Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 75 (2014) 27887-27891

ISSN: 2229-712X

Survey of innovated techniques to Detect selfish nodes

Sagar Padiya, Rakesh Pandit and Sachin Patel

ARTICLE INFO

Article history:
Received: 28 December 2012;
Received in revised form:
15 October 2014;
Accepted: 28 October 2014;

Keywords
ACK2, BMF,
Cooperative System in MANET,
Misbehaving Nodes,
Mobile Ad-hoc Network (MANET)
Area,
Nodes,
Selfish Nodes.

ABSTRACT
An Ad-hoc network is a collection of mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administer. Because of limited communication range among mobile nodes in ad-hoc network, several network hopes may be needed to deliver a packet from one node to another node in the wireless network. In such a network each node acts as an end system as well as a relay node (or router). Most of the routing algorithms designed for MANET such as AODV and DSR are based on the assumption that every node forwards every packet. But in practice some of the nodes may act as the selfish nodes. These nodes use the network and its services but they do not cooperate with other nodes. Such selfish nodes do not consume any energy such as CPU power, battery and also bandwidth for retransmitting the data of other nodes and they reserve them only for themselves. The original AODV and DSR routing algorithms can be modified to detect such selfish nodes. In this paper, we survey innovated techniques as well as proposed techniques to detect Selfish Nodes for MANET. Finally we provide some directions for further research.

Introduction

Mobile ad hoc network is a network consisting of mobile nodes (Laptop, Personal Digital Assistants (PDAs) and wireless phones) with the characteristics of self-organization and self-configuration which enable it to form a new network quickly [01]. A Mobile Ad hoc Network or in short, MANET, is a relatively new communication paradigm. A MANET network consists of a group of mobile devices (nodes) communicating through a wireless medium. Unlike a traditional infrastructure network, the network is established solely by the MANET devices themselves without the need of any fixed infrastructure such as an access point or base station. A node may be able to communicate with other nodes far away with the cooperation of intermediate nodes, forwarding the packets to the destination. In this multi hop communication, each node operates as both host and router.

Routing protocol such as Dynamic Source Routing [DSR] and AODV have been designed to handle such environment [02]. Minimal configuration, quick deployment and the absence of central governing authority make MANET suitable for emergency situations such as natural disasters, military conflicts and emergency medical situations. However, since there is no centralized administration, the performance of a MANET greatly depends on the cooperation of all nodes in the network.
A MANET (Mobile Ad-hoc Network) is a self configuring system of mobile nodes connected by wireless links. In a MANET, the nodes are free to move randomly, changing the networks topology rapidly and unpredictably. MANETs are decentralized, and therefore all network activities are carried out by nodes themselves. Each node is both an end-system as well as a relay node (router) to forward packets for other nodes. Most of the routing algorithms designed for MANET such as DSR and AODV are based on the assumption that every node forwards every packet. But some of the nodes may act as the selfish nodes. These nodes use the network and its services but they do not cooperate with other nodes. Such selfish nodes do not consume any energy such as CPU power, battery and also bandwidth for retransmitting the data of other nodes and they reserve them only for themselves.

This paper discusses three techniques namely 1) *Reputation based* technique, 2) *Credit based* technique and 3) *Acknowledgement based* technique to detect selfish nodes in MANET [03]. In reputation based technique, network nodes collectively detect and declare the misbehaviour of a suspicious node. Such a declaration is then propagated throughout the network. Credit based technique provide incentives for nodes to faithfully perform networking functions. In order to achieve this goal, virtual (electronic) currency (credit) or similar payment system may be set up. Nodes get paid for providing services to other nodes. Acknowledgement based technique provide rely on the reception of an acknowledgment to verify that a packet has been forwarded.

Classification of Techniques

Several techniques have been proposed to detect misbehaving nodes in mobile ad hoc network. These techniques can be classified into three categories:

A Reputation-Based Technique:

Reputation based technique on the other hand rely on building a reputation metric for each node according to its behavioral pattern. A monitoring method used by most systems in this category is called a watchdog. Watchdog was proposed by Marti et al. [04] to detect data packet non forwarding by overhearing the transmission of the next node. [05], [06], [07] use similar monitoring technique but then propagate collected information to nearby nodes and are susceptible to false praise and false accusation attacks.

