SECURITY OF IEEE 802.16 IN MESH MODE

Yun Zhou and Yuguang Fang
Department of Electrical and Computer Engineering
University of Florida, Gainesville, FL 32611
Tel: (352)392-8576; Fax: (352)392-0044
Email: {yzufl@, fang@ece.}ufl.edu

ABSTRACT

IEEE 802.16 (WiMAX) has been seen as a promising technique for future mesh networks to provide broadband wireless access. Meanwhile, its security is becoming a critical issue with the proliferation of wireless threats in current IEEE 802.11 systems. Though incorporating some security methods in conventional one-hop networks, IEEE 802.16 is still vulnerable to malicious attacks in multihop environments such as mesh networks. In this paper, we analyze the security of IEEE 802.16 standard in its Mesh mode, point out some security holes, and propose some solutions to deal with attacks to IEEE 802.16 mesh networks.

INTRODUCTION

IEEE 802.16 standard [1], which is the base of *WiMAX* (World-wide Interoperability for Microwave Access) [2], is seen as a promising technology for next generation broadband wireless access. Compared with IEEE 802.11 standard [3], it operates at larger frequency band up to 66GHZ, covers longer distance up to 50km, and supports QoS services. Therefore, 802.16 becomes an ideal choice for broadband wireless access systems such as *WLAN*s (Wireless Local Area Networks) or *WMAN*s (Wireless Metropolitan Area Networks).

IEEE 802.16 defines two modes. In the *PMP* (Point-to-multipoint) mode, *SSs* (Subscriber Stations, such as laptops) can reach the *BS* (Base Station) in one hop. Otherwise, SSs shall operate in the *Mesh* mode such that those SSs form a multihop network, which is called *mesh network* [4], to the BS.

Compared with the PMP topology, the mesh topology extends BS coverage, and its flexibility on installation and configuration make it a promising architecture for future WLANs and WMANs. In Fig. 1, for example, multiple laptops can form a WLAN of a mesh topology, multiple wireless routers can form a WMAN of a mesh topology, and the mesh WMAN bridges the gap between WLANs and the Internet.

Among all the topics in wireless networks, security is drawing intense attention recently. When IEEE 802.11 is getting more and more popular in the deployment of WLANs, many vulnerabilities have been found in the literature [5]–[9]. This becomes a major obstacle to many security-critical wireless applications such as online shopping or secure communications.

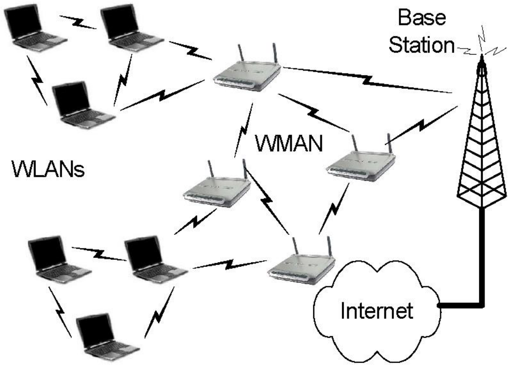

Figure 1. Mesh networks.

The lessons from IEEE 802.11 make people more cautious and lead to the incorporation of security design into IEEE 802.16. Based on *DOCSIS* (Data Over Cable Service Interface Specifications) [10], which was designed to solve the last mile problem for cable systems, IEEE 802.16 defines a *PKM* (Privacy and Key Management) protocol. It provides subscribers with privacy, authentication, or confidentiality across the fixed broadband wireless network. It does this by applying cryptographic transforms to MPDUs carried across connections between SS and BS.

However, IEEE 802.16 security still needs to be examined before its deployment. Since mesh networks are gaining more and more interests and IEEE 802.16 is seen as one of promising techniques to build up mesh networks, we believe that it is necessary to analyze the security of IEEE 802.16 in mesh networks. However, there are only a few work overviewing the potential vulnerabilities of IEEE 802.16 in PMP mode [11]–[13].

