ISSN 2320-9984 04 >
9 772320 998015

Volume 1, Issue 4, December 2013 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

Improved Key Exchange Based Security for MANET

Suruchi Agrawal
M.Tech Scholar
Department of Computer Science
Gyan Ganga College of Technology
Jabalpur (M.P.) [INDIA]
Email: suruchi_agrawal22@yahoo.in

Prof. Shekhar Tandan
Assistant Professor
Department of Computer Science
Gyan Ganga College of Technology,
Jabalpur, (M.P.) [INDIA]
Email: srtandan@yahoo.co.in

Abstract— *The characteristics of Mobile Ad-hoc NETwork (MANET) such as node mobility, dynamic infrastructure, unreliable multi-hop communication channel, resource limitation and physical vulnerability, securing MANET has made more challenging. MANET has no any pre-existing fixed structure and mobile nodes sends packets to the destination nodes directly or via the neighboring nodes, it is of potential security concern because neighbor nodes cannot be trusted so distributing encryption keys between mobile nodes in an authenticated manner is a challenging task.*

Key based processing over MANET requires to generate a new session key for every node as it enters into the network. The keys are distributed using the trust servers in such a way so that keys should be distributed securely so that any unauthenticated node cannot gain the access of MANET. There are many schemes available and are proposed to provide efficient key distribution in MANET. Various routing protocols and techniques are being included in wireless network and making it an area for further research. The need is increasing more due to invention and adaption of wireless communication devices for wireless communication. This work is focusing on security of the MANET routing and simulations are being proposed to show the improved packet delivery ratio. Attacks are being avoided reactively by including changes in the basic implementation of DSDV routing protocol. This work proposes to provide unique key based authentication for DSDV based MANET routing.

Keywords:—*Wireless Networks, Multicast Routing, DSDV, Packet Delivery Ratio, Security, Key Distribution*

1. INTRODUCTION

Mobile Ad-hoc network (MANET) is an infrastructure less and an autonomous systems of mobile hosts over a shared wireless medium. Because of such environment, mobile nodes can directly communicate with other nodes which are in their transmission range and rely on other nodes to communicate with nodes which are outside their transmission range by multi-hop scenario [1].

Security is considered to be more challenging in MANET because of its dynamic topology, multi-hop scenario, self organizing and center-less environment. In MANET, nodes are responsible for basic operations like packet forwarding and routing, distributing keys or any secret information.

These operations can be easily jeopardized if countermeasures are not taken on these operations at early stages.

Key management involves key generation, key distribution, key updation. The difficult task is how to distribute a key and update a key to ensure secure communication between two authenticated nodes. Because any node can enter or leave the network in dynamic topology, key updation must be done securely. If a new node wants a key to communicate with other node, any key must be kept secret should be distributed in a way that authenticity, confidentiality and integrity is not violated.

There have been several research work proposed on key distribution schemes in recent literatures. In this paper, we review three schemes of key distribution techniques based on network coding, message relaying and performance efficient EOMCT algorithm.

Network coding concept was discovered by Yeung, Li, Cai and Zhang [2]. Network coding is used to improve throughput and solves problems like congestion control and reliability. Main principle of network coding is that the intermediate nodes actively code input packets and forward the resulting coded packets [3]. This scheme is used in wireless ad-hoc network to design a light-weight key distribution scheme which provides data confidentiality using X-OR network coding and integrity of distributed keys using Message Authentication Codes (MAC).

Message Relaying key distribution scheme was proposed in [4]. It distributes certificate using an offline authority to issue each node with its keying material in authority-based MANETs. Certificate distribution occurs on peer-to-peer basis by exploiting the routing infrastructure and chaining peer nodes together and certificates are transferred along these virtual chains through by message relaying mechanism.

Scalability of [4] is investigated by evaluating its performance in network of as large as 50 nodes in first scenario and 100 nodes in second scenario by [5]. EOMCT algorithm provides efficient multicast key distribution with multicast group clustering to solve "1 affects n" problem which is due to highly group dynamism in which if any node joins or leaves a group, rekeying process should be done securely Analytical model and simulation result shows average latency of key distribution is propositional to energy consumption. If node changes frequently, it will require a large number of key exchanges per unit time to provide forward and backward secrecy [6].

