International Journal of Applied Environmental Sciences
ISSN 0973-6077 Volume 13, Number 2 (2018), pp. 161-169

http://www.ripublication.com

Analysis of Key Management Schemes in MANET

Nitika Singhi

Dept. of Computer Science and Engineering
RKDF University, Bhopal, India

Ravi Singh Pippal*

Dept. of Computer Science and Engineering
Vedica Institute of Technology, RKDF University, Bhopal, India

Abstract

Wireless Network includes a larger advantage in today's communication application like environmental, traffic, military and health observation. To realize these applications it's necessary to possess a reliable routing protocol. The self-organizing nature of MANETs makes them suitable for many applications and hence, considerable effort has been put into securing this type of networks. Secure communication in a network is determined by the reliability of the key management scheme, which is responsible for generating, distributing and maintaining encryption/decryption keys among the nodes. In this paper various key management schemes for MANETs are discussed. This research work proposes a novel secure Identity-Based Key Management protocol making use of cryptographic and Information Theoretic Security.

Index Terms: MANET, routing protocols, key management, symmetric key, asymmetric key, group key management.

INTRODUCTION

The recent evolution of ad hoc wireless technologies has allowed mobile ad hoc networks (MANETs) to construct spontaneous connections among mobile devices with none infrastructure [1, 2]. Moreover, with the emergence of sensor-enabled smart mobile devices, MANETs became a vital part within the infrastructure of smart city and internet of Things (IoT) situations as a result of individuals with smart devices will freely and dynamically kind a self-configuring MANET to send, receive and share data in an exceedingly restricted zone (as shown in figure 1.2) [3].

In an exceedingly such a smart environment, MANETs, Wireless sensor Networks (WSNs) and Wireless Mesh Networks (WMNs) represent key technologies providing many IoT applications and services to users. moreover MANETs have found a range of applications in health care, battlefield communications, disaster recovery, crisis management services education organizations, ad hoc cooperative computing, social activities and conference halls.

A MANET is a collection of autonomous nodes or terminals that communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner [4]. Due to the limited transmission range of each mobile node, it may be necessary for one mobile node to enlist the aid of other nodes in forwarding a package to its destination. Therefore, in such environment, every node in the network plays the role of a router by being able to determine the paths of transmitting packets to their destinations. Figure 1 illustrates an example of a MANET which contains two laptops, two PDAs and two digital cameras. Since node D is outside node A's transmission range, the data from A to D must be retransmitted by nodes B and C.

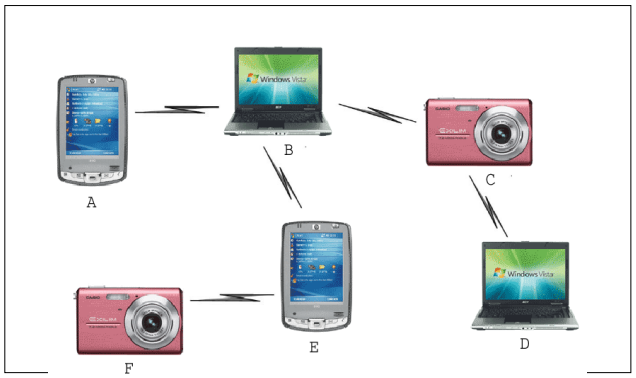

Figure 1. Mobile Adhoc Network

Despite the attractive applications of MANETs, these systems still face several challenges and constraints that need more investigation before the widespread commercial deployment of MANETs [5]. The most constraints that may have an effect on Manet design are as follows: (1) the limited energy and lifetime of the battery, quality of service (QoS),infrastructure-less and autonomous configuration, dynamic network topologies, the mobility of nodes, wireless link reliability, variation in node capabilities, multi-hop routing scalability, multicast support and security threats [6].

