Volume 2, No. 3, May-June 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
TECHNICAL NOTE
Available Online at www.ijarcs.info

Distributed Architecture for Backbone Area Security of Wireless Mesh Networks

Umesh Kumar Singh*
Institute of Computer Science
Vikram University
Ujjain (M.P.), India
umeshsingh@rediffmail.com

Lokesh Laddhani
Institute of Computer Science
Vikram University
Ujjain (M.P.), India
lokesh.laddhani@gmail.com

Shivlal Mewada
Institute of Computer Science
Vikram University
Ujjain (M.P.), India
shiv.mewada@gmail.com

Abstract: Wireless mesh networks have emerged recently as a technology for next generation wireless networking. Due to multi-hop communication and routing on layer two in mesh networks, attacks on the routing, selective forwarding and eavesdropping on confidential data become relatively easy. To avoid such attacks, a differentiated security approach which is based on protection levels associated with nodes in the network is introduced in this paper. Participation in the MAC layer routing is facilitated according to the respective protection level of a node. Using additional cryptographic protection, the approach introduced in this paper would greatly help in avoiding unintentional disclosure of confidential data.
Keywords: Security, Routing, Wireless Mesh Networks

I. INTRODUCTION

Wireless mesh networks can be implemented with various wireless technologies including IEEE 802.11 (WLANs) [1, 2]. The field of Wireless Networking has been experiencing an explosive growth proportional to the Internet. Since, the users and service providers enjoy the flexibility and accessibility of network any-where, any-time, Wireless Networks suffers from risks of unintentional disclosure of confidential data. The major risk involved is that the information is transmitted through air [3]. In contrast to the single-hop communication used in IEEE 802.11 [4] wireless networks, mesh networks apply routing mechanisms on layer 2 based on MAC addresses in order to achieve multi-hop communication. This means that each node taking part in the mesh network has to forward frames according to a specific MAC layer routing protocol, e. g. Hybrid Wireless Mesh Protocol [5].

Security in Wireless Mesh Networks (WMNs) is still in its infancy, as very little attention has been devoted so far to this issue by the research community [1, 6, 7]. Although many security schemes have been proposed for wireless LANs [8] and ad hoc networks [9, 10, 11, 12, 13, 14], they are not suitable for WMNs, which need convincing security solutions that should act as incentives for customers to subscribe to reliable services [1, 15, 16, 17]. In WMNs, two different security areas can be identified: one related to the access of user terminals (user authentication and data encryption) and the other related to network devices in the backbone of the WMN (mutual authentication of network devices, and secure exchange of data and control messages).

In this paper, we focus on backbone area security by proposing a novel and fully Distributed Security Architecture for Wireless Mesh Networks, which provides a security framework for the mesh backbone, that is, access control for mesh routers as well as security and integrity of all data communications that occur in the WMN; this is achieved with layer-2 encryption through the utilization of a shared key whose delivery is assured by a key distribution protocol.

II. RELATED WORK

So far, little attention has been devoted to security in WMNs by the research community [1, 6]. Two main security areas can be identified: the first is related to the access of client terminals, while the second is related to the mesh backbone. *Client authentication* and *access control* can be provided using standard techniques [18, 19, 20], which guarantee a high level of flexibility and transparency: all users can access the mesh network without any change to their client devices and software. However, client mobility can pose severe problems to security architectures, especially when real-time traffic is transmitted. To cope with these problems, proactive key distribution techniques can be devised [17, 21, 22].

Several works investigate the use of cryptographic techniques to secure the information exchanged through a wireless network. In [12], authors proposed to use PANA, the Protocol for carrying authentication for Network Access, to authenticate the wireless clients and to provide them with the cryptographic material necessary to establish an encrypted tunnel with the remote access router to which they are associated.

Other approaches have been proposed to authenticate the users in WMNs, maintaining at the same time a low overhead. In [23], security architecture for high integrity multi-hop WMNs is proposed; a heterogeneous set of WMN providers is modeled as a credit-card based system so that each mesh client does not need to be bound to a specific operator, but can

achieve ubiquitous network access by first obtaining a universal pass issued by a trusted third broker.