The general key distribution problem refers to the task of distributing secret keys between communicating parties to provide security properties such as secrecy and authentication.

In sensor networks, key distribution is usually combined with initial communication establishment to bootstrap a secure communication infrastructure from a collection of deployed sensor nodes. In the setting we study in this chapter, nodes have been pre-initialized with some secret information before deployment, but only after network setup, we know the location of nodes. The node location often determines which nodes need to establish cryptographic keys with which other nodes, so we cannot set up these keys before deployment.

In this chapter, we refer to the combined problem of key distribution and secure communications establishment as the security bootstrapping problem, or simply the bootstrapping problem. A bootstrapping protocol must not only enable a newly deployed sensor network to initiate a secure infrastructure, but it must also allow nodes deployed at a later time to join the network securely. This is a challenging problem due to the many limitations of sensor network hardware and software.

In this chapter, we discuss and evaluate several well-known methods of key distribution. Besides these, we present an in-depth study of random key pre2 distribution, a method that has recently attracted significant research attention, and we have also worked on.

2. KEY MANAGEMENT IN MANET

Many cryptosystems rely on the underlying secure, robust, and efficient key management subsystem. In fact, all cryptographic techniques will be ineffective if the key management is weak. Key management is a central part of the security of MANETs. In MANETs, the computational load and complexity for key management are strongly subject to restriction by the node's available resources and the dynamic nature of network topology. Some asymmetric and symmetric key management schemes have been proposed to adapt to the environment of MANETs. Key management deals with key generation, key storage, distribution, updating, and revocation, deleting, archiving, and using keying materials in accordance with security policies.

A keying relationship is the state wherein network nodes share keying material for use in cryptographic mechanisms. The keying material can include public/private key pairs, secret keys, initialization parameters and non-secret parameters supporting key management in various instances. Key management can be defined as a set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties [2].

The fundamental function of key management schemes is the establishment of keying material. Key establishment can be subdivided into key agreement and key transport. Key agreement allows two or more parties to derive shared keying material as a function of information contributed by, or associated with, each of the protocol participants, such that no party can pre-determine the resulting value. In key transport protocols, one party creates or otherwise obtains keying material, and securely transfers it to the other party or parties. Both key agreement and key transport can be achieved using either symmetric or asymmetric techniques [3].

3. DIFFERENT KEY DISTRIBUTION

The operations like packet forwarding and routing, distributing keys or any secret information can be easily jeopardized if counter-measures are not taken on these operations at early stages. Key management is central to MANET security. Key management involves key generation, key distribution, key updation. The difficult task is how to distribute a key and update a key to ensure secure communication between two authenticated nodes. Because any node can enter or leave the network in dynamic topology, key updation must be done securely. If a new node wants a key to communicate with other node, any key must be kept secret should be distributed in a way that authenticity, confidentiality and integrity is not violated and there should be less message passing for provide authenticity and confidentiality between communicating nodes. There have been several research work proposed on key distribution schemes in recent literatures.

In N. Suganthi, R. S. Mohana Priya and V. Sumathy's scheme, they have suggested to divide the network into clusters. Cluster head will maintain the group key, it will also update the group key whenever there is a change in the membership. Here the re-keying process will be performed only if there is any movement of nodes within the clusters. So the computation and communication cost will be reduced.

They provided authentication between communicating nodes both in inter and intra cluster communication. And also the network life time will be extended with the help of monitoring node. The performance results prove the effectiveness of that key management scheme. Without clusters, the computation time, time delay and packets transferred from central node are more. With the formation of cluster, the computation time and other parameters are greatly reduced. Due to distributed behavior, the performance has been increased.

Another scheme for security is provided by D. Suganya Devi and G.Padmavathi. It illustrates an algorithm which is an enhancement of Optimized Multicast Cluster Tree (EOMCT) with Destination Sequenced Distance Vector (DSDV) routing protocol. It provides efficient multicast key distribution. The main idea of EOMCT is to use DSDV routing protocol to elect the local controllers of the created clusters. The principle of this clustering scheme is to start with the group source Group Controller (GC), to collect its 1-hop neighbors by DSDV, and to elect LCs which are group members have child nodes at the next level. The LC belongs to the unicast path between the source and the child group members. At this step, the elected LCs covers the group members having 2-hops neighbors of the group source. This scheme iterates until LCs cover all the group members. This method is performance efficient and more suitable for secure multicast key distribution dedicated to operate in MANETs. The future work deals with reliability of key distribution, which is an important issue in adhoc network due to the high packet loss during secure multicast key distribution.

