MDAC: A New Reputation System for Misbehavior Detection and Control in Ad Hoc Networks

Marianne A. Azer
Ministry of Communication and Information Technology
National Telecommunications Institute
Nile University
Cairo, Egypt
mazer@nu.edu.eg

Noha Gamal El-Din Saad
Nile University
Giza, Egypt
Noha.Gamal@nileuniversity.edu.eg

Abstract— **Reputation systems are an emerging area of research in ad-hoc networks. They have been introduced as a security solution for nodes' misbehaving problem. A reputation system should cope with any kind of misbehavior. It enables honest nodes to make fair decisions about their neighbors. This may encourage nodes to behave well and cooperate in order to avoid being penalized or isolated. In this paper, we propose a new reputation system for Misbehavior Detection And Control in ad hoc Networks (MDAC). It aims to overcome some of the unsolved issues of other reputation systems, and it is customizable for any ad hoc network. Robustness, stability, and fairness are all primary aspects of a successful reputation system. MDAC adopts a strategy of specific information sharing and collection in order to minimize traffic overhead, and also to override the false reports from nodes about each other. The reputation system's structure is presented, and the new features of the proposed approach are discussed. MDAC's functionality has been tested and evaluated through simulations compared to the OCEAN-DSR protocol.**

Keywords— Ad hoc networks; misbehavior; MANETs; reputation; security; trust.

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) consist of self-configurable nodes, they have no fixed infrastructure [1]. They are stand alone or connected to the bigger internet as per the different applications. MANETs use wireless radio frequency channels to transfer data. Because of the limitations of the radio channel's bandwidth, nodes are obliged to depend on each other to relay data or control messages using their built-in radio hardware [2]. The dynamic nature of MANETs adds many challenges to the network management techniques. For example, routes between nodes are discovered and stored using routing protocols, which must be able to handle the rapid and dynamic change in network topology. MANETs are usually launched in an unsupervised environment, where nodes face many threats and attacks. Node subversion is one of the most recognizable attacks, where any node can be compromised or replaced by a completely new node. The new node is meant to have a malicious behavior in the network. Compromised node can be the gate for many other malicious nodes, which could present a major threat to the whole network. Because of MANET's characteristics such as lack of infrastructure, shared bandwidth, and open physical environment, there is a need to a trust based communications schemes. Reputation plays an essential role in peer-to-peer communications. Reputation in ad hoc networks is the opinion that each node has about its neighbors. Reputation can be defined as "Beliefs or opinions that are generally held about someone or something" [3], it can also be defined as "A wide spread belief that someone or something has particular characteristics" [4].

In this paper, we propose a reputation system that observes the nodes' behavior and assigns reputation values accordingly. These values are used afterwards to penalize the misbehaving nodes. They can also be used to give incentives to the well behaving ones. The remainder of this paper is organized as follows. Section II presents related work and literature review. Section III describes the proposed system's structure and functionality. Section IV presents MDAC's functionality test using simulations compared to the OCEAN-DSR protocol. Finally in section V, conclusions and future work are presented.

II. RELATED WORK

Because of their similar objectives, most of the reputation systems share common phases. Those are; Preparation and Construction, Calculations, Propagation and Broadcasting [5] [6] [7] [8] [9] [10] [11] [12]. Reputation systems are being used for enhancing security in different areas. These systems are featured to be lightweighted, easy to use and capable of facing a wide range of attacks. Among these mechanisms, CORE [8], and OCEAN [13]. Unlike to cryptographic solution, reputation systems do not depend on on the conventional use of a mutual secret to establish trusted and confident communication between two parties. Instead, they are simply established upon each other's observations. As in ad hoc networks cooperation between nodes are inspired by social behavior, reputation systems are used for enhancing security in such model. Reputation systems are used to decide who is trustworth and who is not, also to

978-1-4673-7825-3/15/$31.00 ©2015 IEEE

encourage trustworthy behavior. Resnick and Zeckhauser [14] identify three goals for reputation systems:

- Provide information to distinguish between a trustworthy party and an untrustworthy party.
- Encourage parties to act in a trustworthy manner.
- To discourage untrustworthy parties from participating in the service the reputation mechanism is present to protect.

