Cooperative and Reliable Packet-Forwarding on Top of AODV

Tal Anker[1 2], Danny Dolev[1], and Bracha Hod[1]

[1] School of Engineering and Computer Science, The Hebrew University of Jerusalem, Israel
{anker, dolev, hodb}@cs.huji.ac.il
[2] Marvell Semiconductor, Inc. 700 First Avenue, Sunnyvale, CA 94089
tala@marvell.com

***Abstract*— Cooperative and reliable packet forwarding presents a formidable challenge in mobile ad hoc networks (MANET), due to special network characteristics; e.g., mobility, dynamic topology and absence of centralized management. Lack of cooperation, due to misbehavior caused by selfishness or malice, may severely degrade the performance of the network.**

Previous studies, relying on reputation systems, have demonstrated solutions designed for Dynamic Source Routing (DSR) protocol.

This paper highlights various aspects of cooperation enforcement and reliability, when AODV is the underlying protocol. Furthermore, it presents a scalable protocol that combines a reputation system with AODV that addresses reputation fading, second-chance, robustness against liars and load balancing.

***Index Terms*— AODV, Reliability, Reputation System.**

I. Introduction

The self-organization, which characterizes MANET, combined with bandwidth-constraints of the links and limited battery power, make the network vulnerable to many attacks, primarily on the link and the network layers.

Various research studies have focused on increasing network trustworthiness. Most solutions use cryptographic primitives to address security attributes including availability, integrity, authentication, confidentiality, non-repudiation and authorization [1], [2], [3]. These solutions are not always suited to spontaneous networks, which lack a priori relations. Furthermore, they do not enforce cooperation and cannot prevent selfish or malicious attacks in the packet-forwarding phase.

Recent approaches toward cooperation in MANET [4], [5], can be classified into two different categories: (a) schemes based on reputation system [6], [7], and (b) techniques derived from games theory [8], [9], [10].

This paper deals with the first category, which contains three basic elements: misbehavior detection, misbehavior reaction and a reputation system that integrates between the parts. Our work addresses the various challenges presented by each of these elements, with a final goal of improving the network availability, reliability and robustness, without assuming any a priori relations between the nodes, and without requiring any cryptographic usage.

A. Motivation

AODV [11], [12], [13] is one of the leading routing protocols adopted by IETF for MANET.

It is an on-demand algorithm that builds routes between nodes, but only as desired by source nodes, and maintains these routes as long as they are needed. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and scales to a large number of mobile nodes.

Most of the research thus far has addressed selfishness and cooperation, assuming DSR [14] as the underlying protocol. The primary differences between AODV and DSR are: (a) DSR sources determine the whole path to the destinations, while in AODV the routing decision is made hop by hop; and (b) DSR nodes can maintain multiple paths in the routing cache, while AODV nodes record information of a single route only. The significantly greater amount of routing information that DSR nodes access enable their more rapid recovery from misbehavior. However, AODV surpasses DSR, in terms of storage and memory overhead [15]. For this reason, it is more scalable, and suited for large networks. Thus, handling misbehavior with AODV is a more challenging task.

B. Paper Contribution

Several solutions have been designed for AODV, most of which rely on explicit acknowledgment, rather than on observation [16], [17]. To our knowledge, this work is the first to combine a reputation system with AODV.

DSR nodes use the reputation information much more than AODV nodes. They may rate a full path and select one among multiple paths based on the rating. Thus, the assumption that a reputation system will be as effective in AODV as in DSR is wrong. Hence, it is necessary to examine the benefit of a reputation system in AODV environment.

Scalability is an important characteristic of MANET. However, no previous work has examined the scalability of a reputation system in large mobile ad hoc networks. We also handle cases of partial dropping and advanced liars in a wider manner than previous works.

The main difference between our reputation system and other reputation systems (as CORE and CONFIDANT) is in their approach to node evaluation. Most solutions combine the direct and indirect information into a single rating value, which is used to classify nodes. We incorporate the direct and indirect rating into three variables: total rating, positive actions and negative actions. In this way, two nodes with the same total rating but with a different number of observations (different history) will be classified differently. Therefore, our nodes' evaluation reflect better the performance over time and the number of required self-observations to classify a node as misbehaving is decreased. See section IV-C.1 for more details.