Mr. Bansal and Mr. Baker proposed a system called OCEAN [08] where the reputation of a neighbor is evaluated using only locally available information and thus avoid sophisticated and potentially vulnerable techniques of reputation

Tele:
E-mail addresses: padiyasagar@gmail.com

propagation throughout the network. It is reported that even with direct observations of the neighbor; OCEAN performs almost as well and sometimes even better compared to schemes that share second-hand reputation information.

Credit Based Technique:

The basic idea of credit based technique is to provide incentives for nodes to faithfully perform networking functions. In order to achieve this goal, virtual (electronic) currency or similar payment system may be set up. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services. Credit based schemes can be implemented using two models: 1) *The Packet Purse Model (PPM)* and *2) The Packet Trade Model (PTM)* [03].

Acknowledgement Based Technique:

The last category is acknowledgment based technique, it rely on the reception of an acknowledgment to verify that a packet has been forwarded. Liu et al. [09] proposed the 2ACK system where nodes explicitly send acknowledgment two hops upstream to verify co-operation. This system is susceptible to collusion of two or more consecutive nodes. Furthermore, colluding nodes can frame honest ones by claiming not to receive the acknowledgment. All of the mechanisms mentioned above are designed to detect and handle misleading nodes.

There are a few systems that have been proposed to detect selfish nodes in a MANET. One example is Context Aware Scheme [10] introduced by Mr. Paul and Mr. Westhoff. This system uses un-keyed hash chains and a promiscuous mode to detect the misbehavior during route discovery phase. The observers of misbehavior independently communicate their accusation to the source. To convict a culprit, more than three accusations are needed. If there is only one accusing node, the accusing node itself will be considered to be an attacker.

The drawback of this system is that it is more beneficial for a node not to send the alarm message to avoid the risk being the only accuser and regarded as attacker. In [11], Djenouri et al. propose two different techniques to detect two different types of control packet droppers. They suggest the use of two-hop ACK approach for monitoring directed packets (RREP, RRER) and promiscuous-based overhearing technique for monitoring broadcast packets (RREQ). Huang et al. [12] suggest that the monitoring node simply compares the ratio of relay RREQ number between its neighbor and itself. If the ratio is smaller than a threshold, the neighbor is regarded as selfish and its packet is dropped as the punishment.

Innovated Techniques

Intrusion Detection Techniques:

As there is no any fixed infrastructure in mobile Ad hoc networks, all nodes should cooperate with each other in routing and transmitting the packets to deliver the packets to the specified destination. Intermediate nodes may agree to forward packets, but in fact they delete or modify them, because they are malicious. Only a few misbehaving nodes (malicious nodes, selfish nodes) can decrease whole system performance. Several methods and protocols have been proposed to detect and prevent such misbehaving nodes by Farzaneh et al. [13].

Watchdog

In Kachirski O et. al. [14], the technique identifies misbehaving node by eavesdropping on the transmission of the next hop. When a node forwards packets, Watchdog verifies whether the next node in the route forwards the packets or not. If the next node refuses to forward the packets, then it is known as misbehavior.

The advantages of Watchdog mechanism is that it can identify misbehaving nodes not in forwarding level but also in the level of connection. In other words, it identifies nodes not only in the link layer, but also in the network layer. Implementation of Watchdog is relatively easy.

In Kachirski O et. al. [14], Watchdog has some obvious disadvantages. For example, due to the lack of cooperation in nodes, it may be unable to identify misbehaving nodes in circumstances such as 1) ambiguous collision 2) receiver collision 3) limited transmission power 4) false misbehaving 5) collision 6) minor dropping.

Pathrater

In Kachirski O et. al. [14], the technique calculates "path metric" for every path. Like Watchdog, each node runs Pathrater. The node maintains a degree of other nodes identified in the network. The path metric which is collected from past experience can be calculated by combining the node rating with link reliability. After calculating the path metric for all reachable paths, the path with the highest metric can be chosen by the pathrater.

Routeguard

In Hasswa A et. al [15], the technique employs a smart and smooth architecture in order to effectively discover malicious nodes and then proceeds to protect the network. Simulation results demonstrate that this scheme improves network throughput by smartly classifying the nodes into different categories depending on their current actions and previous history.