II. PROPOSED SYSTEM STRUCTURE

In this section, we propose MDAC, a new reputation system for misbehavior detection and control in ad hoc Networks. MDAC aims to mitigate most of other reputation systems problems and drawbacks. There are four building blocks in this system. The observer, the modeler, the hybrid dissemination, and the decision making modules. They will be presented in sections A, B, C, and D respectively. Fig. 1 depicts the proposed system MDAC's architecture.

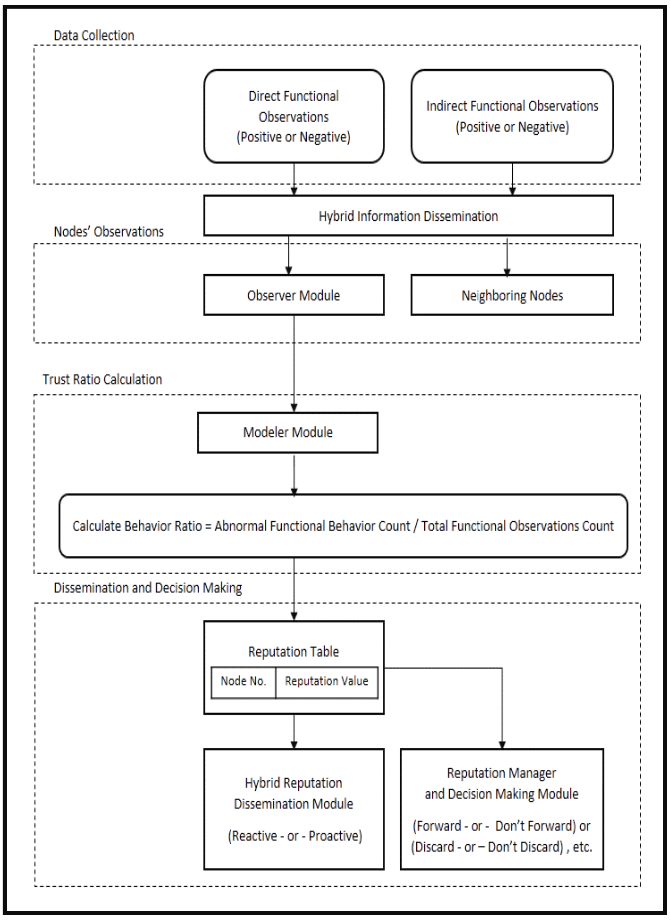
Data Collection
Direct Functional Observations (Positive or Negative)
Indirect Functional Observations (Positive or Negative)
Hybrid Information Dissemination
Nodes' Observations
Observer Module
Neighboring Nodes
Trust Ratio Calculation
Modeler Module
Calculate Behavior Ratio = Abnormal Functional Behavior Count / Total Functional Observations Count
Dissemination and Decision Making
Reputation Table
Node No.
Reputation Value
Hybrid Reputation Dissemination Module
(Reactive - or - Proactive)
Reputation Manager and Decision Making Module
(Forward - or - Don't Forward) or (Discard - or – Don't Discard) , etc.

Fig. 1. MDAC's architecture

A. MDAC Observer Module

The observer module monitors each node in the network and aggregates its available information. The information collected is either direct first hand observations locally obtained by each node or indirect second hand observations by neighboring nodes. The observer module makes use of the watchdog component [15] [16] based on the promiscuous mode.

Second hand observations are used to provide a secondary opinion in order to help fair evaluation for each node's trustworthiness. In addition, using second hand information helps building up trust quicker due to the ability of nodes to learn from other nodes' mistakes.

MDAC adopts a strategy of specific information sharing and collecting in order to minimize traffic overhead, and also to override the false reports from nodes about each other. Each node only keeps track of the total amount of incoming packets for local neighbors (positive information), in addition to the observed abnormal behavior (negative information).

Nodes keep record of the total delay produced by each node in the neighborhood by monitoring the sum of total time taken to deliver all packets and the total number of incoming packets, and so on. Each node collects certain functional parameters continuously, in order to determine trust worthiness in a fair way.

