International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Lightweight Key Distribution for Secure Routing and Secure Information Propagation

Anubha Goyal, Geetanjali Babbar

[1, 2]Chandigarh Group of Colleges,Landran, State Highway 12A, Mohali, Punjab 140307, India

Abstract: ***MANET is considered as a type of wireless sensor networking, it can be affected by many types of attack specifically on clusters and has main concern in the loss of information from the MANETs. Our proposed technique is concerned with selective packet drop from the selective forwarding attack. With this packet, throughput of the system get affected and results in the reduction of throughput. MANET associate with the network of mobile nodes. With the help of secure routing and key management schemes we can secure our MANET. For the proposed technique we have studied the existing models related to routing and key management and find out their shortcomings to far better model than the existing ones. In the proposed paper, security schemes for MANET are proposed that include lightweight key exchange scheme having randomized key generation scheme that provide security to data propagation in the MANET clusters. Experimental result shows that proposed technique gives better results as compared to existing technique.***

Keywords: *MANET, secure routing, key exchange, secure routing update, selective packet drop*

1. 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. There are two types of Sharing resources- software type or hardware type. Wireless Networking is a technology in which communication takes place between two or more computers and for the communication they used standard network protocols and are not connected by cables of any kind. [3]. There are two types of wireless networking. First is infrastructure mode is that mode in which 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 [4].It has a central controller. Second is In infrastructure based network, communication is takes place only between the wireless nodes and the access points. The communication is not directly takes place between the wireless nodes. Here the access point is used to control the medium access as well as it acts as the bridge to the wireless and wired networks. Ad-hoc networks are a new standard of wireless communication for mobile hosts. Basically it's a network which is used in urgent situation causes. No fixed infrastructure in ad hoc network like base stations is 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 robust infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are randomly connected with each other and forming arbitrary topology. They can act as both routers and hosts. 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:

1. Passive Attacks
2. Active Attacks

1. Passive Attacks:
A passive attack obtains data exchanged in the network without disturbing the communications operation. The passive attacks are difficult to detection [4]. 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.

2. Active Attacks:
An active attack is that attack which any data or information is inserted into the network so that information and operation may harm [4]. It involves modification, fabrication and disruption and affects the operation of the network. Example of active attacks is impersonation, spoofing [2]. Other types of attack are as follow:

1. Internal Attack:
Internal attacks are as of compromised nodes that are part of the set of connections. In an internal attack from the network the malicious node gains unauthorized access and behave as a genuine node. Traffic can be analyze between other nodes and may participate in the activities of other networks like blackhole, selective packet drop attack etc [6].

2. External Attack:
The external attack is conceded out by the nodes which do not belong to network. It may cause unavailibity and congestion by sending false information for the network jamming attack [1]. There are many other types of attacks are also possible in MANET which will be discussed in furthers sections. In section 2nd we will do literature survey. In section 3rd we will discussed about selective packet drop attack. After that proposed methodology and conclusion respectively discussed in last sections.

2. Literature Survey

S. Sharmila and G. Umamaheswari discussed about the defensive mechanisms based on cumulative acknowledgement and energy based is proposed to detect

selective forward attack in mobile wireless sensor networks . The scheme is evaluated in terms of packet delivery ratio and throughput. The malicious node is detected based on the acknowledgement and energy level of the node [5]. 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. These results show that the packets can be forwarded without any selective packet drop by minimizing the malicious nodes 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.

N.Bhalaji introduced [6] 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 adhoc 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 adhoc 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 discussed [7] that the development of several applications in MANET is possible with the help of wireless network technologies and mobile computing hardware. The main concern was the attacks increased on the infrastructure of the networks and also increased the requirements of the security as well. For the prevention from attackers several mechanisms are used, for example encryption and authentication, but these are not much helpful for the security purpose and therefore they used 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. In this paper, firstly they have described various intrusion detection systems and then suggested a distributed schema applicable to mobile ad hoc networks. Neural network technique is used for the detection of attackers and is evaluated for packet dropping attacks using features selected from the MAC layer. The performance is measured under different traffic conditions and mobility patterns.

