J. Basic. Appl. Sci. Res., 4(8)26-35, 2014

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Impact Analysis and a Detection Method for Misbehaving Nodes in Mobile Ad-hoc Networks

Saeed Azfar*, Adnan Nadeem, Kamran Ahsan, Muhammad Sarim

Department of Computer Science, Federal Urdu University of Arts, Sciences and Technology, Karachi, PAKISTAN

Received: April 4, 2014
Accepted: June 30, 2014

ABSTRACT

Mobile Ad hoc Networks are one of the fast growing self organized networks, which has application in wider domains such as crisis management, battlefield, personal networking. However, due to cooperative nature of the network MANETs are vulnerable to various types of misbehaviour from both legitimate and malicious users. It is tricky to distinguish clearly between the normal behaviour and misbehaviour. Create a difference in those legal and illegal users are much difficult as we imagine. Mobility and flexibility are major advantages but presence of misbehaviour of nodes is one of the key factors of network performance degradation. In this paper, we first review and categorize possible misbehaviours in MANETs. We have also illustrated specific type of misbehaviours in this paper. We analyze the impact of misbehaving nodes on the network performance using a simulation based case study. Simulation results show the impact of misrouting and selfish misbehaviours of nodes by indicating the effect on throughput, packet delivery ratio and control packet overhead. Finally, we proposed a technique to locate, monitor and prevention of nodes from misrouting misbehaviour.

KEYWORDS: Mobile ad hoc Network, Detection Techniques, Misbehaviour of Nodes, Performance Analysis.

1. INTRODUCTION

The ad-hoc network is a "peer to peer network characterized by communication between nodes without the need for an infrastructure" according to Wireless design glossary. Similarly ad hoc term is accurately described in oxford advanced learner "arrange or happening when necessary and not planned in advance". Everywhere this ad hoc word is used temporarily or not planned but we want to use it permanently and design a good plan for deployments of Mobile Ad hoc Network (MANET) in future. The MANET is an infrastructure-less network & does not rely on the centralize nodes such as routers, AP's and Gateway nodes. Every node performs routing and acts like gateways itself for its own data packets. The complete network is moving from one location to another and coverage area of a MANET depends on the numbers of hosts in the area, their motion and their per host communication range. MANET can establish extreme flexibly with minimal configurations, quick deployments and absence of central governing authority. Due to this, it is suitable for emergencies such as natural disasters, military applications or battlefields, and in some industrial and commercial applications. [1]

Routing and Security are two major concern needs to be addressed in MANET; both areas are still wide opened for researchers for further research. Issues associate with routings are Links change very frequently, packet losses and transmission errors due to moving nodes, distributed channel access, difficulty in avoiding packet collision and supports QoS, security threats like Non cooperating nodes, packet dropping, lying nodes intentionally or un intentionally playing a vital role and necessity of power efficient protocols and better power managements techniques. Routing is entirely different from fixed networks because of decentralized architecture. In [2] Hong et al. presented three major types of routing exist in MANET. Flat routing (Proactive and reactive), Hierarchical routing and Geographic position assisted routing.

MANETs are more vulnerable to security threads than fixed networks, specifically due their cooperative nature of operations. Security is also an important challenge for MANET and need extra attention. Inadequacy in power source with multi hop environment of MANET causes a new type of exposure, which does not exist in traditional networks. It is called misbehaviour of node. Misbehaviours of nodes could cause severe degradation of the network performance. Therefore, It has attracted many researchers to define, discover and proposed mechanism to deal with misbehaving nodes to maintain the desirable performance of the network. One of the major types of misbehaviours is packet dropping which has been the prime focus of researchers, in contrast in this paper we have focus on misrouting and selfishness. In this paper we have first review, classify and illustrate some of the major misbehaviour in MANETs. Then, we analyze the impact of misrouting and selfish behaviours on MANET performance and finally propose a method to detect misrouting misbehaviour.

The article is structured as follows; in next section, we review, classify and illustrate the possible misbehaviours which exist in MANETs based on the literature and our own observations. In section III we present review of proposed mechanisms and techniques for various misbehaviours. In section IV we present we analyze the impact of certain misbehaviours in MANETs through a simulation based case study. We propose prevention against misrouting misbehaviour in section V and finally, summarize our work in section VI.

II. MISBEHAVIOURS IN MANET

Misbehaviour of nodes in MANET is an important problem and this could cause severe degradation on the network performance. Figure 1 shows our misbehaviour classification in MANETs. A node could misbehave by not forwarding data

***Corresponding Author:** Saeed Azfar, Dept. of Computer Science, Federal Urdu University of Arts, Science and Technology, Karachi. saeed.azfar@fuuast.edu.pk, Phone: +923002576613

packets of other nodes or misbehave in performing routing operations and these are two major types of misbehaviours. In these two categorize there are various misbehaviours possible. For example, 'selfishness', refuse to forward packets while 'malicious' launch different types of attacks and generate false reporting.

Selective and complete dropping of packets and misroute packets are part of Packet forwarding Misbehaviour. Route capturing, false reporting, not being part of any route and tunnelling are part of Routing Misbehaviour. We will now illustrate misrouting misbehaviour of nodes in MANETs.

