Noname manuscript No.
(will be inserted by the editor)

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

Nadia Moati, Hadi Otrok, Azzam Mourad, Jean-Marc Robert

Received: date / Accepted: date

Abstract The QOLSR is a multimedia protocol that was designed on top of the Optimized Link State Routing (OLSR) protocol for Mobile Ad hoc Network. It considers the Quality of Service (QoS) of the nodes during the selection of the Multi-Point Relay (MPRs) nodes. One of the drawbacks of this protocol is the presence of selfish nodes that degrade the network lifetime. The limited energy and resources, and the absence of any motivation mechanism cause mobile nodes to behave selfishly during the MPRs selection. A new MPR selection based on cluster head election was proposed in previous work to increase network lifetime [22]. In this paper, 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 nodes. Moreover, 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 decision. Simulation results show that the novel cluster-based QoS-OLSR model can give incentive to nodes to behave 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 · Selfish Nodes · Reputation · Watchdog

Nadia Moati
Department of Computer Science and Mathematics,
Lebanese American University (LAU), Beirut, Lebanon
E-mail: nadia.moati@lau.edu

Hadi Otrok
Department of ECE, Khalifa University of Science, Technology & Research, Abu Dhabi, UAE
E-mail: Hadi.Otrok@kustar.ac.ae

Azzam Mourad
Department of Computer Science and Mathematics,
Lebanese American University (LAU), Beirut, Lebanon
E-mail: azzam.mourad@lau.edu.lb

Jean-Marc Robert
Département de génie logiciel et des TI,
École de technologie supérieure, Montréal, QC, Canada
E-mail: Zbigniew.Dziong@etsmtl.ca

1 Introduction

An ad hoc network is an infrastructureless network characterized by its dynamic topology, limited bandwidth, limited physical security and limited energy resources. The *Optimized Link State Routing* (OLSR) protocol [6] is a proactive routing protocol designed for mobile ad hoc networks. It relies on a set of designated nodes to broadcast the network topology information and to forward traffic flows towards their destination. These nodes are known as the *MultiPoint Relay* (MPR) nodes. Based on the OLSR protocol, the Quality of Service (QoS) OLSR protocol, known as QOLSR [2], was proposed in the literature to consider the nodes' available bandwidth during the selection of MPR nodes and routing paths. It was designed to handle multimedia applications over ad hoc networks. Thus, the bandwidth and

delay metrics are important to ensure QoS and must be considered during the MPR selection. The QOLSR protocol has a main limitation that can ultimately jeopardize the ultimate goal of prolonging network life time. It selects a large number of MPR nodes due to the fact that every node selects independently its own set of MPR nodes. Such a problem can affect nodes' available bandwidth and increase the probability of channel collision, especially in dense networks [9]. The clustered-based QOLSR [22] was proposed to address the main limitation of QOLSR. This new routing protocol prolongs the network lifetime and therefore improves the overall Quality of Service of the network.

In this paper, we address two limitations of the cluster-based QOLSR protocol. 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. 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 to increase accordingly. Thus, adding reputation to the already existing selection process metrics, connectivity, residual energy and bandwidth, will help in selecting more trusted nodes.

The other limitation raises 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. To address this limitation, we propose a novel mechanism relying on a hierarchical cooperative watchdog model to detect any selfish behavior in the network. The nodes that have voted for a CH node should monitor (first layer of the hierarchy). As a second layer, the cluster heads should monitor the MPR nodes they have selected. This mechanism should be collaborative since the final monitoring decision should not be based on just one node, whereas on a weighted decision of all individual decisions. To motivate the watchdogs to run their monitors and cooperate with each other, incentives are given and computed based on cooperative game theory since the decision was made cooperatively. Specifically, shapley value is used to compute the contribution of each watchdog in the final decision and according to this contribution an incentive will be given.

To validate our solution, simulations are conducted to evaluate the (i) impact of selfish nodes on the network performance and (ii) impact of the proposed QoS metric models compared with the classical models and (iii) efficiency of the hierarchical watchdog model. In summary, our contributions is the following:

- Motivate nodes to behave normally during the election/selection process by giving incentives in the form of reputation based on the VCG mechanism.
- Select the most trusted MPR nodes without sacrificing in network lifetime and increasing delay by considering nodes reputation.
- Detect cooperatively selfish nodes after the election/selection process based on the Hierarchical Cooperative Watchdog model. This should decrease false positive and negative alarms and increase the detection.
- Motivate nodes to act as a watchdog nodes by rewarding them according to their contribution value in the final detection.
- Analyze the impact of having less number of watchdogs on the final decision.

