Prevention of Multiple Coordinated Jellyfish Attacks in Mobile Ad Hoc Networks

Marianne A. Azer
Ministry of Communication and Information Technology
National Telecommunications Institute
Nile University, Cairo, Egypt

Noha Gamal El-Din Saad
Nile University
Giza, Egypt

ABSTRACT
Mobile Ad hoc Networks (MANETs) consist of self-governed nodes, they have no fixed infrastructure. They are stand alone or connected to the bigger internet as per the different applications. The dynamic nature of MANETs adds many challenges to the network management techniques. Likewise, their special characteristics such as the lack of infrastructure, self-government, mobility, and limited resources makes them vulnerable to a lot of attacks. Reputation systems can help mitigating attacks. Trust management using a reputation mechanism is considered as a vibrant security solution to enable the collaboration of MANETs. In this paper, we propose a Functional REPutation system for Ad hoc Networks, (FREPAN), which aims to improve the MANETS performance and mitigate selfishness and misbehavior attacks' effects. The overall system structure is introduced and its performance is tested under the presence of the jellyfish attacks.

General Terms
Ad hoc networks, Reputation, Security, Jellyfish.

Keywords
Ad hoc networks; Jellyfish, MANETs; misbehavior; reputation; selfishness; trust.

1. INTRODUCTION
In jellyfish attack, the malicious node introduce unwanted delays in the network [1]. This attack is one of the attacks that should be initiated from inside the network. In this type of attack, the misbehaving node first becomes a part of the network, then it delays all the packets that it receives, after delays are propagated then packets are released in the network. This enables the misbehaving node to yield high end-to-end delay, high jitter and significantly affects the performance of the network.

Reputation systems can prevent many types of observable misbehavior in ad hoc networks. Reputation systems are also beneficial in enabling nodes to make fair decisions about its prospect interactions [2].

Reputation is playing an essential role in peer-to-peer communications. It enables communicating parties to establish new relations in order to achieve mutual goals. Reputation in Ad Hoc Networks is represented by the opinion that each node has about its neighbors. Trust is the degree that each node can be confidant of its neighbors within a certain context.

Also reputation allows different nodes to build trust of each other's, to decide who is trustworthy and who is not and it also encourages and awards trustworthy behavior as well as punishing deceitful behavior. This is done by quantifying and propagating reputation value. 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 2 presents a general background of reputation systems' design issues, their goals and features, and trust metric properties. In section 3, the nodes' misbehavior modes in the literature are classified according to their nature as well as their targeted security parameter. In section 4 the reputation systems proposed in the literature were classified according to their sources of information and information types used in evaluating reputation values was presented. Section 5 describes the Functional REPutation system for Ad hoc Networks, (FREPAN) system's architecture and functionality. In Section 6 simulation setup and results are proposed. Finally in section 7, conclusions and future work are presented.

2. BACKGROUND
The use of reputation and trust-based systems for ad hoc networks, has been suggested in [3][4][5][6][7][8][9][10]. This section presents various design issues, the goals and features of reputation systems, as well as the characteristics of trust metric in sections 2.1, 2.2, and 2.3 respectively.

2.1 Reputation Systems' Design Issues
Some main issues corresponding to MANET's operation should be kept in mind when designing a security solution for such networks, which are:

- Dynamic nature, continuously changing network topology and open physical environment makes the differentiation between the normal and abnormal behavior of nodes really difficult.
- Nodes belonging to any mobile ad hoc network are free to move away at any moment, where it could be compromised, or hijacked by any malicious intruder.
- De-centralized operation of MANETs are also extended to management and decision-making as all nodes are involved and responsible for the overall decisions making process with in the network.

2.2 Reputation System Goals and Features

Reputation-based systems have been introduced as a security solution for the misbehaving dilemma [11]. A reputation system should be able to manage many kinds of misbehavior to permit nodes to make decisions about other network parties based on carefully collected and processed information [12]. Reputation systems are depending on performance observations within the network. They are aiming to five main goals [13]:

- Reputation system should be capable of providing information to distinguish between trusted parties and un-trusted parties.
- Reputation system should encourage network entities to be trustworthy.
- Reputation system should discourage untrusted network entities from participating in network activates.
- Reputation system should handle with any kind of misbehavior.
- Reputation system is required to minimize the damage caused by insider attacker.

