International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 1 (2018) pp. 268-272

A Survey on Key management Schemes in Wireless Ad Hoc Networks

Pooja Singh
Research Scholar, Department of Computer Science and Applications,
Maharshi Dayanad University, Rohtak, Haryana, India
And Assistant Professor, Department of computer Science, Govt. college for Women, Faridabad, Haryana, India.
Orcid Id: 0000-0003-4134-9121

Dr. Nasib Singh Gill
Professor, Department of Computer Science and Applications,
Maharshi Dayanad University, Rohtak, Haryana, India.
Orcid Id: 0000-0002-8594-4320

Abstract

Ad hoc networks have undergone a decade long researches on several of its security issues. Limited battery power, computational complexity, low capacity, mobility of nodes and wireless medium makes the MANET more vulnerable to security attacks. The security management of such networks is quite different and complex than the wired networks. The nodes do the functionality of both as routers and as communication end points. These networks have no fixed infrastructure. In previous years, Cryptographic key management is being used in these networks for secure communication. In this paper, we present a survey of few key management schemes classified as symmetric, asymmetric and hybrid key schemes. A comparison of these schemes is performed on the basis of computational complexity, communication cost, Intrusion Tolerance, Robustness and scalability to determine the applicability area of these schemes.

Keywords: Survey, cryptographic key management, MANET, asymmetric key management, symmetric key management and hybrid key management.

INTRODUCTION

Mobile ad hoc networks are infrastructure less network. The wireless nodes perform the task of router as well as communication end points. Highly unsecured wireless medium imposed many security threats on Ad hoc networks. The applicability of such network ranges from military operations and emergency disaster relief to community networking and interaction.

The wireless medium exposed these networks to more security threats than their wired counterparts. Active and passive threats do more damage to ad hoc networks as compare to wired networks. Active attacks like unauthorized access, rogue access point, man in the middle attack, session hijack or denial of service as well as passive eavesdropping is inherently easy in these networks. All layers of protocol are penetrated by these attacks. For lower layers various techniques like spread-spectrum techniques, frequency hopping, interleaving or any such measures are being used for security and for higher layer cryptography is one of the best ways to place a check on these threats.

The key components of network security are confidentiality, authentication, integrity, availability, non-repudiation, access control, reliability, quality of information and check on malicious activity. The confidentiality, authentication, integrity, availability and non-repudiation can be assure through cryptographic key management known as hard security and access control, reliability and quality of information can be assure through trust management known as soft security.

Cryptography is one of the most explored and widely deployed ways of providing security services. A number of schemes relying on cryptography have been designed and are implemented on wireless ad hoc networks. Cryptographic keys act as proof of authenticity and its possession distinguish legitimate users from malicious one. The hard security components are shown in Fig 1 (a).

Hard security works as one time check where nodes either pass the security check or fail. In some situation nodes can behave as legitimate participants in the initial stage and therefore pass the traditional cryptographic security checks. However, they could turn out to be selfish players and report false measurements either with malicious intentions or due to faulty components.

Hard security scheme alone cannot help in detecting/preventing these kinds of behaviors as these behaviors are continuously changing. In addition reliability/trustworthiness of the information received from nodes, quality of information assessment and providing various levels of access control cannot be done effectively through hard security. The categories of threat which are purely due to node behaviors are classified as soft security [1], [2]. Soft security components are shown in Fig. 1 (b). Soft security threats can be most effectively handled using trust management systems [3], [4]. Trust management cannot be seen as a complete replacement for cryptography, rather a supplement to it. Cryptography key management and trust managements can work together to provide holistic security solutions in MANET.

Figure 1(a). Cryptography based hard security services.

Key management and trust management are two broad areas. In this paper, we have surveyed Key Management Schemes. The section 2 gives a brief overview of few key management schemes. The section 3 gives the comparison of these protocols and section 4 concludes our study.

OVERVIEW OF KEY MANAGEMENT SCHEMES

Previous studies have reported that the security management of an ad hoc network is a complex task. Various constrain like computational complexity, low capacity, dynamicity of nodes and risk prone environment makes the MANET more prone to security threats. Lack of infrastructure complicates the situation more. Despite of this, various key management system for the security of MANETs have been proposed in previous years.