After having a preliminary vision about the trustworthiness of its local neighbors, each node shares this information with its neighbors and the observer module. This dissemination is designed to be hybrid, comprising both proactive and reactive actions. Nodes share the preliminary opinion about neighbors every certain dissemination interval if and only if there is a certain amount of change in the pre-defined trust value of each neighboring node. If there is no change, then nodes do not disseminate anything. This is in order to avoid causing unnecessary traffic overhead.

All these observations and periodical updates (if any) are then forwarded and stored at the observer's module which in turn handles all available information to the modeler Module.

B. MDAC Modeler Module

This module is responsible of combining all collected direct/indirect, positive/negative functional information about each node into a meaningful reputation values. It is also responsible for keeping this value up to date and visible. In order to minimize false reporting either by accusing benign nodes for being malicious or trusting a malicious or a misbehaving node by mistake, information modeling in MDAC takes into consideration only one parameter at a time. For example, this parameter can be forwarding packets or generating route reply and so on. The MDAC's information modeling scheme is summarized in the flow chart shown in Fig. 2.

The proposed system adds more weight to past observations. The reason for this is that benign nodes may temporarily misbehave due to technical problems within the network or critical battery conditions. Recent observations are also important for calculating reputation measure in order to enforce a cooperative behavior between nodes all the times. It follows that if a node starts to misbehave on purpose, it will be discovered in a short period of time. Therefore, nodes cannot depend on their aging in the network and their previous positive reputation. They should keep a cooperative behavior in order to maintain their good reputation.

C. *MDAC Hybrid Dissemination Module*

This module is responsible of propagating the reputation values of nodes. After MDAC finishes calculating all nodes' reputation values, it builds an up-to-date reputation table that is disseminated in a reactive way to any requester node questioning about other node's reputation. It is disseminated in a proactive way such that if there is any change in the nodes' reputation values, the new updates will be propagated on timely basis.

D. *MDAC Reputation Manager and Decision Making Module*

This component is responsible of making reputation decisions according to the information provided by the modeling component. It is responsible for guiding nodes in the network to decide any of the following actions with other nodes in the network: (trust / don't trust), (cooperate / don't cooperate), (forward / don't forward).

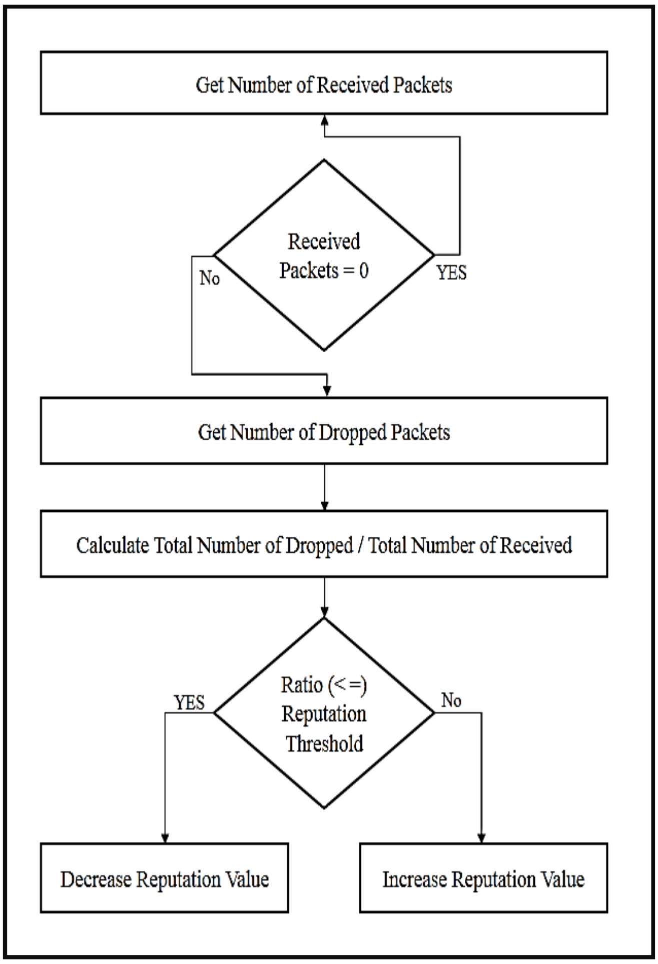
Get Number of Received Packets
Received Packets = 0
No
YES
Get Number of Dropped Packets
Calculate Total Number of Dropped / Total Number of Received
Ratio (<=) Reputation Threshold
YES
No
Decrease Reputation Value
Increase Reputation Value

Fig. 2. MDAC's modeler component flow chart.

