utilizes EAP as its authentication framework. This means that 802.1x-enabled switches and access points can support a wide variety of authentication methods, including certificate-based authentication, smart cards, token cards, one-time passwords, and so on. Standard 802.1x supports open standards for authentication, authorization, and accounting much like AAA in Mobile IP (including RADIUS, so it works with the existing infrastructure for managing remote and mobile users. It can be combined with an authentication protocol, such as EAP-TLS, LEAP, or EAP-TTLS,Standard 802.1x provides port-based access control and mutual authentication between clients and access points via an authentication server. It's authentication protocol consists of three entities:

Authenticator: An access point that has 802.1x authentication enabled. This includes LAN switch ports and wireless access points.

Authentication server: A server that performs authentication, allowing or denying access to the network based on username or password. The 802.1x standard specifies that the RADIUS is the required Authentication Server.

Supplicant (client): An access device requesting LAN service.

Once 802.1x authentication is enabled (both in the client and authenticator), a successful authentication must be completed before any traffic is allowed to transit the network from the client, including critical traffic, such as DHCP requests, regardless of whether a link is established between the client and authenticator (switch port). The 802.1x client will transmit appropriate EAP messages to the authenticator (switch port). The switch port with 802.1x authentication enabled is set to an uncontrolled state, accepting only EAP messages (all other traffic will be discarded). Upon receipt of the client's EAP message, the switch forwards the request to the authentication (RADIUS) server without changing its contents.

Security flaws in 802.1x architecture are concerned with the absence of mutual authentication and may cause a man-in-the-middle attack. Another problem is session hijacking in which the original user is not able to proceed, but the attacker acts as an original user and starts using the session created by original user.

### *4. WiFi Protected Access and 802.11i*

WiFi Protected Access (WPA) is a standards-based, interoperable security specification, which significantly increases the level of data protection and access control for existing and future wireless LAN systems. WPA is a subset of the 802.11i draft standard and will maintain forward compatibility. It will replace WEP as standard Wi-Fi security. The task group's short-term solution is to improve WiFi protected access (WPA) to address the problems of WEP. The group also defines the temporal key integrity protocol (TKIP) to address the problems without requiring hardware changes—that is, requiring only changes to firmware and software drivers.

To strengthen user authentication, WPA implements 802.1x and EAP together by using a central authentication server, such as RADIUS, to authenticate each user on the network before they join it, and also employs mutual authentication so that the wireless user does not accidentally join a rogue network that might steal its network credentials.

The IEEE 802.11i draft standard defines additional capabilities required for secure implementation of IEEE 802.1X on 802.11 networks. These include a requirement for using an EAP method in supporting mutual authentication, key management, and dictionary attack resistance. In addition, 802.11i defines the hierarchy for use with the TKIP and AES ciphers and a four-way key management handshake used to ensure that the station is authenticated to the AP and a back-end authentication server, if present. As a result, to provide adequate security, it is important that IEEE 802.1x are implemented in 802.11 networks for security enhancements.

## IV. COMPARISON STUDY OF WIRELESS SECURITY PROTOCOLS

There are many research efforts on security protocols being carried out from a efficient perspective; but, there is a deficiency of quantitative results showing the effect of security protocols on system performance that can be increased drastically by applying security policies in conjunction with mobility.

Security Policies: Security policies are developed to illustrate the security services provided by the concerned security protocol. Each protocol consists of various authentication and encryption mechanisms to provide security. Therefore, by configuring various security mechanisms for each protocol, multiple security policies are implemented in

 

the test bed. Along with such policies, hybrid security policies are also designed, involving multiple security protocols at different network layers. In Table 1, a total of 12 policies—namely, PN-1 to PN-12 are listed. We consider that no security case as a special policy, PN-1, which is used in evaluating authentication overhead.

Evaluation of the involved security policies in various mobile scenarios are performed by considering the current location of the mobile node (MN) in the network. Therefore, we have presented the novel investigation of both "no roaming" (NR) and "with roaming" (WR) situations. "With roaming" (WR) represents the situation when one of the mobile nodes is visiting a foreign network, whereas "no roaming" (NR) refers to an scene where all MNs stay in their home network.

Moreover, those mobility scenarios consider the presence of correspondent nodes (CN) too. Table 2 stores all the scenarios considered. Table 3 represents authentication time (in seconds) for IPSec and 802.1x security policies. As WEP does not involve itself with the exchange of control messages, so there exists no authentication time involved in it.Also,authentication time for IPSec and 802.1x takes into account Mobile IP authentication time. We have presented the observation that when an MN is not roaming, IPSec authentication takes longer than 802.116. Nevertheless, in a scenarion when an MN roams, the 802.1x authentication time is prolonged. The simple reason for this is the fact that when an MN roams, MN re-authenticates with an FA using the 802.1x mechanism, whereas this is not the scene with IPSec protocol, as the IPSec tunnel is already connected between the MN and the HA. It has been observed that 802.1x with IPSec security mechanisms induces longer authentication latency than 802.1x without IPSec policies. Atlast of our discussion, Table 3 shows that 802.1x-EAP-TLS authentication time is longer than 802.1x-EAP-MD5 due to reason that 802.1x-EAP-TLS involves usage of the digital certificates for mutual authentication, which involves exchange of several control packets.

