REVIEW OF AUTHENTICATION TECHNIQUES FOR WIRELESS NETWORKS & MANET

Rajni Sobti[1]

[1]*Assistant Professor, UIET, Panjab University, Chandigarh, India*
sobtirajni@yahoo.co.in

Abstract

Mobile ad hoc network (MANET) is the most popular area of research nowadays due to its tremendous applications (military battlefield, commercial sectors, disaster areas, collaborative work etc). MANET is self organized network where all nodes are mobile in nature and may act as router as well as host because of its autonomous nature. In such a versatile environment, security of the network becomes a major issue. However, due to dynamic topology of the network and mobility of the nodes, it is very hard to achieve security goals such as confidentiality, authentication, integrity, non repudiation and availability. Among all these security goals, authentication is probably the most complex and important issue in MANET. Before communication, we should know to whom exactly we are talking, and then there is a question of protecting the data by means of cryptography. Authentication deals with identity of sender/receiver which is very important and required aspect for MANET where there is no central administration present in the network. In the present work, the issues related to the authentication in MANET, various techniques of authentication used in Traditional Wireless Network, Cellular Networks and especially in MANET along with their applicability and limitations have been discussed, which need to be addressed carefully before real time application of MANET

Key Words: *MANET, Authentication, Traditional Wireless Network (TWN), Threshold Cryptography, Certificate Authority.*

---***---

1. INTRODUCTION

MANET is a new generation of network offering unrestricted mobility without any underlying infrastructure. Devices in the MANET are able to communicate directly using wireless spectrum in a peer-to-peer fashion, and route messages through intermediate nodes **[1].** In order to exchange data from one node to another node, multiple “hops” may be needed because of limited transmission range of wireless network interfaces **[2, 20].** Link disconnections may occur frequently due to mobility of nodes and dynamic topology of the network **[3].** In MANET nodes have limited resources like battery and bandwidth. It does not have any trusted central authority. These are self-organized networks and intermediate nodes should participate to carry out the end-to-end communication **[4].** Above features of the MANET distinguish it from other communication networks. Some of the characteristics of ad hoc network includes: Self configuring network, no requirement of central administration, flexibility, mobility of nodes, access to information and services regardless of geographic position **[5]**. Mobility of nodes and infrastructure less network and ad hoc nature of these networks makes MANET suitable for many applications including: Military applications (battlefield survivability, operation without pre-fixed infrastructure etc.), sensor networks, collaborative work and personal area network (bluetooth), Communication between small household appliances and, commercial applications (Communication in the natural or manmade disaster areas, emergency/rescue operations, Vehicular ad hoc network for communicating between vehicles to provide traffic information and warnings) **[2, 5-9].** However, at the same time limited bandwidth; dynamic topology; battery constraint and security threats are some of the major challenges of MANET **[5, 9].** Due to existing characteristics of MANET, it is very easy for intruders to damage or disturb the network and hence it is very hard to achieve security goals such as confidentiality, authentication, integrity, non repudiation and availability. Most complex and important security goal for MANET is authentication. It is the first step in security where the identity of sender and receiver is established. If you don't know with whom you are communicating it is worthless to protect your data. If authentication is achieved then confidentiality is matter of encrypting the session using key on which the communicating parties agree **[10].** The issues related to the authentication in MANET, various techniques of authentication used in Traditional Wireless Network, cellular networks and especially in MANET along with their applicability and limitations have been discussed in this article, which need to be addressed carefully before real time application of MANET.

2. MAJOR ISSUES AND CHALLENGES IN SECURITY OF MANET:

Due to unique characteristics of MANET it is very difficult or challenging to design security protocol. Some of the important security issues have been discussed below **[11]:**

2.1 Shared broadcast radio channel: Since all the nodes in MANET use broad cast radio channel. Data transmitted by a node is received by all the nodes in direct transmission range. In such environment it is important to protect data from malicious node. Directional antennas are used to minimize this problem up to some extent.

2.2 Insecure operational environment: Operational environment of MANET is not always secure due to mobility of nodes. This issue is very important when MANET is used in battle field.

