IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DETECTION RATE ANALYSIS FOR USER TO ROUTE ATTACK IN MOBILE AD HOC NETWORKS

1S.Saranya, 2S.Muthulingam, 3S.Barkath Nisha

1Assistant Professor, 2Assistant Professor, 3Assistant Professor

1STC College,

2RVS college of engineering,

3STC College

***Abstract*: we present novel techniques to counter a set of active attacks, such as denial-of-service (DoS), probe, vampire, and user-to-root (U2R) attacks, in a mobile ad hoc network (MANET) environment for a single and multiattack scenario. Attacks are detected using a behavioral analysis for both the single attacks and a trust for distributed multiattacks. Here Network Simulator 2 (NS2) environment is used with an ad hoc. We report a maximum accuracy of 87.80% for a single attack and 90.99 % for a multiattack scenario.**

***Keywords*: MANET, RREQ, TTL, AODV, Honeypot**

I.INTRODUCTION

It says about the mobile ad-hoc networks and the security attacks happening over there. Among them flooding attack is taken into consideration and its impact on medical field is discussed. A network is a group of people or systems or organizations who wants to share their information collectively. Initially computer network were started to share files, later this has moved from that particular job of file and printer sharing to application sharing and business logic sharing. A network can be signalized as wireless or wired. Wireless can be distinguished from wired as physical connectivity between nodes is not needed. Wireless networks use some sort of radio frequencies (900MHz-5.8GHz for Industrial, Scientific and Medical purposes) in air to transmit and receive data instead of using some physical cables. The most admirable feature is that it eliminates the need for laying out expensive cables and maintenance cost. The advantages of wireless network are the time to deployment of wireless networks can be less. The wireless network offer more flexibility. It is easy to setup and can be extended to places which cannot be wired. There are two types in wireless networks: Infrastructure networks are fixed and wired backbone networks. Here Mobile devices or nodes communicate directly with access points. It is suitable for areas where access points can be placed. Additional cost to purchase AP hardware makes one of the disadvantage of infrastructure wireless networks . Ad-hoc network is a self arranging network of mobile nodes without any predetermined infrastructure like base stations or access points. On the basis of network connectivity each node participates in routing by forwarding data to other nodes and which nodes forward data is made dynamic throughout the network. Wireless ad-hoc network can be established in the scenarios where there is no help of wireless access or wired backbone is not feasible. Figure 1 shows the example of MANET,

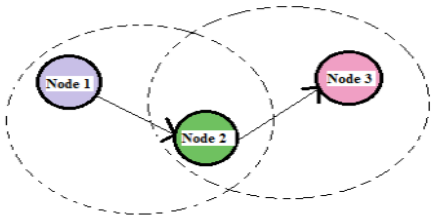

Figure 1 Example of MANET

Thus it is obvious that without any infrastructural support and with high possibility for occurrence of attacks, security in ad-hoc network becomes a great threat. While establishing a secure communication, the node must be capable to identify another node of the network. As a result, a node needs to provide its identity to another node. However, the delivered identity of the sender node needs to be authenticated and protected so that it cannot be interrogated by receiver node.

Every node wants to be sure that the delivered credentials to recipient nodes are not changed. Hence it is essential to provide security architecture to ad-hoc networking in order to ensure secure communication.

II. RELATED WORK

The concept of mobile ad-hoc networks and its security issues was carried out by many researchers. Jian-Ming Chang et al., (2015), proposed the paper "Defending against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach". In mobile ad-hoc networks (MANETs), nodes should cooperate with each other is the primary requirement for the communication to occur among nodes. This requirement may lead to serious security concerns because the presence of malevolent nodes. In this context, the launching gray hole or collaborative black hole attacks is a challenge for preventing or detecting malicious nodes. This paper resolved this issue by designing a Dynamic Source Routing (DSR) based routing mechanism, which is referred to as the Cooperative Bait Detection Scheme (CBDS) which combines the advantages of both proactive and reactive defense architectures. Reverse tracing technique is used to achieve the stated goal. Simulation results are provided, showing that in the presence of malicious-node attacks, CBDS performs better than the DSR, 2ACK, and Best-effort Fault Tolerant routing (BFTR) protocols in terms of packet delivery ratio and routing overhead.

