Securing VoIP Services in Multi-Hop Wireless Mesh Networks

Yi Xian, Chin-Tser Huang

Department of Computer Science and Engineering

University of South Carolina

Columbia, SC 29208, USA

{ xian, huangct }@cse.sc.edu

***Abstract*— Voice over Internet Protocol (VoIP) service has been a very popular and important application over the Internet. Wireless VoIP also becomes more and more popular due to its features of low cost and convenience. Recently, wireless mesh network has been considered as a good solution for VoIP services since it is easy to deploy and provides a larger area coverage. However, the security and performance are the main challenges. In this work, we focus on the security issues and present a new protocol for securing the voice traffic over the wireless mesh network, including the client authentication, intermediate mesh nodes authentication to ensure secure multi-hop communication, voice traffic confidentiality and secure optimal routing selection by using the probing packets.**

Keywords*— *VoIP, wireless mesh network, authentication

I. INTRODUCTION

Recently, owing to the cost savings and conveniences, Voice over Internet Protocol (VoIP) services have gained widespread popularity and still keep growing steadily. For example, a report published by the French telecoms regulator Arcp says the total number of VoIP-based calls doubled in 2006 and accounted for 25% of total fixed line calls in France over the year. Another report shows that at the end of March 2007, 196 million people had registered to use Skype [14].

On the other hand, wireless networks have the advantages of low cost, mobility support and convenience. A significant benefit of deploying VoIP over wireless networks is to provide users mobility and the possibility of using portable phones. In order to gain wide area coverage, multi-hop wireless mesh networks (WMN) [2] can be used where each mesh node cooperates to route the packets. In a multi-hop wireless mesh network as illustrated in Fig. 1, each mesh node has at least two interfaces, in which one interface works as an access point allowing mobile clients to associate with, and the other one is used for communication with other mesh nodes. The ease of deployment and wide coverage make wireless mesh networks a practical solution for providing VoIP services, especially when wired infrastructure is too expensive and not available.

However, ease of access to the medium makes VoIP over wireless mesh networks vulnerable to unauthenticated access and malicious misuse. Such vulnerability makes providing security guarantees a big challenge, which has not gained enough attention so far. Possible attacks on VoIP over wireless mesh networks include traffic eavesdropping, Denial of Service attacks, mesh node impersonation, and unauthorized mesh node access. In order to address these security problems, some security mechanisms such as mobile client authentication and mesh node authentication are needed to ensure that only legitimate users and mesh nodes can access the wireless mesh network and transmit packets. Traffic encryption is needed if data confidentiality is a requirement. A lightweight and efficient encryption algorithm can improve the network performance. Unfortunately, existing standards are not sufficient for these security requirements. For example, current protocols lack mesh node access control and mutual authentication of intermediate mesh nodes.

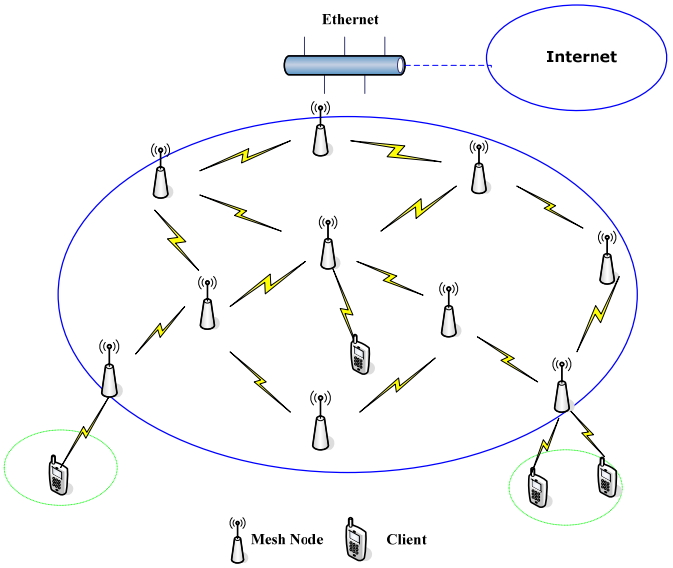

Fig. 1 Architecture of Wireless Mesh Networks

In this paper, we focus on security issues for supporting VoIP over multi-hop wireless mesh networks. Specifically, this paper presents a solution that provides both client authentication and mutual intermediate mesh nodes authentication using the individual key of each node. Moreover it introduces a secure route selection scheme using secured probing packets.

