International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Eliminating Intentional Packet Dropping Attacks in MANETs Using Promiscuous Mode

Tabassum Begum[1], C. Atheeq[2], Syed Raziuddin[3], Arshad Ahmed Khan Mohammed[4]
[1, 2, 3, 4]*Department of CSE,* [1, 2, 3]*DCET,* [1, 2, 3]*Osmania University,* [4]*KL University*

Abstract*: *Mobile Ad hoc Network (MANET) is self-configuring network of mobile node connected by wireless links and considered as network without infrastructure. Routing protocol plays a crucial role for effective communication between mobile nodes and operates on the basic assumption that nodes are fully cooperative. Because of open structure and limited battery-based energy some nodes (i.e. selfish or malicious) may not cooperate correctly. After becoming part of active path, theses nodes start refusing to forward or drop data packets thereby degrades the performance of network. Traditionally, MANETs have been utilized for strategic network related applications to enhance battlefield interchanges and survivability. The dynamic idea of military operations implies it is impractical to depend on access to a fixed preplaced communication on the battlefield. Ad hoc networks display the conventional issues of wireless communication, for example, bandwidth optimization, power control, and transmission quality enhancement. Mobility, multi-hop nature, and the absence of fixed infrastructure, make various complexities and design constraints to mobile ad hoc networks. In this paper, a new reputation-based approach is proposed that deals with such routing misbehaviour and consists of detection and isolation of misbehaving nodes and packet dropping attacks. The main goal is to resolve and eliminate the attacks using Promiscuous Mode. Proposed approach can be integrated on top of any source routing protocol and based on sending acknowledgement packets and counting the number of data packets of active path.

Keywords:* *MANETs, Attacks, security, Promiscuous Mode, Mobile Nodes.

I. INTRODUCTION

MANET consists of wireless mobile nodes that form a temporary network without the aid fixed infrastructure or central administration. Nodes can communicate directly to other nodes within their transmission range. Nodes outside the transmission range are communicated via intermediate nodes such that it forms a multi-hop scenario. In multi-hop transmission, a packet is forwarded from one node to another, until it reaches the destination with the help of using routing protocol. For proper functioning of the network cooperation between nodes is required. Here cooperation refers to performing the network functions collectively by nodes for benefit of other nodes. But because of open infrastructure and mobility of nodes, noncooperation may occur which can severely degrades the performance of network.

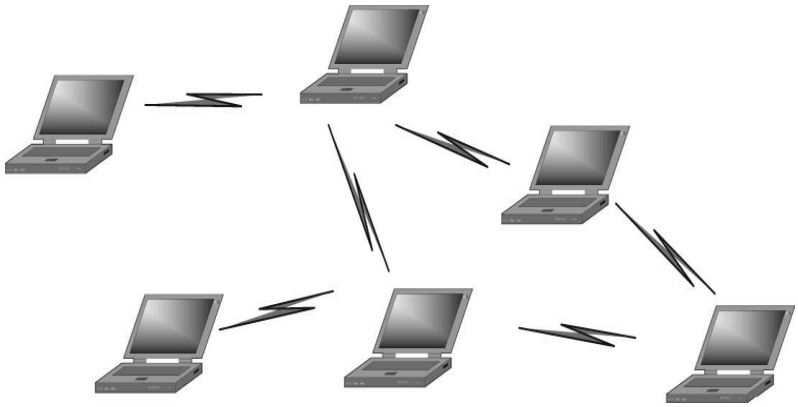

Fig:1 A Mobile Ad-hoc Network

As showed up in Figure 1, an ad hoc network may contain home-processing devices including note pads, handheld PCs, etc. Every node can communicate with various nodes that dwell inside its transmission run. For communicating with nodes that dwell past this range, the nodes needs to use moderate nodes to hand-off messages hop by hop. Henceforth, as a rule MANETs are generally called multi-hop wireless networks.

The fundamental issue with most of the routing protocols is that they trust all nodes of network and based on the assumption that nodes will behave or cooperate properly but there might be a situation where some nodes are not behaving appropriately. Most ad hoc network routing protocols becomes inefficient and shows dropped performance while dealing with large number of misbehaving nodes. Such misbehaving nodes support the flow of route discovery traffic but interrupt the data flow, causing the routing protocol to restart the route-discovery process or to select an alternative route if one is available. The newly selected routes may still include some of misbehaving nodes, and hence the new route will also fail. This process will continue until the source concludes that data cannot be further transferred. Proposed work focus on such misbehaviour for its detection and isolation from network.

