LEBANESE AMERICAN UNIVERSITY

DETECTING ATTACKS IN A CLUSTER BASED QOS-OLSR PROTOCOL

By

HIBA SANADIKI

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

Lebanese American University

School of _Arts and Sciences_______ ;_Beirut______ Campus

THESIS APPROVAL FORM

Student Name: ______Hiba Sanadiki____________ I.D. #: _____200602556_________

Thesis Title : Detecting Attacks in a 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 [redacted] Date : 05/05/14

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

Committee Member's Name Dr. Ramzi Haraty Signature Date: 05/05/14

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

THESIS COPYRIGHT RELEASE FORM

LEBANESE AMERICAN UNIVERSITY NON-EXCLUSIVE DISTRIBUTION LICENSE

Name: Hiba Sanadiki

Signature: [redacted]

Date: 05/05/2014

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: Hiba Sanadiki

Signature: [redacted]

Date: 05/05/2014

ACKNOWLEDGMENT

This project would not have been possible without the support of many people. I would like to express my gratitude and appreciation to my supervisors, Dr. Azzam Mourad and Dr. Hadi Otrok, for their guidance and support. Also I would like to thank my committee member, Dr. Ramzi Haraty, for his time and efforts.

And finally, thanks to my parents, and numerous friends who endured this long process with me, always offering support and love.

Detecting Attacks in a Cluster Based QoS-OLSR Protocol

Hiba Sanadiki

ABSTRACT

In this thesis, we detect attacks targeting the cluster based QOLSR model in Mobile Ad Hoc Networks (MANETs). The QOLSR is a multimedia protocol that was designed on top of the Optimized Link State Routing (OLSR), where the Quality of Service (QoS) of the nodes is considered during the selection of the Multi-Point Relay (MPRs) nodes. One of the drawbacks of this protocol is network lifetime where nodes with limited energy and high bandwidth may be selected to serve as MPRs, which drain nodes' residual energy and shorten the network lifetime. Thus, in this thesis, we consider the trade-off between extending the lifetime of ad hoc network and QoS assurance based on QOLSR routing protocol. We can accomplish the following by (1) decreasing the number of Multi-Point Relay (MPR) nodes without sacrificing the QoS and (2) observing the energy level, connectivity index, and bandwidth of the MPR nodes. We can reach these goals by deploying the clustering model to QOLSR. Therefore, a new clustering approach and MPR selection process are proposed relying on different combinations of metrics, such as connectivity, residual energy, and bandwidth. Four clustered-based models are derived. Moreover, the cluster-based models are highly vulnerable to security attacks. Two attacks that can be launched against the QoS-OLSR protocol where identified: Identity spoofing and worm-hole attacks. 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 watch-dog model and (2) adding the posterior belief function using Bayes' rule to the watchdog model. Simulation results are generated in order to evaluate the efficiency of our proposed approaches.

Keywords: Quality of Service (QoS), Head Election, MPR Selection, Ad Hoc Networks, Mobility, Identity Spoofing Attack, Wormhole Attack, Posterior Belief Function.

Table of contents

List of Figures

List of Tables

Chapter One

Introduction

1.1 Motivations and Problem Statement

Mobile ad hoc network(MANET) [26] is a guaranteed technology for the growth of wireless networks. It relies on a self-configuring and easily deployed network without depending on any fixed infrastructure. MANET is applied in several real world applications where the topology of the network is changed frequently. In MANETs, nodes communicate and send packets to each others through routing.

Routing is the mechanism of exchanging information between the nodes in ad hoc network [27] and forwarding packets from a source towards its destination through the optimal path. The efficiency of a route can be measured by different metrics(i.e., number of hops in a path, minimum delay, maximum bandwidth, etc). Most routing protocols for MANETs are designed without taking into consideration the Quality of Service of the routes generated. In such protocols, the only metric considered for routing is the number of hops. One the proposed routing protocols is OLSR.

The *Optimized Link State Routing*, known as OLSR [7], is a proactive routing method for mobile ad hoc networks. This protocol is based on MPR (MultiPoint Relay) nodes that transmit the topology control information of the network and forward packets from source to destination. Relying on OLSR, Quality of Service (QoS) OLSR protocol, known as QOLSR [3], was proposed in literature to consider nodes' available bandwidth during the MPR and optimal routing paths selection. The protocol was designed to handle multimedia applications over ad hoc networks. The delay and bandwidth metrics that satisfy Quality of Service are considered during the selection of MPR.

The QOLSR protocol [10] has a main limitation that can ultimately jeopardize the ultimate goal of the protocol, where the lifetime of the network can be shorter due to selecting a large number of MPRs. In fact, in QOLSR protocol, every node in the network selects its own set of MPRs independently. Due to this problem, nodes' available bandwidth is affected and the possibility of channel collision is increased, especially in the dense networks.

Moreover, several attacks can be launched against the proposed clustering model. Thus, a security mechanism should be provided for any cluster-based model. In fact, normal nodes or MPR nodes in any cluster can behave maliciously. They can broadcast fake Topology Control (TC) messages since security is not ensured.

Topology control (TC) messages are transmitted 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.

Being a mobile and wireless network, QOLSR is more susceptible to attacks than normal networks. Attacks against the network can be performed each time the TC messages are exchanged. These attacks can lead to network disruptions that can eventually threaten the ultimate goal of the protocol.

The following objectives must be ensured in order to maintain the stability and security of the network. First, a trade-off between reducing the percentage of MPR nodes and maintaining good Quality of Service metrics(i.e., residual energy level, connectivity index, and bandwidth) should be considered during the formation of clusters. Second, the attacks performed against this cluster-based model should be identified and detected. While detecting the attacks, normal and MPR nodes should be monitored because they might be malicious. In addition, watchdogs themselves could be malicious ending up giving false detection decisions. The malicious watchdog may accuse a node that is not malicious to be misbehaving

In this context, many clustering algorithms have been proposed [1, 4, 5, 8, 9, 11, 13]. However, the approaches select a large number of MPR nodes, which can shorten network lifetime, affect nodes' available bandwidth and increase the risk of channel collisions. Also, in some methods, MPRs are selected based on nodes' bandwidth without considering other metrics.

In addition, several approaches have been proposed to detect the misbehaving nodes [14–23]. The existing methods suppose that each node can act as a watchdog and monitor the performance of its neighbors. In fact, this node can be selfish or malicious and hence give false results. A malicious watchdog may accuse normal nodes to be misbehaving unjustly. Moreover, it can also predict that a malicious node is not misbehaving in order to help this node launch its attack. Therefore, the decision of a single monitor is not enough in order to evaluate the behavior of the nodes in the network. Based on this, the accuracy of detection results will decrease and the false detection rates will increase. Thus, a bayesian cooperative approach [31] is proposed in order to enhance the detection, give more accurate results, and reduce the false detection rates.

In summary, the following are the problems listed in this thesis:

- Low Quality of Service due to the high numbers of MPRs.
- Misbehaving and malicious nodes that can launch attacks against the network.

1.2 Objectives

The main purpose of this thesis is to develop a cluster based QoS-OLSR model that maintains high Quality of Service, identifies the attacks that can target this clustered model and ensures the security of this model by detecting these attacks. In summary, the objectives of our approach can be listed as follows:

- Reducing the percentage of MPR nodes without sacrificing the Quality of Service metrics.
- Improving the detection of misbehaving nodes and the false detection rates by using a bayesian cooperative detection approach.

1.3 Approach Overview and Contributions

In this thesis, we propose a clustering model, where nodes can 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 has been proposed 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 metrics such as residual energy or connectivity degree [12,13]. All the proposed models assume the presence of clustering models that can cluster the network, while the MPRs are selected afterwards. While in our model, the heads are selected cooperatively, then they will select the MPRs that can connect the heads with each others into 1-hop, 2-hop, and 3-hop away. In this context, we propose a solution that has four different clustering models based on three metrics: bandwidth, connectivity index and residual energy. To the best of our knowledge, there has not been any work done that considers the tradeoff, for QOLSR, between network lifetime and QoS based on clustering. Simulation results show that the novel cluster based approach is able to prolong network lifetime by selecting less number of MPRs, thus decreasing traffic overhead, delay, channel collision, and increasing cooperation in the network.

