Malicious Attack Detection for Secure and Efficient Routing in MANETs

Asha S[1], Dr. Hema Jagadish[2]
[1]M.Tech Student, [2]Assistant Professor,
Department of Information Science and Engineering,
Bangalore Institute of Technology, Bengaluru, India,

Abstract : An Mobile Ad-hoc Network (MANET) is a sort of wireless network that bring various application in distinctive fields. MANET is an application of the Wireless Ad-hoc Network (WANET) that connects mobile nodes to each other node. Normally node act as link among the sender and receiver. In WANET there will be no particular consolidate network in the management. The proposed system mainly concentrate on defending routing attack caused by the black hole node, grey hole and wormhole which intentionally drops the routing packets without forwarding to the destination.

IndexTerms **- Mobile Ad-hoc Network (MANET), Attacks, Packet drop, Security, Avoidance.**

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) has historically gained a lot of attention because they are mobile and thus have no fixed infrastructure. Applications for MANET vary from business to strategic or armed forces. MANETs are typically multihop networks to dynamically secluded source and destination nodes. MANETs therefore play an important role in the MANETs. While developing the routing protocols, the significant concern of limitations remains, that is, limiting energy and lifetime, Quality of Service (QoS), modifying topologies of a the network due to both the mobility and security problems of a network. Additionally, the current focus in is that if the battery of a node is depleted, the node acts as a dead node. Therefore, the task of limited power source of energy in MANETs requires further study. Table-based or active routing and hybrid routing are the main types of dynamic routing for routing information between other nodes in the MANETs.

Attack is indeed an effort to pass security measures on such a computer system. The intrusion can modify, reveal or refuse data. Types of threats involve acts along with gaining unauthorized credentials, wrongly injecting data, manipulating details, examining data traffic, gaining unlawful access to the network or disrupting network traffic via malware.

II. RELATED WORK

Swain et.al, demonstrated three important routing protocols Topic-Based Synchronization (TBS), Source Demand Routing (SDR), Multicast Ad-hoc on demand Distance Vector (MAODV). These routing protocols are used to solve the problems created by the malicious nodes in the network for the betterment of Packet Delivery Ratio (PDR) with less delay. Concluded TBS routing protocol which comes out to be one of the important protocol compared to SDR and MAODV. TBS protocol consumes less power with lesser delay rates and gives higher PDR factor. [1]

Reda et.al, worked on two routing protocols i.e. Ad-hoc On demand Distance Vector (AODV) and Dynamic Source Routing (DSR) routing protocols. These protocols were used to find the packet drop rate and the percentage of nodes which are able to detect the attacker nodes of the network for their existence. The researcher has generated two methodology, first is normal method and second method is with malicious attacker nodes. AODV shows better performance in normal method due to its cache maintenance. In second method, AODV and DSR both drops packet as malicious node harms the network, but still AODV has better outcomes due to its reactive nature. [2]

Dokurer et al**,** modified the AODV protocol to attack caused by the malicious node in the routing. In this paper, where the source node requests the route to ignore the first two Route Request (RREP) packet then to choose the next hop of any RREP packet because generally black hole replies to RREP packets very quickly than compare to other nodes. [3]

S. R. Deshmukh et.al, proposed the model that is going to depend on the validity of the bit which is set by the Route Request (RREP). In the model, the attacker not knowing the validity of the given bit set upon the sending RREP. Later when source node accept the RREP it will check the bit if it valid then set the path and if not it is considered as RREP is from the black hole and it will be discarded. [4]

S. Zhong et.al, measure the destructive negative impact of wormholes on the quality of network coding systems across tests. Initially implemented an unified algorithm for detecting wormholes as well as intensively demonstrating the reliability. Introduce decentralized wireless network, while examining the shift with in flow movements of the revolutionary packets induced with wormholes. [5]

III. PROPOSED SYSTEM

The proposed techniques developed by creating chaotic map for the black hole, controlling packets for grey hole and by internal worm hole detection for worm hole attack. Initially the proposed work is mainly concentrating the black hole then later it will collaborate with worm hole. While transferring the data it will create a tunneling, where as it will give fake replay then it will mislead the source and destination. Once the malicious node detected then it will update in the network. In chaotic map, once the route request is fake reply then it will create a map then it will not allow to communicate with the next node.