C. Paper Outline

The paper is organized as follows: Section II introduces the related work that was done in this area. The adversary model assumed in this work is described in section III. The main properties of our scheme are presented in section IV. Section V deals with the simulation framework and results. Section VI outlines the conclusions and future work.

II. Related Work

Much research has recently focused on the cooperation issue in MANET. Several related issues are briefly presented here.

Watchdog and Pathrater are two extensions to the DSR algorithm, proposed by Marti, Giuli, Lai and Baker in [18]. The watchdog identifies misbehaving nodes by listening promiscuously to the next node transmission. The pathrater uses the knowledge from the watchdog extension to choose a path that is most likely to deliver packets. The path rating is calculated by averaging the rating of the nodes in the path, where each node maintains a rating for all the nodes it knows in the network.

CONFIDANT protocol and various enhancements are presented by Buchegger and Le Boudec [19], [6], [20], [21] and [22]. Each node monitors the behavior of its next hop neighbors in a similar way to watchdog. The information is given to a reputation system that updates the rate of the nodes. Based on the rating, a trust manager makes decisions about providing or accepting route information, accepting a node as part of a route and similar decisions. When a neighbor is suspected of misbehaving, a node informs its friends by sending them an ALARM message. If a node rating turns out to be intolerable, the information is relayed to a path manager, which deletes all routes containing the intolerable node from the path cache. An enhancement of the basic protocol is presented in [21], providing a strong reputation system that deals well with false reputations. The enhanced protocol uses a modified Bayesian approach and introduces two new mechanisms: re-evaluation and reputation fading. Re-evaluation allows a node to redeem itself. Reputation fading prevents a sudden exploitation of an ephemeral good reputation.

CORE scheme and various related issues were described by Michiardi and Molva in [7], [23] and [24]. In this scheme, every node computes a reputation value for every neighbor, based on observations that are collected in a similar manner to watchdog. The reputation mechanism differs between subjective reputation, indirect reputation, and functional reputation. By avoiding the spread of negative rating the mechanism resists attacks such as denial of service. When a neighbor reputation falls below a predefined value, the service provided to the misbehaving node is suspended.

OCEAN, a scheme for robust packet-forwarding is proposed by Banal and Baker [8]. OCEAN, similarly to previous schemes, is based on nodes' observations. In contrast to previous mechanisms, no rating is exchanged and every node relies on its own information so the trust management is avoided. The rating is based on a counter that counts the positive and the negative steps a node performs and, based on a faulty threshold, the node is added to a faulty list. In the method for route selection, based on DSR, a node appends an avoid list to every RREQ and based on this list, a RREP is generated. A second-chance mechanism is provided to give nodes that were previously considered misbehaving another opportunity to operate.

III. Problem Statement

AODV is vulnerable to various kinds of attacks, as described in [25] and [26]. There are two main motivations which encourage nodes to misbehave: selfishness and malice. When dealing with packet-forwarding, there are several kinds of availability and integrity attacks [27]: dropping (complete or partial), misrouting, modification and fabrication. Malicious cooperation (such as a wormhole attack) and identity changes are also challenges attacks.

In our scheme, we assume a pattern of selfish nodes; a node can drop part or all the data packets that do not belong to it (black or gray holes). Selfish nodes are interested in saving their battery power, as well as having the capability to receive and transmit their own packets. However, these nodes are unlikely to modify or misroute packets, because such an activity consumes no less power than correctly forwarding that packet. Addressing malicious nodes involves a more complex security model, using cryptography primitives which is beyond the scope of this paper.

IV. Properties of the Scheme

A. Observation Method

Misbehavior can be detected with either passive or active acknowledgment methods. Our scheme detects anomalous behavior using neighbors observations by the passive acknowledgment mechanism, as in [18].

