Authentication and Confidentiality in Wireless Ad Hoc Networks

Prof.S.C.Saraf
Department of Electronics and Telecommunication Engineering
Maharashtra Institute of Technology,Aurangabad ,M.S. India.

Prof.M.D.Pawar
Department of Electronics and Telecommunication Engineering
Maharashtra Institute of Technology,Aurangabad ,M.S. India.

Prof.P.P.Patil
Department of Electronics and Telecommunication Engineering
Maharashtra Institute of Technology,Aurangabad ,M.S. India.

Abstract—In this paper, the security and authentication of ad hoc wireless networks is presented by referring various papers by various authors. The various security issues containing cryptographic techniques and key generation techniques and international standard IEEE 802.11 is explained.

Keywords:-Authentication,Ad hoc network,cryptographic

I. INTRODUCTION

A Wireless Ad Hoc Network is a group of low capacity computing devices(laptops, PDAs etc) connected through wireless links. These devices are generally mobile with frequent location changes. Communication between the devices can be established anywhere, in a decentralized manner with-out the support of an established infrastructure. The purpose of ad hoc networks is to enable the mobile device users to share resources, provide adequately addressing the security issues. ITU-T Recommendation X.800[3] – Security Architecture for OSI – identifies the required security services for the communication networks. The simply establish a network on information exchange. Ad hoc networks have a number of applications where infrastructure free communication is required. These applications include emergency relief, military operations, on-demand conferencing and home networking. Like any communication network, the true potential of wireless ad hoc networks cannot be exploited without considering and security services have been broadly categorized into five groups namely authentication, access control or authorization, confidentiality, integrity and non-repudiation. Security management that have been
identified aim at ensuring availability, accountability and event management. Like all communication networks, wireless ad hoc networks require the same set security services. However, the unique characteristics of ad hoc networks(decentralized communication, heterogeneous nature of devices, high mobility and frequently changing network topology) result in unique challenges to the security of ad hoc networks. The focus of this chapter is the security services of authentication and confidentiality with explicit consideration of the security challenges of wireless ad hoc networks. The security service of authentication provides the assurance that any particular entity (wireless device) is the one who it claims to be. With the perspective of wireless ad hoc networks, the service of authentication is further divided into two components: (i) Access Authentication and (ii)Origin Authentication. The objective of access authentication is to ensure that only legitimate devices can access the network services. This in turn protects the network from illegal access and malicious je operdization. On the other hand, the origin authentication ensures that within the authenticated network nodes, a node must be able to prove its identity for every communication session with any other node in the network. This ensures that an authenticated node cannot impersonate another legitimate node in the network. Consequently, the network is protected against misbehaving and compromised nodes. One of the methods used in the Internet for authentication is asymmetric key cryptography. In this cryptographic technique the identity of the user/device is bound with a private and a public key. The public key is known to everyone while the private key is known only to the device that owns the key. Suppose device A intends to communicate with device B, it encrypts the message using its private key and a publically known encryption algorithm. Upon receiving the message, device B verifies if A transmitted the message by decrypting the message using public key of device A. If the message is successfully decrypted (correctness of a message is

verified through Cyclic Redundancy Check, CRC), the message is considered to be originating from the authentic device A, otherwise, it is assumed that an unauthenticated device is impersonating the device Confidentiality ensures that the information transmitted across the network is accessible only b the intended recipients. In the example of the
preceding paragraph, to ensure the confidentiality of the information, device A encrypts the message using public key of device B. Upon receiving the message, device B decrypts the message using its private key. In this case, a device can decrypt the message successfully only if it is in possession of valid private key of device B. Since the private key of device B is only known to the device itself, only the device B can decrypt the message successfully, ensuring the message confidentiality. Authentication and confid Authentication in Wireless Ad Hoc Networks.
The objective of authentication is to ensure that only legitimate devices can access the network services. The network nodes should be able to identify a malicious device, impersonating a legitimate participant node. Furthermore, if a participant device misbehaves after the trust relationship is established, the authentication mechanism should be able to evict the misbehaving node. Such a node should be denied of any further access to the network services or communication with any legitimate node in the network. A comprehensive analysis of the authentication protocols for wireless networks can be found in.[16] The security techniques used to provide the authentication services can broadly be classified into three categories: (i) Symmetric cryptography, (ii) Asymmetric cryptography, and(iii) Collaborative mechanisms (i.e., Threshold cryptography). In this section, we explain the three categories in detail. We detail different solutions proposed for ad hoc networks based on these techniques with a discussion on the objectives of each solution, the employed approach, and strengths and weaknesses of the proposed solution. We also explain the important aspect of revocation, a mechanism used for evicting the misbehaving nodes or refreshing the authentication material for a compromised node.