In this paper, we analyze the security of IEEE 802.16 in mesh mode, point out several potential threats and propose some possible solutions. We find out that though IEEE 802.16 provides some security measures in conventional one-hop networks, it is very vulnerable to malicious attacks in multihop environments. We also propose some security improvements.

SECURITY ARCHITECTURE OF IEEE 802.16 IN MESH MODE

IEEE 802.16 MAC (Medium Access Control) defines a PKM protocol as a sublayer, providing authentication, key management and data traffic privacy services.

IEEE 802.16 MAC is connection-oriented. Each SS establishes a connection to associate with a service flow. In PKM, an *SA* (Security Association) is shared between SS and BS for each connection to main its security state such as the cryptographic

This work was supported in part by the US Office of Naval Research under grant N000140210464 (Young Investigator Award).

suite, *TEKs* (Traffic Encryption Keys) and *IVs* (Initialization Vectors) and managed by a *TSM* (TEK State Machine). An *ASM* (Authorization State Machine) is maintained by each SS for authorization when entering the network and the initialization of TSMs.

A new SS can join a mesh network by the following process:

1) The SS searches for *MSH-NCFG:Network Descriptor* messages to synchronize with the network and build up a list of available BSs and a list of neighboring SSs.
2) The new SS selects from its neighbors a potential *Sponsor* node. Meanwhile the new SS becomes a *Candidate* node.
3) The Candidate node (the new SS) shall be authorized by an Authorization node (a BS or a backend server) through the PKM protocol. The Sponsor node will tunnel the PKM-REQ messages from the Candidate node to the Authorization node through UDP protocol. Upon receiving tunneled PKM-RSP messages from the Authorization node the Sponsor node forwards them to the Candidate node.
4) The Candidate node shall register itself at a Registration node (a BS or a backend server) to get a Node ID. The Sponsor node again tunnels the REG-REQ message from the Candidate node to the Registration node. Upon receiving the tunneled REG-RSP from the Registration node the Sponsor node forwards it back to the Candidate node.
5) After authorization the Candidate node becomes a regular node in the mesh network. Then it will build connectivity at higher layers.
6) After entering the network, the new SS can establish links with nodes other than its Sponsor Node by following a Challenge-Response process based on MSH-NCFG:Neighbor Link Establishment messages.

Upon entering the network, the new SS starts for each neighbor a separate TSM for each SA authorized by BS. Then the TSM takes charge of the SA maintenance, and the ASM maintains the reauthorization of the SS.

Security Threats to IEEE 802.16 In Mesh Mode

In this section, we present the following potential threats to IEEE 802.16 standard in mesh mode.

A. Topological attacks

In the mesh network, every SS broadcasts MSH-NCFG:Network Descriptor messages regularly. Each MSH-NCFG:Network Descriptor carries some physical layer information for the new SS to acquire coarse synchronization. In addition, each MSH-NCFG:Network Descriptor provides a list of available BSs and a list of neighboring SSs of the sender. Those lists include information such as Node ID of BS or neighbors and the corresponding hop-count. To join the network on initialization or after signal loss, a new SS shall search for MSH-NCFG:Network Descriptor messages and build a physical neighbor list. Based on the BS information, the new SS chooses a Sponsor node, which helps the new SS join the network.

The problem here is that MSH-NCFG messages are not encrypted and authenticated. This can lead to the attacks against network topology, which has been studied in ad hoc and sensor networks [14].

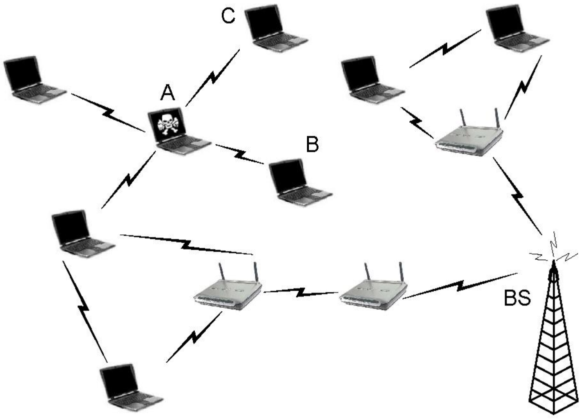

Figure 2. Sinkhole attacks. Node A can spoof routing information to lure nodes B's and C's traffic.

