Computational Research Progress in Applied Science & Engineering

ISSN 2423-4591

CRPASE Vol. 05(03), 71-78, September 2019

Introspection of Availability in Ad Hoc Networks

David TSHIBANGU KADIATA*

Faculty of Computer Science, Network Department, University of Kamina, RD Congo

Keywords

Ad hoc network,
Security,
Availability,
Routing.

Abstract

A mobile ad hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links whose union forms an arbitrary graph. Such a network does not require fixed infrastructure and represents an attractive option for spontaneously connecting mobile terminals. However, this type of network is particularly vulnerable, particularly at the network layer, to attacks aimed at the availability of services. The traditional mechanisms of security based on a fixed infrastructure are not suitable. In this bibliography report, we will present a study of new ad hoc network routing protocols to support availability. Therefore, it is an analysis of the protocol specifications in terms of availability to be able to propose an applicable availability policy in the context of this type of network.

1. Introduction

In recent years, the need for more mobility and to be able to access shared data or exchange information at any time, using mobile devices (mobile phones, PDAs, laptops and etc.) has spread the notion of a network without infrastructure, or ad hoc networks.

Ad hoc networks have an arbitrary graph architecture in which a set of wireless nodes temporarily forms a network without the aid of a centralized infrastructure or administration. According to the definition of the IETF [1], an Ad hoc mobile network is an autonomous system of mobile routers connected by wireless links. Ad hoc networks have several characteristics: a dynamic topology, lack of infrastructure, variable capacity of links and a limited source of energy. On the basis of these characteristics, it is possible to reduce the problems and difficulties that this type of network may pose, in particular problems of security.

Ad hoc networks are beginning to gain traction in different areas of application. It is in the field of routing that there has been a lot of research. There are many other areas to explore and problems to solve or where existing solutions need to be improved. Quality of service (QoS) problems, battery problems and safety problems are among them.

In ad hoc networks, security depends on several parameters (authentication, confidentiality, integrity, non-repudiation and availability) and concerns two aspects, the security of the routing and the security of the data. Both aspects have some vulnerabilities and are vulnerable to multiple attacks.

The internship that was entrusted to me went to a mining company in Lubumbashi, under the responsibility of Serge BADILA. The aim of the internship is to analyze the specifications of the routing protocols in mobile ad hoc networks (MANET) and see if they have "good properties" in terms of availability.

In addition to this introduction, this bibliography report contains six sections. In section 2, we list the technical terms used in this document. In section 3, we discuss some routing protocols and the vulnerabilities and attacks to which ad hoc networks can be exposed. Then in section 4, we introduce the concept of communication group. Next, we present a summary of the main security models proposed to address security issues in ad hoc networks, including the security properties in routing protocols, the concept of reputation, and the availability property in section 5. Section 6 discusses some techniques for evaluating non-functional properties. Finally, our conclusion is presented in section 7.

2. Terminology

The following terms are used in this literature review, but may be used differently elsewhere. A node is a device with a wireless network interface that participates in routing in a mobile ad hoc network. It can be mobile or fixed, and can also be part of another network. It is important to note that a node can be a point of entry to a subnet, or just a simple mobile device such as a mobile phone. A *source* or *transmitter node* is a node that is the source of a data packet, sent to any recipient node.

A node A is said *neighbor node* of another node B when it is at a jump of a node B and there is a direct path from A

* Corresponding Author:
E-mail address: davidkadiata@gmail.com– Tel, (+243) 972817695

Received: 18 June 2019; Accepted: 7 September 2019

to B. If the destination node is not a node next to the sending node, the data packet will have to follow a path composed of several nodes called intermediate nodes.

A *routing packet* is a packet used by a routing protocol to transmit routing information. Such information includes messages concerning the mechanism of road maintenance, signaling, etc. *Road request, road reply and road error* messages are used in reactive protocols. The following section details how these routing packets are used and presents different types of protocols in ad hoc networks.

An Ad hoc network can be modeled by a graph Gt = (Vt, Et) Grammar: Or, where Vt represents the set of nodes of the network and models all the connections between these nodes. If e = (a, b) ∈Et, that means that the nodes *a* and *b* can communicate directly at time *t*. For example, Figure 1 shows an Ad hoc network of ten mobile nodes as a graph.

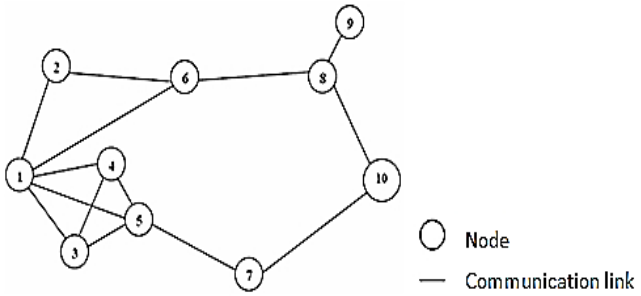

Figure 1. The modeling of an Ad hoc network.