In MDAC, the reputation metric completely depends on functional parameters. Therefore, the decision about misbehaving nodes should also be functionally based. It follows that if a node is misbehaving in forwarding packets, other nodes can penalize such behavior by not forwarding any packets for the misbehaving node's sake. Also if a misbehaving node is delaying packets, then other nodes can simply minimize the transmission priority of the misbehaving node's packets, and so on. In this module, when a node requests a certain network function, other nodes check its reputation value first to decide if the node is eligible for the service or not.

III. SIMULATION RESULTS

This section presents the simulations done in order to evaluate the performance of MDAC in the presence of the selective dropping Grayhole attack [16] [17] [18]-Grayhole node is selectively responding positively to any route request even if it doesn't have any proper information about the route, then it drops all her incoming packets-. The proposed system is simulated and assessed using the OPNET Modeler 14.5. OPNET stands for Optimized Network Engineering Tools, and it is a software for network modeling and simulation [19]. MDAC's performance was simulated and compared to OCEAN-DSR protocol [13].

Table I and Table II show the parameters used for the simulation, and testing scenarios applied respectively.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
MAC Protocol	802.11b
Max Throughput	11 Mbps
Mobility Model	Default Random Waypoint
Ad-Hoc Routing Protocol	DSR
Nodes in Simulation	40
Sender Nodes	2 (Node 1 - 2)
Receiver Nodes	1 (Server)
Transmission Range	250 meters
Transmit Power	0.0002 watts
Simulation Area	10000 meters x 10000 meters
Simulation Time	2000 seconds
Node Speed Uniform	0 - 10 meters/second
Reputation Threshold	(+40)
Punishment Methodology	Malicious node is discarded from the route for 20 seconds then returned back

TABLE II. MDAC SIMULATION SCENARIOS

Scenario No.	Percentage of Malicious Nodes	Comments
1	(0%)	This scenario is designed to collect observations about malicious node (s) in case of Grayhole attack (Selective dropping packets misbehavior)
2	(12%)	
3	(25%)	

A.MDAC's Simulation Results

For each scenario mentioned in table II, after simulating the network topology, behavioral statistics related to the monitored functions are collected before and after using

MDAC. Examples of the collected statistics are the Number of Total Packets Transmitted, Number of Total Packets Received, Number of Total Dropped Packets, Number of modified Packets, Delay Time, Number of Hops, average throughput, and average delay… etc. The resulting network performance parameters are then compared to those resulted by using OCEAN-DSR. In the first scenario with 12% malicious nodes in the network, it was noticed that the overall network's throughput has degraded to 84% of the original throughput due to the Grayhole attack. After using MDAC the throughput has increased to 94% of the original throughput of the network despite having those malicious nodes active in the network as shown in Fig. 3. In addition, in the second scenario having 25% malicious nodes in the network, it was noticed that the overall network's throughput has degraded to 56% of the original throughput. After using MDAC, the throughput has increased to be 78% of the original throughput as shown in Fig. 4. It is noticed that average delay has been increased by 44% in case of 12% malicious nodes but after using MDAC the network's average delay was returned to its original value as shown in Fig. 5. For 25% malicious nodes, MDAC helped keeping the delay 82% less than the case before using MDAC as shown in Fig. 6. Simulations have shown that MDAC is also capable of discovering the misbehaving nodes accurately.