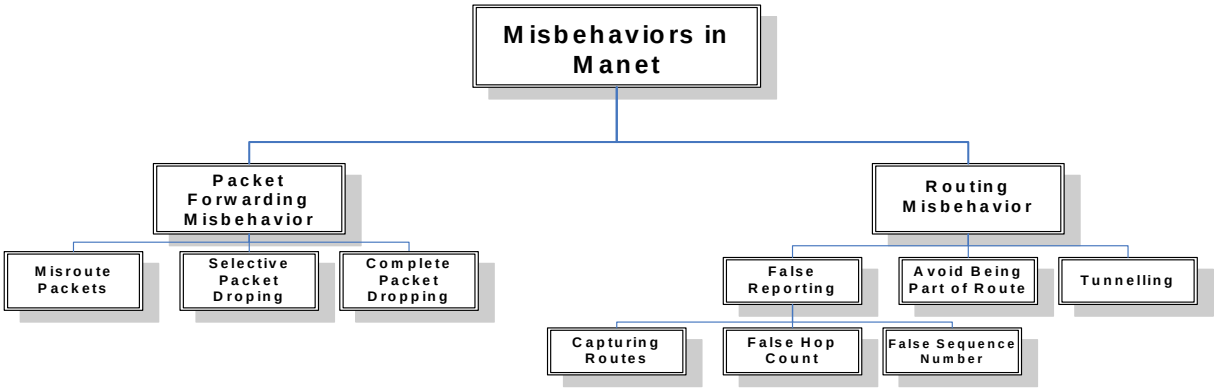

Figure 1. **Misbehavior Classification in MANET.**

A. Packet Forwarding Misbehaviour

Misrouting packets is defined by authors in [3][4]. In misrouting a malicious node can drops as well as misroutes packets to some other paths instead of actual destination. Figure 2 illustrate those node G misroute packets which are originally destined for node I.

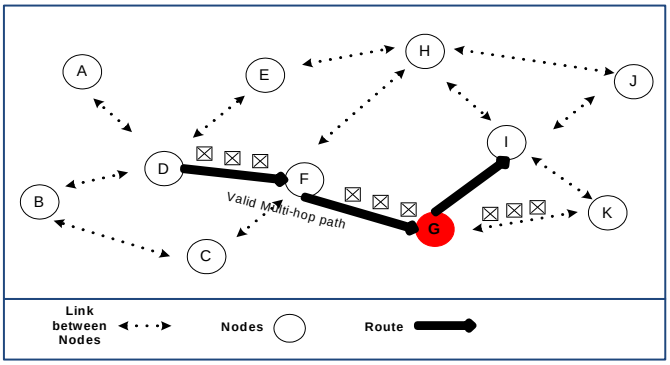

Figure 2. **Node G misroute packets.**

Complete dropping of packets cause Black hole attack in MANET defined by authors in [5]. Figure 3 Illustrate complete packets dropping. The node drop all packet to cause the BH attack in the network similarly in [6] Grey hole attack, the node either drop packets selectively for specific nodes or drops packets probabilistically or in specific pattern [17].

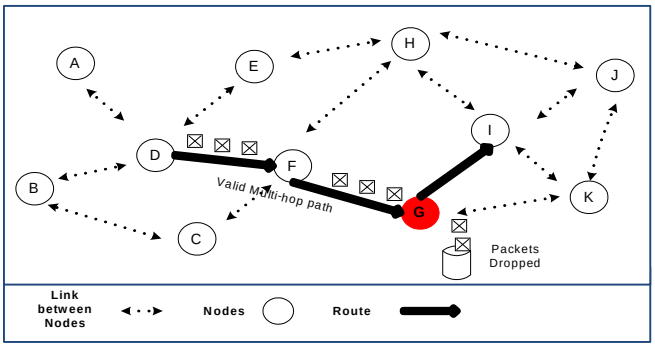

Figure 3. **Node G drops packets completely.**

Figure 4 Illustrate that node G drops packet which is for node K and forward packets which are for other node I.

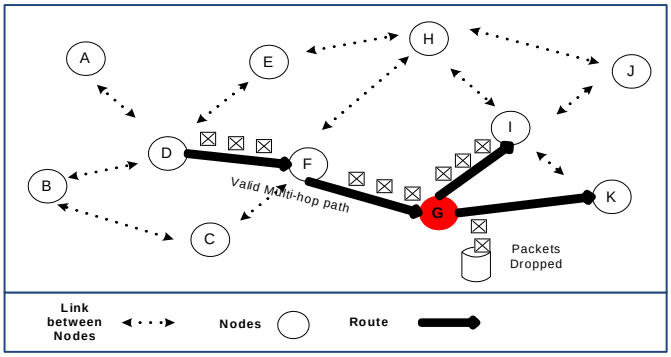

Figure 4. **Example of Selective Packet Dropping.**

B. Routing Misbehaviours

In [1], Authors explains how false reporting of malicious nodes could cause redirection of network traffic by varying some control field of message header for examples sequence numbers. In AODV, any node may reroute traffic through himself by advertising a fake route to a node with a destination sequence number better than the genuine value. Similarly, false reporting of malicious node also alter hop count field in packet header for shortest path. Tunnelling attacks are also a security loop hole in multi path routing. In which two or more than two nodes might collude to encapsulate massage among them.