In the proposed system from source node, it will send the TCP packets. The nodes are deployed randomly and then it will find its neighboring nodes once the neighboring request has sent to every node then it will select source and destination. Later

source will send route request to every individual node to send the data. In between malicious node will drop packets and it will not allow further packets to reach their respective the destination. Figure 1.1 shows the proposed system architecture. Here nodes are not particular it can be any number of source and the destination more over there will be no particular source and the destination in the network.

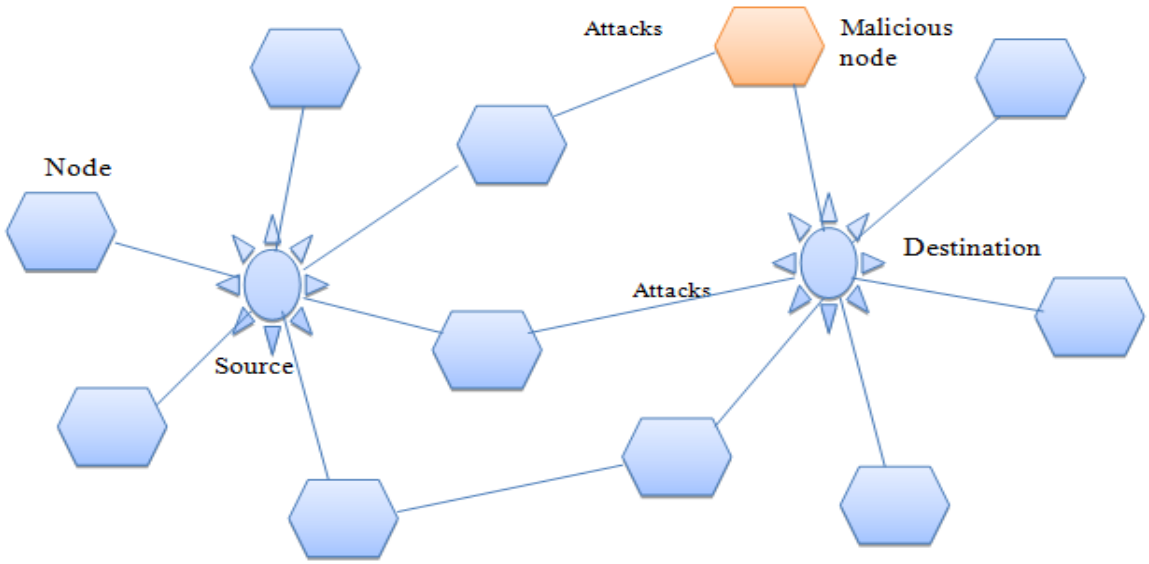

Figure 1.1: System Architecture

IV. IMPLEMENTATION

There are different types of attacks that will create a misbehavior in creating routing path from source and destination. There are mainly three important modules that can be network module, energy module and attacker module, these modules are explained below

1. Network Module

In the network module the nodes are deployed randomly. Here in the proposed system approximately 40 nodes are taken in order to execute the proposed system. The Euclidean distance formula is used to calculate the neighbor node.

2. Energy Module

The nodes are assigned with its initial energy and these nodes are homogeneous. In this module the energy parameter like ideal power, sleep power and transition power (shifting nodes from awake to sleep) are mentioned. The residual energy is calculated by left out energy after data transmission.

RE=Initial Energy (IE) – Consumed Energy(CE)

3. Attacker Module

The attackers like black hole ,grey hole and worm hole are tries to mislead the routing path. These attaker drop the packets and does misbehavior in the network. In the attacker module for the detection of malicious node baiting and control message packets are used.