Also reputation systems are considered as the optimal security solution to control nodes' misbehavior. For reputation-based system to operate effectively and accomplish their designated goals [14], they should have the following features:

- Reputation systems should be light-weight, easy to use and simple. Such that feedbacks and decisions regarding current interactions should be visible in the future.
- Reputation systems should be of strong temporal aspects in order to predict future interaction situations among communicating nodes.
- Reputation systems should be able of making the best use of available honest feedbacks to guide accurate trust decisions.
- Reputation systems should be designed to consume the minimum processing and power capabilities.

2.3 Trust Metric Characteristics

The main function of reputation systems is to combine performance's observations into one metric globally known as "Trust" or "Reputation" [15]. This metric is characterized by the following features:

- Trust is dynamic: In most of reputation systems it is expressed as a continuous variable.
- Trust is subjective: It is completely related to the context of communication model between two nodes. If node A is trusting node B at a certain moment; this doesn't mean that node A can't change its opinion about node B in a different context at another time.
- Trust is not necessarily transitive: If node A trusts node B and node B trusts node C, it is not necessarily that node A trusts node C unless there is a third party that confirms node B opinion about node C.
- Trust is asymmetric: If node A trusts node B, it is not necessarily that node B trusts node A in return.
- Trust is reflexive: such that a node always trusts itself

3. MISBEHAVIOR MODES

The presence of such selfish nodes can degrade the whole network performance or even worse it can make communication impossible. So a serious need for detecting such behavior in MANETs has originated. Sometimes it is so difficult to distinguish selfish behavior and malicious behavior. Following, some misbehavior actions and malicious attacks are discussed.

- **Routing Loop Attacks:** A malicious attacker could intently modify routing packets so that data packets traverse in loops and never reach their destination [16].
- **Wormhole Attacks:** a group of malicious nodes pretend to be connecting two distant nodes with a link of a minimum cost, which can disturb the network's normal operation [16] [17].
- **Black hole Attacks:** a black hole node is 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 [17].
- **Grey hole and Sinkhole Attacks:** they are special cases of black hole attacks as malicious node can be selective regarding the dropped packets [18].
- **DoS Attacks:** a malicious node can perform an excessive resources consumption in order to block or deny the normal network operation [16] [19].
- **False Information Propagation:** a malicious node provides a false negative information about good nodes, in order to isolate them or assign them negative reputations [20] [21].
- **Packet Modification or Creation:** malicious nodes can modify packets routed through it. Or it can create a whole new packet with false or misleading information [21].
- **New Comer Attacks:** a malicious node that has already assigned a negative reputation in the network can simply leave and rejoin as new node just to flush out its previous history [24].
- **Sybil Attack:** a single malicious node can use multiple identities in the same network which affects the network topology [22].
- **Black Mailing Attacks:** A malicious node can black mail another node by propagating false information that the other node is malicious, which can disrupt the network's normal operation and consume network's precious resources [22].
- **Replay Attacks:** a malicious node can resend old packets as if they are new ones they could be very destructive if these packets are old routing information, which will make all nodes are unreachable [23].
- **Selective Misbehavior Attacks:** a misbehaving node can select when and to whom it misbehaves [21].
- **ON-OFF Attack:** a malicious node can alter its behavior between good or bad to not to be caught or detected as malicious [24].
- **Conflicting Behavior Attacks:** a malicious node may behave in different ways to nodes form different groups to make a conflict about their opinion in itself. That leads to non-trusted relations between the two groups [20].
- **Self-Exclusion Attacks:** misbehaving node doesn't participate in route discovery process to save its own power, memory, and processing capabilities [25].
- **Non-Forwarding Attacks:** a misbehavior node is participating in route discovery but doesn't forward any other packets for other nodes [25].
- **Jellyfish attacks:** the malicious node introduce unwanted delays in the network [1]. This attack is one of the attacks that should be initiated from inside the network. This enables the misbehaving node to yield high end-to-end delay, high jitter and significantly affects the performance of the network.

As reputation systems can manage many types of observable misbehavior, they are beneficial in protecting ad hoc networks. Reputation systems are also beneficial in enabling nodes to make fair decisions about its prospect interacting neighbors. The following Fig 1 summarizes nodes misbehavior modes against CIA security parameters.

