

Increasing Security in Mobile Ad Hoc Networks by Incentives to Cooperate and Secure Routing

Ebrahim S. Khosravi, Brandy M. Tyson

Khosravi@cmps.subr.edu

Department of Computer Science, Southern University, Baton Rouge, LA. 70803

Abstract— A mobile ad hoc network is a self-organizing network that relies on the cooperation of participating nodes in order to function properly. In this network, mobile users arrive within the common range of a wireless link and collaborate in constructing the network topology in order to facilitate communication. Mobile ad hoc networks do not rely on any fixed, centralized routing infrastructure, so there is no base station to provide connectivity. This must be provided by the participating nodes.

Although mobile ad hoc networks are quite beneficial in sparse areas and rescue operations, they have several properties, such as unreliable wireless links, dynamic topologies and membership, and constraints in bandwidth and battery power, that increase their susceptibility to security attacks. This creates several security issues that include collaboration and fairness and confidentiality of location.

The new routing protocol extensions presented in this research make it possible to detect and punish selfish behavior; therefore, making it unbeneficial to deter from normal behavior. The presented protocol incorporates an incentive to cooperate in a secure routing protocol. This protocol presents a solution to several security issues in mobile ad hoc networks; however, some issues must still be addressed.

Index Terms—Mobile ad hoc networks, security, routing, cooperation.

I. INTRODUCTION

A mobile ad hoc network is an independent system of mobile users connected by relatively bandwidth constrained wireless links—the union of which forms an arbitrary graph. In this new concept of networking, potential mobile users arrive within the common perimeter of a wireless link and cooperate in constructing the network topology in order to facilitate communication. New users may join and leave at their own discretion. These networks do not rely on any fixed, centralized routing infrastructure. In other words, there is no base station to provide communication connectivity. In these dynamic systems, all network activity is left to the users themselves, requiring efficient distributed algorithms. Each user is responsible for discovering network topology, routing, forwarding, and delivering messages. Therefore, communication in mobile ad hoc networks functions properly only if participating users cooperate in routing and forwarding. This results in fairly weak communication connectivity.

II. MOBILE AD HOC NETWORKS

Mobile ad hoc networks are economical in sparse areas. They provide the only option in emergency and rescue operations and disaster relief efforts. They are also ideal for military and law enforcement operations, in which each user cooperates to accomplish a common goal. Furthermore, they eliminate the large investment required to construct and upgrade fixed networks for communication.

The new routing protocol makes it possible to detect and isolate misbehaving users, and in turn make it unbeneficial to deny cooperation. In the proposed scheme, “trust relationships and routing decisions are made based on experienced, observed, or reported routing and forwarding behavior of other nodes” [BB01]. Therefore, the protocol proposes the following:

- Employ neighborhood watch to be warned by watching what happens to other nodes in the neighborhood, before nodes have to make a bad experience themselves.
- Share information of experienced malicious behavior with friends and learn from them

This protocol makes two assumptions. First, it assumes that the behavior of neighboring users is truly observable behavior. This means it is possible to listen in on the communications of neighbors. This can be accomplished if each user keeps a copy of the packet it sends on to another user and listens to traffic sent on by that user. They clear their memory only after overhearing the packet being sent on by the next node successfully. Secondly, it assumes there is some mechanism to ensure authentication. Without authentication, nodes can accuse each other at will and a trust management scheme is not possible.

Although mobile ad hoc networks are quite beneficial, they also have many properties that increase their susceptibility to security attacks. These properties include the following:

- 1) Unreliable wireless links: Links are easily jammed because there are no firewalls or access control mechanisms. This makes eavesdropping, spoofing, denial of service, impersonation, and masquerading possible.

- 2) Dynamic topologies and membership: The topology of mobile ad hoc networks is dynamic, which makes it difficult to detect behavior anomalies. Node membership is unpredictable and rapidly changing [VJP02].
- 3) Constraints in bandwidth, computing power, and battery power: Mobile devices can lead to application-specific trade-offs between security and resource consumption of the device [BB02]. Therefore, it may be to the advantage of a user to not cooperate in order to save energy.
- 4) Self-organization: These dynamic systems do not rely on a fixed infrastructure.
- 5) Latency: Increased latency forces message exchange for security to be more expensive.
- 6) Multiple paths: In wireless multi-hop networks, multiple paths may be exploited.
- 7) Roaming in dangerous environment: Malicious or selfish users may allow attacks or deprive other users from providing service [VJP02].