In [24], a new authentication technique for hierarchical WMNs based on threshold cryptography is defined, where the certification authority services are provided through the collaboration of a pre-determined set of mesh routers. The proposed architecture extends the Diffie-Hellman key exchange protocol for negotiating a key that authorizes a user to access the backbone network services provided by a mesh router situated in a different zone.

In [11], Komninos et al proposed a distributed detection mechanism that makes use of local agents to collect and analyze audit data. Each agent assigns a *compromised* status to other network agents, and passes it to the neighboring nodes for further decisions. In [25], two protocols are defined to detect replicated nodes by distributing the information about each node's identity and geographical position to a randomly selected set of nodes.

In [12] and [26], two different approaches are presented to allow specific coalitions of devices to act together as a single certification authority, whereas in [27] a hierarchical key management architecture is proposed to obtain an efficient establishment of distributed trust. Capkunet et al in [28] proposed a fully self-organized public key management scheme that, similarly to the PGP scheme, does not rely on any trusted authority to perform the authentication of other peer nodes: each network node is its own certification authority and issues certificates to other nodes; the authentication procedure is performed via trust chains of certificates. The public key management schemes proposed in [29] and [30] further enhance the security of the distributed approaches like those presented in the above works, by using proactive secret sharing and fast verifiable share redistribution techniques which permit to update periodically the secret shares.

Even if these distributed systems improve the network fault tolerance by removing the single point of failure introduced by centralized schemes, they are not very efficient in terms of computational or communication overhead. On the other hand, the centralized architecture proposed in [31] (MobiSEC), provides both access control for mesh users and routers with a negligible impact on the network performance.

Finally, we underline that none of the above solutions addresses all the security problems typical of a wireless mesh network. In fact, the previous proposals deal with security weaknesses related to a specific layer or protocol of the network stack, while in this paper we propose a fully distributed framework that copes with the security problems of the backbone area of a WMN, maintaining a high level of compatibility with current wireless security standards without impacting, at the same time, on the WMN performance.

III. CRYPTOGRAPHIC PRIMITIVES & ALGORITHMS

In this Section we introduce the cryptographic primitives and algorithms used in our architecture to distribute the Key Server functionalities among a group of mesh routers.

We first introduce the Shamir Secret Sharing algorithm, which is used to share the *key service* private key among a set of core mesh routers; then, we provide an overview of the Threshold Signature Scheme, which is used by all generic mesh routers to prove the authenticity of the messages signed by the core mesh routers.

Shamir Secret Sharing Algorithm: In [32], Shamir proposes a method to share a secret among a group of parties. In an (n, t) threshold sharing scheme, a secret S is divided into n secret shares, but only t out of n pieces are necessary to recover the original secret.

The scheme is based on the following property:

If

$$f(x) = S + \sum_{i=1}^{t-1} a_i x^i$$

Is a polynomial of order t − 1 whose coefficients a_i are chosen over a finite field Zq (where q is a large prime) and a_0 = S, then only t distinct points $\{(x_i, f(x_i))\}$ are necessary to recover the secret S, while t − 1 or fewer points provide no information about the shared secret. The method used to recover the secret is known as *Lagrange interpolation*, which is briefly sketched in the following.

Let C = $\{s_1, s_2, ..., s_n\}$ be the set of the n secret shares, where s_i = f(i) mod q, and let A be any subset of C whose cardinality is equal to t (A □ C, |A| = t). The secret S can then be recovered from A, according to the following equation:

$$\begin{aligned} l_i(x) &= \prod_{j \in A, j \neq i} \frac{x-j}{i-j} \\ k_i &= l_i(0) \cdot s_i = l_i(0) \cdot f(i) \bmod q \\ S &= \sum_{i \in A} k_i \bmod q = \sum_{i \in A} l_i(0) \cdot s_i \bmod q \end{aligned} \quad (1)$$

Threshold Signature Scheme: Threshold signature schemes permit to verify the authenticity of the signature applied to a message by a coalition of t out of n parties without revealing the private key.

In an RSA signature scheme [33], the private exponent d of the *key service* private key

$(K_k^{-1} = \langle d, N \rangle)$ can be shared by n parties.

