A Secure Key Management Model for Wireless Mesh Networks

Li Gao, Elizabeth Chang, Sazia Parvin, Song Han, Tharam Dillon
Digital Ecosystems and Business Intelligence Institute
Curtin University of Technology, Australia
{ li.gao1, sazia.parvin }@postgrad.curtin.edu.au,
{ Elizabeth.Chang, Song.Han, Tharam.Dellon}@cbs.curtin.edu.au

Abstract— **As Wireless Mesh Networks (WMNs) are newly emerging wireless technologies, they are designed to have huge potential for strengthening Internet deployment and access. However, they are far from muture for large-scale deployment in some applications due to the lack of the satisfactory guarantees on security. The main challenges exposed to the security of WMNs come from the facts of the shared nature of the wireless architecture and the lack of globally trusted central authorities. A well-performed security framework for WMNs will contribute to network survivability and strongly support the network growth. A low-computational and scalable key management model for WMNs is proposed in this paper which aims to guarantee well-performed key management services and protection from potential attacks.**

Keywords-Wireless Mesh Networks; security; key management

I. INTRODUCTION

Wireless Mesh Networks, an emerging technology, are considered as the promised choices for wireless Internet communications since they allow fast, easy, and low-cost network deployment.

The nature of flexible dynamic deployment and the lack of the fixed infrastructure expose WMNs to suffer varieties of security attacks [4, 5]. It holds back the potential advantages and wide-scale deployment of this promising wireless networking technology. As various applications of WMNs have been explored, the security mechanisms are unfortunately far from mature. Appropriate security frameworks are never more urgent and important for WMNs. While the security of WMNs is a fairly new research topic, the starting point can be to adapt some existing security schemes designed for wireless ad hoc networks and wireless sensor networks which share some similarities with WMNs to some extent.

In this paper, we start with the characteristics of WMNs in section II including architecture, advantages and constrains. The four main critical security challenges existing in WMNs, such as securing routing, securing location information, authentication and key management, will be analyzed in section III with the emphasis on key management. Existing techniques, challenges and potential countermeasures to design secure key management schemes will be discussed in section III as well. A proposed low-computational and scalable key management model will be provided in section IV.

II. CHARACTERISTICS OF WMNS

WMNs are multi-hop and multi-channel wireless networks formed by mesh nodes. Unlike traditional wireless networks, WMNs rely on each mesh node to keep the network connected instead of any fixed infrastructure. Instead, wireless mesh nodes WMNs are designed to resolve the limitations and to significantly improve the performance of ad hoc networks, wireless local area networks (WLANs), wireless personal area networks (WPANs), and wireless metropolitan area networks (WMANs). Numerous applications of wireless mesh networks are being explored and new technical results have been achieved. Wireless service providers in personal, home, campus, community, and municipal areas are starting to use wireless mesh networks [1].

A. Archetecture

WMNs are multi-hop and multi-channel wireless networks formed by mesh nodes which are classified into mesh routers and mesh clients. The architecture of Wireless Mesh Networks in Figure 1 shows that two mesh routers are connected to the conventional wired Internet, other mesh routers and mesh clients are forming the mesh connections and some mesh routers with built-in gateway functions are integrated with most of existing wireless networks, such as WiMAX, celluar network, sensor and WiFi; one mesh router with built-in smart IP is connecting to the wired networking.

1550-445X/10 $26.00 © 2010 IEEE
DOI 10.1109/AINA.2010.110

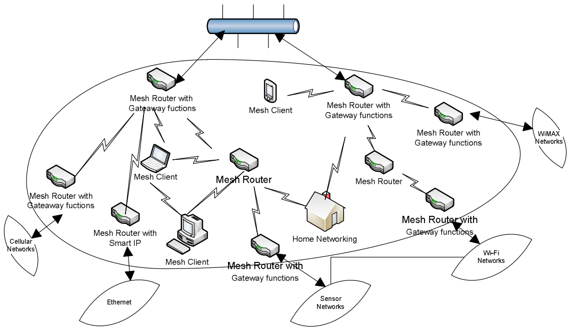

Figure 1. Architecture of WMNs .