The rest of the paper is organized as follows. Section 2 reviews the related work. Section 3 presents the problem statement and why nodes misbehave. Section 4 describes the novel model based on the Clustered-based QoS-OLSR Network. Section 5 presents the detection model based on the Hierarchical Cooperative Watchdog. Section 6 presents an incentive model and a formal analysis of the detection model. Then, Section 7 presents empirical results. Finally, Section 8 concludes the paper.

2 Related Work

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, a 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.

2.1 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 [23] 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 to use game-theoretic approaches to design a secure solution to incite selfish nodes to participate to the collaborative effort.

2.2 Reputation-based Mechanisms

In ad hoc networks, reputation is used to indicate the behavior of the nodes in the network. By direct or indirect observations of a node's 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.

Watchdog and Pathrater [14] 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 [16] 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 other's reputation. Thus, CORE is vulnerable to fake positive ratings.

CONFIDANT protocol [19] also uses reputation to detect selfish nodes. CONFIDANT has four components: the monitor, the reputation manager, the path rater and the 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.

SORI [25] 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, and actions are taken against selfish nodes.

Cooperative on Demand Secure Routing (COSR) protocol [24] 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. Recommendation is other nodes' subjective recommendation. COSR has proven well with selfish nodes, 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 novel model proposed is built over QOLSR protocol, where selfish nodes are detected cooperatively to decrease the false detection.

Moreover, RPASRP [31] 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 relies on the hybrid usage of dynamic reputation mechanism built by subject logic and uncertainty, role based multi-level security technology, hierarchical key management protocol and Merkle Tree technology. RPASRP can provide scalable security services to assure the authenticity, integrity and secrecy of routing packets and defend against certain internal attacks caused by compromised mesh routers. This model showed that it is secure, privacy preserving and efficient. RPASRP 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 [30] that overcome the drawbacks of the reputation system and price-based system which are the two main 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.

3 Problem Statement: Behaviour of Selfish Nodes

To save its own energy and be able to process its own packets without latency, a selfish node tends to avoid participating in the routing and the packet forwarding processes. 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 [14]:

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.

Selfish nodes can severely degrade network performance and eventually partition the network.

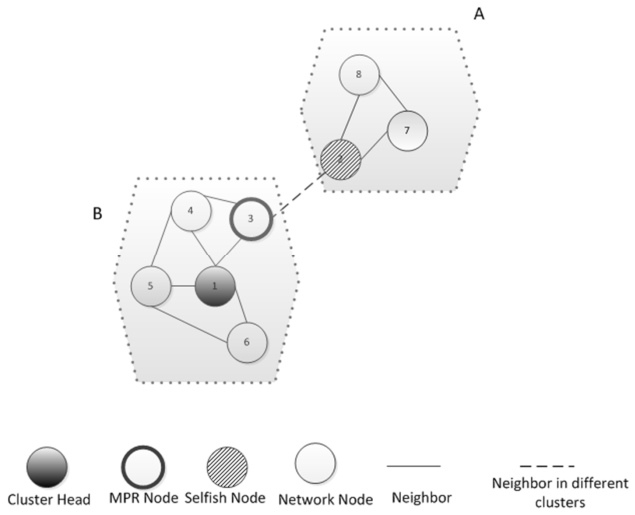

Fig. 1 Ad hoc Network With Selfish Node

Consider the example presented in Fig. 1. Assume that N_2, which has accepted to play the role of 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.

4 Reputation-Based QOLSR Routing Protocol

In this section, 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 election algorithm which elects a set of cluster heads. These elected cluster heads then select a set of the MPR nodes which assure that the network is connected[22].

4.1 The Quality of Service Metric Models

To rely on nodes which are more trustworthy, while keeping the same performance and quality of service, we propose to include the node's 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.

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

1 Reputation Bandwidth - OLSR Model (RB-OLSR)
$QoS(i) = BW(i) + \frac{R(i)}{\sum R(i)}$

2 Reputation Proportional Bandwidth OLSR Model (RPB-OLSR)
$QoS(i) = \frac{BW(i)}{N(i)} + \frac{R(i)}{\sum R(i)}$

3 Reputation Bandwidth & Energy OLSR Model (RBE-OLSR)
$QoS(i) = BW(i) \times RE(i) + \frac{R(i)}{\sum R(i)}$

4 Reputation Proportional Bandwidth & Energy OLSR Model (RPBE-OLSR)
$QoS(i) = \frac{BW(i) \times RE(i)}{N(i)} + \frac{R(i)}{\sum R(i)}$

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

As shown in [2], QOLSR uses the simple $QoS(i) = BW(i)$ metric model. In this paper, this is referred simply as the Classical QOLSR protocol. 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.