The signature of any message m, where h(m) represents the digest of m (computed using a one-way hash function), can be recovered by collecting t out of n partial signatures and multiplying them according to the following expression:

$$\begin{aligned} &\prod_{i=1}^{t} h(m)^{k_i} \bmod N = \\ &= h(m)^{\sum_{i=1}^{t} k_i} \bmod N = \\ &= h(m)^{\sum_{i=1}^{t} l_i(0) \cdot q(i)} \bmod N = \\ &= h(m)^d \bmod N \end{aligned} \quad (2)$$

Finally, to verify the authenticity of the message, the node has to raise the previous signature to the public exponent e, and compare the obtained result with the hash value of the message, according to expression (3).

$$(h(m)^d \bmod N)^e \bmod N = \\ = h(m)^{de} \bmod N = \\ = h(m) \qquad (3)$$

IV. KEY MANAGEMENT

To protect the WMN against outside attackers it is sufficient to deploy one single dynamically-generated key for the whole network { the Global Key (GK). Because the effective transmission key also contains the sender's MAC address and a station-generated sequence number (IV), there is no reuse of key material, provided that the GK is re-generated periodically and on every network restart using a reliable random number generator.

This approach requires a single assigned station, the Mesh Key Distributor (MKD), to generate the initial and following GKs. Similar to the MKD in the 802.11s proposal this can be a station connected to the backbone network and having direct access to the user database. However, it is possible to use a leader election protocol as well, either once or for every round of GK generation.

Because there is only one key, all Mesh Points can decrypt and verify the messages from any other MP. However, when a station leaves the network or when the key has been used for some time, it needs to be re-generated. To allow that, every key is augmented with a relative validity value VN. This value is generated by the MKD and propagated together with the key. A sane value for typical networks is in the order of ten minutes.

The 802.11i standard requires every station to authenticate to every other station. However, this is not really required to ensure secure communication. In WMNSec every station has to perform only one authentication to become part of the network and to receive the Global Key.

At the beginning the Mesh Key Distributor (MKD) is the only "authenticated" station { the WMN consists only of the MKD. A station S1 which wants to participate in the WMN has to authenticate with the Mesh Key Distributor (MKD) using the 4-Way-Handhake. Hereby the MKD is the authenticator and S1 is the supplicant. When the mutual authentication succeeds the new station becomes an "authenticated" part of the WMN and receives the GK using the Group Key Handshake. After that it can switch its role to authenticator and further distribute the key. Another station now can authenticate with the MKD or S1, depending on which connection is more stable. Thus, the iterative authentication forms a spanning tree starting at the MKD and expanding to the whole network. Because a GKx is always augmented by its validity time Vx, the latter has to be transmitted during the handshake. The 802.11i standard allows to transfer user-specific fields as part of the handshake payload, so that the Group Key handshake has been extended to always include Vx for a transmitted GKx.

Station Roles :Two roles are used in the 4-Way-Handhake: supplicant and authenticator. Whenever a station needs to receive a GK it becomes a supplicant (either when it was just started, or when the GK it uses is expiring). A station in possession of the current GK becomes an authenticator and allows other stations to prove their authenticity and to receive the GK. The MKD is always an authenticator because it can generate a new GK whenever required. No station shall play both roles at the same time (either it does not have a current key, and thus cannot spread one, or it has one and does not require a key update).

Re-Keying and Re-Authentication :When a cryptographic key is used actively, the amount of data encrypted with it grows and it becomes easier to perform attacks on the encryption algorithm. To prevent breaking of the security, every key has to be replaced after a certain amount of data has been encrypted with it. When a key is replaced by a new one it can happen that stations are using different keys and thus are not able to communicate with each-other. Because a WMN is a distributed system it is not possible to replace the key in the whole network instantaneously. Still, some applications demand interruption-free communication, requiring seamless exchange of the encryption keys.

To provide service without interruptions a transition phase has been devised (example in Figure 1). This transition phase allows a station to migrate from the old to the new key without losing its ability to communicate with its neighbors, without a strict synchronization scheme. The transition begins when the validity VN of the current global key GKN is almost expired and consists of six steps:

First, the new key GKN+1 is received using the 4-Way-Handhake and Group Key Handshake, at the same time re-verifying the station's authentication (1).

After that both the old and the new key are set up as receiver (RX) keys (2). Now the station can receive packets from stations which already have completed the re-keying as well as from stations which have not started it yet.

