Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 14, Number 4 (2018), pp. 577-589

http://www.ripublication.com

Mathematical View of Secure Routing Technique for Misbehave Node in Mobile Adhoc Network

Mr. S. RAJA

Research Scholar,
Department of Computer Science,
Rathinam College of Arts and Science,
Coimbatore.

Dr. J. THIRUMARAN

Professor,
Department of Computer Science,
Rathinam College of Arts and Science,
Coimbatore.

Abstract

In mobile ad-hoc networks, nodes act as both routers and terminals, for example, a mobile ad-hoc network set up at a conference to distribute files and discuss talks without using any wireless infrastructure that would have to be paid for the lack of routing infrastructure, the nodes have to cooperate to communicate. Cooperation at the network layer takes place at the level of routing, i.e. finding a path for a packet, and forwarding, i.e. relaying packets for other nodes.

In this work, the main solution approaches addressing the problem of misbehavior in mobile adhoc networks are secure routing, economic incentives, and detection and reputation systems. We propose "aggressive and defend based decisive routing" technique. It is a reputation system combined with detection, trust, and path management.

Keywords: Security, Routing, Node Misbehave, Technique, MANET, Aggressive and Decisive.

1. INTRODUCTION

In a MANET, nodes are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. In such networks, communication is achieved by forwarding packets via intermediate nodes on routes that link the source and the destination. Nodes in a MANET do not have a priori knowledge of the network topology.

They have to discover it. A node will find its local topology by broadcasting its presence, and listening to broadcast announcements from its neighbors. As time goes on, each node gets to know about all other nodes and finds one or more ways to reach them. End-to-end communication in a MANET does not rely on any underlying static network infrastructure but requires routing via several intermediate nodes.

Secure routing in mobile ad hoc networks (MANETs) has emerged as an important MANET research area. MANETs, by virtue of the fact that they are wireless networks, are more vulnerable to intrusion by malicious agents than wired networks. In wired networks, appropriate physical security measures, such as restriction of physical access to network infrastructures, can be used to attenuate the risk of intrusions.

Physical security measures are less effective, however, in limiting access to wireless network media. Consequently, MANETs are much more susceptible to infiltration by malicious agents. Authentication mechanisms can help to prevent unauthorized access to MANETs. However, considering the high likelihood that nodes with proper authentication credentials can be taken over by malicious entities, there are needs for security protocols that allow MANET nodes to operate in potential adversarial environments.

There are two general categories of MANET routing protocols: topology-based and position-based routing protocols. We present a brief overview of each group. Before proceeding, it is fitting to list some desirable qualitative properties of MANET routing protocols. This list is adopted from an Internet Engineering Task Force (IETF) MANET Working Group memo [10].

- **Loop-free:** It is desirable that routing protocols prevent packets from circling around in a network for arbitrary time periods.
- **Demand-based operation:** In order to utilize network energy and bandwidth more efficiently, it is desirable that MANET routing algorithms adapt to the network traffic pattern on a demand or need basis rather than maintaining routing between all nodes at all time.
- **Proactive operation:** This is the flip-side of demand-based operation. In cases where the additional latency—which demand-based operations incur—may be unacceptable, if there are adequate bandwidth and energy resources, proactive operations may be desirable in these situations.
- **"Sleep" period operation:** It may be necessary—for reasons such as the need for energy conservation—for nodes to stop transmitting or receiving signals for

arbitrary time periods. Routing protocols should be able to accommodate sleep periods without adverse consequences.

- **Security:** It is desirable that routing protocols provide security mechanisms to prohibit disruption or modification of the protocol operations.

2. PROBLEM DEFINITION

Misbehavior means aberration from normal routing and forwarding behavior. It arises for several reasons. When a node is faulty, its erratic behavior can deviate from the protocol and thus produce non intentional misbehavior. Intentional misbehavior aims at providing an advantage for the misbehaving node.

Without appropriate countermeasures, the effects of misbehavior have been shown to dramatically decrease network performance. Depending on the proportion of misbehaving nodes and their specific strategies, network throughput can be severely degraded, packet loss increases, nodes can be denied service, and the network can be partitioned. These detrimental effects of misbehavior can endanger the functioning of the entire network.

