Lightweight Key Distribution for secure routing and secure information propagation – A Review

Anubha Goyal, Geetanjali Babbar, Chandigarh Group Of Colleges, Landran

Abstract--**The mobile ad-hoc network (MANET) is the network of the mobile nodes. The MANETs are prone to the various kinds of attacks on the cluster, which are launched to steal the information from the MANETs. The MANETs have been made secure using the secure routing and key management schemes. The existing secure routing and key management schemes for MANETs have been studied, and the shortcomings of the existing models have been notified. In the paper, the MANET security scheme has been proposed using the very lightweight key exchange scheme with randomized key generation scheme for secure data propagation in the MANET clusters. The proposed model will be simulated using the network simulator 2 (NS-2).**

Index Terms—**Mobile ad-hoc network, secure routing, key exchange, secure routing update, etc.**

I. INTRODUCTION

To exchange information number of computer are joined together to form networks and share resources. To distribute information and data communication, networking is used. The sharing resources can be of two types- hardware and software types. It is central administration system or supports these types of system. Wireless Networking is a technology in which two or more computers communicate with each other using standard network protocols and cables are not connected to each other. The radio waves are used to connect different devices. It can be characterized in two ways. First is infrastructure mode, in which only one Wireless Access Point is used. In this wireless network adaptor is used to connect with the already existing networks with the help of access point. Wireless adaptor is also known as wireless clients. Second type of Wireless Networking is Infrastructure based networking. The communication takes place only between the access points and the wireless nodes. The communication does not directly takes place between the wireless nodes. The medium access is controlled by the access point and it acts as a bridge between the wireless and wired networks. Ad-hoc networks are a new standard of wireless communication for mobile hosts. These networks are basically local are networks in which data is send directly to one computer to another without using access points. No fixed infrastructure are required. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. MANET stands for Mobile Ad hoc Network. It is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. It can be setup anywhere. Nodes are randomly connected with each other and forming arbitrary topology. They act as both hosts and routers. The topologies between the nodes are changing continuously. They have ability to self-configure makes this technology suitable for provisioning communication to, for example, disaster-hit areas where there is no communication infrastructure or in emergency search and rescue operations where a network connection is urgently required. There are two types of attacks are present in MANET which break the security of the networks. These attacks are as follow:

Passive attacks- A passive attack obtains data exchanged in the network without disturbing the communications operation. The passive attacks are difficult to detection. In its, operations are not affected. The operations supposed to be accomplished by a malicious node ignored and attempting to recover valuable data during listens to the channel. Examples of Passive Attacks are eavesdropping, snooping.

Active attacks- In this attack, the attacker destroys the data while the data exchanged between the network. It disrupts the normal functioning of the network. It involves modification, fabrication and

disruption and affects the operation of the network. Example of active attacks are impersonation,spoofing. Other types of attacks in active attacks are internal or external attacks.

II. LITERATURE REVIEW

Priyanka Goyal et.al has worked on the MANET: Vulnerabilities, Challenges, Attacks, Application. In this paper they have discussed about the Mobile Ad-hoc network is the most promising fields for research and development of wireless network. Over the past few years, the popularity of wireless networks and mobile devices has increased. Now days, the most active and vibrant field of communication and networks is wireless ad-hoc networks. Due to brutal challenges, the special features of MANET bring this technology great opportunistic together. In this paper, the study and the overview of the routing protocols is mentioned. All the problems faced by the ad-hoc networks are present in this paper, including features, categories and vulnerabilities of MANET. It also includes the various challenging issues, emerging applications and the future trends of MANET.

S. Sharmila and G. Umamaheswari have proposed Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks. In this paper, various mechanisms are discussed which are based on cumulative acknowledgement and selective forward attack is detected on the basis of energy mechanism in mobile wireless sensor network. The scheme is evaluated in terms of packet delivery ratio and throughput. In this malicious node is detected on the basis of acknowledgement and energy levels of the node. The energy consumption of the detection scheme is less when compared with existing detection schemes. From the simulations, byte overhead is 0.39 percentages and detection accuracy is 80% are observed and thus increasing the network throughput. The results shows that the without the use of selective packet drop attack the packets are forwarded and malicious nodes are minimized in the network. The further enhancement of the proposed scheme is to improve the success rate to 100% with various mobility and receiver sensitivity of the node.