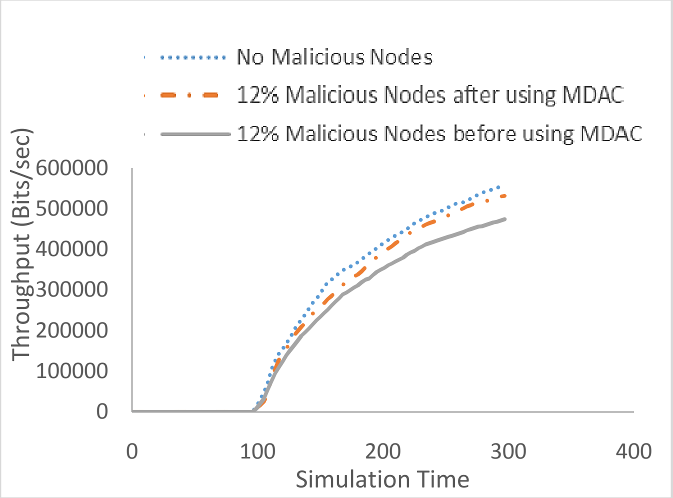

Fig. 3. Average network throughput before and after using MDAC in case of 12% malicious nodes

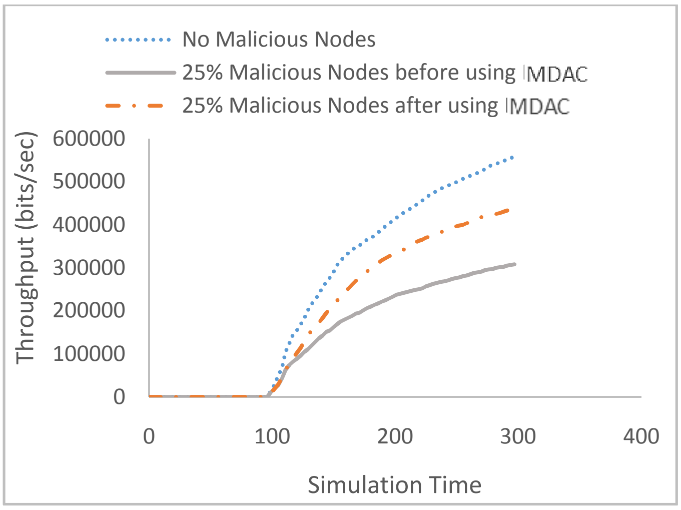

Fig. 4. Average network throughput before and after using MDAC in case of 25% malicious nodes

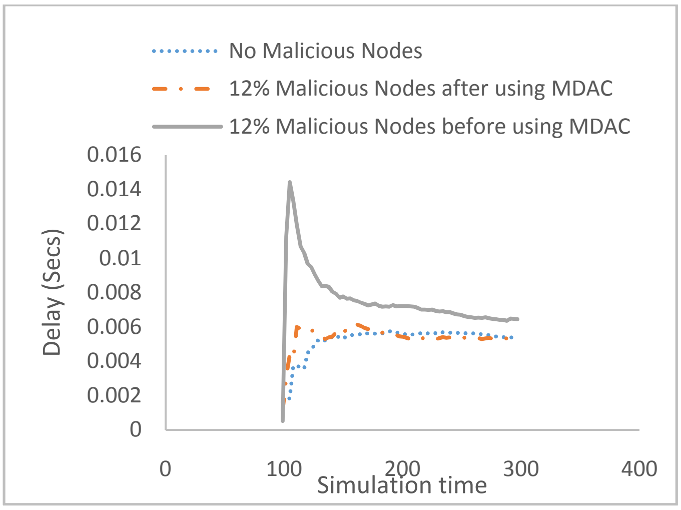

Fig. 5. Average network delay before and after using MDAC in case of 12% malicious nodes

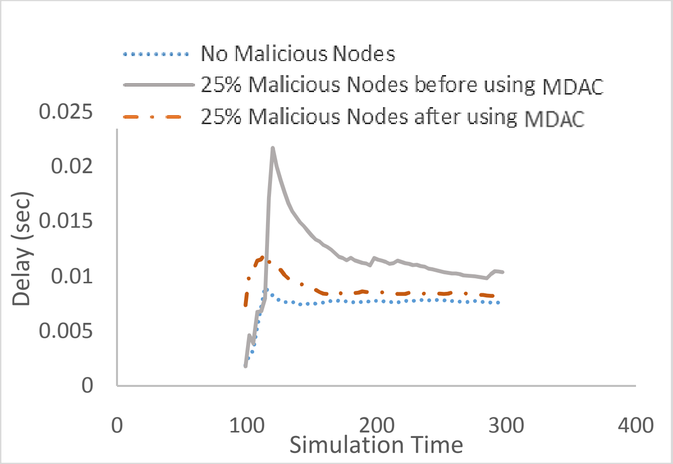

Fig. 6. Average network delay before and after using MDAC in case of 25% malicious nodes

