ISSN: 2320-1363

Secure Routing in the perspective of authentication scheme for mobile Ad hoc Communication

Halavath Peda Sydulu *1, Mohammed Zeeshan Ali *2

M.Tech (IT), Holymary Institute of Technology and Science,Hyderabad, India

M.Tech (IT), Holymary Institute of Technology and Science,Hyderabad, India

Abstract

Technology and its relevance is the most cost effective solution in today's technology market, where security plays most typical role in order to give a glimpse this paper provides the best to the solution network routing security. Technology makes things easier, smarter and efficient and the most challenging one in the communication media. Communication is one of the integral parts of science that has always been a focus point for exchanging information among parties at locations physically apart. Similarly, the term `mobile' has completely revolutionized the communication by opening up innovative applications that are limited to one's imagination. Today, mobile communication has become the backbone of the society. All the mobile system technologies have improved the way of living. It's main plus point is that it has privileged a common mass of society. In addition, the existence of distinct routing protocols presents difficulties in standardization of routing models. Accordingly, it affects the design of authentication schemes because we always take the specific routing procedures into consideration. Therefore, in this paper, we bring forward the problem of designing an adaptable authentication scheme for both AODV and DSR protocols and try to introduce the first scheme in order for the other to come up with more valuable opinions.

Keywords: AODV, Authentication (OTP), TGT (Ticket Granting Control)

ISSN: 2320-1363

1. Introduction

Authentication is one of the most crucial modules for any given system. Since the time of wireless telegraphy, radio communication has been used extensively. Our society has been looking for acquiring mobility in communication since then. Initially the mobile communication was limited between one pair of users on single channel pair. The range of mobility was defined by the transmitter power, type of antenna used and the frequency of operation. With the increase in the number of users, accommodating them within the limited available frequency spectrum became a major problem. To resolve this problem, the concept of cellular communication was evolved. The present day cellular communication uses a basic unit called cell. Each cell consists of small hexagonal area with a base station located at the center of the cell which communicates with the user. To accommodate multiple users Time Division multiple Access (TDMA), Code Division Multiple Access (CDMA), Frequency Division Multiple Access (FDMA) and their hybrids are used. Numerous mobile radio standards have been deployed at various places such as AMPS, PACS, GSM, NTT, PHS and IS-95, each utilizing different set of frequencies and allocating different number of users and channels. A researcher firstly identifies the specific security requirements, and then certain signature is constructed against each requirement. In general, signatures for one application are not adaptable to others. However, we observe that the adaptability of signature schemes is preferable in some cases where standard operation procedures are not available. The adaptability of signature schemes will then be able to deal with the variability of the application domain, and in turn provide generic security for different procedures with the help of a single signature scheme.

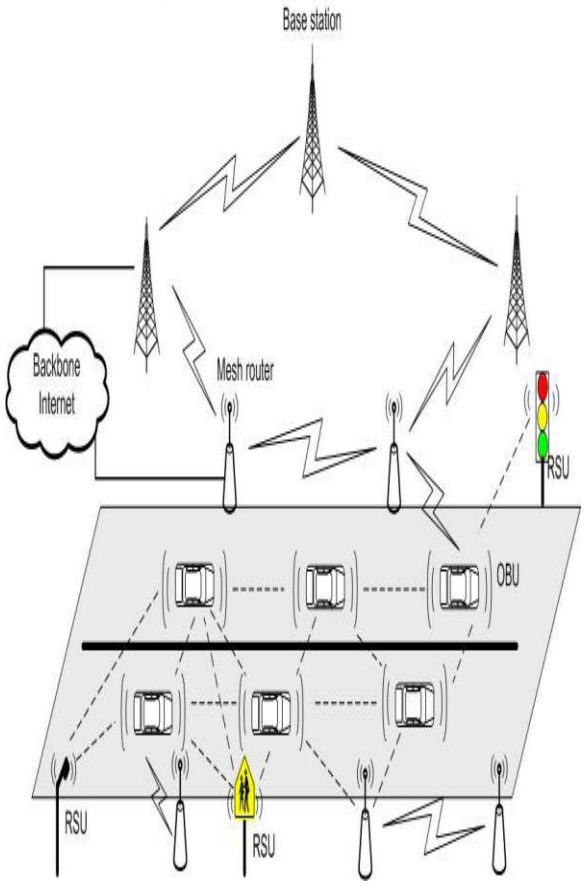

Fig 1.1 The basic radio transmission techniques (Simplex, Half Duplex, Full Duplex)

