# Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks

Pietro Michiardi and Refik Molva
Piero.Michiardi@eurecom.fr – Refik.Molva@eurecom.fr
Institut Eurécom, 2229 Route des Crêtes BP 193
06904 Sophia-Antipolis France

**ABSTRACT**

*The area of ad hoc networking has been receiving increasing attention among researchers in recent years and a variety of routing protocols targeted specifically at the ad hoc networking environment have been proposed. However, little information about the effects of security exposures in terms of network performance has previously been available. This paper provides a simulation study that identifies security issues that are specific to MANET and that illustrate the effects of those threats on network performance when the DSR routing protocol is used. We focused our attention on the evaluation of network performance in terms of global throughput and delay of a mobile ad hoc network where a defined percentage of nodes behaved selfishly. The simulation study brought up two important conclusions. First, it shows that security issues have to be taken into account at the early stages of a routing protocol design. Indeed, when no countermeasures are taken, the simulation results showed that network operation and maintenance can be easily jeopardized and network performance will severely degrade. Second, a cooperative security scheme seems to be a reasonable solution to the selfishness problem: a selfish behavior can be detected through the collaboration between a number of nodes assuming that a majority of nodes do not misbehave.*

## 1. INTRODUCTION

This paper provides the results of a simulation analyzing the impact of security problems in a mobile ad hoc network (MANET). The paper first tries to identify security issues that are specific to MANET. The effect of security attacks is then analyzed in the framework of network scenarios that are significant for MANET.

We claim that security in MANET is an essential component for basic network functions like packet forwarding and that network operation can be easily jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design [6]. Unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in ad hoc networks those functions are carried out by all available nodes. This very difference is at the core of the security problems that are specific to ad hoc networks. As opposed to dedicated nodes of a classical network, the nodes of an ad hoc network cannot be trusted for the correct execution of critical network functions.

If a priori trust relationship exists between the nodes of an ad hoc network, entity authentication can be sufficient to assure the correct execution of critical network functions [1]. A priori trust can only exist in a few special scenarios like military networks and requires tamper-proof hardware for the implementation of critical functions. Entity authentication in a large network on the other hand raises key management requirements.

If tamper-proof hardware and strong authentication infrastructure are not available, the reliability of basic functions like routing can be endangered by any node of an ad hoc network. No classical security mechanism can help counter a misbehaving node in this context. The correct operation of the network requires not only the correct execution of critical network functions by each participating node but it also requires that each node performs a fair share of the functions. The latter requirement seems to be a strong limitation for wireless mobile nodes whereby power saving is a major concern.

With lack of a priori trust, cooperative security schemes seem to offer the only reasonable solution. In a cooperative security scheme, malicious behavior can be detected through the collaboration between a number of nodes assuming that a majority of nodes do not behave maliciously. The threats considered in such a scenario are not limited to maliciousness and a new type of misbehavior called selfishness should also be taken into account to prevent nodes that simply do not cooperate.

In order to come up with an appropriate security approach, we analyzed the impact of various security threats on an essential network function, routing and packet forwarding.

## 2. ASSUMPTIONS AND BACKGROUND

This section outlines the assumptions that were made regarding the properties of the physical and network layer of the MANET and includes a brief description of the Dynamic Source Routing (DSR), the routing protocol that has been used for our simulations.

### 2.1 Physical Layer Characteristics

Throughout this paper we assume bi-directional communication symmetry on every link between the nodes. This means that if a node B is capable of receiving a message from a node A at time *t*, then node A could instead have received a message from node B at time *t*. This assumption is valid because the protocol selected for the simulations is the MAC 802.11 that provides bi-directional communications.

### 2.2 Dynamic Source Routing (DSR)

DSR is an on-demand, source routing protocol [3]. Every packet has a route path consisting of the addresses of nodes that have agreed to participate in the routing of the packet. The protocol is referred to as "on-demand" because route paths are discovered at the time a source sends a packet to a destination for which the source has no path.

