Adaptive Group Key Management in Mobile Ad-hoc Networks (MANETs)

Inderpreet Kaur
Research Scholar
Mewar University, Chittorgarh
Rajasthan

A.L N.Rao, PhD.
Professor (IT) & Head – Research
Amity University
Noida

ABSTRACT:
In recent years, Mobile Ad-hoc Networks have received an immense attention in both industry and academia as they provide dynamic networking services. Such networks are rapidly deployable in the future, so secure wireless environment will be obligatory. In mobile ad hoc networks, due to unreliable wireless media, lack of fixed infrastructure and host mobility, providing secure communications is a big challenge. Because a temporary device recurrently joins or leaves a network, the authentication and security technology should be equipped for the malicious devices used in third-party attacks. Usually, symmetric and asymmetric cryptographic techniques are used for secure communications in wired and wireless networks but they have their advantages and disadvantages. In fact, any cryptographic means is ineffective if its key management is fragile. Key management is one of the vital aspects for security in mobile ad hoc networks. In mobile ad hoc networks, the processing load and complexity for key management are strongly subject to restriction by the node's available resources like energy and the dynamic nature of network topology. In this paper, Adaptive Group Key Management technique is proposed which uses symmetric key management. The proposed technique diagnoses compromised nodes in their regions by a secure key initially generated by the base stations (BSs). BSs carry out an initial key generation and trust is developed among mobile stations / nodes by another key known as group key. Simulations are done to observe the network performance and the results are very outstanding.

Keywords
Mobile Ad-Hoc Networks (MANET), Group key management, Security, Intrusion detection, Cryptography, Trust, Key Management, Symmetric key.

1. INTRODUCTION
In an ad hoc network, a device frequently joins and leaves a given wireless environment. So in such networks security vulnerabilities are high that it is hard to limit user access and, especially, devices with malicious intentions. Group and peer-to-peer communication in mobile cellular based ad hoc networks (MANET) has been of enormous interest in recent years [9].

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 [10]. A reliable routing protocol for Mobile Ad hoc Networks (MANETs) keeps the energy consumption as low as possible [11]. 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. The MANET with infrastructure-support is achieved by a self-configuring networking protocol and provides many benefits [9]. For example, it allows flexible peer-to-peer communication between two Mobile nodes by utilizing a high-speed interface without passing through the BS, and thus providing load balancing in cellular wireless systems.

The group communication is target-oriented in all nodes among clusters regardless of their size will execute the assigned key management scheme throughout their lifetime. Thus, the primary goal of Adaptive key management is to ensure system security and reliability in the presence of security attacks. The secondary goal is to satisfy application-specific performance requirements in terms of throughput, delay, or traffic capacity. This paper aims to address the issue of security in the presence of security attacks by enhancing the reliability of group communication, while satisfying system performance requirements.

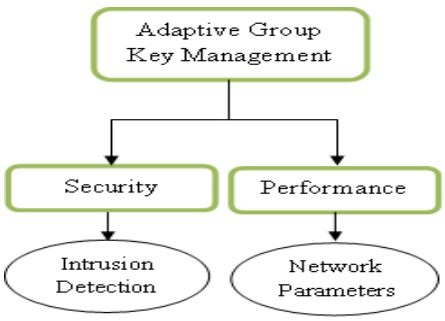

Fig. 1 Goals of Adaptive Key Management Scheme

Basically, this work includes the following: section 2 discusses related work; section 3 explains the "Adaptive Group Key Management technique" in two steps: key generation and key management; section 4 and 5 presents simulation model and numerical result analysis respectively; and lastly, section 6 presents the conclusion and future work directions.

2. RELATED WORK
Earlier research on ad hoc network routing focused on the protocol devise and performance evaluation in terms of the message overhead and loss rate.

In [1] author has proposed a new lightweight and robust group-key management protocol for Ad Hoc Networks which is based on distributed key management, the trust mechanism of the local group, zero-knowledge proof and timestamp exchange mechanism of OLSR routing protocol. By reducing both the number of control messages and the energy spent with cryptographic operations, the protocol achieves the advantages of low energy consumption, high efficiency and high availability. Also, the protocol is demonstrated for security through safety analysis. Finally, simulation results show that the proposed protocol can ensure the security of MANETs with a very little impact on the performance of secure routing protocol.