The topology of the network can change at any time, so it is dynamic and unpredictable so that the disconnection of the nodes is very frequent as shown in Figure 2.

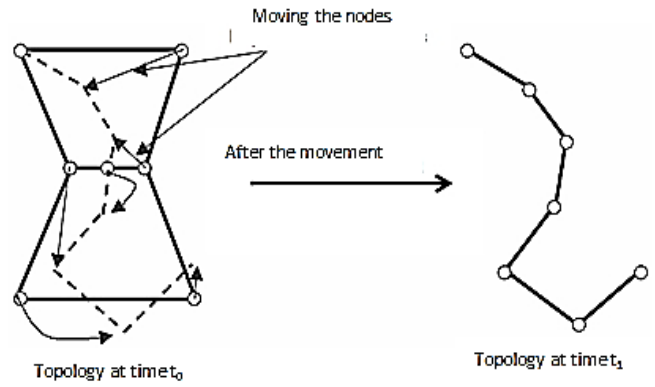

Figure 2. The topology change of ad hoc networks.

3. Routing and Attacks in Ad Hoc Networks

Routing is a major area of research in ad hoc networks because the characteristics of ad hoc networks pose many new challenges compared to traditional cable networks. Existing protocols are not suitable for ad hoc networks. Thus, many solutions using various methods have been proposed and studied recently.

3.1. Routing in Ad Hoc Networks

In this section, we present a synthesis of research articles in the field of routing in ad hoc wireless networks. Ad hoc network routing protocols are based on two operating models: proactive protocols and reactive protocols. They can be differentiated by the method used to discover the path between the sending node and the destination node. To maintain their routing table, proactive protocols regularly check for the different routes available in the network. When a packet has to be transmitted, its route is then known in advance and can be immediately used. Reactive protocols undertake the search for a route only before transmitting a packet.

Figure 3 shows a taxonomy of routing protocols for ad hoc networks [2]. These protocols are differentiated first by the level of implication of the nodes in the routing. They are called uniform if all the nodes of the network play the same role for the function of routing. On the other hand, they can be non-uniform if a hierarchical structure is given to the network and only certain nodes provide routing. Thus, in the neighbor selection protocols, each node sub-processes the routing function to a subset of its direct neighbors. For partitioned protocols, the network is divided into zones in which routing is provided by a master node.

Uniform routing protocols can also be grouped according to the data they use to perform their task. In topology-oriented protocols (Link state), each node uses as data the state of its connections with its neighbor nodes; this information is then passed to the other nodes to give them a more accurate knowledge of the network topology.

The destination-oriented protocols (vector distance) maintain for each destination node information on the number of nodes that separate them (the distance) and possibly on the first direction to be taken to get there (the vector).

With a proactive protocol, the roads are available immediately. However, the traffic induced by the control and update messages of the routing tables can be important and partly useless. In addition, the size of the routing tables increases linearly as a function of the number of nodes. By contrast, in the case of a reactive protocol, no control message loads the network for unused routes. But for the latter, the installation of a flood road can be expensive and cause significant delays before the opening of the road.

In terms of performance, the topology-oriented protocols (Link state) converge faster than the destination-oriented protocols (vector distance). However, in the case of high mobility networks, the traffic induced by the frequent control messages is often penalizing.

In general, the "flat" proactive routing protocols, whether destination-oriented or topology-oriented, are not suitable for networks of large size (number of nodes greater than 100) and high mobility. A first solution for this type of network is the use of so-called hierarchical protocols (such as HSR, FSR, etc.). A second solution may be to use a reactive protocol. This type of routing makes it possible to manage very large networks if the mobility of the nodes remains weak; traffic remains low if it is directed to a small number of destinations. On the other hand, the calculation of a route on demand is very penalizing for multimedia traffic requiring guarantees in terms of quality of service.

At present, no routing protocol in ad hoc networks has been adopted within the IETF [2]. The different protocols shown in Figure 3 are still drafts and remain under development and specification. Some proposals have been dropped and the most successful ones are AODV, DSR and OLSR.