The DSR routing process includes two phases: the Route Discovery phase and the Route Maintenance phase. When a source node (S) wishes to communicate with a destination node (D) but does not know any path to D, it invokes the Route Discovery function. S initiates the route discovery by broadcasting a ROUTE REQUEST packet to its neighbors that contains the destination address D. The neighbors in turn append their own addresses to the ROUTE REQUEST packet and re-broadcast it. This process continues until a ROUTE REQUEST packet reaches D. D must now send a ROUTE REPLY packet to inform S of the discovered route. Since the ROUTE REQUEST packet that reaches D contains a path from S to D, D may chose to use the reverse path to send back the reply.

The second main function of the DSR is Route Maintenance, which handles link outages.

## 3. SIMULATION STUDY

The simulation study has been carried out in order to analyze the effects of security exposures on essential network functions such as routing and packet forwarding. We focused our attention on the evaluation of network performance in terms of global throughput and delay of a mobile ad hoc network where a defined percentage of nodes were misbehaving.

The software we have used to simulate the MANET is a version of the Berkeley's Network Simulator (ns-2) that includes wireless extensions made by the CMU Monarch Project. The simulation software has been modified in order to model misbehaving nodes of different types.

Misbehaving nodes are supposed to operate independently and attacks by several colluding nodes are not taken into account. Our research pointed out two types of misbehavior: a selfish behavior and malicious behavior. *Selfish nodes* (SN) use the network but do not cooperate, saving battery life for their own communications: they do not intend to directly damage other nodes. *Malicious nodes* aim at damaging other nodes by causing network outage by partitioning while saving battery life is not a priority.

### 3.1 Misbehaving node models

This paper focuses on selfish nodes and proposes three different models that have been evaluated for the DSR protocol. We believe that the selfishness problem is of great interest because nodes of a mobile ad hoc network are often battery-powered, thus, energy is a precious resource that they may not want to waste for the benefit of other nodes.

The node behavior has been added as a node definition type in the ns-2 node model: the syntax that is used to define the node configuration has been enhanced with a new optional feature that allows selecting the selfishness model among three possible choices.

It also has been necessary to modify the DSR protocol implemented in ns-2 because the networking functions (routing and packet forwarding) are overridden by the routing protocol selected in the node configuration. The modified version of the DSR protocol checks the current node configuration and, depending on the selfishness model used for that node, decides whether to execute the networking functions.

#### *3.1.1 Selfish node of type 1*

In the first model, the SN does not perform the packet forwarding function [1, 2]. When this behavior is selected, the packet forwarding function performed in the SN is disabled for all packets that have a source address or a destination address different from the current SN. However, a selfish node that operates following this model participates in the Route Discovery and Route Maintenance phases of the DSR protocol.

The consequence of the proposed model in terms of consumed energy is that the SN will save a significant portion of its battery life neglecting large data packets, while still contributing to the network maintenance.

#### *3.1.2 Selfish node of type 2*

The second model focuses on SN that do not participate in the Route Discovery phase of the DSR protocol. The impact of this model on the network maintenance and operation is more significant than the first one. Indeed, if the node does not participate in the Route Discovery phase, then there will be no route including that SN: the consequence is that the packet forwarding function will never be executed. A SN of this type uses the node energy only for its own communications.

#### *3.1.3 Selfish node of type 3*

The third model of selfishness is more complex: the node behavior follows the energy model implemented in ns-2. When the simulator creates an instance of a mobile node, it is possible to specify the initial energy (E) attributed to that node. During a normal operation, the node consumes energy while executing networking functions such as packet forwarding and routing.

We propose a selfishness model that uses two energy thresholds ($T_1$ ,$T_2$) to determine the node behavior. When the node's energy falls within the interval [E ,$T_1$) the node behaves properly, executing both the packet forwarding and the routing function. When the energy level falls in the interval [$T_1$ ,$T_2$) the node will behave as if it was a selfish node of type 1, thus disabling the packet forwarding function. If the energy level is within the interval [$T_2$ ,0) then the same behavior as the one described for a selfish node of type 2 is selected. Whenever a node has no more energy it is possible to set a stochastic recharge phase: within a limited time interval the node's energy is set back to the initial value.

We believe that this selfishness model is more realistic than the others; the objective of our study will be the evaluation of the influence of parameters such as node mobility over the global network performance when nodes behave following this selfishness model.

