Detecting Attacks in QoS-OLSR Protocol

Hiba Sanadiki[a], Hadi Otrok[b], Azzam Mourad[a], and Jean-Marc Robert[c]

[a]Department of Computer Science and Mathematics,
Lebanese American University, Beirut, Lebanon
[b]Department of ECE, Khalifa University of Science, Technology & Research, Abu Dhabi, UAE
[c]École de technologie supérieure, Département de génie logiciel et des TI, Montréal, QC, Canada
{hiba.sanadiki, azzam.mourad}@lau.edu.lb, hadi.otrok@kustar.ac.ae, jean-marc.robert@etsmtl.ca

***Abstract*—In this paper, we detect two attacks targeting the QoS-OLSR protocol MANET. The Cluster-based model QoS-OLSR is a multimedia protocol designed on top of Optimized Link State Routing (OLSR) protocol. The quality of service (QoS) of the nodes is considered during the selection of the multipoint relays (MPRs) nodes. In this work, we identify two attacks that can be launched against the QoS-OLSR protocol: Identity spoofing attack, and wormhole attack. Watchdogs are used to detect the attacks performed by malicious nodes. As a solution, we propose to improve the watchdogs' detection by (1) using cooperative watchdog model and (2) adding the posterior belief function using Bayes' rule to the watchdog model. Simulation results show that the use of the Bayes' rule function along with the cooperative watchdog model improves the detection rate and reduces the false positives.**

***Index Terms*—MANET, Identity Spoofing, Wormhole, Posterior Belief, Watchdogs.**

I. Introduction

QoS-OLSR [13] is a multimedia protocol built on top of Optimized Link State Routing (OLSR) protocol. Based on clustering, nodes can cooperatively select a set of leaders that will form the clusters. Once clusters are formed, elected leaders will cooperatively select a set of multipoint relays (MPRs) nodes that can connect these clusters. The quality of service (QoS) of the nodes is considered during the selection of MPRs. The parameters used for the selection were: bandwidth, connectivity index and residual energy. QoS-OLSR clustered-based approach prolongs the network lifetime by reducing the percentage of MPR nodes. Moreover, it motivates selfish nodes to behave normally. It also considers the tradeoff between network lifetime and network QoS. TC messages are used to ensure the fresh-path selection in the network. In QoS-OLSR, head nodes are responsible of exchanging topology information between the clusters, and only MPR nodes are responsible of exchanging TC messages each time the network topology is changed.

In this work, we have identified two types of attacks that can target QoS-OLSR protocol: Identity spoofing and wormhole attacks. In the identity spoofing attack, the attacker sends fake TC messages by spoofing the identity of another node, which will lead to disconnected clusters in the network. In the wormhole attack, a malicious node copies the TC message of an MPR node and sends it to another attacker through the wormhole tunnel which will lead to fake path selection.

To detect the above attacks, we propose the use of watchdogs. To enhance the probability of detection, we propose a solution based on cooperative watchdogs that will monitor malicious activities. The detection decision will be calculated by aggregating all the observations of MPRs taking into consideration nodes' reputation that was introduced in our previous work QoS-OLSR [13]. To improve the detection rate of the watchdogs, Bayes' rule function is added to the monitor that calculates the posterior belief of a node being misbehaving based on observations. Simulation results are conducted to evaluate the performance of adding Bayes' rule function to the cooperative watchdog model. In summary, our contribution is a cooperative watchdog model based on Bayes' rule that can:

- Improve the detection probability.
- Reduce false positives where malicious nodes are mistakenly identified as normal nodes.

