ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Cooperative Attacker Detection Based on Neighbour Table Information in MANETs

Sajna KH [1], Nithin SS [2]

P.G. Student, Department of Electronics and Communication Engineering, Nehru College of Engineering and Research Centre, Thrissur, Kerala, India[1]

Assistant Professor, Department of Electronics and Communication Engineering, Nehru College of Engineering and Research Centre, Thrissur, Kerala, India[2]

ABSTRACT: The increasing demands and usage of wireless technologies will leads to mew emerging applications in this domain. MANETs(mobile ad-hoc networks)is a dynamic network ,consists of mobile nodes having no centralized points that wish to communicate with each other. There will be voluntary participation of mobile nodes in MANETs mobile nodes for the better communication between nodes. In this dynamic network, some mobile nodes are not willing to participate in the communication process. Hence the overall network will be affected. Collaborative contact based watchdog approach is used for detecting these non performing node in the network. In order to avoid the draw backs of this method we proposed a trust analysis based detection using neighbour table information. For the detection of malicious nodes these mechanism analyses the pattern of messages from multihop neighbors and check whether the node is malicious or not.

KEYWORDS: MANET, Mobile ad-hoc network, Selfish node, Neighbour table.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a wireless network of mobile devices, with no fixed infrastructure. Additionally there is no central base station for MANETs. So each node acts as transmitters and receivers. MANETs has become the emerging trend in the wireless networks because of cheaper, small and more powerful devices. In a MANET all the devices can move in and out or any direction in a dynamic manner. This makes MANETs exposed to vulnerabilities and attacks. Figure 1 shows the basic representation of a mobile ad hoc network. The biggest challenge in building a MANET is to make each device capable of maintaining information required for proper route traffic. MANETs consist of a peer-to-peer, self-forming, self-healing network [1]. Many researches were done on MANETs and their protocols. Different MANET protocols are then evaluated based on parameters such as packet drop rate, overhead by routing protocol, network throughput, end to end packet delays, scaling ability etc.

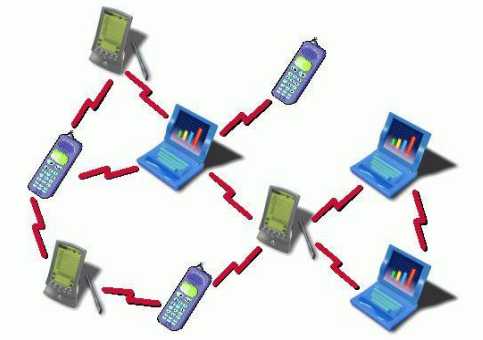


Fig. 1. A Mobile Ad hoc Network

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

A MANET consists of mobile nodes, which are free to move about. An example is a router with multiple hosts. The system may work on isolation or may have gateways to specific network or internet. The important characteristics of MANETs are;

- Nodes are free to move in MANETs and hence the network topology may change randomly, and may have unidirectional and bidirectional links
- Wireless links will have lower capacity than their hardware parts. Additionally the interference effects like noise and fading will be much less than the maximum transmission rate
- Some or all nodes in the MANET may depend on battery for energy. For these nodes, the important system design criteria is energy saving
- Physical security of MANET is limited. Mobile networks are more prone to security threats

Compared to wired networks MANET is more vulnerable to attacks in the network due to limited physical security, dynamic network topology, flexibility, scalability and lack of centralized management. Because of these vulnerabilities, MANETs are prone to security issues. So for proper communication we must detect the presence of these kinds of malicious nodes.

The rest of the paper is organized as follows: Section 2 presents a brief review of the existing detection mechanisms in mobile ad hoc networks. Section 3 describes the proposed scheme. Section 4 presents the experimental results. Finally, Section 5 concludes the paper and outlines future work.

II. RELATED WORK

Recently a lot of researches have been focusing on detection of these non performing nodes in the networks. Here some of the approaches are discussed.

A simple approach of watchdog was proposed by S. Marti *et al* in their study "Mitigating routing misbehavior in mobile ad hoc networks" [8]. Unfortunately this approach is too simple and error prone. The approach also relies on all clients to have equal sending range. This will be a collision with the modern wifi controllers using energy control

Khairul Azmi et al proposed a mechanism to detect the selfish nodes in "A Scheme for Detecting Selfish Nodes in MANET using OMNET++" [9]. According to this proposed model each node is supposed to contribute to the MANET continuously within a time frame. The system is also based on a monitoring node. A monitoring node listens to the request for forwarding the data packet from its neighboring node. It then checks the time difference between the last request and last action and status of the requesting node.