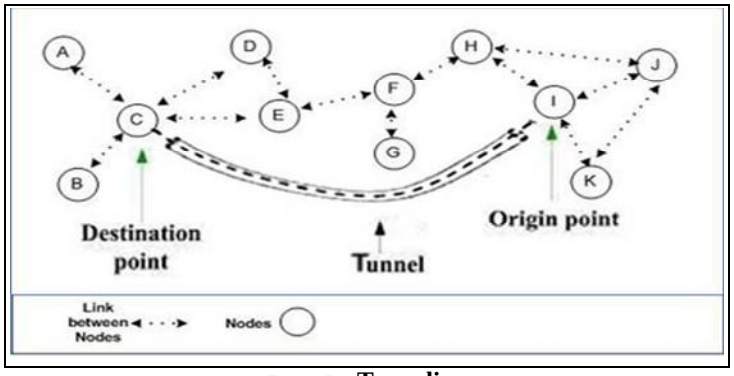

Figure 5. **Tunneling**

In [7], authors describe that nodes due to their limited resources or to conserve their resource does not participate in route discovery operations in the network. Some times their intentions are to avoid being part of any route. This could also be considered as misbehaviour.

In [2], when the node sends a route request and intruder advertise himself as having fresh route in an attempt to become part of every route and capture most of the route in the network. Then choose an intermediate node to drop packets instead of forwarding them.

There are some reasons due to which misbehaviour of nodes occurs. Over loaded nodes lacks available network resource to forward packets. Malicious node can be launched a DoS attack by sinking packets which are must be forwarded by itself. A selfish node is reluctant to waste their power source or existing network resources to forward data or control packets which are not direct concern to it: although they hope others to forward packets on its behalf. Broken node might have very frequent broken links and does not find link availability every time when other nodes required due to their mobility.

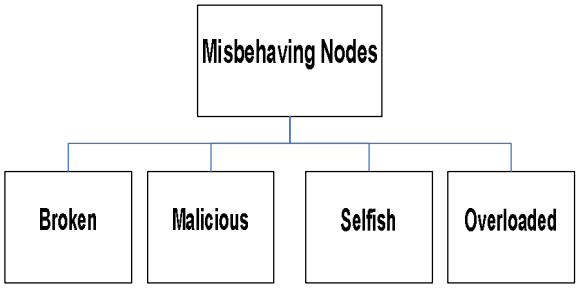

Figure 6. **Reasons for Misbehaviors**

Cooperation of nodes entirely depends upon MANET application like in battlefield nodes belongs to a single authority so their cooperation is legitimate and necessary due to common goal. But in commercial applications nodes do not feel right to a dissimilar management & couldn't be a similar target for communication. Figure 6, highlights the major reasons for nodes misbehaviours in MANETs.

III. OVERVIEW OF PROPOSED MECHANISMS

In this part of the paper we will review and present different proposed mechanisms from existing literature and analyze the research work of different authors what, why and how they develop and proposed their technique for dealing with misbehaviours.

Miciardi and Molva proposed in [8], a collaborative reputation mechanism to enforce node cooperation (CORE). In this article, authors proposed a reputation based selfish node detection system with a mechanism to enforce nodes to cooperate in what they suppose to do. Reputation scheme is totally based on past status which is zero at initially. Three types of reputation used first one is subjective in which reputation calculated directly from a subject's observation, second is Indirect, in which reputation of a subject measured by other society member and third is functional, both subjective and indirect reputation calculated with respect to different function. The protocol nature on which relies guarantee that if a provider is refuses to cooperate then the CORE scheme will react by decreasing the reputation of the provider and may face exclusion if the selfish behaviour persists. Dynamic source routing protocol was base protocol and the basic application of this scheme is applied on route discovery function in DSR.

Buchegger and Le Boudec proposed in [9], Protocol CONFIDANT, some peoples suggest that it is an expansion of DSR protocol which actually makes misbehaviour unpleasant, It uses basically same techniques which is very much similar to watchdog. It is consist of four components. It collects and process its own observation and secondly handle reports from trusted node, if any suspicious event is found and occur very frequently then it reports to reputation system of protocol and if threshold exceeded then reputation system update rating of nodes. In last Trust manager sends an alarms to warn other nodes those are still think selfish nodes as their associates yet.

Bansal and Mary proposed in [10], a protocol which is called Observation based Cooperation Enforcement in Ad hoc Network (OCEAN), which also works as an expansion of DSR and it be located in between network and MAC layer that helps nodes to make smart routing or forwarding decisions. OCEAN uses a monitoring and reputation mechanism and totally depends on his own scrutiny. OCEAN classified routing misbehaviour into Misleading and selfish classes. After monitoring results of its own, either can be negative or may be positive it update neighbour rating according to monitoring results & if rating become lower than threshold value node should be added in faulty list. In last every packet from faulty node will be rejected as a punishment.

Medidis and Richard proposed in [11] Unobtrusive Monitoring Technique (UMT) to find nasty and faulty nodes those making some criminal activities like misrouting and packets dropping. The UMT collect and analyze data which is locally available like route error, request error message, ICMP time out messages which include destination unreachable messages & other official routing messages to detect misbehaviour. In case of TCP timeout occurs, the monitoring daemon first checks if is there are any route error messages indicating that link were broken and absence of route error message the flag is raised and shows that there must be malicious activity. In other case of misrouting, when a node receives a packet and does not find himself in the source route he may drops the packet and sends an ICMP destination unreachable back to the source, in last monitoring daemon repeats the same like packet dropping.