Moreover, to deal with the security of our clustering model, we identify two attacks that can be launched against 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. These attacks may lead to network disruptions. Therefore, a detection approach is proposed in order to identify the malicious nodes in the network. To detect the above attacks, we propose the use of watchdogs. To enhance the detection, we propose a solution based on cooperative watchdogs that will monitor the attackers. The final decision is calculated by the aggregation function that considers the reputation used in QoS-OLSR. MPR nodes are the only nodes selected as watchdogs in our model, because TC messages are exchanged only by the MPRs. Then Bayes' rule function [31], which calculates the posterior belief of a node being misbehaving based on observations, will be added to our cooperative model in order to improve the overall detection. Simulation results are conducted to evaluate the performance of adding Bayes' rule function to the cooperative watchdog model.

The contributions of the thesis are summarized as follows:

- Introducing a novel clustered based QoS-OLSR approach that prolongs the network lifetime by reducing the number of MPR nodes, which decreases the the risk of channel collisions and the possibility of traffic overhead.

- Selecting the MPRs cooperatively based on nodes' QoS metric(i.e., residual energy level, connectivity index, and bandwidth) using MPR nodes selection algorithm.

- Detecting the attacks launched against the QoS-OLSR using an improved cooperative watchdog model that gives more accurate results.

- Reducing false positives where malicious nodes are mistakenly or intentionally considered as normal nodes by adding the posterior belief function using Bayes' rule to the watchdog model.

1.4 Thesis Organization

The rest of the thesis is organized as follows:

In Chapter [2], we present the main ideas provided in the thesis: ad-hoc network, MANET, security in MANET, cooperative watchdogs and bayesian rule. Then, we provide the related works in the areas of clustering and detecting attacks against QOLSR.

In Chapter [3], we propose our clustering approach. We develop a cluster head election and MPRs selection algorithms in order to form our clusters. Then, we give an illustrative example to show how these algorithms work. Finally, we present the simulation results that evaluate the efficiency of the proposed cluster based QoS-OLSR model.

In Chapter [4], we identify the security attacks that can be launched against our QoS-OLSR protocol along with a network example in order to show how the attacks can be launched. Then, we present the bayesian cooperative detection model that is proposed to detect these attacks. Finally, we simulate the effect of the attacks and the detection algorithm applied to the clustering QoS-OLSR model.

In Chapter [5], we conclude the thesis, recapitulate its contributions, state the future works, and provide the publications derived from this thesis.

Chapter Two

Background and Related Work

2.1 Introduction

This chapter presents an overview about the concepts that form our models. We introduce first ad-hoc networks and talk about their characteristics. Then, we describe MANETs and the security concerns in these networks. Moreover, the thesis uses watchdogs to detect the attacks that can be lauched against the QoS-OLSR protocol. To enhance this detection, we propose a cooperative watchdog theory to make the final decision based on an aggregation function. In order to improve the overall detection, we add the Bayes-rule function which calculates the posterior belief of a node being misbehaving based on observations. In this context, we give a definition of the Bayes rule and show the importance of this method. Finally, a summary of the related works in the fields of clustering and detecting attacks in MANETs is provided.

2.2 Ad-hoc Network

An ad hoc network [28] is a set of two or more nodes that compose a network and communicate with each other without the need of centralized access points or base stations. Unlike conventional networks, it does not rely on any fixed infrastructure and can be deployed easily and with relatively low cost.

Figure 1 represents a peer-to-peer multihop ad hoc network. It begins with at least a communication between two nodes broadcasting topology control messages including their respective address information. If two nodes are neighbors, then they can directly send messages to each others. They should both update their routing tables. For example, node A communicates directly with node B because they are neighbors. If two nodes are not neighbors, multi-hop communication is needed. The intermediate nodes between these two nodes should route the packet. Another example is when A wants to communicate with C. It can't do this directly, node B or nodes D and E should act as routers.

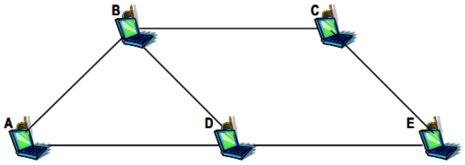

Fig. 1: Ad hoc network

Ad hoc networks history [28] started in 1972, when the US Department of Defence, DARPA, initiated a packet radio network (PRNet) research recognizing packet switching in order to provide reliable computer communication. The advantage of packet switching is the dynamic sharing of bandwidth among multiple users. Then, in 1983, Survivable Radio Network (SURAN) was built, followed by several ad hoc networks developed in

1994 under the Global Mobile Information Systems program (GloMo). SURAN improved by making the radios cheaper, smaller, and power consumers. In the beginning of 1990s, notebook computers, open source softwares and viable communications equipment based on infrared and RF have emerged.

Being dynamic and self-organized, ad hoc networks are functional in many applications where rapid deployment is required or when network infrastructure is very costly to manage [29]. These applications include:

Commercial Area: Ad hoc networks are employed in emergency services. As an example, workers in a field who communicate with each others in a disaster area(e.g., fie, flood, earthquake) and share video updates of specific locations and send the information to headquarters over a small hand held. Armed forces also use ad hoc networks by creating a tactical network in an unfamiliar territory in order to communicate and distribute situational awareness information.

Local level: Ad hoc networks are also used to spread and exchange information over an instant and temporary multimedia network. For example, they are used in conference rooms where people share some files via notebooks or handheld devices. Another example of local networks is home or office networks where the devices share information by communicating directly. Moreover, ad hoc networks can be used in civilian environments such as taxicab, boat, and aircraft.

Personal Area Network: Ad hoc networks simplify the communication between several mobile devices like PDAs, laptops and cellular phones. Wireless connections are used instead of wired cables.

Military Battlefield: The military use ad hoc networks in order to sustain an information network between its headquarters, soldiers and vehicles.

Ad hoc networks are classified into four categories depending on their coverage area: Body networks, personal networks, Local networks, and Wide Area Networks [29]. The main characteristics of ad hoc networks include the following:

Mobility: In ad hoc networks, nodes can rapidly change position and move in the network depending on specific direction and speed. This will result in constantly changing network topologies. Therefore, mobility may affect the network performance and the routing method selection.

Multihop routing: Multihopping is revealed in networks where there are multi paths from source to destination. Multihop network is often used for energy consumption, obstacle negotiation and spectrum reuse.

Self-organization: There is a lack of pre-configuration in ad hoc networks. Thus, the network should be dynamically and automatically managed. All the configuration parameters like clustering, path routing, nodes position and and energy control should be autonomously determined.

Resource limited devices: Most of the nodes in an ad hoc network have limited energy and are not able to generate their own power.

Resource limited communications: This is due to the fact that many nodes in the network use the radio medium at the same time.

Scalability: Hierarchical construction handle the scalability in networks that are based on a fixed infrastructure. Local handoff and Mobile IP methods are also used to deal with the limited mobility in infrastructure based networks. Whereas, fixed hierarchical structure cannot be used in ad hoc networks because of the absence of any fixed infrastructure and the wide mobility level in the network.

Potentially large networks: A network could have of a huge number of nodes. For example, a network of sensors that consists of thousands of mobile nodes.

2.3 MANET

A mobile ad hoc network (MANET) [26] is a wireless network consisting of mobile nodes that exchange information without base stations regardless of their geographical location. They do not have any established infrastructure, and they have constrained bandwidth and energy and dynamic topologies. Nodes that are neighbors can communicate directly with each others over wireless links, and those that are not neighbors use MPR nodes in order to exchange information. The nodes are able to join, leave or move in the network; thus The network topology changes constantly.

In MANET, network configuration and message transfer should be performed by the nodes themselves because the network is decentralized. Message routing is an issue in decentralized environments where the network topology changes. In addition, the optimal path from source to destination in MANET is not the shortest route as in static networks.

MANET introduces several challenges [26] which include:

Quality of Service: The characteristics of MANETS make it difficult to guarantee the services that should be offered to the nodes in the network. Thus, in order to support these services, QoS must be ensured.

Routing: The problem of routing in MANETs is an important challenge because the network topology is changing frequently. Packets delivery should be ensured between the nodes at source and destination. Paths between nodes may consist of multiple hops, which is more difficult than the single hop communication.

Reliability and Security: Reliability problems are introduced in ad hoc networks due to the the broadcast nature of the wireless medium, limited wireless transmission range, mobility nature of the network and data transmission errors. In addition, MANETs are susceptible to many attacks that could be launched against the nodes in the network. Thus, security should also be ensured in these networks.

