Volume : 1, Issue : 1
January - June 2011

ISSN : 2229 - 3515

international journal of ADVANCES IN SOFT COMPUTING TECHNOLOGY

Editor-in-Chief
Dr.Vaka Murali Mohan

Published by
BHAVANA RESEARCH CENTER

Wireless Security Protocol for Quality of Service

Prabhakara Rao, S[1]*., Nagabhooshanam, E[2] and Govardhan, A[3]
1.Head, Dept. of ECE, RRSCET. Muthangi (V) Patancheru(M),Medak (Dt), A.P, INDIA
2.Professor & Head, Dept. of ECE, M G I T, CB Post, Gandipet, Hyderabad, A.P, INDIA
3.Principal, JNTUJ College Of Engineering, Kodimyal(M), Karimnagar(Dt), A.P, INDIA

Key Words:
QOS, Wireless Security, Mobile User, Wireless IP Networks, Authentication, Heterogeneous Networks

Abstract: *The nature of mobile communication, characterized by terminals having poor interface and limited processing capacity, as well as complex combination of network protocols, makes the design of security solutions particularly challenging. In wireless networks, authentication can provide secure communications by preventing unauthorized usage and negotiating the credentials for data transmission. Nevertheless, it induces heavy overhead to data transmission, further deteriorating overall system performance. Thus, an analysis of impact of authentication on security and QoS is been realized in this paper..*

1. Introduction:

The tremendous advance of wireless communication technologies has facilitated the ubiquitous Internet service, whereas inducing more challenges to security due to open medium [1]. In order to provide security services in wireless IP networks, authentication is used as an initial process to authorize a mobile user (MU) for communications through secret credentials [2]. In an authentication process, an MU is required to submit secret materials such as certificates and challenge/response values for verification and encryption/decryption with session keys and algorithms [31-[61. By rejecting unsuccessfully authenticated users, authentication can protect the network resources. The information secrecy and data integrity can also be guaranteed by using the negotiated credentials or encryption and message authentication. Meanwhile, authentication also affects the quality of service (QoS) greatly. When public-key based authentication mechanism is applied, the computation complexity of encryption/ decryption consumes more time and power [7].

**** Prof. S. Prabhakara Rao***
Head, Dept. of ECE
RRS College of Engineering and Technology
Muthangi (V), Patancheru (M),
Medak (Dt) 502 300, AP, INDIA
Ph. No.: 91-9490065307
E-mail: saggurthi_p@yahoo.co.in

For secret key based challenge/response authentication, the credentials of the MU are encrypted and transmitted for remote verification hop-by-hop among authentication servers. The transmission and encryption/decryption of credentials affect many QoS parameters such as delay; call dropping probability, and throughput. Therefore, in some scenarios, a tradeoff between security service and the system performance should be considered because users may have different preferences with respect to security and performance. Moreover, authentication requests are closely related to mobility and traffic patterns of MUS because these requests are generated when an MU either initiates a call, or crosses a boundary of subnets. Therefore, the impact of authentication on QoS parameters is far more sophisticated when mobility and traffic patterns are taken into account. Since the authentication affects both of security and QoS, many authentication schemes are proposed, focusing on the security and efficiency [2], [5], [8]-[15]. However, none of them provide quantitative analysis of security and system performance, simultaneously, and nor do they show the connection between security and system performance. Furthermore, mobility and traffic patterns are not considered in the evaluation of authentication, which are important features in wireless networks.

2. QOS in wireless communication:

Guaranteeing the QoS requirements is a challenging task with wireless communication. One of the key elements in providing QoS is an effective resource allocation policy, which not only ensures meeting QoS of newly arriving calls, if accepted but also not deteriorating the existing on-going services. These enhancements will enable a better mobile user experience and will make more efficient use of the wireless channel.

As the performance of a system with given physical resources (e.g., the available bandwidth of radio spectrum) depends heavily on resource management schemes including multiple access techniques, the call admission control policies and the congestion control schemes, to make efficient use of the available bandwidth while providing high quality of service (QoS) to simultaneous services with different requirements, efficient resource management schemes have to be devised.