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[29].

Once the cluster heads have been elected, they have to select the relay nodes to interconnect them[5]. Thus, a pair of CH nodes which are two-hop away would have to select the best MPR node according to the selected QoS metric. Each of them will have to pay the selected MPR node. This is shown in the Two-hop away MPR Payment algorithm.

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.

$P(k) = QoS(i) - \max\{QoS(j) | j \in N_1(k) \bigcap N_1(l) \backslash \{i\}\}$
$P(l) = QoS(i) - \max\{QoS(j) | j \in N_1(k) \bigcap N_1(l) \backslash \{i\}\}$
$R(i) = R(i) + P(k) + P(l)$.

A pair of CH nodes which are three-hop away would have to select the best chain of two MPR nodes interconnecting them [5]. This pair of MPR nodes corresponds to the path maximizing the minimum of the selected QoS metric value. Each CH node will have to pay its selected neighbor serving as MPR node. This is shown in the Three-hop away MPR Payment algorithm.

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.

1 $P(k) = \min(QoS(i), QoS(j)) - \min(QoS(i^*), QoS(j^*))$
2 $R(i) = R(i) + P(k)$
3 $R(j) = R(j) + P(k)$

Table 1 Quality of Service QoS Metric using the Reputation Proportional BE-OLSR Model

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

4.2 Illustrative Example

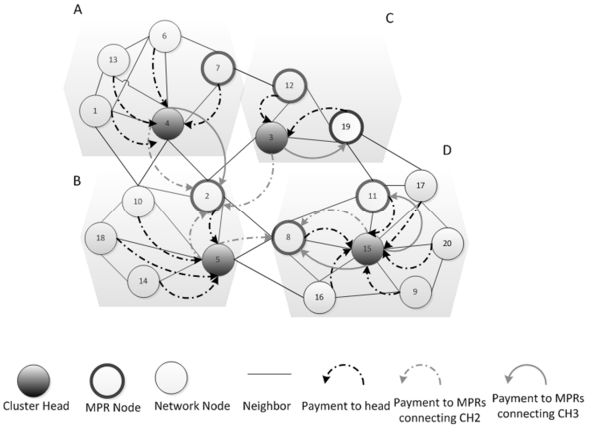

Fig. 2 Reputation Mechanism example

To illustrate the payment mechanism, the example presented in Fig. 2 shows a network where the CH and MPR nodes are selected[22] 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 $R(N_{11}) = R(N_{11}) + P(N_{15})$.

5 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[26]. 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 accusing falsely 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 fi-

nal decision. The Hierarchical Cooperative Watchdog algorithm presents the detection mechanism.

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
1   p has to be transmitted by N_i.
2   Add p to a time-based data structure T.
    if p *has been transmitted by* N_i **then**
3   Remove p from T.
4   N_i is normal.
    else
      if p *is still in* T *after some timer* Δ **then**
5   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 determine 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. 2.

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

$$F(W_i, N_i) = \frac{\sum_{w_j \in W_i} R(w) \times f(w_j, N_i)}{\sum R(w)} \quad (2)$$

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.

Assume node S wants to send a packet to node D as illustrated in Figure 3. 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 selfoshly 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.

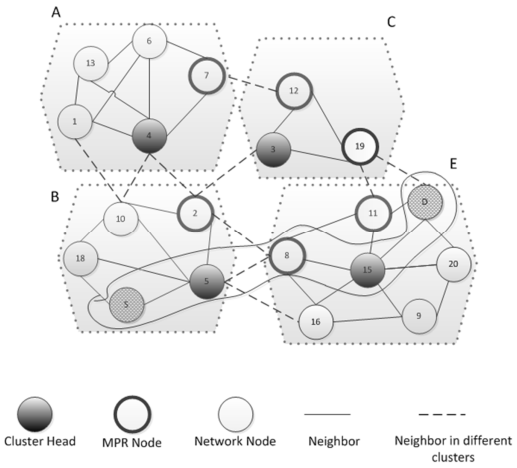

Fig. 3 Hierarchical Cooperative Watchdog Mechanism example

6 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:

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

$$f(x) = \begin{cases} 1 & x \text{ detect } N_i \text{ as selfish} \\ 0 & x \text{ detect } N_i \text{ as normal} \end{cases} \quad (3)$$

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 2 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's 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[33] will be used to present the marginal contribution of each player in the game with respect to a uniform distribution over the set of all permutations on the set of 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.

$$\phi_{N_i}(\Delta) = \frac{1}{\delta} \sum_{\pi \in \prod_{\Delta}} F(P_{\pi}^{N_i} \cup N_i) - F(P_{\pi}^{N_i}) \quad (4)$$

Referring to example 3, where the CH node N_{15} is monitored, Shapley value is used to measure the contribution of each potential watchdog nodes. Table 2 represents the reputation of each watchdog monitoring head N_{15}.

Using equation 4, we calculate the contribution value of each node that will be used to reward each watchdog.

Table 2 NODES' REPUTATION

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

Table 3 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 2. Table 4 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 4 NODES' Validation Value

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

The results in Table 4 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 6. 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 5. N_{20} had $reputation = 180$ and the $contribution = 0.42$, so the new reputation will be $180 + 0.42 \times 100 = 222$. 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 5 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 6 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

7 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 node's 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 [27], a very popular and widely used mobility model is implemented in Matlab to simulate our results. This mobility model is a simple and straightforward stochastic model that was used to demonstrate the movement of the nodes in our network. The node randomly chooses a destination point in the area and moves with a constant speed and on a straight line to the destination. After waiting a pause time, it chooses a new destination and speed, then moves with constant speed to this destination. 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 [32]. The simulation is divided into five 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. Then, we show the effect of selfish nodes on packet delivery. Finally, we present the detection probability of selfish nodes in the presence 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 interval. The simulation parameters are summarized in Table 7.

Table 7 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% $confidence\ level$)

7.1 Percentage of MPR nodes in the Network

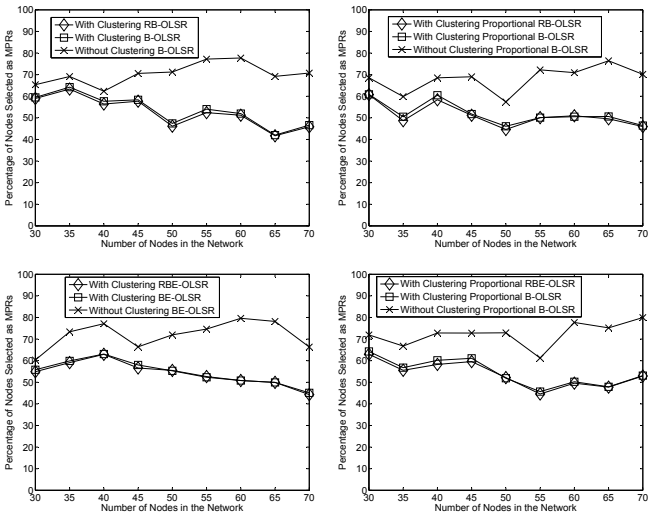

Fig. 4 Percentage of MPR Nodes: (a) B-OLSR (b) Proportional B-OLSR (c) BE-OLSR (d) Proportional BE-OLSR

In Fig 4, the cluster-based models significantly reduce the number of selected MPR nodes. These relay nodes include the cluster heads which act as specialized MPR nodes. It is obvious that the reputation cluster-based models has approximately the same percentages of MPR nodes; that means that including reputation as one of the QoS metrics does not increase the number of nodes selected as MPRs. 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.

7.2 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.
- Energy per Packet.

In Fig 5, we show the percentage of alive nodes and how the energy drain 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 5. This will be done by finding the total number of packets the node i will transfer. This value is obtained 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 5). The residual energy is decreased by the value of Energy consumption. (refer to equation 6)