3. RELATED WORK

In wireless sensor networks "Misbehavior" refers to node that does not behave in proper way and has an abnormal behavior. In other words, if behavior of node deviates from its specification or set of behaviors then the node is said to be misbehaving [1]. Misbehavior takes place in following ways:

- Delay Packets
- Drop Acknowledgements
- Delay Acknowledgements
- Drop packets and modify routing information
- Don't forward packet to save its own resources
- Forward control packets while dropping data packets

There can be various types of misbehaviors [1]. In this section we survey different techniques to detect misbehaving nodes in network.

Buttayan and Hubaux [2] introduced a virtual currency method called Nuglets. In this technique a node has to pay other node for forwarding its packet. This requirement makes all the nodes interested in forwarding other nodes packet as they also need nuglets to forward their data packets. Payment of nuglets is either done by source node or destination node.

Zhong and Yang [3] proposed an incentive based mechanism called Sprite. In this a node collects receipt for each forwarded packet. The receipt is nothing but the hash of the packet. To provide fairness in the network it has a central monitoring mechanism

called credit clearance service. All the nodes send their receipt to the CCS. The CCS is responsible for providing credit to the nodes. The main disadvantage with this method is that the CCS can become a source of bottleneck.

Marti [4] proposed watchdog/Pathrater model in which overhearing technique is used to identify misbehaving nodes. When a node forwards a packet, it observes the next node to find whether it forwards the packet or not. A node is considered as misbehaving if it does not forward the packet. The misbehaving counter is incremented each time misbehavior is detected.

Michiardi and Molva [5] proposed Core, which uses a different reputation mechanism. It calculates a combined reputation rating. This rating is formed by direct observation, indirect observation and task specific behavior.

He and Dapeng Wu [6] proposed Sori, which also rely on watchdog mechanism. It also relies on both direct observation and second hand information. Each node maintains a neighborhood list which contains the number of packets received and forwarded by each neighbor. It also punishes the nodes which are considered misbehaving.

S. Subramaniyan and W. Johnson [7] proposed a reputation based scheme to detect selfish nodes. Technique is known as Record and Trust Based Detection Technique. This technique analyzes detection of selfish node during routing and packet dropping. Selfish node is verified for data packet drop and then checked for false reporting.

M. S. Alnaghes and F. Gebali [8] present a survey of the dif-ferent Intrusion Detection Systems (IDSs) that are proposed for MANETs. It also covers comparison of each IDS including their advantages and disadvantages. Paper discusses three types of IDS namely, Anomaly-based IDS, signature-based IDS and Specification-based IDS. As it is clear, it is difficult to build a completely secure MANET system in spite of using a complex cryptographic technique or secured routing proto-cols.

Sumiti and S. Mittal [9] proposed a distributed agent based technique for detection of passive path selfish node in mobile network. Several intrusion detection systems have been pro-posed to find out misbehaving nodes in MANETs, which are classified into three categories, Credit Based System, Reputation Based System and Acknowledgement Based System. This paper also discusses different techniques to detect misbehavior of node.

4. AGGRESSIVE AND DEFEND BASED DECISIVE ROUTING

In the previous work they propose and implement, new IDS named Secure ACK. The system is proposed to overcome drawbacks of Watchdog and TWOACK stated before. Secure ACK system is purely an acknowledgement based technique. It is based on Enhanced Adaptive Acknowledgement (EAACK) system [10], but includes enhancement in a key technique for detection of misbehaving node present in network. The type of misbehaviour to be detected by proposed system is about packet delay or acknowledgement delay. It detects this malicious activity in the network

within very less time and stops data transmission, so the misbehaving node will not be able to damage the network thereafter.