When a user moves from one cell to the other, to keep the communication between the user pair, the user channel has to be

ISSN: 2320-1363

shifted from one BS to the other without interrupting the call, i.e., when a cell moves into another cell, while the conversation is still in progress, the master cell automatically transfers the call to a new FDD channel without disturbing the conversation. This process is called as handoff.

2. Related Work

Communication in networks implies transmitting data packets along some certain paths, routes. How to find the path (routing) thus enable data transmission is the fundamental step of network communication. Routing is conducted using routing protocols which use metrics to evaluate what path will be the best for a packet to travel. A metric is a standard of measurement, such as path bandwidth, which is used by routing algorithms to determine the optimal path to a destination. To enable the process of path determination, routing algorithms initialize and maintain routing tables, which contain route information. Cellular telephone systems must accommodate a large number of users over a large geographic area with limited frequency spectrum, i.e., with limited number of channels. If a single transmitter/ receiver is used with only a single base station, then sufficient amount of power may not be present at a huge distance from the base station. For a large geographic coverage area, a high powered transmitter therefore has to be used. But a high power radio transmitter causes harm to environment. Mobile communication thus calls for replacing the high power transmitters by low power transmitters by dividing the coverage area into small segments, called cells. Each cell uses a certain number of the available channels and a group of adjacent cells together use all the available channels.

2.5G Mobile Networks:

2.5G networks also brought into the market some popular application, a few of which are: Wireless Application Protocol (WAP), General Packet Radio Service (GPRS), High Speed Circuit Switched Dada (HSCSD), Enhanced Data rates for GSM Evolution (EDGE) etc.

Third Generation Networks

3G networks enable network operators to offer users a wider range of more advanced services while achieving greater network capacity through improved spectral efficiency. Services include wide-area wireless voice telephony, video calls, and broadband wireless data, all in a mobile environment. Additional features also include HSPA data transmission capabilities able to deliver speeds up to 14.4Mbit/s on the down link and 5.8Mbit/s on the uplink.

WCDMA

It supports two basic modes of operation: FDD and TDD. In the FDD

ISSN: 2320-1363

mode, separate 5-MHz carrier frequencies with duplex spacing are used for the uplink and downlink, respectively, whereas in TDD only one 5-MHz carrier is time shared between the uplink and the downlink. WCDMA uses coherent detection based on the pilot symbols and/or common pilot. WCDMA allows many performance-enhancement methods to be used, such as transmit diversity or advanced CDMA receiver concepts. In this transmission technology, code specific frequency may not authenticate as of GSM technology.

3. Methods

Authentication is a process to verify a person's identity for security purposes and authentication factor is the piece of information used to achieve it. With an increase in the need for secure environments, the authentication modules of systems (including operating system) are moving from traditional one-factor authentication (usually based on a static password) to multi-factor authentication. People are now expecting efficient group communication in education, entertainment, and industries enabled by mobile ad hoc networks. The mobile communication has provided global connectivity to the people at a lower cost due to advances in the technology and also because of the growing competition among the service providers. We would review certain major features as well as standards of the mobile communication till the present day technology like Digital modulation formats were introduced in this generation with the main technology as TDMA/FDD and CDMA/FDD. The 2G systems introduced three popular TDMA standards and one popular CDMA standard in the market. Using the security requirements as a scale, we studied some existing secure routing protocols and justified their performance according to our security requirements. We noticed that the security of the existing proposals is not established from a realistic point of view. Some of the assumptions, such as the pre-establishment of security associations, and the requirement of time synchronization, generally conflict to the characteristics of mobile ad hoc networks. Hence of both levels follows authentication.