Jacek Cicho et.al discussed the problem of efficient alarm protocol for ad-hoc radio networks consisting of devices that try to gain access for transmission through a shared radio communication channel [8]. The main problem that it has to face is that whenever it has sensed any alert situation the sensors have to quickly inform the target user, the alert situations can be presence of dangerous radiation, fire, seismic vibrations, and more. In this paper, we show a protocol which uses O (log n) time slots and show that (log n= log n) is a lower bound for used time slots.

3. Experimental Design

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.

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 worm-hole 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 has been 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.

4. Proposed Key Distribution Scheme

The proposed scheme is specially proposed for wireless sensor networks (MANET). The wireless sensor nodes are battery operated devices, Hence, having limited power sources. The MANET usually sends data to Base stations via long distance wireless communication at most of the times. Sometimes, MANETs does not send data anywhere to any BTS. Long distance wireless communications are not considered as the safe communications. Firstly considered option was to host the key management services on BTS. But it was not possible, because, if the key management services will be hosted on BTS, they are prone to hacking because of the long distance communication with the wireless sensor networks. In case BTS does not exist, the key management service will not work. Second consideration was to host the key management services on Cluster Heads, but it could choke the battery of cluster heads quickly, which may dent the performance of MANET. Then, there was a third and final option available which was to make a self-adaptive key management solution for MANET nodes. In the proposed solution, the self-adaptive key management scheme has been implemented.

Algorithm 1: Proposed MANET key exchange scheme

Assumptions

1. All nodes are MANET scheme aware nodes
2. All nodes can serve as client or server
3. All nodes can encrypt decrypt the key information
4. All nodes are battery operated nodes

ALGORITHM STEPS

1. Node X builds a secure key table
2. Node X sends its secure key table with Node Y
3. Node Y saves Node X table in its memory
4. Node X senses the data
5. Node X transmit the data to Node Y for first time
6. Node Y sends a secure key to Node X
7. Node X replies with the secure reply Key
8. Node Y matches the Key

a. If key matches

i. the communication takes place.

b. Else

i. The communication request rejected by Node Y

Key Generation and Usage Control: The key generation policy used in the proposed model is based on the high randomization and mathematical array value shuffling operation, which creates highly randomized and undependable numeric keys. Any of the key in the key table can't be calculated mathematically to find the next key in the table. Unauthorized applications and hackers cannot bypass the MANET scheme running on the sensor nodes because, to gain the authority to send the data to the sensor nodes, one has to obtain the authorization by sending a reply or response key in return to the request or question key sent they sensor node on receiving a data stream. **However, this administrative operation can be recorded in the sensor node audit log and held accountable.**

Key Generation Policy: Key generation policy under the proposed model is using the following mathematical algorithmic flow to populate the key table which is saved and being exchanged between the sensor nodes in the working cluster.

Algorithm 2: Random Function to generate random number

A. First, initialize the random number generator to make the results in this example repeatable.

B. Create a radii value for each point in the sphere. These values are in the open interval, $(0,3)$, but are not uniformly distributed. The values have been created using the mathematic equation:

$$f(x) = 3 * \int_{1}^{1000000} random * \frac{1}{3}$$

C. Randomly select and concatenate the coordinates or values to create the OTP.

D. Return OTP

5. Result Analysis

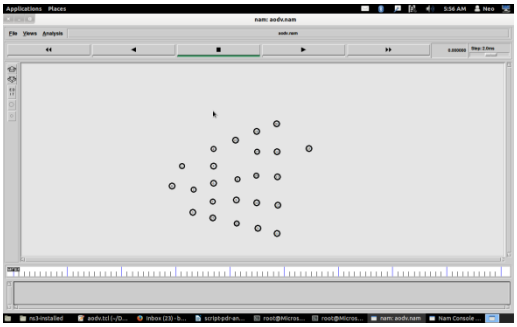

Figure 1: The Simulation Topology

The topology size is kept limited to avoid the confusion and overload of the packet transmissions visualizations. The modified internet protocol is thoroughly tested on all of the nodes to minimize the effect of the Data Forwarding attack on the WSN cluster. The changes have been observed in amount of delay and overhead when implemented then secure code framework in the simulation. The function of all other nodes except the traffic ingress procedure remains the same. The normal scenario simulated in NS-2 is shown in the snapshot displayed in Figure 1. The delay and overhead has been recorded to analyze the performance of the proposed model where the IP protocol has been modified to facilitate the secure code marking to detect the false/attacker nodes in the wireless sensor network. The network simulation after the incorporating the proposed model for secure code marking/embedding has resulted

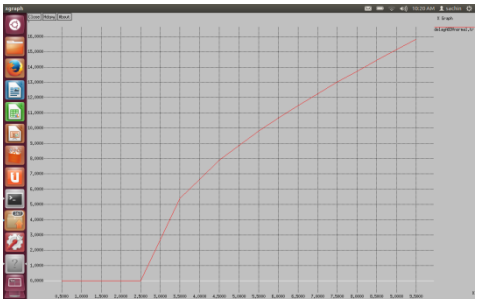

Figure 2: Graph showing delay for the marked and normal traffic

in the minimized overhead and delay as shown in the simulation results below in the figure 2. The overhead is based on the traffic/application/service type used in the simulation, like, CBR and VBR.

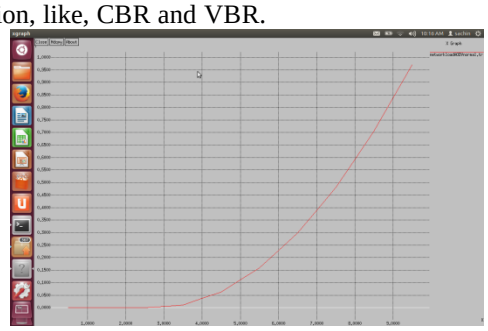

Figure 3: Network Load Comparison Graph

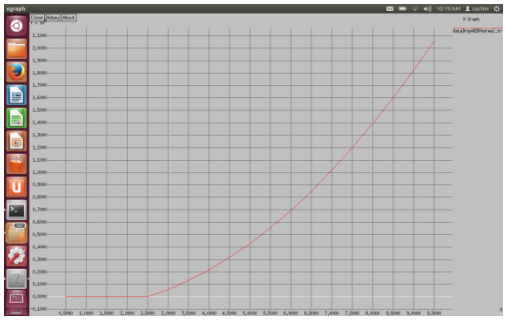

Figure 4: Data Drop Normal Comparison Graph

It also depends upon the packet size offered by the service/application/traffic used in the simulation. The graph in figure 2 shows delay and overhead comparison of the normal and secure marked traffic. This shows the efficiency of this technique. It has been observed from the results that the throughput and network load is higher under the simulation scenario implemented with proposed scheme rather than the existing scheme. The network load is the parameter of total load in the network. The total load is measured by the calculating total computational power used in the network cluster. The data drop and network load is comparatively higher in the normal network cluster, whereas in the cluster with the proposed solution has shown the significant improvement in the network performance.