II. Related Work

In this section, we categorize the detection techniques according to the type of attack:

Collusion attack: The work in [9] presents a new collusion attack against OLSR. To defend against this attack, the authors propose to modify the existing Hello message to contain the 2-hop neighbors list. Based on this information, a node can detect whether one of its neighbors has been sent a forged Hello message or not. The main drawback of this solution is that false alarms may be triggered when links between nodes break if the nodes are highly mobile. In [10], the authors use the FMS-OLSR (Forced MPR Switching OLSR) algorithm to detect this type of attack. When node ”X” generates a HELLO message, it checks the number of nodes in its MPR set. If the number is 1, it checks its 1-hop neighbor set. If node ”X” has more than one neighbor, it adds the lone MPR to an AvoidanceSet after waiting for the duration of an avoidance delay. The entries are deleted from AvoidanceSet after some determined delay.

Node isolation attack: In the node isolation attack, an MPR node does not generate its TC message to prevent its MPR selectors nodes to be reachable by other nodes in the network. To defend against this attack, authors in [1] propose a countermeasure that consists of two phases: detection phase

[1]This work is supported by CNRS Lebanon, Lebanese American University, Khalifa University of Science, Technology & Research, and NSERC Canada

978-1-4673-2480-9/13/$31.00 ©2013 IEEE

and avoidance phase. In the detection phase each node uses the promiscuous mode to verify whether its MPR node generates its TC message or not. In the second phase, to avoid the impact of this attack, a new field named Request-value was included in the Hello message. In [2], the authors use a trust analysis technique to stop a malicious node from isolating other nodes in the network. This analysis uses HOP-INFORMATION table, 2-hop request and 2-hop reply to check whether the corresponding node is malicious or not. Each node in the network must send a Hello message every specific period of time to prove that they belong to the network. Each node then gets HOP-INFORMATION table which has HELLO message sender and its 2-hop neighbors.

Blackhole attack: The work in [3] presents a defense against the blackhole attack which is done to capture routes. TOGBAD, a centralized topology graph approach, is used to protect the network against this attack. The graph is created and the number of neighbors of a node is calculated. Thus, the number of neighbors of a node is determined in its HELLO messages. Then, the number of neighbors determined in the topology graph is compared to the originator's number of neighbors for each hello message. If there is a significant difference between the two numbers, this triggers an alarm.

Link spoofing attack: A malicious node generates control traffic messages reporting an incorrect set of links. An attacker can either hide valid links or insert non-existing links. In all cases, the network connectivity is disrupted. A security aware OLSR(SA-OLSR) was used in [5] in order to detect link spoofing attack. SA-OLSR approach assures that the message generated by a node is successfully received by all its 2-hop neighbors using acknowledgement message(ACKTC). Thus, if a malicious node "X" sends a TC message to N1 claiming to have link to node N2, Node N1 can check if node N2 is its 2-hop neighbor using the ACKTC message. If node N1 does not receive an ACKTC back from node N2, it will learn that N2 is not its 2-hop neighbor and consider "X" as attacker. Another way of detecting the link spoofing attack is proposed by authors in [6]. This attack is defended by adding two-hop information to a HELLO message. Each node should advertise its two-hop neighbors in order to have knowledge about the whole topology up to three hops and checks if there is a significant discrepancy when the attack occurs.

Identity spoofing attack: The attacking node sends TC message which claim to have another node's identity. In [4], the authors use signature and timestamp schemes to ensure authentication and protection against identity spoofing attack, where a node misbehaves by generating incorrect Hello or TC messages under a false identity. The countermeasure proposed is to let the originator of each control generate an additional security element in the TC message. It is called signature message that is associated with a timestamp to estimate the time when the message was established. When a node receives a TC message with its signature, it processes both.

Advertised Neighbor Sequence Number (ANSN) attack: The attacking node listens to a TC message addressed from a node and record its ANSN. It then sends a TC with a wrong originated address of that node with an ANSN value which is much greater than the recorded one. The work of [7] addresses the ANSN attack. This attack can be detected when the fraudulent TC transmits an ANSN that is much higher than that actual TC message received from the node X. The higher the difference between the two ANSNs, the longer TCs from X are ignored. The malicious node may repeat the attack several times by forging spoofed TC messages with slightly greater ANSN.