The remainder of this paper is organized as follows. We first give an overview of related works in Section 2. Then, we describe the possible attacks on VoIP services in wireless mesh networks in Section 3, and present our new protocol for securing VoIP over wireless mesh network in Section 4. We conclude the paper and discuss future work in Section 5.

II. Related Works

IEEE 802.1X port-based authentication [13] uses the Extensible Authentication Protocol (EAP) [1] which introduces the uncontrolled/controlled port model to authorize and control data flow between an access point (AP) and clients. This standard provides authentication, authorization, key management and data confidentiality. However, this standard is designed for authentication occurring between the AP and the mobile client, thus is not suitable for authentication between mesh nodes.

Some studies [6] [11] on VoIP over 802.11 WLAN have been conducted to understand the capacity of VoIP over WLAN. Several methods for improving the performance of deploying VoIP over wireless mesh networks have been proposed in [5], [9], [12]. These methods include combining packet aggregation and header compression, route discovery using destination-sequenced distance vector (DSDV) with label-based routing and probing-based adaptive path selection. However, most of these works only focus on the improvement of performance of VoIP and fall to consider security issues. Our work presents a secure probing scheme to protect against forge response and replay message.

A solution for securing VoIP is presented in [3]. It shows that Tiny Encryption Algorithm (TEA) is superior when offering voice traffic confidentiality. Their results also indicate that stream ciphers with resynchronization capability are preferable to block ciphers for securing VoIP. However, there are many other security problems to be considered when we deploy VoIP in multi-hop wireless mesh networks, such as mobile user control access and mesh node authentication. Traffic confidentiality alone is not enough to ensure the security of VoIP services.

For multi-hop wireless mesh network, the lack of security guarantees is one of the main challenges of its deployment. Recently, several security challenges have been analysed in [10], such as corrupt access point detection, secure multi-hop routing and fairness problem. In [8], Maccari et al. propose a fast and secure mobile client re-authentication scheme in wireless mesh networks. In their scheme, a full costly authentication is performed only at the first network entry. Then re-use of key information, i.e. the token generated in the first authentication, can speed up the following re-authentication when the client roams to another AP. A hybrid authentication protocol for wireless mesh networks is proposed in [4], including mesh node access control by key eraser procedure, topology authentication and communication authentication. These current mechanisms may not be appropriate for securing VoIP application over multi-hop wireless mesh network because they do not consider quality of service requirement.

III. Security Challenges and Possible Attacks

VoIP and wireless mesh network have their own security problems respectively. For VoIP, main security problems include identity theft, traffic eavesdropping, spamming over Internet Telephony (SPIT), call tampering and man-in-the-middle attacks. In [7], the authors discuss various VoIP security threats and the fundamental security requirements of VoIP applications, including confidentiality, integrity and availability. Moreover, for time-sensitive applications such as VoIP, how to balance the Quality of Service requirements and the security requirements is a big challenge. For wireless mesh networks, the open medium nature, the lack of physical protection of AP and the multi-hop characteristic make them vulnerable to several attacks. In addition, some wireless mesh networks suffer from severe capacity and delay constraints. Deploying VoIP over wireless mesh networks will only add to the complication of the aforementioned problems, which have not been sufficiently addressed so far. In this section, we describe some possible attacks on VoIP over wireless mesh networks.