2.3 Lack of central authority: MANETs do not have central points. So it is very challenging to monitor traffic on the network.

2.4 Lack of Association: Proper authentication mechanism of nodes is required in MANET due to its versatile nature. Absence of it makes intruders to get access of network very easily.

2.5 Limited Resources availability: Nodes of MANET have very limited resources like battery power, memory and computational power. So, very complex security protocol/algorithms cannot be implemented.

2.6 Physical Vulnerability: Nodes of MANET can be damaged or can be theft easily due to their small size which will affect the security of the MANET.

3. AUTHENTICATION TECHNIQUES FOR TRADITIONAL WIRELESS NETWORKS (TWN)/CELLULAR NETWORKS & THEIR LIMITATIONS IN MANET

In TWN/Cellular networks if any attacker wants to communicate with network, it must first gain physical access. But in case of MANET, network is easily accessible and is prone to attack because of its characteristics discussed in section 1. So, security is always a big issue in MANET for researchers. Many protocols are available for security in TWN/cellular networks; however, these cannot be employed in MANET. Major reason for this is that TWN/Cellular networks have dedicated nodes to perform functions like routing, network management etc., however, in case of MANET these functions are performed by all available nodes in the network. Nodes in MANET are not trusted for all functions **[12].**

3.1.GSM (Global System for Mobile Communication)

GSM is based on challenge response mechanism with a pre defined algorithm A3. It require following three inputs: **[12, 13]:**

- IMSI (International Mobile Subscriber Identity)
- Secret key (K_i)
- RAND (Random number)

3.1.1 IMSI (International Mobile Subscriber Identity):- The IMSI is unique and stored in the Subscriber Identity Module (SIM) inside the phone**[14].** The IMSI is used to acquire the details of the mobile in the Home Location Register (HLR) or the Visitor Location Register (VLR).

3.1.2 Secret Key: (K_i) This key is 128 bit long and is stored in SIM. It is shared by HLR. (Home Location Register).

3.1.3 RAND (Random number): It is 128-bit function which is transmitted by the Base Station (BS)to the Mobile Station(MS).
Based on the inputs, a 32-bit SRES (Signed Response) is produced after calculation, which is transferred to the BS. The calculation of the signed response is processed within the SIM. Upon receiving the SRES from the subscriber, the BS network repeats the calculation to verify the identity of the subscriber **[15].** If the received SRES agrees with the calculated value, the MS has been successfully authenticated and may continue. If the values do not match, the connection is terminated and an authentication failure is indicated to the MS.
Authentication scheme described for GSM cannot directly be applied to MANET due to constraints such as infrastructure less network, life span of network, low computation power and battery life of nodes **[12].** In GSM AuC (Authentication database) is used to stored shared keys, however, in MANET there is no provision of central authority.

3.2 WEP (Wired Equivalent Privacy)

WEP provides security in terms of authentication and encryption to IEEE 802.11 networks. WEP security has two parts **[12, 16]**:

- Authentication
- Encryption

Authentication in WEP is also based on challenge response mechanism. In WEP, device who wants to connect to the network will send authentication request to the wireless access point (AP). Then the AP sends a challenge message to requesting client. Requesting device uses shared key to compute challenge and it sends a signed message back to access point. Wireless access point decrypts it and verifies whether the send response is correct or not? If it is correct then the requesting device will get access to the network, otherwise not.

This scheme is also not applicable to MANET, because there is no APs present in MANET. The nodes in MANET can leave and join networks at any time.

3.3 Bluetooth

Bluetooth is the most popular single hop ad hoc network with limited geographical coverage. Bluetooth has three security modes **[12, 17]**

- Security mode 1 is an unsecured mode and requires neither authentication nor encryption.

- Security mode 2 is designed with security flexibility such that a decision to use authentication and encryption is possible and lies with the security policy manager.
- Mode 3 provides full security

Bluetooth uses shared key centre (SKC) to achieve authentication using the challenge response scheme with the Link Key. Key establishment is the most complex part of Bluetooth security. A large part of its complexity lies in the key hierarchy because of the large number of keys involved.