Al Shurman et al proposed two different solutions for black hole in their work "Black hole attack in Mobile Ad Hoc Networks" [10]. First solution is unicasting a ping packet from source to destination through multiple routes and then choosing the safest route based on the replies received. The second solution is keeping track of the sequence numbers. The problem with these solutions is longer delay and lower number of verified routes.

In the study "Mitigating routing misbehavior in mobile ad-hoc networks", Marti et al described misbehavior detection and reaction [11]. The paper presents two extensions to the DSR algorithm: the watchdog and the path rater. The watchdog can detect misbehaving nodes by actively listening to the next node transmission but fails to detect misbehavior during collisions or limited transmission power.

Buchegger and Le Boudec proposed the CONFIDANT protocol in the test report "A test bed for misbehavior detection in mobile ad hoc networks" [12]. In this proposed system, similar to watch dog, each node listens to its neighbor for misbehavior. One drawback of the system is deciding the criteria for maintaining the friends list by Trust Manager is difficult.

A similar system was proposed by K. Paul and D. Westhoff in "Context aware detection of selfish nodes in DSR based ad-hoc networks" [13]. However the diffusion is very costly since the approach is based on periodic message dissemination.

CORE (Collaborative Reputation) is a reputation based system similar to CONFIDANT proposed by P. Michiardi and R. Molva in "A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks" [14]. The limitation of the system is that most of the reputed nodes will be congested as most of the routes are likely to pass through them.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

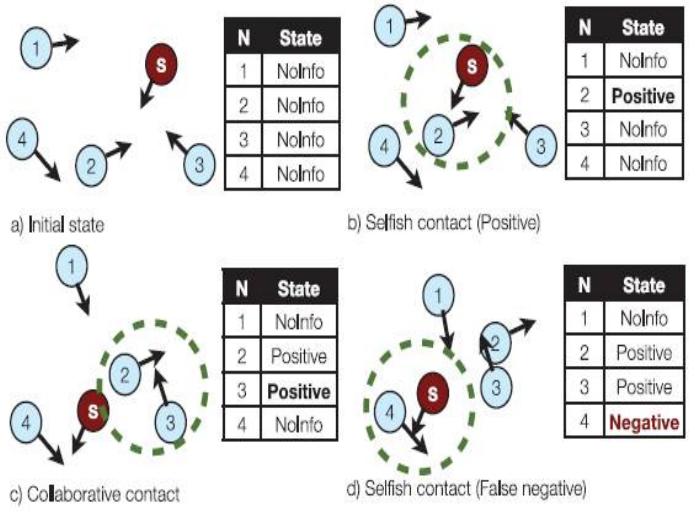
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Bansal *et al* proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) [15]. OCEAN uses both monitoring system and a reputation system to identify malicious nodes. But OCEAN fails to detect misbehaving nodes properly.

A TWOACK scheme was proposed by Balakrishnan *et al* in their work "TWOACK-Preventing Selfishness in Mobile Ad hoc Networks" [16]. Instead of detecting a particular node, this system detects misbehaving link. It is done by sending a TWOACK packs on successful reception of every packet. The basic drawback of this system is that it cannot distinguish which particular node is misbehaving.

A sophisticated system of "Collaborative Contact-based Watchdog (CoCoWa)" was proposed by Enrique Hern et al in the work "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes" [17]. According to this approach, if one node has previously detected a selfish node it can transmit this information to other nodes also. This way all the nodes in the network will have information about the selfish node in the network. This system focuses on reducing the detection time and improving the precision by reducing the effect of both false negatives and false positives. The working of CoCoWa is explained in figure 2.



CoCoWa is based on the combination of local watchdog and the diffusion of information when pair of nodes contacts. A contact here is a transmission between two nodes. When a node detects a selfish node using its watchdog, it is marked as a positive, and if it is detected as a non selfish node, it is marked as a negative.

Later, when this node contacts another node, it can transmit this information to it also. So both the nodes keep information about these positive or negative detections. But it only detects the presence of selfish nodes and it takes the high detection time.