MANET is vulnerable to various types of attacks because of open infrastructure, dynamic network topology, lack of central administration and limited battery-based energy of mobile nodes. These attacks can be classified as external attacks and internal attacks. Several schemes had been proposed previously that solely aimed on detection and prevention of external attacks. But most of these schemes become worthless when the malicious nodes already entered the network or some nodes in the network are compromised by attacker. Such attacks are more dangerous as these are initiated from inside the network and because of this the first defence line of network become ineffective. Since internal attacks are performed by participating malicious nodes which behave well before they are compromised therefore it becomes very difficult to detect.

We can list some of the attacks as

In a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. This mode of operation is sometimes given to a network snoop server that captures and saves all packets for analysis (for example, for monitoring network usage). In computer networking, promiscuous mode is a mode for a wired network interface controller (NIC) or wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the central processing unit (CPU) rather than passing only the frames that the controller is specifically programmed to receive. This mode is normally used for packet sniffing that takes place on a router or on a computer connected to a wired network or one being part of a wireless LAN. Interfaces are placed into promiscuous mode by software bridges also used with hardware virtualization.

The remaining part of the paper is organized as follows: section 2 makes the literature survey/Related Work, section 3 explains the proposed system and results are presented in section 4. Section 5 concludes the paper.

II. RELATED WORK

To prevent routing misbehaviour or selfishness in MANETs, various solutions have been proposed previously which can be roughly classified [13] as:

A. Secure routing-based scheme: aims at securing the establishment and maintenance of routes.
B. Credit based scheme: specifically address forwarding of packets for other nodes.
C. Reputation based scheme: aim at reactively detecting misbehaviour and proactively isolating misbehaved nodes to prevent further damage. This section briefly describes some previously proposed reputation-based schemes as proposed approach is also reputation based.

In work [1] proposed a reputation-based scheme in which two modules (i.e. watchdog and pathrater) are added on at each node. Watchdog module maintains a buffer of recently sent or forwarded data packets. Buffer is cleared only when watchdog overhears the same packet being forwarded by the next hop node over the medium and if a data packet remains in the buffer too long, the next hop neighbour is suspected to be misbehaving. Based on watchdog's suspicion, Pathrater module maintains a rating for every other node in the network and calculates a path metric by averaging the node ratings in the path and then chooses the best path. Main advantage of this scheme is that it can detect misbehaviour at the forwarding level as well as in link level. But it might not detect misbehaviour in presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehaviour and partial dropping.

In work [2] proposed CONFIDANT protocol which is based on selective altruism and Utilitarianism. In CONFIDENT, trust relationships and routing decisions are based on experienced, observed, or reported routing and forwarding behaviour of other nodes. It consists of four modules: The Monitor, the Reputation System, the Path Manager, and the Trust Manager. Each node monitors the behaviour of its next-hop node continuously and if a suspicious activity is detected, information of the suspicion is passed to the Reputation System. The Reputation System changes the rating of the suspected node which depends on how significant and how frequent the activity is and if rating of a node becomes less than certain threshold, control is passed to the Path Manager. Path

Manager then controls the route cache. Warning messages in the form alarm message are propagated to other nodes by the Trust Manager. The pitfall of CONFIDANT includes deciding the criterion for choosing threshold value is difficult. Deciding the criteria for maintaining the friends list by Trust Manager is difficult. It can also generate false ALARMS. There might be a situation where two nodes declare each other misbehaving through ALARM messages.

To prevent selfishness in MANET, in work [4] proposed a TWOACK scheme which can be implemented as an add-on to any source routing protocol. Instead of detecting particular misbehaving node, TWOACK scheme detects misbehaving link and then seeks to alleviate the problem of routing misbehaviour by notifying the routing protocol to avoid them in future routes. It is done by sending back a TWOACK packet on successful reception of every data packet, which is assigned a fixed route of two hops in the direction opposite to that of data packets. Basic drawback of this scheme includes it cannot distinguish exactly which particular node is misbehaving node. Sometime well behaving nodes became part of misbehaving link and therefore cannot be further used the network. Thus a lot of well-behaved node may be avoided by network which results in losing of well-behaved routes.