Satoshi Kurosawa et.al has worked on detecting attacks on AODV-based mobile ad hoc networks by dynamic learning method. In this paper, they proposed the solution emphasis on the dynamically changing conditions of ad hoc networks. In AODV, the routing information is determined from the originating node with the help of destination sequence. The attacker must generate its RREP with the destination sequence number greater than the destination sequence number of the destination node. The attacker will easily find the destination sequence number from the RREQ packet. Other nodes also tries to construct the route to the destination node rather than the source node, then the destination node's sequence number will be significantly different from the current destination sequence number. So the effect of the attack may also change depending on the increased amount of destination sequence number. It uses an anomaly detection scheme. To express state of the network at each node, multidimensional feature vector is defined. Each dimension is counted up on every time slot. When the number of connections increases the destination sequence number tends to rise, when there are few connections it tends to be increased monotonically. The feature vector include number of sent out RREQ messages, number of received RREP messages, the average of difference of destination sequence number in each time slot between sequence number of RREP message and the one held in the list. They compare distance between the mean vector and input data sample. If distance is greater than some threshold value then there is an attack. It uses dynamic training method in which the training data is updated at regular time intervals.

N.Bhalaji has worked on reliable routing against selective packet drop attack in DSR based MANET. In this paper they introduced ad-hoc networks are frequently targeted by participating malicious nodes to sabotage the network. A common mechanism to protect these networks is through the use of encryption and hashing mechanisms. However, the implementation of these mechanisms generally imposes certain unessential requirements, which are considered as restrictive for unplanned environments. In this paper we have discussed the dynamic trust based approach through which association between nodes are used to resist selective packet drop attacks connected to ad hoc networks. With the help of the Network simulator we were able to prove that the proposed scheme increases the routing security and encourages the nodes to cooperate in the ad-hoc structure. Our scheme is equipped with technique to identify and isolate the malicious nodes from the active data forwarding and routing.

Aikaterini Mitrokotsa et. al. has proposed the intrusion detection method to detect the Packet Dropping Attacks in Mobile Ad Hoc Networks. In this paper, they discussed that evolution of wireless network technologies and the recent advances that has been discovered in mobile computing hardware that have made possible the introduction of various applications in mobile ad-hoc networks. Not only is the infrastructure of these networks inherently vulnerable but they have increased requirements regarding their security as well. As intrusion prevention mechanisms, such as encryption and authentication, are not sufficient regarding security, we need a second line of defense Intrusion Detection. The focus of this paper is on anomaly detection techniques in order to exploit their main advantage of being able to detect unknown attacks. First, we briefly describe intrusion detection systems and then we suggest a distributed schema applicable to mobile ad hoc networks. This anomaly detection mechanism is based on a neural network and is evaluated for packet dropping attacks using features selected from the MAC layer. The performance of the proposed architecture is evaluated under different traffic conditions and mobility patterns.

III. RESEARCH GAPS

1. In the existing scheme, the trusted neighbor information in the neighbor table can be falsified by information injection attacks on the MANET nodes, which is a major loophole available for the hackers to gain the unauthorized access to the MANET networks.
2. The existing key exchange mechanisms add the higher overhead and add the data delivery delay in the transmission channel.
3. The diffie-hellman based key exchange scheme has been used in the existing model along with symmetric key cryptography. Diffie-hellman is not considered very secure and the communication channels secured using this can be easily taken over. Although, the symmetric key cryptography has been used in the existing model, the cryptanalysis attack can be merged with diffie-hellman information leakage attacks in order to take over the communication channel.
4.