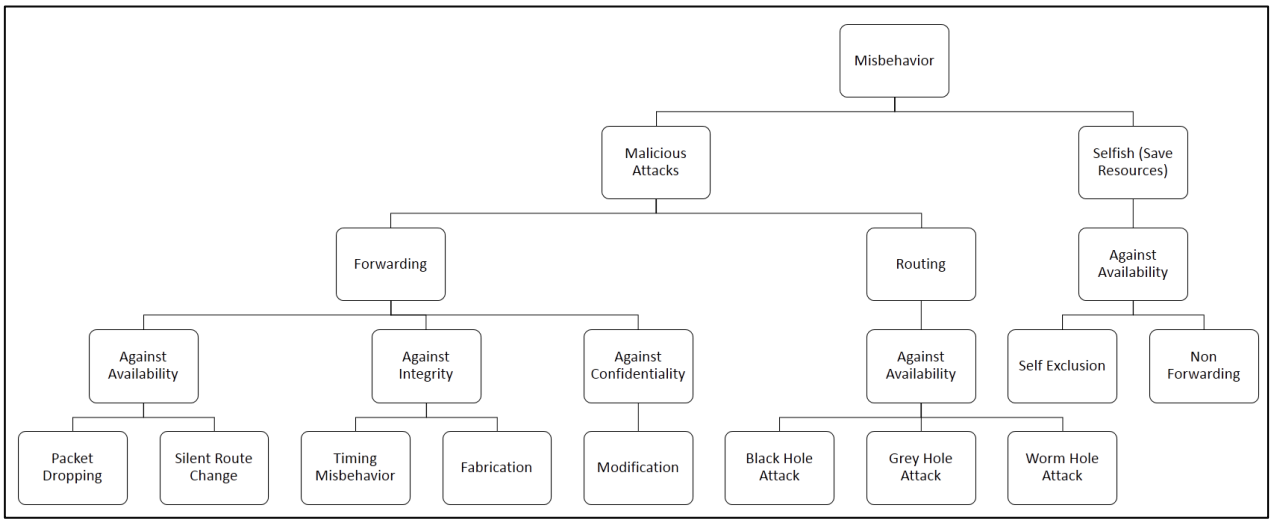

Fig 1: Nodes' misbehavior modes against CIA security parameters

4. RELATED WORK

Reputation information can be collected either considering first-hand information [26] [30] [31] [35] [36] [38] [41] or considering second-hand information [28] [29] [32] [34] [37]. The first-hand (direct) information is the opinion formed by each node on others, whereas the second-hand (indirect) information is the neighboring nodes' feedback on others. Information collected to calculate trustworthiness can be either positive [30] [35] feedback or negative feedback [33] [37] or both [31] [32] [34] [36] [38] [41] [42] [43].

This parameter should be taken into consideration in the system design phase as it is relevant to the system application. If reputation system is only depending on positive feedbacks [35] it can be immune against malicious false reputation feedback attacks, but it can also allow malicious nodes to falsely promote themselves in the system while honest parties are not able to give a real negative feedback about them.

In this section, we present the different reputation systems that have been proposed in the literature, while classifying them according to the source and type of information. Table 1 shows a classification for discussed reputation systems with respect to their source of information and information types used.

4.1 Reputation Systems Based on Negative First and Second-hand Information

Some reputation systems depend on negative first and second-hand sources of information such as CAST [33], AMD [37].

4.1.1 CAST

Context-Aware Security and Trust framework for mobile ad-hoc networks (CAST) [33] is a frame work in which many contextual information such as communication channel status, battery status, weather condition are considered to determine whether the misbehavior is resulting from malicious activity or not.

CAST uses automatic indirect information, and it depends on negative and discrete feedbacks collected by each node. It depends on short term information to define a probabilistic binary reputation measure. Both Calculation algorithm and propagation scheme are distributed and probabilistic. CAST was designed to make use of transient storage for calculation purposes.

4.1.2 AMD

Audit-based Misbehavior Detection in wireless ad hoc networks (AMD) [37] can effectively isolate selective and continuous packet droppers based on integrating reputation management, trust based route discovery and behavioral audits.

AMD uses both first-hand and second-hand available information about neighboring nodes. It only depends on continuous negative feedbacks to calculate the trust value. Trust measure is binary formulated (0: least reliable, 1: most reliable).

Calculation and Broadcasting processes are distributed and probabilistic among nodes. Transient storage for reputation measure is needed as misbehaving nodes are immediately isolated from the network.

4.2 Reputation Systems Based on Positive and Negative First and Second-Hand Observations.

In order to avoid relying only on other nodes, some reputation systems such as CORE [34], REP [36] have been designed to use their own first-hand information in addition to the second-hand information.