Many real-time applications can use different encoding schemes according to their desired quality and generate traffic with different bandwidth requirements. For example, generic video telephony may require more than 40 Kbps, but low-motion video telephony requiring about 25 Kbps may be acceptable. From the standpoint of a system administrator, this property provides an alternative for resource planning, especially for bandwidth allocation in wireless networks. In wireless networks where the bandwidth is a scarce resource, the system may need to block incoming users if all of the bandwidth has been used up to provide the highest QoS to existing users. However, if these users can be degraded to a lower QoS level, it is possible to reduce the blocking probability without degrading the QoS of existing users to an "unacceptable" level. Various approaches and algorithms adopting this idea have been proposed. A graceful degradation mechanism is proposed in to increase bandwidth utilization by adaptively adjusting bandwidth allocation according to user-specified loss profiles. Thus, a system could free some bandwidth for new users by lowering the QoS levels of existing users.

3. Requirements for communication security:

Communication security is often described in terms of confidentiality, integrity, authentication and non-repudiation of transmitted data. These security services are in turn implemented by various mechanisms that are usually cryptographic in nature. In addition there is confidentiality of traffic (i.e. whether or not communication is taking place), of location (where the communicating parties are located) and of the communicating parties' address, all of which are important for privacy. A casual level of security is usually provided implicitly even without taking any extra measures. For example in order to eavesdrop on a particular person's mobile phone conversations the eavesdropper has to be located in physical proximity to the person and carry special radio equipment which in itself represents a certain level of protection. Casual authentication between mobile phone users is indirectly provided by the calling and called party numbers. In case of voice telephony, authentication results from recognizing the other person's voice. Cryptography on the other hand gives the possibility of designing strong security services but often creates inconveniences when using the application. The use of cryptography therefore makes most sense in case of sensitive applications. When strong cryptographic security mechanisms are in place the remaining vulnerabilities are usually due to poor management and operation and not by weaknesses in the cryptographic algorithms themselves. Confidentiality of transmitted data can be provided by encrypting the information flow between the communicating parties, and the encryption can take place end-to-end between the communicating parties or alternatively on separate legs in the communication path. In GSM networks for example, only the radio link between the mobile terminal and the base station is encrypted whereas the rest of the network transmits data in clear-text. Radio link confidentiality in GSM is totally transparent from the user's point of view. Mechanisms for implementing confidentiality of traffic, location and addresses will depend on the technology used in a particular mobile network. Authentication of transmitted data is an asymmetric service, meaning for example that when A and B are communicating, the authentication of B's data by A is independent from the authentication of B's data by A. The types of authentication available will depend on the security protocol used. In the Internet for example, SSL allows encryption with four different authentication options: (i) Server authentication, (ii) Client authentication, or (iii) Both server and client authentication or (iv) No authentication, i.e. providing confidentiality only.

Non-repudiation is similar to authentication in that it is an asymmetric security service. A simple way to describe the difference between authentication and non-repudiation is that with authentication the recipient himself is confident about the origin of a message but would not necessarily be able to convince anybody else about it, whereas for non-repudiation the recipient is also able to convince third parties. Digital signature is the mechanism used for non-repudiation. Crypto graphically seen a message's authentication code and non-repudiation code can be identical, and the difference between the two services might only depend on the key distribution. In general, if a signature verification key has been certified by a trusted third party the corresponding digital signature will provide non repudiation, whereas it can only provide authentication if the key has simply been exchanged between the two communicating parties.

Different parties will have different interests regarding authentication and non-repudiation services. Network operators are interested in authenticating the users for billing purposes and to avoid fraud. Users and content

service providers are interested in authenticating each other and might also be interested in authenticating the network service provider. How and where in the network authentication services are implemented will depend on the technology used and the business models involved. other and might also be interested in authenticating the network service provider. How and where in the network authentication services are implemented will depend on the technology used and the business models involved.