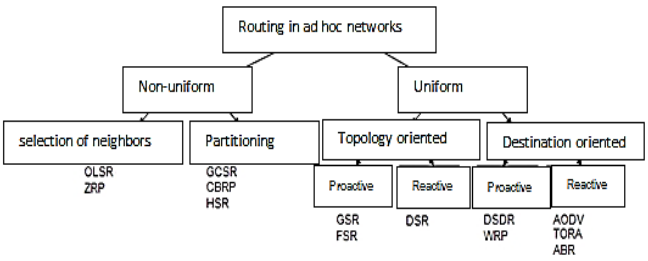

Figure 3. Taxonomy of routing protocols for ad hoc networks.

3.2. Attacks Related to Routing Protocols

In ad hoc networks, attacks against routing protocols involve modifying protocols so that traffic passes through a specific node under the control of an attacker. An attack can also be aimed at preventing the formation of the network by causing the nodes to take incorrect routes, and more generally to disrupt the topology of the network.

Routing attacks are classified into two main categories: incorrect generation of traffic and bad traffic relaying1. Sometimes these correspond to local problems of the nodes that are not due to an attack, for example malfunctioning. A node, the energy of an exhausted device, or interference of radio waves.

If there is no control over the origin and integrity of the ad hoc network routing messages, a malicious node can easily cause network disruptions. This will be easier for Ad hoc wireless networks to have no physical barrier to protect themselves and all elements can potentially participate in the routing mechanism.

If a malicious node has the ability to impersonate a valid node of the network, it can, during the route discovery mechanism, respond to the initiating node with a route reply message by announcing a path, with a minimal cost, to the requested node. The sending node will then update its routing table with this false route. The data packets from the sending node to the destination node will pass through the malicious node that can simply ignore them. This attack is called black hole, black hole. The packets are picked up and absorbed by the malicious node. Figure 4 illustrates this type of attack.

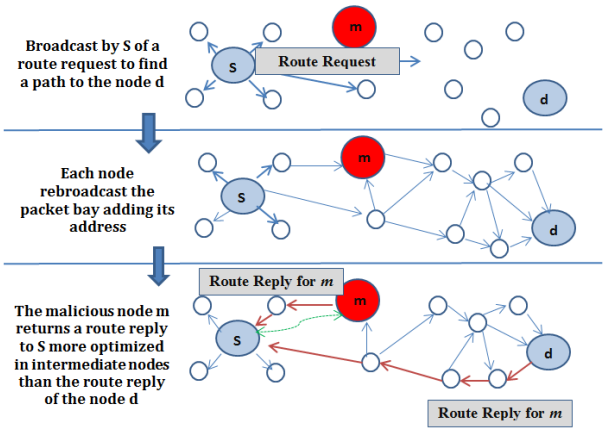

Figure 4. A malicious node m captures the traffic dedicated to node d in a black hole attack.

[1] Each node maintains two types of traffic: control packets and data packets.

In a variant called gray hole, only certain types of packets are ignored by the malicious node. For example, data packets are not retransmitted while routing packets are. An attacker can also create infinite loops in the network or force packets to make detours consuming the radio resource unnecessarily. A malicious node that has impersonated a valid node may also generate route error errors, randomly, to disrupt the operation of the route maintenance mechanism.

3.3. Example of a Routing Protocol

3.3.1. The OLSR Protocol

OLSR (Optimized Link State Routing Protocol) is a proactive routing protocol for Ad Hoc Mobile Networks [3]. This protocol is non-uniform and based on the selection of neighbors. The OLSR protocol is based on the Multi Point Relay (MPR) concept. The MPR relays of a node correspond to all the neighbors that make it possible to reach all the nodes situated at two jumps. Diffusion of the different control messages is only done to the MPR relays as illustrated in Figure 5, thus reducing unnecessary repetitions. On the other hand, the OLSR protocol distinguishes unidirectional links from bidirectional links, which are the only ones used for routing.

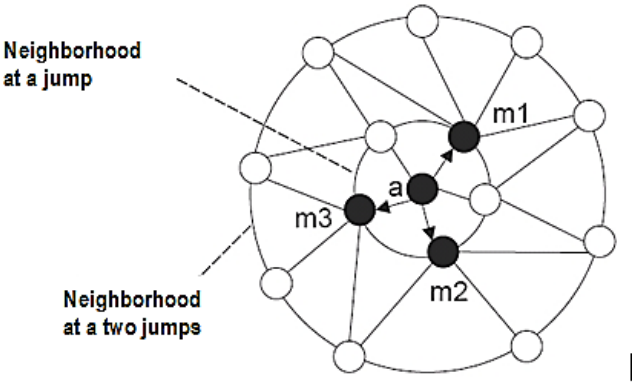

Figure 5. Multipoint Relay: Node A chose m1, m2 and m3 as multipoint relays. When A sends a TC (Topology Control) message, it is only retransmitted by m1, m2 and m3, which in turn transmits it back to their MPR relay.