4.2.1 CORE

A COllaborative REputation mechanism to enforce node cooperation in mobile ad hoc networks (CORE) [34] was presented as a reputation system to prevent malicious and selfish behavior in MANETs.

CORE depends on combined information sources such as direct observations and indirect observable behavior. CORE collects both positive and negative continuous feedbacks, and it gives higher preferences for older observations in order to calculate a deterministic, continuous reputation measure.

Calculations are distributed and of strong temporal aspect as they depend on nodes historical information.

Reputation propagation scheme is distributed and deterministic. CORE depends on transient storage for calculations purposes only. Also it doesn't support redundancy.

4.2.2 REP

Recommendation Exchange Protocol (REP) [36] uses single hop neighbors as the source of information. Both positive and negative feedbacks about nodes' behavior are taken into consideration while calculating the reputation.

REP has strong temporal aspects as it gives greater weights to old neighbors' trust values compared to new neighbors. REP also introduced the concept of relationship maturity. Trust measure is binary formulated (0: least reliable, 1: most reliable) and it is deterministic.

The calculation process is distributed, deterministic and related to time. Broadcasting of trust values is partially distributed among one hop distant neighbors. REP uses transient storage for calculation phase.

REP provides an important feature of saving power and processing capabilities as it gets information from only one hop neighbors.

4.3 Reputation Systems Based on First-hand Observations Only

In order to evaluate reputation values, a number of reputation systems take into consideration only the first-hand observations of each node such as RISM [38], and first published version of CONFIDANT [40]. But after some time Buchegger – founder of CONFIDANT – discovered the importance of considering second-hand observations as well as first-hand information.

4.3.1 RISM

In Reputation Based Intrusion Detection System for Mobile ad hoc Networks (RISM) [38], monitoring module is based on the Passive Acknowledgement (PACK) feature provided with DSR routing protocol, when each node is monitoring its direct neighboring nodes to check if they forward any packets on its behalf. It then assigns a rating to each neighboring node according to its behavior.

During the information gathering process, all nodes are put in promiscuous mode to be able to collect all continuous positive and negative feedbacks at all nodes.

RISM depends in its operation on currently collected information. Reputation measure is deterministic and continuously calculated at each node (centralized). Broadcasting is also centralized. Reputation measures are permanently stored at each node.

4.3.2 CONFIDANT

Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks (CONFIDANT) [39] [40] was introduced to find and isolate selfish and (or) misbehaving nodes.

CONFIDANT was developed to be used with DSR. It uses both first-hand and second-hand positive continuous information to calculate a deterministic, continuous, and binary reputation measure.

Calculation and broadcasting processes are both distributed and deterministic. Storage is transient for calculation phase only.

Table 1. Reputation systems classification

System Name	First-hand	Second-hand	Positive observations	Negative observations
CAST	◙	◙		◙
AMD	◙	◙		◙
CORE	◙	◙	◙	◙
REP	◙	◙	◙	◙
RISM	◙		◙	◙
CONFI-DANT	◙	◙	◙	

5. THE PROPOSED SYSTEM: FREPAN

In this section, we propose FREPAN, a new reputation system for misbehavior detection and control in Ad hoc Networks. FREPAN is designed to manage many types of misbehavior and selfish actions by malicious nodes in ad hoc networks. FREPAN aims to mitigate most of other reputation systems problems and drawbacks as follows:

FREPAN considers both positive and negative behavioral actions of network related functions, in order to avoid false accusation for benign nodes. False accusation is one of CONFIDANT [40] drawbacks which is not the case for FREPAN, as every available information is considered when calculating node's reputation.

FREPAN gives slight weight to past behavior, unlike CORE [34] in which the nodes must keep good behavior all the times.

FREPAN is a network friendly system as it only depends on promiscuous information collected as indirect behavior. It also depends on a hybrid dissemination scheme to minimize network's traffic overhead.

FREPAN takes into consideration that MANETs rely on cooperation between nodes and there is no real benefit of totally excluding of misbehaving nodes unless they are being malicious to the network. The penalizing methodology should be consistent with the nodes' misbehavior.

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 4.1, 4.2, 4.3 and 4.4 respectively. Fig 2 depicts the proposed FREPAN's state diagram.

5.1 FREPAN 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 [44] in 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' feedback. FREPAN 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 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 are then forwarded and stored at the observer's module which in turn handles all available information to the modeler Module.

