Secure and Efficient Key Management Scheme for Wireless Mesh Network

Md. Iftekhar Salam*, Madhusudan Singh*, 이상곤**, 이훈재**
*동서대학교 유비쿼터스 IT 과
**동서대학교 컴퓨터정보공학부
e-mail : iftekharsalam@gmail.com, madhusudanster@gmail.com, nok60@gdsu.dongseo.ac.kr, hjlee@dongseo.ac.kr

무선 메쉬망에서의 안전하고 효율적인 키관리 스킴

Md. Iftekhar Salam*, Madhusudan Singh*, Sang-Gon Lee**, HoonJae Lee**
*Dept. of Ubiquitous IT, Dongseo University, Busan, Korea
**Division of Information Network Engineering, Dongseo University, Busan, Korea

ABSTRACT

Wireless mesh network (WMN) is a type of mobile ad-hoc network consists of wireless router, mobile clients and gateway which connects the network with the Internet. To provide security in the network it is required to encrypt the message sent among the communicating nodes in such way so that only legitimate user can retrieve the original data. Several security mechanisms have been proposed so far to enhance the security of WMN. However, there still exists a need for a comprehensive mechanism to prevent attacks in data communication. Considering the characteristic of mesh network, in this paper we proposed a public key cryptography based security architecture to establish a secure key agreement among communicating nodes in mesh network. The proposed security architecture consists of two major sections: client data protection and network data protection. Client data protection deals with the mutual authentication between the client and the access router and provide client to access router encryption for data confidentiality using standard IEEE 802.11i protocol. On the other hand, network data protection ensures encrypted routing and data transfer in the multi hop backbone network. For the network data protection, we used the pre-distributed public key to form a secure backbone infrastructure.

1. INTRODUCTION

Wireless mesh network (WMN) is a new emerging and attractive communication technology for the next generation to provide better network services. WMN is formed up of radio nodes organized in a mesh topology. These networks are able to provide wireless Internet connectivity in a substantial geographic area and allow network deployment at a much lower cost compare to the conventional wireless network. WMNs combine concepts from a diverse set of existing and emerging wireless technologies. WMN can cover the same geographical area with much less number of routers compared to the Wireless Fidelity (Wi-Fi) and are thus more suitable for areas that do not have existing data cabling or for the deployment of a temporary wireless network.

WMN has been a field of active research in recent years. However, most of the research has been focused around various protocols for multi hop routing leaving the area of security mostly unexplored [1, 2]. Security is one of the major issues in WMN. WMNs are more vulnerable to security breaches than conventional networks because they are physically more accessible to possible adversaries. The memory and energy limitations of nodes are a major obstacle to implement traditional security solutions. The fact that wireless mesh networks utilize unreliable communication media and are left unattended once deployed makes the provision of adequate security countermeasures even more difficult. When the security of any system is discussed it addresses three major concerns: Confidentiality, Integrity and Authenticity [3]. Encryption algorithm is usually used to ensure confidentiality; whereas, cryptographic hash functions or message authentication code (MAC) is implemented in order to ensure integrity of data and authenticity. Security primitives must have to achieve these basic concerns. Many security primitives have been proposed so far to ensure security of network. However, these security primitives are implemented in high-end-systems without considering any memory or energy consumption. Therefore, the security mechanism for ultra-low power devices must be carefully selected taking the limited memory and energy consumption into account.

The objective of this paper is to identify the underlying security problems of wireless mesh network and to provide a potential solution which will be able to enhance the security of the system. In this paper, we focus on providing data confidentiality for communication in WMNs. To ensure the complete security of WMN, a security architecture is presented in this paper which ensures both client and network data protection.

2. RELATED WORK

Two main security areas can be identified for WMN: user

data protection and network data protection. User data protection deals with the mutual authentication between the client and the access router and provide client to access router encryption for data confidentiality. On the other hand, network data protection ensures encrypted routing and data transfer in the multi hop backbone network. In a WMN environment authentication of user and access control can be managed by using standard techniques [4, 5, 6], which provides a high level of flexibility and transparency. Using the standard access control technique all users can access to the mesh network without changing their client devices and software. However, in wireless mesh network clients are often mobile which poses severe challenges to the security of the system. Proactive key-distribution can be imposed to compete with these problems [7, 8, 9]. A self-organized key management scheme was proposed [10] to distribute and manage the security keys in mesh network. In this self-organizing key management system, certificates are stored and distributed by users themselves. When the public keys of two users need to be verified, they first combine the local certificate repositories and then find the suitable certificate chains within the combined repositories that can pass this verification. The algorithm for self-organized key management was further enhanced by C. Srdjan et. al [11]. A distribution of trust in the key management service was proposed which utilizes the idea of threshold cryptography [12]. The algorithm divides the private key of the service into several shares and assigns one shares to each node. For the certificate generation, a partial signature is generated by each node for the certificate using its private key and all partial signature collected from the nodes are then combined by central authority.