Wormhole attack: This attack must be composed of two attackers and a wormhole tunnel. First, the attackers generate a link between them called a wormhole tunnel. Then one attacker receives packets and copies them from its neighbors and sends them to the other attacker through the wormhole tunnel. So after this node receives the packets, it displays them into the network. SA-OLSR has been used to detect the wormhole attack. The work in [5] proposed to calculate the delay between the time a node sends a TC(*Tsent*) and the time the node receives the corresponding ACK*TC*(*Treceived*). The difference between *Treceived* and *Tsent* must be less then a threshold value in order to consider the node as normal node; else, the node will be considered as malicious. Moreover, authors on [8] have defended the wormhole attack where a node sends probe packets to measure their travel time, from which it can compute the travel distance. If this distance is greater than the transmission range, the message may have tunneled through the wormhole.

III. Security Attacks in a QoS-OLSR Network

In this section, we will first present the QoS-OLSR network through an illustrative example in order to present the attacks. Then, we will describe the elements of QoS-OLSR required for the purpose of investigating security issues. In addition, we will identify the attacks that can affect our model, the clustered QoS-OLSR, and we will provide a scenario that shows how each attack is launched.

A. Illustrative Example: QoS-OLSR

Figure 1 shows a network of 20 nodes where the QoS-OLSR protocol is used to select the leaders with the best QoS using Table 1. After receiving the Hello messages from its neighbors, a node votes for its neighbor with the maximal Quality of Service(QoS) Metric value. Nodes 3, 4, 5, and 15 were elected as head nodes.

TABLE I
THE QUALITY OF SERVICE METRIC USING THE HYBRID QoS-OLSR MODEL

Node	$n1$	$n2$	$n3$	$n4$	$n5$	$n6$	$n7$	$n8$	$n9$	$n10$
QoS Metric	370.8	297.3	500.2	479.4	320.1	338.7	231.1	220.4	205.6	246.4
Node	$n11$	$n12$	$n13$	$n14$	$n15$	$n16$	$n17$	$n18$	$n19$	$n20$
QoS Metric	250.6	193.1	127.2	159.9	398.9	109.9	101.5	89.3	96.2	117.7

Once the cluster heads are elected, they in turn select the MPR nodes that connect all heads together. Node 15 in cluster D is considered to illustrate the example where the first step is to find the neighbor cluster heads for node 15.

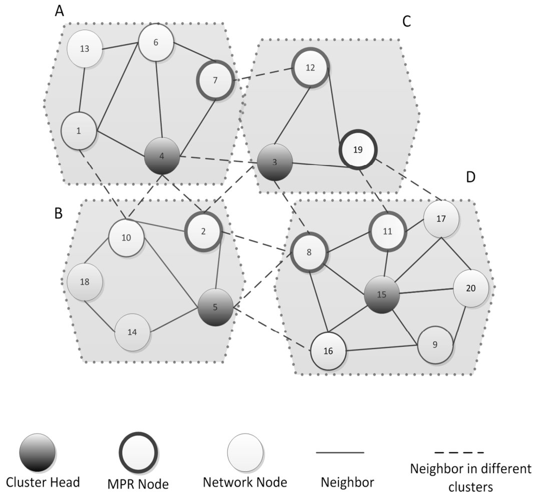

Fig. 1. Network example

The 1-hop cluster head, CH1, the 2-hop cluster head, CH2, and the 3-hop cluster head, CH3 were found. 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, similarly CH3(15)=3 and CH3(15)=4. The second step was 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 node 8 was chosen as the MPR node since it has a better QoS Metric value than node 16. The third step was to find the optimal path for the 3-hop cluster heads. There are two choices to connect head node 15 with head node 3, either {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, by symmetry, head node 3 would select node 19 as an MPR node. Similarly, the optimal path {node 8, node 3} to cluster head node 4 was found.