In a pure MANET considered by Kong et al. [7] and Deng et al. [8], the infrastructure is not present and a mobile node is active as the authority by distributing polynomial for each pair of mobile nodes, which may be undependable in terms of trustworthiness. On the other hand, in the wireless sensor network, the centralized authority pre-specifies the polynomial for each sensor before the deployment of sensors. The cellular based MANET, mobile users may be associated with different cellular BSs that may be charged by several authorities (i.e. service providers). Therefore, a key generation scheme needs to catch into account the security collaboration between them. At the same time, the key generation in cellular-based MANET should take into account the hierarchical architecture that the BS is on the infrastructure level and mobile users on the MANET level. The security association in the MANET level again should be inherit from the security association at the infrastructure level.

Jin-Hee Choa et al [6] have proposed an adaptive intrusion detection technique is based on majority voting by nodes in a geographical region to manage with collusion of compromised nodes, with each node preloaded with anomaly-based or misuse-based intrusion detection techniques to analyze compromised nodes in the same region. When given a set of parameter values characterizing operational and environmental conditions, one identify the optimal intrusion detection rate and the optimal regional area size in which the mean time to security failure of the system is maximized and the total communication cost is minimized for GCSs in MANET environments. The author has taken MTTSF (Mean Time to Security Failure) as security metric and Communication cost as performance metric Lower MTTSF means a faster loss of system integrity or loss of availability. Therefore, a design aim is to maximize MTTSF.

Kyung-Hyune Rhee et al. [5] proposes Implicit Certified Public Keys method, which reduces the overhead of the certificate validation checking process and expand computational efficiency. The architecture uses a two-layered key management approach, where a group of nodes is divided into:

1) Cell groups comprising of ground nodes, and

2) Control groups consisting of cell group managers.

The benefit of this approach is that the effects of a membership change are restricted to the single cell group.

Nen-Chung Wang, and Shian-Zhang Fang in [4] proposed, a hierarchical key management scheme (HKMS) for reliable group communications in MANETs network. For the sake of security, a packet is encrypted twice. The main idea in this proposal is key management for secure group communications in MANETs with multilevel structure. The level 1 subgroup (L1-subgroup) consists of all of nodes in the subgroup. The level 2 subgroup (L2-subgroup) can be established according to the location information of nodes in the L1-subgroup. This scheme is to create a cluster head that manages information, and constructs and transmits the group key. Firstly, in each subgroup, one can select a node with the largest weight value to be the level 1 cluster head (L1-head) in each L1-subgroup. After that, in each L2- subgroup, the node with the highest weight value will be the level 2 cluster head and manage the other nodes of the L2-subgroup. Finally, several L2-heads will be obtained in the L1-subgroup. Thus it maintains clusters and cluster heads.

Georgios Kambourakis et al. [3] have proposed an original public key management scheme using the well-known web-of-trust or trust graph model. The approach is based on a binary tree formation of the network's nodes. The binary tree structure is proved very effective for building certificate chains between communicating nodes that are multiple hops away and the cumbersome problem of certificate chain discovery is avoided. But the scheme is fully distributed or decentralized. This protocol is suitable for the dynamic environments the overhead for issuing, storing, and maintaining certificates is still larger.

3. PROPOSED WORK

The proposed method provides mutual certification via indicators with no information sharing between nodes in an ad -hoc network, and communicates with the communication partner in the proper manner through an Adaptive key. As a number of devices can join and leave an ad hoc network, group authentication is necessary. For the key generating protocol, an inter-cluster and an intra-cluster authentication method are proposed. The ad-hoc network nodes provides mutual authentication and then establishes a session to help communication between devices.

The asymmetric key involves high computation overhead in both encryption and decryption. Due to this, the need is to formulate a symmetric key generation scheme which could develop the trust among the ad-hoc nodes with base stations.

By using the Adaptive Key Generation, any pair of BSs is able to compute a shared secret key between them before communication, and the Adaptive Group Key can be further initiated in the MANET group. Trust relationships are such that no mobile nodes from another MANET cluster should be able to intrude any nodes conversation in which it does not participate in.