5.2 FREPAN 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 FREPAN 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 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.

5.3 FREPAN Dissemination Module

This module is responsible of propagating the reputation values of nodes. After FREPAN 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.

5.4 FREPAN 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).In FREPAN, 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. 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, then, other nodes check its reputation value first to decide if the node is eligible for the service or not.

6. SIMULATION SETUP

This section presents the methodology used for assessing the performance of FREPAN. 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.

6.1 Simulation Parameters

The following tables show the parameters used for the simulation, and testing scenarios applied respectively.

Table 2. Simulation Parameters

Parameter	Value
MAC Protocol	802.11b
Max Throughput	11 Mbps
Mobility Model	Default Random Waypoint
Ad-Hoc Routing Protocol	AODV
Nodes in Simulation	100
Sender Nodes	2 (Node 1 - 2)
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 will be discarded from the route

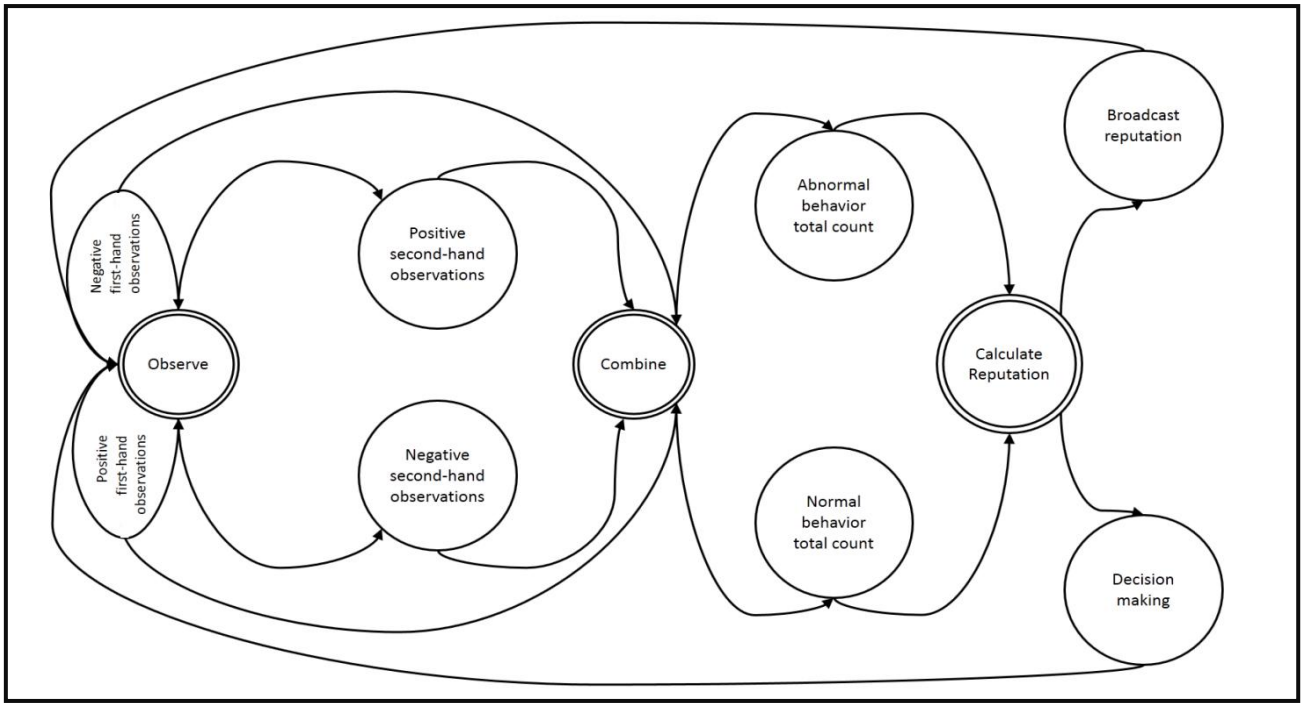

Fig 2: FREPAN's state diagram

Table 3. FREPAN Simulation Scenarios

Scenario No.	No. of Malicious Nodes	Comments
1	0	This scenario is designed to collect observations about malicious node (s) in case of jellyfish delaying attack
2	5 (node 16, node 27, node 36, node 41, node 46)	