The shortage of possessions makes it cautiously logical for nodes to disobey to preserve their properties which make safe directing difficult to accomplish. To ensure secure routing a technique is required to disappoint misbehaviour and conserve the collaboration in the network. The proposed scheme employs a Distributed aggressive model at each node for augmenting the security of the network. Accompanying information concerning misbehaviour in the network is moderately disseminated between the nodes during route establishment which is used as a cautionary measure to ensure secure routing. The offered outline considers the real world scenario where a node may demonstration dissimilar kinds of misbehaviour at different times. Thus, it provides an aggressive resolution construction technique to deal with nodes presenting fluctuating misbehaviours in accordance to their severity.

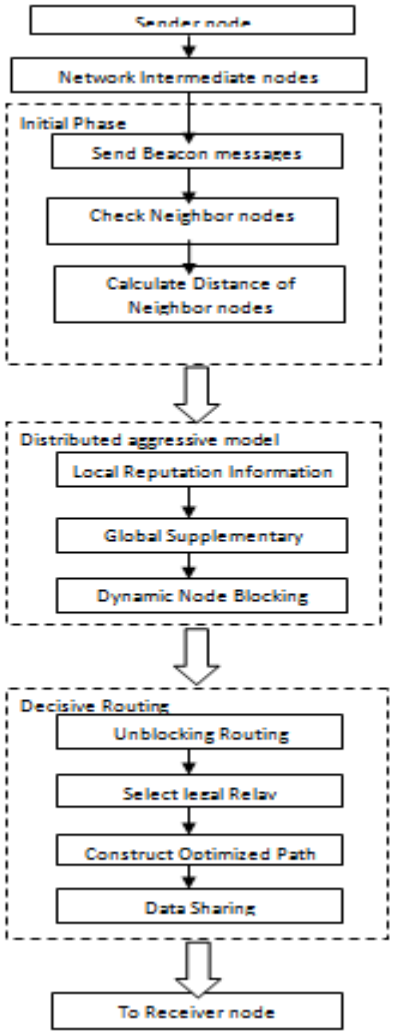

Figure 1: Proposed Architecture

Since our system mainly detects routing misbehavior in mobile ad-hoc networks. Here the role and responsibility of mobile nodes is very important. By using routing protocols the mobile nodes continuously communicating with other nodes and involves in detection of misbehavior of nodes and mitigation. According to this information the following actors are involved in this system.

1. Source node

2. Destination node

3. Intermediate node

Source node Here source node is a node which may be a computer or mobile device or any router which tries to communicate with destination node and involves in detecting routing misbehavior, routing traffic before forwarding packets (data traffic) to the next node in a path to destination.

Destination node It is also either a computer or mobile device or any router which is sending feedback, acknowledgement with communication from source node before receiving data packets and after receiving data packets.

Intermediate node Intermediate node is an observer node or router in between source node and destination node. In general it receives the data packet from source node and forwards it to other nodes towards the destination. Sometimes it may not forward the data packet due to selfishness.

4.1. Neighbourhood Analysis Phase

This module monitors the neighborhood behavior by promiscuous listing the neighbor traffic. The Retaliation process runs on each node for getting information about the neighborhood. It stores the behavior information into a table; NI table (Neighborhood Information Table). This table contains a unique entry for each node of the neighborhood. Nodes have to update the NPRF and

NPF values on the basis of number of packets received for forwarding and number of packets forwarded. The schema of the NI table is given below:

NI (IP, NPRF, NPF, G, BP)

Where

IP : Internet Protocol Address

NPRF : No of Packet Received for Forwarding

NPF : No of Packets Forwarded

G : Grade

BP : Bonus Points

The NPRF and NPF values will be subsequently updated by overhearing the

neighbors on the basis of number of packets received for forwarding and number of packets forwarded.

4.2. Distributed Aggressive Model

After updating the NI table for the threshold time in the promiscuous listening mode, every node has to process the NI table. At first a node calculates the PFR values for its neighbors and broadcast it along with the IP Address to its neighbors. The formula to calculate the PFR is

PFR = No of Packet Forwarded / No of Packet Received for Forwarding

Similarly every node broadcasts its neighbors IP and PFR that will be accepted and filtered (only neighbor information) by the node. This information is kept in a Temp table which is defined as follows.