According to definitions and specifications in [1, 2, 3], Mesh routers are usually fixed on the streetlight top, roof of buildings, or inside vehicles with no energy constraints. Different with the conventional wireless routers, mesh routers have additional functionalities to enable mesh connections rather than perform only routing and form the backbone for the networking. Multiple interfaces of the same or different communications technologies are built in the mesh routers to accommodate the different networking requirements. More coverage can be achieved by using multi-hop communication pattern through the neighbour mesh nodes. Some mesh routers are connected to the conventional wired Internet through the gateway functions. The outstanding functionality in integrating Wireless Mesh Networks with other existing networks such as the Internet, cellular, WiFi, WiMAX and sensor networks and ad hoc networks, etc., can be achieved through the built-in bridging functions in the mesh routers. Mesh routers can be built on general-purpose computer systems or can be built on sensitive hardware platforms. Mesh clients are either static or mobile with energy constraints and have mesh connecting capabilities to communicate with mesh routers and themselves. Mesh clients are usually simple hardware with simple softwares that a single communication interface is built in them and can provide networks access for both mesh and conventional clients.

B. *Advantages*

- Wireless Mesh Networks are considered fast (local packets do not have to travel back to a central server), inexpensive (no wired infrastructure), large coverage (multi-hop and multi-channel) alternatives to WLANs (wireless local area network) and backbone networks to mobile clients [2].
- Mesh networks are self configuring: the network automatically incorporates a new router or client into the existing structure without needing any adjustments by a network administrator [2].
- Mesh networks are self healing: since the network automatically finds the fastest and most reliable paths to send data, even if nodes are blocked or lose their signal [1].
- Wireless mesh nodes are easy to install and uninstall, making the network extremely adaptable and expandable as more or less coverage is needed. They are convenient where Ethernet wall connections are lacking, for instance, in outdoor concert venues, warehouses or transportation settings [1].
- Compatibility: WMNs work on the common WiFi standards (IEEE 802.11a, b and g) already in place for most wireless networks. The existing wireless networking technologies such as IEEE 802.11, IEEE 802.15, IEEE 802.16 and IEEE 802.20 are used for the implementation of WMNs [3].
- MWNs may bring the dream of a seamless connected world into reality because this promising networking technology is designed to have the power of integrating with other existing wired/wireless networks [3].

C. *Constrains*

There are four main constraints in every current wireless networks including wireless WiFi, cellular, sensor, ad hoc and WMNs etc.

- **Battery**: the total power capacity on the end nodes is very limited and only low resource consuming devices can be deployed.
- **CPU**: the total computing power is limited so that devices for large computation are not suitable.
- **Scalability**: the current wireless networks act poorly when the networks enlarged in both aspects of members and computation.
- **Mobility**: mobile devices expose great pressure on the convergence and ability of hand-over to the networks.

III. SECURITY CHALLENGES IN WMNS

Except the general security features, saying confidentiality, integrity and availability, the nature of flexible dynamic deployment and the lack of the infrastructure expose WMNs to suffer varieties of security attacks [4, 5, 22]. This holds back the potential advantages and wide-scale deployment of this promising wireless networking technology. As various applications of Wireless Mesh Networks have been explored, the security mechanisms are unfortunately unexplored. The great starting point can be to utilize and adapt some existing security schemes designed for wireless ad hoc networks and wireless sensor networks which share great similarities with WMNs to some extent.

Assuming the existence of upper layer security mechanism, such as anti-virus software and Secure Sockets Layer (SSL) protocol [22], there are four main security issues in WMNs including securing routing, securing location information, authentication and key management. Due to the vital importance, this paper will focus on key management with the expected outcome of a low-computational and scalable key management framework with well-performed security functions and protection from potential attacks.