In work [6] proposed another acknowledgement-based scheme similar to TWOACK scheme, which is also integrated on top of any source routing protocols. This scheme detects the misbehaving link, eliminate it and choose the other path for transmitting the data. The main idea is to send 2ACK packet which is assigned a fixed route of two hops back in the opposite direction of the data traffic route and to reduce the additional routing overhead, a fraction of the data packets will be acknowledged via a 2ACK packet. This fraction is termed as Rack and by varying the Rack, overhead due to 2ACK packets can be dynamically tuned. This scheme also consists of multicasting method by which sender can broadcast information of misbehaving nodes so that other nodes can avoid path containing misbehaving nodes and take another path for the data transmission. Although routing overhead caused by transmission of acknowledgement packets is minimized but this scheme also suffers to detect the particular misbehaving node.

Work [7] proposed extension to the TWOACK scheme, in which each node must send back a normal Ack to its immediate source node after receipt of any kind of packet. This scheme requires an end to end Ack packet (i.e. Nack) to be sent between the source and the destination. On receipt of the data packets sent by the source, destination responds with a Nack packet. The Nack would reach the source from the destination with the help of the path, which is found in the actual message packet, delivered to the destination. If a node is found to be misbehaving in the precalculated path, the intermediate nodes are free to divert the Nack packet through alternative paths and this path will be stored in the Nack packet along with the older path, which is extracted from the original message. On receipt of the Nack packet, the source node compares the two paths that are in the Nack packet. If variation is found, then the node in the source to destination path, from where the path varies in the destination to source path is isolated and that particular node is marked as a potential misbehaving node by the source node otherwise source node concludes no potential misbehaving nodes in the path. Possible drawback includes lot of routing overhead because of Ack and Nack packets. Also due to nodes mobility probability of Nack packet reaching to source becomes smaller with the large number of intermediate nodes between source and destination.

In work [9] presented a technique to resolve black hole attack where every node observes its neighbor node by placing a cache that records the operation performed on packet with respect to its neighbor. The trust value of the neighbor node is evaluated based on the operation that the neighbor node whether it further forwards the packets that it has received. The evaluated trust value lies below the threshold, it considers the node to be malicious but the evaluation of trust value does not consider the packet dropping reason.

In [11] have proposed Enhance Black hole AODV that develops the parent nodes for identifying misbehaving nodes. When the source node sends RREQ, a timer is set up and within the expected time, the request message is received and a pseudo message is transmitted to the destiny and when the acknowledgement is received, source sends the original message. If the ACK are not received, packets are dropped. In this paper, the proper method of selecting a head node is not specified moreover delivering of pseudo packets leads overhead without considering the reason for packet dropping.

In work [12] have proposed an algorithm for moderating black hole attack in AODV protocol based on secure knowledge. It focuses the packets which are sent in promiscuous mode to guarantee that the packets are conveyed to its destiny before concluding that a particular node is black hole node, our algorithm monitors the node for packet drop reason, in this way keeping a trusted node from turning into a black hole node. But to have effectiveness of the data transmission, authentication of the nodes is also required where we can conclude that the data is being transmitted through trusted nodes in a secure route.

III. PROPOSED SYSTEM

In the proposed method, we are resolving Intentional Misbehaving Nodes using Promiscuous Mode. This Promiscuous Mode is used for resolving the different types of attacks that occur during transmission or sharing of data. It minimizes the attacks and provide security for all the nodes. The proposed model is for selecting of trusted node from the network using promiscuous mode.

A. Intentional Misbehaving Nodes

1) Black Hole Attack: Drop all data packets & cheat the source node. In computer networking, a packet drop attack or black hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. The malicious node can intentionally drop all the forwarded packets going through it (black hole). It can selectively drop the packets originated from or destined to certain nodes that it dislikes.

