LEBANESE AMERICAN UNIVERSITY

Reputation-based Cooperative Detection Model of Selfish Nodes in Cluster-based QoS-OLSR Protocol

By

Nadia Moati

A thesis
Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Computer Science

School of Arts and Sciences
May 2014

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

Lebanese American University

School of Arts and Sciences ; Beirut Campus

THESIS APPROVAL FORM

Student Name: Nadia Moati I.D. #: 200601550

Thesis Title : Reputation-Based Cooperative Detection Model of Selfish Nodes in Cluster-Based QoS-OLSR Protocol

Program: Masters in Computer Science

Department: Computer Science and Mathematics

School: Arts and Sciences

The undersigned certify that they have examined the final electronic copy of this thesis and approved it in Partial Fulfillment of the requirements for the degree of:

Masters of Science in the major of Computer Science

Thesis Advisor's Name Dr. Azzam Mourad Signature A.M. Date: 19/05/14

Co-Advisor's Name Dr. Hadi Otrok Signature Date: 19/05/14

Committee Member's Name Dr. Sanaa Sharafeddine Signature Date: 19/05/14

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

THESIS COPYRIGHT RELEASE FORM

LEBANESE AMERICAN UNIVERSITY NON-EXCLUSIVE DISTRIBUTION LICENSE

Name: Nadia Moati

Signature: Nadia

Date: Monday, May 19, 2014

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

PLAGIARISM POLICY COMPLIANCE STATEMENT

I certify that:

- I have read and understood LAU's Plagiarism Policy.
- I understand that failure to comply with this Policy can lead to academic and disciplinary actions against me.
- This work is substantially my own, and to the extent that any part of this work is not my own I have indicated that by acknowledging its sources.

Name: Nadia Moati

Signature: Nadia

Date: Monday, May 19, 2014

ACKNOWLEDGMENT

I would like to convey my gratefulness to each person who assisted me in completing my thesis. My deep appreciation goes to my supervisors Dr. Azzam Mourad and Dr. Hadi Otrok for their big help and patience. Also, I would like to thank Dr. Sanaa Sharafeddine, the committee member, for her valuable recommendations.

Reputation-based Cooperative Detection Model of Selfish Nodes in Cluster-Based QoS-OLSR Protocol

Nadia Moati

ABSTRACT

The QOLSR is a multimedia protocol that was designed on top of the optimized link state routing protocol for mobile ad hoc network. It considers the quality of service (QoS) of nodes in the network when selecting the multi-point relay (MPRs) nodes. This proto-col suffer major drawbacks regarding network lifetime, where nodes with high bandwidth but limited energy can be selected to serve as MPRs. This would drain the nodes resid-ual energy and shorten the network lifetime, and increase selfish nodes that degrade the network lifetime. The limited energy and resources, and the absence of any moti-vation mechanism cause mobile nodes to act selfishly when selecting the MPRs. In this thesis, we consider the tradeoff between prolonging the ad hoc network lifetime and QoS assurance based on QOLSR routing protocol. This can be attained by (1) decreasing the Multi-Point Relay (MPR) nodes without sacrificing the QoS and (2) taking into consideration the residual energy level, connectivity index, and bandwidth of these relay nodes. The mentioned goals can be attained by implementing the clustering model to QOLSR. Therefore, we suggest a new clustering algorithm and a MPR node selection based on different combinations of metrics, such as connectivity, residual energy, and bandwidth. Moreover, we consider the selfishness during the election and selection process by proposing the use of reputation system that will motivate nodes to participate during the selection of MPRs, where the reputation is calculated based on VCG mechanism design. After solving the selfishness during network formation, we have discovered that nodes can misbehave after being selected/elected. Such a passive malicious behavior could lead to a denial of service attack due to the drop of packets. As a solution, we propose a hierarchal cooperative watchdog detection model for the cluster-based QOLSR, where nodes cooperate in a hierarchical manner to detect selfish n odes. Furthermore, to motivate watchdogs to monitor and cooperate with each other, incentives are given and calculated using cooperative game theory, where Shapley value is used to compute the contribution of each watchdog on the final d ecision. Simulation results show that the novel cluster-based QoS-OLSR model can well extend the network lifetime, ensure QoS and decrease delay. Adding reputation as one of the QoS metrics, motivates nodes to act normally without sacrificing the quality of service of the network. In addition, the hierarchical cooperative detection model shows a more reliable and efficient detection of selfish nodes.

Keywords: Quality of Service (QoS), Head Election, MPR Selection, Ad Hoc Networks, Reputation, Watchdog.

Table of contents

Chapter **Page**

I - Introduction . . . 1
1.1 Motivations & Problem Statement . . . 1
1.2 Objectives . . . 4
1.3 Approach Overview and Contributions . . . 4
1.4 Thesis Organization . . . 6

II - Background & Related Work . . . 8
2.1 Introduction . . . 8
2.2 MANET Networks . . . 8
2.3 MANET Clustering Models . . . 9
2.3.1 QOLSR . . . 9
2.3.2 Connectivity-based and Energy-based Clustering Models . . . 10
2.4 Network Security in MANET . . . 11
2.4.1 Credit-Based Mechanism . . . 12
2.4.2 Reputation-Based Mechanism . . . 13
2.5 Cooperative Game Theory and shapley value . . . 16
2.6 Conclusion . . . 18

III - Reputation-Based Model in Cluster-based QoS-OLSR Protocol . . . 19
3.1 Introduction . . . 19
3.2 The Quality of Service Metric Models . . . 20
3.2.1 Reputation-Cluster-based QoS-OLSR Approach . . . 21
3.2.2 Illustrative Example . . . 27
3.3 Simulation Results . . . 28
3.3.1 Percentage of MPR nodes in the Network . . . 29
3.3.2 Network Lifetime . . . 30
3.3.3 Average Trust Difference . . . 33
3.4 Conclusion . . . 34

IV - Cooperative Detection Model of Selfish Nodes in Cluster-based QoS-OLSR Protocol . . . 36
4.1 Introduction . . . 36
4.2 Detection Model: Hierarchical Cooperative Watchdog . . . 37

4.3 Incentive Model: Contribution of Cooperative Watchdogs based on Shapley Value 40
4.4 Simulation Results 44
4.4.1 Effect of Selfish Nodes on Packet Delivery 45
4.4.2 Selfish Nodes Detection Probability 45
4.5 Conclusion 47

V - Conclusion 48

Bibliography 51

List of Figures

1 Ad hoc Network With Selfish Node 3

2 Ad hoc Network example 24

3 Reputation Mechanism example 27

4 Percentage of MPR Nodes: (a) B-OLSR (b) Proportional B-OLSR (c) BE-OLSR (d) Proportional BE-OLSR 31

5 Percentage of alive nodes over time: (a) B-OLSR (b) Proportional B-OLSR (c) BE-OLSR (d) Proportional BE-OLSR 32

6 Average Path Length: (a) B-OLSR (b) Proportional B-OLSR (c) BE-OLSR (d) Proportional BE-OLSR 33

7 Hierarchical Cooperative Watchdog Mechanism example 39

8 Packet Delivery Percentage 45

9 Detection Probability of Selfish Nodes with different percentage of CH voters 46

10 False Detection Percentage of Selfish Nodes-Cooperative vs. Noncooperative Detection Model 46

List of Tables

1 Marginal Contribution of Player 1 18

2 The Quality of Service Metric Using the Proportional BE-OLSR Model . . 25

3 Simulation Parameters 30

4 Trust Average Difference 34

5 Nodes Reputation 42

6 Contribution Value 42

7 NODES Validation Value 43

8 Nodes Contribution Value in a Subset of Three Nodes 44

9 New Reputation Value After Reward 44

Chapter 1

Introduction

1.1 Motivations & Problem Statement

Mobile Ad hoc Networks have been widely used in many operations where non-infrastructure networks are needed such as in the military. Moreover, MANETs are essential in cases where the usual wired networks are congested or destroyed. Also, MANETs have a commercial use where they deploy telecommunication and internet services in remote areas. Unlike the wired networks, mobile adhoc networks imposes a variety of challenges in security design because of its dynamic network topology, resources constraints, shared wireless medium, and open network architecture. The *Optimized Link State Routing* protocol [44] is a proactive routing protocol aimed to be implemented over mobile ad hoc networks. It depends on a group of special nodes to distribute the network topology information and to pass traffic to their destination. The special nodes are called *MultiPoint Relay* (MPR) nodes.

Based on OLSR protocol, Quality of Service (QoS) OLSR protocol, known as QOLSR

[16], was proposed in literature to consider nodes available bandwidth during the selection of MPR nodes and routing paths. It was designed to handle multimedia applications over ad hoc networks. The bandwidth and delay metrics that are needed to ensure QoS are used during the MPR selection. Therefore, a clustering model is designed to solve the main limitation of QOLSR protocol. It can eventually threaten the ultimate goal of prolonging network life time. It selects a large number of MPR nodes because each node independently selects its group of MPR nodes. Such a problem can affect nodes available bandwidth and increase the risk of channel collision, especially in compact networks [8].

Moreover, the cluster-based QOLSR protocol has two limitations. First, QOLSR lacks a motivation mechanism that encourages mobile nodes to be elected as cluster head (CH) nodes or selected as MPR nodes to interconnect the network clusters. This will lead to selfishness behavior during the selection process by refusing to be elected as head or MPR nodes. Also, a security solution should be built to ensure protection without sacrificing in network performance.

The other limitation arises after network formation where nodes behave normally during the election/selection process yet deviate and act selfishly afterward. Nodes may refuse to be active in packet forwarding causing denials of service. A selfish node tends to avoid participating in the routing and the packet forwarding processes to save its own energy and be able to process its own packets without latency. Such a passive malicious behavior will impede the network services and would eventually cause a denial of service.

In the context of the QOLSR protocol and its derivatives, a node may act selfishly and refuse to reveal its true QoS parameters. Such a node may exclude itself from the election process of the CH nodes or selection process of the MPR nodes. However, a selfish node may also decide to cooperate during the MPR selection/election, but refuse to cooperate later on in the packet forwarding process. Thus, the behavior of a selfish node, in QOLSR, can be described as follows [40]:

1. Refuse to participate in the MPR election/selection process and thus reveal fake information.
2. Behave normally during the election/selection process and deviate after by dropping the forwarded packets.

Network performance may be harshly damaged due to selfish nodes and leads to a partitioned network.