ISSN: 2320-1363

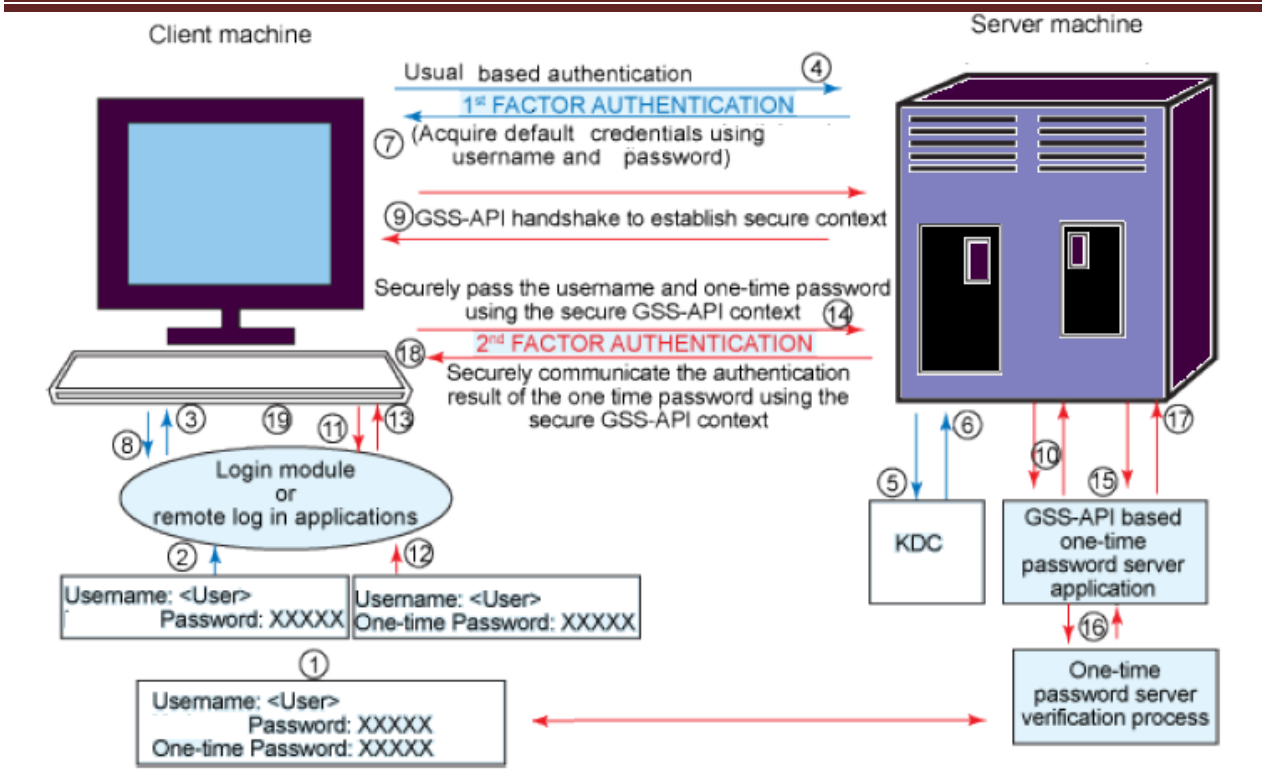

Fig: 3.1 Architecture Showing the Authentication of Mobile communication

The architecture involves following steps to exhibit the authenticated operation.

Steps 1 - Prompt the user to enter the user name and password.

Steps 2, 3, 4, 5, 6, 7 - Use the User Name and the corresponding password (which the user has to remember) to acquire the credential (TGT-Ticket Granting Ticket). If the password entered is incorrect, the authentication fails and the user is not allowed any access. On successful acquisition of the ticket (TGT), the first-factor authentication is completed. This is similar to any regular login module that based on authentication.

Steps 9, 10, 11 - Use the above-acquired credential and establish secure GSS-API context with the GSS-API based OTP application server residing on the system (assuming the OTP server has been using GSS-API).This involves a handshake between the client login module and the GSS-API-base done-time password application server. Note that here both the login module and the OTP application server are GSS-API-based applications running on the communication medium.