$$EN(i) = (BW(i) \ / \ Packet\ size) \times Energy\ per\ Packet\ J \tag{5}$$

$$New\ RE(i) = RE(i) \ - \ EN(i)\ J \tag{6}$$

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

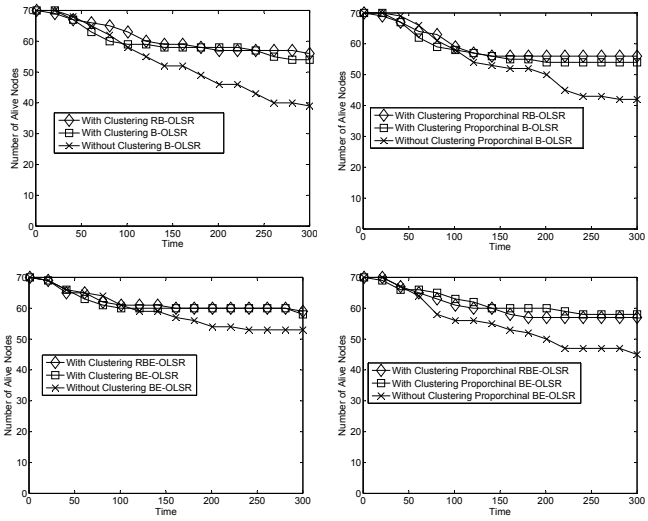

Fig. 5 Percentage of alive nodes over time: (a) B-OLSR (b) Proportional B-OLSR (c) BE-OLSR (d) Proportional BE-OLSR

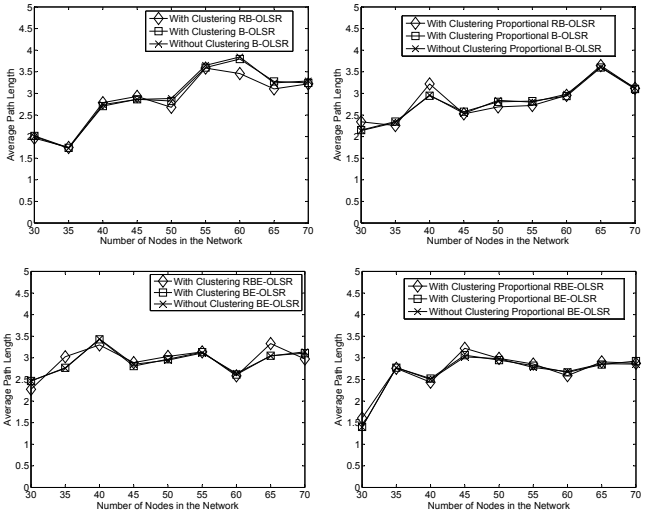

Fig. 6 Average Path Length: (a) B-OLSR (b) Proportional B-OLSR (c) BE-OLSR (d) Proportional BE-OLSR

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.

7.3 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 8 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.

Table 8 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%

7.4 Effect of Selfish Nodes on Packet Delivery

Figure 7 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.

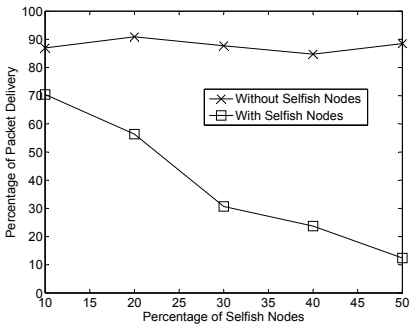

Fig. 7 Packet Delivery Percentage

7.5 Selfish Nodes Detection Probability

Figures 8 and 9 show the efficiency of the two layers hierarchical cooperative watchdog model in detecting selfish nodes in the network and validate the cooperative game theory analysis conducted in section 5. Figure 8 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 9 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.

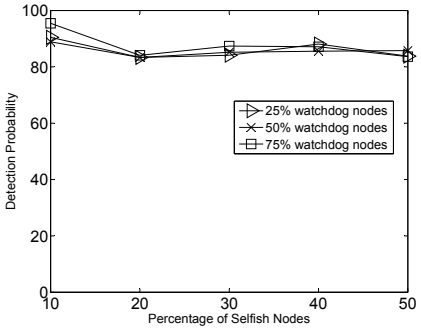

Fig. 8 Detection Probability of Selfish Nodes with different percentage of CH voters

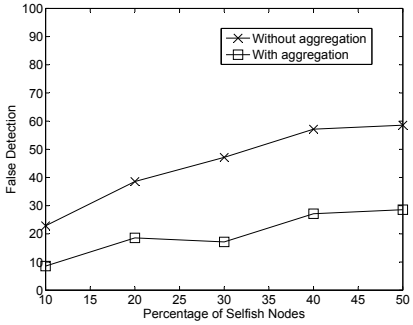

Fig. 9 False Detection Percentage of Selfish Nodes-Cooperative vs. Noncooperative Detection Model

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. On the other hand, 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. Moreover, 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.