Next we focus on the simulation study, specifying the movement and communication patterns and the metrics used to evaluate the network performance.

### 3.2 Movement and communication patterns

In all our node movement scenarios, the node chooses a destination and moves in a straight line towards it at a speed uniformly distributed between 0 meters/seconds (m/s) and some maximum speed. This is called the *random waypoint model*. We limit the maximum speed of a node to 20 m/s and we set the run-time of the simulations to 50 seconds. Once the node reaches its destination it waits for a *pause time* before choosing a random destination and repeating the process. Additionally we developed a script that launches simulations with different random mobility scenarios for every simulation cycle.

The nodes communicate using constant bit rate (CBR) sources that are randomly bound to a subset of all the nodes forming the MANET. The packet size is set to 512 bits while the source throughput (expressed as packet per seconds) is different for each simulation. Additionally we developed a script that randomly chose sources and sinks among the nodes of a network and launches simulations with different random communication patterns for every simulation cycle.

Movement and communication patterns have been generated using the tools provided by the CMU extensions to ns-2.

### 3.3 The metrics

The impact of selfish behavior was measured in terms of aggregate network throughput and delay variations. The measurements of the network performance were made using a script that parses and analyzes the trace file output provided by the ns-2 software. The trace file provides information about a set of defined events that occurred in the simulation such as MAC layer events, routing events and agent events. Analyzing the agent event trace it is possible to evaluate the total number of packets sent by every node of the MANET as well as the total number of packets that have been dropped. We used the following definition for the aggregate network throughput:

$$T = \frac{\text{Tot. \# of Received Packets}}{\text{Tot. \# of Sent Packets}} = \frac{\text{Tot. \# of Sent Packets - Tot. \# of Lost Packets}}{\text{Tot. \# of Sent Packets}}$$

where the term "lost packet" covers all packet losses due to malicious drops, route failures, congestion and wireless channel losses.

The other performance characteristic that was measured is *d* or the average delay for all packets that are correctly received. We believe that selfish nodes also have an influence on the network delay and we use it as a further comparative criterion when the network throughput is not sufficient.

## 4. SIMULATIONS BASED ON SN OF TYPE 1 AND TYPE 2

### 4.1 General Configuration

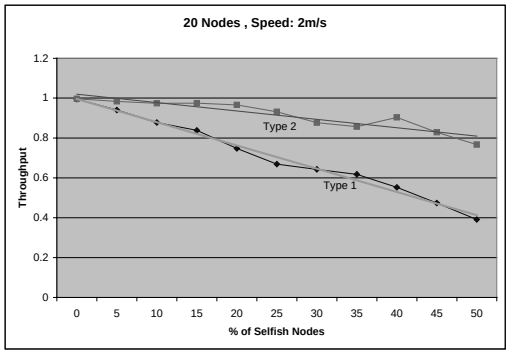
The effects of the selfishness models type 1 and type 2 are studied on four different scenarios where the two parameters that define each scenario are *node density* and *node mobility*. We define node density as the number of nodes that form the MANET deployed over an 800 by 800 meter flat space. On the other hand, node mobility is defined as the average speed each node moves at in the simulation space.

Simulation results are classified in four categories: low node density (20 nodes) and low mobility (2 m/s), high node density (60 nodes) and low mobility, low node density and high mobility (15 m/s), and high node density and high mobility.

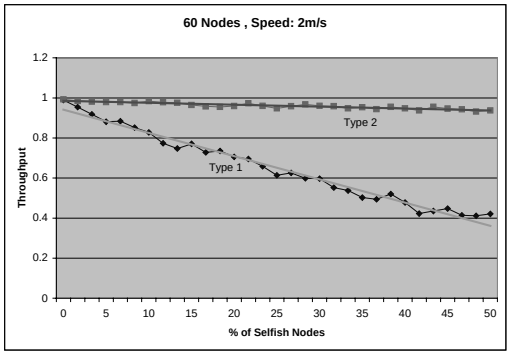
If it is not specified differently, the simulation run-time for all the families of graphs presented in this section is set to 50 seconds. Also, the CBR source throughput is set to 1 packet per second.

The percentage of selfish nodes (*p*) is increased for each simulation run and takes values from 0% to 50%: in each simulation run, only *p* nodes are set to be selfish while the other nodes of the network behaves correctly.