6.2 Simulation Results

In this section some of the simulation results and snapshots are presented. For each scenario mentioned in table 3, some indicative statistics are collected and discussed such as: average delay observed during the presence of five malicious nodes striking jellyfish attack to the network by deliberately delaying packets for certain period of time then release them again into the network which can negatively affect both networks' average delay and throughput, which will disturb the whole network's performance. Those statistics are collected before and after using FREPAN, in order to proof its efficiency and influence on improving network performance even with the presence of misbehaving or malicious nodes. Also average throughput before and after using FREPAN, and the reputation value for each node are presented. . Three scenarios are simulated, scenario 1 presents the normal network performance in the case of no malicious nodes present, scenario 2 presents the case of active collaborative jellyfish attack consisting of 5 malicious nodes before using FREPAN, and scenario3 present the resulting network's performance after mitigating the attack using FREPAN. The average network throughput before and after using FREPAN is shown in Fig 3. The average network delay before and after using FREPAN is depicted in Fig 4. It can be noticed that, the average network throughput has increased by 20%. Also the average network delay has decreased by 20% for the same scenarios. Therefore, FREPAN helps improving the average global throughput and delay as clarified in Tables 4, 5 and Fig 6 showing the percentage of improvement after using FREPAN with respect to the average network throughput and average network delay respectively.

FREPAN is also capable of discovering the misbehaving nodes accurately as shown in Fig 5, presenting the resulting reputation values for each node. It can be seen from the resulting reputation values that, nodes 16, 27, 36, 41, and 46 having reputation values less than the Reputation Threshold are marked as malicious, which is consistent with behavioral observations collected by OPNET.

Table 4. Average network throughput improvement

Network Parameter	Scenario 1 (No Malicious Nodes)	Scenario 2 (One Malicious Node)
Throughput Before using FREPAN	636302	477189
Throughput After using FREPAN	636302	577222
Improvement Percentage %	Same performance	20%

Table 5. Average network delay improvement

Network Parameter	Scenario 1 (No Malicious Nodes)	Scenario 2 (One Malicious Node)
Delay Before using FREPAN	0.006111	0.005367363
Delay After using FREPAN	0.006111	0.004354707
Improvement Percentage %	Same performance	20%