3. PROBLEM STATEMENT

There exist a number of security concerns associated with the WMN. These security concerns are needed to be analyzed in detail in order to design appropriate security mechanisms and overcome security problems that arise in wireless network. Security is always a critical step to deploy and manage WMN. However, these constraints of WMN as well as their network architecture pose new challenges in achieving security goals in a mesh network environment. To provide security it is necessary to encrypt the message sent among communicating nodes. In a mesh network nodes need to agree on an encryption key to establish a secure communication. Agreement of the encryption key in a communication network can be viewed as a part of the key management problem, which is one of the most important tasks for network security. However, achieving such key agreement in a resource constrained environment like WMN is not a trivial task as security protocols always require additional overhead on the computational, storage and energy resources. Moreover, the key management for WMNs becomes much more difficult, because there is no central authority, trusted third party or server to manage security keys [1, 2]. Several key agreement schemes have been proposed so far to ensure security in WMN. Some of the schemes are very effective in terms of security, but quite complex to apply in real world environment. Thus, there is a need for a better security system which can combine low operational costs with a high security performance.

4. SECURITY MODEL FOR WIRELESS MESH NETWORK

The proposed security architecture for wireless mesh network is mainly divided into two parts: client data protection and network data protection. This section addresses the proposed key pre-distribution based security architecture for wireless mesh network which ensures both client and network data protection. The following subsection illustrates the network model for the proposed security architecture and the establishment of cryptographic keys for secure data transmission in wireless mesh network.

4.1 Network Architecture

The network consists of a set of wireless router, mobile clients and gateway which connects the network with the Internet. The set of wireless router is considered to be static and communicate through a multi hop wireless link to form a backbone network. The mobile clients are connected to the backbone network through a local access router and communicate with each other through the multi hop wireless backbone routers. Figure 1 illustrates the network architecture consisting of wireless mesh routers and mobile clients.

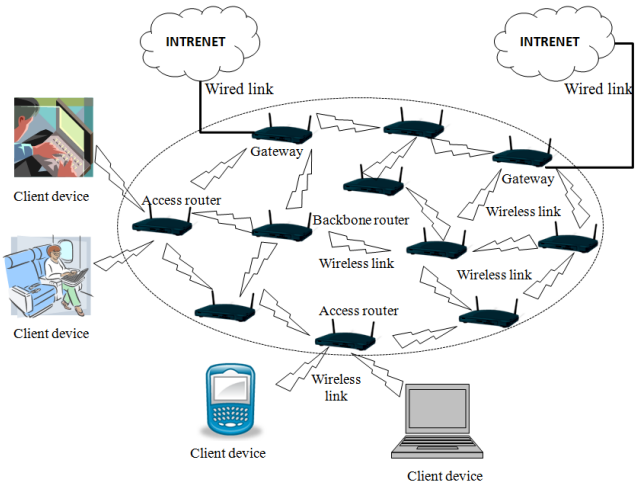

Figure 1: Network Architecture

To be a part of the backbone network all the routers are needed to be authorized by the administrator of the network. The authorization of the routers is ensured by the use of digital signature. Addition of new mesh router in the backbone network is supported through the use of gateway. Each new router joining the network must notify the gateway with the help of administrator and later on gateway will authorized the newly joined router by distributing its public key to all the other backbone routers. All the authorized routers in the backbone network are considered to be trusted.

4.2 Client Data Protection

To ensure the user data protection it is necessary to encrypt the data exchanged between the client and access router. As well as client and the access router needs to verify each other's identity to provide authentication. To achieve the highest level of security the access method to the

backbone router is designed to be identical to that of a standard WLAN, where mobile device connect to an access point. In our security architecture we used the IEEE 802.11i protocol [4] that will allow the mesh client to access the backbone network. The IEEE 802.11i protocol will ensure the authentication and authorization as well as confidentiality of data for the mesh clients. However, this security mechanism will only protect the access link between the mobile client and backbone access router. In the wireless backbone the data is transmitted through multiple hops. As a result, an adversary can eavesdrop in the backbone link when the data is flowed through the mesh routers unless there is some security primitives present to protect the backbone link.