Cluster-based composite key management scheme is suggested by R.PushpaLakshmi, Dr.A.Vincent Antony Kumar. In this scheme, authors have presented a new composite key management scheme based on a combination of techniques such as hierarchical clustering, partially distributed key management, offline certification authority and mobile agent. Initially, cluster head is elected using dominator election algorithm. It computes trust value of each node based on node's neighbour's opinion. The resultant node with maximum trust ability is marked as dominator. Next, the public key of ClusterHead (CH) changes with respect to its trust value. The public key is evaluated based on its previous public key and its trust value. At last, when new node joins the cluster, Offline dealer assigns unique id for the new node. The new node register its public key information in CH. CH records the information about new member in its member table with fields: mem_id, public key. When a node leaves a cluster, the CH removes the node information from it's member list.

Message Relaying Scheme is proposed by Hisham Dahshan and James Irvine. They present an analysis of a message-relaying based key distribution scheme for mobile ad hoc networks that was previously proposed by van der Merwe et al. Considering the message overhead occurring at the MAC layer in addition to the message overhead occurring at the network layer is an important issue in order to get a comprehensive study of the impact of the scheme on both layers. The scalability of the scheme is evaluated by investigating its performance on a network as large as 100 nodes. Message relaying scheme provides an efficient way to distribute keying material. The key distribution scheme is scalable since the one-hop certificate delivery ratio varied between 97% and 84% in the first scenario and between 99% and 81% in the second scenario.

R. Murugan and A. Shanmugam have suggested the scheme for minimum prior trust relationship between the nodes. It provides approach for a distributed key management and authentication approach by deploying the recently developed concepts of identity based cryptography and threshold secret sharing. The identity-based cryptography mechanism provided not only to provide end-to-end authenticity and confidentiality, but also saves network bandwidth and computational power of wireless nodes. which guarantees the ability for an arbitrary pair of devices to exchange a key in a secure fashion. This process is achieved without the prior knowledge of the maximum MANET size. The ad hoc wireless network can grow incrementally and also reduce if the mobile node participated in one ad hoc is detached due to the node movement from one zone to another.

Vishakha B. Sanghavi, Shreya V. Sanghvi, Naren V. Tada, Vijay J. Dubay, in this paper, we aim to evaluate and present an overview of different key distribution schemes for MANET like key distribution through Network coding scheme, Message relaying

scheme and Enhanced Optimized Multicast Cluster Tree (EOMCT) algorithm. Network Coding Scheme allows any two nodes to setup a shared key through a multi-hop route efficiently and provides light-weight key distribution for MANET. The analysis of Message relaying has been done to show the impact of message overhead at network layer and Medium Access Control (MAC) layer and provide scalability. EOMCT algorithm shows the improvement in parameters like average latency and energy consumption for secure multicasting.

4. PROPOSED WORK

Since key distribution schemes apply additional loads on the existing network, therefore it is being proposed to apply a new key distribution technique which will not only apply less load on the existing network, but will also use network efficiently and in secured manner. For testing of the proposed scheme, NS-2 protocol shall be used which will be modified for DSDV protocol for testing. Packet Delivery Ratio (PDR), Throughput, End-to-End Delay (ETOE) and Energy Consumption (EC) shall be evaluated for measuring the efficiency of the network. Proposed work shall work in following steps:

1. A trust server will have database of all keys and will distribute a key to all the nodes.
2. Each node will get a key when added in network by trust server.
3. For communication key will be verified from trust server by every node when it will receive the key of RTS signal sender.
4. If key is verified, then a Mix key is generated by node pair (sender & receiver) to communicate.
5. This key will be different key and hence malicious nodes or any intermediate nodes will not verify this key and hence will not be able to capture the data.
6. The intermediate nodes shall forward the packets to destination directly and hence they will not be verifying the key again and again for further communication.
7. Various metrics as specified above shall be measured to generate results and graphs.