B. Identifying the Attacks

We will start by describing the messages that are generated in the network.

- Hello Message: The Hello messages are broadcasted periodically, each time the network is created and the nodes change places. These messages are used to obtain information about the node's neighbors. A Hello message performs the task of neighbor sensing and MPR selection process. A node's Hello message contains its own address, a list of its 1-hop neighbors and a list of its MPR set. Thus, by exchanging Hello messages, each node will be able to obtain the information about its 1-hop and 2-hops neighbors and will find out which node has chosen it as an MPR.
- TC Message: In order to disseminate the topology information, the MPR nodes must generate a TC message periodically. The TC messages are intended to be flooded throughout the network and only MPR nodes are allowed to forward TC messages. A TC message contains a set of bi-directional links between a node and a subset of its neighbors. TC messages are diffused to the whole network, employing the MPR optimization technique described below.

Now, we will identify the two attacks that can be launched against QoS-OLSR. The malicious node can perform the attack by including false information in its messages. This node does not want to be selected as a cluster head node in order to not be watched by other nodes. Thus, cluster head nodes are considered as trusted nodes. Attacks may be launched by normal nodes or by MPR nodes.

1) Attacks Launched by Normal Nodes: A node should be an MPR node in order to forward TC messages to other nodes in the network. A normal node can spoof the identity of an MPR node in order to launch some attacks.

Identity spoofing attack: This attack can be performed by a normal node that will send TC messages claiming to have an MPR node's identity. In figure 1, consider that node 16 sends TC messages, claiming to have the identity of another node (node 12). The node claims incorrect links to the network. Nodes 15 and 5 will announce reachability to node 12 through their TC messages.

Wormhole attack: A normal node can also copy the message of an MPR node and send it to another attacker through the wormhole tunnel in order to launch the wormhole attack. Consider in figure 1 that node 15 broadcasts its Hello message. Then, node 17 (the first attacker) copies this message and sends it to node 19 through the vortex built. Node 19 receives the message and replays it.

2) Attacks Launched by MPR Nodes: MPR nodes can also launch the above two attacks.

Identity spoofing attack: This attack can also be performed by an MPR node that will send TC messages claiming to have the identity of another MPR node.

In figure 1, consider that node 8 sends TC messages, claiming to have the identity of another MPR node(node 12).The node claims incorrect links to the network. Nodes 15, 5, 11, and 2 will announce reachability to node 12 through their TC messages.

Wormhole attack: An MPR node can also copy the message of another MPR node and send it to the second attacker through the wormhole tunnel in order to launch the wormhole attack. Consider in figure 2 that node 15 broadcasts its Hello message. Then, node 11 (the first attacker) copies this message and sends it to node 19 through the vortex built. Node 19 receives the message and replays it.

When node 3 receives the message replayed, node 3 considers node 15 as a 1-hop neighbor. After a while, a symmetrical relationship can be established between nodes 15 and 3. Once this link is established, nodes 15 and 3 are very likely to choose each other as MPRs, which then leads to

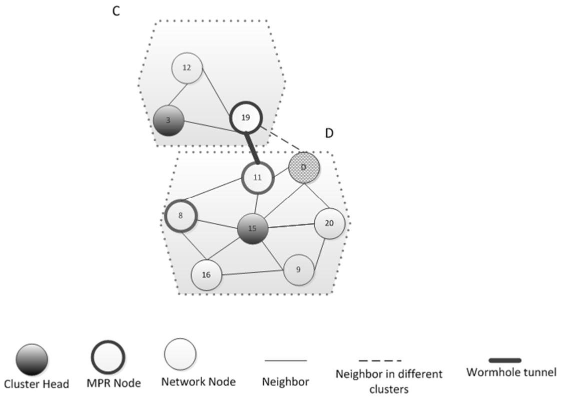

Fig. 2. Wormhole Attack

an exchange of some TC messages and data packets through the wormhole tunnel.This lead to a transmission of erroneous information, disruption of routing and loss of connectivity between clusters.