J. Zhen and S. Srinivas proposed in [12], Round Trip Time (RTT) technique which is used to detect tunnel between 2 nodes. A node say A calculate RTT with another node say B sending a message to B requiring an immediate reply from B. The RTT between A and B is the time between A's sending the request message and receiving the reply message from B. In this mechanism each node called N will compute the RTT between N and all N's neighbours. RTT between two fake neighbours is always higher than two real neighbours so by comparing these RTT between a node and its neighbour, node A can recognize both real and fake neighbours. Method is much easy to implement among all other techniques.

Manvi, Bhajantri and V.K. Vagga proposed in [13], an acknowledgement based scheme to deal with routing misbehaviour and ensure confidentiality of data. This technique relies on the 2-hop acknowledgement to ensure the successful data packet delivery. If receiving time is higher than the wait time and the original message contents are not altered by intermediate node. Then it inform sender about misbehaviour in this link. A different system model also proposed with this scheme along with its algorithm. Simulation also conducted with C language and used 5 parameters to measure performance of this scheme.

Wu and Kholsa proposed in [14], A Secure and objective reputation based Incentive Scheme (SORI) for MANET which mainly focused in detection of packet forwarding misbehaviour. Scheme Consist of three components: neighbours monitoring, reputation propagation with punishments. Each neighbour forwarding function is linked with two parameters Request for forwarding and Has Forwarded. An Evaluation Record is created using the values of RFn(x) and HFn(x) which represent the confidence metrics. The trustworthiness of x depends on higher the packet transmitted to x for forwarding. Exchange information about reputation only with close neighbours. Non cooperative node will be punished by its entire neighbour. Nodes periodically update LERn(x) and the respective value of its neighbour to calculate Overall Evaluation Record. Evaluation record value is lower than a predefined threshold; node n takes punishment, some relaxation of nodes those do not intentionally drop packets.

Rajaram and Gopinath proposed in [15], A Mobility Oriented Trust System (MOTS), It define and uses trust table to favour packets forwarding by maintaining a trust vector. A node is reprimanded or satisfied by lessening or raising the trust vector. In MOTS dynamically calculating the nodes trust vector values, the source node freedom to select the much trusted routes rather than by default shorter routes. It marks misbehaviour nodes and may isolate suspect nodes from participating in network operation. This could reduce the risk of potential damage. After verifications and delivery of successful packets, trust vector value of node is incremented by +1; and decrease by -1 when verification fails. Network simulator (NS2) is used for simulation of proposed algorithm.

A.Nadeem proposed in [16], A network layer selfish node detection protocol-Selfish Node Detection Protocol (SNDP), In this article authors assume that SNDP will work on clustered based organization of MANET with secure communication between cluster head (CH) and cluster nodes (CN). They are focused of selfish behaviour and lightweight mechanism. Proposed mechanism has very low overheads because all detection work performed by CN. SNDP has three modules. First module is 'monitoring and data' collection; it collects data from each node and sends a general report (GR) to cluster head (CH), which include battery status, neighbour list and all other parameters. Second module 'detection' which uses impact metric for evaluates

overall network performance by CH. Impact metric include throughput and packet deliver ratio. Detection module has 3 phases' accusation, investigation and confirmation. In accusation CH scrutinize the GR send by nodes for status of their battery; if battery status falls in low criteria CH accused this node and add in the list of accused. Those could exhibit a selfish behaviour in future. In second phase CH will investigate each node which is in the list of accused. Any accused node with less threshold value of defined accused node behaviour is marked selfish. In order to reduce false conviction probability, CH checks behaviour again with impact metric within certain time interval. In last response module CH broadcast an alarm packet to all CN for mitigate its effect on overall network performance.

IV. IMPACT OF MISBEHAVIOUR

We already discussed that there are two main types of misbehaviours (Routing and Packet forwarding) which exist in MANET. We analyze the impact of different types of misbehaviour including both routing and packet forwarding. Misbehaving nodes can steer the network into collapse by not following appropriate routing and proper packet forwarding function as they suppose to do. We modified the AODV implementation in Glomosim to simulate the different types of misbehaviours. We will analyze and study various matrices and their effects to measure ad hoc network performance.

A: Simulation Environment: We describe the simulation parameters of the scenario simulated with two type of field configuration: 25 nodes distributed over 1050 meter terrain and 50 nodes over 2100 meter terrain. The position of nodes was random and uniform. Table 1 demonstrates general parameter of all the scenarios which would represent the simulation environment.

Table 1. Simulation Environment

Simulation Time	1000 Seconds
Area	2100 m 2
Path Loss Model	Two Ray Model
Radio Range	237 m
Number of Nodes	25 & 50
Nodes Placement	Random and Uniform
Bandwidth	2 Mbps
Packet Size	256 Bytes
Traffic Type	Constant Bit Rate (CBR)
Routing Protocols	AODV

In order to compare the performance of AODV with two types of misbehaviours we create mobility and traffic scenarios to evaluate results and their impact.