2) Grey Hole Attack: A grey-hole attack is extension of black-hole attack used to bluff the source and monitoring system by partial forwarding. Here, attackers utilize selective data packet dropping method to behave as genuine node and try to participate into full communication. Grey-hole malicious node participate into route discovery process and update the source route cache/ routing table as shortest path. Afterwards, source always consider malicious node as next hop node and forward packet to same. Malicious node captures all the incoming packets but drop on random basis. A special case of black hole attack dubbed grey hole attack is introduced. In this attack, the malicious node retains a portion of packets (one packet out of N received packets or one packet in a certain time window), while the rest is normally relayed. The complete phenomena create toughness against detection and prevention mechanism because harder because nodes can drop packets partially not only due to its malicious nature but also due to overload, congestion or selfish nature. Grey-hole attack may apply through two ways which are recorded underneath:

Dropping all incoming UDP packets.

Partial dropping of UDP packets with random selection process.

Grey-hole is an attack that can switch from behaving genuine to sinkhole.

Because it can act as normal node switch over to malicious node it becomes too typical to identify the state whether it us normal node or malicious node.

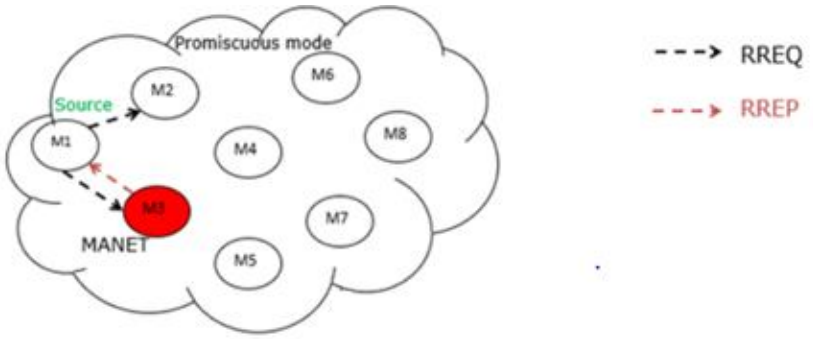

Fig:2 Identification of Misbehaving Node in MANET

B. Proposed System Algorithm:

1) Step 1: Initialize mobile nodes, fixed nodes and gateway.

2) Step 2: Assign mobile nodes battery power, transmission range and queue length.

3) Step 3: All the mobile nodes in IIM observe their neighbour nodes promiscuously.

4) Step 4: Records the behaviour of nodes based on packet operation

5) Step 5: Mobile nodes compares the neighbour nodes information about the number of packets it has received and it has transmitted.

6) Step 6: If the results are equal then the nodes are treated as trusted nodes, else if the packet dropping is intentional and reaches the threshold value then consider the nodes as misbehaviour nodes

7) Step 7: Broadcast the IP address of malicious node in the IIM notifying its misbehaviour.

C. Working of Promiscuous Mode

In this phase, each mobile node watches its neighbour nodes in promiscuous mode that the packets are being sent by its neighbours with a specific end goal to record the conduct of neighbour in regards to packet operation in the trusted knowledge table that is kept up by each node. Each mobile node contrasts the neighbour data and the data it records in its trusted knowledge table. In the event that both are same, they are named as trusted nodes which expect that the packet is sent further, else it waits for specific time period

and checks the purposes behind packet dropping. When packet dropping reaches the threshold value, then the nodes are declared malicious nodes. It is then recorded in the field M_ip_addr of trusted knowledge table and a message is broadcasted in the network announcing that the particular node is malicious and it can be refrained in the routing. Keeping in mind the end goal to affirm, the packets are delivered to its adjacent nodes, the trusted nodes screens all the packets to refrain from selective dropping, as the selected packets are dropped by untrusted nodes. Our algorithm is built on AODV routing protocol, but it can be only used in MANETs.

Following assumptions are made in the proposed scheme:

1) All nodes may work in promiscuous mode.
2) Misbehaving nodes do not drop acknowledgement packets.
3) Misbehaving nodes do not work in groups.
4) Misbehaving nodes do not send or forward false acknowledgement packet.

D. Logical grouping and Ack packet transmission

In this proposed scheme, as soon as the active route is found, all nodes of active route are logically grouped into N- sets (i.e. S1, S2,….,SN) where N=n/3 (n is number of nodes on active route) such that set S1 contains first three consecutive node, set S2 contains next three consecutive nodes and so on. For convenience we refer first nodes, middle node and last node of a set as LNode, MNode, and RNode respectively. Last set SN may contain one, two or more nodes. It behaves normally if contains three nodes. If it contains two nodes then first node act as LNode and second one as RNode. If it contains single node then that node act as RNode. The sets are grouped in a total of M = N-1 groups where two consecutive sets form a group with groups G1, G2… GM such that group GM = SN-1+SN. In a set, each RNode acknowledges its LNode by sending ACK-1 packet for successful reception of data packets. In a group, RNode of second set acknowledges LNode of its first set by sending ACK-2 packet for successful reception of data packet.