A. Denial of Service Attacks

For wireless network, Denial of Service attack is a common threat. It is easy for an adversary to jam the channel of a wireless network. Another type of DoS attacks is that the compromised nodes refuse to relay the traffic or forward the traffic to a specific location in order to disrupt the service or collect sensitive information.

B. Mesh Node Impersonation

A malicious node may pretend to be a legitimate one in the wireless mesh networks in an effort to change the routing information, redirect the traffic to a compromised node to gain more information or reject specific traffic. This necessitates the authentication of every mesh node.

C. Unauthorized Node Access

If a mesh node can be accessed without authorization, then an adversary can control the mesh node to launch attacks such as Denial of Service attacks, sensitive information retrieval, and to change the routing mechanism to benefit themselves. In order to enforce access control, both mobile clients and mesh nodes should be authenticated.

D. Flooding Attacks

In some schemes, probing packets are sent in order to estimate the network condition and ensure the proper operation of the mesh network. An attacker may flood the mesh network by keeping sending a high volume of bogus probing packets to occupy the channel or exhaust the resource of mesh nodes. Therefore, determining the authenticity of probing packets is important.

E. Other Possible Attacks

As in other types of wireless networks, wireless mesh networks are vulnerable to passive eavesdropping, message replaying and man-in-the-middle attacks. All these attacks are easy to launch unless sufficient authentication mechanisms and cryptographic schemes are performed before the attacker can gain illegitimate access. The authentication and encryption should be as efficient as possible but robust enough.

IV. Our Protocol

We have described the security problems of and possible attacks on VoIP over wireless mesh network, and have shown that current standards are not sufficient for addressing these security problems. In this section, we present a new secure protocol that satisfies the following security requirements: 1) only a legitimate user can access the mesh nodes and send/receive messages through the wireless mesh network after successful authentication; 2) the mesh nodes know their neighbours such that a malicious node can be detected as soon as possible; 3) when the probing packets are used to estimate the delay of each path, bogus probing packets and fake responses from malicious nodes are detected and discarded early so that only the correct information is used to select the route.

A. Mesh Node Access Control

Before mobile user can access the wireless mesh network and send traffic to the Internet through the multi-hop mesh network, the identity of the user needs to be verified in order to prevent illegitimate access. For the mobile user authentication, the secure mutual authentication in IEEE 802.1x with EAP-TLS can be used when the mobile user access the network at the first time. After this phase, a shared secret, called Pairwise Master Key (PMK), is generated between the mobile user and the authentication server. The authentication procedure involves a multi-hop path and public key cryptography which incurs a high computational overhead. Since mobile stations often have energy constraint, an efficient re-authentication scheme is necessary. On the other hand, the client re-authentication should be robust enough to prevent attackers from gaining unauthorized access. The authors in [8] propose a token-based re-authentication method. In our work, we perform the client authentication based on this scheme.

Each mobile user has a *permit* after it registers to the authentication server. According to the guidelines in [8], this *permit* can't be replicated or generated by other mobile users. Only the requesting mobile user can generate such a valid credential to prove its identity. This *permit* can be created by the mobile user from the pre-defined secret shared between mobile user and authentication server or derived from its PMK after the first full EAP-TLS authentication if the EAP-TLS method is used. When the mobile user roams from AP_1 to AP_2, the mobile user sends the request message with the *permit* to AP_2. Then the AP_2 checks this *permit* with the authentication server. The content of the request message is shown in Fig. 2.

PMK Request Message (mobile user M → AP):

***permit**: {Cert(M) || T || HMAC (Cert(M), T, PMK(M))}*

Fig. 2 PMK Request Message

Only when the client's *permit* is verified the authentication server sends the secret key of mobile user to the AP. Bogus key request messages from attackers can be detected since only the requesting mobile user can generate a valid *permit*. This *permit* can be re-used each time when the mobile user roams to the range of another AP in the same mesh network. With a timestamp *T* the replay attack can be prevented. The permit should be fast generated and easy to verify. We will evaluate its performance in our future work.