IT (IP, PFR, G, BP)

Where PFR and BP are multivalued attributes, it stores PFR and BP values received from its neighbors. First of all a node writes its own PFR value in the PFR cell and then it appends this field by the received PFR values from its neighbors.

Step 1: - Calculating mean for PFR

$$G_i = \sum_{k=1}^{n} PFR_k / n$$

Step 2: - Assigning Local Bonus Point

$$LBP_i = 2^{(MG_i * 10)}$$

Then the mean value of the LBP is calculated that will decide how many packets will be dropped by an honest node against a selfish node in spite of its misbehavior/packet drops. We have calculated the mean value for the LBP cell to make BP value consistent in a neighborhood.

4.3. Decisive Routing

In this model inclusion of a new node is very simple, the NPRF, NPF, and BP values are initialized to zero and G is initialized with one. The zero values in the given fields indicate a fresh start of the node in network activities and the value one indicates that our model assumes an unknown node is honest. The NPF and NPRF values will be subsequently updated in protected mode by overhearing the neighbors on the basis of the number of packets forwarded or received for forwarding.

In SAODV, whenever a source node needs a route to a destination node, it floods the network with route request RREQ packets. An intermediate node has to reply if it knows a fresh route to the destination, otherwise it propagates the request and nodes

update their routing table with a reverse route to the source. When the RREQ reaches the destination, destination replies by sending a RREP towards the source with the reverse route. In the process of route maintenance, upon detecting a link break, a node sends RERR with the active route(s) towards the source(s).

We can combine this with our scheme, by the involvement of G and BP values. A node needs to check the Grade and Bonus Points whenever it gets any RREQ packet. It can drop the BP amount of RREQ packets of the misbehaved nodes. During route reply and maintenance the same punishment strategy can be applied. The source can exclude low grade nodes to initiate a new route request. Similarly, if selfish node has to send a RREQ, then it has to spend more energy because its packet has been dropped by its neighbor till BP reaches zero.

5. PERFORMANCE EVALUATION

Our simulation contains 30 nodes scattered on a 800X800 meter flat space for data transfer. This space makes the maximum hops to be 3. The physical layer and 802.11 MAC layer are included in the wireless extensions of NS2. Table 1, shows the other simulation parameters. UDP traffic with constant bit rate (CBR) is used with packet size of 512 bytes and data rate of 4 packets per second. Each data point was obtained by running the simulation 10 times with different seed numbers and taking the average value of the results. The misbehaving nodes population varies from 0% to 40% with 10% increments. The smart attackers' number is set to a constant percentage of 40% from the total number of misbehaving nodes.

Table 1: Simulation Parameters

Parameter	Value
No. of Nodes	23
Simulation Area	800 mtr X 800 mtr
Simulation time	10 sec
Mobility Model	Fixed
Traffic Type	CBR
Packet Size	512 bytes
Routing Protocol	SAODV

A selfish node only communicates to other nodes if its data packet is required to send to some other node and refuses to cooperate other nodes whenever it some data packets or routing packets are received by it that it has no interest in. Hence data packets are either refused to retransmit or are dropped for being received by a selfish node.