Malicious nodes, normal or MPR nodes, can severely degrade the network performance by isolating some head nodes and clusters, since communication between nodes depends on TC messages exchanged. Thus, spoofing attack will lead to disconnected clusters. A disconnected network will yield to a decrease in the network lifetime leading to more delay in the network. In addition wormhole attack can create false links in the network leading to false path selection.

IV. Cooperative Detection Model

We will first present how the watchdog detection is working. Second, we will show how this detection is improved using Bayes' rule function added to the cooperative watchdog model.

A. How watchdog is working

1) Identity spoofing attack: We will consider 3 cases where a malicious node launches the identity spoofing attack. In our new model, each node saves its 1-hop neighbors' list in order to identify its neighbors. Thus, as we can see in the scenarios below, the watchdog will decide whether the node is misbehaving or not by comparing the information it receives with its neighbors' list.

- Scenario 1: Consider that node 16 forwards its TC message to a node in the network claiming to have the identity of node 12. Nodes 15, 8, and 5 which are neighbors with node 16 will validate the identity of this node. As nodes 15, 8 and 5 are not neighbors to node 12, they will be able to detect that node 16 is misbehaving.
- Scenario 2: Consider that node 2 forwards a TC message to a node in the network claiming to have the identity of node 8. Nodes 3, 4, and 5 which are neighbors with node 2 will validate if this node has the true identity. As nodes 3 and 5 are neighbors with node 8, they will not be able to distinguish the identity of the malicious node. Thus, they will not be able to detect the attack. Whereas, node 4 is able to detect that node 2 is an attacking node because it does not have node 8 in its neighbors' list.
- Scenario 3: Consider that node 8 forwards a TC message into the network claiming to have the identity of node 12. Nodes 15, 5, 11, and 2 will detect that node 8 is an attacker because they are not neighbors with node 12. Whereas, node 3 will not be able to detect the attack.

2) Wormhole attack: We will consider also a scenario where two attackers launch the wormhole attack and show how watchdogs are able to detect this attack. Consider that node 4 at source wants to send a message to node 15 at destination. A malicious node, node 7 copies the message of the source node 4 and sends it to another attacker, node 11 through the wormhole tunnel (7-12-19-11). Node 11 will replay the message. When the receiver, node 15 gets the message, it will consider that this is the shortest path in the network and select this route. But in fact, there are shorter routes to reach the destination: (4-2-8-15) and (4-3-8-15). The watchdogs, MPR nodes which are neighbors with the candidate nodes at source and destination, will check if an attack is performed. Nodes 4 and 12 will watch node 7; and nodes 8, 15, and 19 will monitor node 11. The monitors at source and destination will check, respectively, if there is a shortest path or equivalent path with larger QoS. If so, then the attack is detected.

B. How to improve detection

We are going to present cooperative watchdogs that improve the detection. Then, we will add Bayes' rule function to the cooperative model.

1) Cooperative watchdogs: Watchdogs are responsible of monitoring the behavior of the candidate node. The watchdogs cooperate together in order to give better results. Therefore, the final decision should be based on an aggregation between more than one watchdog node decision.

2) Posterior belief function: The main objective of the Posterior belief function is to have a trusted detection of attacks in the network. This method increases the efficiency of detection because it is based on a prior knowledge.

