International Journal of Research in Advent Technology, Vol.2, No.2, February 2014

E-ISSN: 2321-9637

A Systematic Review on Detection of Selfish Nodes in Mobile Ad Hoc Network

Heena[1], Neeraj Kumar[2]

Department of Computer Science and Engineering[1, 2], Thapar University [1 ,2], Patiala (Punjab), India

Email: heenasingla88@gmail.com[1], neeraj.kumar@thapar.edu[2]

Abstract- To provide the security to the moving nodes in the mobile ad-hoc networks (MANETs) is always a challenging issue. Few nodes in MANETs do not participate in conversation and behave selfishly to conserve energy and battery power. Due to this selfishly behavior of nodes, performance at routing layer decreases. In this paper, we have provided a detailed analysis of different schemes for finding misbehavior nodes. A detailed comparative analysis of various schemes is provided in the paper.

Index Terms- Mobile Ad-hoc Network; Selfish nodes; Routing misbehavior.

1. INTRODUCTION

Mobile ad-hoc networks (MANETs) are self organizing, self configuring, self cooperating and infrastructure less wireless networks of mobile nodes. An emerging mobile ad-hoc networking is relying upon the communication between the mobile nodes. Routers have freedom to move haphazardly and arrange themselves promptly. Thus, topology of network may change speedily and uncertainly. In such charismatic environment, sending data packets along a path to the target becomes a critical matter.

In MANETs, all the mobile nodes behave as a router and collaborate between themselves for convenient working of the network. It is pretended that all the mobile nodes take part in activity of the network will forward the data packets to neighbor node and along path supportive of other nodes. But this assumption is not true in all scenarios. Sometimes, nodes comply to forward but unsuccessful to do because they want to conserve their energy, battery power and CPU cycles. They simply accepting the data packets targeted to them, and ignore the data of other mobile nodes without sending along a path or forward. Due to this behavior of nodes, throughput of the network decreases. These nodes are known as selfish nodes. Another type of nodes which deliberately ignore data packets, send to some other target node or change the route of data etc. These are known as malicious nodes. Both these malicious and selfish nodes come under the category of misbehaving nodes. This paper considers only selfish nodes.

Selfishness can be managed in two manners. One is to fine or punish the nodes for their selfish behavior. Another manner is to honor the nodes for their unselfish behavior. This paper is arranged as follows. Section 2 illustrates related work in this area. Section 3 defines schemes of identifying and isolating selfish nodes. Section 4 illustrates a framework for finding selfishness and section 5 gives the conclusion.

2. RELATED WORK

2.1. *Credit Based System*

Credit based mechanism is also known as incentive based mechanism. In this mechanism, nodes are not fined due to their selfish behavior rather than prizes given to unselfish nodes for supporting other nodes. This encourages the association of nodes in the MANETs.

Chee-wah Tan et al. [1] proposed a cost credit model to accomplish collaboration. With the use of cost credit model, nodes can deliver large amount of data packets. Drawbacks of this method are: 1) a virtual bank is needed to handle awards, 2) when a node sufficient or awards to forward its own data, it may decide not to collaborate with other nodes in the network and initiates denying packets.

2.2. *Secure Incentive Protocol*

Yanchao Zhang et al. [2] rooted more characteristics from [3] and [4]. This scheme guesses every mobile node (MN) consists a tamper-proof security modules like GSM networks have SIM cards, which considers functions relevant to security and every intermediate node (IN) inserts genuine stamps on the forwarded data packets as a evidence of forwarding SIP (Secure Incentive Protocol) treated credits as the inducement to encourage packet forwarding.

For this aim, every smart-card contains a credit counter (CC) which is pre-loaded with satisfied amount of incentives before drop out. The loading and awarding on a mobile node is accomplished by reducing or raising the CC in that particular node. If the MN is turn off then also CC will passes its value. When MN is turn on freshly, it could retain the incentives in CC. To assure the security of SIP, every

smart card has private and public keys. The nodes do not know about the numbers contained in the smart card and CC value cannot alter by illegal way. SIP is based on session and primarily containing three phases. In session initialization phase which is first phase, a session initiator (SI) consults session numbers and messages with session responder (SR) and INs among them. And every IN inserts a genuine stamp on every data packet sent and SI/SR assemble stamps for purpose to rewarding in next phase which is data forwarding phase. Rewarding phase which is the last phase, satisfied number of incentives given to every IN based on number of packets forwarded by that particular node. Benefits of this method are: 1) SIP is an independent routing protocol. It can synchronize with other on demand routing protocols like AODV (Ad-hoc On Demand Vector)) and DSR (Dynamic Source Routing), 2) it is a session based protocol and 3) it has temper-proof security module. So, illegal access is not possible. Drawback of this scheme is that each nodes need to contains hardware module because SIP is executed in hardware module. Already present mobile nodes don't contain hardware module.