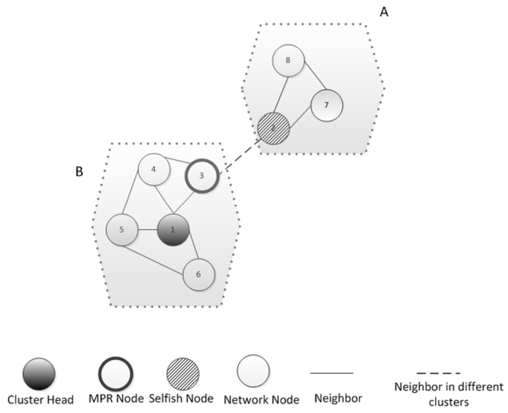

Figure 1: Ad hoc Network With Selfish Node

Consider the example presented in Fig. 1. Assume that N_2, which has accepted to be a cluster head, is a selfish node and N_8 in Cluster A needs to send a data packet to N_3 in

Cluster B. If N_2 in Cluster A acts selfishly and does not forward any data message, the network would quickly become unreliable and disconnected.

1.2 Objectives

The main goal of the thesis is to build a Secure QoS-based clustering model for Mobile Ad-hoc QOLSR networks to prolong network lifetime, to prevent and to detect selfish nodes, while maintaining the Quality of Service. A detection model is built based on the concept of watchdogs to reduce the false alarms of selfish nodes. In summary, the objectives of our thesis are the following:

- Prolong MANET lifetime, ensure QoS and decrease delay.
- Motivate nodes to behave normally without degrading the quality of service of the network.
- Build a more trustworthy and efficient hierarchical cooperative detection model to detect selfish nodes.

1.3 Approach Overview and Contributions

This thesis, we first present a clustered QoS-based model for Mobile Ad-hoc QOLSR network as a solution for prolonging the network lifetime by reducing the percentage of MPRs. Therefore, clusters are formed and then MPRs are selected according to their private information such as residual energy and connectivity index to connect these clusters. Note that all the proposed models assume the presence of clustering models that can cluster the network, then the MPRs are selected. While in our model, the heads are selected cooperatively and then the heads will select the MPRs that can connect the heads with each other (1-hop, 2-hop and 3-hop away). Based on the clustering concept, we propose a solution that has four different clustering models based on three metrics: bandwidth, connectivity index and residual energy. In summary, our first contribution, is a novel cluster-based QoS-OLSR approach that is able to (1)Prolong the network lifetime by reducing the percentage of MPR nodes which in time diminish the traffic over-head and channel collisions(2)collectively select the group of MPRs based on nodes QoS metric.

Then, we addressed the selfishness behavior during the selection process by refusing to be elected as head or MPR nodes. Hence, when a node is elected as a CH node or selected as an MPR node, it should receive a payment from the other electing or selecting nodes. This reward should be in the form of reputation. Such a reputation system could be based on the incentive-compatible VCG-mechanism. Since network services would be delivered in priority to trustable nodes, network nodes should be motivated to play the role of CH or MPR nodes and see their reputation increasing accordingly. Thus, adding reputation to the already existing selection process metrics, connectivity, residual energy and bandwidth, will help in selecting more trusted nodes. The contributions of the thesis can be summarized as follows:

1. Build a novel cluster-based QoS-OLSR approach.
2. Motivate nodes to behave normally during the election/selection process by giving incentives in the form of reputation based on the VCG mechanism.

3. Select the most trusted MPR nodes without sacrificing in network lifetime and increasing delay by considering nodes reputation.

4. Detect cooperatively selfish nodes after the election/selection process based on the Hierarchical Cooperative Watchdog model, which decreases false positive and negative alarms and increases the detection.

5. Motivate nodes to act as a watchdog nodes by rewarding them according to their contribution value in the final detection.

6. Analyze the impact of having less number of watchdogs on the final decision.

1.4 Thesis Organization

The rest of this thesis is structured as follows; Chapter 2 provides an overview about MANETs, Network security, Security in MANETs, cooperative game theory, and shapely value. Then, we present the related research in the domain of clustering, routing, and security in mobile ad hoc networks.

Chapter 3 presents a new clustering model that gives incentives for nodes to be elected as MPR nodes. We give an illustrative example to present our model. Finally, we simulated our results to show the efficiency of our model.

Chapter 4 proposes a hierarchical watchdog detection model to detect selfish behavior after selection of MPR nodes. Thereafter, we proved the efficiency of our models using a formal mathematical analysis and simulations.

Chapter 5 concludes the thesis by summarizing its contribution, announcing the future work, and listing the publications obtained from this thesis.

Chapter 2

Background & Related Work

2.1 Introduction

We present in this chapter an overview about the concepts that form our models. Our clustering model is built over a MANET. Therefore, we present a brief description about MANETs. Then, we provide an overview about network security and what makes security in MANETs a challenge. A summary of the security models that are already implemented in MANETs and their weakness are presented. A definition of game theory and shapley value was presented since they were used to regulate the cooperation in MANET and to have a trustworthy selfish detection model.

2.2 MANET Networks

A MANET is a type of network where mobile nodes can change location and configure themselves for intercommunication with other mobile nodes to form a network. Therefore, mobile nodes have double roles in the network; routers or hosts. MANETs have been used in many operations where non-infrastructure networks are needed such as military. Moreover, they are essential in cases where the usual wired networks are congested or destroyed. Also, MANETs have a commercial use where they deploy telecommunication and internet services in remote areas. To connect them in different geographical areas a wired infrastructure-based network can be used.

The difference between traditional network and MANET is that decision-making, routing, key-distribution, and forwarding packets are decentralized and depend on a cooperative decision between all mobile nodes.

2.3 MANET Clustering Models

2.3.1 QOLSR

OLSR [6] is a classical link state protocol that has been designed based on the requirements of ad hoc networks. The main idea of this protocol is a set of selected nodes, Multi-Point Relay (MPR) nodes, that uses their Topology Control messages to distribute the network topology information and to pass traffic to their destination. The objective of this method is to reduce remarkably the overhead of the control messages. Therefore, the protocol is mainly appropriate for large and dense networks. Unfortunately, OLSR cannot guarantee or ensure QoS since it was not designed for multimedia purposes. To cope with this limitation, QOLSR [2] routing protocol was developed based on OLSR where QoS has been considered. This raises the need for new metrics such as bandwidth and delay. Thus, the aim is to find a source-destination routes, but the optimal ones that satisfies the end-to-end QoS requirements. The selection of MPRs are based on the QoS measurements that allow QOLSR to find optimal paths. Multiple-metric routing criteria were considered in order to improve the QoS of the route. The QOLSR has main limitation. MPRs are selected based on nodes bandwidth without considering nodes energy level and connectivity which can shorten the network lifetime.

2.3.2 Connectivity-based and Energy-based Clustering Models

Research provides many approaches for clustering ad hoc networks where they are all based on dividing the network into clusters then choosing the head nodes. The first approach is the HOLSR protocol [28]. This protocol is based on a two hierarchy of nodes. The first level is an interconnected mesh of head nodes that act as mobile access points because they have higher communication capabilities. The other nodes form the clusters by connecting to cluster head nodes. All traffic is routed through a cluster head node. The second approach is the OLSR Tree protocol [12]. The network is divided into trees where a leaf chooses its parent with the maximum connectivity. A cluster is a tree with the cluster head being its root. To interconnect the roots, a set of MPR nodes are determined based on an extended version of OLSR. The last approach addresses huge ad hoc networks [27]. This approach is based on broadcasting TC messages by cluster heads; thus any source node can define its route towards the destination. This approach presents a simpler solution than the OLSR. Moreover, many approaches were presented to increase network lifetime by considering nodes residual energy as a metric for the routing protocol. Also, connectivity [39] can be added as a metric when choosing MPR nodes. To choose routes with highest energy, some approaches (e.g., [3] and [45]) assign high costs to links with minimum energy, and then chooses routes with minimum cost using Dijkstras algorithm. Other criterion can be defined such as choosing the link that minimize the maximum one node spent energy is preferred [13]. All presented clustering approaches choose the clusters and then cluster head nodes are selected.

2.4 Network Security in MANET

Security has become an essential issue for ensuring secure and protected communication between mobile nodes. In general, network security involves policies applied by a network administrator to prevent and monitor misuse, modification, unauthorized access, or denial of network node or resources. Network security ensures secure communication among business, agencies and individuals.

Unlike the wired networks, MANETs impose a variety of challenges in security design because of its dynamic network topology, resources constraints, shared wireless medium, and open network architecture. Therefore, a security solution should be built to ensure protection without sacrificing in network performance.

The open wireless architecture in MANET makes the wireless channel accessible by both legitimate users and malicious attackers. Therefore, there is no clear line of defense when designing security in MANETs. Moreover, limited resources in MANET is another challenge when designing security. Mobile nodes have limited bandwidth and limited energy. Also, the dynamic nature of MANETs where nodes frequently enter and leave the network imposes higher risk of vulnerability. MANETs are subject to passive and active attacks.

One type of passive malicious behavior in MANETs is selfish nodes. Selfish nodes in MANETs will be addressed in this thesis. The literature provides several protection mechanisms against selfish nodes. These mechanisms can be divided into two categories: incentive-based strategies fostering cooperation among selfish nodes and detection-based strategies. Incentive strategies motivate nodes of the network to participate in the path discovery and packet forwarding. If these incentives are not enough, detection strategies can be used. If a node is not rational and acts selfishly, mechanism should be used to detect this behavior, and eventually punish the node to avoid its negative impact on the network. To implement the above strategies, two different types of mechanisms have been proposed. In credit-based mechanisms, a node should retribute beforehand any other node providing some network services. Such a mechanism should incite a node which would eventually need some services from others to participate in the collective effort. Reputation-based mechanisms are similar to the credit-based mechanisms. Instead of earning some credits, cooperative nodes would gain some reputation. Since network services would be offered in priority to trustworthy nodes, rational nodes should participate in the collective effort.

2.4.1 Credit-Based Mechanism

Credit-based mechanisms reward nodes that forward packets and offer general network services to others. Such cooperative nodes earn credits. Since a node will not be able to send its own packets if it does not own credits, these mechanisms should incite rational nodes to participate to the collaborative efforts. Sprite is a credit-based mechanism [42] that encourages selfish nodes to participate in the general network services. It is an incentive-based strategy in which a node sends to a central Credit Clearance Service (CCS) the receipts of the messages that it has received/forwarded. These receipts are only sent when a node can communicate efficiently with the clearance service. Any node involved in the transmission of a message would be able to show its participation with these receipts. The CCS acts as a virtual bank and determines how much any given node would earn or would pay for any given forwarded message. In any credit-based mechanism, it is important to secure credit values. Misbehaving nodes may try to forge receipts to earn credits or may try to freely send their own messages without reporting them. Sprite proposed using game-theoretic approaches to design a secure solution for initiating selfish nodes to participate in the collaborative effort.