As it is hard to establish a secure communication by key creation among mobile nodes in a MANET, a malicious mobile node can use a counterfeit identity to make feigned trust relations with other nodes, and then attack the MANET. Such nodes would drop all the data packets received that they need to forward during whole simulation [7]. A reliable routing protocol for Mobile Ad hoc Networks (MANETs) keeps the energy consumption as low as possible [8]. On the contrary, in MANET with cellular network integration, it is viable to authenticate mobile nodes before any actual key generation. In order to establish trust relationship between any two mobile nodes in

the cellular-based MANET, it is beneficial to take advantage of cellular infrastructure so as to enable a trustable and secure key generation before communication.

ROUTING PROTOCOLS

Routing is the act of moving information from a source to a destination in an internetwork. During this process, at least one intermediate node within the internetwork is encountered.

The routing concept basically involves, two activities: firstly, determining optimal routing paths and secondly, transferring the information groups (called packets) through an internet work [9]. The later concept is called as packet switching which is straight forward, and the path determination could be very complex.

Routing protocols are classified into different categories depending on their properties.

- Centralized vs. Distributed
- Static vs. Adaptive
- Reactive vs. proactive

In centralized algorithms, all route choices are made at central node, while in distributed algorithms, the computation of the routes is shared among the network nodes another classification of routing protocols relates to whether they change routes in response to the traffic input patterns. In static algorithms, the route used by the source destination pairs is fixed regardless of traffic conditions [10-12]. It can only change in response to a node or link failure. This type of algorithm cannot achieve high throughput under a broad variety of traffic input patterns. Most major packet networks uses some form of adaptive routing where the routes used to route between source-destination pairs may change in response to congestion [13]. Proactive protocols continuously evaluate the routes within the network, so that when a packet needs to be forwarded the route is already known and can be immediately used. Reactive protocols invoke a route determination procedure on demand only. There is need a new routing protocol for communication network which include adaptive, scalable, and secure aspects in it. Some of the cluster based routing protocols are analyzed below in Table I.

SECURITY GOALS IN MANET

When dealing with security in communication network, one is faced with the problem of achieving some or all of the following goals:

- Availability: This means that network assets are available to authorized parties when needed and network should ensure the survivability of network services despite denial-of-service (DOS) attacks, which could be launched at any layer of communication network [4].

Table 1. Analysis of Major Routing Protocols

Protocols	**Strength**	**Drawbacks**
Leach Protocol	Dynamic cluster head selection.	Fixed number of clusters and random cluster head selection.
Hybrid Energy Efficient Distributed Protocol (HEED)	Dynamic cluster head selection.	Fixed number of clusters and inefficient processing time.
Hierarchical, energy efficient routing protocol (HEERP)	It is an energy efficient protocol. It performs well in the dense network.	Sensors are used for data aggregation process. Efficiency is low in case of less dense network.
Hierarchical geographic clustering protocol (HGCP)	It uses virtual grids. Actor acts as a cluster head.	It assumed that both the sensors and actors are static. Small grid area.
LEACH-B	Effectively balance the network load and improve the utilization of energy, so as to extend the network life cycle.	Data fusion issue on cluster head node. Only focuses on residual energy of cluster head.

- Authenticity: In communication network authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). Data authentication allows the receiver to verify that the data was really sent by the claimed sender. Stronger levels of authenticity (e.g. explicit key authentication) are provided by some key establishment protocols [5].
- Confidentiality: A confidential message is resistant to revealing its meaning to an eavesdropper. Even routing information in WAN needs to remain confidential, since it may be used to in a DOS attack. The standard solution to keep sensitive data secret is to encrypt the data with a secret key that only the intended receivers possess, hence achieving confidentiality [6].
- Data integrity: Integrity measures ensure that the received data is not altered in transit by an adversary. The integrity service can be provided using cryptographic hash functions along with some form of encryption. When dealing with network security, the integrity service is often provided implicitly by the authentication service [13].
- Scalability and self-organization: In contrast to general networks that do not put scalability in the first priority, WAN cannot utilize a keying scheme that has poor scaling properties (either in terms of energy cost or latency) for establishing and maintaining a key for the WAN as a whole or for some large subset of nodes [14]. As a consequence, the WAN nodes must be able to self-organize and select the appropriate keying mechanism for the situation.