4. Security across heterogeneous networks:

Network architectures are based on protocol layers that represent an abstract way of modeling and implementing data transmission between communicating parties. The usual protocol architecture consists of 5 layers as illustrated in Fig.1.

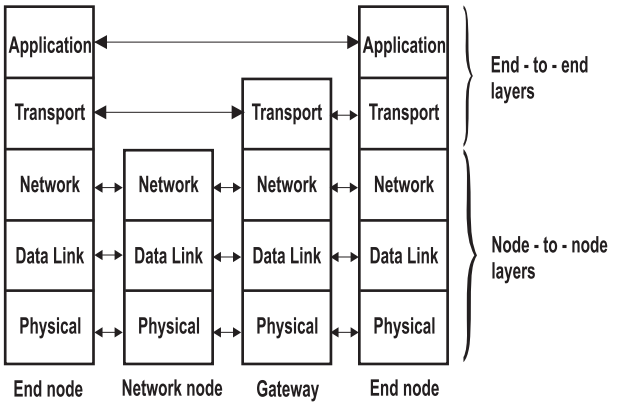

Fig.1. Communication protocol layers

In reality, no data are directly transferred between adjacent layers on opposite sides. Instead, data and control information are passed down through the interfaces between the protocol layers on one side and up through the interfaces between the protocols layers on the other side. The physical data transmission actually takes place through a physical medium underneath the physical protocol layer.

5. Impact of authentication on security and QOS:

The authentication in wireless networks is a process to identify MUs and to negotiate credentials for communications. In a challenge/response-based authentication, a user is identified with a shared security association (SA), which is a trust relationship with many parameters such as keys and algorithms for secure services, between an authentication server. During the process, the server sends a challenge value, a random number, to the user for encryption, and verifies the returned value, called response value, with decryption. In a foreign network, a visiting MLJ sends an authentication request to an access point (AP). The AP relays the request to a local authentication server (LAS), which only takes charge of authentication for visiting MU's from foreign networks. If the LAS have no information to verify the MU, it contacts the home authentication server (HAS) of the MU through authentication architecture. An HAS is an authentication server to identify the MUS who subscribe the service in its network. And, an authentication architecture is composed of many authentication servers that share SAS with the LAS and HAS. If the request is an inter-domain authentication request, the HAS sends a registration request to the MU's home agent (HA): which maintains the current location of the MU, to update the MU's location. Shared SA with the LAS and replies the response value to the LAS. After decrypting the replied value and comparing it with original challenge value, the LAS can authenticate the MU when the decrypted value matches original challenge value.

A) Intra-domain handoff authentication: When an MU crosses the boundary of subnets in the foreign network domain with an on-going service, an intra-domain handoff authentication is initiated, since there is an on-going communication session between the MU and an AP, one session SA exists between the MU and the LAS in the visiting network domain. The MU encrypts the challenge value using shared SA with the LAS and replies the response value to the LAS. After decrypting the replied value and comparing it with original challenge value, the LAS can authenticate the MU when the decrypted value matches original challenge value.

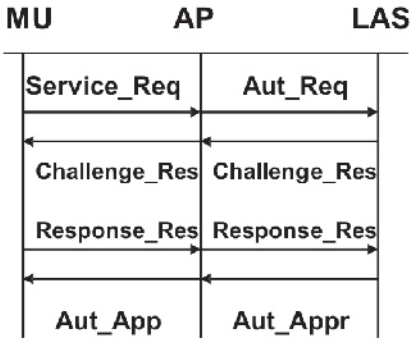

Fig. 2A: Loss-domain Handoff Authentication

B) Session authentication: When an MU starts a communication session in a subnet of a foreign network, a session authentication is initiated. At this time, session SA does not exist between the MU and the AP. Thus, it is necessary to contact the HAS of the MU for authentication. As shown in Fig.2B, when an LAS receives the authentication request, it sends a challenge value to the MU. The MU encrypts the challenge value with the SA shared with the HAS, and replies the response value to

the LAS, which relays the challenge and response values to the HAS of the MU for verification due to lack of SA to decrypt the response value. After authentication at the HAS, the secret credentials such as keys to protect the communication may be generated and sent to the LAS.