2.3. *Stimulating Cooperation in Self Organizing Manets*

L. Buttayam et al. [4] concentrates on packets sending and they notice the issue of encouraging collaboration in self managing MANETs. This method works on security module or hardware module which is temper resistant. This security module preserves a nuglet counter. When a node sends data packets for the advantage of other mobile nodes in the network value nuglet counter is incremented by one. Each node has to retain a positive counter value, if node wants to send its personal data packets. Security module preserves the counter from unauthorized guidance. This scheme guarantees that selfishness of nodes is not profitable. But In general possibility of security module is not ensured.

2.4. *Sprite*

SPRITE (Simple Cheat Proof Credit Based System) was proposed by zhang et al. [5]. The main concept of this method is as follows: a credit clearance service (CCS) is imported to conclude the load and incentive to every node engage in the communication of message. When a node accepts an information, the node retains a acknowledgement of delivery of information and later informs it to the CCS, when the node contains quick communication with CCS. Reward and charges are decided from game theory aspect. The source node rather than the target node is loaded in order to avoid DOS (Denial of Service) attack in the target node by forwarding it huge number of traffic [6]. If node tries to send data packet is repaid but the incentive a node accepts rely upon whether or not its forwarding is profitable if the neighbor node, on the route dispatches a valid acknowledgment of delivery to CCS.

2.5. *Game Theory*

Gupta et al. [7] proposed the game theory algorithm. In this approach, every node treated former experiences to conclude the best route to forward the data packet. The volume of processing power applied is relying upon the particular node. The more power utilized, the best route can be picked, but large amount of power is wasted.

As every node contains finite quantity of battery power, the node must pick among utilizing a huge volume of its power to detect the best route, or utilize a less volume of its power and take risk with another route.

Three selfish operations and equivalent remedies are explained in this paper:

- After accepting a data packet, a selfish node may deliver acknowledgment of delivery. But does not send the packet. To avoid this, the CCS should offer large amount of incentive to a particular node that sends the data packets to stimulate a selfish node to send another node's data packets also. To accomplish this purpose, if the target node does not submit the acknowledgment of delivery, the CCS first concludes the last node on the route that has ever accepted the data packet. Then the CCS gives less credit to this last node as comparison to it gives to every predecessors of the last node [5].
- A node accepted information may not dispatch the receipt. This happens if the source node connives with the in between nodes, thus the source node can give credits to the node in the background allowance, which is more than the CCS will give and source node still achieve a net profit. To avoid cheating activity, the CCS loads the source node an auxiliary quantity of incentive if the target node does not dispatch the acknowledgment of delivery thus colluding class achieve no profit.
- Dispatching an acknowledgement of delivery to the CCS is enough for receiving incentives, a class of colluding nodes may send only acknowledge of delivery of a message, rather than sending the complete data packet to its follower node.

Two scenarios are studied: 1) target node colludes with middle node, 2) target node does not conspire with middle nodes. In the first scenario, the data packet is for the target node and if the target really comply the acknowledgement of delivery, then the middle nodes and target should be given credits as if no cheating had occurred. In the second scenario, if the target node does not dispatch a acknowledge delivery of data packet, the incentive is given to every node should be increased by a chunk, a, where $a<1$.

The author demonstrates the accuracy of the acknowledgment of delivery submission method with

the help of game theory. Main objective of this method is for sending data packets in unicast manner. It can be continued to path detection and multicast as well. This method may have various problems:

- Acknowledgment of delivery of every node throughout a route may be complied with the CCS at various times, making it hard for the CCS to conclude the original credits given to every node [5].
- The mechanism [6] is dependent on DSR, which involves the route in the sending information ahead. A misbehaving node not on the route can conspire with other nodes on the route to produce a receipt and cheat the CCS.

3. IDENTYFYING AND ISOLATING SELFISH NODES

This section illustrates the mechanisms those are involved for expelling the nodes for their misbehavior. Selfish nodes are determined and detached from the network. They are ceased from utilizing the network services. Most of the schemes in the literature are perusing punishing mechanism instead of awarding mechanism.