Power Consumption: Energy conservation and energy-aware routing should be considered in MANET. The communication operations should be optimized in order to consume power in MANETs.

Multicast: The multicast routing protocol must should support mobility.

Location-Aided Routing: The associated areas are identified by using nodes position information so that routing will be limited and spatially oriented.

2.4 Security in MANETs

Being mobile and dynamic wireless networks, MANETs are more susceptible to malicious attacks than static networks. Moreover, due to their open medium and dynamic network topology, MANETs are vulnerable to several types of attacks such as impersonation, passive eavesdropping and denial of service. A malicious node is able to destroy the communication between two nodes by claiming to have another's node identity, sending incorrect link state information and broadcasting false routing information.

The main challenges ad concerns to be considered in MANET security are [26]:

Lack of centralized management: MANET does not rely on a centralized infrastructure. Monitoring all the nodes and detecting malicious attacks in a large mobile network is difficult due to the absence of centralized management.

Resource availability: Ensuring secure communication in dynamic networks and protecting against malicious nodes leads to maintain security mechanisms.

Scalability: The network topology changes every period of time because of the mobility of nodes. Thus, scalability is a major issue for securing MANET. The security schemes should be able to handle small and large networks.

Cooperation: Nodes in ad hoc network are assumed to be trusted and cooperative. Thus, a misbehaving node can easily disrupt the network functions by launching a harmful attack.

Dynamic network topology: Changing network topology may affect the trust relationship between the nodes. Therefore, an adaptive security mechanism should be proposed in order to handle the dynamic behavior.

Limited energy: Nodes in a mobile ad hoc network may act in a selfish way in order to save its power.

Attackers inside the network: Nodes in a mobile network can easily join or leave the network. Attacks may be launched by insiders and outsiders. But attacks launched by nodes inside the network are more dangerous than external attacks; therefore, detection mechanisms should be proposed to detect the misbehaving nodes inside the network.

No predefined boundary: Nodes in MANET are free to join and leave the network. There is no predefined physical boundary that control nodes' movement. Thus, when a malicious node joins the network, it can easily communicate with other nodes and launch an attack such as: eavesdropping, spoofing, replay, wormhole and denial of service attacks.

One way of securing a mobile ad hoc network is by applying detection and prevention methods like authentication and encryption approaches, however, experiments have demonstrated that these methods are not sufficient. Therefore, intrusion detection systems are needed to defend against the malicious attacks.

There are number of attacks that can affect MANETs [26]:

Denial of service: The availability of a node or the entire network is attacked. The attack uses radio jamming and battery exhaustion techniques.

Impersonation: A malicious node can spoof the identity of another node. Thus, it can monitor the network traffic, send fake information to the network and have access to confidential information.

Eavesdropping: The malicious node gains access to the confidential information such as node's location, public and private key, and password.

Routing attacks: This attack aims at blocking the broadcast of routing information to a node in the network. It can also disturb the delivery of packets against a predefined path.

Jamming: The malicious node verifies the frequency at which the destination node is receiving the signal from the sender by monitoring the wireless medium. It then uses this frequency in order to transmit signals and cause errors.

Man in the middle: A malicious node stands between the sender and the receiver and steals the information exchanged. It can also spoof the identity of the sender and communicate with the receiver.

Security in MANETs is an essential component for basic network functions such as sending control messages, packet forwarding and routing. Such networks also have high communication overhead because nodes send periodic control messages each time the network topology changes. Unlike traditional networks that use specific trusted nodes to support basic functions, in ad hoc networks, those functions are used by all the available nodes. These nodes could be malicious and therefore launch attacks against the protocol. In order to secure mobile ad hoc networks, early detection of attacks against the network should be applied.

2.5 Cooperative Watchdogs

Watchdogs are the nodes responsible of monitoring the behavior of the various nodes in the network. It is a well-known intrusion detection mechanism that detects attacks launched by selfish and malicious nodes against the network [30]. When the source node sends a packet, the watchdog listens to the transmissions of the next node in the path in order to verify that this node broadcasts the packet correctly. If not, then this node is identified as malicious. Such systems can then isolate or penalize misbehaving nodes by reducing their reputation (i.e., trust rates). Thus, watchdogs overhear the transmissions of all next nodes in the route. After monitoring the behavior of its neighbors, the watchdog can decide wether a node is selfish or malicious. Figure 2 shows an example of the watchdog behavior:

Suppose that node A needs to forward a message to node D. It can send this message through path A-B-C-D or path A-M-D. The watchdog can listen to the packets sent by B and M who are in range of A. Suppose node M is malicious. If route A-B-C-D is chosen, then B sends all the packets to C which forwards them to D. Else, if route A-M-D is chosen, then an attack is performed and all the received packets are dropped. When M does not

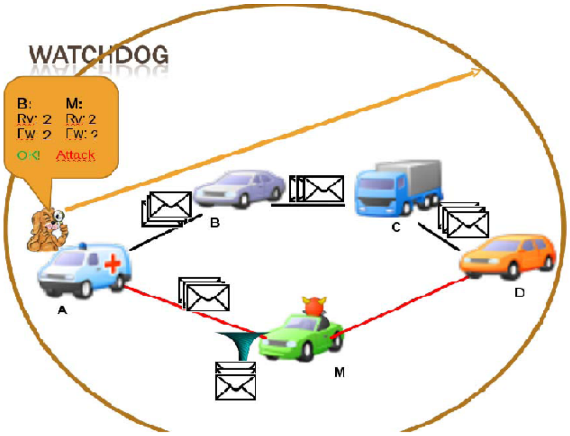

Fig. 2: Watchdog example

forward the packet, the watchdog knows it and identifies node M as malicious.

Another issue is the false detection decision that could be taken by watchdogs. Nodes mobility and collisions reduce the accuracy of the detection results and leads watchdogs to provide false positives and false negatives decisions. This will lead to network disruptions because some malicious nodes are mistakenly identified as normal trusted nodes, and some normal nodes are identified as attackers. One way to improve detection and reduce the detection time of malicious nodes is the use of collaborative watchdog. The watchdogs cooperate together in order to improve their individual and collective performance. The cooperative model also decreases the false negatives and false positives rates.

2.6 Bayesian Rule

The Bayesian rule is a mathematical theorem provided by Thomas Bayes. It explains how the existing beliefs should be changed in the light of new evidence. This theory has been used in a wide variety of contexts such as developing Bayesian spam blockers for email systems and marine biology. In the scheme of science, bayes' rule was useful in clarifying the link between theory and evidence. Several approaches such as confirmation, falsification, relation between science and pseudoscience, etc. were made more accurate, and enlarged or corrected, by the use of Bayes' method.

Bayes rule [31] calculates the estimation probability that a hypothesis H is true in the light of evidence E. Let (1) P(H) be the prior belief of the probability that hypothesis H is true before the observation of E; (2) P(H|E) is the conditional likelihood that E will occur given that H is true; (3) P(E|H) is the probability of observing evidence E given H; and (4) P(E) is the marginal probability of E. Then, the posterior probability of hypothesis H given the evidence E is:

$$P(H|E) = \frac{P(E|H) \times P(H)}{P(E)} \tag{1}$$

As an example, a given population is 40% boys and 60% girls. 30% of the boys like to play football but only 10% of the girls like to play football.

The probability that a person randomly chosen is a boy:

P(boy) = 40% of the entire population

The probability that a person randomly chosen is a girl:

P(girl) = 60% of the entire population

Probability of picking at random from the set of boys someone who likes to play football:

P(football | boy) = 30%

Probability of picking at random from the set of girls someone who likes to play football:

P(football | girl) = 10%

The question is: What would be the probability of randomly choosing a boy from the set of people who like to play football? What is P(boy | football)?

According to Bayes Theorem:

$$P(boy|football) = \frac{P(football|boy) \times P(boy)}{P(football)} \tag{2}$$

Given that,

$$P(football) = P(football|boy) \times P(boy) + P(football|girl) \times P(girl) \tag{3}$$

Thus,

$$P(boy|football) = \frac{30\% \times 40\%}{30\% \times 40\% + 10\% \times 60\%} = \frac{12\%}{18\%} = \frac{2}{3} \tag{4}$$

According to the Bayes rule, the posterior probability is proportional to the product of the likelihood and the prior probabilities. This aspect can be exploited to enhance the detection of attacks in MANETs and reduce the false detection rates. The main objective of the bayes rule function is to improve the efficiency of the detection.