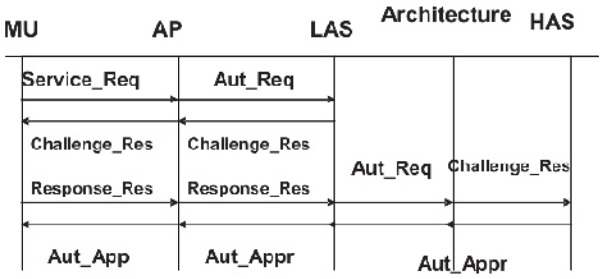

Fig. 2B: Session Authentication

Inter-domain handoff authentication: When an MU is crossing the boundaries of different foreign network domains with an on-going service, an inter-domain handoff authentication occurs. Without an existed SA between the MU and the LAS, the signaling diagram shown in Fig 2. C is similar with that in the case of session authentication, except that the MU needs registration to its HA via the HAS because we assume that the MU needs registration when it is crossing the boundaries of different network domains.

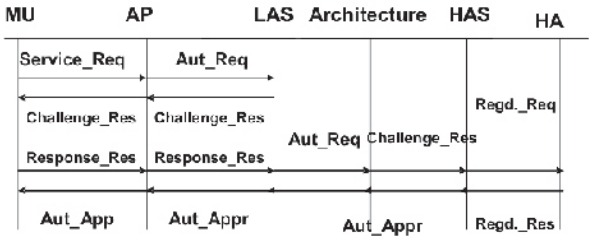

Fig. 2C: Inter domain handoff Authentication

Authentication; Impact QoS Metrics:

Besides the effect on the security, authentication also influences QoS metrics, such as authentication delay, cal1 dropping probability and throughput of communications. The authentication delay is defined as the time from when the MU sends out an authentication request 10 when the MU receives the authentication reply. During this authentication delay, no data for on-going service can be transmitted, which may interrupt the connections. Therefore, the call dropping probability may be increased because of the extended authentication delay.

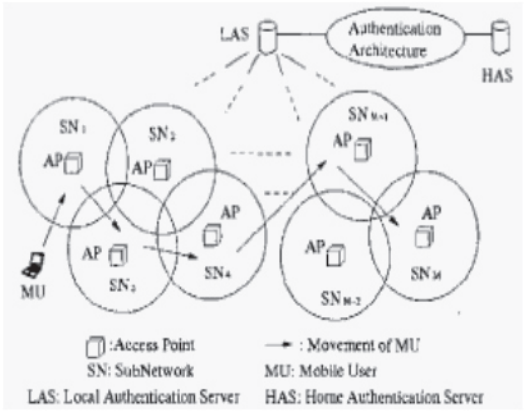

Fig.3. Architecture of Authentication in Wireless Networks.

Authentication in wireless networks has great effects on both security and quality of service such as authentication delay, call dropping probability, and throughput. In order lo improve the security and performance of wireless networks; it is necessary to analyze the authentication effects on both security and QoS metrics by taking into account mobility and traffic patterns.

6. SYSTEM ARCHITECTURE:

A scenario is assumed where there is a MU and is roaming into foreign network domains. Then, the intra-domain handoff authentication, session authentication, and inter-domain handoff authentication in foreign networks are illustrated in Fig. 2 .A, 2 .B, and 2,C, respectively.