2.4.2 Reputation-Based Mechanism

In ad hoc networks, reputation is used to indicate the behavior of the nodes in the network. By direct or indirect observations of a nodes behavior, a node can form an opinion about any other node in the network. This corresponds to the reputation of the node for the observing node. To build its opinion, a node can observe the behavior of the nodes in a given path, the number of retransmissions or acknowledgement messages, and whether a neighbor node retransmits all its packets as expected. In this context, Watchdog and Pathrater [40] propose to detect non cooperating (selfish) nodes. A watchdog is implemented on each node in the network to observe messages sent by neighbor nodes. By comparing the overheard messages and the messages that the node forwards, the watchdog can identify selfish nodes. The weakness of the watchdog is that it can not detect selfish nodes in the following cases: ambiguous collisions, receiver collisions, limited transmission power, false misbehavior and partial dropping.

CORE is a collaborative reputation mechanism [21] that also has a watchdog component. This reputation system differentiates between three different types of reputation: subjective reputation (observations), functional reputation (task specific behavior), and indirect reputation (positive reports by other nodes). These reputations are weighted to give a combined reputation that is used to assess any given node. Unfortunately, CORE allows second-hand information permitting cooperative misbehaving nodes to increase each others reputation. Thus, CORE is vulnerable to fake positive ratings.

CONFIDANT protocol [38] also uses reputation to detect selfish nodes. CONFIDANT has four components: monitor, reputation manager, path rater and trust manager. These components do the critical functions of neighborhood watching, node rating, path rating and sending/receiving alarm messages respectively. When a suspicious event is detected while a node is observing its 1-hop neighbors, the monitoring node sends details about this event to the centralized reputation manager. This component updates the rating of the misbehaving node after identifying the significance of the event. When the bad rating of a node becomes greater than a tolerable threshold, a message is sent to the path manager which controls the route cache. At last, the trust manager sends a warning alarm message to other nodes. The main weakness of CONFIDANT is its complexity, due to the need of extra components and sending extra messages. Moreover, the reliability of the alarms is not guaranteed.

SORI [36] is a mechanism used to detect selfish nodes. The trust of the node is based on a local evaluation (first hand trust). In other words, a node personally evaluates its neighbor nodes, and also uses the second hand trust evaluation from other nodes. Based on these trust evaluation, actions are taken against selfish nodes.

Cooperative on demand secure routing (COSR) protocol [15] is designed on top of the DSR routing protocol. It uses reputation system to detect misbehaving nodes and increase the cooperation between nodes. Contribution of nodes, capability of forwarding packets and recommendation are the parameters that are used to measure the node and route reputation. The contribution refers to the number of routes and data packets forwarded between nodes. Capability of forwarding packets refers to the ability to send packets of a certain node using energy and bandwidth threshold [15]. Recommendation is other nodesâĂŹ subjective recommendation.

COSR has proven well with selfishnodes, wormhole, blackhole and rushing attack but not in DOS attack. Above models have high false detection of selfish nodes because they are vulnerable to collision attacks. Whereas, The proposed model is built over QOLSR protocol, where selfish nodes are detected cooperatively to decrease the false detection.

Moreover, RPASRP [17] is a privacy-aware secure routing protocol based on multi-level security mechanism to provide support for privacy protection and protect against internal attacks in WMNs. It depends on the mix usage of dynamic reputation mechanism built by Merkle Tree technology, role based multi-level security technology, subject logic and uncertainty, and hierarchical key management protocol. RPASRP protect against specific internal attacks initiated by compromised mesh routers and provide authenticity, integrity and secrecy of routing packets. This model showed that it is secure, privacy preserving and efficient. It showed a high packet delivery ratio and shorter average route length with respect to other models. Also, an integrated system was conducted based on the reputation and price-based systems [46] that overcome the drawbacks of the reputation system and price-based system, which are the two major approaches that deal with the cooperation problems in MANET. This system showed the effectiveness in terms of cooperation incentives. This integrated system was based on leveraging the advantages of both systems. Analysis showed that the integrated system provided higher performance than the other two systems regarding detection of selfish nodes and cooperation incentives.

Despite the advantages of the above detection schemes, these mechanism lack efficiency in terms of ambiguous collision, false alarms and detection, non-cooperative decision unlike the security model proposed in this thesis.

2.5 Cooperative Game Theory and shapley value

Game theory is a study of strategic decision making used when an action of a component depends on the others [23]. This theory is used to reach an optimal decision. For example, a company can not take a decision of reducing its products prices without taking into consideration other companies actions. These companies are the players in this game. Without considering all players decision, the company might be taking a wrong decision that will make the company lose. Game theory is extensively used in the domain of computer science, biology, economy and military. This game is built of seven main components; information, players, strategies, actions, outcomes, payoff, and equilibrium. The players are the components that make decisions. The actions are a group of decisions of which the players have to choose. The information is the learning of the player while taking the decision. The principles that control the decision making of the player are the information and the desired decision is the outcome. Shapley value is used in Game theory to represent the marginal contribution of each player in the game according to a uniform distribution over the set of all permutation on the set of players. Shapley value can provide one answer to the following questions; how much important is each player with respect to other cooperating players in the game?what gain that each player expects? Formally, shapley value is defined in equation1.

$$\phi_i(v) = \frac{1}{N}\sum_R v(P_i^R \cup i) - v(P_i^R) \tag{1}$$

Function *v* is the value function which is the worth of a certain coalition of players in *S*. In other words, it represents the anticipated sum of payoffs the players in *S* can have when cooperating. The sum is over all N in the order *R* of the players and P_i^R is the players in *N* which come before *i* in the order *R*.

As an example, consider a coalition game with three players N = 1,2,3 of which 1 and 2 have two right hand gloves whereas 3 has a left hand glove. The game is to form a pairs. The function *v* is given in equation 2.

$$v(S) = \begin{cases} 1 & \text{if S} \in \text{\{1,3\},\{2,3\},\{1,2,3\}} \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

To calculate the marginal contribution of player 1, we refer to equation1. Table1 represents the marginal contribution of player 1 in all orderings.

Table 1: Marginal Contribution of Player 1

Order R	Marginal Contribution of Player 1
$1, 2, 3$	$v(1) - v(\phi) = 0 - 0 = 0$
$1, 3, 2$	$v(1) - v(\phi) = 0 - 0 = 0$
$2, 1, 3$	$v(1, 2) - v(2) = 0 - 0 = 0$
$2, 3, 1$	$v(1, 2, 3) - v(2, 3) = 1 - 1 = 0$
$3, 1, 2$	$v(1, 3) - v(3) = 1 - 0 = 1$
$3, 2, 1$	$v(1, 2, 3 - v(2, 3) = 1 - 1 = 0$

Therefore, $\phi_1(v) = (1)\frac{1}{6} = \frac{1}{6}$. By symmetry, $\phi_2(v) = \phi_1(v) = \frac{1}{6}$. Since the sum of of all shapley values is 1, $\phi_3(v) = \frac{2}{3}$.

This is widely applied to get the expected value of contribution of a player in a game.

2.6 Conclusion

We presented in this chapter the concept of MANETs, security in MANETs and its challenges. Also, we explained game theory and shapely value that were used in this thesis to ensure efficient cooperation between nodes. We presented in this chapter the related works in the fields of clustering and security in mobile ad hoc networks. The existing clustering algorithms lack the ability of selecting and maintaining the best paths with respect to QoS, delay, and overhead. Regarding the misbehaving mobile nodes, the existing approaches have high rate of false detection of selfish nodes.

Chapter 3

Reputation-Based Model in Cluster-based QoS-OLSR Protocol

3.1 Introduction

In this chapter, we present the new metric functions of our proposed models. These functions are based on the available bandwidth, connectivity index, residual energy and reputation of the nodes. Adding reputation as a parameter of the QoS metric functions should increase trust in the network without sacrificing quality of service. These functions are used by the cluster head nodes election algorithm which elects a group of cluster heads. These elected CH nodes then select a group of the MPR nodes which assure that the network is connected [18].

Section 3.2 describes the clustering algorithms used and the novel model based on the Clustered-based QoS-OLSR Network. Then, Section 4.4 presents empirical results. Finally, Section 5 concludes the chapter.

3.2 The Quality of Service Metric Models

In this section, we present the clustering algorithms of our model that are based on the Quality of Service metric function bandwidth, connectivity index, and residual energy. Implementing these concepts will help us to prolong network lifetime without sacrificing QoS. Our clustering algorithm can be briefed with two steps. First, the cluster head election algorithm elects a set of optimal cluster heads. Second, the elected cluster heads will select the set of optimal MPR nodes that can lead to a connected network. To have better performance and quality of service, we introduce the cluster-based QoS-OLSR approach.

Based on the clustering concept, we propose a solution that has four different clustering models based on three metrics: bandwidth, connectivity index and residual energy.

To rely on nodes which are more trustworthy, while keeping the same performance and quality of service, we propose to include the nodes reputation as a parameter of the QoS metric functions. These functions are used to elect the CH nodes and select the MPR nodes interconnecting the CH nodes. In Table 1, the QoS metric functions of the four QOLSR models are defined.

These metric models can be used to define eight different protocols:

- Classical QOLSR with RB-OLSR model (or RPB-OLSR, RBE-OLSR, RPBE-OLSR)
- Cluster-based QOLSR with RB-OLSR model (or RPB-OLSR, RBE-OLSR, RPBE-OLSR)

In the former case, the QOLSR protocol [16] is extended and uses the defined QoS metric models to select the MPR nodes. In the latter case, each node first elects its most

Algorithm 1: Quality of Service Metric Models

```
Let $i$ be a node in the network. Let define;
    $QoS(i)$  =  Its quality of service metric
    $BW(i)$   =  Its available bandwidth
    $N(i)$    =  Its number of neighbors
    $RE(i)$   =  Its residual energy
    $R(i)$    =  Reputation of $i$
Reputation Bandwidth - OLSR Model (RB-OLSR)
    $QoS(i) = BW(i) + \frac{R(i)}{\sum R(i)}$;
Reputation Proportional Bandwidth OLSR Model (RPB-OLSR);
    $QoS(i) = \frac{BW(i)}{N(i)} + \frac{R(i)}{\sum R(i)}$;
Reputation Bandwidth & Energy OLSR Model (RBE-OLSR);
    $QoS(i) = BW(i) \times RE(i) + \frac{R(i)}{\sum R(i)}$;
Reputation Proportional Bandwidth & Energy OLSR Model (RPBE-OLSR);
    $QoS(i) = \frac{BW(i) \times RE(i)}{N(i)} + \frac{R(i)}{\sum R(i)}$;
```

trustworthy neighbor as its local CH node based on its QoS metric. Once all the CH nodes have been identified, these nodes use the defined QoS metric models to select the MPR nodes interconnecting them.