B. Mesh Node Authentication

In wireless mesh networks, the bogus and compromised mesh nodes may launch tampering and Denial of Service attacks. In order to protect the wireless mesh network against these attacks, sufficient authentication of mesh nodes is needed. There are two aspects to consider. First, each mesh node in the wireless mesh network needs to be authenticated by the authentication server, otherwise an adversary can impersonate a legitimate node in order to capture the traffic, retrieve sensitive information or change the routing information. Second, since all the intermediate nodes on the communication path relay end users' the traffic hop by hop, authentication of each intermediate node is needed to ensure that the traffic is coming from a legitimate neighbour. In this way, the intermediate node can check the authenticity and integrity of the traffic such that malicious packets can be discarded as soon as possible.

We incorporate these two types of mesh node authentications into our protocol. The first part is mesh node authentication during the initialization phase, and the second part is mutual authentication between neighbour nodes during the transit of the packets of the mobile users.

1) Initial Mesh Node Authentication

During the initialization phase, mesh node authentication takes place between each mesh node and the authentication server. It is a practical method to use public key cryptography in the initial node authentication since it happens rarely (only during the first deployment and the re-configuration of wireless mesh networks). It is also reasonable to assume that the available energy of both mesh nodes and the authentication server are not impacted by the usage of public key cryptography. Suppose each node A and the authentication server (AS) has a public/private key pair, denoted as {*PubKey(A), PrivKey(A)*} and {*PubKey(AS), PrivKey(AS)*}, assigned by the service provider. After successful authentication, the authentication server will distribute the group key, denoted as *GroupKey*, and the passport, *Pass(A)* to the authenticated node A, encrypted by the node's public key such that only that specific node can decrypt it. The group key can be used to provide end-to-end encryption of the traffic transmitted over the mesh network (if traffic confidentiality is required) and to protect the broadcast of a mesh node's individual key to the neighbour nodes against sniffing and tampering. The passport of node A, *Pass(A)*, can be a signature created using authentication server's private key, that is $E_{PrivKey(AS)}$ *(Cert (A))*, such that other legitimate nodes in the WMN can verify its identity. By using a timestamp *T* the replay attacks can be prevented. By checking the HMAC the authenticity and integrity of this

message can be ensured. The Group Key Distribution Message is shown in Fig. 3.

Group Key Distribution Message (AS → node A):

$$E_{PubKey(A)}(GroupKey, Pass(A)) \,||\, T \,||\, HMAC(E_{PubKey(A)}(GroupKey, Pass(A)), T, PrivKey(A))$$

Fig. 3 Group Key Distribution Message

2) Mutual Authentication Between Mesh Nodes

In a wireless mesh network, an attacker may insert malicious nodes into the network or perform node impersonation. In order to detect the malicious nodes as soon as possible, it is important to perform mutual authentication between mesh nodes. In this way every mesh node in the WMN knows its neighbours and the malicious nodes can be detected at early stage. In multi-hop mesh networks, using public key cryptography to authenticate each hop will incur a high overhead since it usually involves a multi-hop path. Instead, using the symmetric key shared between neighbouring APs is a practical solution. This key can be used to compute a HMAC on the relayed packets to authenticate the mesh node hop by hop.

In our protocol, we perform the mutual node authentication as follows. Each legitimate mesh node has an individual key, denoted as *Key*, which is only known to the authenticated nodes within the neighbourhood. Assume each node maintains a list of its neighbours. First, every mesh node broadcasts to its neighbours an authentication request message which contains its certificate and its passport generated with the authentication server's private key. This broadcast message is shown in Fig. 4.

Broadcast Message (node A → all neighboring nodes):

$$E_{GroupKey}\{Cert(A), Pass(A)\}$$

Fig. 4 Authentication Request Message

Using the group key and public key of the authentication server, its neighbours can verify the node's identity. In this way, each node gets the certificate of each of its neighbours. Then each node can send its individual key to all its neighbours as shown in Fig. 5.