2.7 Related Work

In this section, we present a summary of the research contributions in the areas of network clustering and detecting attacks in MANETs. Then, we explain the problems and limitation of the proposed models and motivate the need for our approaches.

2.7.1 Clustering in MANET

In this section, the previous work of QOLSR and the cluster based approaches for OLSR are reviewed.

OLSR [7] is a classical link state protocol that was adapted to fulfil the needs of ad hoc networks. Multi-Point Relay (MPR nodes) are the base of this approach. The role of these selected nodes is to broadcast the topology information of the network in their control messages. In addition, the MPRs send traffic flows from source to destination.

Significantly, the overhead of TC messages will be reduced by this optimization technique. Therefore, OLSR protocol is mostly applicable in 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 [3] routing protocol was developed based on OLSR where QoS has been considered. This raises the need for new metrics like delay and bandwidth. Thus, the aim is to find a source-destination routes, but the optimal ones that ensures the end-to-end QoS requirements. The MPR selection is based on the QoS measurements that allow finding optimal paths in QOLSR. Multiple-metric routing criteria were considered in order to improve the QoS of the route. The QOLSR has two main limitations. MPRs are selected based on nodes bandwidth without considering nodes energy level and connectivity which can shorten the network lifetime.

In this regard, new clustering models have been proposed based on connectivity and energy levels. [1,5,13].

The HOLSR protocol was proposed in [13]. This protocol depends on the type of nodes in the network: nodes with greater transmission potentials and ordinary nodes. Previous nodes work as an organized network of connected heads likely identified as mobile access points. Whereas, ordinary nodes are arranged into different clusters where every node discovers the head to which it should be connected. Then, the traffic should be directed to the local cluster head and sent to the proper remote cluster head in order to reach any remote destination.

Authors in [1] present the OLSR Tree protocol. In this approach, every node chooses an adjacent node that have the largest number of neighbors as its parent. In this context, the network is partitioned into a set of overlapping trees where any leaf node can be part of different trees. Thus, clusters are formed from each tree where the root node will be the local cluster head. A prolonged form of OLSR that establish a set of super MPRs is used by cluster heads in order to interconnect between them. In this extended approach, each cluster behaves as a unique super node.

To deal with the scalability issues of dense ad hoc networks, a solution that is totally independent of the approach applied was proposed in [5]. OLSR protocol and its traditional messages are bounded to the local clusters. Cluster heads send super topology control messages to interconnect these clusters. These kind of messages help any source node to locate the next hop reaching its destination. Thus, this technique is easier than the extended OLSR method applied earlier.

Many approaches [4, 8, 9, 11] that used node's remaining energy as a metric for the routing protocol proved that energy consumption is reduced and the network lifetime is prolonged. In these methods, MPR selection will depend either on a simple measure that considers the nodes' residual energy level or on a mixed weighted measure where nodes' connectivity is considered along with the nodes' residual energy [9]. Choosing the method relies on the physical model of nodes' power consumption. In some methods, high costs are assigned to links coming out from the nodes that have degraded residual energy level. These approaches use Dijkstra's algorithm in order to calculate the paths with the smallest total cost (as in, [4] and [8]). Yet, other methods that select a path reducing the maximum total energy consumed by all the nodes along the route are desired. [11].

All these proposed approaches are based on forming the clusters first, then heads are selected. While, our model is based first, on head selection and then clusters are formed. Clusters are connected through the selection of the best MPRs. In our previous work [6], we have only addressed the problem of lifetime and security for OLSR. In this work, we address the impact of clustering on QoS, and how this can affect multimedia applications in ad hoc networks.

2.7.2 Security in MANETs

Unfortunately, QoS-OLSR is susceptible to attacks that can be launched by malicious nodes against the network. Many attacks that can be launched against QoS-OLSR protocol were identified. These attacks can degrade the network performance by isolating some head nodes and clusters. The attacks are classified into two categories: Attacks by normal nodes and attacks by MPRs. Several approaches are proposed to defend against these attacks. [14–23]

To secure the network against collusion attack, authors in [22] suggest to alter the existing Hello message by adding the 2-hop neighbors list. Hence, a node can identify if a forged Hello message was sent to one of its neighbors have. One of the drawbacks of this approach is that false alarms may be prompted when links between the nodes break if the nodes are highly mobile.

In [23], they use the FMS-OLSR (Forced MPR Switching OLSR) algorithm to detect collusion attack. When node X sends a HELLO message, it verifies the number of nodes in its MPR set. If the number is 1, it verifies its 1-hop neighbor set. If node X has more than 1 neighbor, it adds the MPR to an AvoidanceSet after waiting for the duration of an avoidance delay. The entries are deleted from AvoidanceSet after some determined delay.

In the node isolation attack, MPR node avoids sending its TC message in order to prevent its MPR selectors to be reachable by other nodes in the network. A countermeasure is proposed in [14] in order to defend against this attack. The method consists of two phases: In the first phase, each node checks whether its MPR node sends its TC message. In the second phase, a new field named Request-value was included in the Hello message in order to avoid the impact of this attack.

Authors in [15] use a trust analysis technique to stop a malicious node from isolating other nodes in the network. Every node in the network should send a Hello message during a 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.

TOGBAD, a centralized topology graph approach, is used in [16] to protect the network against blackhole attack. The graph is created and the number of neighbors of a node is calculated. Then, this number is compared to the originator's number of neighbors. If there is a major difference between the two numbers, an alarm is triggered.

A malicious node generates control messages that state an incorrect set of links. An attacker can drop existing links or add non-existing links. The link spoofing attack is defended in [19], where 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. Moreover, SA-OLSR (Security Aware OLSR) is used in [18] to detect link spoofing attack.

The attacking node sends TC message which claim to have another node's identity. Authors in [17] 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 using a fake identity. The countermeasure proposed follows the following protocol:

- The node checks the timestamp of the signature message and place it in memory.
- The node checks the signature of the TC message.
- The message is accepted and processed based on the standard OLSR specifications for the message type when the node finds that the timestamp is fresh and the signature is valid. If the message proved to be fraudulent, it will be dropped.

When launching the Advertised Neighbor Sequence Number (ANSN) attack, the attacking node listens to a TC message addressed from a node X and records its ANSN. It then sends a TC with a wrong originated address of that node with an ANSN value greater than the recorded one. This attack is detected in [20] when the fraudulent TC transmits an ANSN that is much higher than that actual TC message received from the node X.

The wormhole attack is composed of two attackers, which generate a link between them called wormhole tunnel. The first attacker receives packets from its neighbors, copies, and sends them to the other attacker through the tunnel. So after this node receives the packets, it displays them into the network. In [18], they calculate the delay between the time a node sends a TC (*Tsent*) and the time the node receives the ACK*TC* (*Treceived*). The difference between *Treceived* and *Tsent* must be less then a threshold value; else, the node will be considered as malicious.

Moreover, authors in [21] have defended wormhole attack by computing the travel distance. If this distance is larger than the transmission range, the message may have tunneled through the wormhole.

All the presented approaches have only addressed the attacks launched against the OLSR model. In this work, we identify the attacks that can be launched against the QoS-OLSR protocol and propose different detection approaches.

2.8 Conclusion

We presented in this chapter the ad hoc network characteristics, MANET and its security concerns, cooperative watchdog approach and bayesian rule function that form our thesis. Then, we presented the related works in the areas of clustering and detecting attacks in MANETs. We showed that the previously proposed clustering algorithms select a large number of MPR nodes, which can shorten network lifetime, and hence affect nodes' available bandwidth and increase the probability of channel collision. Moreover, the existing clustering approaches consider only nodes' bandwidth during MPRs selection without considering other Quality of Service metrics such as energy and connectivity. Regarding the attacks that can be launched against the QoS-OLSR protocol, nodes may act maliciously and lead to network disruptions that can eventually threaten the ultimate goal of the protocol. The existing approaches only detect attacks that can be launched against the OLSR protocol. Moreover, nodes mobility and collisions reduces the accuracy of the detection results and leads to many false positives and false negatives decisions.