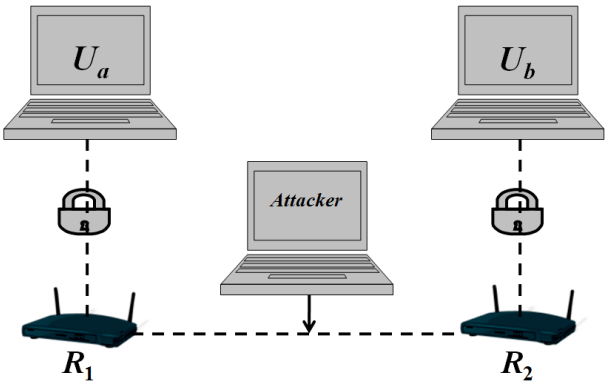

Figure 2: Attacker can mount an attack unless a security mechanism is present to protect the backbone link

Figure 2 illustrates such a scenario, where two users Ua and Ub are communicating with each other over the mesh backbone network. Ua and Ub are connected in a secure way to the mesh backbone network through access router R1 and R2 respectively. If the wireless link established in the backbone network between router R1 and R2 are not protected then an adversary can eavesdrop the traffic that is forwarded through the backbone network. Therefore, it is necessary to encrypt the data forwarded through the backbone network as well to ensure the complete security of the system. In our proposed security architecture, the security of the backbone network is ensured by exploiting the public key cryptography.

4.3 Network Data Protection

In this section we propose a security mechanism to ensure the security of the data in the backbone network. The proposed backbone network security architecture will use the pre-distributed public key to establish a secure network infrastructure. The main steps associated with the backbone network security architecture are illustrated as follows:

Initialization – The first step is referred as the initialization phase or key pre-distribution phase. This phase is performed offline before deploying the wireless backbone routers. First, a master public key and the corresponding master private key will be generated which will be used for the communication with central gateway. The master public key will be stored in all the nodes memory and gateway has knowledge about the corresponding private key. Nodes will use this master public key to establish a secure communication link with the gateway. Following this based on some asymmetric key algorithm/public key algorithm the system administrator will generate a random public key and corresponding private key for each of the routers in the network. Each router will store these random pair of keys before deployment. Let, N is the number of routers in the backbone network. The system manager will generate N number of public keys (PU1, PU2, PU3,…, PUN) along with the corresponding private key (PR1, PR2, PR3,…, PRN); where PUN defines the N-th public key whereas PRN defines the corresponding private key . After the key generation is performed each pair of keys (PUN, PRN) will be assigned to a random router in the network. For example, router R1 will be assigned a pair of key (PU1, PR1) where PU1 is the public key and PR1 is the private key for this node. System administrator will enable each router to store the public keys of all other routers in the network and the corresponding ids. In mesh network, all the nodes are deployed manually; so each node can know exactly about its neighboring nodes identity. Therefore, each node will store the information of their neighbor nodes identity before the deployment with the help of system administrator. Finally, system administrator will register these entire groups of router to the gateway. The registration needs to be performed in person or by means of some secure communication. After the registration gateway will have the information of all authorized routers id and their public keys.

Establishing a secure backbone network – In this phase, a secure and authenticated communication through the multi hop wireless backbone network is formed where the nodes are pre-initialized with some secret information without having any direct contact with each other. The authentication is provided by means of digital signature using the private key of a router. When sending data to the next hop router, the sending node (router) will encrypt the data first by using sending nodes private key and further encrypt it by using the public key of the receiving node. Once the message is received by the intended receiver, it will first decrypt the message by using its own private key followed by decrypting it with the public key of sending node. The encryption with the public key ensures the confidentiality of the message since the message can only be decrypted by the node for which it is intended for; this is because only the intended receiving node has the knowledge of the corresponding private key. On the other side, authentication of the message is ensured by encrypting the message with the sender's private key, this encryption with the private key of sending nodes provide a digital signature which guarantee the origin of data.

To support the addition of new mesh routers the advantage of digital signature is exploited in the proposed architecture. When the system deploys a new mesh router in the network it will first have to register with the gateway through the help of system administrator. The administrator will store the information (e.g public key, node id) of the newly deployed node to the memory of the gateway through some secure communication. Once the registration process is completed, gateway will flood the information of the newly deployed node to the entire network. When flooding the information the confidentiality of the message will be protected by the use of the receiving nodes public key. The message will be digitally signed by using the master private key to ensure the authenticity of the origin. Each and every other node will

store the newly deployed nodes information and confirm it as an authorized member of the network. The newly deployed node can then communicate with other nodes in the network once it is recognized as an authorized node.