These properties create several security issues in mobile ad hoc networks. According to [BB01], in addition to authentication, integrity, availability, access control, non-repudiation, and confidentiality, mobile ad hoc networks raise the following security issues:

- 1) Collaboration and fairness: There must be incentives for a node to forward messages that are not destined to itself. Nodes are assumed to be greedy, selfish, and economic. Attacks include “incentive mechanism exploitation by message interception, copying, or forging; incorrect forwarding; and bogus routing advertisement” [BB01]. There is a tradeoff for having good membership and resource consumption. It may be beneficial to an individual node to save resources rather than cooperating to send messages. However, if a node chooses not to cooperate, other nodes may deny service to them. Complete un-cooperation with other nodes and taking advantage of their willingness to cooperate is a boycotting behavior pattern. Boycotting behavior patterns deprive cooperating nodes of resources and services and simultaneously exploit their resources.
- 2) Confidentiality of location: Privacy of location, as required in military applications, can be just as important as message content. Privacy of routing information and privacy of location prevents routing and forwarding to intermediate users (neighbors).
- 3) No traffic diversion: Routes should be advertised and set up according to the chosen routing protocol and topology of the network. By diverting traffic in

the following manner, nodes can work against that requirement:

- a. Routing: Nodes may attract traffic to themselves and other collusive nodes to obtain information to facilitate malicious behavior. They may do this by false routing advertisements. Bogus routing advertisements can introduce denial-of-service attacks by inserting incorrect or old routing information.
 - b. Forwarding: Nodes may forward messages to partners in collusion for “analysis, disclosure, or monetary benefits” [BB01]. Nodes may not forward at all and choose to boycott communications.
- 4) Motivation for malicious behavior: Nodes may choose to be uncooperative to obtain better service, to prevent other users from obtaining proper service, to gain monetary benefits by taking advantage of incentive measures, to extract data to get confidential information, or simply to save power.

Detecting and punishing malicious and uncooperative behavior is the key. Some reaction should be in place that puts a malicious or selfish node at a disadvantage. This punishment may be isolation. Furthermore, a mechanism should be in place to “re-socialize” or “re-integrate” [BB01] a node wrongfully accused of malicious behavior or one that is reformed and has not misbehaved for a certain amount of time. In mobile ad hoc networks, it is favorable to isolate misbehaving nodes. This can be done by defining suitable cost and profit to routing and forwarding favors and maintaining a record of experiences with uncooperative node (Hypothesis, Null Hypothesis). In order to accomplish this, the following questions must be answered:

- 1) Is incorrect forwarding prevented?
- 2) Is it possible to insert bogus routing information or traffic attraction?
- 3) Is it possible to maliciously alter the route cache?
- 4) Is there any mechanism in place to punish selfishness?
- 5) Is collaboration and fairness encouraged and effective?
- 6) Is malicious and selfish behavior detected and discouraged?
- 7) Are error messages sent and recorded correctly?
- 8) Are users motivated to stay switched on and forward packets?
- 9) Does the mechanism discourage or prevent overloading the network?
- 10) Is it robust?
- 11) Is security increased in mobile ad hoc networks by incorporating incentives to cooperate in a secure routing protocol?

An incentive to cooperate mechanism and a secure routing protocol are efficient in their own right. However, combining the two separate mechanisms may cause the following: Network overloading

- 1) Slow detection of malicious behavior
- 2) Decrease in security of mobile ad hoc networks.

III. METHODOLOGY

A Instruments

GloMoSim (Global Mobile Information System Simulator) is the simulation mechanism used to implement the proposed protocol in this research. GloMoSim is a scalable simulation environment, developed at UCLA Parallel Computing Laboratory, which effectively utilizes parallel execution to reduce the simulation time of detailed models of large communication networks. GloMoSim can be used to simulate a variety of wireless networks including multi-hop ad hoc networks, traditional Internet protocols, and symmetric communication using direct satellite broadcast.