A transmitting node verifies successful unicast forwarding upon receipt of link-layer acknowledgement from the receiver. Then, it observes its neighbors' behavior by overhearing, either in direct mode (getting packet explicitly) or via promiscuous mode. By examination of the overheard packets, the node is able to confirm its neighbors' good behavior.

There are some inherent weaknesses in the passive acknowledgment, such as limited transmission power and collisions. There are more drawbacks to this technique in the AODV environment, such as the requirement for promiscuous mode and the need to add a next_hop field in the route entries [28]. Additionally, this technique analyzes wrong AODV nodes in several situations; e.g., when a node drops packets after a timeout during local repair, it is considered to be misbehaving. Still, we prefer this mechanism more than end-to-end acknowledgments [16] or probing packets [29], because it is associated with less overhead and delay, and suited more to traffic over UDP. Due to mistakes of this method, an appropriate number of observations is required before classifying nodes as misbehaving.

In highly reliable or very loaded system, the observations can be performed once for multiple packets, in order to save resources.

B. Reputation System

A reputation system is a system in which nodes participating in the system compute rating values and then advertises these values among the other nodes.

The rating representation is an important property of a rating scheme, since it characterizes the system's flexibility, robustness, and effectiveness. The rating is represented by a 32-float value in the continuous range [-1,1]. Use of a positive to negative range enables both reward and punishment. A continuous range is used in order to achieve maximal precision, but it comes at the cost of float value calculation, which is higher than integer values.

a) Neighbors Rating: Calculation and management of neighbors rating is done using the Beta distribution function [30], [31]. The Beta function is commonly used to represent probability distributions of binary events. It is defined as:

$$P(x) = \frac{(1-x)^{\beta-1}x^{\alpha-1}}{B(\alpha,\beta)} = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}(1-x)^{\beta-1}x^{\alpha-1}$$

$$\text{where } 0 \le x \le 1 \ , \ \alpha > 0 \ , \ \beta > 0$$

Given a process with two possibilities $\{x, \bar{x}\}$, the Beta function estimates the probability of x, based on past observations of x and $\bar{x}$, and by setting:

$$\alpha = 1 + observed\ number\ of\ x$$
$$\beta = 1 + observed\ number\ of\ \bar{x}$$

A node's behavior resembles a binary process. The amount of positive events over a given period are related to x, while negative events are related to $\bar{x}$ accordingly. It is possible to assign variable weights to various events; e.g., greater weight to data packet dropping than to control packet dropping.

Using the derived reputation function and its scaling, given in [30], we denote the direct rating of a node j by its 1-hop neighbor i, based on observations as:

$$DR_{i,j} = \frac{p_{i,j} - n_{i,j}}{p_{i,j} + n_{i,j} + 2} \tag{1}$$

$$\text{where } p_{i,j} = recent\ positive\ actions\ of\ j\ observed\ by\ i$$
$$n_{i,j} = recent\ negative\ actions\ of\ j\ observed\ by\ i$$

Past behavior is an integral part of the rating. The rating can be defined accordingly, as:

$$DR_{i,j}(t) = \frac{p_{i,j}(t) - n_{i,j}(t)}{p_{i,j}(t) + n_{i,j}(t) + 2} \tag{2}$$

$$\text{where } p_{i,j}(t) = \gamma p_{i,j}(t-1) + p_{i,j}(\Delta t)$$
$$n_{i,j}(t) = \gamma n_{i,j}(t-1) + n_{i,j}(\Delta t)$$
$$\gamma = weight\ of\ past\ behavior \ \ , \ 0 \le \gamma \le 1$$

Attacks of positive ratings misuse can be limited by giving more weight to the recent behavior than the past behavior, expressed by a small γ. Our computation uses the entire history, but as time progresses the impact of old history is diminished. This technique of fading allows effective rating in high mobility network.

$DR_{i,j}(t)$, as defined in equation (2), is the rating value published in the reputation protocol.

The total rating, expressed by $TR_{i,j}$, combines the direct rating $DR_{i,j}$ with reputation information from a set of 1-hop neighbors K, denoted by $DR_{k,j}$ for every $k \in K$.