Chapter Three

A Cluster-Based Model for QoS-OLSR Protocol

3.1 Introduction

The problem of clustering in ad hoc networks is introduced in this chapter. Many models have been previously proposed for clustering in MANET [1,4,5,8,9,11,13]. However, the approaches select a large number of MPR nodes, which can shorten network lifetime. Such a problem can affect nodes' available bandwidth and augment the possibility of channel collision especially in large networks. In other approaches [3,7], MPRs are selected based on nodes' bandwidth without considering other metrics such as energy and connectivity. Our proposed approach is a new cluster based QOLSR algorithm that considers a tradeoff between percentage of MPRs and QoS metrics. The goal is to form clusters and reduce the percentage of MPRs, while satisfying the QoS metrics, thus decreasing traffic overhead, delay and channel collision, and increasing cooperation in the network. The rest of this chapter is organized as follows: Section 3.2 introduces the cluster-based QoS-OLSR model and presents an illustrative example in order to show how the clustering approach works. Section 3.3 evaluates the efficiency of the cluster-based QoS-OLSR model. Finally, section 3.4 concludes the chapter.

3.2 Cluster-Based QoS-OLSR Model

In this section, we present the Quality of Service metric function of our models that are bandwidth, connectivity index, and residual energy. Implementing these concepts will help us to prolong network lifetime without sacrificing QoS. Our approach is recapitulated as follows: First, optimal cluster heads are elected using the cluster head election algorithm. Second, MPR nodes are selected by those elected head using the MPR selection algorithm, which will form a connected network.

3.2.1 Quality of Service Metric Models

We introduce the cluster based QoS-OLSR approach in order to have a better performance and quality of service. In the classical QOLSR, each node chooses its own MPR according to maximum bandwidth and minimum delay. In this paper, the classical QOLSR will be known as "without clustering" under different models according to the QoS metric used. The models are presented in Table 1. Note that throughout this paper the QOLSR will be called as "without clustering BOLSR".

Our proposed model is known as "with clustering" and it has four different models according to the different QoS metrics. In the modified approach, the network is divided into clusters by selecting the set of optimal head clusters that can serve as MPR node. Heads are elected according to the highest QoS Metric value. After the head election is done, each head will elect the MPR nodes according to nodes' QoS Metric function that are based on the QoS parameters. By introducing clustering to the classical QOLSR, we are distributing the energy consumption and thus increasing the network lifetime. In Table 1, we define the Quality of Service Metric function of our four models with the new metrics and the notations used.

Table 1: Quality of Service Metric

Notations and Quality of Service Metric Function
Let i be a node in the network. Let define:
QoS(i) = Quality of Service Metric of a node
BW(i) = Available bandwidth of i
N(i) = Neighbors of i
RE(i) = Residual energy of i
Bandwidth Model (B-OLSR)
1 QoS(i) = $BW(i)$;
Proportional Bandwidth Model (Proportional B-OLSR)
2 QoS(i) = $\frac{BW(i)}{N(i)}$;
Bandwidth and Energy Model (BE-OLSR)
3 QoS(i) = $BW(i) \times RE(i)$;
Proportional Bandwidth & Energy Model (Prop. BE-OLSR)
4 QoS(i) = $\frac{BW(i)}{N(i)} \times RE(i)$

3.2.2 Cluster Head Election

An election algorithm is modeled in order to elect the optimal heads and divide the network into distinct clusters. The algorithm works as follows: each node in the network votes for one of its neighbor nodes having the largest Quality of Service value. Note that, if certain node has the largest local QoS metric value, it can vote for itself to be the cluster head. This method provides a 1-hop clustering model where every node is only 1-hop distant from its elected cluster head.

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

At the end of the cluster head election process, the designated head nodes act as MPRs for their electors. This method should be altered by including a flag in order to show which node was assigned as a cluster head. In addition, a flag should be included presenting that a neighbor was assigned as a head. Thus, each node will be able to know which node each of its neighbors has elected. All the neighbors will receive information about head election before changing their local information.

3.2.3 MPR Nodes Selection

After being designated, the cluster heads are responsible of selecting a group of optimal MPRs. The group of MPRs combines the clusters into a connected graph. Selecting MPR

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

nodes in between the 1-hop cluster heads is not required because they can reach each others directly since they are neighbors. In addition, it is not needed to select any MPR in between 2-hop cluster heads that are connected to 1-hop cluster heads. Therefore, only the 3-hop cluster heads problem should be covered consistently.

To cover the 2-hop cluster heads, we compute the MPR nodes in MPR-Part II:

```
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 $QoS(k)$ all the nodes in $CH_2(k)$
      reachable from $x$.
```

Finally, the 3-hop cluster heads are selected in MPR-Part III. In this case, 2 MPRs are needed in order to reach any 3-hop cluster head.

```
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 $CH_3(k)$
        that can be reached from $x$.
```

The correctness of this part should be verified properly. Suppose that MPR node x is selected by the cluster head k, then MPR node y should be selected by cluster head l in order to assure that heads k and l are connected.

We should state that the proposed approach is competitive. Therefore, each cluster head must have different ways in order to connect to its neighbor heads using the MPR selection algorithm stated in Part II or the one stated in Part III.

3.2.4 Illustrative Example

An illustrative example is given to show how the head election and the MPR selection algorithms work. Figure 3 presents a network with twenty nodes and Table 2 gives the Quality of Service Metric value of each node 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 connectivity index and multiplied by bandwidth. Once the Hello messages are broadcasted, a node votes for its neighbor with the maximal Quality of Service metric. Referring to the Head Election Algorithm, nodes: 3, 4, 5, and 15 are elected as head clusters (MPRs).

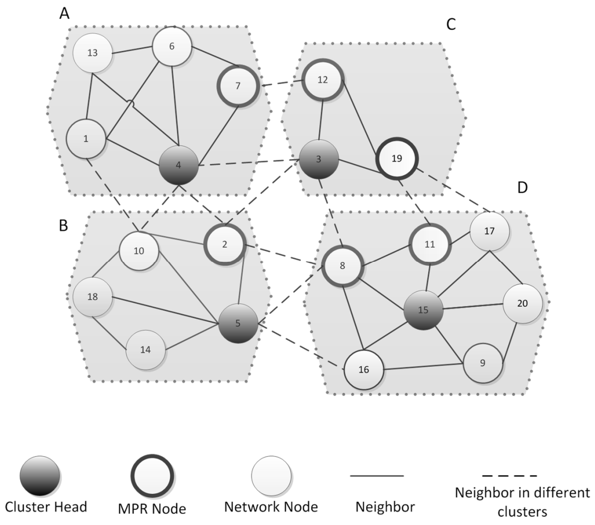

Fig. 3: Network example

Table 2: The Quality of Service Metric Using the Proportional BE-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

After being elected, the cluster heads select the MPRs nodes that connect all heads together. We will consider node 15 in cluster D to illustrate our example. First, discovering the neighbor cluster heads for node 15 is required. Referring to MPR-Part I, we need to find the 1-hop away cluster head, $CH1$, the $2-hop$ away cluster head, $CH2$, and the 3-hop away 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 choose only node 11 as MPR node and, likewise, head node 3 chooses node 19 as MPR node. Similarly, the optimal path with $\{$nodes 8 and $3\}$ to reach cluster head node 4 is found.

3.3 Simulation Results

Matlab-8.0 was used to simulate with clustering and without clustering QOLSR to compare between the novel cluster-based QOLSR and the classical one (without clustering). The simulation is divided into five subsections. The first subsection shows the percentage of selected MPR nodes in the two scenarios: with clustering and without clustering models. The second part presents the percentage of alive nodes in these models. The third subsection shows the path lengths in the models that represent delay in the network. Finally, the bandwidth average difference for the models is presented to show the quality of service in the network. The simulation parameters are summarized in Table 3.