The main theme behind every communication technology is to be effective i.e. Efficient and secure authentication with integrity. Efficient secure features provide

ISSN: 2320-1363

protocol algorithm for two significant mobile ad hoc routing protocols, AODV and DSR. We intend to provide authentication, integrity and non-repudiation for AODV and DSR routing operations. It is generally recognized that the security deployment for mobile network routing protocol is difficult because of the following reasons.

- No central control exists in network. In a pure ad hoc environment, there is no trusted third party in the network.
- Nodes are resource constraint. The security deployment, such as signature generation and verification, will somehow consume the limited resources, which in turn affects the performance of the node.
- Routing protocols are distinct. Accordingly, an authentication scheme designed for certain types of routing protocols will not be applicable to others. On the other hand, design a general authentication scheme without considering the nature of protocols will result in huge waste in routing operation overhead.

Cryptographic primitives which provides authentication, integrity and non-repudiation are especially suitable for the mobile ad hoc scenario. Digital signatures, which have been long used as an authentication method, offer the above three properties. However, the deployment of a digital signature enabled authentication scheme in mobile ad hoc networks is not straightforward. The way leading to secure mobile ad hoc environments is full of disturbances.

Performance Analysis:

Following factors analyses the performance.

- ✓ Transmitted power
- ✓ Received power
- ✓ Area and shape of the cell
- ✓ Mobility of users

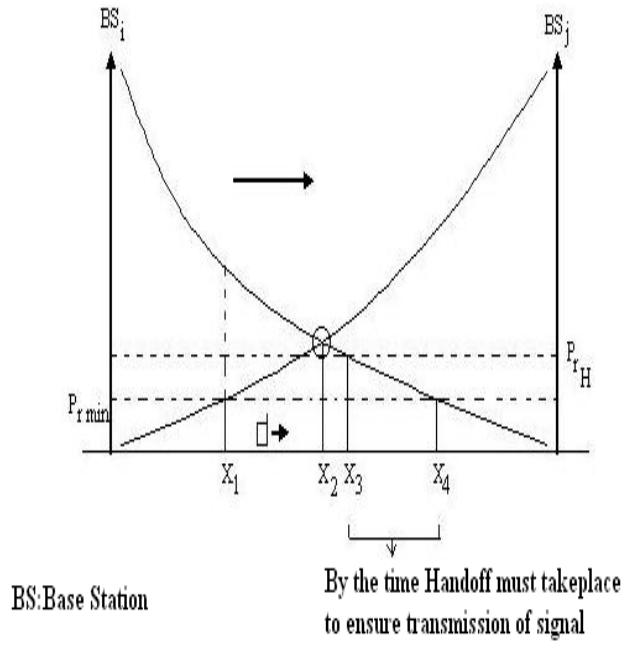

Fig.3.2 Association of cell tower when moving from i-th cell to j-th cell

ISSN: 2320-1363

Let us consider rectangular cell with sides R1 and R2 inclined at an angle _ with horizon, as shown in the Figure 3.2. Assume N1 users are having handoff in horizontal direction and N2 in vertical direction per unit length.
The number of crossings along R1 side is: (N1cosθ+N2sinθ) R1 and the number of crossings along R2 side is: (N1sinθ + N2cosθ) R2

Then the handoff rate Λ_H can be written as

$$\Lambda_H = (N1\cos\theta + N2\sin\theta)\ R1 + (N1\sin\theta + N2\cos\theta)\ R2$$

It follows the angle based approach for coupling while changing the network in order to ensure the authentication.

4. Conclusion

Tremendous changes are occurring in the area of mobile radio communications, so much so that the mobile phone of yesterday is rapidly turning into a sophisticated mobile device capable of more applications than personal computers/ laptops were capable of only a few years ago. Rapid development of the Internet with its new services and applications has created fresh challenges for the further development of mobile communication systems. As a highly dynamic, infrastructure less network, how to find peer nodes and establish links, namely routing, become the major issue to be solved. In our routing paradigm, shorter key size and signature size can reduce the data transmission overhead. In turn, the network performance can be enhanced by this means. Thus, the future work lead to the generation based speed and device based service.