3.2.1 Reputation-Cluster-based QoS-OLSR Approach

The Cluster Head Election

To elect the set of optimal cluster head nodes and partition the network into clusters, an election algorithm is modeled, where each node votes for its neighbor node that has the maximum value of Quality of Service Metric. In case the node has the maximum value, then it can vote for itself. This solution presents a one-hop clustering model because every node is one-hop away from its elected cluster head. The elected cluster heads would act as MPR nodes for their electors after the election algorithm is finished. Some modifications

```
Cluster Head Election Algorithm
Let $i$ be a node in the network.
1 Let $k \in N_1(i) \cup \{i\}$ be s.t.
    $QoS(k) = \max\{QoS(j) | j \in N_1(i) \cup \{i\}\}$.
2 The node $i$ votes for $k$.
3 $MPRSet(i) = \{k\}$.
```

have to be done:

1. Flag a node to show that it has been assigned as a cluster head.

2. Flag a neighbor that has been elected as a cluster head.

For each of its neighbors, a node shows for which node its given neighbor has voted for. Before the nodes can update their local information, the results of the election have to be broadcasted to them.

The MPR Nodes Selection

Once the cluster heads have been designated, they are responsible to select a group of optimal MPR nodes. This group of nodes links the clusters into a connected graph, if one exists. Note that the 1-hop cluster heads can be directly reached and therefore there is no need to select MPRs in between. Moreover, the 2-hop cluster heads connected to 1-hop

```
MPR - Part I: Computing the neighbor clusters
Let $k$ be any elected cluster head.
1 the 1-hop cluster heads as
    $CH_1(k) = \{i \in N_1(k) | i \text{ has its CH flag set}\}$.
2 the 2-hop cluster heads as
    $CH_2(k) = \{i \in N_2(k) | i \text{ has its CH flag set}\}$.
3 the 3-hop cluster heads as
    $CH_3(k) = \{j | (\exists i \in N_2(k))[i \text{ voted for } j]\} \setminus N_{1,2}(k)$.
4 the set of cluster heads to be covered as
    $CH(k) = CH_3(k) \cup$
    $CH_2(k) \setminus \{j | (\exists i \in CH_1(k))[j \in N_1(i)]\}$.
```

cluster heads do not have to select any MPR to connect them. Therefore, the main problem is to reliably cover the 3-hop cluster heads. In MPR-Part II, the algorithm computes the MPR nodes to cover the 2-hop cluster heads.

```
MPR - Part II: MPR nodes for the nodes in $CH_2(k)$
Let $k$ be any elected cluster head.
While $CH(k) \neq \emptyset$
  Find $l \in CH(k) \cap CH_2(k)$ s.t.
    The path $(k, x, l)$ maximizes $QoS(x)$ among all paths
    connecting $k$ to any other uncovered node.
      $MPRSet(k) = MPRSet(k) \cup \{x\}$.
      Remove from $CH(k)$ all the nodes in $CH_2(k)$
      reachable from $x$.
```

Finally, the 3-hop cluster heads are selected in MPR-Part III. In such a case, To reach any 3-hop cluster head, two MPR nodes are needed.

```
MPR - Part III: MPR nodes for the nodes in $CH_3(k)$
Let $k$ be any elected cluster head.
While $QoS(k) \cap CH_3(k) \neq \emptyset$
  Find $l \in QoS(k) \cap CH_3(k)$ s.t.
    The path $(k, x, y, l)$ maximizes $min(QoS(x), QoS(y))$ among
    all paths connecting $k$ to any other uncovered node.
      If there are two such paths, take the first one
      in the lexicographic order.
        $MPRSet(k) = MPRSet(k) \cup \{x\}$.
        Remove from $CH(k)$ all the nodes in $CH_3(k)$
        reachable from $x$.
```

The correctness of this part has to be proven formally. If the cluster head k selects the MPR node x, the cluster head l has to select the MPR node y to assure that k and l are connected.

It is very crucial for each cluster head to have more than one choice to connect to its neighbor cluster heads.

Illustrative Example

To clarify the election and selection of cluster head and MPR, respectively, Figure 2 presents a network with twenty nodes and Table 2 provides the Quality of Service Metric values of each node in this network using the Proportional BE-OLSR Model (refer to Table 1). To find the Quality of Service metric of each node in the network, the residual energy which is a random value between 500 and 550 (refer to Table 2) is divided by the connectivity index and multiplied by bandwidth.

Each node votes for its maximal Quality of Service metric value neighbor node, after receiving the Hello messages from it. Using the Cluster Head Election Algorithm, nodes: 3, 4, 5, and 15 are elected as head clusters (MPRs).

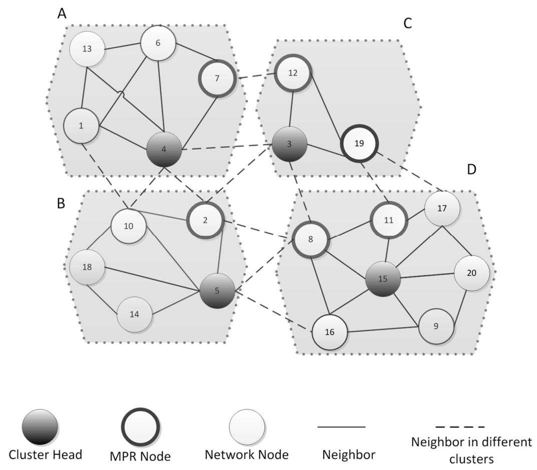

Figure 2: Ad hoc Network example

Once the cluster heads are elected, they select the MPR nodes that connect all cluster heads together. We will consider node 15 in cluster D to illustrate our example. First, is to find the neighbor cluster heads for node 15. Referring to MPR-Part I, we need to

Table 2: Quality of Service QoS Metric using the Reputation Proportional BE-OLSR Model

Node	$n1$	$n2$	$n3$	$n4$	$n5$	$n6$	$n7$	$n8$	$n9$	$n10$	$n11$	$n12$	$n13$	$n14$	$n15$	$n16$	$n17$	$n18$	$n19$	$n20$
QoS Metric	370.85	297.35	500.25	479.45	516.75	338.75	231.15	220.45	490.65	246.45	250.65	193.15	127.25	159.95	600.95	109.95	101.55	495.35	400.55	550.75

find the 1-hop cluster head, $CH1$, the $2-hop$ cluster head, $CH2$, and the 3-hop cluster head, CH3. So, $CH1(15)$=ϕ since there is no $1-hop$ cluster head connected to node 15. $CH2(15)=5$ since node 5 is a 2-hop cluster head to node 15, and similarly for $CH3$(15)=3 and CH3(15)=4.

The second step is to find the optimal path that will connect the 2-hop cluster heads that are node 15 and node 5. Node 8 and node 16 are common neighbors for these 2 head nodes, but according to MPR-Part II Algorithm, node 8 is chosen as the MPR node since it has a better QoS metric value than node 16. Now, we need to find the optimal path for the 3-hop cluster heads referring to MPR-Part III. There are two choices to connect head node 15 with head node 3, either through {node 11, node 19} or {node 17, node 19}. Head node 15 chooses the path {node 11, node 19} which has the maximal QoS metric value. However, head node 15 would select only node 11 as an MPR node and, symmetrically, head node 3 would select node 19 as an MPR node. Similarly, the optimal path with {nodes 8 and 3} to reach cluster head node 4 is found.

The Reputation Payment

A node will gain reputation when elected as a CH node or selected as a MPR node. Hence, a node j should pay to an elected/selected node i some $P(j)$ in the form of reputation if node i accepted to play its role. Cluster Head Payment algorithm represents the payment mechanism to a CH node where each elector will pay using the incentive compatible mechanism VCG where truth telling is the dominant strategy. Such a payment does not depend on what nodes reveal. But it depends on the second best choice, where the payment is the difference between the QoS of the elected node (CH/MPR) and the second best QoS node in their neighborhood.

```
Algorithm 2: Cluster Head Payment algorithm
Let $i$ be an elected CH node.;
for $\forall j \in N_1(i) \cup \{i\}$ do
    $P(j) = QoS(i) - \max\{QoS(k) | k \in N_1(j) \cup \{j\} \backslash \{i\}\}$;
    $R(i) = R(i) + P(j)$;
```

The electing nodes send their payments using their Electing message (a specialized Hello message). Once a CH node has received its payment, it should rebroadcast them in its Hello messages. Thus, any electing node can check whether or not a CH node follows the protocol honestly. For more details, refer to the RBC-OLSR protocol [24].

Then, a pair of CH nodes which are two-hop away will have to pay the selected MPR node. This is shown in the Two-hop away MPR Payment algorithm.

```
Algorithm 3: Two-hop away MPR Payment algorithm
Let $k$ and $l$ be two CH nodes that are two-hop away.;
Let $i$ be the MPR node connecting $k$ and $l$ s.t. $\min(QoS(i))$ is maximized among all paths.;
$P(k) = QoS(i) - \max\{QoS(j) | j \in N_1(k) \bigcap N_1(l) \backslash \{i\}\}$
$P(l) \ = QoS(i) - \max\{QoS(j) | j \in N_1(k) \bigcap N_1(l) \backslash \{i\}\}$
$R(i) = R(i) + P(k) + P(l)$;
```

The pair of CH nodes which are three-hop away will have to pay its selected neighbor serving as MPR node. This is shown in the Three-hop away MPR Payment algorithm.