Table 3: Simulation Parameters

Parameter	Value
Simulation area	500×500 m
Number of nodes	Between 30 and 70
Transmission range	125 m
Residual energy	Random value in $[500..550]$ Joules
Packet Size	1 kb
Energy Per Packet	0.0368 J
Idle Time	Random value in $[0..1]$
Link Bandwidth	2Mbps
Available Bandwidth	$Idle\ Time \times Link\ Bandwidth$

3.3.1 Percentage of MPR nodes

In Figure 4, it is significant that the clustered models decrease the percentage of selected MPRs. The cluster heads are included in the set of MPRs and behave as specialized MPR

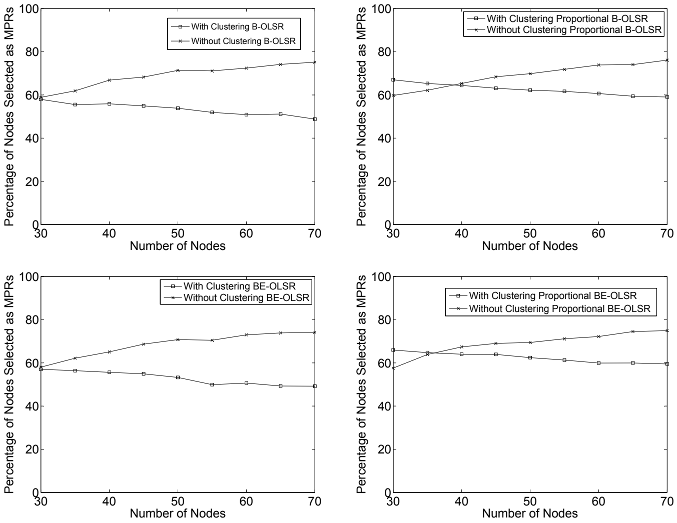

Fig. 4: Percentage of MPR Nodes: (a) B-OLSR (b) Proportional B-OLSR (c) BE-OLSR (d) Propor-tional BE-OLSR

nodes. In fact, the outcome is ordinary because a small number of special nodes are responsible of selecting the MPR nodes. Therefore, clustering techniques must decrease the congestion level and must be more convenient for large networks.

Comparing the four models, obviously in Figure 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.

- Energy per Packet.

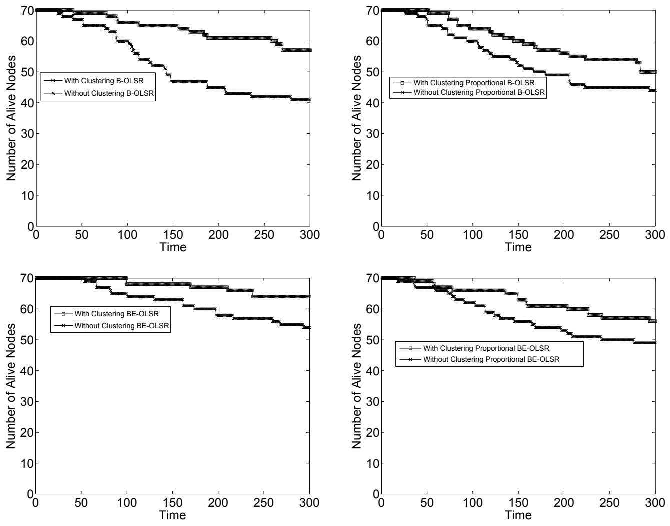

Fig. 5: Percentage of of alive nodes over time: (a) B-OLSR (b) Proportional B-OLSR (c) BE-OLSR (d) Proportional BE-OLSR

In Figure 5, we show the percentage of alive nodes and how the energy drain for a 70 nodes network for all the models. 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 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 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 in Figure 5 prolong the network lifetime compared to the without clustering models because we have less number of selected MPRs. It is significant that the with clustering proportional B-OLSR (see Figure 5,a) has the worst network life time among all clustered models, whereas, with clustering BE-OLSR shows the best result 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. Also, the concept of clustering helped to reduce the energy consumption by selecting a set of specialized nodes.

3.3.3 End-to-End Average Delay in the Network

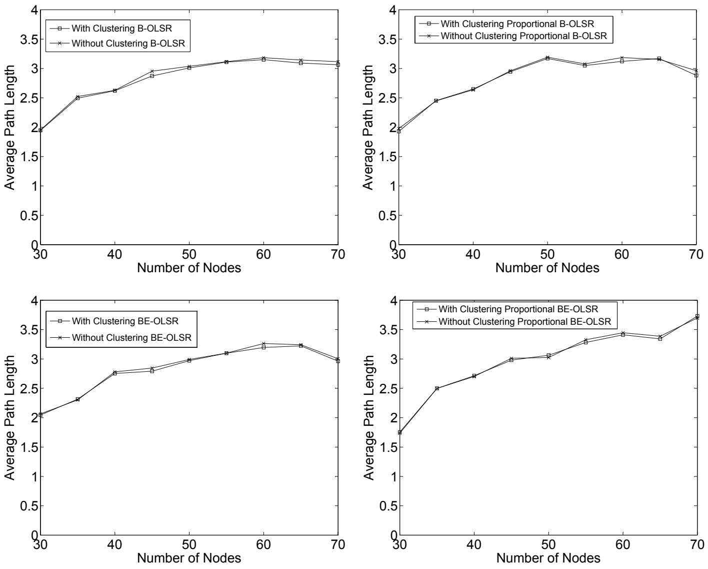

Fig. 6: Average Path Length with and without Clustering: (a) B-OLSR (b) Proportional B-OLSR (c) BE-OLSR (d) Proportional BE-OLSR

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 “with clustering” and “without clustering”. 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 both models.The "with Clustering" and "without Clustering" Models showed similar results. Thus, to differentiate between the performances of the models, another criterion should be used. According to the results of the simulation, the BE-OLSR model with clustering gives better performance for the network lifetime and should be favored over other cluster based models.

3.3.4 The Bandwidth Average Difference

Table 4: Bandwidth Average Difference

Models	Transmission Ranges		
	100	150	200
without clustering B-OLSR	0%	0%	0%
with clustering B-OLSR	0%	0%	0%
without clustering Prop. B-OLSR	10.55%	3.08%	4.9%
with clustering Prop. B-OLSR	10.6%	4.22%	2.59%
without clustering BE-OLSR	0.04%	0.15%	0.02%
with clustering BE-OLSR	0.09%	0.19%	0.09%
without clustering Prop. BE-OLSR	9.17%	5.88%	4.89%
with clustering Prop. BE-OLSR	9.24%	6.2%	3.42%

The bandwidth average difference is one of the aspects that we can consider in our models. It is the percentage average of the difference between the optimal bandwidth and the bandwidth currently available in the network. As the percentage decrease, the quality of service in the network improves. Table 4 represents the percentage average difference for a 70 nodes network for the two scenarios: without clustering and with clustering. According to this table, the with clustering B-OLSR and without clustering B-OLSR have zero average difference because the optimal path is chosen according to the optimal bandwidth path. Other clustered approaches showed slightly more percentage average difference, especially the with Clustering BE-OLSR which is more by less than 0.1% , but it have better network lifetime and delay. Thus, it should be preferred over the B-OLSR. Choosing the best model regarding the percentage average difference, depends on the application. If the application is related to multimedia services that are error tolerated and delay not tolerated, the percentage average difference loses its importance compared to delay. Whereas in data services applications, errors are not acceptable so percentage average difference should be considered.

In Summary, based on the results in the above subsections, we are able to show that the novel cluster-based approaches are able to prolong network lifetime by selecting less number of MPRs, thus decreasing traffic overhead, delay, channel collision, and increasing cooperation in the network. On the other hand, comparing the clustered models with each others, we conclude that the energy is an essential metric that must be considered while selecting the MPRs. The cluster-based BE-OLSR model showed a marginal impact on average difference, whereas a large impact on the network lifetime. Therefore, the cluster-based approach must be preferred over the classical one taking into consideration nodes' energy.

3.4 Conclusion

In this chapter, we proposed a cluster based QoS-OLSR protocol which considers the tradeoff between prolonging the ad hoc network lifetime and QoS assurance. We may accomplish the following by (1) decreasing the percentage of Multi-Point Relay (MPR nodes) without sacrificing the QoS and (2) observing the connectivity index, residual energy level, and bandwidth of the MPRs. Head and MPRs selection algorithms are first presented. Moreover, a comparison between the "without clustering" and "with clustering" models was presented. The comparison addressed the percentage of MPR nodes, percentage of alive nodes in the network, path length which reflects the delay and quality of service. Simulation results showed that the "with clustering" models, in general, lead to a better results compared to the classical QOLSR (i.e., without clustering). Our model was able to reduce the number of MPR nodes by 27%. Moreover, the "with clustering" BE-OLSR considered the tradeoff between delay, network lifetime and QoS. The model shows much better results in network lifetime; the number of alive nodes increased by 16%. In addition the "with clustering" model shows better results in path length and very close result in terms of bandwidth with average difference of 3%.