K is defined as a set of neighbors that are either evaluated as trusted, or their rating report passes the deviation test, as proposed in [21]. The deviation test of a node i checks that the difference of a given rating value $DR_{k,j}$ from the expected rating value $TR_{i,j}$ is not too great. The test is formulated as:

$$\begin{array}{ll} if\ |TR_{i,j} - DR_{k,j}| \le \Delta & accept\ DR_{k,j} \\ otherwise & reject\ DR_{k,j} \end{array} \tag{3}$$

There is no synchronization between the nodes, so we do not define those values with time dependency. A node i may calculate the total rating at time t, either with $DR_{k,j}(t-1)$ or with $DR_{k,j}(t)$.

These two conditions make the system robust against some types of liars, but do not perfectly prevent smart liars, as shown in section V-B.3.

Combination of direct and indirect rating can be done easily by accumulation of the direct and indirect positive and negative actions, as described in [30]. However, the rating distribution includes one float value, since distribution of two values that represents $p_{k,j}$ and $n_{k,j}$ is much too expensive in terms of storage and bandwidth. Thus, it is possible to define a weight, denoted by w, such that $p_{k,j} + n_{k,j} = w$. Using the given w, a node can estimate $p_{k,j}$ and $n_{k,j}$ as the following:

$$\tilde{p}_{k,j} = \frac{w(1+DR_{k,j})}{2}, \quad \tilde{n}_{k,j} = \frac{w(1-DR_{k,j})}{2}$$

so that the total rating is defined as:

$$TR_{i,j}(t) = \frac{p'_{i,j}(t) - n'_{i,j}(t)}{p'_{i,j}(t) + n'_{i,j}(t) + 2} \tag{4}$$

$$\text{where } p'_{i,j}(t) = \delta p'_{i,j}(t-1) + p_{i,j}(\Delta t) + \textstyle\sum_{k \in K} \tilde{p}_{k,j}$$
$$n'_{i,j}(t) = \delta n'_{i,j}(t-1) + n_{i,j}(\Delta t) + \textstyle\sum_{k \in K} \tilde{n}_{k,j}$$
$$\delta = weight\ of\ total\ past\ behavior \ \ , \ 0 \le \delta \le 1$$

w represents the weight that the node scores, which is a trade-off between robustness and second-hand information usage.

The value of w determines the influence of surrounding neighbors, as well as the vulnerability of the system due to false information. Too small of a value for w might make the whole reputation system irrelevant, since the effect of distributed information is negligible.

Different weights may be assigned to nodes' reports, based on trustworthiness. In the current simulations, we have decided to apply an equal weight value to all the nodes. This value is contingent on the number of neighbors, thus creating a correlation between the effect of the indirect information over the direct rating, when there are many neighbors.

Since the rating combination is both commutative and associative, and we apply the same weight to all the nodes, the total positive and negative actions, $p'_{i,j}(t)$ and $n'_{i,j}(t)$, can be defined alternatively as:

$$p'_{i,j}(t) = \delta p'_{i,j}(t-1) + p_{i,j}(\Delta t) + \tfrac{w}{2}(|K| + \textstyle\sum_{k \in K} DR_{k,j})$$
$$n'_{i,j}(t) = \delta n'_{i,j}(t-1) + n_{i,j}(\Delta t) + \tfrac{w}{2}(|K| - \textstyle\sum_{k \in K} DR_{k,j})$$

b) Remote Nodes Rating: Holding full information about the nodes along the path is neither feasible and nor scalable in AODV. Our simulations show that managing rating even for 2-hop nodes is not worthwhile. The mobility of the nodes renders this information relevant, but as the information tables grow, more overhead and latency are involved. This significantly decreases the scalability, which is an essential property in our scheme.

c) Trust: Misbehaving nodes might spread false rating information to obtain their own benefit. There is no direct correlation between the routing protocol and rating protocol behavior. Therefore, it is essential to maintain information about the trustworthiness of the nodes and the estimation of the rating reports reliability. The amount of recent belief on node j by node i can be expressed as:

$$T_{i,j} = \frac{t_{i,j} - f_{i,j}}{t_{i,j} + f_{i,j} + 2} \qquad (5)$$

where $t_{i,j} = recent\ true\ reports\ of\ j\ received\ by\ i$
$f_{i,j} = recent\ false\ reports\ of\ j\ received\ by\ i$

If the reported rating is close enough to the estimated rating, then the number of true reports is incremented; otherwise the number of false reports is incremented.