B. Comparison between MDAC and OCEAN Regarding improving Network's Performance

As per A. Ghandar the founder of OCEAN-DSR [13], OCEAN-DSR succeeded to maintain the throughput of the network in case of 12% malicious nodes to an average of 81% of the actual throughput and in case of 25% malicious nodes to an average of 68%. OCEAN-DSR proved to decrease the average delay of packets in the presence of malicious nodes. This is expected because in normal DSR, the dropped packets are re-sent again which increase the overall delay. OCEAN-DSR has decreased the overall delay by 78% in case of 12% malicious nodes and decreased the delay by 80% in case of 25% malicious nodes. This shows the strength of MDAC compared to OCEAN-DSR as one of the recognizable reputation systems for ad hoc networks as depicted in Fig. 7 and Fig. 8.

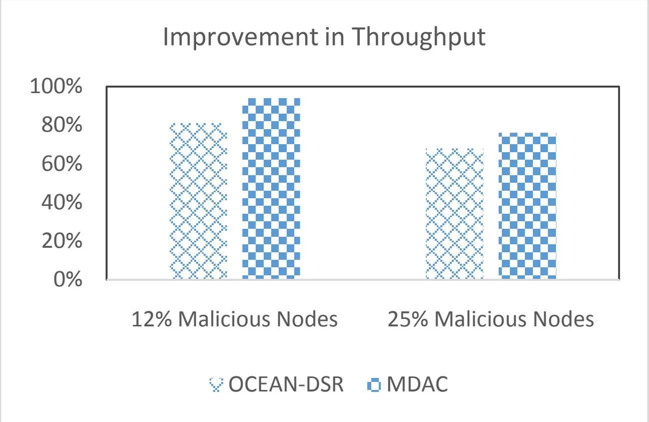

Fig. 7. Comparison between Throuput's imporovement using both OCEAN-DSR and MDAC

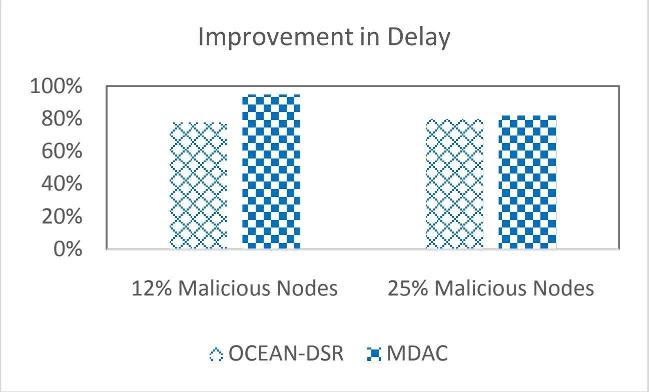

Fig. 8. Comparison between Delay's imporovement using both OCEAN-DSR and MDAC

IV. Conclusions and Future Work

In this paper, we highlighted the importance of reputation systems for ad hoc networks and proposed a new reputation system MDAC for ad hoc networks. MDAC is designed while taking into consideration the drawbacks of other reputation systems. The proposed system observes the behavior of each node and present references that describe how each node acts in the network. The proposed system's structure and modules were explained in details.

MDAC introduced a different way of reputation measurement. It has adopted a strategy of sharing specific information that is only relevant to certain network functions or services in order to minimize the traffic's overhead, and also to avoid the false reports from nodes about each other.

MDAC's performance and functionality have been tested using the OPNET Network Simulator. Results have shown that MDAC has improved the network's performance by keeping the average network throughput 80% of the original throughput despite that 25% of the nodes are malicious. As well as keeping the average delay almost the same as the network's original average delay despite that 25% of the nodes are malicious. MDAC's performance was compared to OCEAN-DSR protocol which is able to maintain the throughput of the network in case of 25% malicious nodes to an average of 68%, which means that MDAC's performance surpasses it by 12%.