Each node maintains information on the nodes that elected it as a relay MPR. This is done through messages (Hello messages) sent by each node to its neighbors. These messages contain:

- ✓ A list of the nodes with which the transmitter has bidirectional links,
- ✓ a list of the nodes that the transmitter can hear (they maintain a unidirectional link towards him)
- ✓ A list of the nodes that the transmitter has chosen as relay MPR.

The broadcast of these Hello messages allows the nodes of the network to store, in their neighbor table, a vision with two jumps of their neighborhood and to calculate all of their MPR relays. This set is recalculated when a change is detected in the two-hop neighborhood. The broadcast over the entire network (via the MPR relays) of topology control

messages (TC messages) gives the topological information necessary for the routing mechanism. These messages contain, for each MPR relay, the list of nodes that have chosen it. At these messages, the nodes can maintain a Topology Table, indicating the last hop for each destination.

A shorter path algorithm, applied to the neighbor table and the topology table, builds the routing table for each node. This table stores, for all the nodes of the network, the number of jumps and the first jump to reach it. It must be recalculated as soon as one of the two source tables is modified.

OLSR provides optimal routes in number of hops. It is suitable for large networks thanks to its MPR relay mechanism, but is probably less efficient for small networks.

3.3.2. Attacks on the OLSR Protocol

The OLSR protocol does not include any security features [4]. Thus, he is vulnerable to different types of attacks. In [4], Raffo examines security issues related to routing protection in ad hoc networks. It classifies the different attacks that can be carried out and examines in detail the case of the OLSR protocol. The OLSR protocol is vulnerable to the two categories of attacks presented earlier: incorrect generation of traffic and bad traffic relaying.

Recent research has focused on creating authentication and encryption techniques to protect the OLSR against external attackers. A second line of defense is required to provide intrusion detection and intervention techniques to protect the OLSR protocol from intruder attacks.

3.4. The Notion of Flood

In routing protocols for ad hoc networks, flooding or pure broadcasting involves propagating a packet (of data or control) throughout the network. A node that initiates the flood sends the packet to all its direct neighbors. Similarly, if any node in the network receives the packet, it rebroadcast it to all its neighbors. This behavior repeats until the packet reaches all network nodes as shown in Figure 6.

Figure 6. The flood mechanism.

It should be noted that the nodes may be required to apply control processes during the flood, in order to avoid certain problems, such as looping and duplication of messages. The flood mechanism is generally used in the first phase of routing, more exactly in the route discovery procedure, and in the case where the sending node does not know the exact location of the destination. The source floods the network with a route search packet to reach the destination node. In fact, the flood is very expensive especially in the case where the network is bulky (latency, overloading messages, etc.). For this reason, routing protocols try to minimize as much as possible the propagation of flood topology discovery packets by adding other broadcast parameters.

4. Communication Group

4.1. The Group Concept

In group communication, messages are transmitted to abstract entities or groups; the issuers do not need to know the members of the target group. Group communication has already been the subject of much work, mainly within the framework of the ARLES project [5]. Managing members of a dynamic group allows a node to join a group, leave that group, move to another place, and join the same group. It is in this sense that the group communication ensures an independence of the localization; which makes it perfectly suited to dynamic network topologies, such as ad hoc network architectures.

Lin and Gerla propose in [6], a group decomposition algorithm for wireless mobile networks. The algorithm partitions the network into a set of groups so that any node in the network can reach any other node using at most one intermediate node. The following figure shows an example of partitioning.

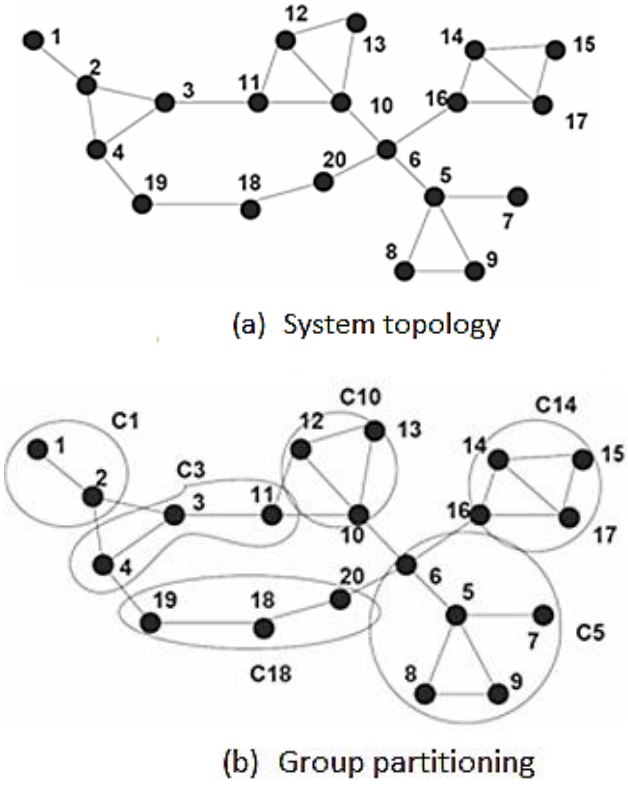

Figure 7. (a) and (b) The decomposition of the network into groups.