GloMoSim is built using a layered approach similar to the OSI seven layer network architecture with standard APIs defined between the different simulation layers. This allows rapid integration of models developed at different layers by independent people without affecting the other layers. Actual operational code can also be easily integrated into GloMoSim with this layered approach, which is ideal for a simulation model as it has already been validated in real life and no abstraction is introduced [BTA03].

GloMoSim is a scalable simulation library for wireless network systems built using PARSEC (PARAllel Simulation Environment for Complex systems), a parallel programming language for sequential and parallel execution of discrete-event simulation models. GloMoSim is a so-called event driven simulator meaning that the simulation model consists of different events controlling the course of action throughout the simulation. An event, such as a packet reception or a movement of a node, is defined as an incident which causes the system to change its state. Discrete events can only occur during a distinct unit of time during the simulation and events are not permitted to occur in between time units [TN02].

Its primary purpose is to simulate very large network models that can scale up to a million nodes using parallel simulation to significantly reduce execution times of the simulation model [BTA03]. Table 1 lists the protocols currently supported by the different simulation layers.

Layers	Protocols
Mobility	Random waypoint, Random drunken, Trace based
Physical Propagation (Radio)	Two ray, Free space, Rayleigh, Ricean, SIRCIM
Radio Model	Noise Accumulating
Packet Reception Models	SNR bounded, BER based
Data Link (MAC)	CSMA, IEEE 802.11, MACA
Network (Routing)	AODV, DSR, Bellman-Ford, Fisheye, OSPF, WRP
Transport	TCP and UDP
Application	CBR, FTP, HTTP, Telnet

Table 3.1 Models currently supported by GloMoSim

GloMoSim is configured by a number of predefined parameters supplied in a configuration file. These parameters will be defined here in order to understand their use in the proposed protocol:

- **SIMULATION-TIME:** represents the maximum simulation time

- **SEED:** a random number used to initialize part of the seed of various randomly generated numbers in the simulation
- **TERRAIN-DIMENSIONS:** the physical terrain in which the nodes are being simulated
- **NUMBER-OF-NODES:** number of nodes being simulated
- **NODE-PLACEMENT:** describes how nodes are placed in the terrain during the simulation
- **MOBILITY:** describes the movement of nodes
- **PROPAGATION-LIMIT:** tells the simulator how weak a signal may become before it is ignored in the simulation
- **PROPAGATION-PATHLOSS:** describes the attenuation of the radio signal depending on many factors in the surrounding environment
- **NOISE-FIGURE:** represents the background noise found in the simulated environment
- **TEMPERATURE:** represents thermal noise
- **RADIO-TYPE:** describes what radio model is being used
- **RADIO-FREQUENCY:** represents the radio frequency used to transmit and receive packets
- **RADIO-BANDWIDTH:** represents bandwidth (bits per second)
- **RADIO-RX-TYPE:** represents the packet reception model
- **RADIO-TX-POWER:** describes the radio interface transmission power in dBm (Decibel milli)
- **RADIO-ANTENNA-GAIN:** represents the ratio of the radiation intensity in a given direction to the radiation intensity averaged over all directions
- **RADIO-RX-SENSITIVITY:** describes how weak a signal may be
- **RADIO-RX-THRESHOLD:** the minimum power for a received packet
- **MAC-PROTOCOL:** the Medium Access Protocol used by the MAC layer
- **PROMISCUOUS-MODE:** determines whether or not nodes can overhear packets destined for another node in DSR (Dynamic Source Routing) protocol
- **ROUTING-PROTOCOL:** the routing protocol used
- **APP-CONFIG-FILE:** the location of a list of applications to be run during the simulation and their formats
 - FTP <source node><dest node><amount sent><start time>
 - TELNET <source node><dest node><duration><start time>
 - CBR <source node><dest node><items to send><item size><interval><start time><end time>

A. Design

In order to determine whether or not security will be increased by incorporating an incentive to cooperate in a secure routing protocol, a routing protocol must be chosen. DSR (Dynamic Source Routing) is the protocol of choice. In

DSR, if a packet needs to be sent, the sender constructs a source route in the packet's header, giving the address of each intermediate node in the network through which the packet should be forwarded in order to reach the destination. The sender transmits the packet over its wireless network interface to the first hop identified in the source route. When a node receives a packet, if it is not the destination, it transmits the packet to the next hop identified in the source route located in the packet's header.