Figure 1 and Figure 2 respectively show the variations of global network throughput and communication delay as a function of the percentage of selfish nodes.

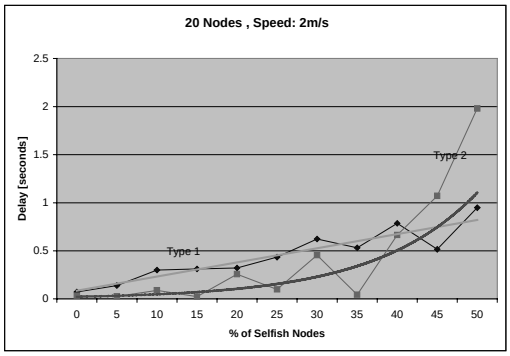



(a)

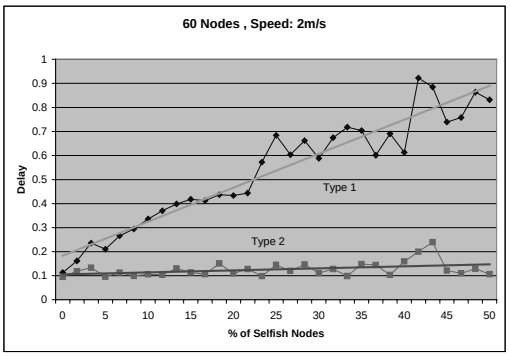



(b)

Figure 1. Network Throughput for low and high node density, low mobility.




(a)




(b)

Figure 2. Communication Delay for low and high node density, low mobility.

### 4.2 Observations

*4.2.1 Selfishness of type 1: "no packet forwarding"*

Figure 1 a) and b) point out that *T* degrades by 60% when 50% of the nodes of the network misbehave. The linear regression of the experimental data shows that *T* degrades by 10%-15% every time the percentage of selfish nodes increases by 10%. On the other hand, Figure 2 a) and b) show that *d* increases linearly with the percentage of selfish nodes. These observations are valid both for low and high node density, while node mobility have a negligible influence on the measurements.

The obtained results show that when the packet forwarding function is disabled by a large percentage of nodes of the MANET the global network performance severely degrade. Countermeasures for this type of selfishness have to be taken into account for the design of secure routing mechanisms. We claim that a cooperative security scheme offers a reasonable solution to the problem: an important requirement for the security mechanism is to verifies the correct execution of the packet forwarding function and to force the nodes of a MANET to collaborate for the network operation.

*4.2.2 Selfishness of type 2: "no DSR"*

Figure 1 a) shows that *T* degrades by 20% when 50 % of the nodes follow the second type of selfishness. Figure 2 a) indicates that *d* increases exponentially when the percentage of misbehaving nodes increase. On the other hand, when node density is high, it is possible to notice that network performance improve: *T* degrades only by 7%-10% and *d* has a linear growth.

When the Route Discovery phase of the DSR protocol is disabled, the node does not participate in the route construction: the node will never appear in a source route. The reason why the average throughput degrades is that it is more difficult to find a route to the destination leading to a higher packet loss probability. Furthermore, delays are high especially when node density is low. Depending on the MANET topology, it is possible that selfish nodes partially or totally isolate a node that behaves well because they do not provide route information; the result is that the node that behaves well loses data packets and time to find the next hop where to send them. When node density is high, the effect of the selfish behavior is mitigated and the probability to find a route to the destination increases: packet loss and delay decrease.

*4.2.3 Selfishness of type 1 vs. Selfishness of type 1*

The analysis of the results obtained with the first two families of simulations indicate that the effects of a node selfishness of type 1 are more important than the one caused by a selfishness of type 2. The apparent conclusion is that the mechanism for secure routing in MANET has to focus on the first type of selfishness, obliging misbehaving nodes to correctly perform the packet forwarding function.

However, if a selfish node does not participate in the Route Discovery phase of the DSR then it will never appear in any source route. It is implicit then that also the packet forwarding function will not be correctly executed, thus a mechanism that simply force a node to perform the packet forwarding function can be easily tricked by disabling the DSR function. On the other hand, a mechanism that only force a selfish node to correctly perform the DSR function does not assure that also the packet forwarding function will be properly executed.