This system categorizes each neighbor node by combining Watchdog and Pathrater. This categorization is as follows: Fresh, Member, Unstable, Suspect, or Malicious. Moreover, the class of each node depends on the ratings achieved from the Watchdog according to its behavior. Furthermore, each class or tag implies a different trust level which goes from trusted (Member), allowing the node to participate in the network, to completely un-trusted (Malicious), being excluded from the network. A simulation model for this system has been developed in NS-2.

Hop-by-hop signing

In Caballero et. al [16], the technique proposed a secure routing system which would allow intrusion detection. This technique contains the different public key management protocols for MANETs. The public key infrastructure provides public key encryption and signatures for every node. According to the structure, A could send signed packets to C through B, and C could authenticate that they came from A. Lastly, Watchdog technique is presented as a solution to avoid denial of service attacks such as Black and Grey Hole routers. However, this system has been thought for short paths (for one or two hops as maximum).

Patwardhan secure routing and intrusion detection system

In Caballero et. al [16], the technique presents a proof of concept where a secure routing protocol is implemented by using public key encryption, intrusion detection, and a reaction system. The system implements a secure routing protocol, adding public key signatures to validate the ownership of the messages. In addition, it has an intrusion detection system where each node monitors its neighbors in a promiscuous mode by listening to their routing activity. When a node claiming to be a router, is detected as misbehaving, the detection system marks

the node as malicious node and the reaction system isolates the node from the MANET.

ExWatchdog

Nasser and Chen [17] have proposed techniques to identify IDS called ExWatchdog which is actually an extension of Watchdog. ExWatchdog also detects intrusion from malicious nodes and reports this data to the response system. Watchdog which is based on overhearing resides in each node. Each node can detect the malicious action of its neighbors through overhearing and can report this misbehaving to other nodes. However, if the node that is overhearing and reporting is malicious itself, it can make a serious impact on network performance. The main feature of the proposed system is the ability to detect malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then it proceeds to protect the network. So, ExWatchdog solves the fatal problem of Watchdog. [18]

Confidant

In Buchegger et al [18], proposed a CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad hoc Networks), which is in fact an expansion of DSR protocol. This technique is similar to Watchdog and Pathrater. Each node monitors the behaviors of neighbor nodes within its radio range and learns from them. This protocol resolves the Watchdog and Pathrater problem, meaning that it does punish misbehaving nodes by not using them in routing and not forwarding packets through them. In addition, when a node detects a misbehaving node, it sends a warning to all other nodes and they do not use this node either. CONFIDANT protocol consists of Monitoring System, Reputation System, Trust Manager and Path Manager. Their tasks are divided into two sections: the process to handle their own observations and the one to handle reports from trusted nodes.

For observations, the monitoring node uses a “neighborhood watch" within its radio range to discover any malicious behaviors. If a dubitable event is detected, monitoring node then reports it to the reputation system. At that time, the reputation system accomplishes several checks and updates the rating of the reported node in the reputation table. If the rating result is dubitable, it forwards the information to the path manager, which then omits all paths containing the misbehavior node. Then the trust manager sends An ALARM to warn other nodes that consider these nodes as friends. [18]. When the monitoring node receives an ALARM message from trusted nodes, at first the trust manager evaluates the message to see if the source node is trustworthy. If so, the ALARM message with the trust level will be stored in the alarm table[18].

Core

In Michiardi et. al [19], the technique detects selfish nodes and forces them to cooperate as well. Similar to CONFIDENT, This technique is based on monitoring system and reputation system, which includes both direct and indirect reputation from the system. Sometimes nodes do not misbehave intentionally; for example when their battery is low, they should not be considered misbehaving nodes and be fired from the network. To do so, the reputation should be rated based on past reputation, which is zero (neutral) at the beginning.

In addition, participation in the network can be categorized into several functions such as routing discovery (in DSR) or forwarding packets. The difference between CORE and CONFIDANT is that CORE only allows positive reports to pass through but CONFIDANT allows the negative ones. This means that CORE prevents false reports, and thus it prevents a DOS attack which CONFIDANT cannot do. When a node cannot cooperate, it is given a negative rating and its reputation decreases. In contrast, a positive rating is given to a node from which a positive report is received and then its reputation increases.