T.C. Gayathri et al., (2015) provided the paper "Radical Health Monitoring System Using Body Sensor Network" that had dealt with Wireless Body Sensor Network (WBSN) that can observe the physiological behavior of the patient or human being. Sensors are used to collect the data and then send it to the central unit through the Local Area Network (LAN) or Metropolitan Area Network (MAN). The Biomedical Wireless Sensor (BWS) which are attached to the human body is capable of establishing wireless communication link. WBSN`s can be treated as the distributed system, here nodes are distributed on the human body. This system uses the cluster head node selection technique that chooses the best node. The reliable and efficient communication is increased between the local nodes, Wireless Local Gateway (WLG) and the Hospital Gateway (HG) for increasing the number of nodes. The implementation of automatic connection establishment improves the time delay in the system. The aim of this method is to give instantaneous and remotely accessible monitoring system. The implementation is done using the Unified Technology Learning Platform (UTLP).

Mistry et al. (2010) proposed a method that the AODV protocol consists of adding a new table known as Cmg_RREP_Tab, a new timer known as MOS_WAIT_TIME and a variable known as Mali_node. The RREP_WAIT_TIME is the time between the value of the source node that sends first RREP packet until it receives the response of the RREP control message. The Cmg_RREP_Tab stores RREP packets. The Mali_node variable records the malicious node id and discards the control messages from these nodes.

Nadeem and Howarth (2013) proposed a protectionscheme which detects and prevents attacks in MANET. The proposed technique use knowledge base for imple-menting training and testing the data . Their proposed techniqueconsists of network monitoring and data collection, training and testing modules to detectattacks. Various types of attacks were used for detecting the attacks. Rutvij et al. (2012) proposed a technique which makes use of AODV protocol to detect Black Hole attack. In this work, a dynamic node calculates a peak value for every time interval. The peak value calculates RREP sequence number, routing table sequence number and number of replies received during a particular time interval. These values are calculated for every time interval and in this way the attacks are calculated dynamically. According to their algorithm when an intermediate node receives RREP packets having higher sequence number than the peak value that node are marked as malicious node. Further the other nodes in the routing path get the details about malicious node information and isolate that vulnerable node from the network.

Wu et al. (2007) proposed a distributed and co-operative mechanism to detect collaborative attacks in MANET. Their technique consists of four phases. They are a global reaction, local detection, local data collection and a co-operative detection. The Local data collection phase consists of estimation table which containsthe information about the malicious nodes. The local detection phase is responsible fordetecting the suspicious Black Hole node in the network. If the value of the inspectionprocess is positive, the node is considered as a normal node. Otherwise, the initial detectionnode starts the detecting process and notifies it to all its one hop neighbors, who participatein the detection process. A global reaction system present in their model warns the entirenetwork about the attack.

III. NHBADI METHOD

It consists of three layers: Malicious NodeDetection Layer, Route Lookup in Network Layer and Isolation in Network layer. The input from network layer trace data is initially obtained by the malicious node detection layer from which it gets. The maliciousnode detection layer analyzes the input by initializing malicious node detection layer. Malicious node detection layer initializes Black Hole detection process by broadcasting spoofed RREQ packets. The spoofed RREQ packets wait for the reply from the neighbor nodes. If any nodes reply for this spoofed RREQ packet that node id is updated in the routing table. The route lookup layer gets the malicious node id's information from the malicious node detection layer.

The route lookup in the network layer plays the important role in verifying the malicious Black Hole node id. The route lookup layer verifies whetherthe reply is for the malicious spoofed RREQ packets. Thus the proposed technique act as Honey pot by attracting the attackers by sending spoofed RREQ packets. In this manner,the route lookup layer identifies the malicious Black Hole nodes by cross checking the routing table entry.

Finally, the Isolation in the network layer isolates the Black Hole nodeby black listing the malicious node id. Further this Black Hole node id is broadcasted throughout nodes in the network that not to communicate through the node. This is the method used for the communication through the Black Hole by which the node is prevented and the Black Hole node is isolated from the network.