5. Comparative Analysis

Due to the constrained resource in the wireless environment, the basic approach to secure communication in wireless networks is to match the protocol structure with the structure of wireless networks in order to achieve improved performance and efficiency [13]. Traditional wireless network have many key management technique such as topology matching key management (TMKM) [14] scheme, group key management scheme (GKMPAN) [15], Chinese Remainder Theorem and the Diffe-Hellman key agreement (CRTDH) [16]. However, these key management schemes are not well suited for wireless mesh network. For exampleTMKM does not consider the problem of key distribution among BSs, GKMPAN scheme uses pair-wise keys to distribute a common group key for data encryption among group members whereas CRTDH requires a number of messages linear to the group size to refresh the key for every group join and leave. Thus, it is not scalable in a wireless environment with limited bandwidth resource. None of the existing protocols considered the unique features of WMNs, such as static backbone routers and multiple clients sharing the same router, all of which can be leveraged for designing more optimized protocols. Our work tries to fill this gap by designing such a scheme specifically for WMNs. In our scheme, we provide two type of protection in wireless mesh network. First one is client data protection and second is network data protection. In client data protection we provide the security between client's data during communication and network data protection we protect our network data from outside attacker. Other existing schemes do not provide protection in two parts client data and network data as our scheme.

6. CONCLUSION

The unique architecture of the WMN requires a dedicated security solution in addition to a traditional security scheme. In this paper, we present some critical factor involved in the design of a secure key agreement protocol for wireless mesh network. We have described a key agreement scheme using public key cryptography to establish a secure communication link in the mesh backbone network. With the pre-distribution of public keys among the mesh routers, each node is able to establish authenticate and secure communication link with every other nodes in the network. To ensure the protection of client data, we proposed the standard IEEE 802.11i protocol [4] that will allow the mesh client to access the backbone network with complete security. The proposed key agreement architecture is able to work with minimal resource consumption while achieving sufficient security in both client and network data protection.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (Grant number: 20100010488).

REFERENCES

[1] I. F. Akyildiz, X. Wang, W. Wang, "Wireless mesh networks: a survey," Computer Networks, 2005, pp. 445–487.

[2] M. S. Siddiqui, C. S. Hong, "Security Issues in Wireless Mesh Networks," International Conference on Multimedia and Ubiquitous Engineering, 2007, pp. 717 – 722.

[3] W. Stallings, Cryptography and Network Security-Principles and Practices, 3rd ed. Upper Saddle River, NJ: Prentice Hall, 2003.

[4] IEEE Standard 802.11i, Medium Access Control (MAC) Security Enhancements, Amendment 6, IEEE Computer Society, 2004.

[5] IEEE Standard 802.1X, Port-based Network Access Control, IEEE Computer Society, 2004.

[6] A. Mishra, W.A. Arbaugh, "An initial security analysis of the IEEE 802.1X standard," UM Computer Science Department, Technical Report CS-TR-4328, 2002.

[7] R. Fantacci, L. Maccari, T. Pecorella, F. Frosali, "A secure and performant token-based authentication for infrastructure and mesh 802.1X networks," Infocom'06 Poster Session, April 2006.

[8] M. Kassab, A. Belghith, J.-M. Bonnin, S. Sassi, "Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks," Proceedings of the First ACM Workshop on Wireless Multimedia Networking and Performance Modeling, 2005, pp. 46–53.

[9] A.R. Prasad, H. Wang, "Roaming key based fast handover in WLANs," Proceedings of the IEEE Wireless Communications and Networking Conference, vol. 3, March 2005, pp. 1570–1576.

[10] J.P. Hubaux, B. Levente, and C. Srdjan. "The quest for security in mobile ad hoc networks," Proc. of the 2001 ACM International Symposium on Mobile ad hoc networking and computing, USA, pp.146-155, 2001.

[11] C. Srdjan, N. Levente, and J.P. Hubaux. "Self-organized public-key Management for mobile ad hoc networks," IEEE Transactions on mobile computing, vol.2, no.1, pp. 52-64, Jan-Mar. 2003.

[12] L. Zhou, and Z. J. Haas. "Securing ad hoc networks," IEEE Networks Special Issue on Network Security, vol.13, no.6, pp.24-30, Nov/Dec. 1999.

[13] J. Dong, K. E. Ackermann and C. Nita-Rotaru, "Secure Group Communication in Wireless Mesh Networks," In Ad Hoc Networks (Elsevier) Journal, Special Issue: Privacy and Security in Wireless Sensor and Ad Hoc Networks, Nov 2009.

[14] Y. Sun, W. Trappe, and K. J. R. Liu, "A scalable multicast key management scheme for heterogeneous wireless networks," IEEE/ACM Trans. Network, vol. 12, no. 4, pp. 653-666, 2004.

[15] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN: An efficient group rekeying scheme for secure multicast in ad-hoc networks," Mobiquitous, vol. 00, 2004.

[16] R. Balachandran, B. Ramamurthy, X. Zou, and N. Vinodchandran, "CRTDH: an efficient key agreement scheme for secure group communications in wireless ad hoc networks," in Proc. of IEEE ICC '05