Thus, in all, each group consists of two sets and each set consists of three consecutive nodes. First node of a group receives two acknowledgement packets (i.e. ACK-1 from RNode of its first set and ACK-2 packet from RNode of its second set). For example if S→ N1→ N2→ N3→ N4→ N5→ N6→ N7→ D be the active path then the nodes of active path forms three sets (i.e. S1, S2,S3) and two groups (i.e. G1,G2) as shown below : Set S1= S→ N1→ N2 Set S2 =N3→ N4→ N5 Set S3 = N6→ N7→ D Group G1 = Set S1 + Set S2 Group G2 = Set S2 + Set S3

1) *Algorithm :* In proposed approach, each node maintains a LIST which consists of ID of every data packets sent or forwarded. After forwarding data packet to the next hop along the active route, LNode of every group will make an entry of forwarded data packet in the LIST and wait for ACK-1 and ACK-2 packet which are sent from RNode of first set and RNode of second set respectively. Also ACK-1 and ACK-2 packet must be received within the time T1 and T2 respectively. From here execution of proposed algorithm begins:

```
BEGIN For each group {
                    for each set
                    if
                   ACK-1 is not received within T1
                   Then
                   LNode observe the behavior of MNode for time T3 by rating the behavior
                  And if
                  Rating fall certain threshold TS1
                  Then
                  LNode declares its MNode as misbehaving node
                  Else
                  LNode declares its RNode as misbehaving node
          Else
         Wait for ACK-2 for T2
          End For
          If ACK-2 is not received within T2
         Then
         After T2 both MNode automatically goes to
```

promiscuous mode and start rating the behavior of their RNodes till T4
And if
Rating falls below threshold TS2
Then
MNode declares its RNode as misbehaving node
Else
LNode of second set is declared as misbehaving node
Else
LNode deletes the ID of corresponding data packet from the LIST
}
End For
END

2) Proposed approach includes following three steps:

a) Detection of malicious group: Before identifying malicious or misbehaving node, network should know whether some malicious activity is present or not. Suppose S→ N1→ N2→ N3→ N4→ N5→ N6→ N7→ D be the active route discovered by any source routing protocol (i.e. Dynamic Source Routing protocol [13]). As active route is discovered, source node S will start proposed algorithm and forms N number of sets and each set consists of three consecutive nodes (i.e. LNode, MNode and RNode respectively). LNode and RNode of any set act as temporary source and temporary destination. After forwarding data packet to next hop along the active route, each LNode makes an entry of forwarded data packet in LIST and then waits for two acknowledgement packets (i.e. ACK-1, ACK-2). If any ACK-1 or ACK-2 packet is not received within their time limit T1 and T2 respectively, that group is considered as misbehaving group.

b) Identification of particular misbehaving node: If ACK-1 is received within time T1 then LNode waits for ACK-2 else observers its MNode for time T3 by rating the behavior and if rating falls threshold TS1, LNode declares its MNode as misbehaving nodes and if not, LNode declares its RNode as misbehaving nodes and then flood this information. If ACK-2 is not received within time T2, then after time T2 both MNode of that group automatically goes into promiscuous mode and starts observing their next hop nodes (i.e. RNode) for time T4. As now both MNode are in promiscuous mode, therefore can counts the number of packets coming into and going out its RNode and when it is found that number of dropped packets exceeds threshold TS2 within time T4 then that RNode is declared as misbehaving node otherwise LNode of second set is declared as misbehaving node. Finally information of misbehaving node is flooded across the network.

c) Isolation and mitigation of misbehaving node: Each node of network maintains a LIST of misbehaving nodes. Thus upon receiving information of misbehaving nodes, each node update their LIST and avoid using detected misbehaving node for time T5. With the expiration of time T5, the entry of misbehaving node is temporarily deleted from the LIST thereby giving a chance to previously declared misbehaving nodes to be used by network again and if the same node is caught as misbehaving node more than certain number of time (i.e. TS3) then that node is permanently isolated from network.