3.1 Key generation Scheme

In the proposed Adaptive Key generation scheme, one Base Station or group of BSs acts as trusted authority and are Key distributors for MANET nodes in their respective clusters. They collaboratively make decision on the key and distribute it on to their respective cluster members. Thus, while key generation it does not allow intruder to participate in the cluster and decipher the key. On the other hand for inter cluster communication to be able the cluster head (BS) of one cluster collaborate with the trusted entity of other cluster.

3.2 Key Management Scheme

The principal objective of our scheme is to enable each MANET node to be able to securely communicate with any other MANET node. This should be possible without any prior communication between the nodes. The group key is required for intra cluster communication. The BS elects the cluster head and for further transaction is the cluster head is defined as the initiator of the localized MANET cluster. For the peer-to-peer communication between two nodes, each node can securely communicate with any other node using the group keys established between the nodes within the cluster. The symmetric key enables effectively data encryption/decryption, even for volume data transmission by employing a high speed interface. For inter cluster communication once the BS helps to establish trust between nodes of different clusters than communication can be continued without support of BS for the session.

4. SIMULATION AND RESULTS

We implement proposed concept in a network simulator called NS2. To create a realistic simulation environment, one configures NS2. The proposed scheme is simulated by taking 25 nodes with 5 randomly distributed intruders in a 1000m X 1500m. Among 25 nodes 5 are configured as base station by keeping 'wiredRouting' ON. In this mobility model, a node goes in the direction of the destination with a speed uniformly chosen between the minimal speed and maximal speed. The Adaptive group key management is implemented with two routing protocols: AODV, DSR for comparison. For simulation purpose one chosen simulation parameters as given in Table 1.

Table 1: Simulation Parameters

Type	Values
Channel	Channel/Wireless Channel
Radio Propagation Model	Propagation/TwoRayGround
Network Interface	Physical/WirlessPhy
MAC	MAC/802_11
Interface Queue	Queue/DropTail/PriQueue
Antenna	Antenna/OmniAntenna
Link Layer	LL
Interface Queue Length	50
Routing Protocol	AODV,DSR
Simulation Time	100s
No. of Nodes	25
No. of attackers	5
Mobility Scenarios	5
Traffic type	Constant Bit Rate
Packet Rate	5, 10 packets/sec

5. RESULTS AND ANALYSIS

As the network intruders are increased all the protocols show major reduction in the network performance as well as security. To calculated performance of Adaptive key management with that of AODV and DSR protocol, one compares them using these metrics:

5.1 Packet Delivery Rate

The ratio of packets reaching to the destination node to the total packets produced at the source node.

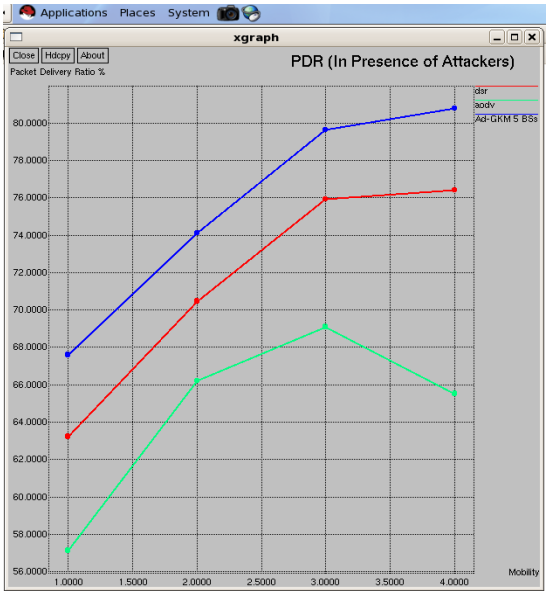

Fig 1: Packet Delivery Rate vs Mobility Scenario

5.2 End-to –End Delay

The average time gap between packet transmissions at source node until packet delivery to a destination.