A. Securing Routing

In WMNs, the data travels via multi-hops from the source node to its destination. The routing protocols for WMNs are designed to achieve availability and robustness against both dynamically changing topology and external/internal attacks [22]. Although routing protocols with well-performed security features are under active research [6], very few routing protocols have been proposed specifically for the newly emerging WMNs. The great similarities between WMNs and wireless ad hoc networks make it feasible for WMNs to borrow the ideas from the domain of wireless ad hoc networks.

B. Securing Location Information

Most current routing protocols are adopted from wireless ad hoc networks including both topology-based and geographic routing schemes [4]. For geographic routing schemes, the location of the mesh routers are crucial to multi-hop routing schemes and thus subject to passive/active attacks. For example, the WMNs deployed for the military and public safety are relying highly on the location information for the sake of safety. While very little research has been done for the fairly new WMNs, securing location information has been addressed in wireless sensor networks [6]. It is inspiring and feasible to utilize some schemes from the domain of wireless sensor networks.

C. Authentication

Most current routing protocols are adopted from wireless ad hoc networks including both topology-based and geographic routing schemes [4]. For geographic routing schemes, the location of the mesh routers are crucial to multi-hop routing schemes and thus subject to passive/active attacks. For example, the WMNs deployed for the military and public safety are relying highly on the location information for the sake of safety. While very little research has been done for the fairly new WMNs, securing location information has been addressed in wireless sensor networks [6]. It is inspiring and feasible to utilize some schemes from the domain of wireless sensor networks.

D. Key Management

All the current security mechanisms (e.g. encryption, digital signature and authentication) which can be used for WMNs are based on cryptographic keys and thus high degree key management services are in demand.

1) Techniques

Key management service is responsible for keeping track of binding between keys and nodes and for assisting the establishment of mutual trust and secure communication between nodes [9]. Different approaches for key management are listed in [8] including key distribution, key transport, key agreement and key updating. Optional techniques for designing secure key management schemes can be obtained from some successful schemes that have been worked out for wireless networks including ad hoc, sensor, cellular and WiFi.

A composite key management service was proposed by Yi and Kravets in [10] for asynchronous ad hoc networks which achieved the distribution of certificate authority using threshold cryptography.

Utilizing elliptic curve cryptography, Du et al. proposed a novel routing-driven key management scheme for heterogeneous sensor networks, which establishes shared keys only for neighbour sensors that may communicate with each other in the key pre-distribution stage. Better security can be provided with significant saving on sensor storage space and energy consumption than some existing key management schemes [10]. The small key size and low computation overhead of Elliptic Curve Cryptography (ECC) provides new opportunities to utilize public-key cryptography in WMNs.

Based on a polynomial-based key pre-distribution scheme, Ning and Li presented a general framework for establishing pair-wise keys between sensors including a random subset assignment key pre-distribution scheme and a grid-based key pre-distribution scheme [11].

Li and Xin proposed a distributed key management approach by using the self-certified public key system and threshold secret sharing schemes [12]. Without any assumption of prefixed trust relationship between nodes, the ad hoc network works in a self-organizing way to provide the key generation and key management services using threshold secret sharing schemes, which can effectively solve the problem of single point of failure. The claimed advantages of self-certified public key system include that (1) the storage space and the communication overheads can be reduced since the certificate is unnecessary; (2) the computational costs can be decreased since no public key verification required; (3) there is no key escrow problem since the Certificate Authority (CA) does not know the users' private keys. As compared with previous work, which is implemented with the certificate-based public key system and identity-based (ID-based) public key system, the proposed approach is more secure and efficient.

Mu and Liu proposed a mesh based multicast key management scheme for mobile ad hoc networks [13]. Among multicast groups, some physically more secure and subjectively more trustworthy members form a mesh and use threshold cryptography to share the responsibility and provide group key services with strong security and high availability. Adaptive policy and a token mechanism are introduced to avoid conflict during group key updating. The analysis shows that the scheme has perfect security and efficiency.

With the future large-scale deployment of worldwide wireless connection, group communication is a very important pattern in WMNs [14, 15]. Securing group communication in dynamic and large-scale groups is more complex than securing one-to-one communications due to the inherent scalability issues of group key management. In particular, the high computation overhead for key establishment and key renewing is usually relevant to the group size and consequently becomes a performance bottleneck in achieving scalability [15].