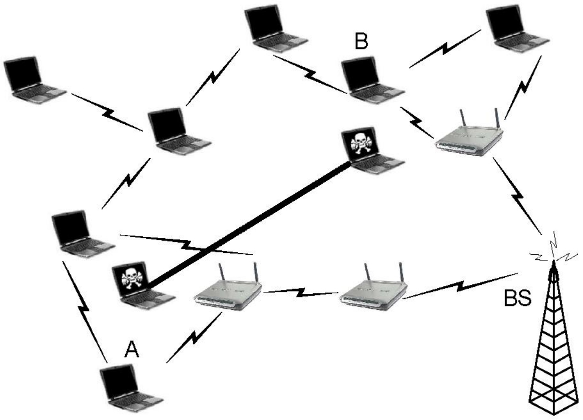

Figure 3. Wormhole attacks. Attackers can tunnel messages through a secret channel so that node A and node B believe they are neighbors.

By claiming a shorter path to BS, for example, a malicious node has much more chance to become a Sponsor node. In this way, the Sponsor node can lure the network entry traffic in the local area like a *Sinkhole* [15]. Then the Sponsor node can monitor, modify or spoof the authorization information exchanged between new nodes and BS. An example is illustrated in Fig. 2, where node A can create a sinkhole and becomes the Sponsor for nodes B and C. In addition, false topological information contained in MSH-NCFG messages can cheat the new SS into forming an incorrect view of network topology, which can introduce problems to routing protocols.

Attackers can even replay MSH-NCFG messages instead of modifying or spoofing. One example is the *Wormhole* attack [16]. As is illustrated in Fig. 3. Attackers establish a secret channel, tunnel MSH-NCFG messages from nodes A and B through the channel and replay them. In this way, nodes A and B believe they are neighbors of each other. Attackers can also record MSH-NCFG messages at one place, move and reply them at another place. Obviously, the distorted network topology can become a serious attack to routing protocols.

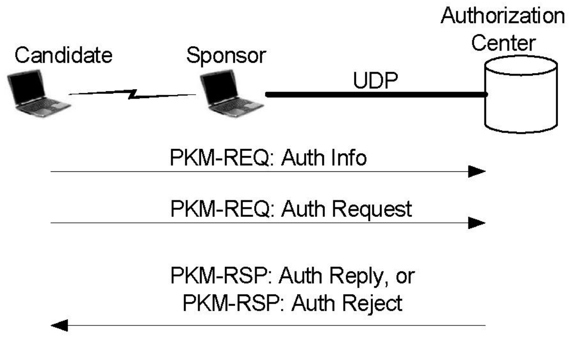

Figure 4. Node authorization. The Sponsor node tunnels the PKM-REQ messages from the Candidate node to the Authorization center through UDP protocol. Upon receiving tunneled PKM-RSP messages from the Authorization center the Sponsor Node forwards them to the Candidate node.

B. Authorization threats

A Candidate node needs authorization to access the mesh network. This can be achieved through a handshake between the Candidate node and an Authorization center. The handshake is carried out by PKM-REQ and PKM-RSP messages (Fig. 4).

The Candidate node first sends a PKM-REQ:Auth Info message to the Authorization center. The message only carries the X.509 certificate for the manufacturer of the Candidate node.

Then the Candidate sends a PKM-REQ:Auth Request message to the Authorization center. The message contains the Candidate's X.509 certificate issued by its manufacturer, the Candidate's cryptographic capabilities, the Candidate's Basic CID.

The Authorization center verifies the Candidate's X.509 certificate with its manufacturer's public key extracted from the PKM-REQ:Auth Info message. If the verification fails, the Authorization center simply replies to the Candidate a PKM-RSP:Auth Reject message containing an error-code and a display-string.