B: Evaluating Parameters: We evaluated three parameters, includes originated and received packets, throughput and Packet delivery ratio, which we simulate our scenario and observed variation and compare them among other collected values without modification.

1. Average network throughput
2. Packet Delivery Ratio (PDR): This is the ratio between packets originated from CBR source or Nodes and delivered completely to the destination.
3. Analysis of the Control and Data Packets: We use total number of packets to analyze the utilization of bandwidth in terms of control and data packets. We analyze this in both with and without misbehaviours.

IV. (A) Simulation Results

We have simulated two types of misbehaviors a) misrouting packets and b) exhibiting selfish behavior. During the simulation we analyze and observed the impact on the performance of the network in the presence of the two misbehaviours.

Scenario 1: Misrouting Misbehaviour

We ran simulation with 1, 3 and 5 misrouting nodes in 25 nodes similarly in maximum 5 nodes in 50 node networks. The graphs in Figure 7 & 8 show the analysis of PDR in the presence of various percentages of misbehaving nodes in 25 and 50 nodes networks. The graphs indicate significant decrease in the PDR in the presence of nodes misbehaving through misrouting. However, there is no real difference with the percentage of nodes misbehaving; this indicates that the network performance degrades as soon as a single node starts misbehaving.

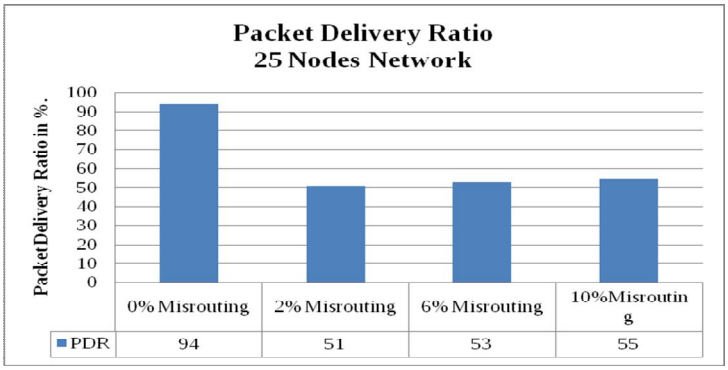

Figure 7. **Analysis of PDR in the presence of various % of misrouting nodes in 25 nodes network.**

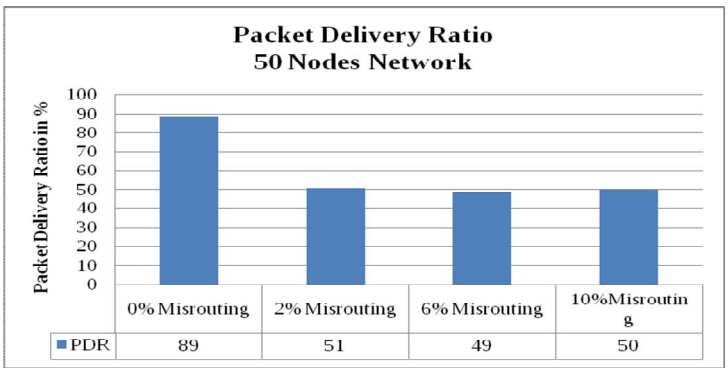

Figure 8. **Analysis of PDR in the presence of various % of misrouting nodes in 50 nodes network.**

The graphs in Figure 9 & 10 show the analysis of average network throughput in the presence of various percentages of misbehaving nodes in 25 and 50 nodes networks. The graphs show the throughput decreases in the presence of nodes exhibiting misrouting misbehaviour.

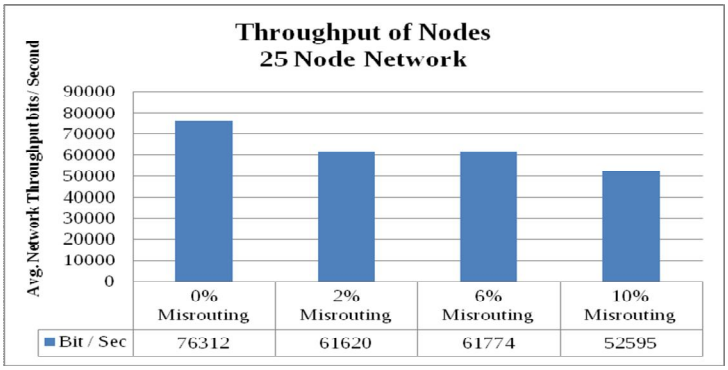

Figure 9. **Analysis of PDR in the presence of various % of misrouting nodes in 50 nodes network.**

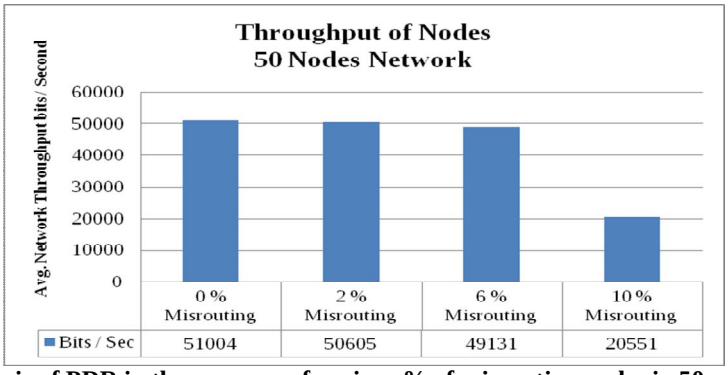

Figure 10. **Analysis of PDR in the presence of various % of misrouting nodes in 50 nodes network.**