Scalability is a desirable property of a system, a network, or a process, which indicates its ability to either handle growing amounts of work in a graceful manner, or to be readily enlarged [16]. There are some successful scalable key management protocols.

Lee and Shieh proposed a new approach that features decoupling of group size and computation cost for group key management in [14]. By using a hierarchical key distribution architecture and load sharing, the load of key management can be shared by a group of third parties without revealing group messages to them. The proposed scheme is claimed to achieve better scalability because the cost for key management of each component is independent of the group size.

Mittra addressed the scalability issue by partitioning the group members into many subgroups, which are arranged in a hierarchy to create a single multicast group in [13]. Scalability is achieved by making each subgroup relatively independent and thus group membership changes can be limited to the respective subgroups. Another essential method that helps the protocol to achieve the scalability is the subgroup agents, which assist in translating messages among subgroups using different subgroup keys.

2) Challenges

Even though all existing key management schemes for wireless sensor networks and ad hoc networks are claimed to have high security, their weaknesses such as high computation overhead, vulnerability to some kinds of attacks, and poor scalability are undeniable [4, 14, 22]. In addition, the unique characteristics of WMNs make security more challenging. Three challenges with the development of key management schemes are identified specifically for the new emerging WMNs.

a) The lack of infrastructure is not the only difficulty for key generation but also makes it harder to share, transport and update keys in WMNs. Additionally, very constrained devices, both in computational capacity and input/output capabilities, pose great challenges on low-computational security services.

b) A distributed CA scheme is required due to the absence of a pre-established trusted network infrastructure in WMNs obstructing direct application of PKI.

c) Scalability is in high demand due to potential large networks deployment resulting from one of the main advantages of WMNs, i.e. being adaptable and expandable.

3) Potential Countermeasures

Keeping all these challenges in mind, more comprehensive research is needed to find new approaches to achieve the proposed research objectives. One promising and important starting point comes from the great similarities that WMNs share with wireless ad hoc, sensor networks. The security mechanisms within wireless ad hoc and sensor networks have been extensively studied. Ideas and methods can be borrowed from the domains of wireless ad hoc and sensor networks since some successful key management schemes have been worked out for them. Feasibility of combination of the unique features of WMNs with existing security approaches has been showed by key management protocols integrating mesh into ad hoc networks [17]. Even with such a promising starting point, it is still very challenging to develop a well-performed key management. Some new definitions should be worked out to suit the new Mesh system initialization. Proper cryptographic schemes need to be adapted to have the compatibility with the Mesh functions.

More comprehensive requirements should be considered carefully in developing key management schemes specific for WMNs. Some designing principles would be as follows:

- Low-computation is a highly pursued feature in my research project to avoid the drawbacks due to the lack of any wired infrastructure in WMNs. Thus, If possible, low-computational cryptographic methods, such as symmetric cryptographic technique, Elliptic Curve Cryptography and threshold schemes, and probabilistic approach, should be used rather than high-computational schemes, such as RSA, asymmetric cryptography and polynomial-based techniques. Some new definitions and parameters should be developed in the system initialization stage and some improvement should be done to the common cryptographic methods to accommodate the Mesh environment.
- A distributed CA scheme will be used instead of centralised CA to utilise applications of PKI which is the most common practice in key management. Distributed CA distributes the functionality of the centralised CA to the whole network by applying threshold cryptography [18] which has been proved efficient and well-performed. Partially

Distributed Certificate Authority, Fully Distributed Certificate Authority and Self-issued Certificates [19] are some successful schemes dealing with Distributed CA, but they are still not good enough to fully address the problem. More work needs to be done to explore the finely defined distributed CA and bridge the traditional PKI with Mesh functions.

- Scalability is another highly pursued feature in order to deal with the stress on scalability caused by the potential large-scale networks deployment. As an important feature of all security mechanisms, scalability is discussed in depth by [15] and some scalable key management schemes proposed in [15, 13] will give researchers inspiration in combining the specific requirements of WMNs with existing scalable schemes for other wireless networks.