3.1. *Watchdog and Pathrater*

When a node sends data packet information, the node's watchdog demonstrates that the later node in the route also sends the data packets [6]. The watchdog does this by hearing promiscuously to forward node's communication. If the later node does not send packet, then it is treated as misguiding. The pathrater utilizes this information of misguiding nodes to pick the network route to transfer packets. The nodes depend on their peculiar watchdog particularly and do not transfer reputation data message with other nodes. Fig. 1 explains the working of watchdog. Guess there occurs a route from X to Y via in between nodes P, Q and R. Node P cannot conveys all the path to node R, but it can hear on node Q to send to R, can generally say if Q conveys the message. If encryption is not implemented individually for every transmission, which can be costly, then P can also say if Q has compromised with the header or payload of the data packet.

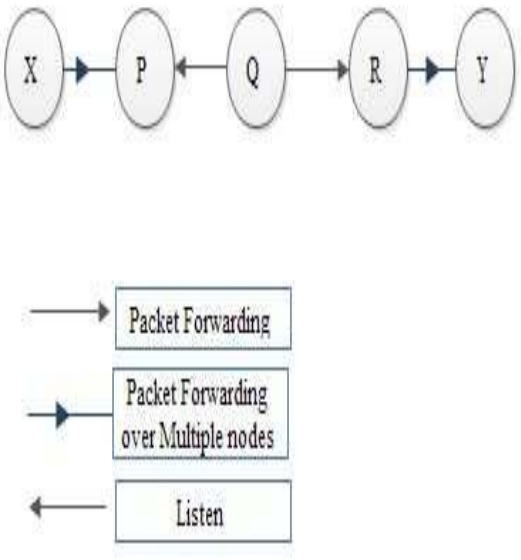

Fig. 1. Watchdog Method [6]

When Q sends the message from X to Y via R, P can listens Q's communication and can demonstrate that Q has tried to forward the message to R. The directed line denotes that P is under communication range of Q and can hear the sent message. The solid line represents the direction of message sent by P to R. The watchdog is started by managing a buffer currently message and correlating every overhead message with the message in the buffer to watch if there is equality. If so, the message in the buffer is deleted and erased by the watchdog. If the message has kept in the buffer for more time instead of finite time out, the watchdog raises a decline tally for the particular node answerable for sending of the message. If value of a tally is more than a finite value, it concludes that the node is misguiding and forwards a message to the sender regarding the node's misbehavior. In the network every node can run pathrater, includes the information of misguiding with communication data to choose the path. If there are different routes to same target node, the route with large value of metric is picked. The scheme is called as pathrater.

A high negative value is given to nodes which are detected as selfish nodes by watchdog technique. When path rater computes the value of path parameter, negative route value represents the presence of more than one misguiding nodes in the route. So, nodes with negative grades should have their grades slowly raised. In watch dog and path rater scheme, wireless medium which support promiscuous node activity are guessed, which is not suitable for all MANETs scenarios.

3.2. *Core*

Michiardi et al. [8] proposed a cooperative reputation (CORE) scheme that also has a watchdog constituent for examine. The value of reputation is utilized for conclusion about collaboration or isolation of the node. Reputation values are achieved by respecting nodes as requesters and providers, and correlating the familiar conclusion to the real achieved conclusion of a request. In CORE, scope of the value of reputation is from positive (+) via null (0) to negative (-). The benefit of this scheme is that containing a scope from negative to positive and grants good behavior to be awarded and misguiding nodes to be punished. This method provides more significance to the recent behavior and hence sustainable infrequently bad behavior e.g. failure of battery power. But guesses that the recent behavior to be representative of the future behavior may make the mobile nodes to increase incentive and then initiate behaving like selfishly.

3.3. *Confidant*

CONFIDANT (Cooperation of Nodes Fairness in Dynamic Ad-hoc Network) [9], assembles clue from past events and instructions. Trust cooperation is achieved among nodes dependent on assembled clue. Trust conclusions are made based on these collaborations. There are four mutually dependent modules: 1) monitor, 2) reputation mechanism, 3) trust manager and 4) path manager. Monitor assembles clue by examining the communication of neighbor node after sending information to other neighbor node. It then dispatches to the reputation mechanism only if the assembled clue indicated misbehavior. Reputation mechanism transmits the grades for a node if the clue assembled for a node's misguiding behavior is more than the previously illustrated threshold value. Then, manager of the path draws a conclusion to erase the misbehaving node from the route. Path manger also helps the node to make the conclusion like whether to send accepted message by verifying the recent node's existence in the black list. The manager of trust is answerable for sending and accepting instructions to and from reliable nodes. Here instructions are also called ALARM messages and reliable nodes are called as friends. The ALARM data packets accepted from reliable nodes are calculated for checking reliability before being forwarded to reputation mechanism. Trust manager helps in taking trustworthy conclusions for the following: 1) give and receive routing messages or data packets, 2) receive a node as a chunk of a path and 3) execute path developed by few another nodes. CONFIDANT demonstrates to display good performance of the network which includes the malicious nodes correlated to DSR protocol.