If the Candidate is authentic, the Authorization center replies a PKM-RSP:Auth Reply message. This message contains an *AK* (Authorization Key) encrypted with the Candidate's public key, the AK lifetime, the AK sequence number, SA-descriptors, PKM configuration, an *OSS* (Operator Shared Secret), the OSS lifetime, the OSS sequence number.

In the PMP mode, the AK is used for the Candidate to access the network. In the Mesh mode, however, the Candidate shall use the OSS to access the network. Here the OSS is shared by all the nodes in the mesh network.

Because the Candidate usually cannot communicate with the Authorization center directly in the Mesh mode, the Sponsor node help to tunnel the PKM-REQ messages from the Candidate to the Authorization center through UDP protocol and forward the PKM-RSP messages tunneled back from the Authorization center to the Candidate.

The above process is supposed to guarantee the authenticity of the Candidate before it joins the network. However, all the messages are not encrypted and authenticated. Though the AK in PKM-RSP:Auth Reply messages is encrypted, it is useless in the Mesh mode. Hence, there are several security holes failing the goal of the authorization process.

First, all the messages can be intercepted and modified by attackers between the Candidate and the Sponsor. Though we can assume the UDP tunnel can prevent eavesdropping and tampering from attackers between the Sponsor and the Authorization center because all the links between the Sponsor and the Authorization are secured by MAC layer TEKs, we cannot guarantee the loyalty of the Sponsor. Therefore, a malicious Sponsor as an internal attacker can also intercept all the messages and modify them.

In the PKM-REQ:Auth Request message, the Candidate includes its cryptographic capabilities. The Authorization center chooses from them a set of cryptographic algorithms that the Candidate node uses to communicate with the network. The stronger the algorithms are, the securer the traffic is. However, attackers can modify the PKM-REQ:Auth Request message to prevent a weaker cryptographic setting to the Authorization center so that a set of weak cryptographic algorithms is used to secure the communication between the Candidate and the network. This is called the *Security Level Rollback* attack, which has been discussed in IEEE 802.11 [9].

In the PKM-RSP:Auth Reply message, the information of all SAs that the Candidate can access is contained. An authorized SS should get the services to which it has subscribed. But attackers can modify the SA information and remove any SA so that the SS gets less or even no service, leading to the *DoS* (Denial of Service) attack.

In addition, an OSS is included in the PKM-RSP:Auth Reply. The OSS is used as a global key shared by all the nodes in the network. The Candidate shall use the OSS to establish links with neighbors and access the network. Unfortunately, the OSS can be intercepted by attackers such that they can use it to join the network. Attackers can even modify it so that the new node gets wrong OSS and thus fails to join the network. Moreover, attackers can reduce the OSS lifetime so that the Candidate has to update its OSS more frequently, leading to faster energy consumption.

Because the PKM-RSP:Auth Reject message is not authenticated, attackers can spoof the message such that the Candidate fails in the authorization process, leading to the DoS attack.

The entire authorization process is carried out in one connection, but there is no clear definition of Authorization SA that is associated with the connection [11]. Therefore the Authorization center is incapable of distinguishing the authorization messages from different authorization processes. All the messages in an authorization process can be replayed.

In Fig. 5, for example, an attacker can intercept a PKM-REQ:Auth Request message and later replay it to the BS B. The BS can not distinguish it from new PKM-REQ:Auth Request messages and then reply with a PKM-RSP:Auth Reply message. In this way, the attacker can learn the OSS. In another case, the attacker can replay the intercepted PKM-REQ:Auth Request to another mesh domain registered at BS A. As well BS A will accept the message and reply with a PKM-RSP:Auth Reply message, which discloses the OSS used by BS A.