Ocean

In Bansal et al. [20], also proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) which is an extension of the DSR protocol. OCEAN like previous techniques uses a monitoring and a reputation system. However, contrary to previous approaches, OCEAN relies only on its own observation to avoid the new vulnerability of false accusation from second-hand reputation exchanges. So, OCEAN can be considered a stand-alone architecture.

OCEAN classified routing misbehavior into two classes: misleading and selfish. If a node participates in the route discovery but does not forward a packet, its class is misleading as it misleads other nodes to route packets through it. But if a node does not even take part in the route discovery, it is considered to be selfish.

In order to detect the misleading routing behaviors, a node buffers the packet checksum after forwarding a packet to a neighbor, then it can monitor if the neighbor attempts to forward the packet within a given time. As a result of monitoring, either a negative or positive event is produced to update the neighbor rating. If the rating is lower than the faulty threshold, that neighbor node is added to a faulty list and then to the RREQ as an avoid-list. In addition, all the traffic from the misbehaving neighbor node will be rejected.

Cooperative Intrusion Detection System

In Huang and Lee [21], proposed a Cooperative Intrusion Detection System based on clustering approaches was similar to Kachirski and Guha’s system [14]. In this method, IDS not only detects an intrusion but also identifies the type of attack and the attacker. This is possible by using statistical anomaly detection. Statistical formulas can define Identification rules to discover attacks. These rules help to detect the type of attack and in some cases the attacking node itself [21]. In this technique, IDS architecture is hierarchical, and each node has an equal chance of becoming a cluster head.

Monitoring the data obtained from the traffic would be which is analyzed for possible intrusions consume power. Therefore, instead of every node capturing all features themselves, the cluster head alone is responsible for computing traffic-related statistics. This can be done because the cluster head overhears incoming and outgoing traffic on all members of the cluster since it is one hop away (a clique: a group of nodes in which each pair of members can communicate via a direct wireless link). As a result, the energy consumption of member nodes is decreased, whereas the detection accuracy is just a little worse than that of not implementing clusters. Besides, the performance of the overall network is noticeably better decreased in CPU usage and network overhead. One of these systems which are worked cooperatively is being as follow.

Snooping packets technique:

In Parker et. al [01], Snooping protocols have two inherent characteristics in most of the MANET protocols. 1) The first feature is that each node in the network keeps a list of addresses of those nodes near or on the route from source to destination. 2) The Second one is 802.11 and MACAW link layer protocol, when a node is able to “hear” RTS / CTS transmission of its neighbors. So, in the process of intrusion detection of a

neighbor, each node "snoops" on its neighbor's transference to ensure that it is not distorted or misrouted.

Parker and his colleagues [01] have introduced a technique based on the snooping packets to discover misbehavior in mobile ad hoc networks. In this plan, appropriate for DSR and other routing protocols, the Snooping nodes listen to all nodes in their proximity. This technique is in complete contrast with Watchdog and (CONFIDENT) Neighborhood watch on DSR that are only watching the next node from source to destination path. Listening to the transferring of neighbors, if a node discovers that another one is malicious then a response mechanism for isolating a malicious one will be launching.

Proposed Techniques

Brain Mapping Function Scheme :

Overview of the Proposed Architecture: In Abhishek et. al [23], proposed a scheme on the real fact that everyone want to live and struggle for its existence if anyone is sure that he will not going to die because of deficiency of resources then it will be more chances that he will not cheat others for resources . The same concept is used in the core of proposed theoretical model.

The Brain Mapping Function Node: (BMFN): These nodes perform Brain Mapping functions for all nodes present in ad hoc network. The important parts of Brain Mapping nodes are

1) *IDPS module*: This Module has the capability of detection and prevention of selfish node.

2) *Turi machine*: It comprises of infinite memory capability to store virtual node.

3) *Virtualization* Layer: This Layer is used for creating virtual node.

Working of proposed model: The working of model is very simple the Brain Mapping Function Nodes (BMFN) are created in ad hoc network the number of BMFN depends on factors like area, radio range strength, data importance etc. The BMFN is very robust and effective because it takes concepts of various fields like theory of computation (TOC), neural network, artificial intelligence, and many more so it has advantages of all these fields.

The paper proposed a new technique to detect and prevent selfish node furthermore it could be possible for some networks this scheme provide fully freedom from selfish nodes and increases throughput and performance that could not be achieved till yet.