In a mobile ad hoc network, each participating node must maintain a route cache in which it retains source routes that it has learned. If a packet needs to be sent, the sender first checks the route cache for a source route to the destination. If no route is found, the sender may attempt to discover one using the route discovery protocol. This protocol allows any node in the mobile ad hoc network to dynamically discover a route to any other node in the network, whether directly reachable within wireless transmission range or reachable through one or more intermediate nodes [JM88].

Each node monitors the correct operation of a route in use. This route maintenance is accomplished by continuously sending periodic routing updates. Routing updates are triggered if a node moves out of transmission range, fails, or powers off.

DSR has already been implemented in GloMoSim. It has been modified in order to include an incentive to cooperate called a bean. Within each node structure, two parameters have been added, *ttlbeans* and *beanpurse*. The *ttlbeans* parameter represents the total number of beans that each node has. Initially, each node has 500 beans. The *beanpurse* parameter is used to transmit a packet. Each time a packet must be sent by a node, there must be enough beans in its *beanpurse* to reach the destination. As each intermediate node forwards the packet, it removes beans from the *beanpurse* for providing the forwarding service; therefore, it increases its total bean count. A node cannot transmit a packet without any beans.

A C structure, called "GloMoNode", holds these parameters. Within this structure, a node's address, id, and other variables are defined. In order to implement the incentive to cooperate, several files within GloMoSim were modified. These files include *dsr.h*, *dsr.pc*, and *nwip.pc*. Within *dsr.h*, two variables, *MAX_BEAN_COUNT* and *DSR_WAIT_TIME_TO_REJOIN*, were included. *MAX_BEAN_COUNT* determines the initial value of beans that any node is allowed to have. *DSR_WAIT_TIME_TO_REJOIN* determines how long a node will have to wait if it has run out of beans and would like to rejoin the network.

To prove or disprove the hypothesis, several simulations were performed. The main simulation parameters are given in Figure 3.1. The variations within the simulations are in the number of nodes and the applications used within the APP-CONFIG-FILE. Furthermore, the simulations were run both with and without the incentive to cooperate. In order to determine the degree of cooperation among the nodes, the following formula was used from [LBH02]:

$$out_f = (NB - C)/(N+1),$$

where out_f is the number of packets a node must forward if it wants to maximize its own benefit, N is the maximum number

of intermediate nodes, B is the battery power, and C is the current value of the bean counter.