Numbers of nodes in ad hoc network are very large as compared to Bluetooth, so, it is very difficult to store record of keys for nodes due to their less battery. Numbers of keys are directly proportional to the no. of nodes participated in the network. **[12]**

4. AUTHENTICATION IN MOBILE AD HOC NETWORKS (MANET)

Mobile Ad hoc networks (MANETs) are formed on demand. Due to the lack of infrastructure, there is no centre device present and the network topology may change rapidly and unpredictably due to the mobility of nodes. Moreover, each node has to act as a router and as a host for other nodes. This complexity of MANET has led to a variety of proposals which concentrate on different security problems. Authentication in MANET is achieved using certification authority, which is implemented using threshold cryptography.

4.1 Certificate Based Authentication In MANET [12, 18, 19]

Authentication in MANET is achieved through CA (Certification Authority). A CA is entity that issues certificates to the participating nodes for their authentication. A certificate is signed document /statement from CA that hold specific information of the node. While issuing certificate to the nodes CA gets Information from the node.

Some of the important functions performed by CAs are described as follows:

- *Certificate issue*: CA issues certificates to the nodes for authentication purpose. Before issuing certificates to the nodes CA gets some unique information from the node so that the certificate should be issued to the genuine node only.
- *Certificate Renewal*: All certificates are issued for specific time period and each certificate has its expiry time. Before its expiry it must be renewed by the CA.
- *Certificate Revocation:* If CA found any corrupted or misbehaved node then it can also revoke the certificate

All certificates are stored in local repository of CAs.

4.2 Method to Implement CA

CAs can be achieved either centrally or distributed manner. Central implementation of CA in Ad hoc network is not good approach due to its characteristics; however, distributed or decentralized system is possible in MANET. Threshold cryptography is one amongst the various distributed schemes for authentication in MANET and is discussed below.

4.3 Threshold Cryptography

It is distributed approach used for authentication and for key management in MANET **[12, 18, 19].** A pair of public and private keys is used in threshold cryptography. Where public key of the CA is known to all participates and private key or system secret is known to CAs. Virtual CAs are created in Threshold secret sharing approach. A trust (Shared secret) is distributed among multiple nodes of network, to achieve virtual CA. If L no. of nodes which would form the virtual CA, then system secret is divided into X parts, such that L(<X) of these parts are enough to carry out a cryptography operation that would have been possible with system secret. It means that system can tolerate the compromise of up to L-1 nodes without the security of the whole system being compromised.

5. LIMITATIONS OF CERTIFICATION BASED AUTHENTICATION MECHANISM IN MANET

In this section, limitations of CA and its implementation method through threshold cryptography **[12, 18, 19**] have been discussed.

CA mechanism has following limitations:

- It is very difficult for CA to be available throughout the time.
- It is very difficult to choose efficient method for certification so that security of network should not be compromised.
- If the network is growing then it is very difficult to give certificate to all nodes by same CA all the time.

Limitations of threshold cryptography:

- In this method it is very critical to set the value of threshold, so that mechanism should work efficiently.
- Out of X servers if one is moved out of the range due to mobility then it is very difficult for the system to work.
- Storing of public key on server is again very difficult if network is growing.

6. CONCLUSIONS

In this article, the issues related to the authentication in MANET, various techniques of authentication used in Traditional Wireless Network, Cellular Networks and especially in MANET along with their applicability and limitations have been discussed, which need to be addressed carefully before real time application of MANET. From the literature cited above, it can safely be concluded that due to lack of the central administration, dynamic topology of the network and mobility of the nodes, it is very difficult to achieve the security in MANET, especially authentication. Further, owing to the limitations of the CAs and its implementation using threshold cryptography, there is a need for the new/innovative and secure authentication mechanism for the real time application of MANET.

REFERENCES

[1]. Hinds A, Ngulube M, Zhu S and Al-Aqrabi H, “A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)”, International Journal of Information and Education Technology , 3(1), pp1-5, 2013.

