Distributed Key Management Scheme for Mobile Ad-Hoc Network-A Survey

N. Vimala[1] Dr. R. Balasubramaniam[2]

GJCST Computing Classification
E.3, C.2.1, C.2.2

***Abstract*-Ensuring security in Mobile Ad-hoc Network is a challenging issue. Mobile ad-hoc networks (MANET) are networks designed to operate in more volatile and rapidly changing environment. Establishing MANET security is entirely different from the traditional methods of providing network security. The two main approaches that are widely used in securing MANET are proactive and reactive. The first attempts to prevent security threats through various cryptographic key generation techniques. One among the various cryptographic techniques is distributed key management system for MANET security. This paper discusses various cryptographic techniques determined by researchers to provide MANET security. The efficient key distribution scheme for secure communication is essential to ensure network security. In addition, this paper discusses various key management schemes for secure wireless sensor network communication.**

Keywords: Cryptographic key generation, Distributed Key, Mobile Ad-hoc network (MANET), Network Security, Proactive, Reactive.

I. Introduction

Network Security remains a major issue for connected wireless communication. The most advanced cryptographic technique in providing network security for wireless communication is Key management Schemes. According to the key management scheme, the cryptographic key should only exist in one of the following three states: pending, active, or pro-active [1]. The keys should be applied with a number of key state transition operations to transit the key between the three states. Such key transition operations mentioned in [1] are key: generation, activation, deactivation, reactivation, and destruction. Together these states, and the circumstances under which a state transition operation is triggered, help to define a key management life cycle. The network security of wireless communication can be ensured by encrypting and authenticating the messages. There are many issues that lament to implement security in wireless sensor networks because of the nature of wireless communication, resource limitation of sensor nodes, size and network density, unknown topology prior to deployment, and high risk of physical attacks to unattended sensors [2]. Obviously, this secure communication depends very much on the use of strong and efficient key distribution mechanisms in uncontrolled environments. Using a single shared key for a whole network may raise some issues. Hence, it is necessary to introduce pair-wise key, enabling secure communication using cryptographic technique.

This necessitates finding an effective way of distributing keys and keying materials to sensor nodes prior to deployment. The networks such as MANET are frequently viewed as a key communication technology enabler for network-centric warfare and disaster relief operations. As the technology matures, MANETs are increasingly reaching many other applications in areas like intelligent transportation system and fault tolerant mobile sensor grids [3].

The MANET is a network consisting of collection of nodes capable of communicating with one another without the assistance of network infrastructure. The five main security services for MANET are authentication, confidentiality, integrity, non-repudiation, and availability [4]. The main advantage of using MANET is that it can operate in isolation or in coordination with the wired infrastructure, often through a gateway node participating in both networks for traffic relay. The main application area includes battlefield applications, rescue work, as well as civilian applications like an outdoor meeting or an Ad-hoc classroom.

II. Background Study

The number of applications that utilizes the Ad-Hoc Networks has increased gradually over the years. Hence, it is necessary to consider the security issue of Ad-Hoc Networks like MANET. Numbers of research have contributed many security systems to authenticate the MANETs. This section of the survey mainly focuses on earlier contributed research works in the field of security to MANETs through Cryptographic techniques like Distributed Key generation, Pair-wise key generation etc.

Laurent Eschenauer et al. in [5] described a key management scheme that ensures the authenticity of distributed network. Distributed Sensor Networks (DSNs) are Ad-hoc mobile networks that include sensor nodes with limited computation and communication capabilities. The operational and security requirements of DSNs can be satisfied by a key management scheme presented in their work. Moreover, their scheme also includes selective distribution and revocation of keys to sensor nodes as well as node re-keying without substantial computation and communication capabilities. Table1 summarizes the comparison of various algorithms discussed on literature based on five major security services of MANET.

About[1]Senior Lecturer, Department of Computer Science, CMS College of Science and Commerce, Coimbatore, India.
About[2]Dean Academic Affairs, PPG Institute of Technology, Coimbatore, India.

Ricardo Staciarini Puttini et al. in their work in [6] describe, a new authentication service for securing MANET routing protocols. An authentication service is considered as a basic preventive protection for the routing protocol. Table2 summarizes various MANET routing protocols and MANET Authentication Extension (MAE) requirements for various protocols. Table2 particularly makes note of routing protocols in MANET, since routing protocols plays a critical role in ensuring the network security of any wireless sensor networks.