A fading mechanism as time progresses is performed in the same way as the direct rating, defined in equation (2). Each node maintains its own trust map, so trust values are not exchanged between the nodes.

d) Rating Exchange: Rating exchange in MANET is derived from its unique characteristics. The transmission cost affects the frequency and the range of dissemination towards a local and limited scheme.

The mobility of nodes, however, encourages a global model for better performance. In a dynamic network or a large area with a local rating exchange, the long-living property of a reputation system [32] may not be applied. Two scenarios that may happen in such networks are: (1) a node might not have enough time to discover misbehaving nodes or to punish them. (2) a misbehaving node may act faultily in a region, and while detected by its neighbors, it can move to a new area, where nobody knows it.

The basic conflict between transmission cost and mobility cannot be solved easily. In order to avoid the broadcast storm problem [33], we limited the reputation distribution into 1-hop range and the data within the rating packets. When the misbehaving is widespread, flooding is better than polling. Consequently, our reputation distribution is performed continuously, when both good and bad ratings of 1-hop active neighbors and the misbehaving nodes who are on the black list, are broadcast. Other possibilities, e.g. black list distribution for a larger area, are too costly or have the risk of malicious nodes misuse.

As will be shown, this conflict directly impacts the reputation system's performance in large networks.

C. Reaction

Every node utilizes the rating information to classify its neighbors. Then, it can make the forwarding decision, both for path selection for its own data packets, and to decide which node to punish or reward, by dropping or forwarding this node's traffic.

1) Nodes' Classification: Nodes are evaluated by a combination of both total rating $TR_{i,j}(t)$ and total number of observations $p'_{i,j}(t)$ and $n'_{i,j}(t)$. Two nodes with the same total rating, but with different history are classified differently. For example, a node with a neutral rating can be either new in the system or inconsistent. Its history reveals its real behavior.

Misbehaving nodes are evaluated by their total rating and the recent negative actions they perform. Two nodes with the same bad record, one because of temporarily incorrect analysis and the other because of constant misbehavior, are classified differently. The first node, which has only a few negative actions, is given a chance to operate while the second node, which evidences significant misbehavior, is isolated.

The same concept applies to good nodes. One node with more positive actions than another node, but with the same rating is considered more reliable.

Load nodes are also estimated by their total rating and their recent positive actions. Basically, a node with a good reputation by several nodes and a large number of recent observations relays more traffic (and has more load) than a node with a lower number of observations.

The usage of both rating and number of observations leads to an improved classification of the nodes.

2) Path Selection: Several solutions may be applied to increase paths reliability, using the 1-hop neighbors rating that every node maintains. Using multipath algorithms [34], such as: [35], [36] and [37], to enable selection from various potential routes, is accompanied by high overhead, latency and poor effectiveness in low-density networks. Solution that involves multiple RREP from the destination hold problems of loops and requires costly maintenance [38].

Our solution is a simpler variation of the original protocol, using a greedy strategy. Every node selects the most reliable next hop that it knows on the path. This strategy maximizes the reliability of the path in terms of probability that the packet will be forwarded correctly, if no cooperation exists between malicious nodes.

The concept of reliable paths is based on differentiation between three reliability levels of nodes who are taking part in the path selection. These levels are based on both the total rating and the total number of positive actions, as follows: (1) an unreliable node is a node with low rating, but with not enough evidence to identify it as misbehaving. Such a node is never chosen as part of a path. (2) a reliable node is a node with average good rating. This node is a good candidate for participating in a route. (3) a very reliable node is a node with a higher rating. Such a node is preferred by multiple nodes, so we wish to balance the load among such nodes. When a reliable node is favored by many nodes, it may become congested; thus, there is another metric that also considers load balancing. In this metric, every node estimates the load of its neighbors by their recent positive actions, and selects the less congested node among a group of nodes with a high rating.