4.2. Group Management

In an ad hoc network, users can move and resource availability changes over time. The communication group concept enables an adaptive service that responds to environmental changes in a way that maintains the quality of service perceived by users (i.e., response time). Issarny et al. [7] address this problem by proposing middleware to manage dynamic groups in ad hoc networks. Applications can run on groups when the complexity of the network environment is highly dynamic.

Group membership is primarily defined for a group to achieve functionality, for example, defining a collaboration, sharing a compute load, improving performance, providing fault-tolerant service, and so on. In general, a node can leave a group because it fails, explicitly requests to leave, or is expelled by other nodes in the group. On the other hand, a node can join a group because it explicitly asks it or because it works after a failure. A group management protocol logically controls the dynamic changes, which means that all members of the group must have a consistent view of group membership even in the event of outages.

The groups are defined with respect to a feature denoted *f* that can characterize a functional property supported by certain nodes (i.e. resources and services). Issarny et al. use *support (x,f)* to denote the fact that a node x guarantees f and G^f to denote a group that guarantees f*:* $G^f = \{x \mid x \in N$ and *support(x,f)*$\}$. In [7], the attributes of group membership are defined as follows:

Network Model: This network model is considered as a set of N nodes. A node x in N has a unique identity denoted I d (x). The routing protocol below this layer is not fixed. The following functions are used to reason about the connectivity of nodes for a node x ∈ N and a duration t during which the topology of the network is not changed.

- *Proximity (t, x, p)* returns the geographical distance between the position of a node *x* and the geographical position *p* during *t*.
- *Distance (t, x, y)* returns the geographical distance between the nodes *x* and *y (x, y ∈ N)* during t.
- *Connectivity (t, x)* returns the set of all *N* nodes with which *x* can communicate using the underlying network protocols during *t*;
- *Dual Connectivity (t, x)* returns the set of all nodes *y* in *N* such that *y ∈ Connectivity (t, x)* and *x ∈ Connectivity (t, y).*
- *Hops (t, x, y)* returns the number of hops for the communication between *x* and y for all accessible from *x (y ∈ Connectivity (t, x)).*

Location: Issarny et al. [5] have defined functions that characterize membership in a group taking into account the set of constraints on the relative location of the member nodes. The members of the group are in a geographical area whose location can be fixed a priori or linked to the position of each member. Suppose *pos* denotes a geographic position of reference and *dist* denotes the maximum geographical distance, we get Eq. (1) and Eq. (2)

$$Geographical\_Proximity(Gf,t,pos,dist) \Leftrightarrow \forall x \in Gf: Proximity(t, x, pos) < dist \quad (1)$$

$$Relative\_Proximity(Gf,t,dist) \Leftrightarrow \forall x,y \in Gf: Distance(t,x,y) < dist \quad (2)$$

Groups are defined based on the number of hops that separate the member nodes. They are defined in the same way based on the maximum number of jumps (noted hops) between the nodes. (Eq. (3))

$$Bounded\ (Gf,\ t,\ hops) \Leftrightarrow \forall x,\ y \in Gf:\ H\ ops\ (t,\ x,\ y) \leq hops \quad (3)$$

Admission to a group: Only authorized nodes can join a group. This is done through the definition of a *security domain*. A security domain S^f manages the nodes that trust each other to perform a function *f*. In practice, a security domain is controlled by another trusted third party that authenticates and registers the nodes. The nodes then obtain a signed certificate to authenticate with other nodes of the domain S^f.

The communication in this secure group can be done by the sharing of a group key by the members of the group Eq. (4)

$$Closed\ (Gf,\ Sf) \Leftrightarrow \forall x \in Gf:\ x \in Sf \quad (4)$$

Connectivity: Group members may have *loose*, *partial*, or *complete* connections to each other.