5. Reference

[1] D. Boneh and H. Shacham. Group Signatures with Verifier Local Revocation. In proceedings of the 11th ACM conference on Computer and Communications Security (CCS), pp.168-177, 2004.

[2] J. Baek and Y. Zheng. Identity-Based Threshold Signature Scheme from the Bilinear airings. International Conference on Information Technology: Coding and Computing (ITCC04), Vol.1, pp. 124-128, April, 2004.

[3] M. Rahnema, "Overview of the GSM system and protocol architecture," IEEE Commun. Mag., vol. 31, no. 4, pp. 92–100, Apr. 1993.

[4] B. Mallinder, "An overview of the GSM system," in Proc. 3rd Nordic Seminar Digital Land Mobile Radio Commun., Copenhagen, Denmark, 1998, pp. 12–15.

[5] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks," IEEE Personal Commun., vol. 1, no. 1, pp. 24–31, 1993.

[6] M. S. Hwang, Y. L. Tang, and C. C. Lee, "An efficient authentication protocol for GSM networks," in Proc. AFCEA/IEEE Euro-Comm, 2000, pp. 326–329.

[7] S. Suzuki and K. Nakada, "An authentication technique based on

ISSN: 2320-1363

distributed security management for the global mobility network," IEEE J. Sel. Areas Commun., vol. 15, no. 8, pp. 1608–1617, Oct. 1997.

[8] C. H. Lee, M. S. Hwang, and W. P. Yang, "Enhanced privacy and authentication for the global system for mobile communications," Wireless Netw., vol. 5, no. 4, pp. 231–243, 1999.

[9] L. Buttyan, C. Gbaguidi, S. Staamann, and U.Wilhelm, "Extensions to an authentication technique proposed for the global mobility network," IEEE Trans. Commun., vol. 48, no. 3, pp. 373–376, Mar., 2000.

[10] K. F. Hwang and C. C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," IEEE Trans. Wireless Commun., vol. 2, no. 2, pp. 400–407, Mar. 2003.

[11] C. C. Lee, M. S. Hwang, and W. P. Yang, "Extension of authentication protocol for GSM," IEE Proc., Commun., vol. 150, no. 2, pp. 91–95, 2003.

[12] L. Harn and W. J. Hsin, "On the security of wireless network access with enhancements," in Proc. ACM Workshop Wireless Security, 2003, pp. 88–95.

[13] A. Peinado, "Privacy and authentication protocol providing anonymous channels in GSM," Comput. Commun., vol. 27, no. 17, pp. 1709–1715, 2004.

[14] C. C. Chang, J. S. Lee, and Y. F. Chang, "Efficient authentication protocol of GSM," Comput. Commun., vol. 28, no. 8, pp. 921–928, 2005.

[15] C. Tang and D. O.Wu, "An efficient mobile authentication scheme for wireless networks," IEEE Trans. Wireless Commun., vol. 7, no. 4, pp. 1408–1416, Apr. 2008.

[16] M. Al-Fayoumi, S. Nashwan, S. Yousef, and A. R. Alzoubaidi, "A newhybrid approach of symmetric/asymmetric authentication protocol for future mobile networks," in Proc. Wireless Mobile Comput., Netw. Commun., 2007, pp. 29–29.

[17] V. Kalaichelvi and R. M. Chandrasekaran, "Secure authentication protocol for mobile," Proc. Comput., Commun. Netw., pp. 1–4, 2008.

[18] K. P. Kumar, G. Shailaja, A. Kavitha, and A. Saxena, "Mutual authentication and key agreement for GSM," in Proc. ICMB, 2006, p. 25.

[19] K. Ammayappan, A. Saxena, and A. Negi, "Mutual authentication and key agreement based on elliptic curve cryptography for GSM," in Proc. ADCOM, 2006, pp. 183–186.

[20] 3rd Generation Partnership Project; Technical Specification Group SA; 3G Security, "Security architecture, version 4.2.0, release 4," 3GPP, TS 33.102, 2001.