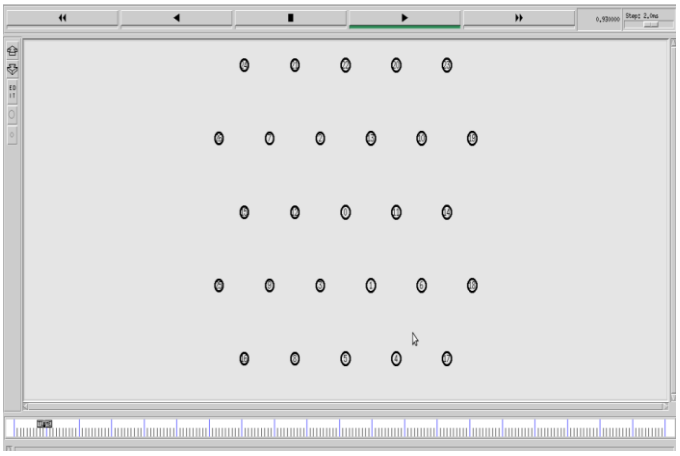

Figure 2: Total No. of Nodes in Simulation

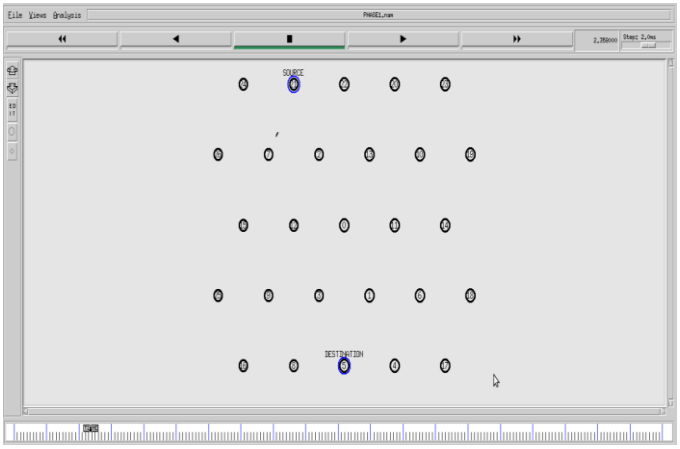

Figure 2: Defining Source & Destination Nodes

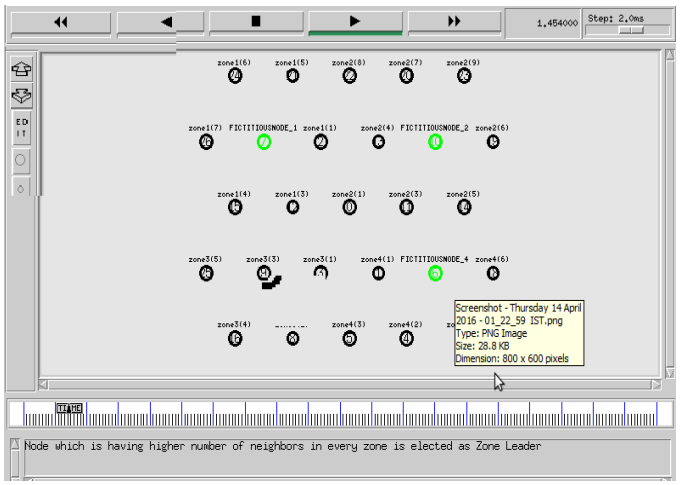

Figure 4: Misbehaving or Fictitious Node

These following metrics are used to evaluate the performance of IIDS for existing and proposed technique which are defined as follows:

Packet Delivery Ratio: -

It is the ratio of the total number of received packets at the destination to the total number of sent packets by the source.