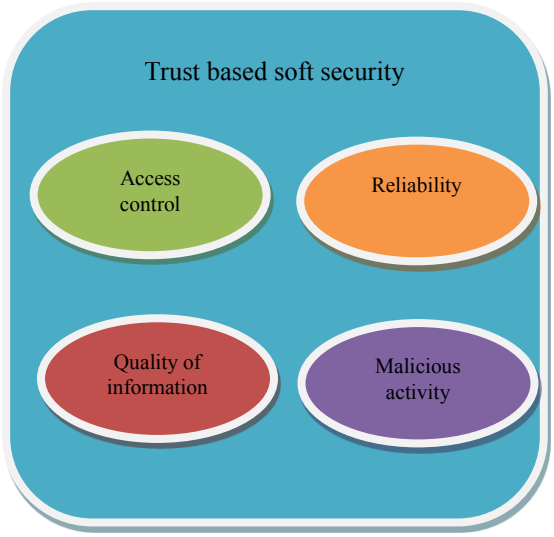

Figure 1(b). Trust based soft security services

In this paper, we broadly classify these schemes as symmetric, asymmetric and hybrid keys management schemes. The symmetric key management follows the private key infrastructure, which establishes common private keys used for symmetric cryptography. The asymmetric key management scheme considers the public key infrastructure, which provides a pair of keys i.e. public and private key used for asymmetric cryptography. The hybrid key management scheme uses both symmetric and asymmetric cryptographic keys in different phases of the scheme.

The symmetric key scheme is further categorize into pre distributed in which the secret key is shared before deployment by the trusted third party and the second is key agreement in which the users mutually agree on the common private key after deployment. Similarly, the asymmetric key management scheme is further categorize into Certificate based in which the third trusted party certified the authenticity of public key of users, the ID Based in which the user ID is used as the public key and the third certificate-less in which no third party is required while the user itself certified its public key. Our classification is illustrated in Fig. 2.

Symmetric Schemes

SKiMPy[5] is specially designed for MANETs. In this scheme the symmetric key is distributed by advertising it within one hop neighbours nodes through HELLO messages. The process repeat itself until the best key i.e. the key with lowest ID number and freshest timestamp is not get distributed among the group nodes. SKiMPy is a pre distributed symmetric key scheme. The initialization phase is complex and time consuming whereas after establishment of best key it works in very efficient manner.

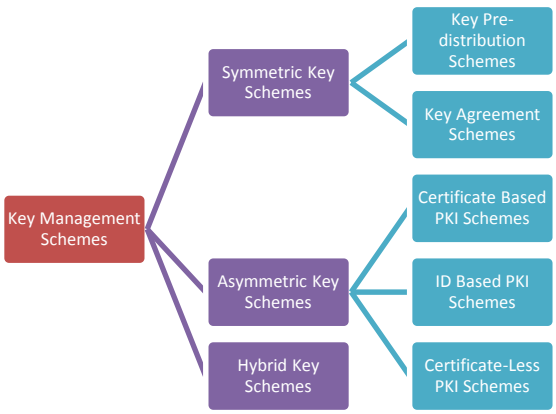

Figure 2: Classification of Key Management Schemes.

A security protocol for sensor network (SPINS) [6] is designed for wireless sensor networks. It assumes the pre distribution of pair wise secret key between the nodes and base station before deployment. For secure communication between nodes, the base station provides the common key, encrypted with their respective individual keys. SPINS uses SNEP for data security and µTESLA for authenticated broadcasting. The main drawback of this scheme is that it

presumes a secure routing protocol for communication between nodes and the base station.

Localized encryption and authentication protocol (LEAP) [7] is basically designed for static WSNs. In this scheme, a number of pre-installed keys are generated for different activities. Pre-distributed individual keys are used for communication between sensor nodes and base station. A different pre-shared group key is used for security of broadcast messages by base station. A pre-installed network wide key is used to generate pairwise keys between the nodes and its one-hope neighbours. This scheme implements μ-TESLA for route recovery and one-way key-chain authentication. The major drawback of this scheme is that it assumes that sink node is never compromised.