III. PROPOSED SCHEME

The important part of the proposed architecture depicted in figure 3 is the watchdog system which is virtually present in each node. The detection of attackers or malicious nodes and the detection of new contacts or with neighbor nodes are the two main functions of watchdog. By obtaining the information from the neighbouring nodes it generates the following events about neighbour nodes: PosEvt (positive event) is the indication for when the watchdog detects a malicious or non performing nodes, NegEvt (negative event) no information about the malicious nodes. Detection of new contacts is done by overhearing the neighbourhood packets. This information and watchdog event is continuously gives to information update.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

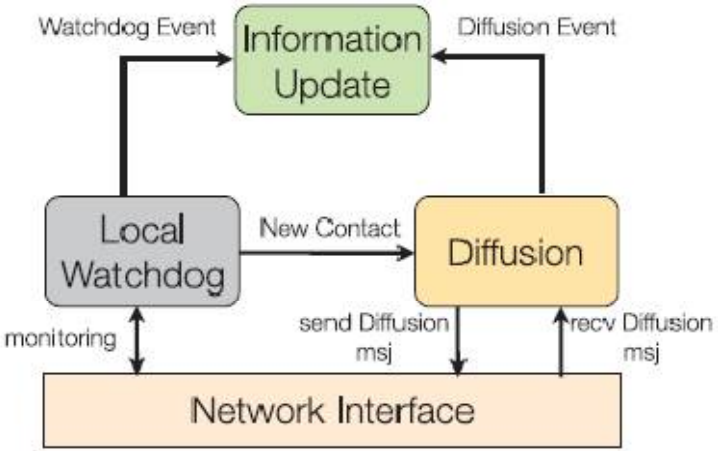


Fig. 3. Proposed System Architecture

The main purpose of diffusion module is the transmission of as well as the reception of positive (and negative) detections. The transmission of both positive and negative detections is needed to neutralize the effect of false positives .Otherwise the transmission of positive detections only lead into serious problems like transmission of false positives very fast. Reception of a new contacts event from watchdog transmits this information to neighbouring ones. Finally, all events from diffusion module are also get updated in information module.

Next part is the updating or consolidating the information. This is the function of the Information Update module. The watchdog events like PosEvt or NegEvt from local watchdog system are updated continually for each node in information update. A node can have direct information (from the local watchdog) and indirect information (from neighbour nodes. In previous approach information update is done by probabilistic approach. That is giving "0"for selfish nodes or Malicious nodes and giving 1' for good nodes. But this approach is not trust worthy because updates from 1-hop neighbours are only considered. In this case information from multi hop neighbours are not considered. The nodes which found good nodes are seen to be bad while considering the multi hop neighbours. In the proposed system information update is done using trust analysis and by link quality. According to this information the presence of attacker node is detected.

IV. ATTACKER DETECTION

The figure 4 shows the block diagram of the proposed scheme. The creation of nodes in the network is first takes place. Here we consider 50 nodes. Neighbour table creation is done with the help of both one hop neighbours and two hop neighbours. The virtual watchdog system present in the network which updates and monitoring the information about each nodes. Then the broadcasting of messages takes place by continuously sending the HELLO packets for to check whether the neighbouring nodes are active or not. After checking, selection of shortest path in the network takes place it is done by sending route request, route reply hence routing. Malicious nodes are detected by using the trust and link values of multihop neighbours. At last elimination of these nodes takes place.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