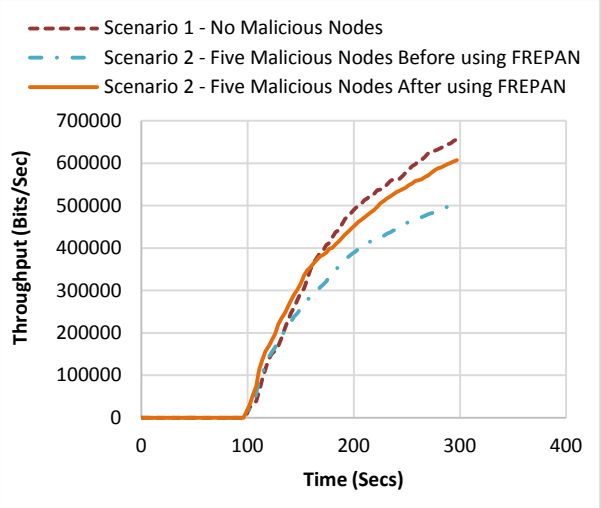

Fig 3: Average network throughput before and after using FREPAN

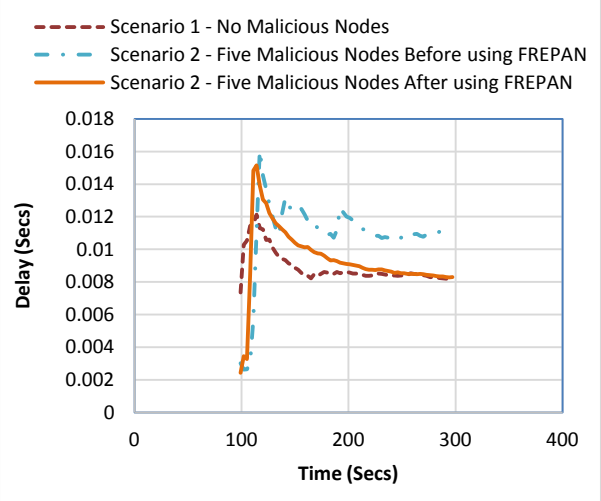

Fig 4: Average network delay before and after using FREPAN

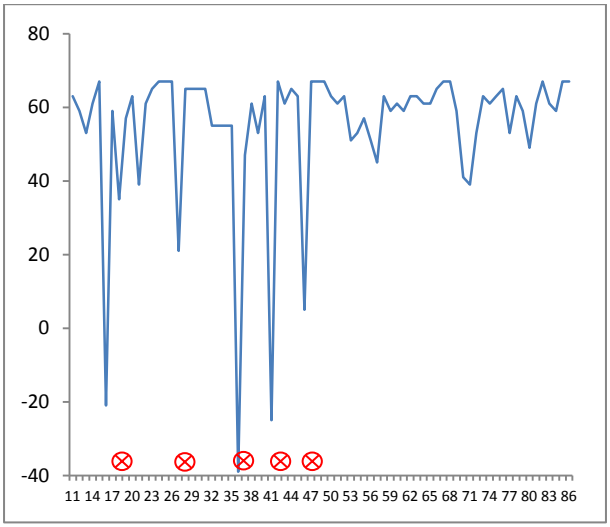

Fig 5: Reputation values for all nodes and malicious nodes discovered by FREPAN

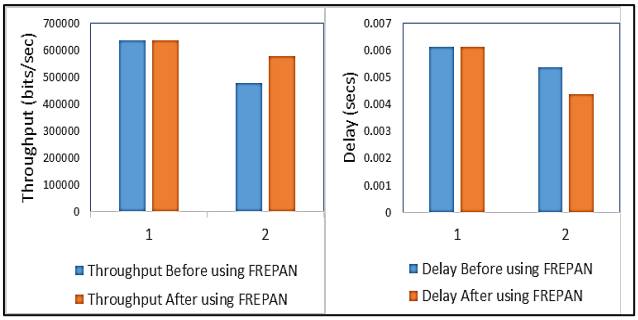

Fig 6: Improvement of network throughput and delay after using FREPAN

7. CONCLUSIONS and FUTURE WORK

In this paper, the importance of reputation systems for ad hoc networks was highlighted. We studied reputation systems from different aspects. First the reputation system's designing issues have been presented. Next, reputation system goals and features were explored. We discussed the main properties of any reputation systems' output. Then nodes' misbehavior modes are presented and classified according nature as well as their targeted security parameter. The reputation systems proposed in the literature were classified according to their sources of information and information types used in evaluating reputation values was presented. We proposed Functional REPutation system for Ad hoc Networks, (FREPAN) system's architecture and functionality. The proposed system FREPAN consists of four modules, observer, modeler, hybrid dissemination, and decision making. FREPAN observes the behavior of each node and builds histograms that describe how each node acts in the network.

FREPAN 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.

FREPAN's performance and functionality have been tested using the OPNET network simulator. The performance of FREPAN has been tested under multiple coordinated jellyfish attacks. Results have shown that FREPAN has improved the network's performance by increasing the average network throughput and decreasing the average delay overcoming the effect of jellyfish attacks. In the future, we plan to test the performance of FREPAN against other types of nodes' misbehavior or attacks.

8. REFERENCES

[1] H.L.Nguyen,U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks," International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr,2006.Patel.

[2] V. H., Zaveri, M. A., & Rath, H. K. (2015). Trust Based Routing in Mobile Ad-Hoc Networks. Lecture Notes on Software Engineering, 3(4).

[3] Neeli, J., & Cauvery, N. K. (2015). Comparative Study of Secured Routing Protocols in Wireless Ad hoc Networks: A Survey.

[4] 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.

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

[6] 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

[7] P. Mirchiardi and R. Molva, "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks" In Proceedings of the European Wireless Conference, 2002.

[8] S. Buchegger and J-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes- Fairness In Dynamic Ad-hoc NeTworks), In Proceedings of MobiHoc 2002, Lausanne, CH, June 2002.

[9] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom 2000) 2000.

[10] S. Buchegger and J.-Y. Le Boudec, "The Effect of Rumor Spreading in Reputation Systems in Mobile Ad Hoc Networks", In Proceedings of Wiopt' 03, Sofia-Antipolis, March 2003.

[11] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, "Reputation System", Communications of the ACM, 43(12): 4548, 2000.

[12] Wang, K., Wu, M., & Shen, S. (2008, April). A trust evaluation method for node cooperation in mobile ad hoc networks. In Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on (pp. 1000-1005). IEEE.

[13] Visalakshi, P., & Kasmir Raja, S. V. (2014). Distributed node level security monitoring system for mobile ad hoc networks. International Journal of Mobile Network Design and Innovation, 5(3), 157-165.