Now, to give other stations enough time to perform the re- keying, a transition delay T is performed (3). This time interval has to be dimensioned to allow all neighbors of the current station to perform a re-keying and to receive GKN+1.A typical value is in the order of 10s.

After the delay the station can assume that all neighbors have received the new GKN+1, so it can be used for transmissions (TX; 4). Still, it is possible that other nodes are in their own transition phase, and still use the deprecated GKN for transmitting.

To allow neighbors to finish their own transition the old key GKN has to be allowed as a receive key (RX) for the same time other stations could use it: it is kept valid for a second transition time T (5).

Finally, when it can be assumed that all stations have completed step 4 and thus are using GKN+1, the old GKN can be invalidated and deleted from the key storage (6).

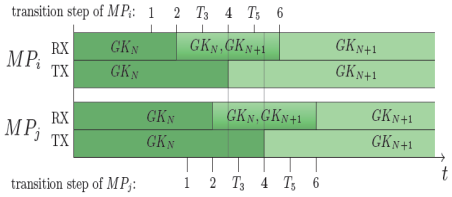

Figure-1: Re-Keying: Six Steps of Distributed GK Update and Transition. (MPx = Mesh Point x; RX = receive key(s); TX = transmit key).

The whole transition phase requires 2 · T to complete, meaning that it should be started when the remaining key validity is $V_N = 2 \cdot T$, preventing the old key from being used after its expiry. The transition of two stations M Pi and MPj can be seen in Figure 1. Even though MPj begins the transition at a later time, interruption-free communication is possible:

when M Pi switches to the new key, MPj has already completed step 2 and can successfully decrypt the packets. When MPj switches to the new key, MPi accepts packets encrypted with both keys, causing no packet losses. The transition algorithm steps are summarized as follows:

1.Change role to supplicant, perform Global Key Handshake, receive GK_N+1
2. Change role to authenticator, install GKN+1 as additional receive key
3. Wait transition time T (T_3)
4. Setup GK_{N+1} as new transmit key
5. Wait transition time T (T_5)
6. Invalidate GK_N

V. CONCLUSIONS

In this paper a distributed architecture for Wireless Mesh Networks, which provides a security framework for the mesh backbone is presented. By concentrating on protection against external attackers the authentication and key management overhead could be significantly reduced. The proposed architecture is appropriate in scenarios where interruption-free connectivity and mobility are required, e.g. teleportation of mobile robots. Still the proposed scheme relies on the secure mechanisms introduced by 802.11i { the 4-Way-Hand- hake and the periodic update of the used cryptographic keys. The main restriction compared to 802.11i is that there is no protection against attackers with insider knowledge (i.e. participants of the WMN). While this has some relevance in roof-net WMNs, it is not an issue in centrally organized industrial networks.

VI. REFRENCES

[1] Akyildiz and X. Wang, "A survey on wireless mesh networks," IEEE Communications Magazine, vol. 43, no. 9, pp. 23–30, 2005.

[2] W. A. Arbaugh, "Wireless security is different," Magazine of IEEE Computer Society, Computer, vol. 36, no 8, pp. 99–101, 2003.

[3] J. Zhu, and J. Ma, "A new authentication scheme with anonymity for wireless environments," IEEE Transactions on Consumer Electronics, vol. 50, no 1, pp. 231–235, 2004.

[4] IEEE Computer Society. IEEE Standard for Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 2007.

[5] IEEE Computer Society. IEEE P802.11s/D2.0 – Draft STANDARD for Local and Metropolitan Area Networks – Specific Requirements – Amendment to Part 11: Mesh Networking, March 2008.

[6] N. Ben Salem and J.-P. Hubaux. Securing wireless mesh networks. IEEE Wireless Communications, 13(2):50–55, April 2006.

[7] C. Adjih, D. Raffo, and P.M¨uhlethaler. Attacks against OLSR: Distributed key management for security. In Proceedings of the 1st OLSR Interop and Workshop, San Diego, CA, USA, August 2005.

[8] W. Stallings. Cryptography and Network Security, Fourth Edition. McGraw-Hill, September 2003.