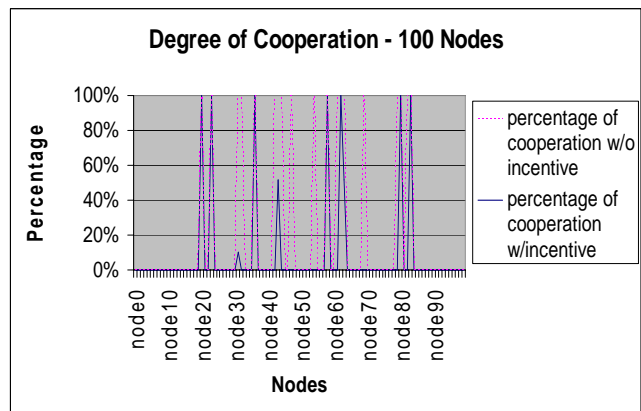
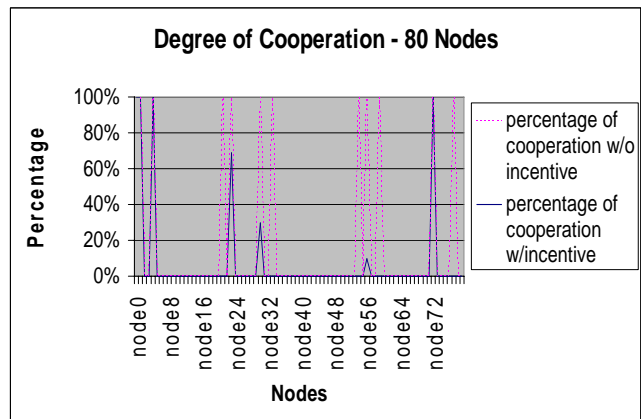
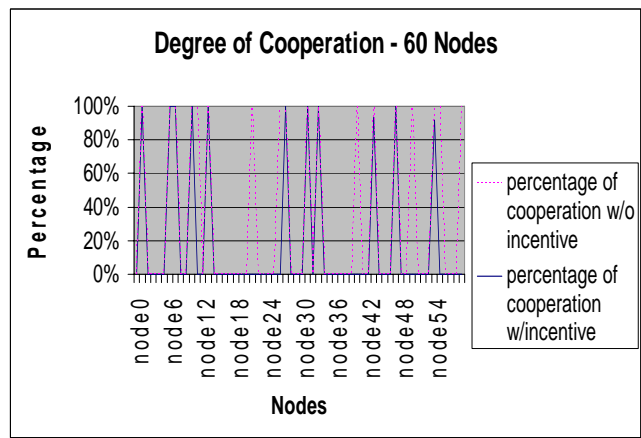
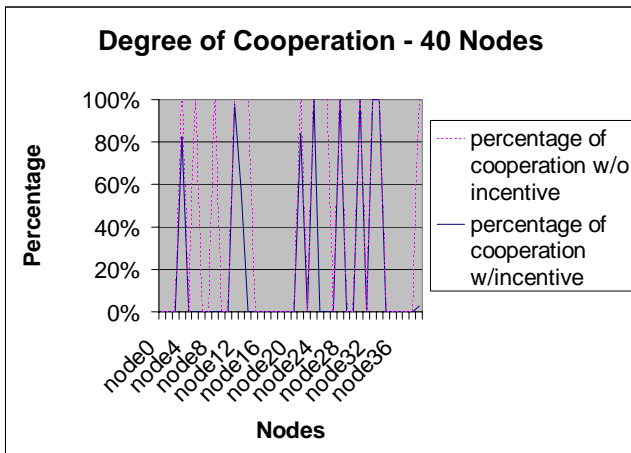
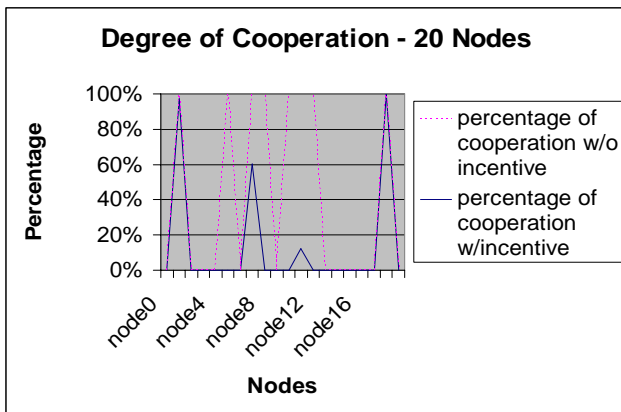
SIMULATION-TIME		
5M		
SEED	9	
TERRAIN-DIMENSIONS		(1000, 1000)
NUMBER-OF-NODES	10	
NODE-PLACEMENT	RANDOM	
MOBILITY		RANDOM-WAYPOINT
MOBILITY-WP-PAUSE		30S
MOBILITY-WP-MIN-SPEED	1	
MOBILITY-WP-MAX-SPEED	3	
MOBILITY-POSITION-GRANULARITY	0.5	
PROPAGATION-LIMIT		-111.0
PROPAGATION-PATHLOSS		TWO-RAY
PROPAGATION-FADING-MODEL		RICIAN
RICIAN-K-FACTOR	5	
NOISE-FIGURE	10.0	
TEMPERATURE	290.0	
RADIO-TYPE		RADIO-ACCNOISE
RADIO-FREQUENCY		2.4e9
RADIO-BANDWIDTH	2000000	
RADIO-RX-TYPE		SNR-BOUNDED
RADIO-RX-SNR-THRESHOLD	10.0	
RADIO-TX-POWER		15.0
RADIO-ANTENNA-GAIN		0.0
RADIO-RX-SENSITIVITY		-91.0
RADIO-RX-THRESHOLD		-81.0
MAC-PROTOCOL		CSMA
PROMISCUOUS-MODE		YES
NETWORK-PROTOCOL		IP
NETWORK-OUTPUT-QUEUE-SIZE-PER-PRIORITY	100	
ROUTING-PROTOCOL		DSR
APP-CONFIG-FILE		./app.conf
APPLICATION-STATISTICS	NO	
TCP-STATISTICS		NO
UDP-STATISTICS		NO
ROUTING-STATISTICS	YES	
NETWORK-LAYER-STATISTICS	YES	
MAC-LAYER-STATISTICS	NO	
RADIO-LAYER-STATISTICS	YES	
CHANNEL-LAYER-STATISTICS	YES	