Algorithm 4: Three-hop away MPR Payment algorithm

```
Let $k$ and $l$ be two nodes that are three-hop away.;
Let $i$ and $j$ be two MPR nodes connecting $k$ and $l$ s.t. $\min(QoS(i), QoS(j))$ is maximized among all paths.;
Let $i^*$ and $j^*$ be two nodes connecting $k$ and $l$ s.t. $\min(QoS(i^*), QoS(j^*))$ is maximized among all paths avoiding $i$ and $j$.;
$P(k) = \min(QoS(i), QoS(j)) - \min(QoS(i^*), QoS(j^*))$
$R(i) = R(i) + P(k);$
$R(j) = R(j) + P(k);$
```

3.2.2 Illustrative Example

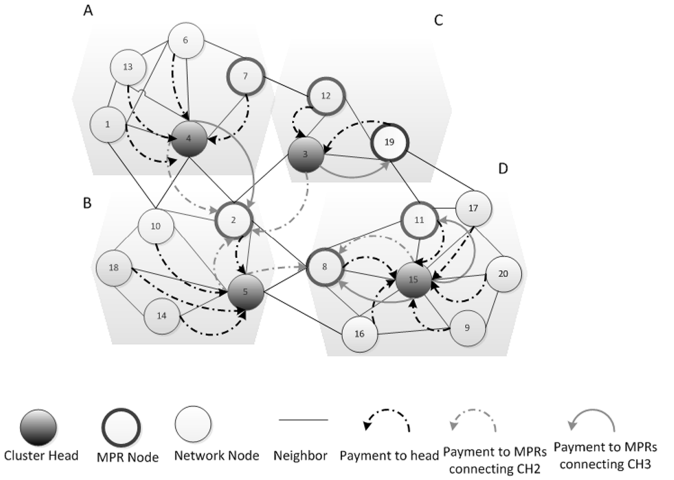

Figure 3: Reputation Mechanism example

To illustrate the payment mechanism, the example presented in Fig. 3 shows a network where the CH and MPR nodes are selected [18] and with arrows representing the direction of the payments. First, using the Cluster Head Payment algorithm, the CH nodes $\{N_3, N_4, N_5, N_{15}\}$ are paid by all their neighbors. For example, the nodes $\{N_2, N_{10}, N_{14}, N_{18}\}$ will pay the CH node N_5. $R(N_5)$ will be equal to $R(N_5) + P(N_2) + P(N_{10}) + P(N_{18}) + P(N_{14})$. $P(N_2)$ is equal to $QoS(N_5) - QoS(N_3)$ which is 16.5. Similarly, $P(N_{10}) = QoS(N_5) - QoS(N_{18}) =$ 21.4, $P(N_{18}) = QoS(N_5) - QoS(N_{10}) =$ 270.3, $P(N_{14}) =$

$QoS(N_5) - QoS(N_{18}) = 21.4$. If the initial reputation $R(N_5)$ is 100, its new reputation is given by $100 + 16.5 + 21.4 + 270.3 + 21.4 = 429.6$.

Second, we need to calculate the new reputation of the MPR nodes connecting the 2-hop away CH nodes using Two-hop away MPR Payment algorithm. Consider the MPR node N_8 to illustrate the mechanism. N_8 connects the CH node N_{15} with the CH node N_5 so each CH node should pay N_8. Since N_{16} is a common neighbor between N_5 and N_{15} and the next best candidate nodes (with respect to the QoS metric), $R(N_8) = R(N_8) + 2(QoS(N_8) - QoS(N_{16}))$.

Finally, we need to calculate the new reputation of the MPR nodes connecting 3-hop CH nodes using Three-hop away MPR Payment algorithm. Consider the CH node N_{15} and the CH node N_3, that are connected through N_{11} and N_{19}. The second best QoS path uses N_8 and N_2.

The difference between the two QoS is $P(N_3) = P(N_{15}) = \min(QoS(N_{11}), QoS(N_9)) - \min(QoS(N_8), QoS(N_2)) = 30.2$. However, the CH node N_3 will pay N_{19} and the CH node N_{15} will pay N_{11}. Then, $R(N_{19}) = R(N_{19}) + P(N_3)$ and $R(N_{11}) = R(N_{11}) + P(N_{15})$.

3.3 Simulation Results

Matlab-8.0 has been used to simulate the Classical QOLSR with B-OLSR, PB-OLSR, BE-OLSR, PBE-OLSR, and Cluster-based QOLSR with B-OLSR, PB-OLSR, BE-OLSR, PBE-OLSR, RB-OLSR, RPB-OLSR, RBE-OLSR, RPBE-OLSR models to present the impact of adding the nodes reputation as a parameter of the QoS metric functions on the network performance. Nodes in all networks are considered to be mobile. Random Waypoint

Mobility Model [43], a very common and widely used mobility model is implemented in Matlab to simulate our results. This mobility model is a straightforward model that was used to move nodes in our network. A node moves in a straight line with a constant speed to a randomly choosen destination node in the network. This recurse at a constant pause time. The coordinates of the nodes are based on a discrete-time stochastic process where they are distributed over the network space using a uniform random stochastic model. The speed, direction and pause time are also defined based on a uniform random distribution process where they are defined in the parameter table. This model is suitable for low speed mobility and for open area systems where no barriers are induced [11]. The simulation is divided into four subsections. The first, second, and third subsection shows the percentage of selected MPR nodes, number of alive nodes and the path lengths that represent delay, respectively, in the three scenarios: Classical QOLSR, Cluster-based QOLSR, and Cluster-based QOLSR with reputation. The fourth subsection presents a table of the average trust difference. All our simulation results have a 95% confidence level. The upper and lower bounds are calculated accordingly to make sure that the calculated means of the simulations are within such interval. The simulation parameters are summarized in Table 3.

3.3.1 Percentage of MPR nodes in the Network

In Fig 4, the cluster-based models considerably decrease the number of selected MPR nodes. These selected MPR nodes contain the cluster heads which act as specialized MPR nodes. It is obvious that the reputation cluster-based models have approximately the same percentages of MPR nodes; this means that including reputation as one of the QoS metrics

Table 3: Simulation Parameters

Parameter	Value
Simulation area	500×500 m
Number of nodes	Between 30 and 70
Transmission range	125 m
Mobility Speed	Random value in [1...10] msec
Mobility Direction	Random value in $[0...\pi]$ m/sec
Pause Time	10 sec
Residual energy	Random value in [500..550] Joules
Initial Reputation	100
Packet Size	Random value in [0.5..1.5] kb
Energy Per Packet	0.0368 J
Idle Time	Random value in [0..1]
Link Bandwidth	2Mbps
Available Bandwidth	$Idle\ Time \times Link\ Bandwidth$
Run Iterations	$100\ iterations\ (95\%\ confidence\ level)$

does not increase the number of selected MPR nodes. Comparing the four models, obviously in Fig 4, the "with clustering" BE-OLSR model has the minimum percentage of MPR nodes, since these nodes are selected according to the two parameters that are bandwidth and energy without being proportional to the number of neighbor nodes.

3.3.2 Network Lifetime

The energy consumption at node i is computed using the following parameters:

- $BW(i)$: Available bandwidth at node i.
- $RE(i)$: Residual energy of node i.
- $EN(i)$: Energy consumed by node i.
- Packet size.

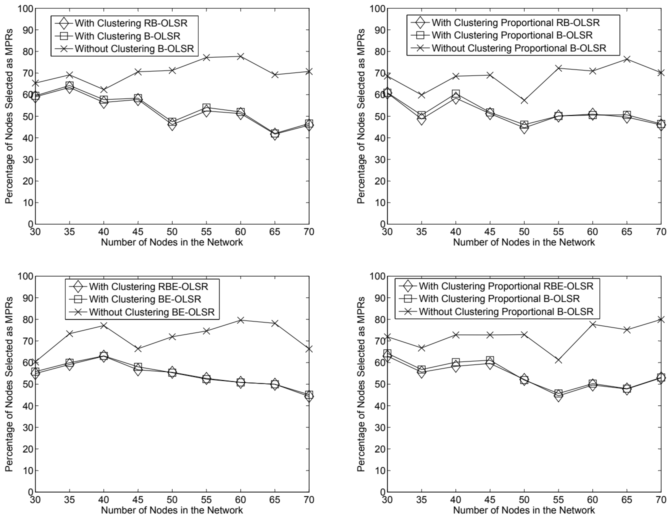

Figure 4: Percentage of MPR Nodes: (a) B-OLSR (b) Proportional B-OLSR (c) BE-OLSR (d) Proportional BE-OLSR

- Energy per Packet.

In Fig 5, we show the percentage of alive nodes and how the energy drains for a 70 node network for all the models. The energy spent by relay nodes is considered where the Energy Consumption (EN) is calculated using Equation 3. This will be done by finding the total number of packets the node i will transfer. This value is achieved by dividing the available bandwidth at node i by the mean packet size 1kb. Then, we have to multiply the total number of packets transferred by the energy per packet which is $0.0368J$ according to the simulation parameters table (refer to equation 3). The residual energy is decreased by the value of Energy consumption. (refer to equation 4)

$$EN(i) = (BW(i) \; / \; Packet\ size) \times \; Energy\, per\ Packet\ J \tag{3}$$

$$New\ RE(i) = RE(i) \; - \; EN(i)\ J \tag{4}$$

As expected, the clustered models "with reputation" and "without reputation" in Fig 5 have the same network lifetime because they have the same number of selected MPRs. It

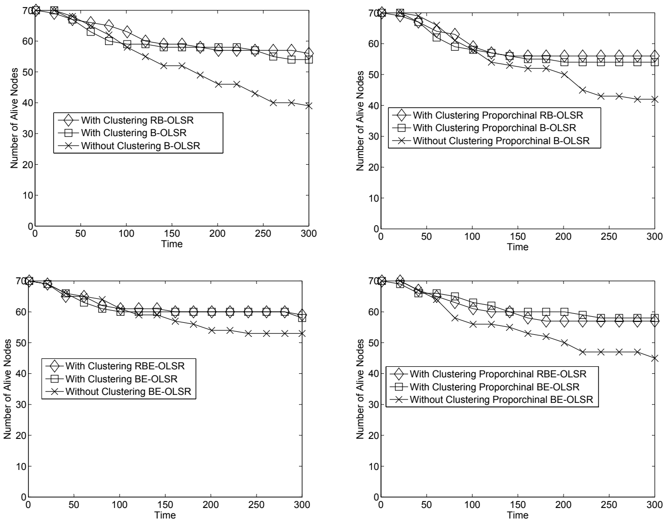

Figure 5: Percentage of alive nodes over time: (a) B-OLSR (b) Proportional B-OLSR (c) BE-OLSR (d) Proportional BE-OLSR

is significant that the with clustering proportional B-OLSR (see Fig 5, a) has the worst network life time among all clustered models, whereas, with clustering BE-OLSR shows the best results overtime compared to others. The models that depend on the residual energy prolong the network lifetime because the MPR nodes are chosen based on the residual energy of nodes. It is clear that the reputation does not affect network life time.

Another aspect to consider, in this analysis, is the end-to-end delay in the network. Figure 6 represents the source-destination path length of the four different models of the "reputation with clustering”, "with clustering" and “without clustering” networks. The path length is presented by the average number of hops between source and destination. The path with the best Quality of Service metric is selected as the source-destination optimal path. In each figure, we show a comparison of the average path length for the three models. The “reputation with Clustering”, "with Clustering" and “without Clustering” Models show similar results. Thus, including reputation as a QoS metric in the election phase does not increase the delay in the network.