A new efficient Hierarchical Binary Tree (HBT) Model to form Ad-hoc group was proposed by Erdem in [7]. This model employs a new key distribution scheme to bring an alien device to group and to exchange a secret key at that moment. The binary tree model proposed in this work is an Efficient Distributed Key Management (EDKM) model. The main attributes of EDKM is that it is self-organizing, and can be deployed incrementally in the network. On comparison of EDKM with other HBT scheme it is proposed that EDKM provides entire backward and forward security in case of modification in the membership and moreover it does not increase the processing or storage requirements. The model proposed in their paper is based on the one-way hash function and the secret key cryptography. Hence, EDKM seems to be efficient and practical for MANETs.

A Security scheme was put forth by Sugata Sanyal et al. in [8], for distributed Denial of Service (DoS) in MANETs. Because of inherent limitations of the routing protocols employed in MANETs various kinds of DoS attacks are possible on MANET. In [8] Sugata Sanyal et al., suggest a proactive scheme that can prevent a specific kind of DoS attack and identify the misbehaving node. The performance of this proposed algorithm in a series of simulations revealed that the proposed scheme provides a much better solution than the existing approaches with no extra overhead. The proposed scheme shifts the responsibility to monitor the parameters of the compromised node on the node's neighbor, thus ensuring the compliance of restriction. This eliminates the problems due to flooding of Route REQuests (RREQs) from the compromised node.

Aldar Chan and Edward Rogers in their work [9], describe a distributed symmetric key management for MANETs. Existing key management schemes are too inefficient, not functional on an arbitrary network or unknown network topology, or not tolerant to a changing network topology or link failures. Hence they are not suitable for Ad-hoc networks. Key Pre-distribution Schemes (KPS) are the only practical option for scenarios where the network topology is not known prior to deployment. But however this scheme relies on Trusted Third Parties (TTP). The approach introduces Distributed Key Pre-distribution Scheme (DKPS) and constructs the first DKPS prototype to realize fully distributed and self organized key pre-distribution without relying on any infrastructure support. This approach of implementing DKPS eliminates the drawbacks in the earlier methods.

Gligor proposed an approach in [10], for security enhancement in Ad-Hoc Networks. A common characteristic of all Ad-hoc networks is that of emergent properties. Spontaneously, emergent properties are features that cannot be provided by individual network nodes themselves but instead result from interaction and collaboration among network nodes. The emergent properties and their security characteristics proposed in this approach are different from traditional network properties established via protocol interactions in several fundamental ways. The distinguishing characteristics of emergent properties and their security implications are determined in this approach. They present several examples of desirable and undesirable emergent properties in different types of Ad-hoc networks.

Katrin Hoeper and Guang Gong proposed a method for bootstrapping security in MANETs in [11]. Two full functional IDentity (ID) based Authentication and Key Exchange (IDAKE) schemes are proposed in their work. Pre-shared secret keys from pairings and efficient key management are some special features of Identity-Based Cryptographic (IBC) scheme. Moreover IBC scheme can be employed to design MANET-IDAKE scheme which meets the special constraints and requirements of MANETs. These merits are utilized in this method of bootstrapping the security of MANETs. The method mentioned in their work uses a TTP which initializes all devices before they join the network and a fully self-organized MANET-IDAKE scheme that does not require any central TTP. They also present an efficient IDAKE scheme that can be implemented for various types of MANET applications. Their approach enables the use of authentication, key exchange, and other security protocols in real world applications.

A novel approach to ensure the security of MANETs was proposed by Fagen Li et al. in [12]. In this novel approach, they proposed a distributed key management approach by using the self-certified public key system and threshold secret sharing schemes. The use of self-certified public key system in this approach has the advantages such as, the storage space and the communication overheads can be reduced in that the certificate is unnecessary, the computational costs can be decreased, since it requires no public key verification, there is no key escrow problem since the Certificate Authority (CA) does not know the user's private keys. This approach is much better and efficient when comparing it with the certificate-based public key system and IDentity-based (ID-based) public key system.

Mansoor Alicherry et al. present an approach in [13], a novel distributed security policy enforcement architecture that is specially designed for MANETs. The capabilities of network communication are harnessed and extended on implementation this approach. This proposed approach is especially suitable for mobile and heterogeneous communications environments. This method however obliges communication restrictions between the MANET nodes by enforcing hop-by-hop policies in a distributed manner. The compromised nodes are allowed to access only

the authorized services using deny-by-default principle. The impact on throughput for different network topologies and classes of traffic was not discussed in this paper. This well as limits the exposure of MANET to compromised and malicious nodes.