Cache Scheme :

Basic Cache Scheme: In Hongxun Liu et. al [24], proposed a technique in which, hardware assisted detection scheme, the hardware is responsible to detect the misbehavior of the software and report such misbehavior to other nodes. In the cache based detection scheme, there is a cache unit as well as a few counters. The cache stores the identity information of the recently received packets and is used to differentiate original packets from duplicate packets received by wireless node.

A mobile node could receive the same route request multiple times due to the broadcast effect during the route discovery process. When node A receives a route request packet and broadcasts that packet, its neighbor B will receive and broadcast the route request packet. Due to the nature of broadcast, node A will receive the same route request packet again from node B. If node A has a few neighbors within its transmission range, it is likely that A will receive a few duplicate route requests. The cache can help the detection hardware recognize the original route request from the duplicate route requests.

There are four counters used in the cache based detection scheme: TC (Total Counter), DC (Drop Counter), TDC (Total Data Counter) and DDC (Data Drop Counter). The first two counters are used to detect simple dropping while TDC and DDC are used to detect selective dropping. TC is used to record the total number of unique packets received, while DC is used to record how many unique packets are dropped by this node. TDC is used to record how many data packets are received by the node while DDC records the number of data packets dropped.

2ACK Scheme

In Manv*ia et. al [25]*, proposed a system which is used to detect the misbehavior routing using 2ACK and also check the confidentiality of the data message in MANETs environment. Here, author used a scheme called 2ACK scheme, where the destination node of the next hop link will send back a 2 hop acknowledgement called 2ACK to indicate that the data packet has been received successfully. The proposed work (2ACK with confidentiality) is as follows.

• If the 2ACK time is less than the wait time and the original message contents are not altered at the intermediate node then, a message is given to sender that the link is working properly.

• If the 2ACK time is more than the wait time and the original message contents are not altered at the intermediate node, then a message is given to sender that the link is misbehaving.

• If the 2ACK time is more than the wait time and the original message contents are altered at the intermediate node, then message is given to sender that the link is misbehaving and confidentiality is lost.

• If the 2ACK time is less than the wait time and the original message contents are altered at the intermediate node then, a message is given to sender that the link is working properly and confidentiality is lost.

At destination, a hash code will be generated and compared with the sender's hash code to check the confidentiality of message. Hence, if the link is misbehaving, sender to transmit messages will not use it in future and loss of packets can be avoided.

Two-Timer Scheme

In Hongxun et. al [26], proposed a hardware assisted detection scheme which can be used to detect routing attacks and packet forwarding attacks. In this scheme, the hardware monitors the upper and software layers of its own node. The hardware consists of two logical components. One component contains tamper-resistance mechanisms, protecting the hardware from hardware attacks and logical attacks. With the help of tamper-resistance component, each wireless node could be easily identified. The other component is responsible for detecting misbehavior of the upper layer.

The hardware detection unit is the foundation of defending MANET. When the software of the node is compromised or is mounting attacks, the hardware can detect the misbehavior of the software layer and report it to the network [26].

Conclusion And Discussion

As the use of Mobile Ad hoc Networks (MANETs) has increased, the MANETs security has become more important accordingly. No doubt the IDS are here to keep our systems safe; however, future systems will definitely take a different form from our modern-day versions. In this survey research, we have discussed Classification of selfish nodes detection techniques, Various Intrusion detection techniques, Various Innovated selfish node detection techniques and Various Proposed selfish node detection techniques for mobile ad hoc networks.

Intrusion detection techniques also should be integrated with existing MANET application. This requires an understanding of deployed applications and related attacks in using suitable intrusion detection mechanisms. An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the IDS systems itself. In our future we plan to propose a new efficient technique to detect selfish nodes in MANET.

Reference

[01] Parker J, Undercoffer J, Pinkston J, Joshi A. (2004). "On intrusion Detection and Response for Mobil Ad Hoc Networks", in Proceeding IEEE International Conference on Performance Computer and Communications, Workshop on Information Assurance, pp 747-52.