IV. PROBLEM FORMULATION

In the existing scheme, the secure routing mechanism has been developed and merged with the integrated local key management protocol to protect the MANETs from false information injection or communication channel hijacking attacks. The existing secure routing and key exchange mechanism is using the local key exchange protocol to secure the MANET clusters against the inside and outside attacks. The existing model uses the Least Common Minimum (LCM) based broadcast key distribution mechanism combined with the symmetric encryption algorithm scheme. After a thorough study and analysis of the existing scheme, various research gaps and shortcomings have been listed down. The existing scheme is not secure against the route poisoning attacks, which is caused by false information injection as the routing update to create the warmhole or other similar attacks to route the information towards the false target. The existing mechanism uses the predictive key exchange, which makes it prone to the replication or guessing attacks to take the unauthorized access of the MANET resources. The existing key exchange mechanism adds the higher overhead in the communication channel, which adds the transmission delay. Also, the use of diffie-hellman scheme is not efficient enough because it is prone to the information leakage attacks. The proposed model will use a very lightweight non-predictive key exchange scheme with secure routing mechanism in order to protect the MANETs. The proposed scheme will be designed to overcome the shortcomings of the existing model. The proposed model will be using the multi-column random key table generation to improve the level of security and lower the overhead and transmission delay. The proposed scheme will use the secure periodic update to change the key table, which removes the need of encryption, hence will definitely lower the transmission delay due to the encryption or decryption algorithm.

V. METHODOLOGY

The detailed literature review on the key exchange and secure routing schemes for the MANETs will be conducted. The literature review will help us to read the merits and demerits of the existing models in order to get the path to design the new security scheme. The new security scheme will be proposed to overcome the shortcomings of the existing

models and to increase the performance of the MANETs. Then the proposed scheme will be implemented using the NS-2 simulator and the results would be obtained and analyzed in detail. After the results analysis, the results would be compared to the results of the existing models. The performance parameters of transmission delay, routing overhead, network load and throughput will be obtained from the simulation in the form of the results.

VI. CONCLUSION AND FUTURE WORK

The existing model has been studied in detail to notify the shortcomings of the existing system. Then the new system will be designed to overcome the shortcomings of the existing model and to provide an efficient MANET security mechanism for the best performance MANET clusters with secure information propagation. The proposed model will definitely improve the performance of the MANETs than the existing model in terms of transmission delay, network load, communication overhead, throughput, etc and will help to implement the high performance secure MANET clusters. In the future, the proposed model will be implemented using the network simulator 2 (NS-2). The proposed model simulation will be programmed to return the desired performance parameters. The performance parameters would be obtained and analyzed in order to estimate the performance of the proposed scheme.

REFERENCES

[1] Talawar, Shrikant H., Soumyadev Maity, and R. C. Hansdah. "Secure Routing with an Integrated Localized Key Management Protocol in MANETs." In*Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on*, pp. 605-612. IEEE, 2014.

[2] S. Sharmila and G. Umamaheswari, " Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks", *International Journal of Computer Applications (0975 – 8887) Volume 39– No.4, February 2012*

[3] Priyanka Goyal et.al , "MANET: Vulnerabilities, Challenges, Attacks, Application" , IJCEM, 2011

[4] Sunil Taneja, Dr. Ashwani Kush, Amandeep Makkar, "End to End Delay Analysis of Prominent On-demand Routing Protocols", IJCST Vol. 2, Issue1, March 2011

[5] Jacek Cicho, Rafał Kapelko, Jakub Lemiesz, and Marcin Zawada "On Alarm Protocol in Wireless Sensor Networks", 2010

[6] Sevil Şen, John A. Clark, Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks", 2010

[7] N.Bhalaji , "Reliable Routing against Selective Packet Drop Attack in DSR based MANET",*JOURNAL OF SOFTWARE, VOL. 4, NO. 6, AUGUST 2009*

[8] Aikaterini Mitrokotsa Rosa Mavropodi, Christos Douligeris, "Intrusion Detection of Packet Dropping Attacks in Mobile Ad Hoc Networks", *Ayia Napa, Cyprus, July 6-7, 2006*

[9] ABDUL HAIMID BASHIR MOHAMED, thesis, "ANALYSIS AND SIMULATION OF WIRELESS AD-HOC NETWORK ROUTING PROTOCOLS"2004

[10] Satoshi Kurosawa et.al "Detecting Attacks on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", IJNS, 2002