Since WEP does not involve exchange of control messages, there is no authentication time involved with it. Since Mobile IP is used for enabling mobility in the test bed, authentication time AT for IPsec and 802.1x involves Mobile IP authentication time as well. We observe that the developed IPSec security strategies do reduce the throughput than WEP and 802.1x security policies. This is due to the reason that IPSec uses the 3DES encryption algorithm which is algorithmically slower than the encryption algorithm used in WEP and 802.116.

But IPSec contains even more stronger security services, which compensates for the higher encryption overhead.

Table 1. Security Policies

| Policy Number | Description of Security Policies |
|---|---|
| PN-1 | No Security |
| PN-2 | WEP-128 bit key |
| PN-3 | IPSec-3DES-SHA |
| PN-4 | IPSec-3DES-SHA-WEP-128 |
| PN-5 | 8021x-EAP-MD5 |
| PN-6 | 8021x-EAP-TLS |
| PN-7 | 8021X-EAP-MD5-WEP-128 |
| PN-8 | 8021X-EAP-ELS-WEP-128 |
| PN-9 | 8021X-EAP-MD5-WEP-128-IPSec-3DES-MD5 |
| PN-10 | 8021X-EAP-TLS-WEP-128-IPSec-3DES-MD5 |
| PN-11 | 8021X-EAP-MD5-WEP-1280IPSec-3DES-SHA |
| PN-12 | 8021X-EAP-TLS-WEP-1280IPSec-3DES-SHA |

Table 2. Mobility Scenarios

| Number | Scenario | Roaming or No-Roaming |
|---|---|---|
| M1 | Mobile to mobile node in the same domain | No Roaming (NR) |
| M2 | Mobile node to home agent | |
| M3 | Mobile node to corresponding node (fixed) in the same tomain (register to HA) | |
| M4 | Mobile node to mobile node in different subnets | |
| M5 | Mobile node to corresondeing node (fixed) in the same domain | With Roaming (WR) |
| M6 | Mobile node to mobile node in different domains | |
| M7 | Mobile node to corresponding node (fixed) in different domain (register to FA) | |
| M8 | Mobile node and corresponding node (fixed) in different domains | |
| M9 | Mobile to mobile node in the same Domain | |

Table 3. Authentication Time Measurements for Different Security Policies

| Policy | IPsec (seconds) | 802.1x-EAP(MD5) with IPsec (seconds) | 802.1x-EAP(MD5) without Ipsec (seconds) | 802.1x-EAP(TLS) without Ipsec (seconds) | 802.1x-EAP(TLS) with IPsec (seconds) |
|---|---|---|---|---|---|
| Non-Roaming | 1.41 | 0.43 | 1.72 | 1.82 | 3.12 |
| Roaming | 2.84 | 2.18 | 3.47 | 4.97 | 6.28 |

 

## V. CONCLUSION

We conclude this paper, by stating the fact that effective authentication and security protocols for ubiquitous wireless communications in integrated 3G and WLAN systems is quite a research challenge for practitioners in this field. Authentication is a robust security technique, designed so as to protect networks which has probability of acceptance of a fraudulent transmission by establishing the validity of a transmission, a message, or an originator. Therefore, it is an important issue in ambient intelligence that involves pervasive computing of portable devices. In this paper, we first considered the new challenges and design considerations of authentication protocols in wireless networks. We then presented different authentication architectures and security protocols in UMTS, WLANs, Mobile IP, and the integrated 3G and WLAN systems.

## REFERENCES

[1] Karygiannis, T. and L. Owens, "Wireless Network Security 802.11, Bluetooth and Handheld Devices," NIST Special Publications 800-48, November 2002.

[2] Buddhikot, M., et al., "Integration of 802.11 and Third-Generation Wireless Data Networks," IEEE INFOCOM'03, April 2003.

[3] Cappiello, M.. A. Floris, and L. Veltri, "Mobility amongst Heterogeneous Networks with AAA Support," IEEE ICC 2002, Vol. 4, pp. 2064–2069, 2002.

[4] Glass, S., et al., "Mobile IP Authentication, Authorization and Accounting Requirements," RFC2977, October 2000.

[5] Perkins, C., and P. Calhoun, "Mobile IPv4 Challenge/Response Extensions," IETF RFC 3012, November 2000.

[6] 3GPP. "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; 3G Security; Security Architecture," *Technical Specification 3G TS* 33.102V3.7.0 (2000-12), 2000.

[7] Johnson, D. B., C. Perkins, and J. Arkko, "Mobility Support in IPv6," *IETF Internet Draft*, draft-ietfmobileipv6-17.txt, May 2003.

 