- The *loose* connection is the available network connection for a time *t* and does not impose any specific constraints.
- The *partial* connection is defined according to the roles of the nodes (client and server) according to *f*. The relation *customer (x, f)* denotes that *x* is client for a function *f* and the relation *server (x, f)* denotes that *x* is a server for *f*: (Eq. (5))

$$Partial\ (Gf,\ t) \Leftrightarrow \forall x \in Gf,\ \forall y \in Gf:\ server\ (x,\ f):\ y \in DualConnectivity\ (t,\ x) \quad (5)$$

- A *fully* connected group is characterized by: Eq. (6)

$$Connected\ (Gf,\ t) \Leftrightarrow \forall x, y \in Gf: y \in DualConnectivity\ (t,\ x) \quad (6)$$

We can note that $Connected\ (G^f) \Rightarrow Partial\ (G^f)$. In addition, symmetric links are not required between the client and server nodes. Only bidirectional connectivity is considered for applications.

4.3. Group Management Interest for Our Study

Group management can be an intermediate feature to assist application development over ad hoc networks [7]. Group management is used to control a dynamic subnet on which the application runs for the implementation of functional and non-functional properties. Group management in an ad hoc network has led to various studies and different specific applications. However, a distinctive set of main attributes can be identified for group-oriented ad hoc networks. These attributes can be later exploited to design a generic service of a group that must be adapted to the specifications of the applications.

In [5], key attributes are introduced for group management in ad hoc networks, especially application-based networks. These attributes are used to set membership constraints for a group, related to the location, connectivity, authentication, and quality of service of members. The functional and non-functional properties of group management can be very useful for our study in terms of availability.

5. Routing Security Model

This section illustrates a security model for ad hoc networks. We present several basic properties for routing

security in ad hoc networks. We were particularly interested in availability property in our study.

5.1. Security Properties for Ad Hoc Network Routing

In [8], Buchegger and Boudec define five basic conditions for security in ad hoc network routing protocols:

- **Confidentiality**: Due to the limited scope of each node, communications between two nodes are usually established using a number of intermediate nodes. Unfortunately, some of these intermediate nodes may be malicious, posing a threat to the confidentiality of the data exchanged. Data encryption can protect information exchanged between nodes.
- **Integrity**: The integrity of a network depends on all the nodes in that network that correctly follow routing procedures. This allows each node to have correct routing information. Threats to integrity exist when malicious people broadcast fake routing messages or alter useful messages that circulate in the network.
- **Authentication**: An unauthorized node does not have permission to access routing information and is not allowed to participate in the ad hoc routing protocol. At present, there is no explicit and formal protocol that handles authorization in Ad-hoc routing. There is simply an abstract notion for that. However, authentication is a must. It is used to provide access control services in the ad hoc network.
- **Reliability**: Ad hoc networks are often used as a solution in backup situations when the use of a fixed infrastructure is impossible. Routing must be reliable and back-up procedures may be required. For example, if a routing table is full because of limited memory capacity, a responsive protocol should always be able to find a backup route for a given destination.
- **Availability**: The previously presented properties are in terms of "which node has permission to do a task" (ie, for a read / write operation, can we read, can we write?) While availability concerns this that an authorized node can actually do (ie, one has the right to write, but does it work, if one tries to do it?) [9].

Among these properties, we are interested in availability because there is very little research currently on this topic, especially in the area of ad hoc networks. This availability property is detailed in section 5.3.

5.2. The Concept of Reputation

Another security mechanism is based on the concept of reputation and serves to establish a link between the behavior of a node and the use of the network. To detect malicious nodes, test packets are sent into the network and a reputation value is evaluated for each node. A node with a low reputation will not be able to use the network.

Each node of the network observes the behavior of its neighbors with respect to a specific function, for example packet forwarding, and collects information on the execution of this function. If the expected result coincides with the observed result, the observation will have a positive value, otherwise it will have a negative value. Based on observations collected as time passes, each node calculates a reputation value assigned to each of its neighbors using a sophisticated evaluation mechanism. In their framework of study of the CORE protocol [10], Michiardi and Molva define three types of reputation: *subjective*, *indirect* and *functional*.

5.2.1. The Subjective Reputation

The subjective reputation is a reputation calculated directly from the observation of a node. A subjective reputation $R_{ni}^{t}(nj|f)$ at time t from the point of view of a node or on the node n_j with respect to a function f is calculated by the following formula: Eq. (7)

$$R_{ni}^{t}(nj|f) = \sum \rho(t, tk).\, \sigma k \qquad (7)$$

where $\rho\ (t,\ t_k)$ is a temporal function that gives a higher relevance to the old values σ_k which is the estimation factor given to the k-th observation. It is a variant that varies from -1 (for a negative impression and means that the result observed does not correspond to the expected result) to +1 (for a positive impression, for example, when the expected result coincides with the result observed). When the number or quality of the observations collected since *t* are not sufficient, the final value of the subjective reputation takes the value 0 to be neutral.