Mobility pattern:

The mobility pattern of an Mu is represented by the residence time of the MU in one subnet, denoted as T. Tr is a random variable and the probability density function (PDF) of Tr, denoted as fTr(t), is Gamma distribution with mean l / μr and variance V[16]. Then, the Laplace transform of fTr(t), Fr(s), is:

$$Fr(s)=\left(\frac{\mu_r\gamma}{s}+\mu_r\gamma\right)^{\gamma},\ where\gamma=\frac{1}{V\mu_r^{\ 2}} \qquad (1)$$

the PDF of the residence time in a network domain, denoted as Fγm (t), can be expressed with a Laplace transform FM(s) as:

$$F_M(s)=\frac{1}{M}\left(\frac{\mu_r\gamma}{s+\mu_r\gamma}\right)^{\gamma}\frac{1-\left(\frac{\mu_r\gamma}{s+\mu_r\gamma}\right)}{1-\left(\frac{\mu_r\gamma}{s+\mu_r\gamma}\right)^{\gamma}} \qquad (2)$$

the mean value of residence time in this network domain, denoted as TM, can be expressed as:

$$T_M=-\frac{\partial F_M(s)}{\partial s/s=0}=\frac{M+1}{2\mu_r} \qquad (3)$$

Traffic pattern:

Call arrival rate and call duration time is used to indicate traffic patterns. The PDFs of the call inter-arrival time and call duration time, denoted as fTA(t) and fTd(t). Respectively, become:

$$fT_A(t)=\lambda_u e^{\lambda_u t};\ and\ fT_D(t)=\eta e^{-\eta t} \qquad (3)$$

7. PERFORMANCE EVALUATION

1) Computing Average Authentication Delay:
Authentication delay as the time from when an MU sends an authentication request to when the MU receives the authentication reply.

$$T(i)=\sum_{\beta=1}^{3}\lambda_\beta T_\beta(i) \qquad (3)$$

2) Average Call Dropping Probability during Authentication: When an extended waiting time for authentication is induced and greater than a threshold time, the connection will be broken. On the other hand, even though the authentication delay is small and the MU is a valid user, an authentication failure may happen regardless of security level because of damaged credentials caused by transmission error, packet drop at queues, attack of intruders and software application failure. Therefore, the call dropping probability is defined as the probability that the service of an MU is dropped during one authentication operation because of either extended authentication delay, or an authentication failure.

Let P(i) denote the average call dropping probability at security level i, it can be written as:

$$P(i)=\frac{\sum_{\beta=1}^{3}\lambda_\beta(P_\beta(i)+P_e)}{\sum_{\beta=1}^{3}\lambda_\beta} \qquad (4)$$

and,

$$P_\beta(i)=PT_\beta(i)(T_\beta(i)>T_{th}) \qquad (4)$$

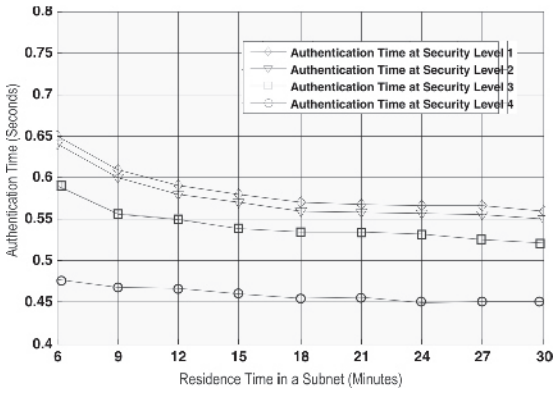

Figure 4. Authentication Time vs. Residence Time in a Subnet.

8. RESULTS ANALYSIS AND CONCLUSION

The effects of mobility pattern on the authentication delay and call dropping probability are shown in Figures below: The effect of call dropping probability in authentication is shown in Fig. 4. The call dropping probability increases with the increase of the residence time of an MU in a subnet. When the residence time of an MU in a subnet increases, the arrival rate of intra-domain handoff authentication requests will decrease.