In our case, the type of a node sending TC message can be selected from a set $\Theta = \{Malicious(M), Normal(N)\}$. Bayesian Equilibrium, proposed in [12], dictates the performance of the candidate node depending on its type Θ. By observing the behavior of the sender, the watchdogs can calculate the posterior belief evaluation function $\mu(\theta_i|\alpha_i)$ using the following Bayes' rule (refer to equation 1):

$$\mu(\theta_i|\alpha_i) = \mu(\theta_i)P(\alpha_i|\theta_i)/\Sigma_{\theta_i \varepsilon \theta}\mu(\theta_i)P(\alpha_i|\theta_i) \tag{1}$$

where $\mu(\theta_i) > 0$ and $P(\theta_i|\alpha_i)$ is the probability that strategy α_i is observed given the type θ of the node i. It is computed as follows:

$$P(Attack|\theta_i = M) = E_m \times O + F_m(1 - O) \qquad (2)$$

$$P(Attack|\theta_i = N) = F_m \qquad (3)$$

where O is the probability of attack determined by the watchdog node. F_m is the false rate generated by the watchdog and E_m is the expected detection rate. We define the intruders pure strategy as $\alpha_i = \{Attack, NotAttack\}$.

We implemented the following algorithm that computes the probability of detecting the attack based on the cooperative watchdogs' decisions and reputations (Algorithm I):

```
Algorithm I: Identity Spoofing and Wormhole Attack Detection Algorithm
Let P be the Probability of detection
Let w be the Watchdogs' list
Let MN be the Malicious Node
Let SN be the Spoofed Node
Let $\theta$ be the type of the node; $\theta_i$ = M(Malicious) or N(Normal)
Let rep(w(i)) be the reputation of each watchdog i;
  rep(w(i)) between 0 and 1
Let sumrep be the sum of reputations of the watchdogs;
  sumrep = $\sum_i rep(w(i))$
For i = 1 to length(w)
  If w(i) and MN are neighbors
    If w(i) and SN are neighbors Or shorter path not detected
      If $\theta_{w(i)} = M$
        P = P + rep(w(i))
      End
    Else
      If $\theta_{w(i)} = N$
        P = P + rep(w(i))
      End
    End
  End
End
P = P/sumrep
```

The monitoring nodes are the MPR nodes that are neighbors with the candidate node sending the message. Each watchdog will now check if it is neighbor with the spoofed node as we can see in Algorithm I. If it is not neighbor with the spoofed node, then it will directly know that an attack is launched. However, the watchdog might be a neighbor with the spoofed node. Therefore, it will make a false prediction about the malicious node, and the attack is launched. In addition, the watchdog can itself be malicious. So, it will behave improperly, listing the normal nodes as malicious ones and the attackers as normal ones. Therefore, the final decision should be based on an aggregation between more than one watchdog node's decision. A weight is added to each decision depending on the reputation value associated with each watchdog because the reputation represents how much a node is trustworthy. The reputation is a value between 0 and 1. When head nodes and MPR nodes are selected, reputation values are given to each node depending on their trustworthiness. The highest values are given to the most trusted nodes (head nodes), then to MPR nodes, and finally to normal nodes.

As for the wormhole attack, the monitors at source and destination will check, respectively, if there is a shorter path or equivalent path with larger QoS. If so, then the attack is detected if the node was normal and the decision of each monitor will be added with its reputation weight to the detection rate. If the watchdogs were malicious or were not able to find a shorter route, they will not contribute in detecting the attack.

V. Simulation results

Matlab-8.0 has been used to simulate the effect of the attacks and the detection algorithm applied to the clustering QoS-OLSR model. The first subsection shows the percentage of disconnected clusters in QoS-OLSR model due to identity spoofing and wormhole attacks. The second part presents the probability of detecting the two attacks and the false rate given different percentages of attackers. The simulation parameters are summarized in Table II.