Algorithm using bait at source node:

Step 1 If CurrentTime then = = Bait Time
Step 2 Generate Request for Bait;
Step 3 Create an ID at random and set it to Bait request;
Step 4 Bait request TTL set to 1;/ TTL (Time-To-Live)
Step 5 Request for Broadcast Bait;
Step 6 Bait-time reset to random time;
Step 7 Exit if
Step 8 Do for every Bait reply received
Step 9 In the Blackhole list store NWSP ID;/ NWSP (NodeWith the Shortest Path)
Step 10 End at

V. RESULTS

In the work the simulation tool is used cooja simulator. Initially create a simulation process by the name and later it will browse the contiki processes and compilation of the terminal will be opened. Once the compilation of project done then it will move to the project terminal.

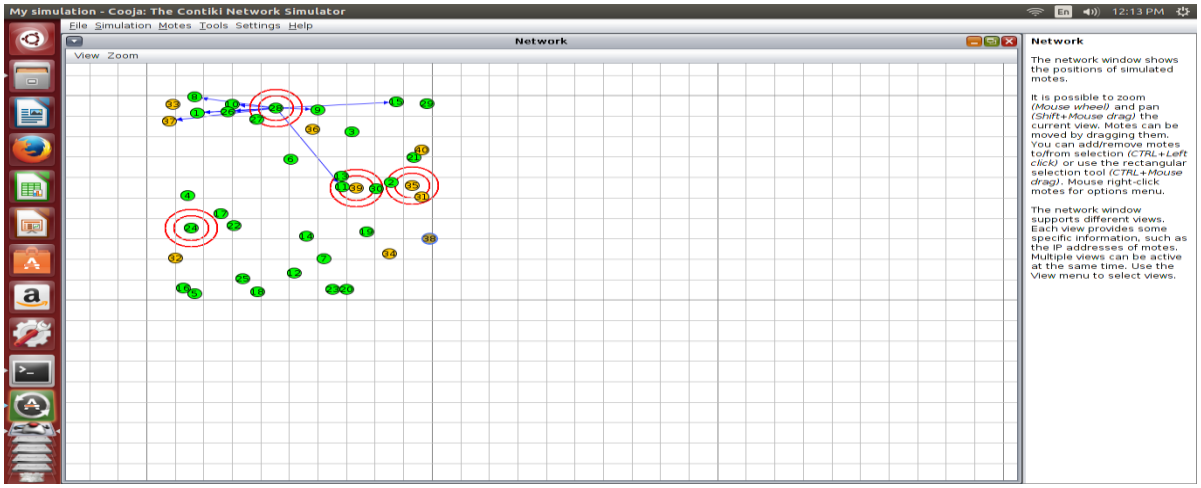

Figure 1.2: Launching of Attacker Node

The Figure 1.2 attacker tries to launch the attacker node and create a collision between the packets. It will detect the malicious node if the malicious node detected then it start packet dropping and it will not forward the packets from source to destination.