Scenario 2: Selfish Misbehaviour

When we introduce Misbehaviour (Selfishness) in MANET we observe significant change in both PDR and avg. network throughput in both networks. Table 2: illustrate that how much reduction of packets generations and decrease in throughput we

may observe and much PDR increase with respect to the packet generation in 25 and 50 nodes network. Figure 11 demonstrate difference between two networks with the presence of selfish nodes and without selfish nodes occurrence in network and see drastic change in throughput of networks, (we have illustrate value of normal behaviours in multiples by 10 due to graph scaling). In figure 12 we demonstrate PDR, which is also differ and relatively high in presence of selfish nodes.

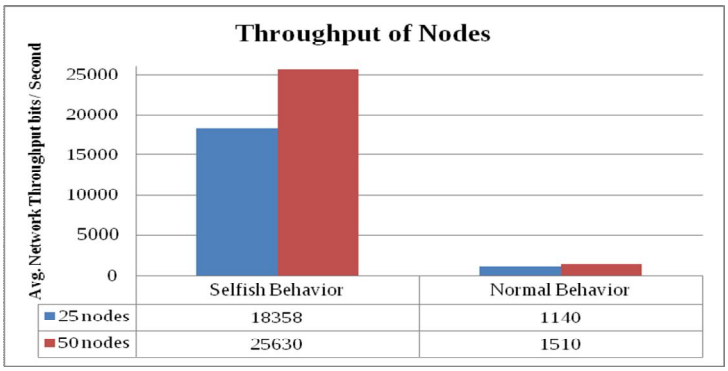

Figure 11. **Avg. throughput of both Networks.**

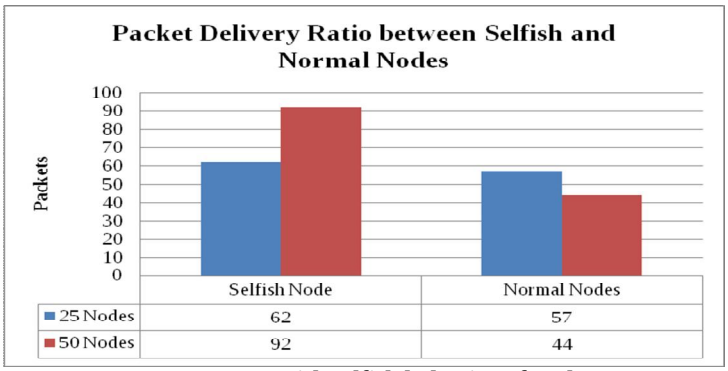

Figure 12. **PDR with selfish behavior of nodes**

IV. (B) Control and Data Packets analysis

We can observe a drastic variation in packet generation, when we add some of misbehaviour in normal operation of Manet. Figure 13 shows data packet generation in the all three phenomena.

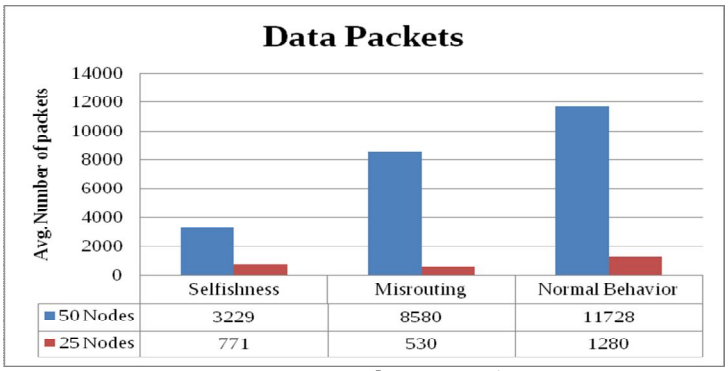

Figure 13. **Data packet generation.**

Similarly control packet variation in selfishness and normal behaviour is almost in reverse order to data packets, it does not mean that bandwidth and Packet delivery ratio goes down due to heavy increase in control packets. It increases due to node's selfishness. Figure 14 shows the high frequency in control packet with respect to data in normal behaviour.

Increase in control packet generation shows that data packets moves across the network and does not found destination and wasting resources i.e. nodes power and network bandwidth.

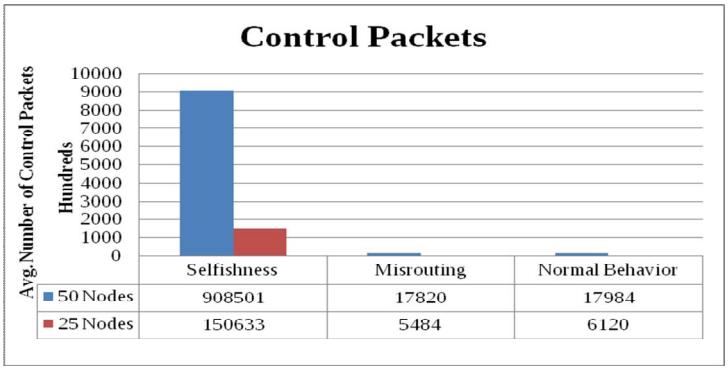

Figure 14. **Control packet generation.**

V. DETECTION OF PACKETS MISROUTING

In order to detect those nodes which misroute packets and to prevent network from them: we propose a network layer procedure to avoid such misrouting and to keep packets on their way to destination via shortest and appropriate paths without wasting other node's power.