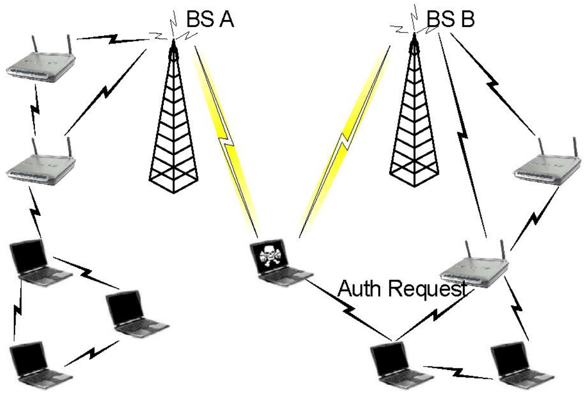

Figure 5. Replay attacks. An attacker can intercept a PKM-REQ:Auth Request message from a normal node and replay it to BS A or BS B to get a PKM-RSP:Auth Reply message, which includes critical information such as the OSS.

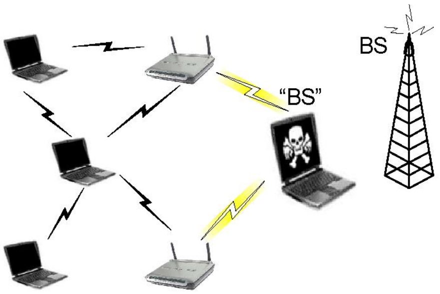

Figure 6. False base station. An attacker impersonates the base station in the authorization process and then control the network.

The authorization process is asymmetric in that the Authorization center authenticates the Candidate but not vice versa. This renders attackers an opportunity to impersonate the Authorization center 6. An attacker can achieve this goal by intercepting PKM-RSP messages from the Authorization center and replaying them or totally forging those messages. The Candidate node cannot verify the authenticity of those messages. This will leave the entire network under the control of the attacker and become a major threat to the authorization process. This is also the case in the PMP mode [11].

C. Threats to link establishment

After entering the network, the new SS can establish links with its neighbors other than its Sponsor Node. The link establishment follows a Challenge-Response process based on the OSS of the network (Fig. 7). All the messages exchanged between two neighboring nodes are encapsulated in the MSH-NCFG:Neighbor Link Establishment messages.

When node A needs to establish a link with node B, A sends a challenge,

HMAC{OSS, frame number, ID of node A, ID of node B},

where the OSS is the global key obtained in the authorization process and the frame number is the last known frame number in which node B sent an MSH-NCFG message.

Upon receiving the challenge, node B computes the same value because it knows the OSS and the fame number. If the two values do not match, node B returns a rejection. If a match is achieved, node B accepts the link and replies a challenge response containing

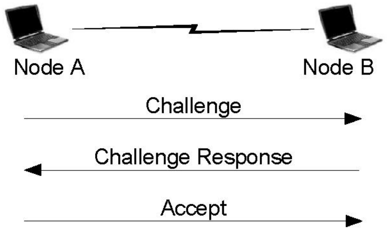

Figure 7. Link establishment. Two nodes A and B establish a link by following a Challenge-Response process based on the OSS of the network.

HMAC{OSS, frame number, ID of node B, ID of node A},

where the frame number is the one of the MSH-NCFG message that node A just sent. Node B also randomly selects and includes an unused Link ID indicating the link from B to A.

Upon receiving the challenge response, node A verifies it like node B does. If a match is achieved, node A replies an Accept. It also randomly selects and includes an unused Link ID indicating the link from A to B. Otherwise, a rejection is returned.

The security of the 3-way handshake depends on the secrecy of OSS, which makes the authentication between neighbors too weak. As is mentioned in Section III-B, the OSS is shared by all nodes and there are many opportunities for attackers to get it. For example, a malicious node can disclose it to an external attacker, or the attacker directly eavesdrops it when a new node gets a PKM-RSP:Auth Reply message from its Sponsor node. Using the OSS, the attacker can join the network without being authorized and establish links with its neighbor. Then the attacker can get services from its neighbors.

D. Threats to TEKs

Each SA includes two TEKs at the same time. The TSM (TEK state machine) associated with the SA is in charge of the TEK update for the SA (Fig. 8).