Since $\sigma_k \in$[-1, 1] and $\rho(t,\ t_k)$ is a normalized value, then $IR_{ni}^{t}(nj|f) \in$ [-1, 1]. The set n_j is limited to a set of neighbors of n_i.

5.2.2. Indirect Reputation

The subjective reputation is evaluated only by considering the direct interaction between a node and its neighbors. In complex networks, the final value of a node's reputation is also influenced by information from other members of the network.

$IR_{ni}^{t}(nj|f)$represented the value of the indirect reputation of the node n_j collected by a node or at time *t* with respect to a function *f*. The information collected by the indirect reputation can only take positive values. This helps protect against denial of service attacks based on spreading negative estimates for nodes.

5.2.3. Functional Reputation

The functional reputation is the subjective and indirect reputation calculated with respect to the different functions *f*. This makes it possible to calculate an overall value of a node's reputation that takes into account different observation and evaluation criteria. For example, a node n_j can evaluate a subjective reputation $R_{ni}^{t}(nj|f(packet\ forwarding))$ of the node n_j with respect to the packet transfer function and the subjective reputation $R_{ni}^{t}(nj|f(routing))$ with respect to the routing function and the combine using the different weights to obtain an overall reputation value on node n_j.

5.2.4. The Global Reputation

Global reputation can be defined by a combination of reputation information as follows: Eq. (8)

$$R_{ni}^{t}(nj) = \sum_k Wk.\{R_{ni}^{t}(nj|fk) + IR_{ni}^{t}(nj|fk)\} \qquad (8)$$

where w_k represents the weight associated with each functional reputation value. The choice of w_k weights to evaluate the overall reputation should be accurate because it can affect the robustness of the overall system.

This mechanism provides a final reputation value that is the result of a linear combination of subjective reputation, indirect reputation, and functional reputation. Each type of reputation is obtained by combining the different observations made by one node on another node according to *f*. Each observation is related to the correct execution of f. It is necessary to define a validation mechanism (based on the acknowledgment information) that compares the observed result with the expected result. If the expected result coincides with the observed result, the observation will have a positive value, otherwise it will have a negative value.

5.3. Availability Property

In our context, the property availability is set to access the routing information at any time on request. If there is a path to reach a mobile node, then any node should be able to get that way when they need it. In addition, a routing operation should not take too long to run on a node or delay a node to receive the maintenance messages from the routes. In addition, a node must be able to perform normally without excessive interference operations caused by the routing protocol or security protocol.

One of the first analyzes of the denial of service problem is made by Gligor [9]. He introduced the concept of Maximum Waiting Time (M W T). The system should report an expected M WT for each service it provides when entities (nodes) request access to a service and perform a task.

Yu and Gligor [11] have studied the problem of denial of service related to resource management. They show that to check an availability property it is necessary to know the resources and constraints of service behavior. Users must accept some additional restrictions on their behavior, called user agreements. In the model, Yu and Gligor have two parts. The first part consists of the specification of resources and the processing of queries. The second part describes the constraints that services must respect in their use of resources.

Millen [12] proposes a Trusted Computing Base (TCB) global availability monitor model with strong confidence assumptions to ensure that behavior constraints can be safely enforced. It is a state transition model with probabilistic wait time policies to capture the effect of realistic system behavior. It is based on the set theory approach and includes an explicit representation of time.

Cuppens and Saurel [13] worked on the expression of availability policies. An availability policy allows you to perform tasks and use the resources needed to complete the tasks. The main objective of an availability policy is to specify M WTs. This corresponds to obligations to guarantee these M W Ts (for access to resources and achievement of tasks).

In a recent paper [14], Cuppens et al. propose a new approach based on a formal security model called Nomad [6] that combines deontic logic and temporal logic to analyze the consistency of an availability policy and derive the availability properties. Cuppens et al. show how to use this Nomad template to specify availability policies. This approach is based on aspect-oriented programming. The availability requirements in Nomad are transformed into availability aspects.

The context of our study can be seen as an adaptation of this approach to availability properties in mobile ad hoc networks.

6. Validation of Non-functional Properties by Simulation

One of the goals of studying an availability model in ad hoc networks is to produce realistic scenarios and simulations to properly examine security mechanisms in terms of availability. These mechanisms are designed to deal with different types of node behavior by producing feasible solutions that will work in real systems. Ad hoc dynamic network topology makes it difficult to perform a simulation that conforms to protocol specifications and availability policies.

In [8], some properties are defined to prevent the threats identified in the security model. These properties are considered when designing security protocols and simulations to examine such protocols.