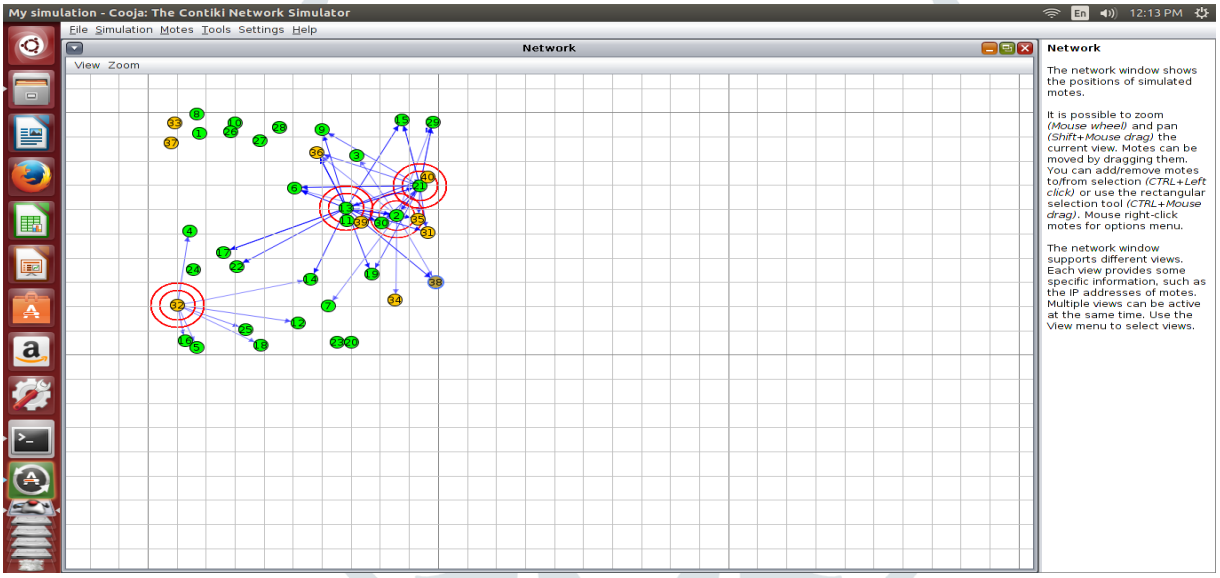

Figure 1.3: Creating Tunneling

The Figure 1.3 creates a tunneling by wormhole. The tunnel is created by giving fake reply, then it will mislead the source and destination. Here the node 13 and node 2 are said to be attacker in the given figure.

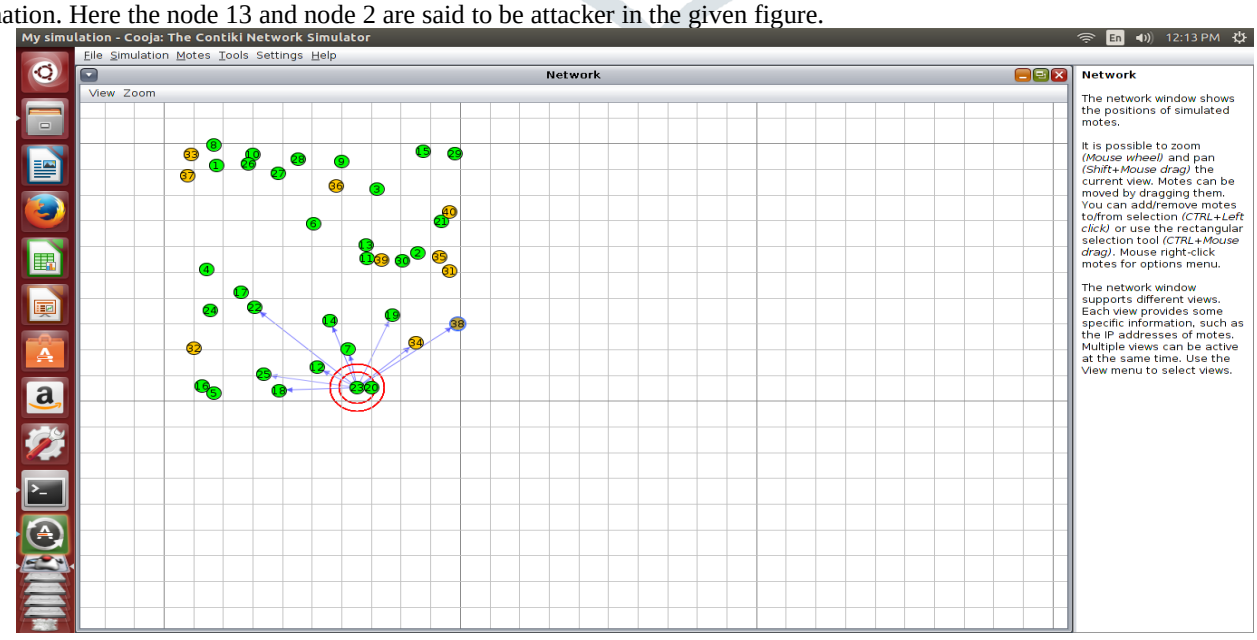

Figure 1.4: Nodes Updating

Figure 1.4, once the malicious node detected then the nodes are going to update by calculating its neighbor distance formula. Later from the source node it will take near alternative routing path to reach the destination.