[9] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. M¨uhlethaler, and D. Raffo. Securing the OLSR protocol. In Proceedings of the 2nd Mediterranean Workshop on Ad-Hoc Networks (Med- Hoc-Net), Mahdia, Tunisie, June 2003.

[10] D. Raffo, C. Adjih, T. Clausen, and P. M¨uhlethaler. An advanced signature system for OLSR. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN'04), pages 10–16, Washington DC, USA, October 2004.

[11] N. Komninos, D. Vergados, and C. Douligeris. Detecting unauthorized and compromised nodes in mobile ad hoc networks. Elsevier Ad Hoc Networks, 5(3):289–298, 2007.

[12] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang. Selfsecuring ad hoc wireless networks. Proceedings of the 7th International Symposium on Computers and Communications (ISCC 2002), pages 567–574, Taormina, Italy, July 2002.

[13] N. Milanovic, M. Malek, A. Davidson, and V. Milutinovic. Routing and security in mobile ad hoc networks. IEEE Computer, 37(2):61–65, February 2004.

[14] L. Zhou and Z. J. Haas. Securing ad hoc networks. IEEE Network, 13(6):24–30, November 1999.

[15] R. Bruno, M. Conti, and E. Gregori. Mesh networks: commodity multihop ad hoc networks. IEEE Communications Magazine, 43(3):123–131, March 2005.

[16] O. Cheikhrouhou, M. Laurent-Maknavicius, and H. Chaouchi. Security architecture in a multi-hop mesh network. In Proceedings of the 5th Conference on Security and Network Architectures (SAR 2006), Seignosse, France, June 2006.

[17] R. Fantacci, L. Maccari, T. Pecorella, and F. Frosali. A secure and performant token-based authentication for infrastructure and mesh 802.1X networks. In Proceedings of Infocom '06, Barcelona, Spain, April 2006.

[18] IEEE Standard 802.11i. Medium Access Control (MAC) security enhancements, amendment 6. IEEE Computer Society, 2004.

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

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

[21] M. Kassab, A. Belghith, J.-M. Bonnin, and S. Sassi. Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks. In Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling (WMuNeP'05), pages 46–53, Montreal, Quebec, Canada, 2005.

[22] A. R. Prasad and H. Wang. Roaming key based fast handover in WLANs. Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC'05), 3:1570–1576, New Orleans, LA, USA, March 2005.

[23] Y. Zhang and Y. Fang. Arsa: An attack-resilient security architecture for multihop wireless mesh networks. IEEE Journal on Selected Areas in Communications, 24(10):1916– 1928, October 2006.

[24] Y. Fu, J. He, R. Wang, and G. Li. Mutual authentication in wireless mesh networks. In Proceedings of ICC'08, pages 1690–1694, Beijing, China, May 2008.

[25] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. In Proceedings of the 2005 IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 2005.

[26] S. Yi and R. Kravets. Moca: Mobile certificate authority for wireless ad hoc networks. Proceedings of the 2nd Annual PKI Research Workshop (PKI03), pages 612–613, Gaithersburg, MD, USA, April 2003.

[27] G. Xu and L. Iftode. Locality driven key management architecture for mobile ad-hoc networks. Proceedings of the 1st IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS), pages 436–446, Fort Lauderdale, Florida, USA, October 2004.

[28] S. Capkun, L. Buttyan, and J.-P. Hubaux. Self-organized public-key management for mobile ad hoc networks. IEEE Transactions on Mobile Computing, pages 52–64, 2003.

[29] B. Wua, J. Wua, E. B. Fernandeza, M. Ilyasa, and S. Magliveras. Secure and efficient key management in mobile ad hoc networks. Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS 2005), Denver, Colorado, USA, April 2005.

[30] J. Kim and S. Bahk. Meca: Distributed certification authority in wireless mesh networks. Proceedings of the 5th IEEE Consumer Communications and Networking Conference,pages 267–271, Las Vegas, NV, USA, January 2008.

[31] F. Martignon, S. Paris, and A. Capone. Design and Implementation of MobiSEC: a Complete Security Architecture for Wireless Mesh Networks. Elsevier Computer Networks, 53(12):2192–2207, August 2009.

[32] A. Shamir. How to share a secret. Communications ACM, 22(11):612–613, 1979.

[33] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'91), pages 457–469, Santa Barbara,CA, USA, August 1991.