III. Distributed Key Management Scheme

Cryptographic Key generation and other techniques are established to encrypt and authenticate the messages that are transferred through various wireless networks. The applications that utilize the wireless infrastructure to transfer the message have been increased over past years. Therefore, approach is capable of protecting both end host resources and the network bandwidth from denial of service attacks, as

it is necessary to concern on the security issues of wireless networks. The widely used wireless network is MANET. Several Cryptographic techniques have been proposed to generate key that can authenticate the MANET to ensure network security. The security of this network completely depends on the mode of key utilized to a particular network. Using a single shared key [14] for the entire network that runs more number of applications is not secure. Therefore, pair-wise key generation using some of the well-known cryptographic techniques can be used to authenticate the network from unauthorized user.

TABLE 1 Comparison of various Algorithms based on the security services of MANET

H, M and L denotes High, Medium and Low respectively.

Algorithm	Authentication	Confidentiality	Integrity	Non-repudiation	Availability
Laurent Eschenauer et al.	H	M	H	H	L
Erdem	H	M	M	L	H
Sugata Sanyal et al.	M	H	L	H	H
Aldar Chan and Edward Rogers	H	H	H	L	M
Fagen Li et al.	H	H	M	M	L

The utilization of the traditional pair-wise key such as public key is not suitable for sensor nodes due to resource constraints. In such a case, the main challenge is to find an efficient way of distributing keys and keying materials to sensor nodes prior to deployment. In the last few years, different pair-wise key distribution schemes have been developed for peer-to-peer wireless sensor networks [15]–[17] and hierarchical wireless sensor networks [18], [19].
The problem of how resources can effectively be used to distribute session keys is referred to as the group key distribution problem. The group key distribution problem has been studied extensively in the larger context of key management for secure group communications [20] and [21], mainly on balancing the storage complexity and the communication complexity.

TABLE 2 Key Features of MANET routing protocol and MAE requirements for each protocol. DS is the Digital Signature and HC denote Hash Chain

Routing Protocol	Routing Discovery	Routing Algorithm	Relevant Message	Authorized objects
DSR	On-Demand	Source routing	RREQ	DS+HC
			RREP	DS
AODV	On-Demand	Distance vector	RREQ	DS+HC
			RREP	DS+HC
			RERR	DS
			RREP-ACK	DS
OLSR	Proactive	Link state	Hello, TC	DS
TBRPF	Proactive	Link state	Hello, TU	DS

where DSR is Dynamic Source Routing protocol, AODV is Ad hoc On-demand Distance Vector routing protocol, OLSR is Optimized Link State Routing protocol, and TBRPF is Topology dissemination based on Reverse-Path Forwarding protocol. In the similar way RREQ represent Route Request, RREP denote Route Reply and RRER stand for Route Error, TC represents Topology Control and TU denotes Topology Update.

There exists a distributed approach, in which members contribute to the generation of group key by sending the hash of a random number during initialization phase within the cluster [22]. They regenerate the group key themselves by obtaining the rekeying message from one of its members during rekeying phase or whenever membership changes occur. Symmetric key is used for communication between the
members of a cluster and asymmetric key cryptography for distributing the rekeying messages to the members of the cluster.

IV. Future Enhancements

Network security and authentication prove to be a challenging issue in most of the real time application that relies on wireless communication. Therefore, providing security and authentication is important as much as providing network connection to the user. This is the major concern for most of the network service providers today and hence data encryption and key distribution scheme are very critical in enhancing the security. Future enhancements mainly focus on improving network security using cryptographic techniques in MANETs. Future work may concentrate on any of the following areas. Developing a new distributed key management scheme mainly focusing on the heterogeneity features of MANET. Employing encrypting algorithms that reduces the computational complexity of each member in a group. This approach develops an effective distributed key that resolves the problems in group

communication. The merits of a distributed key management system should be utilized effectively to eliminate the necessity of TTP. To eliminate TTP the key management system must implement a key generation function by sending partial initialization parameters from several nodes during the initialization phase. Another approach of designing distributed key for ensuring network security in MANET is providing an IDentity (ID)-based cryptography with threshold secret sharing. In this approach, the distributed scheme dynamically selects nodes with master key shares to provide the private key generation service. Node security and Energy states in the process of selecting best nodes to construct a private key generator (PKG) are the primary attributes to be noted in the above approach. Future work relies on one of the approach that best enhances the network security and user authentication in MANET.