Wireless communication networks is challenging because of the unpredictable behaviour of the medium and the proactive effect of interference. Compared to the wired networks the degree of variability of the state of wireless networks is quite high. Also the performance of the network, in terms of delay and throughput, is highly dependent upon the state of the network. it is important that the layers coordinate and adapt to the change in network state. To deal with the dynamic variations in networking and computing resources gracefully, both the mobile computing environment and the applications also need to adapt their behaviour depending on the available resources [15].

Recent advances in the portability, power, and capabilities of wireless devices and applications have resulted in the proliferation and increased popularity of these devices. As the number of users continues to grow, wireless routing protocols will be required to scale to increasingly larger populations of nodes [17]. Networking scenarios can require the formation of networks on the order of tens to hundreds of nodes, while many military applications can involve thousands to tens of thousands of nodes. Furthermore, as the deployment of wireless communication networks becomes more widespread, new applications may encourage the formation of large communication networks. The main objective is to design a secure routing protocol for a large wireless sensor network in which the nodes as well as the base station are mobile. The protocol should be secure, energy efficient and scalable with respect to all existing algorithms.

KEY MANAGEMENT IN MANET

Cryptography reduces the confidentiality and integrity of a message to the confidentiality and integrity of a key. When using symmetric cryptography, the parties involved have to negotiate a secret key [18]. A good key establishment scheme provides entity authentication (all parties know the identity of the other parties with whom they are establishing a key), key authentication (all parties are assured that no unauthorized parties could have obtained the secret key), and key confirmation (all parties are assured that all other parties have knowledge of the secret key). Key establishment schemes can be divided into three major categories: (1) key pre-distribution schemes, (2) schemes using a trusted third party, and (3) schemes based on public key cryptography.

Key pre-distribution schemes have received a lot of attention in the setting of ad ho c networks [19]. They are very suited for ad ho c networks as they do not require a trusted third party to b e available at all times, and are very efficient. Schemes using trusted third parties are not really suited for ad ho c networks as they assume that the trusted third party is available to anybody. The disadvantage of public key based schemes is that they require certificates and those public key algorithms are in-efficient.

Symmetric key algorithms are computationally very efficient and are therefore of high interest for MANETs. However, as previously stated, the major challenge in using

symmetric key cryptography in MANETs is the secure exchange and efficient storage of symmetric keys. Any data exchange over a wireless channel is initially unauthentic, making it almost impossible to exchange a key without a back-link or pre-configuration [20].

In asymmetric cryptography, two keys are required for each nodes, is used by the transmitting node for encryption and his secret private key is used by the receiving node for decryption. Asymmetric key cryptography requires a fewer number of keys compared to symmetric key cryptography. More precisely, the number of keys is K=2*n, for n communicating nodes [21]. In Hybrid Key Management Schemes, hybrid or composite keys are a combination of two or more symmetric, asymmetric, or symmetric and asymmetric keys. These schemes need to set two keys instead of one, which can present a problem for MANETs.

In Cluster Based Composite Key Management the network is divided into clusters and a cluster head, which is the node with the maximum trust ability and is selected by network administrator for each cluster. Moreover, k nodes with high trust value are selected in each cluster as Public Key Generation (PKG) nodes. Each node is assigned an ID by a CA prior to joining the network and has a self-assigned public key. The mobile agent collects node information and provides certificate revocation. A new node joining the network registers its information in the cluster head and the PKG nodes generate its private key shares. The shares are combined by the cluster head. The public key of the cluster head is available to all the nodes in the cluster. The system uses a low frequency for communication between cluster members and a high frequency for communication between cluster heads [20].

Zone-Based Key Management scheme is based on the Zone Routing Protocol [21]. For each node, a zone is defined as all the nodes that are in the circle with centre the considered node and radius equal to a predefined value. Each node uses symmetric key inside its zone and asymmetric key for inter-zone communications. The Diffie-Hellman scheme is used for symmetric key generation and threshold cryptography is used for certificate generation [21].

In Group Key Management Schemes, group key is a unique key that is assigned to a group of nodes. In order to establish a group key, the group needs to create and distribute the key to all members [21].