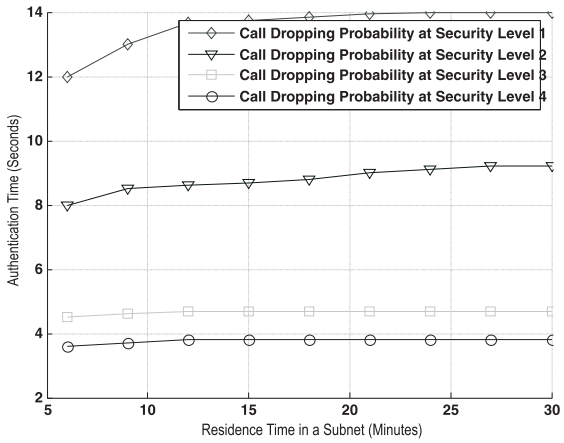

Fig.5. Call Dropping Probability vs. Residence Time in a Subnet.

9. CONCLUSION

It is observed that the aspects of mobile networks can make it both harder and easier to implement communication security as compared to for example the Internet. Communication between mobile and fixed networks creates particular problems regarding security protocol design. Mobile devices usually have a poor user interface thereby creating problems for the usability of security. The observation made reveals the impact of authentication on security and quality of service (QOS) in combination of mobility and traffic patterns, which are critical to deliver secure and efficient services in wireless IP networks. A quantitative analysis of the security and quality of service, which is of extreme importance to the adaptation of new security solutions to various mobile environments, is also realized.

10. REFERENCE

1. A. Arumugam, A. Dwfexi. A. Nix, and P. Fletcher, "of the Coexistence of 802.11g WLAN An Investigation and High Data Rate Bluetooth Enabled Consumer Electronic Devices in Indm Home and Office Environments," IEEE Transaction and Consumer Electronics, vol. 49, , August 2003, pp. 587-596.

2. L.Salgarelli.M.Buddhikot.J.Garay, S.Patel and S.miller, " The Evolution of Wireless LANs and PANS Efficient Authentication and Key Distribution in Wireless IP Networks," IEEE Personal Communications on Wireless Communications, Vol.10, Dec 2003, pp.32-61.
3. P.Calhoun, 1.Loughney, E.Guttman. G.Zorn and J.Arkko, "Diameter 3ase protocol," draft-ietf- aan-diameter-17.txt, December 2002.
4. S.Jacobs, "Mobile IF Public key Based Authentication :" 5th Edi 1999.
5. C.Perkins and P. Calhoun, Mobile Ipv4 Challenge/Response Extensions,"RFC3012. Nov, 2000.
6. Andersen, R., "Security Engineering" (2001), Wiley Publications 12th Edition.
7. Dierks, T&Alien, C. (1999), RFC2246 - The TLS (Transport Layer Security) protocol, Version 1.0 IETF. URL: http://www. ietf .org/rtf/rtf2246.txt
8. H.Kim and H.Afifi. "Improving Mobile Authentication with New AAA protocols." in IEEE international Confer, on Communications. vol.1, pp. 497-501,2003.
9. W.Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)," RFC1334. Aug 1996
10. S.Shieh, E Ho. and Y. Huang, "An Efficient Authentication Protocol for Mobile Networks," Journal of Information Science and Engineering.
11. W. Liang and W. Wang. "A Cost-Aware Control Scheme for Efficient Authentication in Wireless Networks." in 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMARC'04. Dec 2004.
12. B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol." RFC2716, Oct 1999.
13. L.Dell'Uomo and E. Scarrone, "The Mobility Management and Authentication/ Authorization Mechanisms in Mobile Networks beyond 3'3." in Personal, Indoor and Mobile Radio Communications. 2001 12th IEEE International symposium on, vol. 1, pp. c44-c48, Sept. 2001.
14. S. Glass. T. Hiller, S. Jacobs, and C. Perkins. "Mobile IP Authenticahon. Authorization and Accounting Requirements." RFC2977. Oct 2000.
15. W. Stallings, "Network Security Essentials." Applications and Standards, 2000.
16. W. Wang and I. Akyildiz. "Intersystem Location Update and Paging Schemes for Multitier Wireless Networks," in Proc. of ACWIEEE Mobi-Com'2000. pp. 99-109. August 2000.