An SS can start to update its TEKs by sending a PKM-REQ:Key Request message containing SS-Certificate, SAID, HMAC-Digest.

Its neighbor verifies the SS-Certificate. If the verification successes, the neighbor replies with a PKM-RSP:Key Reply containing SAID, old TEK parameters, new TEK parameters, HMAC-Digest. Otherwise, the neighbor replies with a PKM-RSP:Key Reject.

To protect the confidentiality of TEKs, The SS's public key extracted from the PKM-REQ:Key Request message is used to encrypt TEK parameters. To protect the integrity of TEKs, the HMAC-Digests are attached to these messages. However, those HMAC-Digests are calculated with the OSS. This leads to possible message tampering when the OSS is disclosed to attackers. In such a case, attackers cannot find TEKs, but they can spoof a PKM-RSP:Key Reply including false TEKs encrypted with SS's public key and authenticate the message with the OSS.

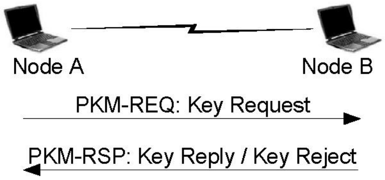

Figure 8. TEK update. Node A requests to update its TEKs by sending a PKM-REQ:Key Request message. Node B replies with a PKM-RSP:Key Reply message containing TEKs information.

E. Traffic threats

In IEEE 802.16, only data traffic is encrypted. Particularly, only the MAC PDU payload is encrypted. The generic MAC header and all MAC management messages are not encrypted. Therefore, attackers can eavesdrop or forge those clear information to raise problems.

To protect data traffic, two cryptographic methods are defined: DES in CBC mode [17] and AES in CCM mode [18]. DES-CBC provides confidentiality by encrypting the MAC PDU payload with corresponding TEKs. AES-CCM provides confidentiality and authenticity for the MAC PDU payload. Particularly, AES-CCM algorithm appends an 8-byt ICV (Integrity Check Value) to the end of the payload and then encrypting both the payload and the ICV. Therefore, DES-CBC is weaker than AES-CCM because the messages encrypted by DES-CBC can be tampered or spoofed. DES-CBC is required by all the implementations of IEEE 802.16 devices but AES-CCM is optional. Attackers can launch the Security Level Rollback attack as is mentioned in Section III-B to cheat the SS and BS into using DES-CBC, which can give attackers more opportunities to attack the data traffic.

802.16e Security In Mesh Mode

An amendment to IEEE 802.16-2004 [1] is passed in 2005 as IEEE 802.16e [19]. This amendment increases the support to mobile devices and the security. The original PKM protocol in IEEE 802.16 becomes the PKMv1 protocol in IEEE 802.16e, and a new protocol PKMv2 is incorporated. In this section, we talk about the security improvement of 802.16e over 802.16 and discuss its threats.

A. Security improvements

802.16e supports two authentication methods: RSA-based and EAP-based [20]. The RSA-based authentication is similar to that in 802.16. The handshake is like:

1) RSA-Request (SS → BS): MS_Random, MS_Certificate, SAID, SigSS.
2) RSA-Reply (SS ← BS): MS_Random, BS_Random, Encrypted pre-PAK, Key Lifetime, Key Sequence Number, BS_Certificate, SigBS.
3) RSA-Acknowledgement (SS → BS): BS_Random, Auth Result Code, Error-Code, Display-String, SigSS.

Here the differences are: random numbers are included in authentication messages to prevent replay attacks; the BS includes its own certificate in the authentication reply message to prove its identity. The optional EAP-based authentication can be used independently or combined with the RSA-based one. The real EAP methods are not specified in 802.16e. Both the methods support mutual authentication between SS and BS, which is a significant improvement to 802.16.

A master AK (Authorization Key) is established between SS and BS during authentication. Then the SS uses the AK to negotiate security capabilities and acquire available SA information. Three messages are defined for the handshake: SA-TEK-Challenge, SA-TEK-Request and SA-TEK-Response. These messages are authenticated with message authentication digests. Therefore attackers cannot forge these messages.