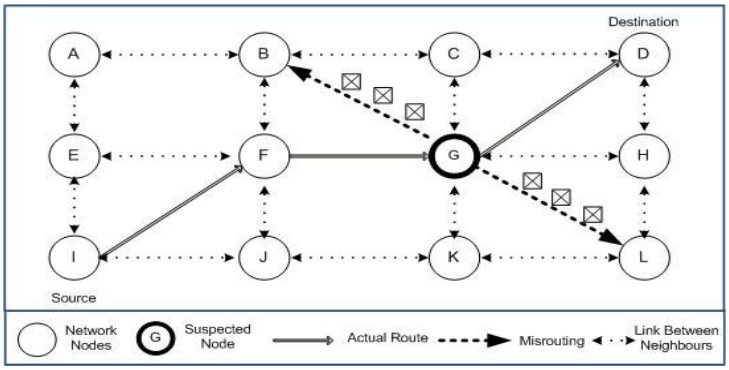

Figure 15. **Packet Misrouting (Scenario 1)**

We already assume that each node in network maintains two tables, route error table (RET table. 3) and two hop table (THT Table 4); both tables are maintained by routing protocol. RET contains errors related data like route error requests for both broken link and destination unreachable, and all ICMP time out messages. At the other end THT contains two hop entries of each node in the network which can be retrieved by trigging an event.

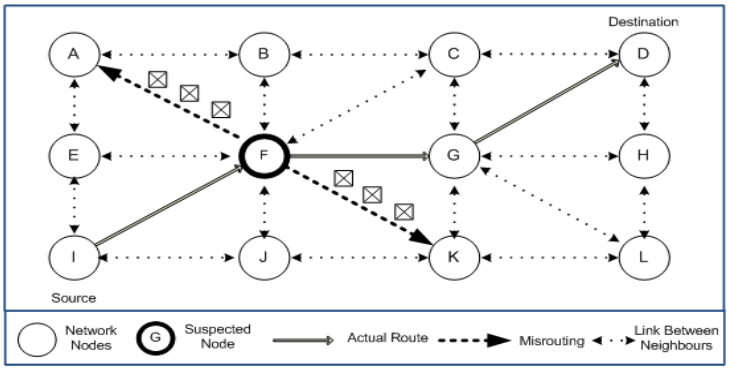

Figure 16. **Packet Misrouting (Scenario 2)**

During communication, when a node receives packet from its neighbour, first it scrutinizes its header and finds out source and actual destination of packet; then checks whether he himself is in the route? If node finds himself in the route of packet he will forward packet to appropriate next hop node. Else, it first checks RET for any error which could be possible reason for receiving such packet. Then he tries to obtain two hop entries of source node from protocol and checks both of his neighbours and packet route which could exist in two hop table. Similarly he may also checks hop count value for packet destination. If he finds entry of destination or route of packet to destination, first or second hop in his table. He should inform source that you forward it to actual node first, because you already have entry in your table. Then he informs other node that there is some illegal activity in routing from suspected node. Then he forward packet to appropriate route of destination.

Finally, two measures would be taken; first, information to others via an alarm or message about suspected node and his activity and secondly, mark particular node as suspected node for certain time and if other neighbours of suspected node also complained about such behaviour; node may refuse to perform routing via suspected node again.

Figure 16 illustrates that, if node 'A' receives packet from its neighbour node 'F', first he remove packet header and finds out destination of packet as well as its hop count value. Both would shows that how could he be its route or destination? So he

may trigger an event and will get route error table and two hop table of source node; both must verified that packet is misrouted; because there is no route error or broken link message in RET. Destination also exist in THT of source node and packet should be on other route instead of him. He would mark packet misrouted and inform suspected node 'F' that you should send packet on appropriate path rather than others. Also keep him on monitoring for certain time and if behaviour of suspected node is persist or other nodes complaining him about the same behaviour so it will be beneficial for network that particular node should isolate from network.

Route Error Table		
Error Msg	**Status**	**Node**
rerr-brklnk	Y / N	A
rerr-destun	Y / N	C
time out	Y / N	G

Table 3: **Route error table**

Two hop table		
Node	**1 Hop Neighbor**	**2 hop neighbors**
A	B,E,F	C,G,I,J,K
B	A,E,F,G,C	I,J,K,L,H,D
C	B,D,F,G,H	A,E,I,J,K,L
D	C,G,H	B,F,J,K,L
E	A,B,F,I,J	C,G,K
F	A,B,,C,E,G,I,J,K	D,H,L
G	B,C,D,F,H,J,K,L	A,E,I
H	C,D,G,K,L	B,F,J
I	E,F,J	A,B,C,G,K
J	E,F,G,I,K	A,B,,C,D,H,L
K	F,G,H,J,L	A,B,C,D,E,I
L	G,H,K	B,C,D,F,J