[14] Soltanali, S., Pirahesh, S., Niksefat, S., & Sabaei, M. (2007, June). An efficient scheme to motivate cooperation in mobile ad hoc networks. In Networking and Services, 2007. ICNS. Third International Conference on (pp. 98-98). IEEE.

[15] Maamar, M., Liu, J., & Liu, W. (2014, May). A new lightweight link quality based reputation model for Space-Air-Ground Integrated Wireless Sensor Network (SAGIWSN). In Electronics, Computer and Applications, 2014 IEEE Workshop on (pp. 230-236). IEEE.

[16] Boukerche, A., & Ren, Y. (2008, October). A security management scheme using a novel computational reputation model for wireless and mobile ad hoc networks. In Proceedings of the 5th ACM symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks (pp. 88-95). ACM.

[17] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2), 293-315.

[18] Li, J., Li, R., & Kato, J. (2008). Future trust management framework for mobile ad hoc networks. Communications Magazine, IEEE, 46(4), 108-114.

[19] Liu, Z., Joy, A. W., & Thompson, R. A. (2004, May). A dynamic trust model for mobile ad hoc networks. In Distributed Computing Systems, 2004. FTDCS 2004. Proceedings. 10th IEEE International Workshop on Future Trends of (pp. 80-85). IEEE.

[20] Li, H., & Singhal, M. (2007). Trust management in distributed systems. Computer, (2), 45-53.

[21] Sun, Y. L., Yu, W., Han, Z., & Liu, K. R. (2006). Information theoretic framework of trust modeling and evaluation for ad hoc networks. Selected Areas in Communications, IEEE Journal on, 24(2), 305-317.

[22] Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks: challenges and solutions. Wireless Communications, IEEE, 11(1), 38-47.

[23] Yu, Y., Peng, Y., Yu, Y., & Rao, T. (2014). A new dynamic hierarchical reputation evaluation scheme for hybrid wireless mesh networks. Computers & Electrical Engineering.

[24] Li, Z., & Chigan, C. (2014). On Joint Privacy and Reputation Assurance for Vehicular Ad Hoc Networks. Mobile Computing, IEEE Transactions on, 13(10), 2334-2344.

[25] Yu, Y., Guo, L., Wang, X., & Liu, C. (2010). Routing security scheme based on reputation evaluation in hierarchical ad hoc networks. Computer Networks, 54(9), 1460-1469.

[26] Ding, Q., Li, X., Jiang, M., & Zhou, X. (2010, October). Reputation-based trust model in vehicular ad hoc networks. In Wireless Communications and Signal Processing (WCSP), 2010 International Conference on (pp. 1-6). IEEE.

[27] Li, J., Li, R., & Kato, J. (2008). Future trust management framework for mobile ad hoc networks. Communications Magazine, IEEE, 46(4), 108-114.

[28] Ding, Q., Li, X., Jiang, M., & Zhou, X. (2010, October). Reputation-based trust model in vehicular ad hoc networks. In Wireless Communications and Signal Processing (WCSP), 2010 International Conference on (pp. 1-6). IEEE.

[29] Li, J., Li, R., & Kato, J. (2008). Future trust management framework for mobile ad hoc networks. Communications Magazine, IEEE, 46(4), 108-114.

[30] Ren, Y., & Boukerche, A. (2008, May). Modeling and managing the trust for wireless and mobile ad hoc networks. In Communications, 2008. ICC'08. IEEE International Conference on (pp. 2129-2133). IEEE.

[31] Shen, H., & Li, Z. (2008, June). Arm: an account-based hierarchical reputation management system for wireless ad hoc networks. In Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on (pp. 370-375).

[32] Kraounakis, S., Demetropoulos, I. N., Michalas, A., Obaidat, M. S., Sarigiannidis, P. G., & Louta, M. D. A Robust Reputation-Based Computational Model for Trust Establishment in Pervasive Systems.

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

[34] 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.

[35] 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.

[36] 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.

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

[38] 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.

[39] Buchegger, S., & Le Boudec, J. Y. "Performance analysis of the CONFIDANT protocol". In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing (pp. 226-236). ACM, 2002.

[40] Buchegger, S., & Le Boudec, J. Y. (2003). A robust reputation system for mobile ad-hoc.

[41] He, Q., Wu, D., & Khosla, P."SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks". In Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE (Vol. 2, pp. 825-830). IEEE, 2004.

[42] 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.

[43] 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.