IV. Proposed key management model

To achieve the objective of developing a low-computational and scalable key management for WMNs, this proposed model will be carried out in the following steps:

A. Theoretical Framework

The theoretical framework would be designed to accommodate Attack Models and Key Management Models. In the Attack Models part, the project will start with some most well-defined and important attacks including eavesdropping (the most common passive attack), DoS (Denial of Services) and replaying attack (two most common active attacks). The defined attack models would be used to analyze the security level of the proposed key management schemes, that is, if the proposed schemes coped well corresponding to the attack models, then high level of security is achieved. If possible, more attacks will be measured in order to strengthen the security level of proposed key management schemes. Some new definitions and parameters should be developed in the system initialization stage and some innovative features should be added to the common cryptographic methods to accommodate the Mesh environment. Definitions of node “joining”, “leaving”, “low-computation”, and “scalability” would be given to address the WMN environment at this stage as well.

B. Key Management Model

At this step, the network model and the system setup would be clarified. Three levels of key management schemes would be targeted including key management protocols for (1) Mesh routers (RR) pattern, for (2) Mesh clients (CC) pattern, and for (3) Mesh router and Mesh clients (RC) pattern addressing the different status of entities within WMNs.

- RR Pattern: because the mesh routers form the backbone for the entire networking and have reasonable high input/output capability, highest level of security is required. Additional, the RR model has the good tolerance of computation overhead and most routers are static making the Trusted Third Party (CA) possible. Thus, complicated cryptographic methods, such as PKI, two-party and n-party Diffie-Hellman schemes [20], can be used to design the key management schemes for RR pattern.

- CC Pattern: because the mesh clients are usually mobile and form the lower layer of communication with low input/output capability, low computation is the most challenging feature and reasonable level of security is required. Thus, in order to design the key management schemes for CC model, some low-computational cryptographic methods, such as symmetric cryptography and threshold secret sharing schemes can be used to host the unique system requirement.
- RC Pattern: the key management schemes for the Mesh router and Mesh clients (RC) pattern can be in between.

In addition, since these three patterns belong to group communication models, the existing results for group key management [14, 15, 21] can be a great help to accomplish the development of key management schemes for the above three patterns.

Furthermore, for each pattern, key management approaches, saying key distribution, key transport, key agreement and key updating, would be developed in order to fulfil the whole process and functions of key management services. As mentioned before, the well-defined distributed CA scheme is the bridge in utilising the existing key management schemes into WMNs.

C. Security Analysis and Performance Analysis

The theoretical proof, security analysis and performance analysis for the proposed key management schemes will be done at this step. Two common tools can be used for the simulation at this stage, MatLab, which is a powerful tool in the numerical computing area and NS-2, which is popularly used in the routing and multi-cast protocols. First of all, the mathematical proof would be done to check the proposed schemes with aims of having general security features, saying confidentiality, integrity and availability, and coping well against the defined attack models to ensure the high level of security. Then by using Matlab, implementation would be carried out to measure the communication and computation costs with the aims of being low-computational. Scalability will be simulated to ensure the proposed key management schemes can cope well with the large extendable networks. At the end, advantages and disadvantages analysis would be provided to evaluate the developed key management model.

V. Conclusion and Future Work

With more and more applications coming out, the destination of this promising technology, saying WMNs, will be well-performed, secure, and wide-spread wireless connection. To support the quality of large-scale deployment, it is rewarding and important to address the critical key management issue for WMNs. This paper proposed a low-computational and scalable key management model for WMNs which aims to guarantee well-performed key management services and protection from potential attacks. Future work in this topic will include integrating routing with key management, and providing fault-tolerance and robustness for wireless mesh networks key management.

References

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey", Computer Networks and ISDN Systems, Vol.47, 2005, pp.445-487.

[2] I. F. Akyildiz, and X. Wang, "A Survey on Wireless Mesh Networks", IEEE Radio Communications, Vol.43, 2005, pp.s23-s30.