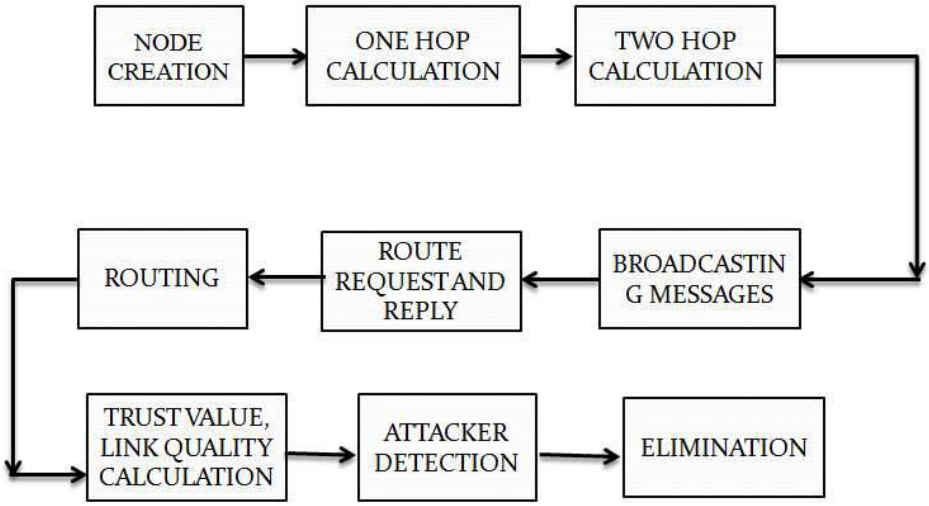


Fig. 4. Proposed System Block Diagram

1. Multi Point Relays (MPR)

The Main aim for MPR selection is that reducing redundant retransmission of the messages in the same region. Only some numbers of nodes are selected for further forwarding of messages to the neighbouring nodes. This set of nodes is known as multipoint relay set. By periodically broadcasting HELLO packets the nodes for the link sensing, neighbour detection and MPR selection processes and it gets the topology up to 2 hops from HELLO messages. Every node periodically broadcasts list of its MPR selectors instead of the whole list of neighbours.

2. Neighbour Sensing

Each node in the network continuously forwards Hello messages, to detect the neighbour nodes with which it has a direct link. The task of neighbour sensing and MPR selection process is done by Hello messages. A node‘s HELLO message consisting of its own address, a list of its 1-hop neighbours and a list of its MPR set. Thus the main aim of neighbour sensing is that to check whether the node is active or not.

3. Trust Value Analysis and Link Quality

Trust evaluation helps to distinguish between good and malicious entities. It also offers a prediction of one‘s future behavior and improves network performance. The trust values are calculated from each node in the network based on the information which is given by the particular watch dog system. Each node in the network maintains the trust value of its neighbour node. Or we can say it is time sensitive or dynamic. So trust party has to periodically evaluate the nodes trustworthiness. In order to improve the cooperative routing and eliminate the malicious and selfish nodes in the route, trust analysis is done. It is calculated by the ratio of receiving events to the sending events. The values of trust analysis are in between 0 and 1.the node with highest trust value is the most trustworthy node.

Link quality shows the successful transmission of packets between nodes without any loss. Also says how good a given link exists in between a neighbour and ourselves is in the direction from the neighbour to ourselves. Its value lies in between 0 and 1.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

V. SIMULATION RESULTS

Network Simulator (NS2) version 2.32 is used to evaluate the performance of proposed scheme with wireless extension is used. It is one of the most popular and commonly used simulation packages due to free license(availability).Also it test new protocols and possibility to implement and applications. In both wired and wireless domains For simulation purpose NS-2 is commonly used for simulation purpose due to the advantages like it supports several networking protocols and various standards . In the simulation experiments, the underlying scheme uses DSR protocol. Around 50 mobile nodes was simulated here. The simulation time is 30 seconds. Randomly chooses two attacker or malicious nodes in the network. Table I shows the required parameters for simulation.

Table 1. Simulation Parameters

S. No.	Parameters	
1	Simulator	NS2
2	Simulation time	30 sec
3	Traffic type	CBR
4	No: of total nodes	50
5	No: of attackers	2
6	Protocol used	DSR
7	Topology	Flat grid

The figure 5 (a) shows the deployment of nodes. Here we considered 50 nodes. In this process configuration of nodes by setting the power, energy, protocols etc. or simply the configuration of nodes takes place. Figure 5 (b) shows the attacker detection. According to the trust values calculated of each nodes from two- hop neighbors attacker is found in which attackers having the least trust value. Figure 5 (c) shows the routing process of finding routes from source to destination. Here we choose two source and two destination nodes. Hence the routing takes place along the path in between source and destination by ignoring the attacker path.