PROPOSED MODEL

Following points are considered as pre-assumptions for designing secure data transmission in cluster based WSN:

1. The nodes in the network system are mobile with available onboard memory, computing capability, communication bandwidth, and available battery power.
2. Battery may be renewable or not renewable.
3. The sensor nodes are not reliable and they need to be authenticated.

4. The attackers may eavesdrop the radio transmissions. The attackers can also deploy some identical nodes to mislead legitimate nodes.

For proposed algorithm, 3 different types of keys are generated i.e. Initial secret key (ISK), sensor-cluster-gateway key (SCGK) and gateway-base key (GBK) in proposed model.

Every sensor node has an Initial Key (initially loaded into memory of each sensor node) along with their ID. Each sensor node uses the ISK and ID initially to authenticate itself with base station.

SCGK key is used for the communication inside a cluster among cluster head and sensor nodes. SCGK is generated by base station along with cluster ID and send to all cluster heads. This key is then distributed among all nodes using ISK.

GBK is used to communicate between gateway node and base station.

Steps of Proposed algorithm:

1. The authentication phase consists of following steps:

   Each node send authentication request to base station. The request message contains ID encrypted with ISK

   Base station then decrypt ID using ISK of node

   If ID matched then authenticated and base station assigns SBK to each node.

2. After deployment of the sensor nodes in the field, the base station divides the sensor field into some clusters.

3. In each cluster assign one Cluster Head Nodes (CH). All Sensor Nodes in a cluster communicate with the Cluster Head Node and finally, the Gateway Nodes are responsible for transmitting data to the base station (as depicted in below figure).

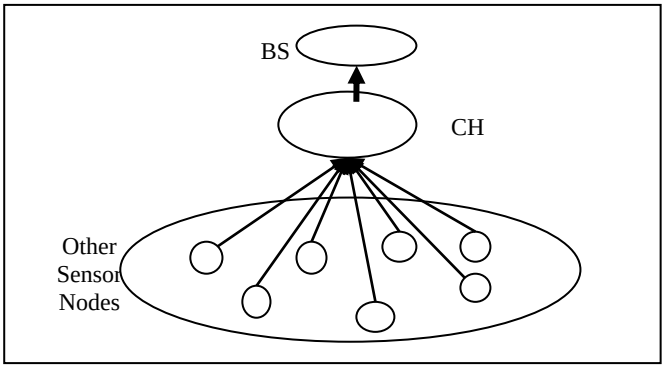

Figure 2. Proposed Model

If any Sensor Nodes sense data from the environment then it forwards the data to its respective Cluster Head node. Further the Cluster Head node forwards the data to the base station.

CONCLUSION

In this paper, a comparative analysis of wireless sensor network (WSN) routing protocols. The protocols are divided into two categories i.e., cluster based and non-cluster based. It is observed that among all routing protocols cluster based protocols are hierarchical, reliable, and energy efficient routing protocol that outperforms others. Hence, it can inferred that cluster based protocols are more popular among the research community of WSN. One of the key issues in WSN is security issue in which authentication is a fundamental issue for a reliable network service. The nodes must be able to distinguish trustworthy from untrustworthy nodes in the neighbor discovery process, and they must be able to verify both routing message origin and integrity. Any cryptographic authentication scheme requires proper key management. That is, mutual authentication of the involved parties is required during the key setup. This paper includes a comprehensive survey of key management methods proposed for Adhoc networks. The applicability of identity-based public key schemes for protection of Adhoc routing information is also discussed. Finally, a novel secure algorithm is proposed which is based on Identity-Based Key Management protocol that may be used to enhance security level in MANET.

REFERENCES

[1] National Institute of Standards and Technology (NIST). Wireless Ad Hoc Network Projects. Available at http://www.antd.nist.gov/wahn_home.shtml.

[2] C. E. Perkins, Ad Hoc Networking, Addison-Wesley, Boston, MA, 2001.

[3] Marjan Radi, Behnam Dezfouli, Kamalrulnizam Abu Bakar and Malrey Lee," Multipath Routing in Wireless Sensor Networks: Survey and Research Challenges", Sensors 2012, 12, pp.650-685.