3.4. *Ocean*

OCEAN (Observation-based Cooperation Enforcement in Ad-hoc Networks) protocol was proposed by Bansal et al. In [10]. OCEAN is the extended version of DSR. Mechanism such as reputation and monitoring is utilized in this protocol. In OCEAN, each network node has grades for every neighbor mobile node and examines their nature in promiscuous mode. This protocol has two categories of routing misbehavior: 1) selfish and 2) misleading. Node which takes part in route discovery scheme but does not send the data packets to other nodes in the network is called as misleading node. Selfish node does not involve in route discovery mechanism. For finding the misleading nodes, after sending a data packet to neighbor node, forwarding node stores the data packet. When the neighbor node sends the packet to other nodes in the network in given time interval, then it is examined. It generates a event (positive or negative) as its results of examining are used to upgrade the grades of neighbor node. If rating is less than value of pre-defined threshold, then neighbor node is placed in both issuing node's list and avoid list. According to conclusion all traffic will not utilize this issue node. A finite time is given to this issue node to come back to network because it may be possible that some misleading node has misleads this particular node or if it is a selfish node, then node must improve in given time interval.

3.5. *ExWatchdog*

ExWatchdog (Extended Watchdog) was proposed by Nidal Nasser et al. In [11]. ExWatchdog is the extended version of watchdog. This scheme is used to find the misbehaving nodes and informs to Pathrater. Every mobile node upgrades ratings of node with respect to the data packets given by any mobile node in MANET.

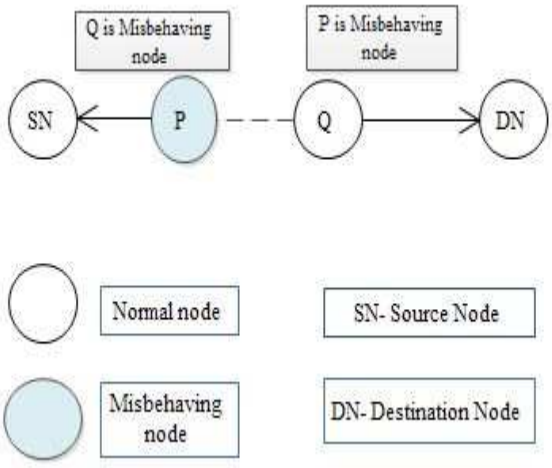

Fig. 2. ExWatchdog Scheme [11]

Every node contains watchdog and rely upon over-listening. So a critical issue arises when a network node which is over-listening and informing itself as misbehaving node, and then it can effect the performance of network. In fig. 2, mobile node P could inform the node Q is not sending data packets in

fact it does. Due to this source node (SN) tick the Q as malicious node, but in actual P is a problematic node. Encryption based technique is also used in ExWatchdog. It also maintains a table which contains information of source node, target node, sum (total amount of data packets sends or accepts) and route. Thus it can find if mobile nodes wrongly informs other nodes as malicious. The basic concept of this method is its ability to establish misbehaving mobile nodes those can split the MANET by wrongly informing other nodes in the network as malicious. This scheme fails when mishbehaving node is on all routes among particular sender and target node.

3.6. *Cache Mechanism to find Selfish nodes*

Hongxun liu et al. [12] proposed a hardware supported disclosure mechanism is introduced and calculated. In this mechanism, the hardware can find the misbehavior directed by the misguiding nodes. Selfish node either denies all the information not concerned to it or denies the information only. After finding the misguiding nodes, the hardware will dispatch the selfish node to other nodes in the network. Another node will utilize the data packets accepted to secure the network. In this mechanism, there is a split among software and hardware in a mobile node. The software could be misguiding in nature, but hardware is secure module and maintaining trust communications between nodes in the network. Here the main concentration is on the disclosure of misguiding node which denies information. There are four counters utilized in the scheme: 1) total counter (TC), 2) drop counter (DC), 3) total data counter (TDC) and 4) data drop counter (DDC). TC and DC are utilized to find simple dropping, in which selfish node will deny all the information not to or from them. While TDC and DDC are utilized to find selective dropping, in which selfish node will deny only information not to or from them rather them sending the route reply and request packets. To improve the performance of disclosure, a penalty timer is introduced. This timer utilizes to give extra penalty if a particular node does not send a route request control packet. Penalty timer is initiated only when an actual control packet is accepted. The cache entity in the disclosure hardware can inform if the accepted control packet is authentic or equivalent. This scheme can find the selfish nodes correctly in term of disclosure of effectiveness and false positive in both simple and selective dropping methods. Software layer is needed some changes, but it is hardware dependent scheme which is practically hard to start.