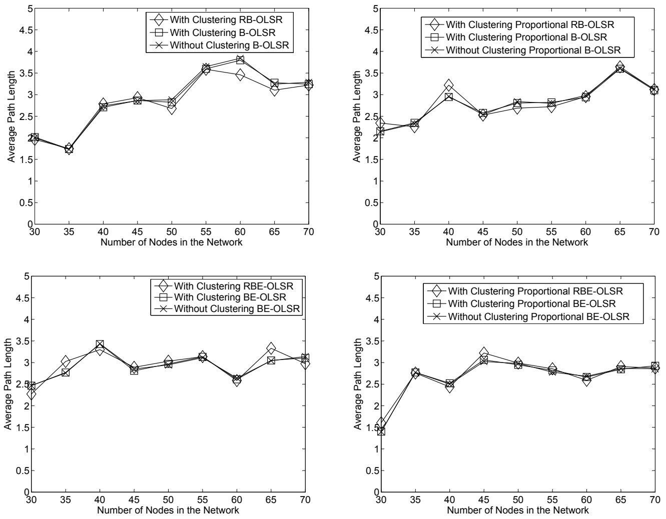

Figure 6: Average Path Length: (a) B-OLSR (b) Proportional B-OLSR (c) BE-OLSR (d) Proportional BE-OLSR

3.3.3 Average Trust Difference

Moreover, trust is an essential property of nodes in a mobile ad-hoc networks which leads to a more reliable and cooperative network. It is essential to measure how much our model is trustworthy. Therefore, we measured the average difference of reputation which is the difference between the optimal reputation and the current reputation in the network for all models having 30, 50, 70 and 100 nodes in the network. The optimal reputation is measured by choosing the packet forwarding path just according to the best reputation, whereas the current one is measured based on our models. As the percentage difference decrease, the model is more trusted. Table 4 represents the percentage average difference for different number of nodes in the network for the four models that take into consideration reputation in its QoS metrics. According to this table, the with clustering proportional RB-OLSR has less than 1% reputation average difference percentage which is the minimal.

In Summary, our clustering approach prolonged network lifetime by decreasing the

Table 4: Trust Average Difference

Models	Number of Nodes in Network			
	30	50	70	100
with clustering Prop. RBE-OLSR	15.49%	19.7%	24.16%	25.14%
with clustering Prop. RB-OLSR	1.32%	0.65%	0.95%	0.79%
with clustering RBE-OLSR	6.54%	12.95%	26.19%	19.04%
with clustering RB-OLSR	2.43%	4.86%	3.52%	2.9%

number of selected MPR nodes. The clustered-based RBE-OLSR model showed best results regarding network lifetime. Moreover, results show that adding trust in the form of reputation did not affect the percentage of MPRs, network lifetime, and delay in the network. Comparing the four models, the most trusted one is the clustered-based RB-OLSR which show a very low average difference between the optimal reputation and the reputation in the network. The payment mechanism gives an incentive to the network nodes not to act selfishly during the electionselection of MPR nodes.

3.4 Conclusion

The shortage of energy and the struggle of recharging in ad hoc networks made selfish nodes a common problem during and after selection of MPR nodes in a cluster-based QOLSR network. All experimental results are done on the mobile cluster-based QOLSR models. We present a novel efficient motivation model that motivates nodes during selection to behave normally by increasing their reputation then consider it when selecting MPR nodes. Also, nodes with higher reputation have higher priority in the network to get access to services. As expected, results show that including reputation as one of the QoS metric does not affect the performance and Quality of Service QoS of the network, whereas it makes the network more reliable and trustworthy.

Chapter 4

Cooperative Detection Model of Selfish Nodes

4.1 Introduction

After designing a model that elects trusted CH nodes and selects trusted MPR nodes, we present in this chapter a mechanism to detect CH or MPR nodes behaving selfishly after their selection. Unfortunately, a node can refuse to serve other nodes after being elected/selected. Therefore, we propose to use a detection system based on the concept of watchdogs to monitor the elected/selected nodes. This system is implemented over the cluster-based QOLSR network in order to detect and catch passive malicious (selfish) nodes. Then, we present a formal analysis to prove the efficiency of our detection model based on shapley value.

Section 4.2 presents the detection model based on the Hierarchical Cooperative Watchdog. Section 4.3 presents an incentive model and a formal analysis of the detection model.

Then, Section 4.4 presents empirical results. Finally, Section 5 concludes the chapter.

4.2 Detection Model: Hierarchical Cooperative Watchdog

After designing a model that elects trusted CH nodes and selects trusted MPR nodes, we need to use a mechanism to detect CH or MPR nodes behaving selfishly after their selection. Unfortunately, a node can refuse to serve other nodes after being elected/selected. Therefore, we propose to use a detection system based on the concept of watchdogs to monitor the elected/selected nodes. This system is implemented over the cluster-based QOLSR network in order to detect and catch passive malicious (selfish) nodes.

A watchdog is a node that monitors the behavior of CH and MPR nodes [32]. One of the main problems of the watchdog detection model is the high rate of false positive and false negative alarms. The former case corresponds to alarms falsely accusing nodes to be selfish while the latter case corresponds to nodes dropping packets without being detected. Thus, our main objective is to increase the trustworthiness of the model and decrease the rate of false alarms. To improve performance, reduce false detection rate, and overcome the limitations of the watchdog nodes, we reuse the hierarchical structure of the cluster-based QOLSR network to build our monitoring system.

The hierarchical model has two layers. The nodes that have elected the CH node belong to the first layer and they are responsible to monitor their corresponding CH node. As the second layer, the CH nodes that have selected the set of MPR nodes must monitor them. Hence, the evaluation of a given node as *normal* or *selfish* node is based on the evaluation of all the watchdog nodes monitoring this node. Based on our model, nodes with higher reputation has leading impact on the final decision. The Hierarchical Cooperative Watchdog algorithm presents the detection mechanism.

Algorithm 5: Hierarchical Cooperative Watchdog algorithm

```
Let $w$ be a watchdog monitoring $N_i$.;
while a packet $p$ is received do
    if $N_i$ is the source or the destination of $p$ then
        Simply ignore $p$.;
    else
        $p$ has to be transmitted by $N_i$.;
        Add $p$ to a time-based data structure $T$.;
        if $p$ has been transmitted by $N_i$ then
            Remove $p$ from $T$. ;
            $N_i$ is normal.;
        else
            if $p$ is still in $T$ after some timer $\Delta$ then
                $N_i$ is Selfish.;
```

The watchdog nodes should monitor the intermediate nodes responsible of forwarding data packets between the source and the destination nodes. A watchdog can monitor any neighbor node in its transmission range. Thus, an electing node should watch its elected CH node. Similarly, a CH node should watch its selected MPR node(s). Any watchdog should maintain a buffer (or any other efficient data structure) to decide whether or not the supervised node N_i forwards the data packet as supposed. If a packet p stayed in the time-based data structure T more than a time Δ, then N_i is considered a selfish node. Otherwise, N_i behaves normally.

The evaluation of a monitored node (either a CH or an MPR node) should be based on the weighted decisions of all neighbor watchdog nodes. Thus, the decisions of a given watchdog should be weighted according to its reputation. A more trustable watchdog should be considered over a less trustable one. Such an evaluation can be achieved by the aggregation function given in Eq. 6.

$$f(w_j, N_i) = \begin{cases} 1 & w_j \text{ detect } N_i \text{ as selfish} \\ \\ 0 & w_j \text{ detect } N_i \text{ as normal} \end{cases} \tag{5}$$

$$F(W_i, N_i) = \frac{\sum_{w_j \in W_i} R(w_j) \times f(w_j, N_i)}{\sum_{w_j \in W_i} R(w_j)} \tag{6}$$

where W_i is the set of nodes monitoring N_i.

If $F(i)$ is greater than a specific threshold, in the example we use it as 0.5, then N_i is considered a selfish, otherwise it is considered as a normal.

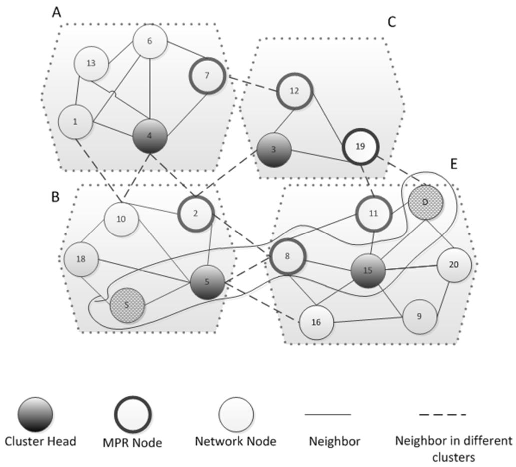

Figure 7: Hierarchical Cooperative Watchdog Mechanism example

Assume node S wants to forward a packet to node D as illustrated in Figure 7. The packet should be forwarded through the path $\{N_5,\ N_8,\ N_{15}\}$. These nodes should be monitored by watchdog nodes. In this example, since N_5 is a CH node then it should be monitored by its electing nodes $\{N_2, N_{10}, N_{18}, S\}$; N_8 should be monitored by the CH nodes $\{N_5,\ N_{15}\}$; N_{15} should be monitored by the electing nodes $\{N_8, N_9, N_{11}, N_{16}, N_{20}, D\}$. We illustrate the monitoring steps of N_5. First, N_{20} should compare the packets sent by N_8 to N_{15} with the packets sent by N_{15} to node D. Thus, a watchdog N_{20} should determine whether N_{15} forwards packets as expected or whether it acts selfishly and drop them. Assume that CH node N_{15} is a selfish node and that $f(N_8) = 1$, $f(N_9) = 0$, $f(N_{11}) = 1$, $f(N_{16}) = 1$, $f(N_{20}) = 1$, $f(N_{17}) = 0$, and $R(N_8) = 150$, $R(N_9) = 120$, $R(N_{11}) = 165$, $R(N_{16}) = 100$, $R(N_{20}) = 180$, $R(N_{17}) = 110$, then $F(N_{15}) = (1 \times 150 + 0 \times 120 + 1 \times 165 + 1 \times 100 + 1 \times 180 + 0 \times 110) \div (150 + 120 + 165 + 100 + 180 + 110) = 0.73$. Thus, N_{15} could be truly detected as selfish node since $F(N_{15})$ is greater than 0.5. The main issue here is how to motivate watchdogs to not behave selfishly and cooperate with each other.