Table 4: **Two hop routing table**

Pseudo Code of Proposed Mechanism

```
Begin
Node received packet;
Check any route error message from route table;
Find source and destination node addresses;
Compare with route table for forwarding;
Check Route error table for errors;
Check Two hop table for destination;
If destination address of packet exist in 2nd hop in routing table;
        Mark packet misrouted;
        Mark source node suspect;
        Check destination available in routing table;
        Forward packet to actual destination;
        Inform source about his monitoring;
        Broadcast alarm message about suspect node and its monitoring;
If Behaviour persist;
        Other neighbour also complained;
        Then
         Isolate from Network;
Else
Do forward to appropriate next hop node;
End
```

VI. CONCLUSION AND FUTURE WORKS

In this paper, we have review, classify and analyze impact of the misbehaving nodes with two major types of misbehaviours i.e. misrouting and selfishness in MANETs. In the classification we have categorized misbehaviours based on the nodes which are malicious (has intension to harm the network) and non malicious (misbehaving may to conserve their scarce resources.) To analyze the impact of misbehaviours we have created various simulation scenarios. The results suggest the misbehaviours can significantly degrade the network performance. Finally we propose technique for detecting nodes which misroute packets in the network. In [11] Medidis already proposed a packet mishandling technique but our technique show some uniqueness: It introduce two hop table and route error table both could be available locally and provide some help to prevent illegitimate activities and makes system more fair and reliable. If this technique integrate with other routing protocols it may be more beneficial for MANETs user and will make system more flexible and error free. Still some areas are wide open for more secure and user friendly. In Future, we will focus on mitigating the effect selfish nodes by developing misbehaviour prevention techniques.

REFERENCES

[1] Nishu Garg and R. P Mahapatra "MANET security Issues "International Journal of computer Science and Network Security, vol. 9, No. 8, August 2009.

[2] X. Hong, K.Xu , M. Gerla "Scalable routing protocol for Mobile ad hoc network", proceeding of the IEEE Network, Vol 16. No. 4, PP 11-21, August 2002.

[3] Sirisha R. Medidi, Muralishar Medidi, Sireesh Gavini and Richard L. Griswold ", Detecting Packet Mishandling in MANET", Washington State University, Pullman 99164-2742.

[4] B Mahdavi, B. Najafpour, S. Nejhad, M. Sardarpour, N. L. Navid," Application of Artificial Immune System for Detection of Misbehaviour Nodes in MANET, J.Basic. Apl. Sci. Res., 3(1s)160-164, 2013 ISSN 2094-4304.

[5] S.Kurosawa and A. Jamalipor "Detecting black hole attack on AODV-based mobile ad hoc Networks by dynamic learning method", International Journal of Network Security, Vol. 5. No. 3 pp 338-345, November 2007.

[6] J. Sen, M. Chandra, Hasihara S.G, H. Reddy and P. Balamuralidhar,"A mechanism for detection of Grey Hole attack in Mobile ad hoc network", Proceeding of IEEE 6th International conference on information Communication and Signal Processing ICICS, Singapore, December 2007.

[7] D. Burman Roy, R. Chaki, "MADSN: Mobile agent based Detection of Selfish Nodes in MANET", International Journal of Wireless & Mobile Networks (IJWMN), Vol. 3, No. 4, August 2011.

[8] Michiardi P, Molva R (2002), "CORE: A collaborative reputation mechanism to enforce node cooperation in Mobile ad hoc networks " In (CMS'02)

[9] Buchegger S, Le Boudec J. (2002). Performance analysis of the CONFIDANT protocol ", in proceeding 3rd ACM (MobiHoc'02), pp 226-336

[10] Bansal S. Baker M. (2003), Observation Based Cooperation enforcement in ad hoc Networks. In Technical Paper on Network and Internet Architecture. .

[11] Sirisha R. Medidi, Muralishar Medidi, Sireesh Gavini and Richard L. Griswold ", Detecting Packet Mishandling in MANET", Washington State University, Pullman 99164-2742

[12] J. Zhen and S. Srinivas," Preventing replay attacks for secure routing in ad hoc networks. Proc of 2nd ad hoc networks and wireless (ADHOCNOW' 03), pp. 140-150, 2003.

[13] S.S. Manvi, L.B. Bhajantri and V.K. Vagga, "Routing Misbehavior detection in MANETs using 2ACK."

[14] Q.He.D.Wu and P. Kholsa, "A Secure and objective reputation based Incentive Scheme (SORI)", in Proc IEEE WCN2004, Mar' 04.

[15] A. Rajaram and S. Gopinath, "Efficient Misbehavior System for MANET", International Journal for Advances in Computer Science, Vol 1, Issue 1, December 2010.

[16] A. Nadeem, "Evaluating network layer selfish behavior and a methods to detect and mitigate its effect in MANET", Department of Computer Science, Federal Urdu University of Arts, Science & Technology.

[17] M. Nasir, J.A Khan, F Umer, N. Javaid, I. Haq, M. Shakir, "Security Enhancement of Pro-Active Protocols in Mobile Ad-Hoc Networks, J.Basic. Apl. Sci. Res., 3(3)101-107, 2013 ISSN 2094-4304.