The whole processing shall be as follows:

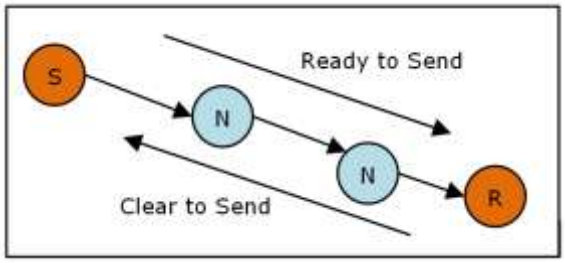

Figure 1: Proposed Key Distribution

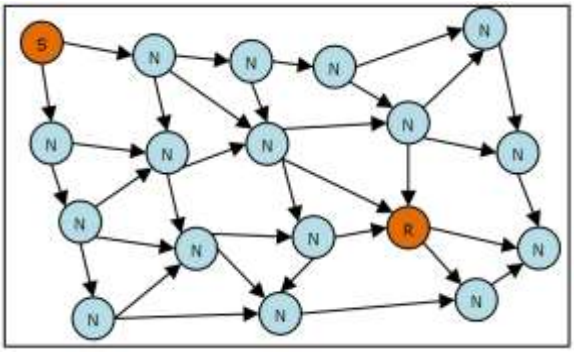

Figure 2: Proposed Network Topology

5. SIMULATION MODEL AND PERFORMANCE METRICS

Even though the performance evaluation/ analysis of ad hoc routing protocols is usually measured in homogeneous network, this evaluation is not much effective in the real applications where nodes have different capabilities. To study the efficiency and the effectiveness of routing protocols in heterogeneous ad hoc networks, NS-2 simulator [12] is used to construct the simulation. The details of the simulation scenarios and performance metrics are illustrated in the following sections.

A. Simulation Model

In heterogeneous ad hoc networks, each node normally has different capabilities since some nodes are portable devices with limited capacity and battery life, while the others may be stationary or equipped with vehicle. These nodes are not power-constrained and usually have higher capacity than the former one. In this research work, there are two types of nodes which are High-capacity nodes (H-nodes) and General capacity nodes (G-nodes). These two types of nodes have different capacity which are bandwidth and transmission range.

Simulation scenarios are constructed by varying number of nodes. In each scenario, a few nodes approximately 5-20% are included as malicious nodes. For example, if there are totally 50 nodes in the heterogeneous networks, 5 nodes of them are the malicious nodes while other nodes are correct nodes performing good communication practices.

Table 1: Simulation Parameters

Channel Type	**Channel / WirelessChannel**
Radio-Propagation model	Propagation / TwoRayGround
Network interface type	Phy/WirelessPhy
MAC type	Mac/802_11
Interface queue type	Queue / DropTail / PriQueue
Link layer type	LL
Antenna model	Antenna / OmniAntenna
Routing protocol	AODV
X dimension of the topography	1080
Y dimension of the topography	1080
Max packet in ifq	500
Seed for random number gen.	0
Simulation time	25
Number of mobile nodes	500

B. Performance Evaluation Metrics

The performance metrics which are used to analyze the performances of routing protocols in heterogeneous ad hoc networks are discussed in the following:

- **Packet delivery ratio (PDR):** the ratio of total number of packets received by destinations to total number of packets sent by sources

∑ Number of packet receive / ∑ Number of packet send

The greater value of packet delivery ratio means the better performance of the protocol.

- Average end-to-end delay: the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

∑ (arrive time – send time) / ∑ Number of connections

The lower value of end to end delay means the better performance of the protocol.

6. CONCLUSION

The proposed work in this research is focusing on the security aspect of the wireless networks in DSDV based routing protocol. The need of security is growing day by day as the newer wireless communication devices are invented and adapted. The proposed work is expected to provide better end to end delay, packet delivery ratio and energy consumption value and therefore it is expected to provide better performance. Since most of the processing shall be done locally on the nodes therefore network overhead shall be minimized by the proposed algorithm.

The proposed work can be tested in future for other routing protocols for the MANET such as AODV, DSR, and OLSR etc.

Security can be further made flexible by incorporating a mechanism for modifying the key through a user interface.

REFERENCES:

[1] Vishakha B. Sanghavi, Shreya V. Sanghvi, Naren V. Tada, Vijay J. Dubay, "Analysis of Different Key-Distribution Schemes for Mobile Ad-hoc Network", 2012 Nirma University Internaltion Conference on Engineering, NUiCONE-2013, 06-08 December, 2012, 978-1-4673-1719-1 2013 IEEE

[2] P. Michiardi and R. Molva, "Ad hoc networks security", ST Journal of System Research, vol. 4, pp. 1-3.