V. CONCLUSION

This paper generally discusses on various key management schemes proposed in literature. These distributed key generation techniques are based on cryptographic techniques. MANET's security is the challenging issue in providing authentication. Single shared key for many applications may raise problems in ensuring authentication. The approach of employing distributed key scheme for MANET ensures the network security. This paper discusses on different cryptographic key generation techniques that are proposed in literature. Some of the techniques described are Symmetric Key Cryptography, Digital Certificates, and Threshold Cryptography. The future work utilizes one of the best cryptographic techniques for generation of distribution

key that improves the network security in MANETs and in other wireless sensor networks.

VI. Reference

1) ISO/IEC 11770-1:1996. Information Technology-Security Techniques-Key Management –Part1-Framework, 1996
2) S. A. Camtepe, and B. Yener, "Key Distribution Mechanisms for Wireless sensor networks: a survey," Department of Computer Science, Rensselaer Polytechnic Institute, Technical Report TR-05-07, March 23, 2005.
3) Marco Carvalho, "Security in Mobile Ad-hoc Networks," IEEE Transactions on Security and Privacy, vol. 6, no. 2, March/April 2008, pp. 72-75.
4) Shuyao Yu, Youkon Zhang, Chuck Song, and Kai Chen, "Security Architecture for Mobile Ad-Hoc Network," 2004.
5) Laurent Eschenauer and Virgil D. Gligor, "A Key Management Scheme for distributed sensor networks," Proceedings of ninth ACM Conference on Computer and Communications Security, 2002, pp. 41-47.
6) Ricardo Staciarini Puttini, Ludovic Me, and Rafael Timoteo de Sousa, "Certification and Authentication services for Securing MANET Routing Protocols," The Proceedings of fifth IFIP-TC 6 International Conference, 2003, pp. 278-281.
7) O. M. Erdem, "EDKM: efficient distributed key management for mobile ad hoc networks," Proc. 9th IEEE Symposium on Computers and Communication, vol. 1, July 2004, pp. 325-330.
8) Sugata Sanyal, Ajith Abraham, Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia, and Nirali Mody, "Security Scheme for Distributed DoS in Mobile Ad Hoc Networks," May 2004.
9) Aldar C-F. Chan and Edward S. Rogers, "Distributed Symmetric Key Management for Mobile Ad Hoc Networks," IEEE INFOCOM 2004, vol. 4, March 2004, pp. 2414-2424.
10) Virgil D. Gligor, "Emergent properties in ad-hoc networks: a security perspective," Workshop on Wireless Security, Proc. Of 4th ACM Workshop on Wireless Security, 2005, p. 55.
11) Katrin Hoeper and Guang Gong, "Bootstrapping Security in Mobile Ad hoc Networks using Identity Based Schemes with key Revocation," 2006.
12) Fagen Li, Xiangjun Xin, and Yupu Hu, "Key Management in Ad hoc Networks using self-certified public key system," International Journal of Mobile Communication vol. 5, Issue 1, 2007, pp. 94-106.
13) Mansoor Alicherry, Angelos D. Keromytis, and Angelos Stavrou, "Deny-by-Default Distributed Security Policy Enforcement in Mobile Ad-Hoc Networks," 2009.
14) Lihao Xu, and Cheng Huang, "Computation-Efficient Multicast Key Distribution," IEEE Transactions on Parallel and Distributed system, vol. 19, no. 5, May 2008, pp. 577-587.
15) W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in Proc. 10th ACM Conference on Computer and Communications Security, Oct. 2003, pp. 42-51.
16) W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in Proc. IEEE INFOCOM, vol. 1, March 2004, pp. 586–597.
17) Y. Zhou, Y. Zhang, and Y. Fang, "LLK: a link-layer key establishment scheme for wireless sensor networks," in Proc. IEEE WCNC, vol. 4, March 2005, pp. 1921–1926.
18) Y. W. Law, R. Corin, S. Etalle, and P. H. Hartel, "A formally verified decentralized key management for wireless sensor networks," in Personal Wireless Communications, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, Sept. 2003, vol. 2775/2003, pp. 27–39.
19) S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," in Proc. CCS '03: 10th ACM conference on Computer and communications security. NewYork: ACM Press, 2003, pp. 62–72.
20) S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication," ACM Computing Surveys, vol. 35, no. 3, 2003, pp. 309-329.
21) O. Rodeh, K. Birman, and D. Dolev, "The Architecture and Performance of Security Protocols in the Ensemble Group Communication System," ACM Trans. Information and System Security, vol. 4, no. 3, Aug. 2001, pp. 289-319.
22) A. Renuka and Dr. K. C. Shet, "Hierarchical Approach for Key Management in Mobile Ad hoc Network," International Journal of Computer Science and Information Security, vol. 5, no. 1, 2009, pp. 87-95.