For future research we are planning to investigate MDAC's performance under other types of attacks as well as different types of simultaneously cooperative attacks.

References

[1] Neeli, J., & Cauvery, N. K.. "Comparative Study of Secured Routing Protocols in Wireless Ad hoc Networks: A Survey", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.2 2015.

[2] Chakrabarti, C., Banerjee, A., Chakrabarti, S., & Chakraborty, A. "A Novel Approach for Non-cooperative Node Detection and Avoidance Using Reputation-Based Scheme in Mobile Ad hoc Network". In Computational Advancement in Communication Circuits and Systems (pp. 279-289). Springer India, 2015.

[3] Merro, M., & Sibilio, E.. "A calculus of trustworthy ad hoc networks". Formal Aspects of Computing, 25(5), 801-832, 2013.

[4] Hoffman, K., Zage, D., & Nita-Rotaru, C. "A Survey of attacks on Reputation Systems", 2007.

[5] Huang, K. L., Kanhere, S. S., & Hu, W. (). "On the need for a reputation system in mobile phone based sensing". Ad Hoc Networks, 12, 130-149, 2014

[6] Li, W., Joshi, A., & Finin, T. (). "Cast: Context-aware security and trust framework for mobile ad-hoc networks using policies. Distributed and Parallel Databases", 31(2), 353-376, 2013.

[7] W.Kun, W. Meng. "A trust approach for node cooperationin manet". In 3rd International Conference on Mobile Ad-hoc and Sensor Network, pages 481–491, 2007.

[8] Michiardi, P., & Molva, R.. "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks". In Advanced Communications and Multimedia Security (pp. 107-121). Springer US., 2002.

[9] Adams, W. J., Hadjichristofi, G. C., & Davis IV, N. J. "Calculating a node's reputation in a mobile ad hoc network". In Performance, Computing, and Communications Conference, 2005. IPCCC 2005. 24th IEEE International (pp. 303-307). IEEE., 2005.

[10] Velloso, P. B., Laufer, R. P., de O Cunha, D., Duarte, O. C. M. B., & Pujolle, G. "Trust management in mobile ad hoc networks using a scalable maturity-based model". Network and Service Management, IEEE Transactions on, 7(3), 172-185, 2010.

[11] Zhang, Y., & Lazos, L. William Jr. Kozma."AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks". IEEE transactions on mobile computing, 10, 2009.

[12] Trivedi, A. K., Kapoor, R., Arora, R., Sanyal, S., & Sanyal, S. "RISM-Reputation Based Intrusion Detection System for Mobile Ad hoc Networks". arXiv preprint arXiv:1307.7833, 2013.

[13] Ghandar, A., Shabaan, E., & Fayed, Z. T. Performance Analysis of Observation Based Cooperation Enforcement in Ad Hoc Networks. arXiv preprint arXiv:1201.3782, 2012.

[14] Resnick, P., Zeckhauser, R. "Reputation System", Communications of the ACM, 43(12): 4548, 2000.

[15] Dai, W., Moser, L. E., Melliar-Smith, P. M., Lombera, I. M., & Chuang, Y. T. ''The iTrust Local Reputation System for Mobile Ad-Hoc Networks". In Proceedings of the 2013 International Conference on Wireless Networks, 2013.

[16] Marti, S., Giuli, T. J., Lai, K., & Baker, M. "Mitigating routing misbehavior in mobile ad hoc networks". In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 255-265). ACM., 2000.

[17] Capra, L. (2004). Towards a human trust model for mobile ad-hoc networks. Proc. 2nd UK-UbiNet, Workshop, Cambridge University, Cambridge, UK.

[18] Eschenauer, L., Gligor, V. D., & Baras, J. (2004, January). On trust establishment in mobile ad-hoc networks. In Security Protocols (pp. 47-66). Springer Berlin Heidelberg.

[19] http://www.opnet.com/university_program/itguru_academic_edition/