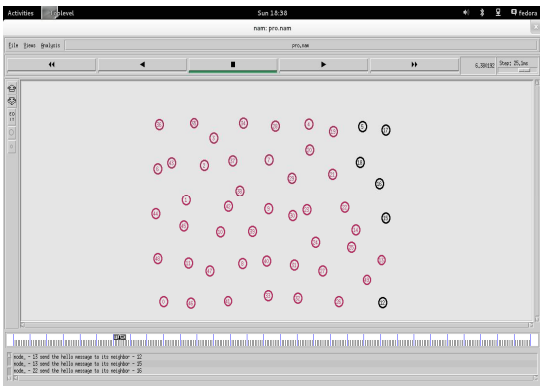


Fig. 5 (a) Node Deployment

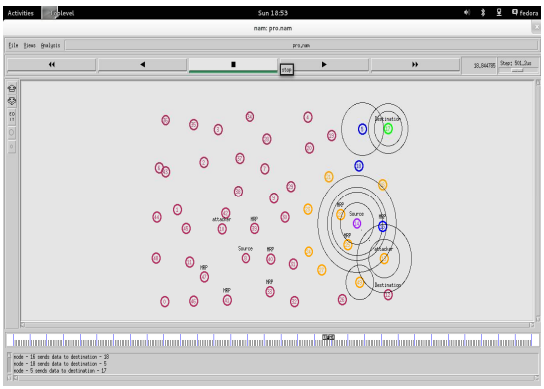


Fig. 5 (b) Attacker Detection

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

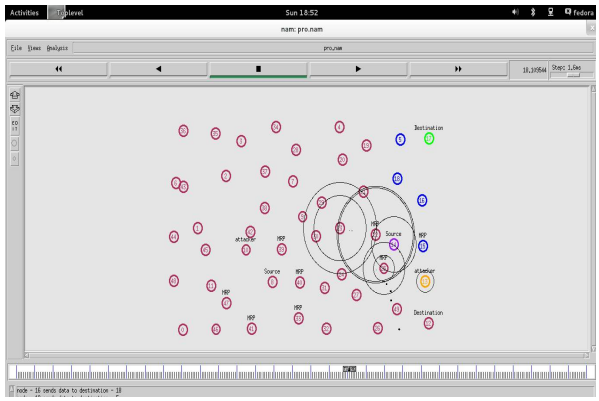


Fig. 5 (c) Routing

VI. ANALYSIS

The commonly used metrics for evaluating the performance are overhead, throughput and packet delivery ratio(PDR). This results shows that the how strong is the proposed system compared to existing ones. We compared the results in through graphs.

1. Overhead

The figure 6 (a) shows the overhead, it is the time needed to detection of misbehaving nodes. The detection time is reduced in the proposed method.

2. Throughput

The figure 6 (b) shows the throughput of existing method (collaborative contact based watchdog system) and the proposed method is compared .It shows the total number of packets delivered in the simulation time. The total number of packets delivered is less compared to proposed system. Hence in the proposed system throughput is high.

3. Packet Delivery Ratio

The figure 6 (c) shows the packet delivery ratio. It is ratio of packets received to the packets send. Here there will be no packet loss at the routing time hence the ratio will become 1.