MOBILITY-STATISTICS	YES
GUI-OPTION	
	YES
GUI-RADIO	
	YES
GUI-ROUTING	
	YES

Figure 3.1 Main simulation parameters

IV. DATA ANALYSIS

The data collected is grouped by the number of nodes in the simulation. In order to determine the actual and calculated out_f , a set of statistics about each node was collected. For the simulations without the incentive to cooperate, the following statistics were collected: the maximum number of intermediate nodes, battery power, the number of packets forwarded for another node, out_f , and the percentage of cooperation. For the simulations with the incentive to cooperate, the current value of the bean counter was collected in addition to the above statistics.



V. RESULTS

In order to validate the hypothesis, several questions must be answered. First let's consider the results. The following charts display the degree of cooperation for the simulations performed for 10, 20, 30, 40, 50, 60, 70, 80, 90, and 100 nodes.

It is evident from the results displayed in the previous charts that with or without the incentive to cooperate, the number of nodes that participate in forwarding for one another is small and varying compared to the total number of nodes in the network. However, with the incentive to cooperate, there is a slightly lower percentage of cooperation.

With this lower percentage, there are certain disadvantages for security. The incentive to cooperate does not encourage users to stay switched on and forward packets, even though this is the only method to increase their stock of beans. With the incentive to cooperate incorporated in the DSR protocol, there is no significant increase in complexity or battery consumption. However, users refrain from collaboration and fairness which further degrades the quality of security within the mobile ad hoc network.

On the other hand, the proposed protocol discourages overloading the network and creating unnecessary traffic, because overloading requires sending packets and packets require depletion in the stock of beans. Selfish behavior can be detected and punishment enforced. For example, if a node chooses to overload the network with a surplus of packets and at the same time refuse to forward packets for other nodes, it will use up all of its beans. Once a node's bean count is zero, it has to wait a specified amount of time before it can begin to transmit packets again.

In addition to the before mentioned limitations, the proposed protocol has several other weaknesses. It does not consider the activity in each node's route cache; therefore, it is still possible to forward packets incorrectly, insert bogus routing information, and possibly generate phony error messages. Therefore, some malicious behavior remains undetected and unpunished.

VI. CONCLUSION

The protocol extensions presented in this paper include a mechanism to punish selfishness. Once a node has used all of its stock of beans, it has to wait a specified amount of time (minutes, hours, or days) before it can rejoin the network. With this mechanism in place, nodes are discouraged from overloading the network with packets. This fact exists because overloading requires sending packets and packets require depletion in the stock of beans. This solution ensures that the benefit each node receives from the network does not exceed what it contributes to it.

Also, this protocol presented is an extension to the Dynamic Source Routing protocol. Because this protocol allows nodes to operate in promiscuous mode, nodes are capable of overhearing packets destined for neighboring nodes. This ability enables neighboring nodes to quickly detect malicious and selfish behavior, and, in turn, generate the necessary error messages.

On the other hand, this implementation does not encourage nodes to remain switched on and forward packets for one another, even though this is the only way to increase their stock of beans. Nodes are assumed to be greedy, and they always want to increase their stock of beans. However, the results from the simulation indicate a decrease in the degree of cooperation when an incentive to cooperate is incorporated within the Dynamic Source Routing protocol. The following table describes the amount of decrease in collaboration and fairness:

Other weaknesses also exist. The fact still remains that malicious nodes may incorrectly forward packets, insert bogus routing information, and even alter their route cache.