[02] Khairul Azmi Abu Bakar and James Irvine "Contribution Time-based Selfish Nodes Detection Scheme" ISBN: 978-1-902560-24-3 © 2010 PGNet

[03] Dipali Koshti, Supriya Kamoji "Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks", (IJSCE) ISSN: 2231-2307, Volume-1, Issue-4, September 2011

[04] S. Marti, T. Giuli, K. Lai, and M. Bakar, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annual Int. Conf. on Mobile Computing and Networking (MobiCom'00), August 2000, pp. 255–265.

[05] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputation based incentive scheme for ad-hoc networks," in WCNC 2004, 2004.

[06] S. Buchegger and J. L. Boudec, "Performance analysis of the confidant protocol: (cooperative of nodes - fairness in dynamic ad hoc networks)," in Proc. IEEE/ACM Workshop on (MobiHoc'02), June 2002, pp. 226–336.

[07] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in (CMS'02), September 2002.

[08] S.Bansal and M.Baker, "Observation-based cooperation enforcement in ad hoc networks" Stanford University, Tech. Rep., 2003.

[09] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in manets," in IEEE Transactions on Mobile Computing, 2006, pp. 536–550.

[10] K. Paul and D. Westhoff, "Context aware detection of selfish nodes in dsr based ad-hoc networks," in proceedings of IEEE Vehicular Technology Conference 02, 2002.

[11] D. Djenouri, O. Mahmoudi, M. Bouamama, D. Llewellyn-Jones, and M. Merabti, "On securing manet routing protocol against control packet dropping," in The 4th IEEE (ICPS'2007), Istanbul, July 2007, pp. 100–108.

[12] L. Huang, L. Li, L. Liu, H. Zhang, and L. Tang, "Stimulating cooperation in route discovery of ad hoc networks", in Proceedings of the 3rd ACM Workshop on (Q2SWinet'07), October 2007.

[13] Farzaneh Pakzad and Marjan Kuchaki Rafsanjani "Intrusion Detection Techniques for Detecting Misbehaving Nodes", in Computer and Information Science Vol. 4,-1; January 2011.

[14] Kachirski O, Guha R. (2003). "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks", in Proceeding IEEE, (HICSS'03), pp 57.1.

[15] Hasswa A, Zulkernine M, Hassanein H. (2005). "Routeguard: an intrusion detection and response system for mobile ad hoc networks", in Proceeding IEEE (WiMob'2005).

[16] Caballero E J. (2006). "Vulnerabilities of intrusion detection systems in mobile ad hoc networks- the routing system", Seminar on Network security, Helsinki University of Technol.

[17] Nasser N, Chen Y. (2007). Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc network*, in Proceeding IEEE (ICC'07),* pp 1154-9.

[18] Buchegger S, Le Boudec J. (2002). "Performance analysis of the CONFIDANT protocol (Cooperation of nodes fairness in dynamic ad-hoc network)", in Proceeding 3rd ACM (MobiHoc'02), pp 226–336.

[19] Michiardi P, Molva R. (2002). "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", in International Conference on (CMS'02).

[20] Bansal S, Baker M. (2003). "Observation-based cooperation enforcement in ad hoc networks", in Technical Paper on Network and Internet Architecture (cs.NI / 0307012).

[21] Huang Y, Lee W. (2003). "A Cooperative Intrusion Detection System for Ad Hoc Networks", in Proceeding of the ACM Workshop on SASN'03, pp 135-47.

[22] Abhishek Gupta and Amit Saxena "Detection and Prevention of Selfish Node in MANET using Innovative Brain Mapping Function: Theoretical Model" in IJCA, Vol. 57/12, Nov-12.

[23] Hongxun Liu, José G. Delgado-Frias, and Sirisha Medidi "USING A CACHE SCHEME TO DETECT SELFISH NODES IN MOBILE AD HOC NETWORKS" in Proceeding of the sixth IASTED July 2-4, 2007

[24] Sunilkumar S. Manvia, Lokesh B.Bhajantrib, and Vittalkumar K. Vaggac "Routing Misbehaviour Detection in MANETs Using 2ACK", in 4/2010 JT&IT.

[25] Hongxun Liu, José G. Delgado-Frias, and Sirisha Medidi "USING A TWO-TIMER SCHEME TO DETECT SELFISH NODES IN MOBILE AD-HOC NETWORKS" in Proceeding of the sixth IASTED July 2-4, 2007.