A key pre-distribution scheme for general and grid-group deployment of wireless sensor networks [8] is based on deterministic key pre-distribution. The entire deployment zone is broken into square regions. The square regions form the groups having two types of nodes viz. ordinary and special nodes. Special nodes have high computational power and energy than the ordinary nodes. Two different types of key pre-distribution are establish before deployment. A symmetric key pre-distribution scheme is used between the special and ordinary nodes for within group communication and a separate key pre-distribution scheme between the special nodes of groups. The sensor nodes within a group communicate directly while the nodes belonging to different square regions communicate through special nodes.

Asymmetric Schemes

In a conventional public key infrastructure (PKI), the central authority CA is responsible for all certification related activities like certificate generation, certificate revocation etc. However, it is difficult to deploy such a certificate-based PKI in MANETs for the lack of fixed infrastructure and other centralized services. Although a distribute CA's among a pre-selected set of nodes can be implemented to overcome the problem of single point of failure. A number of distributed PKI are discussed below:

Mobile Certificate Authority (MOCA) [9] is a certificate based asymmetric key scheme. It follows the principle of distributed PKI. The central authority (CA) distribute the share of its private key among a set of n server nodes, n<M, where M is the total nodes in the network. The threshold value for CA private key reconstruction is k ($1 <= k < n$) so that k server nodes cooperate to reveal the key. A server acting as combiner collects the partial keys and produces a valid signed certificate.

Secure and Efficient Key Management (SEKM) [10] is the extension of MOCA where all server nodes that have the partial share of CA private key connect to form a server group. Servers are specialized nodes that form a multicast group to provide the threshold share of private key for generation of certificate for service requesting nodes.

Khalili, Katz, and Arbaugh [11] proposed an ID based PKI with threshold cryptography. During the network formation, t nodes get the share of master private key over the total n nodes using t-over-n scheme. The nodes obtain their private key by combining the node ID with the t partial master private keys.

A composite identity and trust based model (CIDT) [12] is also an ID based PKI where the node private key is a composite key obtained by combining the node ID and the trust value of a node received from its threshold neighbors. The scheme assures the secrecy but at the cost of computational complexity.

Table 1. Comparison of key management schemes.

SCHEMES	APPROACH	COMMUNICATION COST		COMPUTATIONAL COMPLEXITY	INTRUSION TOLERANCE	ROBUSTNESS	SCALABILITY
		DURING INITIAL SETUP	AFTER INITIAL SETUP				
SKiMKy[5]	Symmetric	High	Low	Low	Limited	Fair	Fair
SPINS[6]	Symmetric	Medium	Low	Medium	Fair	Good	Poor
LEAP[7]	Symmetric	Medium	Low	Medium	Limited	Limited	Fair
[8]	Symmetric	high	Medium	Low	Fair	Fair	Limited
MOCA[9]	Asymmetric	High	Medium	High	Good	Good	Limited
SEKM[10]	Asymmetric	medium	Medium	High	Good	Good	Limited
[11]	Asymmetric	Medium	Medium	Medium	Fair	Good	Good
CIDT[12]	Asymmetric	High	Medium	High	Good	Fair	Limited
[13]	Asymmetric	Medium	low	Low	Good	Fair	Fair
[14]	Hybrid	High	Medium	Medium	Good	Fair	Good
[15]	hybrid	Medium	Medium	High	Fair	Fair	Good
[16]	Hybrid	Medium	Medium	Medium	Good	Good	fair

The certificate-less PKI is an intermediate between certificate based PKI and the ID based PKI eliminating the drawbacks of both. A Three Level Key Management Scheme [13] proposed by Xiong and Gong is based on certificate-less key schemes. It combines ID based cryptography with threshold secret sharing, elliptic curve cryptography (ECC) and bilinear computation. ECC provides small keys and with threshold secret sharing (t, n) the security level is increased. Bilinear pairing technique is applied to cryptography which provides confidentiality and authentication with less computational cost.

Hybrid Schemes

In hybrid schemes, both symmetric and asymmetric key schemes are applied at different phases of protocol.

Hybrid Key Management for Mobile Ad Hoc Network [14] proposed a hybrid key scheme, which combines the concepts of PKI's for MANET with trusted-third-party-based infrastructure. During the initial network setup, the PKI is used to generate a trust graph between the nodes. These trust paths are used to distribute the trust information and symmetric keys for secure communication.