The implementation presented here does not alter how the DSR

# NODES	% COOPERATING NODES WITH INCENTIVE	% COOPERATING NODES WITHOUT INCENTIVE	% DECREASE
10	20	30	10
20	20	25	5
30	16.7	23.3	6.6
40	17.5	25	7.5
50	12	16	4
60	16.7	23.3	6.6
70	10	12.9	2.9
80	7.5	13.75	6.25
90	6.7	15.6	8.9
100	9	12	3

Table 5.1 Percentage of Cooperating Nodes

protocol handles its source routing and route cache. This should be considered in future studies.

Several changes need to be made in order for this protocol to be more robust. It is still susceptible to various security attacks which include the following: message interception, copying, or forging; incorrect forwarding; and bogus routing advertisement.

Mobile ad hoc networks exhibit new vulnerabilities to security attacks because the success of the network depends on the cooperation of the nodes to facilitate communication. As opposed to traditional networks, mobile ad hoc networks do not rely on any fixed, centralized routing infrastructure; therefore, they can be highly dynamic, mobile, and unreliable. Mobile ad hoc networks have relatively unreliable wireless links, dynamic topologies and membership, constraints in bandwidth, computing power, and battery power, and often roam in dangerous environments.

When designing protocols for mobile ad hoc networks, special attention must be given to the security mechanisms for the increased requirements in this environment. Security mechanisms for traditional networks can not be readily applied to mobile ad hoc networks, because they often rely on infrastructures or are not scalable to a large distributed and dynamic environment.

This paper identifies the special requirements of mobile ad hoc network security and introduces a scheme to cope with them by retaliating for selfish behavior. The proposed scheme slightly increases security in one aspect; however, there are other aspects that have not been covered which can lead to failed communication within the network and denial-of-service attacks.

Security is a major challenge for mobile ad hoc networks, because good citizenship can not be assumed in the real world. This fact may deter users from participating in mobile ad hoc networks.

This research requires the analysis of a mechanism that combines an incentive to cooperate with a secure routing protocol. This research effort used analysis and simulation data provided by the specified references. The results are based only on previously recorded data as well as results

obtained from simulations performed using GloMoSim, a network simulator.

REFERENCES

- [BB01] Buchegger, Sonja, and Jean-Yves Le Boudec. 2001. *The Selfish Node: Increasing Routing Security in Mobile Ad Hoc Networks*. IBM Research Report, RR 3354.
- [BB02] Buchegger, Sonja, and Jean-Yves Le Boudec. 2002. *Cooperative Routing in Mobile Ad-hoc Networks: Current Efforts Against Malice and Selfishness*. In Lecture Notes on Informatics, Mobile Internet Workshop, Informatik 2002, Dortmund, Germany.
- [BH00] Buttyán, Levente, and Jean-Pierre Hubaux. *Enforcing Service Availability in Mobile Ad-Hoc WAnS*. In Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC).
- [BH02] Buttyán, Levente and Jean-Pierre Hubaux. *Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks*. <http://icawww.epfl.ch/Publications/Buttyan/ButtyanH03monet.pdf>.
- [BTA03] Bajaj, Lokesh, et al. *GloMoSim: A Scalable Network Simulation Environment*. http://pcl.cl.ucla.edu/projects/glomosim/obtaining_glomosim.html.
- [HR03] Rajan, Hridesh. *Ad hoc Mobile Networks*. <http://www.cs.virginia.edu/~hr2j/MANET.html>.
- [JM88] Johnson, David and David Maltz. *Dynamic Source Routing in Ad Hoc Wireless Networks*. <http://www.ics.uci.edu/~atm/adhoc/paper-collection/johnson-dsr.pdf>.
- [LBH01] Buttyán, Levente, and Jean-Pierre Hubaux. *Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks*. http://ntrg.cs.tcd.ie/htewari/papers/tr01_001.pdf.
- [TN02] Nilsson, Thomas. *A Tutorial On GloMoSim*. www.cs.umu.se/kurser/TDBD16/HT02/gsimtut.ps.
- [VJP02] Vinayakray-Jani, Preetida. 2002. *Security within Ad hoc Networks*. Position Paper, PAMPAS Workshop.