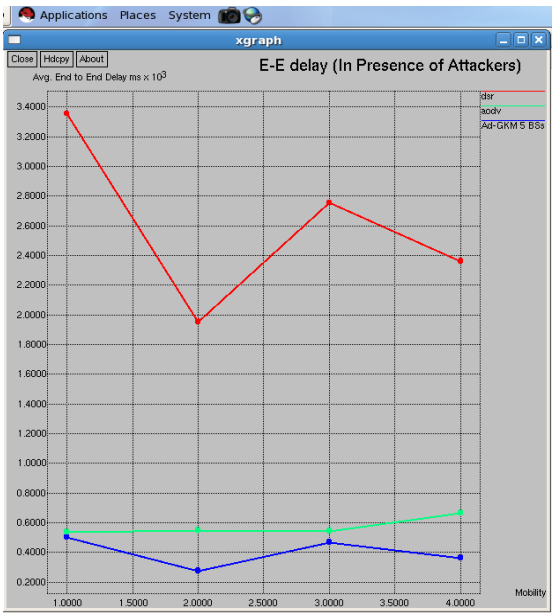

Fig 2: End-End delay vs Mobility Scenario

6. CONCLUSION & FUTURE WORK

In this work, one offering a new group key management scheme for cellular MANET based on adaptive symmetric key generation mechanism. There are two main contributions in this work. One is intrusion detection mechanism by generating trust using secretly shared keys; the other is the performance improvement in terms of Packet Delivery Rate

and End-to-End Delay. While comparing with AODV, result shows that the Packet Delivery Rate is increased upto 40% and End-to-End Delay is improved upto 55%. In case of DSR Packet Delivery Rate is increased upto 26% and End-to-End Delay is improved drastically. Performance evaluation has been done using NS2 simulator tool and comparison done by adapting Adaptive group key management scheme with AODV and DSR. The results are evaluated with AODV and DSR without key management schemes in presence of attackers / intruders. Results show that our protocol can effectively reduce end to end delay while maintaining a good packet delivery ratio thus showing more reliability against intruders. In future, the proposed scheme can be tested with other protocols also.

7. REFERENCES

[1] Changsheng Miao, Fengling Cao; Dong Chen; Guiran Changl, "A Lightweight Group-Key Management Protocol for Ad Hoc Networks", Genetic and Evolutionary Computing (ICGEC) 2012 Sixth International Conference in: IEEE, pp 288-291

[2] C. Peng Xiao, Jingsha He and Yingfang Fu, "Distributed Group Key Management in Wireless Mesh Networks", International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012.

[3] Georgios Kambourakis, Elisavet Konstantinou, Anastasia Douma, Marios Anagnostopoulos, and Georgios Fotiadis, "Efficient Certification Path Discovery for MANET", "EURASIP Journal on Wireless Communications and Networking" Hindawi Publishing Corporation Volume 2010, Article ID 243985, 16 pages, doi:10.1155/2010/243985.

[4] Nen-Chung Wang, and Shian-Zhang Fang, "A hierarchical key management scheme for secure group communications in mobile ad hoc networks", Elsevier - The Journal of Systems and Software 80 (2007) 1667–1677.

[5] Kyung-Hyune Rhee, Young-Ho Park, Gene Tsudik "A Group Key Management Architecture for Mobile Ad-hoc Wireless Networks", Journal Of Information Science And Engineering 21, 415-428 (2005).

[6] Jin-Hee Choa, Ing-Ray Chen, "Performance analysis of hierarchical group key management integrated with adaptive intrusion detection in mobile ad hoc networksl", Elsevier Performance Evaluation 68 (2011), pp 58-75, www.elsevier.com/locate/peva.

[7] R. Blom, "An optimal class of symmetric key generation systems", Advances in Cryptology: Proceedings of Euro crypt 84, Lecture Notes in Computer Science, vol. 209, Springer, Berlin, 1984.

[8] H. Deng, A. Mukherjee, D.P. Agrawal, "Threshold and identity-based key management and authentication for wireless ad hoc networks", IEEE International Conferences on Information Technology (ITCC'04), April 5–7, 2004.

[9] D. Cavalcanti, C.M. Cordeiro, D.P. Agrawal, B. Xie, A. Kumar, Issues 37 in integrating cellular networks, WLANs, and MANETs: a futuristic heterogeneous wireless network, in: IEEE Wireless Communications 39 Magazine, June 2005.

[10] Roopal Lakhwani , Sakshi Suhane, Anand Motwani, "Agent based AODV Protocol to Detect and Remove Black Hole Attacks", International Journal of Computer Applications (0975 – 8887) Volume 59– No.8, December 2012,pp.35-39.

[11] Tripti nema, akhilesh waoo, PS Patheja, Sanjay Sharma "Energy based AODV Routing Algorithm with Sleep Mode in MANETs", International Journal of Computer Applications (0975 – 8887) Volume 58– No.19, November 2012, pp.17-20.