The protocol modifications are presented below.

Processing Route Requests

a) *Constructing full path:*
When a node has a reply to the request, and this is the first request that was received, it sets a reverse route and generates a reply only if the previous hop is the request originator or a very reliable node.
Otherwise, it sets a timer and processes every identical request that it receives from other nodes.
On subsequent requests, if it has not previously transmitted a reply, it checks the node's reliability and if it finds a very reliable node, it sets a reverse route and generates a reply.
On a timeout, if no reply was sent, the node chooses the most reliable node from the reliable request transmitters, sets a reverse route to it and transmits the reply.
If there are no reliable transmitters, the node does not reply at all.
The result of use of this method is that a node prefers transmission through a very reliable node over transmission through some other reliable node, if it is not too far or too congested. This enhances the path reliability.

b) *Constructing a reverse path:*
If the node does not receive a reply to the request, it examines every request with a hop_count that is identical to, or less than, the first request received from any node.
If the request was received from an unreliable node, then the node drops it.
Upon receiving an initial request from a reliable node, the node processes it per the original protocol: sets a reverse route, relays the request and transmits buffered packets.
If a request was previously processed, but the later request originates from a significantly more reliable node (with load-balancing consideration), then the node sets a new reverse route and transmits buffered packets, if such exist.
In this way, the node ensures a higher probability of reliable reverse paths.

Processing Route Reply

a) If the reply was received from the destination itself, or from a node that appears reliable, then the node processes the reply and sets a route to the destination. Otherwise, the node ignores the reply.

b) If the receiving node is an intermediate node, it forwards the reply, only if the next hop in the path is reliable.

The Modified AODV Protocol

This new path selection utilizes the information about 1-hop neighbors only, in contrast to DSR solutions, which use rating on several nodes along the path. It involves drawbacks as additional processing overhead and latency, and includes other significant weak points, relating to the protocol properties: (1) A basic characteristic of AODV is that the most available (and shortest) route is chosen in each route discovery. This property is not saved in our modified AODV protocol and there are many situations in which a node chooses a longer path that is more vulnerable to misbehaving nodes and route breaks, so in the overall view it does not provide the highest reliability.

Naturally, because of the short delay that is configured (80ms - which is based on the assumption of the simulation, that node traversal time is 40ms), the path length is bounded. Additionally, the selection of a longer path can be done only once - by the reply originator, so practically the length of new paths is not much longer than the original paths. (2) The reliability requirements may result in dropping more packets, because there are fewer routes. This dropping may affect the rating protocol, when well-behaving nodes are considered as misbehaving.

Despite that, the results show that even the limited information helps to improve the throughput considerably.

3) Punishment and Reward:

a) Routing Protocol: In optimal systems with full fairness, nodes get service according to their network contribution. This is achieved by various Quality of Service (QoS) mechanisms. QoS is a significant issue in networking and in MANET, and has been discussed in many papers. We leave it for a future work. We offer a simpler approach which differentiates between well-behaving nodes and misbehaving nodes, with an emphasis on punishment. A misbehaving node is isolated from a well-behaving node when its rating decreases below a predefined threshold. The isolation is done by performing a link-break operation (sending RERR packet) and by ignoring further packets from this isolated node (as if the link to this node is down). If a node receives packets of a misbehaving node through a highly reliable node, it transmits them in order to avoid erroneous suspicions of misbehavior. In the absence of discrimination, when the node behaves badly in a consistent manner, most of its neighbors isolate it and thus it does not merit proper service. Over time, the rating of the misbehaving node fades and increases to zero, so it is afforded a second chance to return back to the network. In this second chance, the node is considered as disaster-prone. This means that further identification of it as a misbehaving node requires fewer observations, and if it is found to be misbehaving again, it is rejected for a significantly larger period. Well-behaving nodes receive service, and a short temporary problem does not harm their operation.

b) Rating protocol: Nodes that distribute correct rating information have the chance to modify rating of misbehaving nodes and thus to speed up their detection and isolation. There are many situations where two nodes report honestly, but due to inconsistency of the node or missing evidence, their rating reports are considered as false. Since there are many fragile situations, rating of the nodes is not affected by their trustworthiness, so liar nodes are not punished in the routing protocol for their misbehavior in the rating protocol.