A. Symmetric Cryptographic Techniques –

The symmetric cryptographic techniques employ the use of a shared secret key among the participating nodes (pair of nodes intending to communicate or the nodes requesting access to the network) to provide the service of authentication. In its simplest form, a common key is issued to all legitimate nodes in the network. This key can be distributed manually to the participant nodes. Any node in possession of the key can authenticate itself by presenting the key and can access the network or any service offered by the network. The computational and communicational overheads involved in this kind of authentication are negligible. However, symmetric key based techniques are only suitable for small scale networks. The probability of the shared secret key being compromised increases proportionally with the increasing network size. Furthermore, if a single node is compromised, The entire network is compromised. Therefore, the secret key needs to be changed frequently in order to ensure the appropriate level of security. Wired Equivalent Privacy (WEP) protocol: the security mechanism initially employed by the IEEE 802.11i stand for WLAN security[4] is predominantly based on the symmetric cryptographic technique. In addition to the issues identified above, a number of additional security issues have been identified. We do not go into details of these issues here.
Interested readers are referred to the related publications Asymmetric cryptographic solutions involve the use of a pair of keys (a public key and a private key) for each participating node. The private key is known only to the node to whom it was issued, while the public key of the node is known to all the participating nodes. These keys are pre-distributed(often before joining the network) to the nodes by a Certification Authority in form of a digital certificate. A digital certificate binds the node identity with the two keys and associates an expiration time with the certificate. The certificate is then signed by the private key of the certification authority to make it tamper proof. To authenticate itself and to access the network services (join the network or start a communication with a member node) a node presents its digital certificate. The existing member nodes can extract the information stored in the certificate by decrypting the certificate using the public key of the certification authority, which is distributed among all participant nodes. The validity of the certificate can then be verified to ensure that the certificate was issued to the node which is presenting the certificate and that the certificate has not expired yet. If the certificate is valid, the node is allowed to access the services it requested, otherwise, the node is considered a malicious attacker and is denied network access. Note that the certificate of the misbehaving nodes can be revoked. This is achieved through a certificate revocation list that can be maintained at a centralized location where all the revoked certificates can be listed. Several issues specific to ad hoc networks are involved with the above mentioned authentication technique: (i) the decentralized and infrastructure free nature of ad hoc networks make it impractical to have a centralized certification authority; (ii) computational and communicational overhead can be significantly high in case of asymmetric cryptography; and (iii) in the case of misbehaving nodes, certificate revocation can be a challenging task as a centralized certificate revocation list maintenance is impractical. Nevertheless, the strengths of asymmetric cryptographic techniques have encouraged the researchers to employ the technique for authentication and security of wireless ad hoc networks. Several solutions to the above mentioned problems have been proposed in the literature. we

discuss the techniques that focus on the distribution of the certification authority and authentication server within the network nodes.

B . The key revocation mechanisms employed in wireless ad hoc networks.

Collaborative Mechanisms confidentiality are discussed together in this chapter

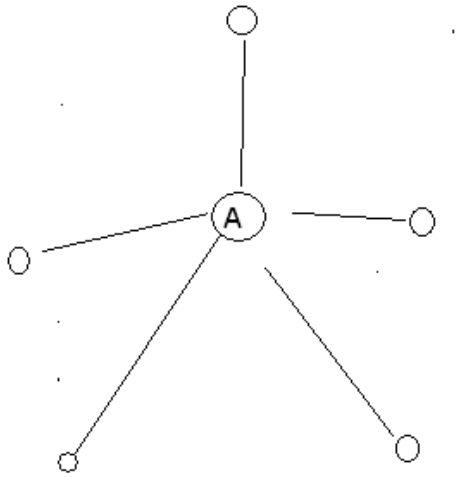

Figure. 1. Neighbor collaboration for private key generation in Wireless Mesh Networks.