3.7. *Reputation based Schemes to Isolate Selfish nodes*

M. Tamer Rafaei et al. [13] proposed reputation dependent scheme which create trust between nodes. The scheme depends upon the concept that node individually (i.e. no collaboration with other nodes) calculates its neighbor nodes based on completion of work. Trust organized based mechanism does not depend on the examining of next nodes communications and change of reputation data packets between the nodes. Thus contains low overhead, and the scheme does not depend on routing protocol. This mechanism gives scattered reputation calculation method started individually or separately at each node in MANET with concept of determining and detaching selfish nodes. Every node has a reputation table, in which reputation index is preserved for immediate nodes of each node in the network. A node gives a reputation index to all of its neighbor nodes based on outstanding delivery of information sent via neighbor nodes. For every successful delivery of information, every node along a path raises the reputation index of its next node that sent the information. Unsuccessful deliveries of packet conclude a punishment given to such neighbor nodes by decreasing their index value by one. The success or failure of the data packet information is achieved from the feedback accepted by the target node. This function is utilize to evaluate the reputation index is design conclusion that is effected by factors involves behavior of nodes, location of node etc.

To avoid the selfish behavior and give inspiration for nodes to develop their reputation, every node concludes whether to send or deny a data packet with respect to reputation of packet's predecessor node. If the node's reputation index value falls below a pre-established threshold value all data packets sent via that particular node discarded and node become isolated. Benefits of this scheme are: 1) isolation of routing protocol, 2) no need to examining the next or previous nodes in the promiscuous mode, 3) overhead decreases if mobile nodes do not send reputation related data and 4) value of reputation index is evaluated without the assistance of neighbor nodes, thus cooperative misbehavior can be decreased. But the issue with this scheme is that , it utilizes feedback schemes such as acknowledgements of transmission control protocols in connection based application for recognizing whether a data packet has successfully reached to target node or not. Thus, this scheme is not applicable for connectionless applications. The reputation schemes individually evaluates the behavior of mobile nodes in the network, thus there are large number of possibility for false positives.

4. A FRAMEWORK FOR FINDING SELFISH NODES

This paper [14], represents about a framework rely upon Dempster-Shafer theory-based selfish behavior nodes detection framework (DST-SDF) with few mathematical feedback. The DST-SDF is committed for MANETs rely upon standard routing protocols

such as DSR. The basic objective depend upon end-to-end successful information delivery in the following manner: each time a sender forwards a data packet to the target node, it waits for the finite pre-established time for a successful delivery of a packet. If the acknowledgement is received in predetermined time, a sender can say that all the mobile nodes along a route are collaborative in nature. Otherwise there are misbehaving nodes along a route. On the basis of acknowledgement received or not in a particular time, a recommendation message is forwarded to all the nodes in the network to describe about the situation. Each node contains a constituent, executed a DST-based algorithm that utilizes accepted instruction packets to calculate the misbehavior of every node. The concluded values can be utilized as routing parameters.

5. COMPARISON

Most of the mechanisms are rely upon trust relationship among nodes in the network. Watchdog used in many of schemes, but has various drawbacks and not able to do work accurately due to collisions in the network. When every node has various transmission ranges or executes antennas, the watchdog cannot examine the neighbor nodes correctly. ExWatchdog is developed to reduce the issue of overhearing of the watchdog. Thus, if the mobile node which is overhearing and informing itself as misbehaving, then it can affects the performance of MANET. OCEAN is used to prevent the vulnerabilities of nodes. CONFIDANT raises this problem implicitly. CORE cannot find misbehaving nodes which create problem in routing behavior. Reputation based scheme used the reputation index to find the misbehaving nodes in the network. Nodes in this scheme are autonomous in nature. In cache based scheme, various counters are used to find the packet dropping methods and penalty timer is used to give the punishment to misbehaving nodes for their selfishness.