Concluding, it is necessary that the security scheme adopted to face the selfish behavior of a node have to enforce the execution of both the packet forwarding and the DSR functions.

Moreover, we believe that a selfish behavior that selectively disables the packet forwarding or the DSR function is not realistic: it is more likely that the node behavior dynamically changes depending on the node's energy level. This is why we decided to design a third type of selfishness that is based on the energy model implemented in ns-2.

## 5. SIMULATIONS OF SN OF TYPE 3

### 5.1 General configuration

The last set of simulations focuses on the analysis of the network performance of a MANET when the third model of selfishness is used. The movement and communication patterns have been generated using the tools provided by the CMU extensions to ns-2, but they are different from the one that were used in the first two family of simulations.

In all our node movement scenarios, the node chooses a destination and move in a straight line towards it at a constant speed, chosen in a defined set. Once the node reaches its destination it waits for a *pause time* before choosing a random destination a repeating the process. We defined the set of possible speeds as the values that go from 1m/s to 20m/s with a step of 5m/s: {1, 5, 10, 15, 20}.

The nodes communicate using constant bit rate (CBR) sources that are randomly bound to a sub-set of all the nodes forming the MANET. The packet size is set to 512 bits while the source throughput (calculate as packet per seconds) is set to 20 packets/second. Additionally we developed a script that randomly chose sources and sinks among the nodes of a network and launches simulations with different random communication patterns for every simulation cycle.

Also, the global network throughput *T* is expressed in percentage and the global communication delay *d* has not been evaluated.

### 5.2 The energetic model

This section concentrate on the third model of selfishness, which is an energy-based model: it is possible to decide which is the initial value for the energy (E) associated to each node through the node configuration. We decided to set different values for E using a uniform distribution in the interval $[E_i - 0.25J, E_i + 0.25J]$ where the energy is expressed in Joules (J) and $E_i$ = 2.75*J*. The consequence of this choice is that every node will run out of energy at different times, adding a degree of randomness to the simulation.

### 5.3 The simulations

Differently from the previous analysis made for the first and the second model of selfishness, we decided to study the effects of node mobility over the global network throughput when the DSR protocol is used. As it is possible to see in the graph below, the y-axe represents *T* expressed in percentage, and the x-axe represents the speed of the node expressed in m/s. The first series represent *T* when all nodes of the MANET behaves correctly. The second series represents *T* when every node of the MANET behaves following the third model of selfishness.

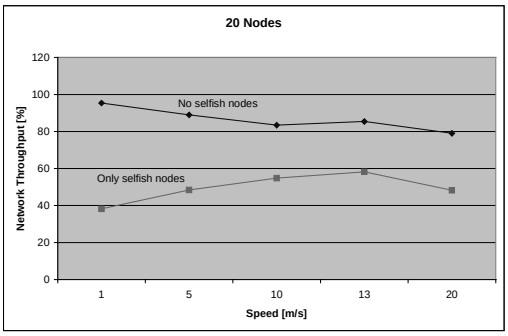



Figure 3. Global Network Throughput vs. Node Speed.

### 5.4 Observations

The last family of simulations pointed out an interesting characteristic of *T*. It has already been showed [4, 5] that the global network throughput decreases when the node mobility increases: the reason is that link outage becomes more frequent causing a higher packet loss probability.

On the other side, when every node of the network is selfish of type 3, simulation results indicate that *T* increases when node mobility increases until it reaches its maximum; then it decreases when node mobility increases.

We believe that this particular behavior depends on the mobile node topological position in the network. Referring to section 3.1.3 , when the third model of selfishness is applied to a mobile node, the node behavior dynamically change depending on its energy level.

Now, a MANET topology can be represented by an arbitrary graph $G = (V, E)$ where *V* is the set of mobile nodes and *E* is the set of edges. An edge exists if and only if the distance between two mobile nodes is less or equal than the node's radio range *r*. Accordingly, the neighborhood of a node *x* is defined by the set of nodes that are inside a circle with center at *x* and radius *r*, and it is denoted by:

$$N_r(x) = N_x = \left\{ n_j \middle| d(x, n_j) < r, x \neq n_j, \forall j \in N, j \leq |V| \right\}$$

where *x* is an arbitrary node in the graph.