Individual Key Exchange Message (node A → node B):

$$E_{PubKey(B)}\{Key(A) \,||\, T_A \,||\, E_{PrivKey(A)}(Key(A), T_A)\}$$

Fig. 5 Individual Key Exchange between neighbouring nodes A and B

Upon receiving this message, only node B can decrypt it to get node A's individual key *Key(A).* Using node A's public key, node B can check the signature to verify the authenticity and integrity can be achieved. After these steps are performed, all the nodes know the individual key of their neighbors. This scheme can also defeat a possible man-in-the-middle attack. For example, a malicious node E might launch a man-in-the-middle attack by forwarding the authentication request message between node A and node B. Then both nodes A and B send their individual keys to the malicious node E. However, without the private keys of node A and B, node E can not decrypt the key exchange messages and therefore can not know the individual key of node A and node B.

Each time a new AP joins the mesh network, it needs to exchange its individual key with all its neighbouring nodes. This scheme can also be used to renew the individual key.

3) Hop-by-Hop Authentication

After a call is placed by an end user, the voice traffic generated or received by the mobile user is relayed by the intermediate mesh nodes hop by hop. To ensure authenticity and integrity of the voice traffic, the individual key of each node can be used to compute a hash on the forwarded packets. When receiving the packets, each node first verifies the hash using the sender's individual key. Then a new hash using its own individual key is computed before sending the packet to the next hop such that all the nodes on the path can be authenticated hop by hop. The group key can be used to encrypt the packets if data confidentiality is a requirement. The main advantage of using group key is that during the whole transit from the first hop to the last one, only one encryption is enough. The incorporation of hop-by-hop authentication information is shown in Fig. 6.

Hop by Hop Authentication:

$$E_{GroupKey}(MSG) \,||\, T \,||\, HMAC(E_{GroupKey}(MSG), T, Key)$$

Fig. 6 Hop-by-Hop Authentication

It is not uncommon for wireless networks to have severe capacity constraints. Since traffic encryption often incurs considerable overhead on the performance of wireless mesh networks, a lightweight secure encryption algorithm is highly desirable. The authors in [3] show that the Tiny Encryption Algorithm (TEA) is a fast and secure algorithm for securing VoIP. It can be considered as a practical solution to encrypt voice traffic in wireless mesh networks.

C. Secure Routing Selection

One of the major challenges of supporting real time applications, such as VoIP, over wireless mesh networks is to adopt good routing schemes in order to maintain the voice traffic quality. The authors of [10] run DSDV with different metrics (including ETX, end-to-end loss, quantized end-to-end loss) to choose the top five popular routes and then use probing packets to evaluate the delay of each path in order to select the optimal path adaptively. However, their routing selection schemes mainly focus on the performance without enough security considerations. For example, because the probing packet needs other mesh nodes to process, an attacker

may launch a flooding attack by flooding a mesh node with a lot of fake probing packets so as to occupy the resource of mesh nodes. In addition, a compromised node can send a bogus response in advance in order to enhance the chance that it is included in the selected route or send a delayed bogus response to disconnect a legitimate node. Replay attack is also possible. In order to prevent and detect the malicious node manipulating the routing information, a secure probing packet is needed. In order to detect faked and replayed response, the probing packet includes a hash computed using a nonce and the individual key. The secured probing packet is shown in Fig. 7.

Probing Packets:

MSG || Nonce || HMAC (MSG, Nonce, Key)

Fig. 7 Probing Packets

In this way both fake response sent in advance and replayed response can be detected early. With the individual key, any bogus probing packets sent by an illegitimate node can be detected at the first hop. The probing packet has the same size of voice packet in order to better estimate the delay of each path. Besides, one advantage of using a hash is that the estimation of round-trip time will be more accurate since the voice packet also contains a hash computed using individual key.