IV.RESULTS

The proposed model is developed using NS2.34 & examined the overall performance of proposed model by comparing with the existing models. We evaluated the misbehaving nodes of proposed model with respect to number of nodes in mobile nodes of MANETs. For evaluation we have taken into account the scenario in such a manner that misbehaving nodes are compared with number of nodes in MANETs.

In the below fig:3, we have measured the misbehaving nodes of proposed system with the number of nodes. As the number of nodes increases the misbehaving nodes also increases. In this graph, the comparison of misbehaving nodes and number of nodes is shown. The proposed system gives more number of malicious nodes compared to the existing system.

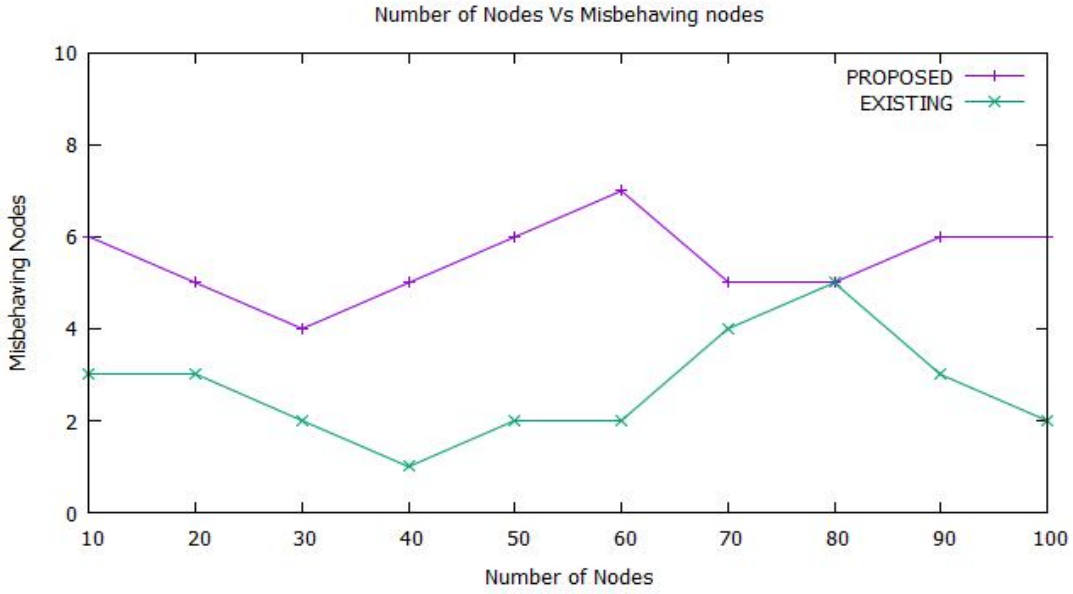

Fig:3 Comparison of Misbehaving Nodes vs Number of Nodes

The below fig:4 shows the comparison of misbehaving nodes with the pause time(sec). As the pause time(sec) increases, the misbehaving nodes also increases. In the existing system, there was less pause time(sec) for misbehaving nodes.