Chapter Four

Detecting Attacks in a Mobile Cluster-Based QoS-OLSR Protocol

4.1 Introduction

This chapter tackles the problem of attacks against our clustering QoS-OLSR protocol proposed in chapter 3. According to this protocol, normal and MPR nodes may act maliciously and lead to network disruptions that can eventually threaten the ultimate goal of the protocol. As a solution, we identify the attacks that can be launched against our QoS-OLSR model and we propose a cooperative detection approach that is based on cooperation between watchdogs. Then, we add Bayes rule to our cooperative approach in order to improve the detection rate and reduce false positives. The rest of this chapter is organized as follows: Section 4.2 identifies the security attacks in a QoS-OLSR network and presents an illustrative example to show how the proposed model works. Section 4.3 identifies the attacks that can be launched against the cluster-based model. Section 4.4 proposes the bayesian cooperative detection approach that is used to detect the attacks, improve the detection and reduce the false rates. Section 4.5 evaluates the performance of the the bayesian cooperative detection approach. Finally, section 4.6 concludes the chapter.

4.2 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 needed to explore 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.

4.2.1 Illustrative Example: QoS-OLSR

To review the cluster head election and the MPR selection presented, figure 7 presents a network involving twenty nodes:

Table 5 gives the Quality of Service Metric value of each node (refer to Table 5). Once Hello messages are broadcasted, a node votes for its neighbor with the maximal QoS Metric value. Nodes 3, 4, 5, and 15 were elected as head nodes.

After being elected, the cluster head nodes select the MPR nodes that connect all heads together. Node 15 in cluster D is considered to illustrate the example. First, discovering the neighbor cluster heads for node 15 is required. The 1-hop cluster head, CH1, the 2-hop

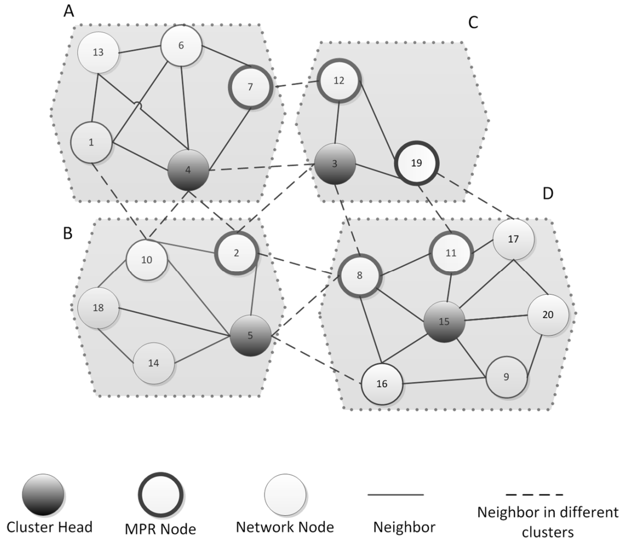

Fig. 7: Attack Network example

Table 5: 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

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 choose only node 11 as an MPR node and, likewise, head node 3 chooses node 19 as an MPR node. Similarly, the optimal path {node 8, node 3} to cluster head node 4 was found.

4.2.2 Identifying the Attacks

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

- Hello Message: The Hello messages are transmitted periodically, each time the network is created and the nodes change places. They are used in order to gain information about the node's neighbors. These messages are responsible of sensing neighbors and selecting MPRs. Every node's Hello message includes its own address, a list of its 1-hop neighbors and a list of its MPR set.
- TC Message: MPR nodes must generate a TC message periodically in order to spread topology information each time the network topology changes. The aim of TC messages is to be distributed throughout the network and they are forwarded only by MPR nodes. A set of bi-directional links between each node and its neighbors is constituted using TC message.

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.

4.2.2.1 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 launched by a normal node that will send TC messages declaring that it has an MPR node's identity. In figure 7, consider that node 16 sends TC messages, claiming to have the identity of another node (node 12).The node states incorrect links to the network. Nodes 15 and 5 will predict reachability to node 12 via 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 7 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.

4.2.2.2 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 7, 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 8 that node 15 broadcasts its Hello message.

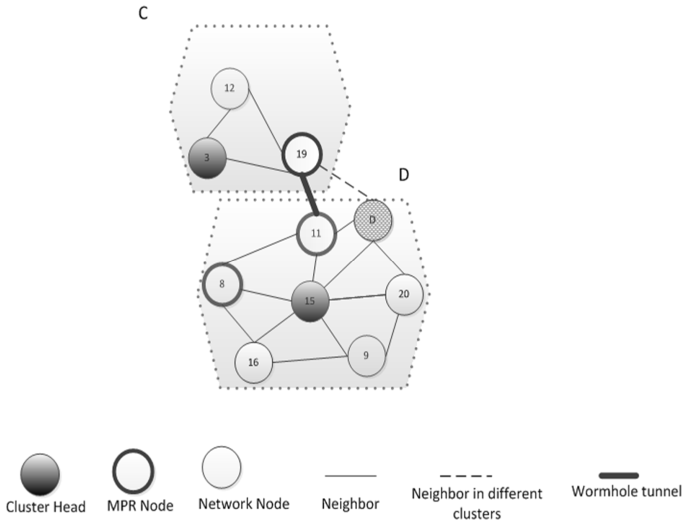

Fig. 8: Wormhole Attack

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 select each other as MPRs. This will lead to an exchange of TC messages and data packets through the wormhole tunnel.ăThis 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, identity 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.

4.3 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.

4.3.1 How watchdog is working

4.3.1.1 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.

4.3.1.2 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.

4.3.2 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.

4.3.2.1 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.

4.3.2.2 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 [22], dictates the performance of the candidate node depending on its type Θ. By observing the performance of the sender, the watchdogs can compute the posterior belief evaluation function $\mu(\theta_i|\alpha_i)$ using the following Bayes' rule (refer to equation 9):

$$\mu(\theta_i|\alpha_i) = \mu(\theta_i)P(\alpha_i|\theta_i)/\Sigma_{\theta_i\varepsilon\theta}\mu(\theta_i)P(\alpha_i|\theta_i) \tag{9}$$

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 calculated as follows:

$$P(Attack|\theta_i = M) = E_m \times O + F_m(1 - O) \tag{10}$$

$$P(Attack|\theta_i = N) = F_m \tag{11}$$

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 intruderŠs 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):