4.3 Incentive Model: Contribution of Cooperative Watchdogs based on Shapley Value

Watchdog nodes may behave selfishly while detecting selfish nodes and give false alarms, therefore in this section, we propose an incentive model based on Shapley value to motivate watchdogs to behave normally and monitor the elected/selected nodes. Also, Shapley can be used to analyze our proposed hierarchical model where the detection does not require the detection level of all the watchdogs. Assume that *N* is the set of nodes in network *G*, each node in *G* will represent a player in the cooperative *n* person game where *n*=*N*. A coalition is a set of players cooperating to reach a decision. In our model, the players have to cooperate to decide if a node is behaving selfishly or normally. In cooperative game theory, a coalition is defined as:

$$\Delta \subseteq N \text{ and } \forall x \in \Delta$$

$$f(x) = \begin{cases} 1 & x \text{ detect } N_i \text{ as selfish} \\ 0 & x \text{ detect } N_i \text{ as normal} \end{cases} \tag{7}$$

So, a coalition is the set of watchdog nodes that are voters of N_i in case it is a CH node, or CH nodes in case N_i is an mpr, where N_i the node that is being monitored. Each player in the coalition will report if N_i is selfish or not and give the value 1 or 0. We use the weighted aggregation function 6 over Δ to decide whether the node should be considered selfish or normal. Each node in Δ, will have certain value of impact on the final decision. It is important in our model to show that the incentive is allocated over the nodes in Δ that influenced the decision. This will motivate nodes to always monitor and not to be selective while monitoring in order to receive a reward of detection. To be able to find the impact of each player, we need to calculate the contribution of each node N_i in Δ. Shapley value [19] will be used to present the marginal contribution of each player in the cooperative game according to a uniform distribution over the set of all arrangements on the players.

First, we find all different subsets for the nodes $\prod_{\Delta}$ in Δ. The contribution of node N_i will be the average of all the differences between the function including all nodes in the subset including node N_i and the same function of all nodes but excluding N_i where δ is the number of subsets.

$$\phi_{N_i}(\Delta) = \frac{1}{\delta} \sum_{\pi \in \prod_{\Delta}} F(P_{\pi}^{N_i} \cup N_i) - F(P_{\pi}^{N_i}) \tag{8}$$

Referring to example 7, where the CH node N_{15} is monitored, Shapley value is utilized to measure the contribution of each potential watchdog nodes. Table 5 represents the reputation of each watchdog monitoring head N_{15}.

Table 5: Nodes Reputation

Node	N_8	N_9	N_{11}	N_{16}	N_{17}	N_{20}
Reputation	150	120	165	100	110	180

Using equation 8, we calculate the contribution value of each node that will be used to reward each watchdog.

Table 6: Contribution Value

Node	N_8	N_9	N_{11}	N_{16}	N_{17}	N_{20}
Contribution Value	0.19	0.11	0.21	0.08	0.11	0.3

It is clear that nodes with higher reputation have higher contribution on deciding whether a node is selfish or normal. This is one of the advantages of our hierarchical watchdog model where nodes with low reputation has less impact. This is why we introduced the idea of having an incentive model that motivates nodes with high reputation to serve as monitors and cooperate with others. Therefore, subgroups of the 6 nodes were selected and their corresponding validation value was calculated using the weighted aggregation function 6. Table 7 presents the validation values of the different subgroups starting with all the 6 watchdogs followed by the decision of the set of 5 nodes $\{N_{11}$,N_8,N_9,N_{20},$N_{17}\}$ with highest reputation, then, the other set of 4 nodes $\{N_{11}$,N_8,N_9,$N_{20}\}$ with the highest reputation, and finally, the set of 3 nodes $\{N_8$,N_{11},$N_{20}\}$ with highest reputation.

Table 7: NODES Validation Value

Count of Nodes	6	5	4	3
Validation Value	0.73	0.68	0.80	1

The results in Table 7 show that the final trusted decision can be reached by electing the watchdog nodes that have the highest reputations instead of using all CH voters to be watchdog nodes, since all the validation values are greater than 0.5. This means that even with less number of watchdog nodes, head N_{15} was detected as selfish because including the reputation is giving higher impact to more trusted nodes on the final detection result. The watchdog nodes will be motivated by increasing their reputation as shown in Table 9. The reputation increase will be equal to their contribution to the final detection. In example, we calculated the contribution value of watchdog nodes in a subset of the first three highest reputation monitors in Table 8. N_{20} had $reputation = 180$ and the $contribution = 0.42$, so the new reputation will be $180+0.42\times100 = 222$. As a result, this analysis show that the performance of the detection model will be more efficient in terms of resource consumption since less number of monitoring nodes are needed for a trusted decision. Thus, there is no need to have all the voters of the head, whereas a subset of the highest reputation nodes will be able to detect any selfish activity.

Table 8: Nodes Contribution Value in a Subset of Three Nodes

Node	N_8	N_{11}	N_{20}
Contribution Value	0.33	0.35	0.42

Table 9: New Reputation Value After Reward

Node	N_8	N_{11}	N_{20}
Old Reputation	150	165	180
New Reputation After distributing the Rewards	183	200	222

4.4 Simulation Results

Matlab-8.0 has been used to simulate the efficiency of our detection model implemented over the clustered-based QOLSR networks simulated in chapter 4. The simulation is divided into two subsections. The first subsection shows the effect of selfish nodes on packet delivery. Second, we present the detection probability of selfish nodes with the existence of selfish nodes and how false alarms of selfish nodes is affected in our model. All our simulation results have a 95% confidence level. The upper and lower bounds are calculated accordingly to make sure that the calculated means of the simulations are within such an interval. The simulation parameters are summarized in Table 3.

4.4.1 Effect of Selfish Nodes on Packet Delivery

Figure 8 presents the affect of selfish nodes on packet delivery. It is obvious that the packet delivery percentage drops to more than half in the presence of selfish nodes in the network. As the percentage of selfish nodes increase, the probability for a packet to reach its destination will decrease because selfish nodes will refuse to forward it.

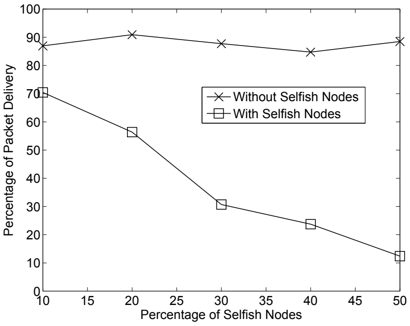

Figure 8: Packet Delivery Percentage

4.4.2 Selfish Nodes Detection Probability

Figures 9 and 10 show the efficiency of the two layer hierarchical cooperative watchdog model in detecting selfish nodes in the network and validate the cooperative game theory analysis conducted in section 4.2. Figure 9 presents the detection probability of selfish nodes, i.e.the number of nodes detected as selfish from total number of selfish nodes monitored, taking subsets of 25%, 50%, and 75% from the total watchdogs in layer one, i.e. the voters of the CH nodes monitoring the CH. The subsets are chosen according to the monitors with highest reputation. The results validate the analysis by showing that not all watchdog nodes monitoring at a specific layer are needed to have a reliable selfish nodes detection, whereas a subset of high reputation watchdog nodes can give a reliable detection. Also, Figure 10 validates the formal cooperative game theory analysis because the false-positive and false-negative detections in our model diminished. This shows that our model is an accurate and efficient one.

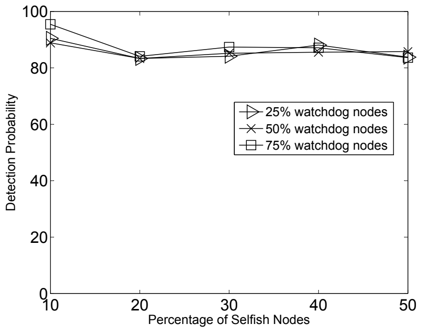

Figure 9: Detection Probability of Selfish Nodes with different percentage of CH voters

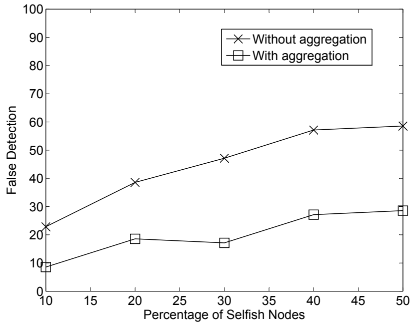

Figure 10: False Detection Percentage of Selfish Nodes-Cooperative vs. Noncooperative Detection Model

In Summary, based on the simulations, we show that selfish nodes have a serious negative effect on packet delivery. As a result, the network becomes unreliable and an efficient detection model is needed. The detection model that is based on the hierarchical cooperative watchdog concept show good results regarding the detection of selfish nodes. Therefore, we are able to show that adding reputation to avoid security problems does not have a negative influence on the QoS of the network, yet it decreased the false detection of selfish nodes by approximately 50% since the watchdog node with the highest reputation has the highest contribution on the final destination.

4.5 Conclusion

The results show that if 50% of the nodes are selfish, the packet delivery percentage drops to 10%. All experimental results are done on the mobile cluster-based QOLSR models. We present a novel efficient detection model that detects nodes behaving selfishly after selection basing the final decision of the detection on a weighted decision where the most trusted node has the leading contribution. Incentives are granted to watchdogs based on their final contribution and calculated based on Shapley value. The cooperative game analysis of the proposed watchdog model and simulation results show that not all watchdog nodes are needed for a truthful detection, only a subset of monitors at each layer having the highest reputation; thus saving the resources of the network nodes. Also, the novel detection model is reliable and show approximately 50% drop in the false detection of selfish nodes.

Chapter 5

Conclusion

Mobile ad hoc networks are widely used for multimedia application. The main objective is to provide the best quality of service and a secure communication. Therefore, we proposed a clustering model that considers the QoS parameters while electing MPRs. Network nodes cooperatively select a set of heads to serve as MPRs. Once the head nodes are elected and consequently clusters are formed, the elected nodes will cooperatively select the set of MPRs that can connect these clusters. In literature, clustering in OLSR was addressed as a solution for prolonging the network lifetime, by reducing the percentage of MPRs, where clusters are formed and then MPRs are selected according to their private information such as residual energy or connectivity index (valency) [14, 28]. Note that all the proposed models assume the presence of clustering models that can cluster the network and then the MPRs are selected. While in our model, the heads are selected cooperatively and then the heads will select the MPRs that can connect the heads with each others (1-hop, 2-hop and 3-hop away). This model reduced the number of MPR nodes by 30% which lead to prolonging the network lifetime. Since, nodes can behave selfishly while electing MPR nodes to save their energy, a new model was proposed that considers the nodes reputation as one of the QoS metrics. This will motivate the nodes to be selected as MPRs. Simulation results proved that including reputation in the QoS metrics does not affect the quality of service in the network. Then, a detection model based on watchdog concept was implemented over Mobile QOLSR networks to detect selfish nodes. Simulation results showed a decrease of 50% in false detection compared to other models. The formal analysis showed that watchdogs with higher reputation have higher contribution in the detection of selfish nodes which makes our model very efficient.