PDR = Received Packets at Destinations / Sent packets by Sources

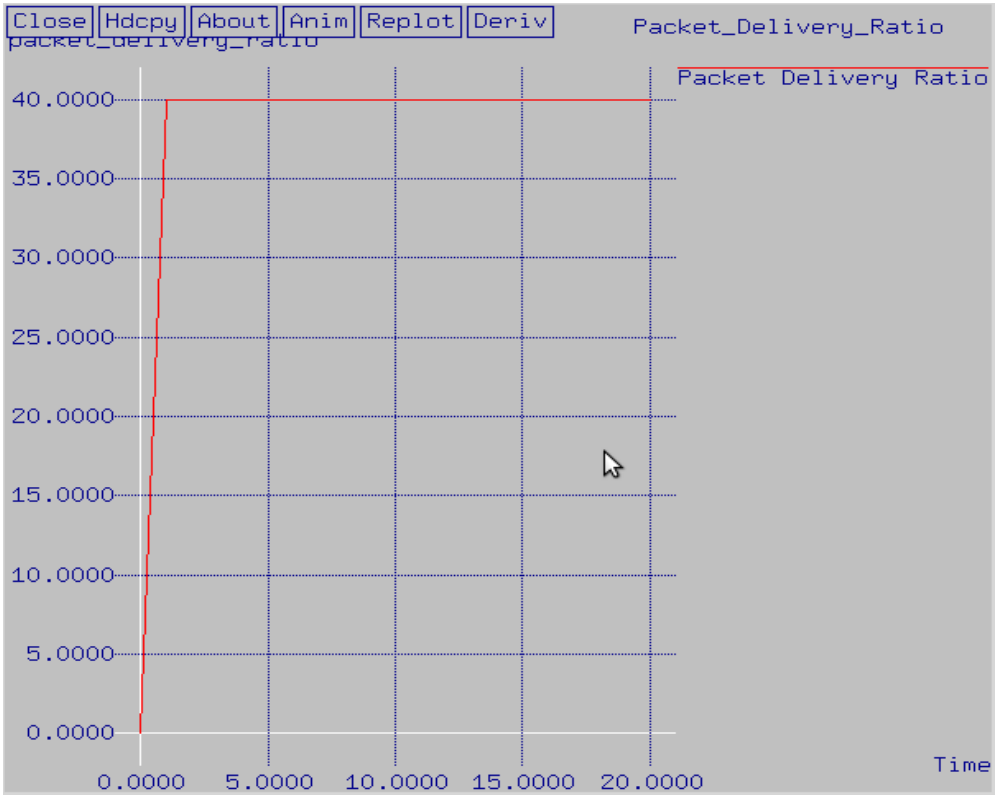

Figure 5: Packet Delivery Ratio

Average Delay: -

The average end-to-end delay for all successfully received packets at the destination. It is calculated for each data packet b subtracting the sending time of the packet from the received time at final destination. Then the average represents the AED.

Average Delay = $T_{reveived} - T_{sent}$ / N

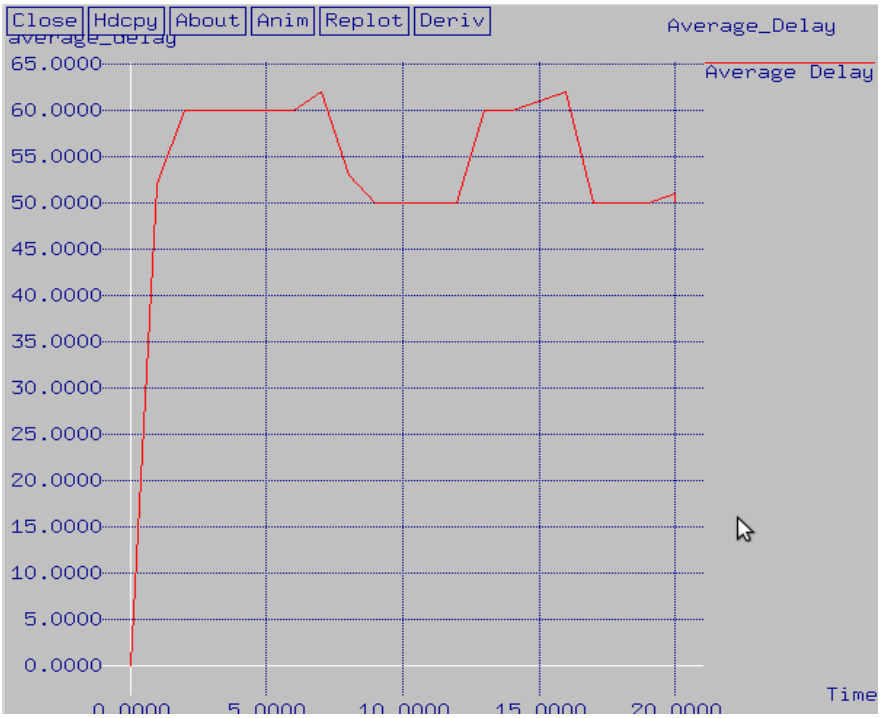

Figure 6: Average Delay

6. CONCLUSION

Mobile Ad Hoc Networks (MANETs) have been an area for active research over the past few years, due to their potentially widespread application in military and civilian communications. Such a network is highly dependent on the cooperation of all its members to perform networking functions. This makes it highly vulnerable to selfish nodes. One such misbehavior is related to routing. When such misbehaving nodes participate in the Route Discovery phase but refuse to forward the data packets, routing performance may be degraded severely.