In networks, Certificate Revocation Lists (CRL) are maintained at some centralized, publically accessable location This list comprises of the information about the revoked certificates. Network nodes can access the list from a centralized location. Alternatively, the list can be broadcasted that regular intervals to the participating nodes. In wireless ad hoc networks, the assumption of a centralized location is impractical and a single computationally limited node cannot be responsible for maintaining and broadcasting CRL.Another technique proposed by Michell et al.[28] is a state based key hop protocol based on stream ciphers. The authors have proposed the use of the RC4 algorithm, however, unlike WEP where the state of RC4 is reinitialized for every packet, the authors propose that same seed should be used to generate the streams for a specific duration of time. The issue of a weak key is avoided by using a stream offset. The offset indicates the starting point down the stream from which the packet encryption should start. The two communicating nodes are synchronized such that the nodes know the initial seed for the stream (Base key), duration for which the key remains valid, RC4 states, and the offset. The RC4 states define the offset for the subsequent packets after the first packet is transmitted using initial offset. After the fixed duration, the base key expires and new base keys should be achieved (hence the name key hop) and the states should be re-synchronized by the two nodes. Note that no method is detailed for distribution of the synchronization parameters among the two nodes. The proposed algorithm offers a strong and light weight encryption algorithm and reduced computational overhead. However, the issue of distributing the parameters required for synchronization is not addressed. Knowledge of these parameters can enable an adversary to easily decrypt the entire communication between any pair of nodes. Therefore, a secure method for distribution of these parameters is of utmost importance for the secure
operation of the protocol. Soliman and Omari[5] have proposed a security framework based on stream cipher for encryption to provide the services of data confidentiaity, data integrity, and authentication. This framework ensures per packet mutual authentication between the two communicating nodes within the network. The objective of using stream cipher is to allow online processing of the data. Consequently, minimum delay is introduced because of the security provisioning. Two secret security keys, Secret Authentication Key (SAK) and Secret Session Key (SSK), are used for authentication of the supplicant and authenticator. SAK is exchanged between the supplicant and the authenticator after initial mutual authentication from the authentication server.Junaid et al.[15] have proposed a piggyback challenge-response protocol, which relies on Advanced Encryption Standard (AES) in Counter Mode[30]for providing data confidentiality. AES in counter mode requires a counter block and an encryption key to encrypt the message. The message is divided into blocks of 128 bits and each block is encrypted using the encryption key and a unique counter block (see[30] for details). The authors propose the extension

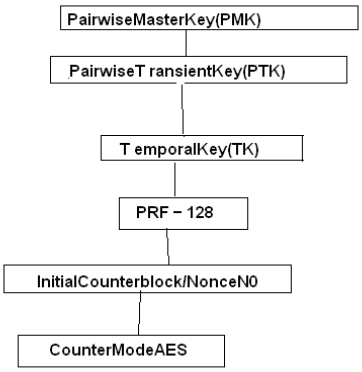

Figure.2. Key Generation Mechanism

IEEE 802.11i[4] key generation mechanism as shown in Figure2.
The temporal key (TK) generated through IEEE 802.11i using four-way handshake is used as seed for the pseudo-random function (PRF-128) to generate the initial counter. This initial counter is used as the AESinitial counter block, which is linearly incremented to generate subsequent counter blocks. The initial counter is also used as the first nonce N_0, which is transmitted with the first message.