In addition to the DES-CBC and AES-CCM methods in 802.16, 802.16e also defines an AES-CTR mode [21] and an AES-CBC mode [22] to protect the MAC PDU payload. These two methods provide confidentiality by encrypting the MAC PDU payload.

B. Potential threats

The MSH-NCFG:Network Descriptor message is still a security hole in 802.16e. It can be modified or forged by attackers to launch topological attacks. Though 802.16e introduces mutual authentication in the authorization process, it does not mention how to distribute the OSS for the Mesh mode. Therefore, the threats to the OSS in 802.16 are still problems. Attackers can find the OSS and use it to establish links with normal nodes. All the management messages are not encrypted either and thus can be eavesdropped.

New Security Improvements

In this section, we propose some improvements to strengthen IEEE 802.16 security in the Mesh mode.

A. Neighbor authentication

In IEEE 802.16 Mesh mode, two neighbors rely on an OSS to establish a link. It is vulnerable to attacks as is stated in previous sections. Here we propose to use certificates to achieve authentication between neighbors.

Before a node establishes links with its neighbors, it must be authenticated by an Authorization center through an authorization process. The node can acquire a certificate issued by the Authorization center during the authorization process. We can call it a *mesh certificate*. After that, the node can use the mesh certificate to join the network. The entire process is performed as the following:

1) Challenge (A → B): A's mesh certificate, encrypted nonce-A, frame number, ID-A, ID-B, A' signature.
2) Challenge-Response (B → A): B's mesh certificate, encrypted nonce-B, frame number, ID-B, ID-A, B' signature.
3) Accept (A → B): accept, A' signature.

Node B first verifies A's mesh certificate with the Authorization center's public key and extracts A's public key. Then B uses A's public to verify A's signature to check the authenticity of the Challenge. As long as these two verification success, node B accepts node A and decrypt nonce-A with A's public key. Likewise, node A can authenticate node B based on the Challenge-Response message and get nonce-B. At last, node A replies with an Accept message to finish the handshake.

Now nodes A and B both know nonce-A and nonce-B. They can compute a link key as

K-AB=H(ID-A, ID-B, nonce-A, nonce-B) ,

where H() is a hash function such as HMAC or CMAC in 802.16.

Later node A can use the link key K-AB to update TEKs from node B. The process is the following:

1) Key Request (A → B): SAID, random number, MAC-Digest.

2) Key Reply (B → A): SAID, random number, encrypted old TEK parameters, encrypted new TEK parameters, MAC-Digest.

Here the random numbers are used to prevent the replay attack. The shared link key K-AB is used to compute MAC-Digests and encrypt TEK parameters.

The above neighbor authentication process is much securer than the original one in IEEE 802.16, because it is based on mesh certificates instead of the global shared OSS. In addition, the TEK update is secured by the shared link key instead of the original public key. Because the TEK update is performed periodically, we can expect our neighbor authentication process it is more efficient than the original one in IEEE 802.16.

B. Cryptographic issues

Generally, RSA-based public key cryptography is more expensive in computation than symmetric key cryptography. Therefore, the use of public key algorithms should be as less as possible in a security protocol. Meanwhile the performance can be increased if more efficient public key techniques are developed.

One substitute to the RSA-based public key cryptography is the *Elliptic Curve Cryptography* (ECC) [23], [24]. ECC can achieve the same level of security as RSA with smaller key sizes. It has been shown that 160-bit ECC provides comparable security to 1024-bit RSA and 224-bit ECC provides comparable security to 2048-bit RSA [25]. Under the same security level, smaller key sizes of ECC offer merits of faster computational efficiency, as well as memory, energy and bandwidth savings. Therefore ECC can be incorporated into IEEE 802.16 in future to replace RSA-based cryptography.