In this paper, we have investigated the performance degradation caused by such selfish (misbehaving) nodes in MANETs. In this work, we have focused only on link misbehavior. It is more difficult to decide the behavior of a single node. This is mainly due to the fact that communication takes place between two nodes, and is not the sole effort of a single node. Therefore, care must be taken before punishing any node associated with the misbehaving links. When a link misbehaves, either of the two nodes associated with the link may be misbehaving. In order to decide the behavior of a node and punish it, we may need to check the behavior of links around that node.

REFERENCES

[1] I. Hatware, A. Kathole, M. Bompilwar "Detection of Misbehaving Nodes in Ad Hoc Routing," *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, Feb. 2012.

[2] Buttyan, L. and Hubaux, J.2002 .Stimulating

cooperation in self-organizing mobile ad hoc

networks. Mobile Networks and Applications, vol. 8: 579–592.

[3] Zhong, S., Chen, J. and Yang, Y. 2003. Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks. *INFOCOM 2003.Twenty-Second Annual Joint Conference of the IEEE Computer and*

Communications vol.3 :1987 – 1997

[4] Marti, S.,Giuli, T.J., Lai, K. and Baker , M. 2000. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks .*In: Proc.* International conference on mobile computing and networking (*MobiCom).*

[5] Michiardi, P. and Molva, R. 2002 .CORE: A

collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. *Communication and Multimedia Security Conference 2002*.

[6] Qi, H., Wu , O.D. and Khosla ,P. 2004. SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks. *IEEE Wireless Communications and Networking Conference* vol. 2: 825-830.

[7] S. Subramaniyan, W. Johnson and K. Subramaniyan "A Distributed Framework for Detecting Selfish Nodes in MANET using Record- and Trust-Based Detection (RTBD) Technique," *EURASIP Journal on Wireless Communications and Networking*, Springer, 2014.

[8] M. S. Alnaghes and F. Gebali "A Survey on Some Currently Existing Intrusion Detection Systems for Mobile Ad Hoc Networks*," In Proceedings of Second International Conference on Electrical and Electronics Engineering*, Clean Energy and Green Computing, Konya, Turkey, 2015.

[9] Sumiti, S. Mittal "Identification Technique for All Passive Selfish Node Attacks in a Mobile Network," *International Journal of Advance Re-search in Computer Science and Management Studies*, vol. 3, Issue 4, Apr. 2015.

[10] E. M. Shakshuki, Nan Kang and T. R. Sheltani, "EAACK – A Secure Intrusion Detection System for MANETs," IEEE Transactions on Industrial Electronics, vol. 60, no. 3, March 2013.

[11] I. Hatware, A. Kathole and M. Bompilwar, "Detection of Misbehaving Nodes in Ad Hoc Routing," International Journal of Emerging Technology and Advanced Engineering, vol. 2, February 2012.

[12] Rasika Mali and Sudhir Bagade, "Techniques for Detection of Misbehaving

Nodes in MANET: A Study," International Journal of Scientific & Engineering Research, vol. 6, Issue 8, August 2015.

[13] Md. Amir Khusru Akhtar and G. Sahoo, "A Novel Methodology for Securing Adhoc Network by Friendly Group Model", The Fourth International Conference on Networks & Communications (NetCoM) Chennai, LNEE, Springer, Sep, 2012.

[14] Molva, R., and P. Michiardi. "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks." Institute Eurecom-Research Report RR-02-062 (2001).

[15] Koshti, Dipali, and Supriya Kamoji. "Comparative study of Techniques used for Detection of Sel_sh Nodes in Mobile Ad hoc Networks." International Journal of Soft Computing and Engineering (IJSCE) ISSN (2011): 2231-2307.

[16] Gupta, Shailender, C. K. Nagpal, and Charu Singla. "IMPACT OF SELFISH NODE CONCENTRATION IN MANETS." International Journal of Wireless and Mobile Networks 3.2 (2011).