[3] R.W. Yeung, R. Li, N. Cai, and Z. Zhang, "Network Coding Theory, Foundation and Trends in Communication and Information Theory", vol. 2 no. 4 and 5, pp. 241-381, 2005.

[4] J. Dong, R. Curtmola, R.Sethi, and C. Nita-Rotaru, "Toward Secure Network Coding in Wireless Networks: Threats and Challenges", The Fourth IEEE workshop on Secure Network Protocols (NPSEC), pp. 33-38, Oct. 2008.

[5] J. van der Merwe, D. Dawoud, and S. McDonald, "Key Distribution in Mobile Ad Hoc Network based on Message Relaying" in fourth European workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS'07), Cambridge, UK, July 2007.

[6] H. Dahshan and J. Irvine, "Analysis of Key Distribution in Mobile Ad Hoc Networks Based on Message Relaying", IEEE International Conference on Wireless and Mobile Computing (WIMOB), pp. 538-542, Oct. 2008.

[7] D. Suganya Devi and G.Padmavathi, "Performance Efficient EOMCT Algorithm for Secure Multicast Key Distribution for Mobile Ad hoc Networks", IEEE International Conference on Advances in Recent Technologies in Communication and Computing, pp. 934-938, Oct. 2009.

[8] J. Liu and R. Du, "A Key Distribution Scheme using Network Coding for Mobile Ad hoc Network", Security Comm. Networks, vol. 5, issue. 1, pp. 59-67, Jan. 2012.

[9] G. Acs, L. Buttayan, and I. Vajda, "Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks", IEEE Trans. On Mobile Computing, vol. 5, no. 11, pp. 1533-1546, 2006.

[10] K. Fall and K. Vardhan, "The Network Simulator (ns-2)".

[11] M.Bouassida, I. Chrisment, and O. Festor, " Efficient Clustering for Multicast Key Distribution in MANETs", LCNS 3642, pp. 138-153,Jan 2008.

[12] M. Bouassida, I. Chrisment and O. Festor, "Efficient group key management protocol in MANETs using multipoint relaying techniques", Proc. IEEE International Conference on Networking, pp. 64, Apr. 2006.

[13] J.Macker and S. Corson, RFC 2501, Mobile Adhoc Networking (MANET):Routing Protocol Performance Issues and Evaluation Consideration, IETF 1999.

[14] Johann van der Merwe, "Key Management in Mobile Ad-hoc Network", M.Sc. Thesis, Nov. 2005.

[15] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook in Applied Cryptography. CRC Press, 1996.

[16] N. Suganthi, R. S. Mohana Priya, V. Sumathy, "An Efficient and Dynamic Key Management Scheme for Mobile

Ad-hoc Nework", European Journal of Scientific Research, ISSN 1450-216X, Vol.55, No.4 (2011), pp.no. 538-548.

[17] D. Suganya Devi and G.Padmavathi, "Performance Efficient EOMCT Algorithm for Secure Multicast Key Distribution for Mobile Ad hoc Networks", IEEE International Conference on Advances in Recent Technologies in Communication and Computing, pp. 934-938, Oct. 2009.

[18] R.PushpaLakshmi, Dr.A.Vincent Antony Kumar," Cluster Based Composite Key Management in Mobile Ad Hoc Networks", International Journal of Computer Applications, Vol. 4, No.7, pp. No. 30-35, July 2010.

[19] H. Dahshan and J. Irvine, "Analysis of Key Distribution in Mobile Ad Hoc Networks Based on Message Relaying", IEEE International Conference on Wireless and Mobile Computing (WIMOB), pp. 538-542, Oct. 2008.

[20] R. Murugan and A. Shanmugam, "Key Distribution System for MANET with Minimum Prior Trust Relationship", International Journal of Recent Trends in Engineering, Vol. 1, No. 2, pp. no. 75-79, May 2009.

[21] S. Katti, H. Rahul, W. Hu, D. Katabi, M. M´edard, J. Crowcroft, "XORs in The Air: Practical Wireless Network Coding", SIGCOMM'06, 11–15 Sep. 2006, Pisa, Italy.