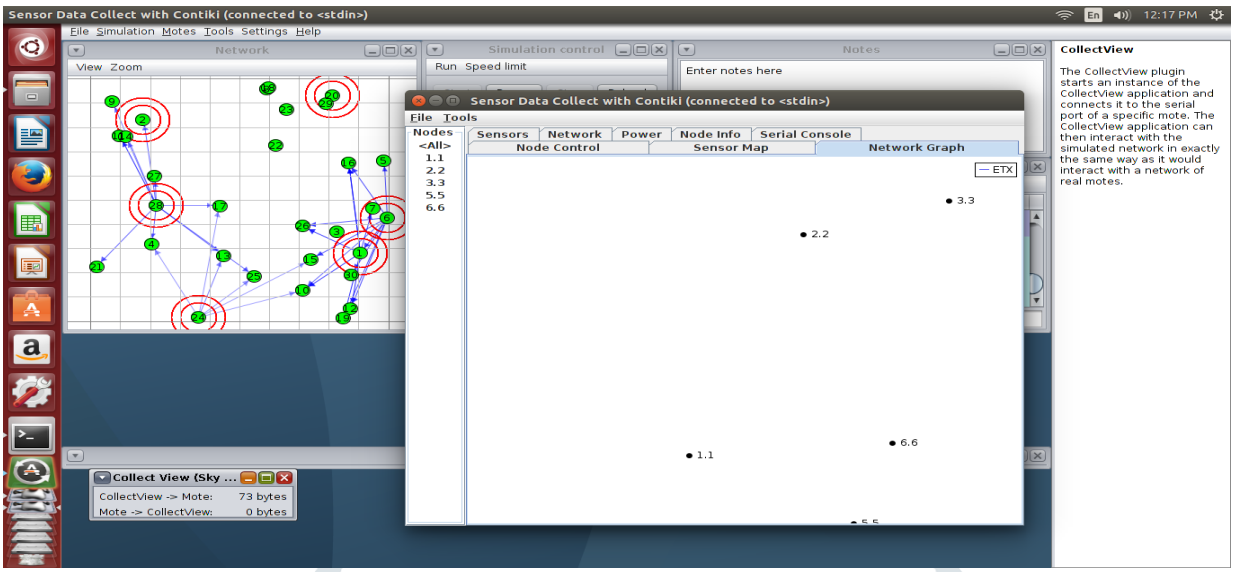

Figure 1.5: Mobility Map

The Figure 1.5, mobility map shows it's neighboring location. Mobility is said be one of the major role in the performance of the MANETs. Topography showing movement of nodes for random mobility model.

VI. CONCLUSION AND FUTURE WORK

In the proposed system, the study and analysis of the black hole attack and grey hole and worm hole attacks is evaluated. AODV is one of the important reactive routing protocol. In the system, the detection and avoidance of the attacks are implemented using chaotic map. In the proposed system secure route by applying AODV routing protocol that affect the nodes by dropping packets and weaken the network. Wormhole attacks which create tunnelling is detected and avoided. In future, the concept of threshold key management scheme can be implemented for better efficiency for detecting malicious activities of the node in the network.

VII. REFERENCES

[1] Jhum Swain, Binod Kumar Pattanayak and Bibudhendu Pati, "study and Analysis of Routing Issues in MANET", International Conference on Inventive Communication and Computational Technologies, (ICICCT. 2017

[2] Mahmoud Reda, Marianne A. Azer (2017), "Correlation between Protocol Selection and Packet Drop Attack Severity in Ad Hoc Networks", 978-1-5386-4266-5/17/ Â © IEEE.

[3] S. Dokurer, Y. M. Erten, and C. E. Acar, ``Performance analysis of adhoc networks under black hole attacks," in Proc. IEEE SoutheastCon, Richmond, VA, USA, Mar. 2007, pp. 148153.

[4] S. R. Deshmukh, P. N. Chatur, and N. B. Bhople, "AODV Based secure routing against blackhole attack in MANET," in Proceedings of the 1st IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2016, pp. 1960–1964, Bangalore, India, May 2016.

[5] S. Ji, T. Chen, and S. Zhong, ``Wormhole attack detection algorithms in wireless network coding systems," IEEE Trans. Mobile Comput., vol. 14, no. 3, pp. 660674, Mar. 2015.