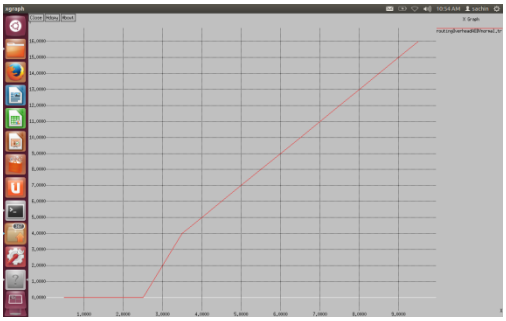

Figure 5: Graph of Routing overhead in the proposed scenario of MANETs

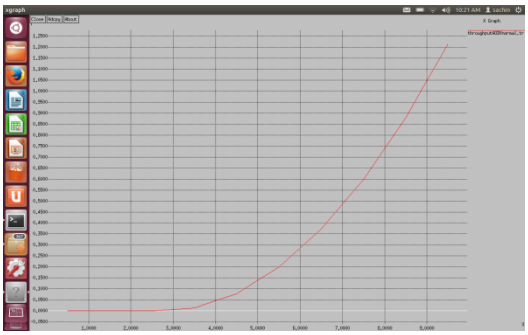

Figure 6: Throughput in the normal network cluster

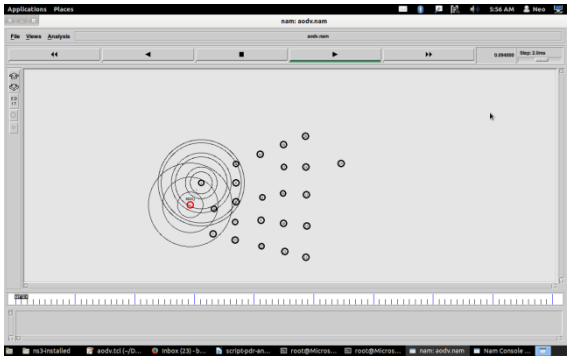

Figure 7: The beginning of the simulation from node 0. Node 0 is the seed node in the simulation and connects to everywhere

The figure 7 describes the topology of the proposed model. The proposed model simulation is consisted of 24 nodes at total. The simulation has been designed to protect against the selective packet dropping attacks in MANETs by using the key exchange scheme based authentication prior to route information exchange. The simulation has been designed with three paths where the major target is to find the target node using the secure routing process based upon authentication. In the figure 8, the simulation has been shown where the node 0 or the seed node is connecting the next hop nodes in order to find the routing destination. The red colored nodes are showing the route request being exchanged between the two MANET nodes during the routing information exchange process. The secure routing information exchange process protects the MANETs against the false route information injection attacks which may lead to the various kinds of attacks. The circles around the nodes are showing that the nodes are broadcasting the information to their next hops nodes.

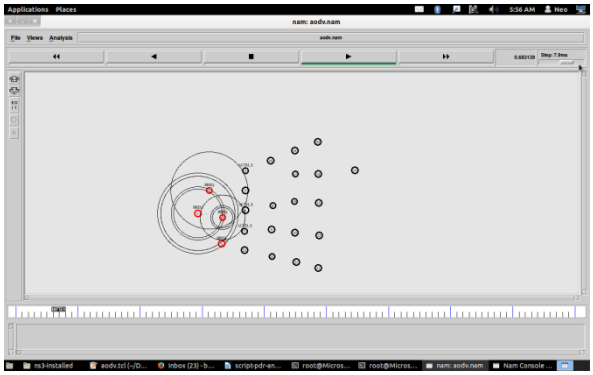

Figure 8: During the simulation of all four paths, node 0 sending authentication request to the next hop nodes