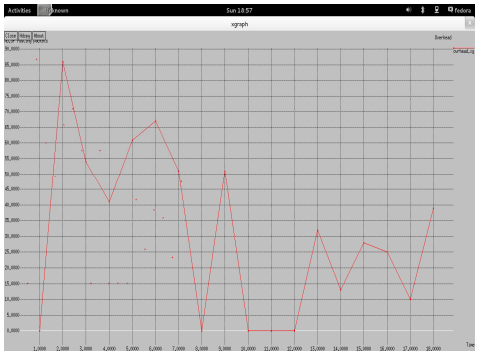


Fig. 6 (a) Overhead

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

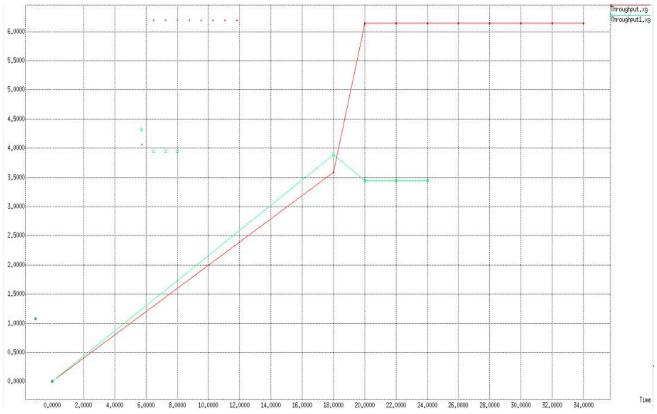


Fig. 6 (b) Throughput

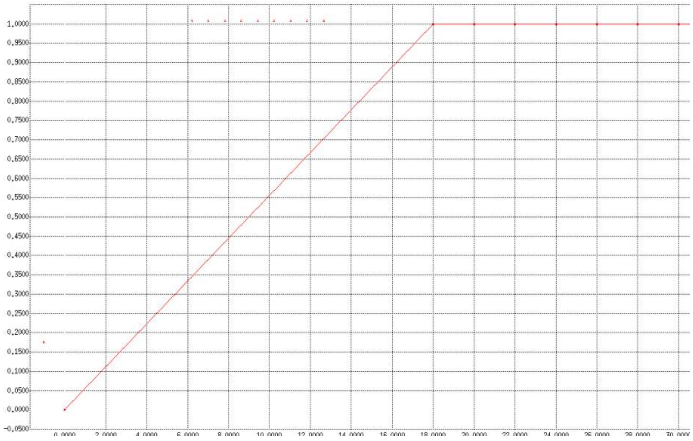


Fig. 6 (c) Packet delivery ratio

VII. CONCLUSION

As the use of the MANETs has increased, the security of the MANETs has become a big concern. Selfish or other misbehaving nodes are always a security threat to mobile ad hoc networks. In this study, we have reviewed different selfish node detection mechanisms and proposed a new detection mechanism based on the trust and neighbour information table. Many protocols were suggested to enforce cooperation and as to detect misbehaving nodes. All of them make certain premises which make them more suitable for some scenarios and less suitable for others. We saw most of the selfish node detection schemes use the conventional watchdog system. None of the system was found to be perfect. However, we analysed the proposed one with different performance metrics and found it is the efficient among them. Detection is done by the information from the multihop neighbours trust values hence we can say that the method is trustworthy. The system literally increases the performance of the mobile ad hoc network. Successful transmission of packets to the destination without any loss is considered and the parameters are evaluated.

REFERENCES

[1] Wikipedia. Available at: www.wikipedia.org/Mobile_ad_hoc_network
[2] Y-C Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Sec. and Privacy, May–June 2004

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

[3] C. K. N. Shailender Gupta and C. Singla, "Impact of selfish node concentration in MANETs," Int. J. Wireless Mobile Netw., vol. 3, no. 2, pp. 29–37, Apr. 2011
[4] C. Toh, D. Kim, S. Oh, and H. Yoo, "The controversy of selfish nodes in ad hoc networks," in Proc. Adv. Commun. Technol., Feb. 2010, vol. 2, pp. 1087–1092
[5] Y. Yoo, S. Ahn, and D. Agrawal, "A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks," in Proc. IEEE Int. Conf. Commun., May 2005, vol. 5, pp. 3005–3009
[6] Amitabh Mishra, "Security And Quality Of Service In Ad Hoc Wireless Networks" (chapter 1, 3), ISBN- 13 978-0-521-87824-1 Handbook
[7] Sevil¸ Sen, John A. Clark, and Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks
[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking. New York, NY, USA: ACM Press, 2000, pp. 255–265
[9] Khairul Azmi, Abu Bakar and James Irvine. " A Scheme for Detecting Selfish Nodes in MANET using OMNET++", 2010 Sixth International Conference on Wireless and Mobile Communications, pp 411-414, 2010
[10] Al-Shurman, M. Yoo, S. Park, "Black hole attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference", 2004, pp. 96-97
[11] Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000), "Mitigating routing misbehavior in mobile ad-hoc networks", Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom), ISBN 1-58113- 197-6, pp. 255-265
[12] S. Buchegger, C. Tissieres, and J. Y. Le Boudec. "A test bed for misbehavior detection in mobile ad hoc networks". Technical Report IC/2003/72, EPFL-DI-ICA, November 2003
[13] K. Paul and D. Westhoff, "Context aware detection of selfish nodes in DSR based ad-hoc networks," in Proc. IEEE Global Telecommun. Conf., 2002, pp. 178–182
[14] P. Michiardi and R. Molva. Core: "A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks", In Proceedings of the 6th IFIP Communications and Multimedia Security Conference, Portorosz, Slovenia, September 2002, pp 107-121
[15] S. Bansal and M. Baker. "Observation-Based Cooperation Enforcement in Ad hoc Networks", July 2003. Available on: http://arxiv.org/pdf/cs.NI/0307012
[16] 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. 2137-2142
[17] Enrique Hern_andez-Orallo, Manuel David Serrat Olmos, Juan-Carlos Cano, Carlos T. Calafate and Pietro Manzoni, "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes", in IEEE Transactions On Mobile Computing, VOL. 14, NO. 6, JUNE 2015, pp. 1162-1175