The credit-based mechanism needs temper-proof hardware, connection to internet and more security for payment methods. Currently we are dealing with performance of reputation based mechanisms with respect to reduction of transmission overhead and improvement of throughput.

TABLE I. COMPARISON OF MECHANISMS FOR DETCTION OF SELFISH NODES IN MANETS

Mechanisms	Observation		Finding Misbehavior				P	PMNPD	A
	SN	NN	Selfish		Malicious				
			R	PF	R	PF			
Watchdog / Pathrater	Y	N	N	Y	N	Y	N	N	DC
CORE	Y	N	Y	Y	N	N	Y	N	DC
CONFIDANT	Y	Y	Y	Y	Y	Y	Y	Y	DC
OCEAN	Y	Y	Y	Y	N	N	Y	Y	SA
ExWatchd-og	Y	N	N	Y	Y	Y	N	N	DC
Cache-based	Y	N	Y	Y	Y	Y	Y	Y	DC
Reputation based	Y	N	Y	Y	Y	Y	Y	Y	DC

NN= Neighbor to Neighbor; SN = Self to Neighbor; R = Routing; PF= Packet Forwarding; P = Punishment; DC = Distributed and Cooperative; A = Architecture; SA = Stand Alone; PMNPD = Prevent Misbehaving Node in path detection; Y = Yes; N = No.

6. CONCLUSION

This paper explains various schemes for dealing with the selfish behavior of nodes. Detection of Selfish nodes is one the prominent issue for MANETs since they influence the throughput of the network. This paper provides a detailed analysis of various selfish nodes detection schemes in the literature. Detailed comparative analysis of various schemes with respect to various metrics is also provided in the text.

References

[1] Chee wah Tan, “Enforcing cooperation in an ad hoc Network using cost-credit based forwarding and Routing Approach”, WCNC, IEEE, 2007.

[2] Yanchao Zhang , Wenjing Lou , Wei Liu, Yuguang Fang, “ A secure incentive protocol for mobile ad hoc networks” in Journal of Wireless Networks, 2007.

[3] L. Buttyan and J.P. Hubaux, “Enforcing service availability in mobile ad-hoc WANs”, in Proc. of IEEE/ACM MobiHoc, 2000.

[4] L. Buttyan and J.P. Hubaux, “Stimulating cooperation in self-organizing mobile ad hoc networks,” ACM Journal for Mobile Networks, 2003.

[5] S.Zhong, J.Chen, and Y.R.Yang, “ Sprite: A Simple, Cheat Proof, Credit based System for Mobile Ad Hoc Networks”, in Proceedings of INFOCOM, 2003.

[6] S.Marti, T.Giuli, K.Lai and M.Baker, “Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks,” in Proc. ACM MOBICOM, 2000.

[7] Gupta, Rohit, and Arun K. Somani. "Game theory as a tool to strategize as well as predict nodes' behavior in peer-to-peer networks." In Parallel and Distributed Systems, 2005. Proceedings. 11th International Conference on, 2005.

[8] Pietro Michiardi and Refik Molva, “CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” Sixth IFIP conference on security communications, 2002.

[9] Buchegger, Sonja, Le Boudec, Jean-Yves, " Performance Analysis of CONFIDANT Protocol: Cooperation of Nodes - Fairness in Dynamic Ad-Hoc Networks," in Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC). IEEE, 2002.

[10] S. Bansal and M. Baker. "Observation-Based Cooperation Enforcement in Ad-hoc Networks" , Techical Report, Stanford University, 2003.

[11] Nidal Nasser and Yunfeng Chen, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks", Proc. ICC, 2007.

[12] Hongxun Liu, José G. Delgado-Frias, and Sirisha Medidi, "Using a cache scheme to detect selfish nodes in mobile adhoc networks " in proceedings of IEEE international Conference on Networks, 2007.

[13] M. Tamer Refaei, Vivek Srivastava, Luiz DaSilva, Mohamed Eltoweissy, " A Reputation-based Mechanism for Isolating Selfish Nodes in Ad Hoc Networks",in Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems, 2005.

[14] Jerzy Konorski and Rafał Orlikowski "A Framework for Detection of Selfishness in Multihop Mobile Ad Hoc Networks " in Jounral of telecommunications and information technology, 2009.

[15] Hameed Janzadeh, Kaveh Fayazbakhsh, bahador bakshi, "A secure credit-based cooperation stimulating mechanism for MANETs using hash chains", Future Generation Computer Systems –Elsevier, 2009.