The spoofed RREQ packet contains two different fields fromoriginal RREQ packets. Spoofed RREQ packet contains non existence node id and TTLvalue which is set to

1.Initially, the Black Hole detector node broadcasts the spoofed RREQ packets, and waits for the reply from neighbors. If any node replies to this message, then that node is marked as malicious node, because other valid nodes won't have the invalid DSN number in their routing table.

PARAMETERS	VALUES
Simulator	NS2.34
Simulation area (Grid size)	1400m x 1200m
No. of nodes	40
Simulation time	50s
MAC type	IEEE 802.11
Traffic type	Cbr
Mobility model	Random
Mobility speed	5 m/s
Protocol	AODV

node id is updated in the routing table. The malicious node details is updated by the the Route Lookup which is in the network layer. This layer verifies whether the reply is for non existence node id from the malicious node. Finally, the seclusion in network layer will update the Black Hole details which are in the list, and it will broadcasts it to the network and inform that not to forward packets through the malicious Black Hole node. Thus, the proposed technique acts as a Honeypot (spoofed RREQ packet).

In order to reduce the network overhead, the proposed technique uses small modification in the RREQ packet. The destination sequence number field is marked as the non-existence node id and the TTL field is marked as 1. In usual communication, the RREQ packet contains the correct destination sequence number and the TTL value. The normal AODV RREQ packet will consists of several fields such as the Destination Sequence Number(DSN) destination IP address, originator DSN, originating IP address and so on, while they are in normal routing, when anode broadcasts a RREQ, the TTL value is set up to a maximum value, because the lifetime of the active route is updated until it reaches the destination node.

The destination IP address which is the another field for which it is used to indicate the node about which route it is desired. During the normal route discovery process, a valid destination ID and a TTL are assigned to the nodes.Since whenever a node wants to transfer a packet from the source node to the destination node, the field DSN in AODV packet will check for the fresh route.

The fresh route is determined by the destination sequence number. The node which has the fresh route towards the other node will have the highest sequence number compared to that of other nodes which are in the network. So a malicious Black Hole node will exploit this feature and it will broadcast the network to which it has the highest sequence number. Hence the other nodes will forward their packets through Black Hole nodes. The proposed detection technique uses invalid DSN number which is the highest number among the nodes in the network. Hence whenever a node replies to this message that

IV. RESULTS

Algorithm steps for broadcasting malicious node id are given below:

Input: Black Hole node ids from Route Lookup module
Output: Broadcast Black Hole node id.
Step 1: Function broadcast (RTF_id)
Step 2: Begin
Step 3: for all nodes in the network {
//If the node id is the Black Hole id
Step 4: if (Detection Flag =True & Malicious node id=True)
Step 5: Broadcast (Malicious node)}
Step 6: End.

The parameters as shown in Table 1 are done on the variable settings associated by the NS2 scenario.

TABLE 1 NETWORK PARAMETERS

Control overhead refers to the resources consumed or lost in a particular process. For protocols in MANET, the overhead depends mainly on the way routes are constructed.Normalized Routing Load (or Normalized Routing Overhead) is defined as the total number of routing packet transmitted per data packet. Both are calculated from awk script.

End-to-End delay is the average time taken by a data packet from source node to destination node. It also includes about the queue which is present in data packet transmission and the delay which is caused by route discovery process. The data packets that are successfully delivered to destinations are counted. The lower value of end to end delay indicates the better performance of the protocol.

Throughput is defined as the average rate of successful delivery of packets over a communication channel from source to destination. It denotes how many data packets are received by the receiver within the data transmission time. It is represented in bits/bytes per second. Higher throughput is essential in any network.

The ratio of the number of delivered data packet to the destination is said to be the packet delivery ratio. It is used to calculate the loss rate of data packets during transmission in network and it gives the efficiency of ad-hoc routing protocols.

A higher packet delivery ratio is essential in any network.