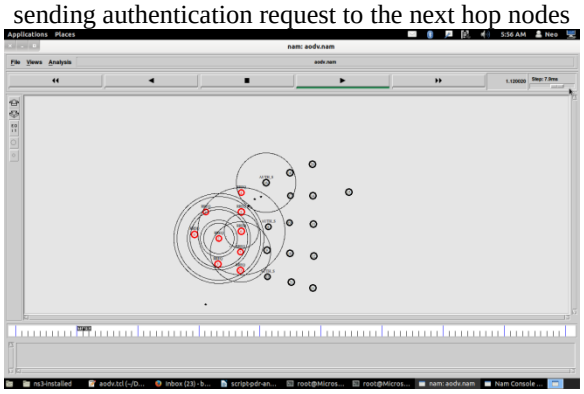

Figure 9: Next hop nodes sending authentication request to their next hop nodes

In the figure 9, the nodes have been shown connecting the next hop level where looking for the destination node. The layered routing or route exchange approach (the approach where the nodes connected from one hop to next hop of the neighbor nodes) is considered the most efficient method because of its distributed nature. In the figure 10, the blue nodes are indicating the nodes with no further route information. Such nodes reply with route not found and mark themselves unavailable for the requested route. It means the blue nodes have existed the route information exchange process because of lack of information or lack of neighbor approach.

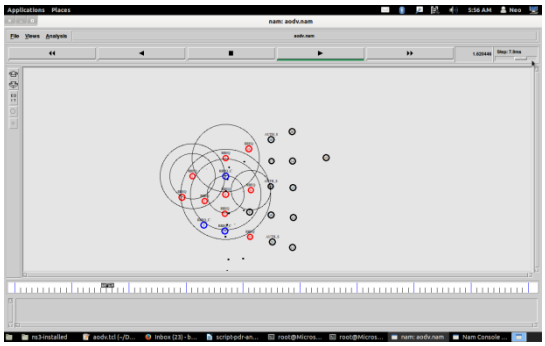

Figure 10: The blue nodes are showing the nodes with no further path information, whereas red nodes are waiting for the route and authentication query

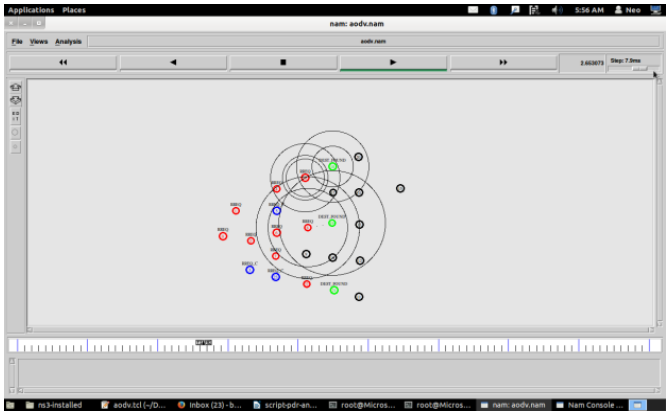

Figure 11: The green nodes are showing that the destination nodes are found

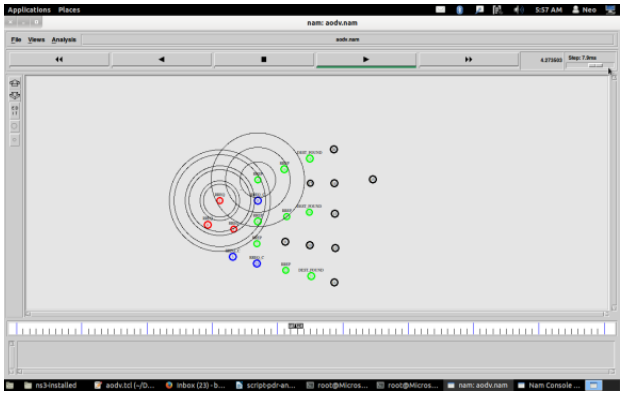

Figure 12: The more green nodes show the route reply and authentication acceptance