V. Conclusions and Future Works

The lack of security guarantees is one of the main challenges faced by VoIP over wireless mesh networks, but it has not gained enough attention. In this paper, we analyze four main possible attacks on VoIP services in wireless mesh networks, and present a new secure protocol to address these attacks. First, client authentication provides mesh node access control. Second, in order to ensure secure multi-hop routing within the mesh network, a mutual node authentication method using the individual key shared by the neighbor nodes is presented. In this way when a call is placed by the end user, the voice traffic can be authenticated hop by hop and the bogus packets can be detected at early stage. Group key that is established during the initialization phase can be used to encrypt the voice traffic if the traffic confidentiality is a requirement. Third, to select the optimal route, the secure probing packet including a HMAC is sent out to estimate the end-to-end delay of each path. The HMAC in the probing packet helps detect the fake or replayed responses.

In the future work, we will study what key materials should be included in the *permit* such that other malicious users cannot duplicate or crack, and the specific HMAC function that could be used. We will also evaluate the security overhead of deploying our protocol, including client authentication, mutual nodes authentication, and traffic encryption. We will evaluate the performance of applying TEA in our protocol in the future work. Moreover, the computation of HMAC at each node on the path may introduce a delay. In most cases, the number of intermediate nodes is not large. Whether the accumulated delay is within a tolerable range is important for practical application. We will study the impact of the delay introduced by intermediate nodes on the performance of VoIP service.

References

[1] B. Aboba, L. Blunk, j. Vollbrecht, J. Carlson and H. Levkowetz. “Extensible Authentication Protocol,” RFC 3748, June 2004.

[2] I. F. Akyildiz, X. Wang, and W. Wang, “Wireless Mesh Networks: a Survey,” *Computer Networks and ISDN Systems*, Vol. 47, No. 4, pp. 445–487, 2005.

[3] A. D. Elbayoumy and S. Shepherd, “A Comprehensive Secure VoIP Solution,” *International Journal of Network Security*, Vol. 5, No. 2, pp. 233–240, Sept. 2007.

[4] R. Frank, “Authentication in Wireless Mesh Networks,” M. Eng. thesis, Universite Joseph Fourier, Grenoble, France, Sep. 2006.

[5] S. Ganguly, V. Navda, K. Kim, A. Kashyap, D. Niculescu, R. Izmailov, S. Hong, and S. R. Das, “Performance Optimizations for Deploying VoIP Services in Mesh Networks,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 11, pp. 2147–2158, Nov. 2006.

[6] D. Hole and F. Tobagi, “Capacity of an IEEE 802.11b Wireless LAN supporting VoIP,” in *Proceedings of IEEE ICC*, 2004.

[7] P. C.K. Hung, M. V. Martin, “Security Issues in VOIP Applications,” in *Proc. of IEEE CCECE/CCGEI*, Ottawa, 2006.

[8] L. Maccari, R. Fantacci and T. Pecorella, “A Secure and Performant token-based Authentication for Infrastructure and Mesh 802.1x Networks,” in *Proceedings of IEEE INFOCOM*, 2006.

[9] D. Niculescu, S. Ganguly, K. Kim, and R. Izmailov, “Performance of VoIP in a 802.11 Wireless Mesh Network,” in *Proc. of IEEE INFOCOM 2006*, Barcelona, 2006.

[10] N. B. Salem, J. P. Hubaux, “Securing Wireless Mesh Networks,” in *IEEE Wireless Communications*, Vol. 13, No. 2, pp. 50-55, April 2006.

[11] M. Veeraraghavan, N. Cocker, and T. Moors, “Support of Voice Services in IEEE 802.11 Wireless LANs,” in *Proceedings of IEEE INFOCOM*, 2001.

[12] H.Y. Wei, K. Kim, A. Kashyap, and S. Ganguly, “On Admission of VoIP Calls over Wireless Mesh Network,” in *Proceedings of IEEE ICC*, 2006.

[13] IEEE 802.1X – Port Based Network Access Control. [Online]. Available: http://www.ieee802.org/1/pages/802.1x.html

[14] Skype. [Online]. Available: http://www.skype.com