[3] M. Lee et al., "Emerging Standards for Wireless Mesh Technology", IEEE Wireless Communications, Vol.13 (2), 2006, pp.56-63.

[4] N.B. Salem, and J-P Hubaux, "Securing Wireless Mesh Networks", IEEE Wireless Communications, Vol.13, Issue2, 2006, pp.50-55.

[5] S. Han, E. Chang, L. Gao, T. Dillon, T., Taxonomy of Attacks on Wireless Sensor Networks, in the Proceedings of the 1st European Conference on Computer Network Defence (EC2ND), University of Glamorgan, UK, Springer Press, SpringerLink Date: December 2007. http://www.springerlink.com/content/h51q706064p6x30j/

[6] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks 1, 2003, pp. 293-315.

[7] Y. Yang, Y. Gu, X. Tan and L. Ma, "A New Wireless Mesh Networks Authentication Scheme Based on Threshold Method," he 9th International Conference for Young Computer Scientists (ICYCS 2008), 2008, pp. 2260-2265.

[8] F Buiati, R. Puttini, R. de Sousa, et al, "Authentication and auto-configuration for MANET nodes," LNCS, Springer, Berlin/Heidelberg, vol. 3207, 2004, pp. 41-52.

[9] N. Asokan and P. Ginzboorg, "Key Agreement in Ad Hoc Networks", Computer Communications, 2000, vol. 23, pp. 1627-1637.

[10] S. Yi and R. Kravets, "Composite Key Management for Ad Hoc Networks," in the Proceedings of the 1st Annual International Conference on Mobil and Ubiquitous Systems: Networking and Services (MobiQuitous'04), 2004, pp. 52-61.

[11] P Ning, R. Li, D. Liu, "Establishing pair-wise keys in distributed sensor networks", ACM Transactions on Information and System Security, Vol. 8 (1), 2005, pp. 41–77.

[12] F. Li, X. Xin and Y. Hu, "Key management in ad hoc networks using self-certified public key system", International Journal of Mobile Communications 2007, vol. 5(1), pp. 94-106.

[13] S Mittra, "Iolus: a framework for scalable secure multicasting," in Proceedings of ACM SIGCOMM'97, Canada, September, 1997, pp. 14-18.

[14] F Lee and S. Shieh, "Scalable and Lightweight Key Distribution for Secure Group Communications," International Journal of Network Management, 14:167-176, 2004.

[15] Y. Fu, J. He, R. Wang and G. Li, "A key-chain-based keying scheme for many-to-many secure group communication," ACM Transactions on Information and System Security (TISSEC), 2004, vol. 7(4), pp. 523 – 552.

[16] M S. Siddiqui, and C. S. Hong, "Security Issues in Wireless Mesh Networks", Proceedings of the International Conference on Multimedia and Ubiquitous Engineering (MUE'07). New York IEEE Press, 2007, pp.41−47.

[17] H. Mu and Y. Liu, "Mesh Based Multicast Key Management Scheme in Ad Hoc Networks," in Proceedings of IEEE ICSP 2006, pp. 1092-1192.

[18] Y. Desmedt, "Threshold cryptography," European Transactions on Telecommunication, vol. 5(4), 1994. pp. 449-457.

[19] J. P. Hubaux, L. Buttyan and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks", in Proc. Of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc2001), Lonf Beach, Oct. 2001.

[20] William Stallings, "Network Security Essentials", Third Edition, Prentice Hall, July 2006.

[21] K. Lu, Y. Qian and J. Hu, "A framework for distributed key management schemes in heterogeneous wireless sensor networks," 25thIEEE International Conference on Performance, Computing, and Communications (IPCCC), pp. 513-519, Arizona, USA, April 10-12, 2006.

[22] B. Wu, J. Chen, J. Wu and M. Cardei, "A Survey on Attacks and Countermeasures in Mobil Ad Hoc Networks", Chapter 12 in Wireless/Mobile Network Security, 2006, Springer.