V. Simulation and Analysis

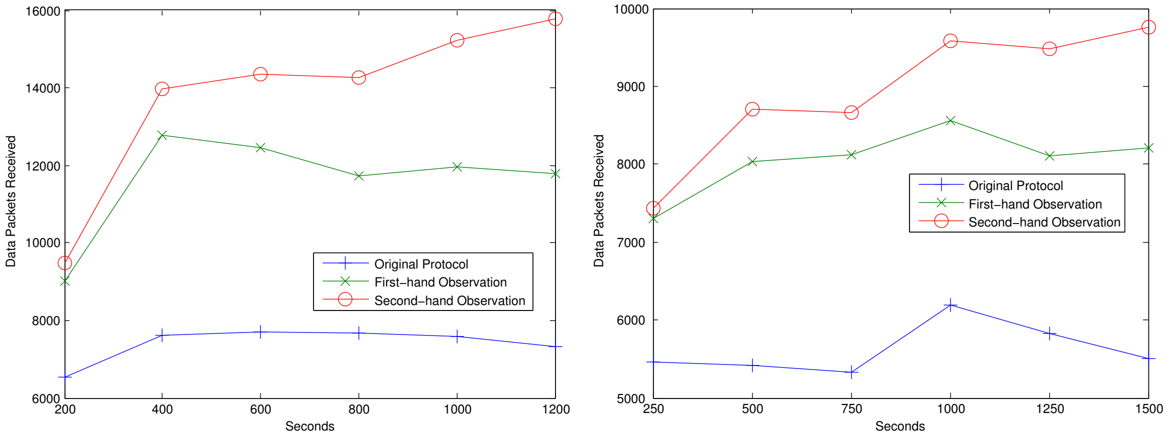
A. Simulation Model

We performed our simulation on a GloMoSim simulator [39]. Various network scenarios were analyzed to prove the accuracy of the model and its characteristics.

Every plot was taken as an average of ten different runs. In the simulation experiment, we tested networks from 10 to 500 mobile hosts.

The area, in which the nodes were placed randomly, was chosen based on the metrics presented in [40] and [41] to maintain the network density and connectivity as constant and balanced. Specifically, the area size was 1000m x 1000m, 1500m x 1500m and 3500m x 3500m for networks with 50, 100 and 500 nodes, respectively.

In all the simulations, we used standard parameters of the channel and radio model: a channel capacity of 2MB/s, free



(a) Throughput of Well-behaving Nodes - 50 Nodes, 15 Sources, 15 Black Holes.

(b) Throughput of Well-behaving Nodes - 100 Nodes, 20 Sources, 30 Black Holes.

Fig. 1. First-hand and Second-hand Observation Effects on Well-behaving Nodes Reward. The network is characterized by full mobility and load. Every node runs 4 different sessions in each period (200 seconds) at a rate of 10 packet/second. The sources, destinations and start time are selected randomly. Different sessions provide various possibilities for path selection. The relatively high rate of packets (usually 4 packets/second is the normal rate) was used to decrease the cost of the path, by using it intensively for a short period of time, when it was first constructed. Our solution works also for slower rates, but slower rates require more control packets.

space propagation model and radio propagation range of 250 meters. The IEEE 802.11 protocol was used as the Medium Access Control protocol.

The mobile nodes use the random waypoint as the movement model. The range of the speed is from 5 to 20 m/s. Simulations in [42] have shown that zero minimum speeds in the random waypoint model cannot reach a steady state because the speed continuously decreases as the simulation progresses. The solution is to set a positive minimum speed and, thus, we assign our simulation a minimum speed of 5. The pause time varies randomly between 0 and 500.

The traffic was produced using a traffic generator, which randomly generated Constant Bit Rate (CBR) sessions. The data packet size was 64 Bytes, and no fragmentation was used. We avoided data packet transmissions between neighbors, and all the results refer to packets on routes that are above 1-hop length, so more accurate results are achieved.