[4] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", Proceedings of 7th International Workshop on Security Protocols, ser. LNCS 1796, B. Christianson, B. Crispo, and M. Roe (eds.), Berlin, Germany: Springer-Verlag, pp. 172-194, 1999.

[5] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Adhoc Networks", In Proceeding of IEEE Int'l Conf. Network Protocols, Nov. 2001.

[6] M. Narasimha, G. Tsudik, and J.H. Yi, "On the Unitility of Distributed Cryptography in P2P and Manets: The Case of Membership Control", In Proceeding of IEEE Int'l Conf. Network Protocols Nov. 2003.

[7] M. Bechler, H.-J. Hof, D. Kraft, F. Pahlke, and L. Wolf, "A Cluster-Based Security Architecture for Ad Hoc Networks", In Proceeding IEEE INFOCOM, Mar. 2004.

[8] Y. Zhang, W. Liu, W. Lou, Y. Fang, and Y. Kwon, "AC-PKI Anonymous and Certificateless Public-Key Infrastructure for Mobile Ad Hoc Networks", In

Proceeding of IEEE Int'l Conf. Comm pp. 3515-3519, May 2005.

[9] Rajesh Patel, Sunil Pariyani, Vijay Ukani," Energy and Throughput Analysis of Hierarchical Routing Protocol (LEACH) for Wireless Sensor Network", International Journal of Computer Applications (0975 – 8887) Volume 20– No.4, April 2011, pp.32-36.

[10] Qi Yang, Yuxiang Zhuang, Hui Li," An Multi-hop Cluster Based Routing Protocol for Wireless Sensor Networks," Journal of Convergence Information Technology, Volume 6, Number 3, March 2011, pp.318-325.

[11] L. Haiyun, K. Jiejun, P. Zerfos, L. Songwu and Z. Lixia, "URSA: ubiquitous and robust access control for mobile ad hoc networks," in IEEE Transactions on Networking, vol.12, no.6, 2004.

[12] B. Wu, J. Wu, E. B. Fernandez, M. Ilyas and S. Magliveras, Secure and efficient key management in mobile ad hoc networks Journal of Network and Computer Applications, Vol. 30, No. 3, 2007.

[13] Jun Luo, Jean-Pierre Hubaux," Joint sink mobility and routing to maximize the lifetime of wireless sensor networks: the case of constrained mobility", IEEE/ACM Transactions on Networking (TON) archive Volume 18 Issue 3, June 2010 Pages 871-884.

[14] Laiali Almazaydeh, Eman Abdelfattah, Manal Al- Bzoor, and Amer Al-Rahayfeh," Performance Evaluation of Routing Protocols in Wireless Sensor Networks", International Journal of Computer Science and Information Technology, Volume 2, Number 2, April 2010,pp.64-73.

[15] Sanjay Kumar Padhi, Prasant Kumar Pattnaik, ,B.puthal ," Review of routing protocols in sensor and Adhoc networks,"International Journal of Reviews in Computing (2009- 2010),pp. 11-17.

[16] Rajashree.V.Biradar, V.C .Patil , Dr. S. R. Sawant , Dr. R. R. Mudholkar , "classification and comparison of routing protocols In wireless sensor networks", Special Issue on Ubiquitous Computing Security Systems, Vol.4, pp.704-711.

[17] Alka Singh, Shubhangi Rathkanthiwar, Sandeep Kakde, "LEACH Based-Energy Efficient Routing Protocol for Wireless Sensor Networks", IEEE, 2016.

[18] R. Dalal, Y. Singh and M. Khari, A Review on Key Management Schemes in MANET International Journal of Distributed and Parallel Systems, Vol. 3, No. 4, 2012.

[19] T. Khdour and A. ybrid Schema Zone-Based Key Management for in Journal of Theoritical and Applied Information Tecnology, vol. 35 No. 2, 2012.

[20] Bassant Selim, Chan Yeob Yeun, "Key Management for the MANET: A Survey", International Conference on Information and Communication Technology Research, IEEE, 2015.