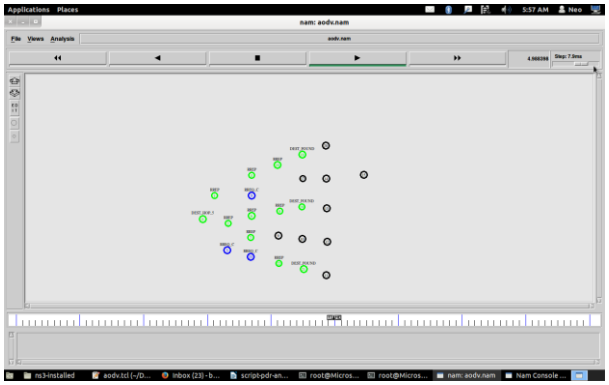

Figure 13: The lower level of authentication towards the seed node

In the figure 12, the green colored nodes on the right hand side are indicating the destination nodes. Now, the destination node will forward the route reply to the nodes sending request towards the destination nodes. The further process has been shown in the figure 12 and 13. The figure 12 is showing that almost half of the nodes in the paths have received the route reply and have turned themselves on for the specific route defined by the route request and route reply process. The route figure 13 is showing the converged paths after the completion of the path request and reply process. The path selection process is secured using the randomly generated lightweight key exchange scheme on the MANETs.

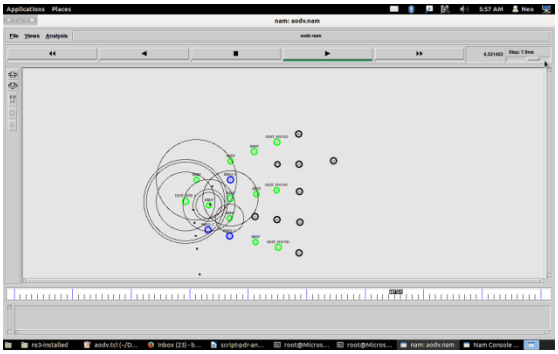

Figure 14: The communication has been taken place between the seed node and the destination nodes

In the figure 14, the nodes have started the communication in the MANET cluster after the path convergence. The path forwarding is the procedure of sending the data over the selected path. The path selection is the part of the routing protocols. The secure routing protocol is the base mechanisms which automatically protects the MANETs against the false information exchange, selective packet dropping or selective jamming attacks.

6. Conclusion and Future Work

The wireless adhoc network is the self configuring network; mobile nodes can leave or join the network when they want. These types of networks are much vulnerable to security attacks. Much type of active and passive attacks is possible in Adhoc network. Among all the possible active attacks, Selective Packet drop attack is the most common and harmful attack. This attack degrades network performance and leads to denial of service attack. The attack is triggered by the malicious node which is present in the network. In this work, novel technique has been proposed to detect and isolate malicious nodes from the network which are responsible for triggering the attack. The novel technique is based on Diffie-Hellman authentication. The experimental results show that, proposed technique detects and isolate the malicious nodes from the network efficiently. It will improve network efficiency, delay and increase throughput of the network. In future selective packet drop attack can be prevent using another authentication techniques.

References

[1] Sunil Taneja, Dr. Ashwani Kush, Amandeep Makkar, "End to End Delay Analysis of Prominent On-demand Routing Protocols", IJCST Vol. 2, Issue1, March 2011
[2] ABDUL HAIMID BASHIR MOHAMED, thesis, "ANALYSIS AND SIMULATION OF WIRELESS AD-HOC NETWORK ROUTING PROTOCOLS"2004
[3] Giovanni Vigna Sumit Gwalani Kavitha Srinivasan Elizabeth M. Belding-Royer Richard A. Kemmerer, "An Intrusion Detection Tool forAODV-based Ad hocWireless Networks", 2004
[4] Sevil Şen, John A. Clark, Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks", 2010
[5] 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*
[6] N.Bhalaji , "Reliable Routing against Selective Packet Drop Attack in DSR based MANET", *JOURNAL OF SOFTWARE, VOL. 4, NO. 6, AUGUST 2009*
[7] Aikaterini Mitrokotsa Rosa Mavropodi, Christos Douligeris, "Intrusion Detection of Packet Dropping Attacks in Mobile Ad Hoc Networks", *Ayia Napa, Cyprus, July 6-7, 2006*
[8] Jacek Cicho, Rafał Kapelko, Jakub Lemiesz, and Marcin Zawada "On Alarm Protocol in Wireless Sensor Networks", 2010