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, 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
```

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'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.

4.4 Simulation results

Matlab-8.0 was 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 6.

Table 6: 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

4.4.1 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 9 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.

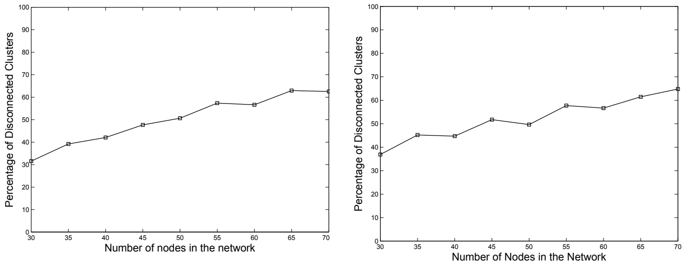

Fig. 9: Percentage of disconnected clusters with 10% attackers: (a) Identity Spoofing Attack (b) Wormhole Attack

Figure 10 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.

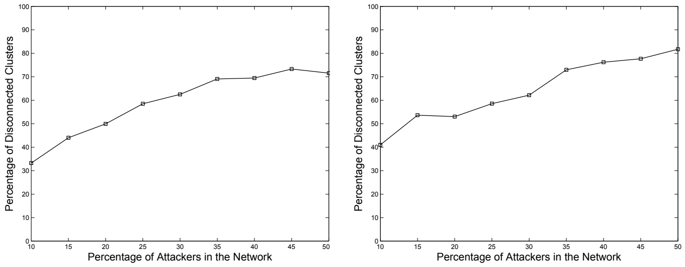

Fig. 10: Percentage of disconnected clusters with different percentage of attackers: (a) Identity Spoofing Attack (b) Wormhole Attack

4.4.2 Probability of Detecting Attacks and False Rate With Different Percentage of Attackers

Figure 11 shows the percentage of detected attacks. The detection percentage is simulated along with the corresponding false detection percentage (in figure 12) 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:

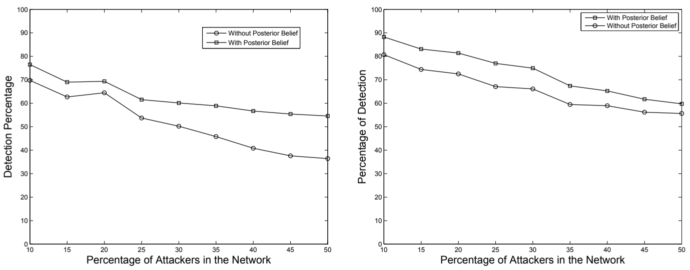

Fig. 11: Detection percentage with different percentage of attackers: (a) Identity Spoofing Attack (b) Wormhole Attack

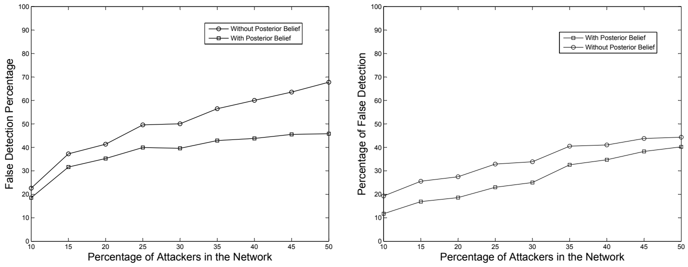

Fig. 12: False detection percentage with different percentage of attackers: (c) Identity Spoofing Attack (d) Wormhole Attack

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.

4.5 Conclusion

In this chapter, we have tackled the problem of malicious nodes in Mobile Ad Hoc Networks. We showed how these nodes can lead to network disruptions that can eventually threaten the ultimate goal of the protocol. As a solution, we identified the attacks that can be launched against our QoS-OLSR model and we proposed a bayesian cooperative detection approach that is able to (1) improve the watchdogs' detection by using cooperation and (2) reduce the false detection rates by using Bayes function. The detection is done first using the an aggregation function where all the watchdogs cooperate with each others in order to make the final decision, and then by adding posterior belief function to this approach.

Simulation results show that the use of the Bayes' rule function along with the cooperative watchdog model improves the detection rates(7% to 15%) and reduces the false positives.

Chapter Five

Conclusion

The multimedia QOLSR was proposed to handle multimedia applications over ad hoc networks. The MPRs are selected based on nodes bandwidth and delay without considering nodes' residual energy which can affect network lifetime. As a solution, we proposed in chapter 3 different models based on the clustering concept with different QoS metric. Such models will reduce the channel collision and increase the throughput. The head and MPRs selection algorithms are presented. Moreover, a comparison between the "without clustering" and "with clustering" models was presented. The comparison addressed the percentage of MPR nodes, percentage of alive nodes in the network, path length which reflects the delay and quality of service. Simulation results showed that the "with clustering" models, in general, lead to a better results compared to the classical QOLSR (i.e., without clustering). Moreover, the "with clustering" BE-OLSR was able to deal with the tradeoff between network lifetime, delay and QoS. The model shows much better results in network lifetime and path length and very close result in terms of bandwidth with average difference of 3%.

However, the cluster-based models are highly vulnerable to security attacks. We have identified two attacks in chapter 4: Identity spoofing and wormhole attacks. These attacks can degrade the network performance by isolating some head nodes and clusters. Thus, a bayesian cooperative detection technique was proposed in order to detect these attacks. As we have shown in chapter 4, the percentage of disconnected clusters has reached 80% with 50% of the nodes being malicious. To deal with this issue, we have presented a novel detection approach based on cooperation between watchdogs. The detection was then enhanced by adding posterior belief function. Our simulation results show that posterior belief function increases the true detection and decreases the false detection rates. 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. As for the wormhole attack, 88% of the malicious nodes were detected using the cooperative watchdog-based model with the posterior belief function; whereas, around 80% of the attackers were detected without the posterior belief function.

In summary, the main contributions of our thesis are:

- Reducing the percentage of MPRs while maintaining the Quality of Service.
- Prolonging the network lifetime and reducing the energy consumption by selecting a set of specialized nodes.
- Identifying attacks that can be launched against our models and detecting the malicious nodes in the network

- Improving the detection rate by using bayesian cooperative watchdog model and reducing the false detection rates

This thesis presented the problem of clustering in Mobile Ad Hoc Networks and identified malicious nodes that can launch attacks against the network. Many research topics emerging from this work may be continued. In fact, malicious nodes in the network can perform other types of attacks against our QoS-OLSR network(e.g., add link and drop link attacks). These nodes would degrade the network performance considerably. Moreover, choosing all the nodes to serve as watchdogs consumes a lot of time and energy. Therefore, there should be a tradeoff between the number of monitors and the time/energy consumption. Our future work will be identifying and detecting other attacks that can harm the network, and taking different percentages of watchdogs that are responsible of detecting the malicious action in order to save time and energy consumption.

The following is the list of publications derived from the thesis work:

- "Detecting attacks in QoS-OLSR protocol".IWCMC 2013: 1126-1131
- "A cluster-based model for QoS-OLSR protocol".IWCMC 2011: 1099-1104

Bibliography

[1] F. N. Abdesselam, B. Bensaou, and J. Yoo, “Detecting and Avoiding Wormhole Attacks in Optimized Link State Routing Protocol”, in *IEEE WCNC*, 2007, pp. 3119-3124.

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

[3] K. Agha and S. Martin, “Routing in Mobile Ad Hoc Networks”, in *Wireless Network Design: Optimization Models and Solution Procedures*, J. Kennington, E. Olinick, and D. Rajan, Springer, 2011, vol. 158, ch. 9, pp. 199-217.

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

[5] H. Badis and K. A. Agha, “QOLSR, QoS routing for ad hoc wireless networks using OLSR”, *European Transactions on Telecommunications*, vol. 16, pp. 427-442, 2005.

[6] 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)*, 2006, pp. 14-19.

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

[8] 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 *Proc. of the 7th IFIP Annual Mediterranean Ad Hoc Networking Conference*, 2008, pp. 97-108.

[9] 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.

[10] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, October 2003.

[11] M. Gerla, "Ad Hoc Networks: Emerging Applications, Design Challenges and Future Opportunities", in *Ad Hoc Networks: Technologies and Protocols*, P. Mohapatra and S. Krishnamurthy, Springer, 2006, ch. 1, pp. 1-22.

[12] P. Goyal, V. Parmar, and R. Rishi, MANET: Vulnerabilities, Challenges, Attacks, Application, In *IJCEM International Journal of Computational Engineering and Management*, vol. 11, pp. 32-37, 2011.

[13] F. Hong, L. Hong, and C. Fu, "Secure OLSR", in *19th International Conference on Advanced Information Networking and Applications*, 2005.

[14] J. Hortelano, J.C. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs", in *IEEE ICCW*, 2010.

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

[16] B. Kannhavong, H. Nakayama, and A. Jamalipour, “SA-OLSR: Security Aware Optimized Link State Routing for Mobile Ad Hoc Networks”, in *IEEE Communications Society*, 2008, pp. 1464-1468.

[17] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, “A study of a routing attack in OLSR-based mobile ad hoc networks”, in *International Journal of Communication Systems*, vol. 20, no. 11, pp. 1245-1261, March 2007.

[18] T. Kunz, “Energy-Efficient Variations of OLSR”, in *Proc. of the International Wireless Communications and Mobile Computing Conference*, 2008, pp. 517-522.

[19] 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*, 2007, pp. 1253-1259.

[20] 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*, 2004, pp. 480-491.

[21] B.A. Olshausen, E.W. Weisel, and M.D. Petty, “A Bayesian Approach to Assessing Expected Utility in the Simulation Decision”, in *SCSC ’13 Proceedings of the 2013 Summer Computer Simulation Conference*, 2013.

[22] 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, 2008, pp. 608-612.

[23] 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*, 2007, pp. 1043-1049.

[24] R. Ramanathan and J. Redi, “A Brief Overview of Ad Hoc Networks: Challenges and Direction”, in *IEEE Communications Magazine*, 2002.

[25] 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)*, 2008, pp. 1-7.

[26] 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)*, 2007, pp. 202-207.

[27] 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.

[28] 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*, vol. 2, no. 3, pp. 18-29, 2010.

[29] 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.

[30] L. Villasenor-Gonzalez, G. Y. Ge, and L. Lament, “HOLSR: a Hierarchical Proactive Routing Mechanism for Mobile Ad Hoc Networks”, *IEEE Communications Magazine*, vol. 43, pp. 118-125, 2005.