[2]. Cheuk Han N, “Trust and clustring-based authentication service in MANET” A M.Phil. thesis in Computer Science and Engineering, The Chinese University of Hong Kong, 2004.

[3]. Gupta AK, Sadawati H and Verma AK, “Review of various routing protocols for MANETs”, International Journal of Information and Electronics Engineering, 1(3), pp251-259, 2011

[4]. Chlamtac I, Conti M, Jennifer J.-N. Liu, “Mobile ad hoc networking: Imperatives and challenges”, Elsevier, Ad Hoc Networks 1 pp13–64, 2003.

[5]. Aarti and Tyagi SS, “Study of MANET:Characteristics, Challenges, Application and Security Attacks”, International Journal of Advanced Research in Computer Science and Software Engineering, 3(5):252-257, 2013.

[6]. Haas JDZ., Liang B., Papadimitatos P and S. Sajama, "Wireless ad hoc networks", In Encyclopedia of Telecommunications J. W. John Proakis, Ed., 2002.

[7]. Raya M and. Hubaux JP, “The Security of Vehicular Ad Hoc Networks,” In proc. ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN’05), 2005.

[8]. Dawoud DS and Gordon RL, “Trust Establishment in Mobile Ad-Hoc Networks:Key Management. In. Mobile Ad-Hoc Networks:Application”, Wang X (Ed.), InTech, Available from: http://www.intechopen.com/books/mobile-ad-hoc-networksapplications/trust-establishment-in-mobile-ad-hoc-networks-key-management, 2011.

[9]. Bakshi A, Sharma AK and Mishra A, “Significance of Mobile ad hoc networks (MANETs) ”, International Journal of Innovative Technology and Exploring Engineering, 2(4):1-5, 2013.

[10]. Shuyao Yu Youkun Zhang Chuck Song Kai Chen, "A security architecture for Mobile Ad Hoc Networks", http://www.researchgate.net/publication/228382762_A_security_architecture_for_Mobile_Ad_Hoc_Networks .

[11]. Murthy CSR and Manoj BS, “Ad Hoc Wireless Networks: Architecture & Protocols”, 2nd Edition, Pearson Education, pp 498-500, 2005.

[12]. Safdar GA, McGrath C and McLoone M, “Existing Wireless Network Security Mechanisms and their Limitations for Ad Hoc Networks”, ISSC 2006, Dublin Institute of Technology, June 28-30,pp 197-202, 2006,.

[13]. Mishra S and Modi N, "GSM Mobile Authentication Based on User SIM," IJCST, ISSN-2347-8578, Vol-2, Issue-6, pp 121-125, 2014.

[14]. http://www.techopedia.com/definition/5067/international-mobile-subscriber-identity-imsi

[15]. http://www.tutorialspoint.com/gsm/gsm_security.htm

[16]. Vibhuti S, "IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability, CS265 Spring, 2005.

[17]. Kumar T," Improving Pairing Mechanism in Bluetooth Security," IJRTE,Vol-2 No-2, 165-169,2009.

[18]. Shaveta, Singh P and Preet R, "Reviewing MANETs & Configuration of Certificate Authority(CA) for node Authentication," IJCSIT, ISSN-0975-9646,Vol-4 (6),pp 974-978, 2013.

[19]. Mamatha. T," Network Security for MANETS," IJSCE, ISSN: 2231-2307,Vol-2,Issue-2, May-2012.

[20]. Broch J, Maltz DA., Johnson DB. Hu YC and Jetcheva J, “A performance comparison of multi-hop wireless ad hoc network routing protocols”, In The 4th Annual International Conference on Mobile Computing and Networking (MobiCom’98), pages 85–97, Oct. 1998.

BIOGRAPHIES

RAJNI SOBTI received M.E. in Information Technology from University Institute of Engineering and Technology, Panjab University, Chandigarh. She is currently working as Assistant professor in I.T. department, U.I.E.T. Panjab University, Chandigarh. Her main research interest is Mobile Ad hoc networks.