8 Conclusion

The scarcity of energy and the difficulty 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. 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 motivation and detection model that (1) motivates nodes during selection to behave normally by increasing their reputation then consider it when selecting MPR nodes and (2) 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. 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. Moreover, 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. For further work, we will consider a punishment system that will punish detected selfish nodes and malicious watchdog nodes that give false detection.

References

1. 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.
2. H. Badis and K. A. Agha. QOLSR, QoS routing for ad hoc wireless networks using OLSR. *European Transactions on Telecommunications*, 16:427–442, 2005.
3. A. Benslimane, R. E. Khoury, R. E. Azouzi, and S. Pierre. Energy Power-Aware Routing in OLSR Protocol. In *Proc. of the 1st Mobile Computing and Wireless Communication International Conference (MCWC)*, pages 14–19, 2006.
4. 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.
5. 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 (WiMob 2009)*, 2009.
6. T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (OLSR). RFC 3626, Internet Engineering Task Force, October 2003.
7. T. Kunz. Energy-Efficient Variations of OLSR. In *Proc. of the International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 517–522, 2008.
8. 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.
9. 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.
10. F. D. 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)*, pages 1–7, 2008.
11. 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)*, pages 202–207, 2007.
12. L. Villasenor-Gonzalez, G. Y. Ge, and L. Lament. HOLSR: a Hierarchical Proactive Pouting Mechanism for Mobile Ad Hoc Networks. *IEEE Communications Magazine*, 43:118–125, 2005.
13. S. Vuppala and A. Bandyopadhyay and P. Choudhury and T. De. A Simulation Analysis of Node Selfishness in MANET using NS-3. *Int. J. of Recent Trends in Engineering and Technology*, 1:103–106, 2010.
14. S. Marti and T.J. Giuli and 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.
15. R. Carruthers and I. Nikolaidis. Certain Limitations of Reputationbased Schemes in Mobile Environments. In *Proc. of ACM Symposium on Applied Computing*, pages 2–11, 2005.
16. 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.
17. M. Hollick and 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.

18. N. Komninos and D. Vergados and C. Douligeris. Detecting unauthorized and compromised nodes in mobile ad hoc networks. *Ad hoc Networks-Elsevier*, 5:289–298, 2007.
19. 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.
20. S. Bansal and M. Baker. Securing the OLSR Protocol. In *Proc. of the 2nd IFIP Annual Mediterranean Ad Hoc Networking Workshop*, pages 1–10, 2003.
21. S. Bansal and M. Baker. Observation based cooperation enforcement in ad hoc networks. *Technical Report*, pages 1–10, 2003.
22. H. Otrok and A. Mourad and JM Robert and 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.
23. S. Zhong and 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.
24. F. Wang and Y. Mo and B. Huang. COSR: Cooperative on Demand Secure Route Protocol in MANET. In *Proc. of IEEE ISCIT, China*, pages 890–893, 2006.
25. Q. He, D. Wu, P. Khosla. SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks. *IEEE INFOCOM, San Francisco, CA, USA*, 2:825–830, 2004.
26. N. Mohammed and H. Otrok and L. Wang and M. Debbabi and P. Bhattacharya. Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET. *IEEE Transactions on Dependable and Secure Computing*, 8:89–103, 2011.
27. T. Camp and J. Boleng and V. Davies. A Survey of Mobility Models for Ad Hoc Network Research. *Wireless Communication & Mobile Computing*, 2:483–502, 2002.
28. A.E. Roth. The Shapley Value: Essays in the Honor of Lloyd S.Shapley. *Cambridge University Press*, 1988.
29. J.M. Robert and H. Otrok and A. Chriqi RBC-OLSR: Reputation-based clustering OLSR protocol for wireless ad hoc networks. *Journal Computer Communication*, 35:488–499, 2012.
30. Z. Li and H. Shen Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing*, 11:1287–1303, 2012.
31. H. Lin and J. Hu and J. Ma and L. Xu and A. Nagar A Role Based Privacy-Aware Secure Routing Protocol for Wireless Mesh Networks. *Springer Wireless Personal Communications*, 2013.
32. C. Bettstetter and H. Hartenstein and X. PerezCosta. Stochastic Properties of the Random Waypoint Mobility Model. *ACM/Kluwer Wireless Networks, Special Issue on Modeling and Analysis of Mobile Networks.*,2003.
33. H. Otrok and M. Debbabi, and 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.