In summary, the main contributions of our thesis are:

1. Building a novel cluster-based QoS-OLSR approach.
2. Improving the trustworthiness of the network by selecting the most trusted MPR nodes.
3. Detecting cooperatively selfish nodes after the election/selection process based on the Hierarchical Cooperative Watchdog model.
4. Building a more efficient detection model by using less number of watchdog

For further work, we will consider a punishment system that will punish detected selfish nodes and malicious watchdog nodes that give false detection.

The following is the list of journal articles submissions derived from the thesis work:

- “A Cluster-Based Model for QoS-OLSR Protocol”, to the conference of Wireless Communications and Mobile Computing , IEEE, 2011

- “Reputation-Based Cooperative Detection Model of Selfish Nodes in Cluster-based QoS-OLSR Protocol”, to the journal of Wireless Personal Communications, Springer, 2014

Bibliography

[1] A. Adnane, C. Bidan, and R. T. de Sousa Jr., “Validation of the OLSR Routing Table based on Trust Reasoning”, In *Proc. of the International Workshop on Trust in Mobile Environments*, 1–12, 2008.

[2] A. Adnane, R. T. de Sousa Jr, C. Bidan, and L. Mé, “Autonomic Trust Reasoning Enables Misbehavior Detection in OLSR”, In *Proc. of ACM Symposium on Applied Computing*, 2006–2013, 2008

[3] A. Benslimane, R. El Khoury, R. El Azouzi, and S. Pierre, “Energy Power-Aware Routing in OLSR Protocol”, In *Proc. of the 1st Mobile Computing and Wireless Communication International Conference (MCWC)*, 14–19, 2006.

[4] A. Chriqi, H. Otrok, and J-M. Robert, “SC-OLSR: Secure Clustering-Based OLSR Model for Ad hoc Networks”, In *Proc. of* 5^{th} *IEEE International conference on Wireless and Mobile Computing, Networking and Communications*, 2009.

[5] A. Laouti, P. Muhlethaler, A. Najid, and E. Plakoo, “Simulation Results of the OLSR Routing Protocol for Wireless Network”, In *Proc. of the 1st IFIP Mediterranean Ad-Hoc Networks workshop*, 2002.

[6] A. Mas-Colell, M. Whinston, and J. Green, “Microeconomic Theory”, In *Oxford University Press*, 1995.

[7] A.E. Roth, “The Shapley Value: Essays in the Honor of Lloyd S.Shapley”, In *Cambridge University Press*, 1988.

[8] B. Mans and N. Shrestha, “Performance Evaluation of Approximation Algorithms for Multipoint Relay Selection”, In *Proc. of the 3rd IFIP Annual Mediterranean Ad-Hoc Network Workshop*, pages 480–491, 2004.

[9] C. Adjih, T. H. Clausen, A. Laouiti, P. Muhlethaler, and D. Raffo, “Securing the OLSR Routing Protocol with or without Compromised Nodes in the Network”, In *INRIA*, 2005.

[10] C. Adjih, T. H. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, “Securing the OLSR Protocol”, In *Proc. of the 2nd IFIP Annual Mediterranean Ad Hoc Networking Workshop*, 1–10, 2003.

[11] C. Bettstetter, H. Hartenstein, and X. Perez-Costa, “Stochastic Properties of the Random Waypoint Mobility Model”, In *ACM/Kluwer Wireless Networks, Special Issue on Modeling and Analysis of Mobile Networks.*,2003.

[12] E. Baccelli, “OLSR Trees: A Simple Clustering Mechanism for OLSR”, In *Proc. of the 4th IFIP Annual Mediterranean Ad Hoc Networking Conference*, pages 265–274, 2005.

[13] F. De Rango, M. Fotino, and S. Marano, “EE-OLSR: Energy Efficient OLSR Routing Protocol for Mobile Ad Hoc Networks”, In *Proc. of the Military Communications Conference (MILCOM)*, 1–7, 2008.

[14] F. J. Ros and P. M. Ruiz, “Cluster-based OLSR Extensions to Reduce Control Overhead in Mobile Ad Hoc Networks”, In *Proc. of the 2007 International Conference on Wireless Communications and Mobile Computing (IWCMC)*, 202–207, 2007.

[15] F. Wang, Y. Mo, and B. Huang, “COSR: Cooperative on Demand Secure Route Protocol in MANET”, In *Proc. of IEEE ISCIT, China*, pages 890–893, 2006.

[16] H. Badis and K. Al Agha, “QOLSR, QoS routing for ad hoc wireless networks using OLSR”, In *EUROPEAN TRANSACTIONS ON TELECOMMUNICATIONS*, 16:427–442, 2005.

[17] H. Lin, J. Hu, J. Ma, L. Xu, and A. Nagar, “A Role Based Privacy-Aware Secure Routing Protocol for Wireless Mesh Networks”, In *Springer Wireless Personal Communications*, 2013.

[18] H. Otrok, A. Mourad, JM Robert, N. Moati, and H. Sanadiki, “A Cluster-Based Model for QoS-OLSR Protocol”, In *Proc. of IEEE Wireless Communications & Networking Conference (WCNC)*, pages 1–6, 2010.

[19] H. Otrok, M. Debbabi, C. Assi, and P. Bhattacharya, “A Cooperative Approach for Analyzing Intrusions in Mobile Ad hoc Networks”, In *Proc. of 27th International Conference on Distributed Computing Systems Workshops*, 2007.

[20] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and P. Bhattacharya, “A Game-Theoretic Intrusion Detection Model for Mobile Ad-hoc Networks”, In *Computer Communications*, 31:708–721, 2008.

[21] I. Michiardi and R. Molva, “CORE: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks”, In *Proc. of IFIP CMS02, Communication and Multimedia Security Conference*, September 2002.

[22] J. C. Harsanyi, “A general theory of rational behavior in game situations”, In *Econometrica*, 34:613–634, 1966.

[23] J. M. Robert, H. Otrok, A. N. Quttoum, and R. Boukhris, (2012). *“A distributed resource management model for virtual private networks: Tit-for-Tat strategies”*, [Online]. 56(2), pp. 927-939. Available: `http://dx.doi.org/10.1016/j.comnet.2011.11.013`

[24] J.M. Robert, H. Otrok, and A. Chriqi, “RBC-OLSR: Reputation-based clustering OLSR protocol for wireless ad hoc networks”, In *Journal Computer Communication*, 35:488–499, 2012.

[25] K. Chen and K. Nahrstedt, “iPass: an Incentive Compatible Auction Scheme to Enable Packet Forwarding Service in MANET”, In *Proc. of the 24th International Conference on Distributed Computing Systems (ICDCS)*, 534–542, 2004.

[26] L. Anderegg and S. Eidenbenz, “Ad hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents”, In *Proc. of the ACM*

9th Annual International Conference on Mobile Computing and Networking (MobiCom), 2003.

[27] L. Canourgues, J. Lephayand, L. Soyer, and A.-L. Beylot, "A Scalable Adaptation of the OLSR Protocol for Large Clustered Mobile Ad hoc Networks", In *In Proc. of the 7th IFIP Annual Mediterranean Ad Hoc Networking Conference*, pages 97–108, 2008.

[28] L. Villasenor-Gonzalez, G. Y. Ge, and L. Lament, "HOLSR: a Hierarchical Proactive Pouting Mechanism for Mobile Ad Hoc Networks", In *IEEE Communications Magazine*, 43:118–125, 2005.

[29] L. -H. Yen, C. W. Yu, and Y. -M. Cheng, "Expected k-coverage in wireless sensor networks", In *Ad Hoc Networks*, 4:636–650, 2006.

[30] M. Hollick, J. Schmitt, and C. seipl, "On the Effect of Node Misbehaviour in Ad hoc Network", In *Proc. IEEE Conference on Communication*, 6:3759–3763, 2004.

[31] N. Komninos, D. Vergados, and C. Douligeris, "Detecting unauthorized and compromised nodes in mobile ad hoc networks", In *Ad hoc Networks-Elsevier*, 5:289–298, 2007.

[32] N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya, "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", In *IEEE Transactions on Dependable and Secure Computing*, 8:89–103, 2011.

[33] N. Nisan, "Introduction to Mechanism Design for Computer Scientists", In *Algorithmic Game Theory*, 209–242, 2007.

[34] P. Krishna, N. H. Vaidya, M. Chatterjee, and D. K. Pradhan, “A Cluster-based Approach for Routing in Dynamic Networks”, In *Proceedings of the ACM SIGCOMM Computer Communication Review*, 49–64, 1997.

[35] P. Michiardi and R. Molva, “Analysis of Coalition Formation and Cooperation Strategies in Mobile Adhoc Networks”, In *Ad hoc Networks*, 3:193–219, 2005.

[36] Q. He, D. Wu, and P. Khosla, “SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks”, In *IEEE INFOCOM, San Francisco, CA, USA*, 2:825–830, 2004.

[37] R. Carruthers and I. Nikolaidis, “Certain Limitations of Reputation-based Schemes in Mobile Environments”, In *Proc. of ACM Symposium on Applied Computing*, pages 2–11, 2005.

[38] S. Buchegger and JY Le Boudec, “Analysis of the CONFIDANT Protocol:Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks”, In *Proc. of the 2nd IFIP Annual Mediterranean Ad Hoc Networking Workshop*, pages 1–10, 2003.

[39] S. Mahfoudh and P. Minet, “A Comparative Study of Energy Efficient Routing trategies based on OLSR”, In *Proc. of the 22nd International Conference on Advanced Information Networking and Applications*, pages 1253–1259, 2007.

[40] S. Marti, T.J. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”, In *Proc. of ACM Symposium on Applied Computing*, pages 103–106, 2000.

[41] S. Vuppala, A. Bandyopadhyay, P. Choudhury, and T. De, “A Simulation Analysis of Node Selfishness in MANET using NS-3”, In *Int. J. of Recent Trends in Engineering and Technology*, 1:103–106, 2010.

[42] S. Zhong, J. Chen, and Y. Yang, “Sprite: a simple, cheat-proof, creditbased system for mobile ad-hoc networks”, In *Proc. of IEEE INFOCOM, San Francisco, CA, USA*, 3:1987–1997, 2003.

[43] T. Camp, J. Boleng, and V. Davies, “A Survey of Mobility Models for Ad Hoc Network Research”, In *Wireless Communication & Mobile Computing*, 2:483–502, 2002.

[44] T. Clausen and P. Jacquet, “Optimized Link State Routing Protocol (OLSR)”, In *Internet Engineering Task Force*, October 2003.

[45] T. Kunz. “Energy-Efficient Variations of OLSR”, In *Proc. of the International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 517–522, 2008.

[46] Z. Li and H. Shen, “Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks”, In *IEEE Transactions on Mobile Computing*, 11:1287–1303, 2012.