TABLE II
Simulation Parameters

Parameter	Value
Simulation area	500 × 500 m^2
Number of nodes	Between 30 and 70
Transmission range	125 m
Residual energy	Random value in [500...550] J
Packet Size	1 kb
Energy Per Packet	0.0368 J
Idle Time	Random value in [0...1]
Link Bandwidth	2Mbps
Available Bandwidth	Idle Time × Link Bandwidth
Direction	Random value in [0...2pi]
Speed	Random value in [1...10]
E_m	0.8

A. Effect of Identity Spoofing and Wormhole Attacks on the Network

A malicious node performing the identity spoofing attack or two attackers that launch the wormhole attack can lead to disconnected clusters in the network. Figure 3 presents the percentage of disconnected clusters when 10% of the nodes are attackers. The attack was launched every time the topology is changed and the average number of disconnected clusters was calculated for different number of nodes in the network. We can realize that the attack has affected the network since more than 60% of the clusters have been disconnected.

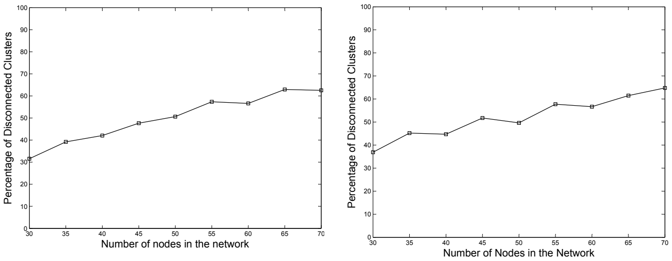

Fig. 3. Percentage of disconnected clusters: (a) Identity Spoofing Attack (b) Wormhole Attack

Figure 4 presents the percentage of disconnected clusters with different percentages of attackers in the network. The average number of disconnected clusters was calculated for

30 nodes in the network. It is obvious that the percentage of disconnected clusters reach around 80% when the percentage of attackers increase to 50% of the nodes in the network.

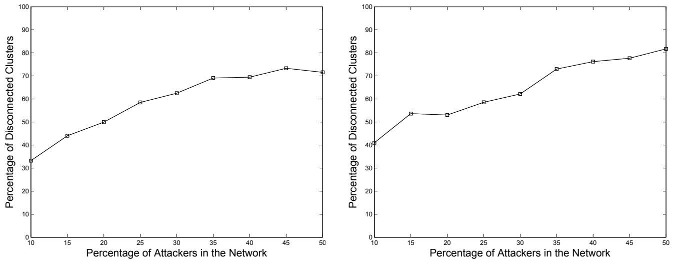

Fig. 4. Percentage of disconnected clusters: (a) Identity Spoofing Attack (b) Wormhole Attack

B. Probability of Detecting Attacks and False Rate With Different Percentage of Attackers

Figure 5 shows the percentage of detected attacks. The detection percentage is simulated along with the corresponding false detection percentage (in figure 6) for the two attacks with and without posterior belief function given different percentage of attackers. Given that 10% of the nodes are attackers, we can realize that posterior belief function provides more efficient results. 77% of the malicious nodes corresponding to identity spoofing attack were detected using the cooperative watchdog-based model with the posterior belief function; whereas, around 70% of the attackers were detected without the posterior belief function. Moreover, around 88% of the wormhole attacks were detected using the cooperative watchdog-based model with the posterior belief function; and, 80% of the attackers were detected without the posterior belief function:

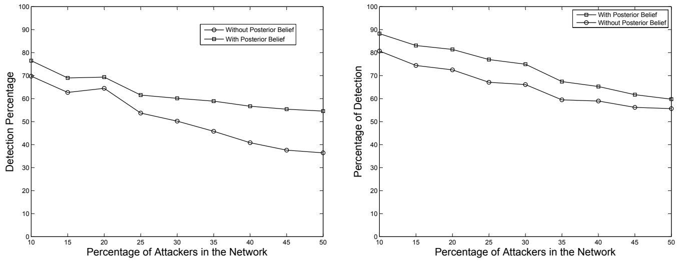

Fig. 5. Detection percentage with different percentage of attackers: (a) Identity Spoofing Attack (b) Wormhole Attack

In Summary, based on the simulations, we proved that malicious nodes affect the network negatively by increasing the percentage of disconnected clusters. Thus, we need a detection model in order to stop the misbehaving nodes from perturbing the network. Our detection model that is based on the cooperative watchdogs' reputation concept along with posterior belief function demonstrates good results regarding the detection of malicious nodes.