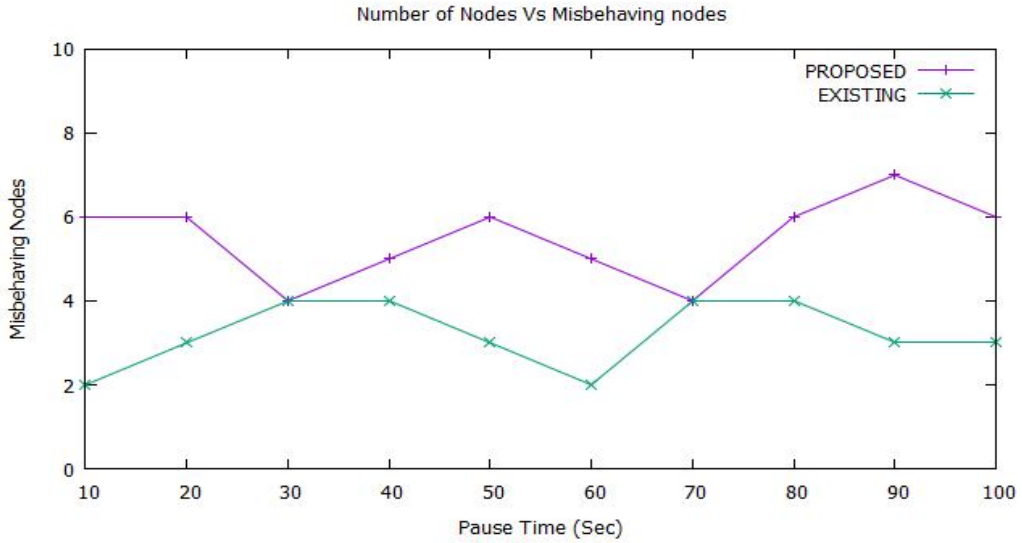

Fig:4 Comparison of Misbehaving Nodes vs Pause Time(sec)

V.CONCLUSION

Mobile Ad Hoc Network has been an active research area over the past few years, due to their widespread application in military and civilian communications. But it is also vulnerable to various types of attacks. Misbehaviour of nodes may cause severe damage, even fails whole of the network. In this paper, investigation is done on the misbehaviour of nodes and a new approach is proposed for detection and isolation of misbehaving nodes. In this paper, we have detected and eliminated the various packet dropping attacks using the promiscuous mode. This method is advantageous for misbehaving nodes. Here we are proposing the elimination of intentional packet dropping attacks using the promiscuous mode. We have seen the graphs in which the proposed system is better than the existing one. The main goal we achieved is resolving and elimination of the packet dropping attacks with the help of Promiscuous Mode.

REFERENCES

[1] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks," in Proc.of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000), August 2000, pp. 255-265.

[2] Sonja Buchegger Jean-Yves Le Boudec, "Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks" in Proc. IEEE/ACM Workshop Mobile Ad Hoc Netw. Comput. (MobiHoc 2002), June 2002, pp. 226-236.

[3] [3]Atheeq, C. and Rabbani, M., 2017. Secure Intelligence Algorithm for Data Transmission In Integrated Internet MANET. International Journal of Computer Science & Applications, 14(2).

[4] K. Balakrishnan, D. Jing and V. K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad hoc Networks," in Proc. of Wireless Communications and Networking Conference (WCNC'05), vol. 4, March 2005, pp. 21372142.

[5] Mohammad, A.A.K., Mirza, A. and Vemuru, S., 2016. Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks. Indian Journal of Science and Technology, 9(26).

[6] K.Vijaya "Secure 2Ack Routing Protocol In Mobile Ad Hoc Networks," TENCON 2008, IEEE Region 10 Conference, November 2008, pp. 1-7.

[7] S. Usha, S. Radha, "Co-operative Approach to Detect Misbehaving Nodes in MANET Using Multi-hop Acknowledgement Scheme," in 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, December 2009, pp. 576-578.

[8] Atheeq, C. and Rabbani, M.M.A., 2016. Secure Data transmission in integrated internet MANETs based on effective trusted knowledge algorithm. Indian Journal of Science and Technology, 9(47).

[9] Thachil, F. and Shet, K.C., 2012, September. A trust-based approach for AODV protocol to mitigate black hole attack in MANET. In Computing Sciences (ICCS), 2012 International Conference on (pp. 281-285). IEEE.

[10] Atheeq, C. and Rabbani, M.M.A., 2017. Mutually authenticated key agreement protocol based on chaos theory in integration of internet and MANET. International Journal of Computer Applications in Technology, 56(4), pp.309-318.

[11] Rachh, A.V., Shukla, Y.V. and Rohit, T.R., 2014. A Novel Approach for Detection of Blackhole Attacks. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN, pp.2278-0661.

[12] Siddiqua A, Sridevi K, Mohammed AA. Preventing black hole attack in MANETs using secure knowledge algorithm. In Signal Processing And Communication Engineering Systems (SPACES), International Conference on Institute of Electrical and Electronics Engineers (IEEE); 2015 Jan 2. p. 421–5.

[13] S. Zhong, J. Chen, and Y. Yang, "Sprite: A Simple, Cheat Proof, Credit- Based System for Mobile Ad-Hoc Networks," in Proc. of IEEE INFOCOM'03, March 2003, pp. 1987-1997.