Network size: The size of the network must necessarily vary. Indeed, the size should be assigned to a dynamic variable that changes as the nodes enter and leave the network. Simulations should cover the case where a large number of nodes enter or leave the network simultaneously.

Node Density: Denial of Service attacks are more difficult to achieve in non-peoples areas. A very simple reason is that the more nodes there are, the more alternative routes exist. However, attacks on network integrity may be more interesting in dense areas because false information would spread quickly.

Locating Nodes: Some routing protocols in ad hoc networks are based on the location information of mobile nodes. This type of protocol broadcasts data for a certain node by performing partial flooding and using location data to minimize network load. Each node of the ad hoc mobile network periodically exchanges control messages to inform other nodes of its location. When sending the data, if the source has recent information on the location of the destination node, it chooses a set of neighboring nodes that are located in the source-to-destination direction. If such a set does not exist, the network set is flooded by the data. In the case where such nodes exist, a list containing their identifiers is inserted into the header of the data packet before transmission. Only the nodes that are specified in the header list process the packet.

Grouping: With the notion of localization, nodes that are close to each other can form a communication group. Sizing must be taken into account using some form of hierarchical model as in the Internet. The grouping must be dynamic because nodes can leave or join a group or leave it permanently.

Node mobility: In an Ad hoc network, the network topology can change rapidly, randomly and unpredictably, and traditional network routing techniques, based on pre-established routes, can no longer function properly. But, not all nodes are necessarily mobile. A simulation must also consider stationary nodes.

7. Conclusion

In this comprehensive investigation, some routing protocols in the Ad hoc network, vulnerabilities and attacks related to routing protocols by giving an example with the OLSR routing protocol are presented. And also, the basic security properties are mentioned. Among these properties, we are interested in that of availability which is defined by the guarantee of access to routing information `at any time upon request. If there is a path from one mobile node to another, then that node (if it has permission to use network resources) should be able to get that path when it needs it. And the routing operation should not take too much time to complete this task.

Finally, a collective observation technique and a reputation mechanism are extracted. Each node of the network observes the behavior of its neighbors with respect to a specific function, for example the routing of packets, and collects information on the execution of this function. This mechanism provides a final reputation value that is the result of a linear combination of subjective reputation, indirect reputation, and functional reputation. This reputation approach can in particular help solve the availability problem.

References

[1] D. Raffo, Security Schemes for the OLSR Protocol for Ad Hoc Networks, PhD thesis, Université de Paris 6 – INRIA Rocquencourt, 2005.

[2] C.S.R. Murthy, B.S. Manoj, Ad Hoc Wireless Networks Architectures and Protocols. PRENTICE HALL, 2004.

[3] Th. Clausen, Ph. Jacquet, Optimized Link State Routing Protocol (OLSR).

[4] J.K. Millen, A resource allocation model for denial of service. In IEEE Symposium on Security and Privacy, 1992.

[5] M. Boulkenafed, V. Issarny, J. Liu, Group Management for In-home Ad Hoc Networks, In Proceedings of ECRTS International Workshop on Real-Time for Multimedia - Special Focus on Real-time Middleware for Consumer Electronics (RTMM), 2004.

[6] V.D. Gligor, A Note on the Denial-of-Service Problem. In IEEE Symposium on Security and Privacy (1983) 139–149.

[7] Ch. R. Lin, M. Gerla, Adaptive Clustering for Mobile Wireless Net- works, IEEE Journal on Selected Areas in Communications 15 (1997) 1265–1275.

[8] S. Buchegger, J. Y. Le Boudec, Performance analysis of the CONFIDANT protocol: Cooperation of nodes — fairness in dynamic ad-hoc networks, In Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, June 2002.

[9] F. Cuppens, C. Saurel, Towards a formalization of availability and deny of service, First Information System technologies panel symposium on protecting NATO information systems in the 21th century, octobre 1999.

[10] J. Liu, D. Sacchetti, F. Sailhan, V. Issarny, Group management for mobile Ad Hoc networks: Design, Implementation and Experiment, In MEM '05: Proceedings of the 6th international conference on Mobile data management, New York, NY, USA, ACM Press (2005) 192–199.

[11] B. Shrader, A proposed definition of Ad hoc network. Technical report, Royal Institute of Technology (KTH), Stockholm, Sweden, May 2002.

[12] P. Michiardi, R. Molva, Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, In Communications and Multimedia Security (2002) 107–121.

[13] F. Cuppens, N. Cuppens-Boulahia, Th. Sans, Nomad: A Security Model with Non Atomic Actions and Deadlines, In CSFW (2005) 186–196.

[14] IETF RFC 3626, Network Working Group, October 2003.