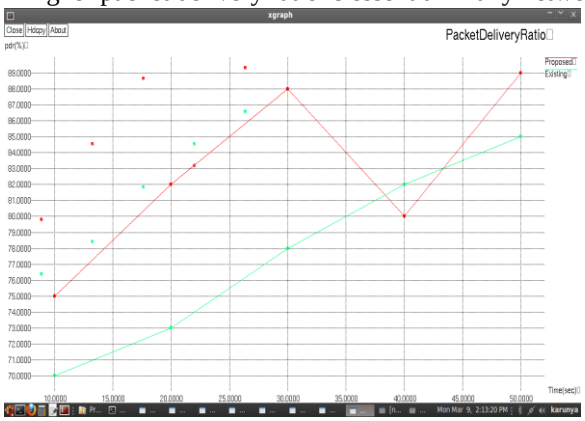

Figure 3 Packet delivery ratio

Packet drop is the total number of packets dropped during the simulation. It mainly occurs when one or more data packets travelling across a computer network fails to reach their own destination. Its impact should be less in any network. Packet Loss is however calculated using the awk script on which processes the trace file and then it produces the result.

V. CONCLUSION

In future, continuation of the work could be carried out to prevent MANET against flooding attack. SSecurity against flooding attack plays an important role in MANET for the network to be in co-operative nature and better performance. In the proposed method, CoCoWa mechanism is used to detect and find a secure route against flooding attack in ad-hoc network. Flooding attacks are serious problems that need to be addressed in wireless network security. Although significant research has been done to defend flooding attacks, with use of this method one can detect flooding nodes in wireless ad-hoc network. The malicious node detection is based on collaborative contact based watchdog (CoCoWa) and an alternate path for forwarding data packets is chosen in case of malicious node detection

VI. REFERENCES

[1] G.Vaseer, G.Ghai, and P.S. Patheja, “A novel Intrusion detection algorithm: An AODV routing protocol case study,” in Proc.2017 IEEE Int.Symp. Nano electronic and Inform.Syst., pp.111-116.

[2] S. S. Roy, D. Puthal, S. Sharma, S. P. Mohanty, and A. Y. Zomaya, “Building a sustainable Internet of Things: Energy-efficient routing using low-power sensors will meet the need,” IEEE Consum. Electron. Mag., vol. 7, no. 2, pp. 42–49, 2018

[3] M.Ficco and M.Rak, “Stealthy denial of service strategy in cloud computing” ,IEEE Trans. Cloud Computing volume 3 ,no.1, pp.80-94,2015.

[4] S.Bahl and S.K.Sharma , “Detection rate analysis for user to root attack class using correlation feature selection” in Proc.Int.Conf.Computing, communication and automation,2015,ppp.66-71.

[5] W. L. Al- Yaseen Z. A. Othman, and M. Z. A. Nazri, “Multi-level hybrid support vector machine and extreme learning machine based on modified k-means for intrusion detection system,” Expert Syst. Appl. vol. 67, pp. 296–303, Jan. 2017.

[6] K.Badran and P.Rockett, “Multi class pattern classification using single, multi dimensional feature space feature extraction evolved by multi objective genetic programming and its application to network intrusion detection “,Genetic Evolvable Mach.,vol.13,no.1,pp.33-63,2012.

[7] F.Amiri , M.R.Yousefi ,C.Lucas, A.Shakery and N.Yazdani,” Mutual information based feature selection for intrusion detection systems,” J.Network Comput. Appl.,Vol.34, no.4,pp 1184-1199,2011.

[8] S.J.Horng et al.,”A novel intrusion detection system based on hierarchical clustering and support vector machines,” Expert Syst. Appl.,vol.38, no.1,pp.306-313,2011.

[9] W.L.Al-Yaseen, Z.A.Othman, and M.Z.A. Nazri, “Multi level hybrid support vector machines and extreme learning machine based on modified k means for intrusion detection system ,” Expert Syst. Appl.,vol.67,pp.296-303,Jan.2017.

[10] [10] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, “Multi-level hybrid support vector machine and extreme learning machine based on modified k-means for intrusion detection system,” Expert Syst. Appl.,
vol. 67, pp. 296–303, Jan. 2017.