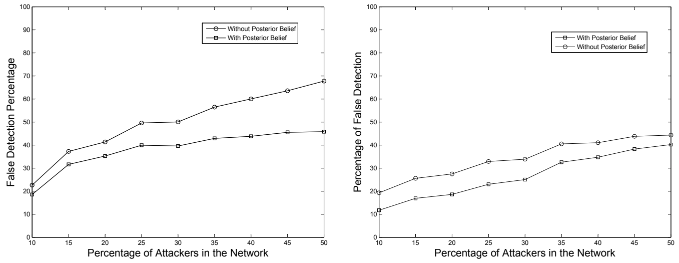

Fig. 6. False detection percentage with different percentage of attackers: (c) Identity Spoofing Attack (d) Wormhole Attack

VI. Conclusion

Identity spoofing and wormhole attacks are identified as possible attacks against QoS-OLSR protocol. These attacks can degrade the network performance by isolating some head nodes and having disconnected clusters. To detect the two possible attacks, we have presented a novel detection approach based on the cooperation among watchdogs where the reputation of nodes is considered in the aggregation function. The detection was then enhanced by adding the posterior belief function that increases the true detection and decreases the false detection rates as shown in the simulation results.

References

[1] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto. A study of a routing attack in OLSR-bases mobile ad hoc networks. In *International Journal of Communication Systems*, March 2007.

[2] K. U. Vidhya, and M. M. Priya. A Novel Technique for Defending Routing Attacks in OLSR MANET. In *IEEE International Conference on Computational Intelligence and Computing Research*, 2010.

[3] E. G. Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. Tolle. Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs. In *IEEE Computer Society*, pages 1043–1049, 2007.

[4] R. Song, and P. C. Mason. ROLSR: A Robust Optimized Link State Routing Protocol for Military Ad-Hoc Networks. In *IEEE Military Communications Conference*, 2010.

[5] B. Kannhavong, H. Nakayama, and A. Jamalipour. SA-OLSR: Security Aware Optimized Link State Routing for Mobile Ad Hoc Networks. In *IEEE Communications Society*, pages 1464–1468, 2008.

[6] C. Adjih, D. Raffo, and P. Muhlethaler. Attacks Against OLSR: Distributed Key Management for Security. In *DGA/CELAR*.

[7] A. Bhattacharya, and H. N. Saha. A Study of Secure Routing in MANET: various attacks and their countermeasures. In *IEMCON*, pages 256–261, 2011.

[8] F. Hong, L. Hong, and C. Fu. Secure OLSR. In *19th International Conference on Advanced Information Networking and Applications (AINA'05)*, 2005.

[9] B. Kannhavong, N. Hidehisa, and A. Jamalipour. A Collusion Attack Against OLSR-based Mobile Ad Hoc Networks. In *IEEE GLOBECOM*, 2006.

[10] L. P. Suresh, R. Kaur, M. S. Gaur, and V. Laxmi. Collusion Attack Resistance Through Forced MPR Switching in OLSR. In *International Journal of Computer Science and Security*, 18–29, vol.2, no.3, 2010.

[11] F. N. Abdesselam, B. Bensaou, and J. Yoo. Detecting and Avoiding Wormhole Attacks in Optimized Link State Routing Protocol. In *IEEE WCNC*, pages 3119–3124, 2007.

[12] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and P. Bhattacharya. A Moderate to Robust Game Theoretical Model for Intrusion Detection in MANETs. In *IEEE International Conference on Wireless and Mobile Computing, Networking and Communication*.

[13] H. Otrok, A. Mourad, J. M. Robert, N Moati, and H. Sanadiki. A cluster-based model for QoS-OLSR protocol. In *IWCMC*, pages 1099–1104, 2011.