Zone-Based Key Management [15] is also a hybrid approach. In this scheme, the network is divided into zones according to some predefined parameters. The nodes within a zone uses Diffie-Hellman scheme for symmetric key generation and threshold cryptography as PKI for inter-zone communications.

A fully distributed ECC-based key management for MANET [16] proposed a self-certified fully distributed ID-based system which is based on elliptic curve cryptography. All nodes are equally capable and the whole key generation center tasks are distributed among nodes using verifiable secret sharing. The secret values are transfer using ECC cryptosystem. An off-line initiator starts the network initialization phase by distributing the share of master pair of public and private key among nodes. A node may generate its private key by its witness value and the threshold share of master private key. In this scheme, the nodes have the ability of using both kinds of asymmetric or symmetric encryptions. The symmetric key can be generated between any two nodes in a non-interactive manner.

COMPARATIVE STUDY

The symmetric, asymmetric and hybrid key schemes serves different purposes. In this paper, we have chosen few protocols based on these approaches. A comparison of these protocols based on computational complexity, communication cost, intrusion tolerance, robustness and scalability is performed to broadly define the applicability areas of these schemes. The table 1 shows the comparative study of these protocols.

CONCLUSION

In this paper, we briefly describe few protocols on the basis of key schemes they follow. Symmetric key schemes show minimum computational complexity as compare to asymmetric and hybrid key schemes. Likewise, intrusion tolerance is high in asymmetric key schemes and hybrid key schemes have high scalability as compare to other schemes.

REFERENCE

[1] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision", Decision Support System, vol. 43, no. 2, pp. 618–644, 2007.

[2] B. Yu and M. P. Singh, "An evidential model of distributed reputation management", In Proc. First International Joint Conference on Autonomous Agents and Multiagent Systems, pp. 294–301, 2002.

[3] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," Proc. IEEE, vol. 98, no. 10, pp. 1752–1754, Oct. 2010.

[4] M. Carbone, M. Nielsen and V. Sassone, "A formal model for trust in dynamic networks," in In Proc. International conference on software engineering and formal methods, S4M03, pp. 54–63, 2003.

[5] M. Puzar et al., "SKiMPy: A Simple Key Management Protocol for MANETs in Emergency and Rescue Operations," Proc. ESAS '05, 2005.

[6] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, no. 5, Sept. 2002, pp.521–34.

[7] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," Proc. CSS '03, 2003.

[8] Samiran Bag and Bimal Roy, "A new key predistribution scheme for general and grid-group deployment of wireless sensor networks", EURASIP Journal on Wireless Communications and Networking2013, open access.

[9] S.Yi, and R. Kravets, "MOCA: MObile Certificate Authority for Wireless Ad Hoc Networks", Report No. UIUCDCS-R-2004-2502, UILU-ENG-2004-1805, University of Illinois at Urbana-Champaign, 2002.

[10] B. Wu et al., "Secure and Efficient Key Management in Mobile Ad Hoc Networks", Proc. IPDPS'05, 2005.

[11] A. Khalili, J. Katz, and W. A. Arbaugh, "Towards Secure Key Distribution in Truly Ad-Hoc Networks", Proc. IEEE Workshop. Security and Assurance in Ad hoc Networks, 2003.

[12] P. Khatri, "Using identity and trust with key management for achieving security in Ad hoc Networks", Proc. IACC, IEEE International, 2014.

[13] W. A. Xiong and Y. H. Gong, "Secure and highly efficient three level key management scheme for MANET", in WSEAS Transactions on Computers, Vol. 10, No. 1, 2011.

[14] D.S. Sanchez, H. Baldus, "Hybrid Key Management for Mobile Ad Hoc Networks", In: Al Agha K., Guérin Lassous I., Pujolle G. (eds) Challenges in Ad Hoc Networking. IFIP International Federation for Information Processing, volume 197. Springer, Boston, MA.

[15] T. Khdour and A. Aref, "A Hybrid Schema Zone-Based Key Management for MANETS", Theoretical and Applied Information Technology, volume 35, No. 2, 2012.
[16] M. Gharib et al., "Fully distributed ECC-based key Management mobile ad hoc networks", Internal journal of computer and telecommunications, volume 113, issue C, pages 269-283, February 2017.