II.EXPERIMENT AND POOF FOR DATA CONFIDENTIALITY AND ORIGIN AUTHENTICATION

Suppose node A and node B share a PMK and wish to communicate. Assume that node A initiates the communication by sending an initial message to node B. Node A will use TK as the encryption key for this message. It will encrypt the first message along with the nonce N_0 (generated using Fig. 2) and the Meta Data .$E_{TK}(N_0||Data||MetaData)$. The field Meta Data is used for message integrity and is beyond the scope of this chapter. The intended recipient (node B), upon receiving the message will also generate the initial counter (also the nonce N_0) using the procedure shown in Fig. 2. It will decrypt the message , TK being the decryption key. After decryption, node B will compare its own generated nonce value with the received nonce. Since both nodes A and node B share the PMK, the N_0 generated should be the same as the N_0 which was transmitted as a part of the message by node A. The nonce will act as challenge text to authenticate the source of the message. $D_{TK}(E_{TK}(N_0||Data||MetaData)) = N_0||Data||Metadata$ Node B will then use N_0 as the encryption key for the reply, rather than the TK. PRF-128 will be used to generate a new nonce N_1, which will be concatenated with the data and Meta Data, encrypted using N_0 and transmitted back to Node A. Thus, a new nonce is generated iteratively for each subsequent message, which enhances the robustness of the security IEEE 802.11i[4] is the defined standard for the MAC layer security of the wireless networks. We dedicate this section to discuss the IEEE 802.11i standard. The section begins with the explaination of the security methods used for the services of authentication and confidentiality in the IEEE802.11i standard. Subsequently, we expose the vulnerabilities in IEEE 802.11i that render the standard prone to security attacks. These weaknesses lead to attacks including: pre-computation and partial matching attacks; session hijacking attacks; man-in-the-middle attacks exploiting vulnerabilities in IEEE 802.1X; and DoS attack exploiting vulnerabilities in four-way handshake. We also briefly discuss the proposed prevention mechanisms for these attacks.IEEE 802.11i standard consists of three components: Key Distribution component, Mutual Authentication component, Data Confidentiality, Integrity, and Origin Authentication component.

III.CONCLUSION

In this chapter, we considered the two security services of authentication and data confidentiality in wireless ad hoc networks. The security issues relating to authentication and confidentiality, specific to ad hoc networks ,have been identified and the characteristics of these services have been outlined. The proposed security solutions for the two services of authentication and confidentiality have been categorized into three categories, depending upon the underlying security techniques. The proposed solutions within each category are discussed in detail. Finally, IEEE 802.11i, standard for wireless security is detailed, its vulnerabilities are highlighted and the solutions proposed for the vulnerabilities are discussed. The chapter ends with a note on the open issues relating the two security issues of authentication and confidentiality in wireless ad hoc networks.

REFERENCES

[1] Arunesh Mishra, William A. Arbaugh, An Initial Security Analysis of the IEEE 802.1X Standard, Technical report, university of Marryland. February 2002.
[2] Hao Yang, Shu. J, Xiaoqiao Meng, Songwu Lu. SCAN: self-organized network-layer security in mobile ad hoc networks, Appears in: IEEE Journal on Selected Areas in Communications, Volume: 24, Issue: 2, pages 261- 273,Februry 2006.
[3] Security Architecture for Open Systems Interconnection for CCITT Applications, ITU-T Recommendation X.800, March 1991.
[4] IEEE Std. 802.11i-2004, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements.
[5] Hamdy S. Soliman, Mohammed Omari. Application of synchronous dynamic encryption system in mobile wireless domains. In Proceedings of the 1st ACM international workshop on Quality of service and security in wireless and mobile networks (Q2SWinet '05), Pages 24-30, October 2005.
[6] IEEE Std. 802.1X-2004, IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control June, 2001. http://standards.ieee.org/getieee802/download/802.1X-2004.pdf
[7] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Ed., Extensible Authentication Protocol (EAP), RFC 3748, June 2004.
[8] C. Rigney, S. Willens, A. Rubens, W. Simpson, Remote Authentication Dial In User Service (RADIUS), RFC 2865, June 2000.
[9] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, Diameter Base Protocol, RFC 3588, September 2003.
[10] D.Whiting, R. Housley, N. Ferguson, Counter with CBC-MAC (CCM), RFC 3610, September 2003.
[11] L. Zhou and Z. J. Haas. Securing Ad hoc networks, IEEE Network Magazine,13(6), November/December 1999.
[12] H. Luo and S. Lu. Ubiquitous and robust authentication