The degree of a node *x* in *G* is the number of edges that are connected to *x*, and it is equal to $\deg(x) = |N_r(x)|$.

Given that the communication pattern used in the simulation produce a dense traffic, a central node (i.e. a node that has a central position in the MANET) consume more energy than a peripheral node because it acts as relays for other nodes, wasting its energy for routing and packet forwarding. A central node has also another characteristic: the degree $\deg(x)$ is high, which implies that nodes with a higher degree consume more energy than nodes with a lower degree.

When mobility is low, all nodes located in a central position stay in the central area of the network and consume more energy than peripheral nodes. Energy consumption leads to a selfish behavior: the packet forwarding and the routing functions will not be correctly executed and the network can be partitioned. As it is possible to see in Figure 3 for a 1m/s speed, the global network throughput is drastically reduced.

When node mobility increases, the location of a node changes from a central to a peripheral position and vice-versa with a high rate, implying that the energy consumption will be equally distributed among the nodes. The selfish behavior is mitigated and, as it is possible to see in Figure 3, *T* increases considerably.

However, when the node mobility reaches higher values the influence of the link outage over *T* is more important than the impact of a selfish behavior: speed affects negatively the network performance, as it is possible to see in Figure 3 for speed higher than 13m/s.

## 6. CONCLUSIONS

The area of ad hoc networking has been receiving increasing attention among researchers in recent years, as the available wireless networking and mobile computing hardware bases are now capable of supporting the promise of this technology. Over the past few years, a variety of routing protocols targeted specifically at the ad hoc networking environment have been proposed, but little information about the effects of security exposures in terms of network performance has previously been available. This paper provides a simulation study that identifies security issues that are specific to MANET and that illustrate the effects of those threats on network performance when the DSR routing protocol is used.

The simulation study brought up two important conclusions. First, it shows that security issues have to be taken into account at the early stages of a routing protocol design. Indeed, when no countermeasures are

taken, the simulation results showed that network operation and maintenance can be easily jeopardized and network performance will severely degrade. Section 4.2.3 shows that a mechanism that only forces the correct execution of the packet forwarding function would apparently improve network performances: however such a mechanism can easily be tricked by disabling the DSR function relative to the Route Discovery phase. This kind of threat would allow a node to avoid performing the packet forwarding function without rising any suspects in the security mechanism. Indeed, a node that does not participate in the Route Discovery phase will never appear in any path and the packet forwarding function will never be invoked. On the other hand, any mechanism forcing only the correct execution of the DSR protocol would not assure the correct execution of the packet forwarding function. We believe that the security mechanism adopted to overcome selfish behavior has to force the execution of both the packet forwarding and the routing function. Second, a cooperative security scheme seems to be a reasonable solution to the selfishness problem: a selfish behavior can be detected through the collaboration between a number of nodes assuming that a majority of nodes do not misbehave. Furthermore, it has been showed that node mobility improves network performance when limited to an upper limit: this result can be used as a trigger parameter for the cooperative mechanism as we envision to study in future work. Our next goal will be to conduct an analytical study of the impact of node mobility on network performance with misbehaving nodes. We plan then to design and evaluate a collaborative security scheme that solves the selfishness problem, analyzing the effects of such mechanism on network throughput and communication delay.

**REFERENCES**


[1] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proceedings of Mobicom 2000, Boston, August 2000

[2] Levente Buttyan and Jean-Pierre Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WANs", 1st IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC 2000),
Boston, MA, USA, 11 August 2000

[3] David B. Johnson David A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", Mobile Computing, edited by Tomasz Imielinski and Hank Korth, Chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.

[4] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu, Jorjeta Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols", Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking, ACM, Dallas, TX, October 1998

[5] Tony Larsson, Nicklas Hedman, "Routing Protocols in Wireless Ad hoc Networks - A Simulation Study", Master Thesis, LuleÅ Tekniska Universitet

[6] Frank Stajano and Ross Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", Proceedings of the 7th Security Protocols Workshop, 1999, pp. 172-194