CONCLUSION

We discussed the security of IEEE 802.16 in mesh mode and found out it is very vulnerable to malicious attacks in multihop environments. Some improvements were proposed to secure IEEE 802.16 in Mesh mode.

REFERENCES

[1] IEEE Std 802.16-2004, *IEEE standard for local and metropolitan area networks, part 16: air interface for fixed broadband wireless access systems*, June 2004.

[2] WiMAX Forum, *http://www.wimaxforum.org/home/*, May 2006.

[3] IEEE Std 802.11-1999, *Information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part 11: wireless lan medium access control (MAC) and physical layer (PHY) specifications*, 1999.

[4] I.F. Akyildiz, X. Wang and W. Wang, "Wireless mesh networks: a survey," *Computer Networks Journal (Elsevier)*, Vol. 47, pp. 445-487, March 2005.

[5] N. Borisov, I. Goldberg and D. Wagner, "Intercepting mobile communications: the insecurity of 802.11," *ACM Mobicom'01*, 2001.

[6] W.A. Arbaugh, N. Shankar, Y.C. Wan, and K. Zhang, "Your 802.11 wireless network has no clothes," *IEEE Wireless Communications*, December 2002.

[7] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," *USENIX Security Symposium*, 2003.

[8] A. Mishra, N.L. Petroni, W.A. Arbaugh, and T. Fraser, "Security issues in IEEE 802.11 wireless local area networks: a survey," *Wiley Wireless Communications and Mobile Computing*, 4:821-833, 2004.

[9] C. He, J. C. Mitchell, "Security analysis and improvements for IEEE 802.11i," *Proc. the 12th Annual Network and Distributed System Security Symposium* (NDSS'05), pages 90-110. Feb. 2005.

[10] DOCSIS Home, *http://www.cablemodem.com/*, May 2006.

[11] D. Johnston and J. Walker, "Overview of IEEE 802.16 security," *IEEE Security & Privacy*, May/June 2004.

[12] M. Barbeau, "Wimax/802.16 threat analysis," *Proc the 1st ACM international workshop on Quality of service & security in wireless and mobile networks* (Q2SWinet'05), Montreal, Quebec, Canada, October 13, 2005.

[13] F. Yang, H. Zhou, L, Zhang, and J. Feng, "An improved security scheme in WMAN based on IEEE standard 802.16," *Proc 2005 International Conference on Wireless Communications, Networking and Mobile Computing*, Wuhan, China, Sept. 23-26, 2005

[14] Y. Zhou and Y. Fang, "Defend against topological attacks in sensor networks," *Proc IEEE Military Communications Conference* (Milcom'05), Atlantic City, New Jersey, October 17-20, 2005.

[15] Chris Karlof, David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Proc. First IEEE International Workshop on Sensor Network Protocols and Applications* (SNPA'03), May 2003.

[16] Y. Hu, A. Perrig, D. B. Johnson, "Pachet leashes: a defense against wormhole attacks in wireless networks," *Proc IEEE INFOCOM'03*, 2003.

[17] IETF RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*, November 1998.

[18] IETF RFC 3610, *Counter with CBC-MAC (CCM)*, September 2003.

[19] IEEE Std 802.16e-2005, *IEEE standard for local and metropolitan area networks, part 16: air interface for fixed and mobile broadband wireless access systems, amendment 2: physical and medium access control layers for combined fixed and mobile operation in licensed bands and corrigendum 1*, December 2005.

[20] IETF RFC 3748, *Extensible Authentication Protocol (EAP)*, June 2004.

[21] IETF RFC 3686, *Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)*, January 2004.

[22] IETF RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*, September 2003.

[23] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203-209, 1987.

[24] V. Miller, "Uses of Elliptic Curves in Cryptography," *Lecture Notes in Computer Science 218: Advances in Cryptology - CRYPTO'85*. Berlin: Springer-Verlag, 1986, pp. 417-426.

[25] S. Vanstone, "Responses to NIST's proposal," *Communications of the ACM*, 35, July 1992, 50-52 (communicated by John Anderson).