Default values for some of the protocol parameters are given in Table I. These values do not purport to be the optimal ones for any network, but we found them as reasonable and effective in the simulation. All the original parameters of AODV remained.

B. Simulation Results and Analysis

In the following simulation results, we analyze: (1) complete and partial dropping (black holes and gray holes, respectively), which are the most common attacks by selfish nodes; (2) advanced liars, to verify the robustness of the scheme, when there are smart liars; (3) the benefit of the reputation system in large networks.

1) Advantages of Reputation System: The assumption of use of reputation systems is that additional information helps nodes to detect and react better. This assumption should not be taken for granted. There are many scenarios in which the additional information hardens the detection, as a case of a black hole that seems reliable to those nodes which do not forward data through it, so their good rating advertising slows down its detection. Additionally, due to the strict reputation acceptance, that limits the influence of liars, further information might not be used appropriately.

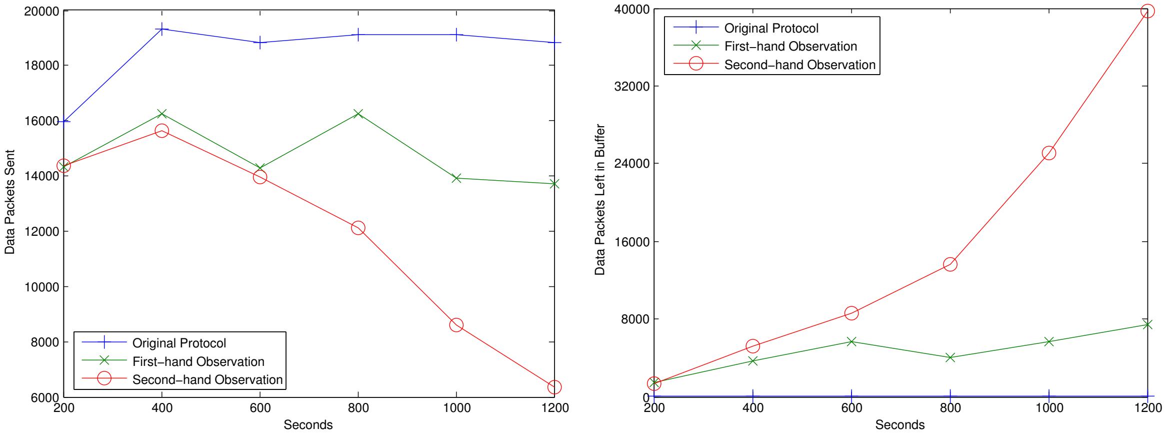
Parameter	Value
rating interval for rating calculation and distribution	8.5s
γ, δ, weight of past behavior for direct and total rating	0.8
μ, weight of past belief	0.8
Δ, the deviation test window size	0.5
w, maximum weight of indirect rating (depends on the number of neighbors)	5
minimal rating for black list insertion (together with some minimal observations. As much as the rating is smaller, the smaller number of observations that required)	-0.2
unreliable node's rating (together with number of observations)	(-0.2 - 0.25)
reliable node's rating (together with number of observations)	[0.25 - 0.75)
very reliable node's rating (together with number of observations)	[0.75 - 1]
reply delay	80ms

TABLE I
CONFIGURATION PARAMETER

The reputation exchange is found valuable mainly for the following reasons:

1. Generally, a minimal number of observations is required before a nodes is suspected to be a misbehaving one. By sharing the experience of other nodes, the number of self-observations is decreased and the detection is quicker, even when the minimal number is low.
2. The number of false positives is usually lower with reputation exchanges, because other nodes' observations moderate a temporary mistaken rating.
3. In a high mobility network, when a node does not have enough information about its surrounding, the information it receives may be useful during its first steps.

However, a system with a rating exchange may not always have a significant advantage, and may even perform worse



(a) Data Packets That Misbehaving Nodes Succeed in Transmitting to Each Period.

(b) Data Packets That Were Left in The Buffer Because No Route Was Found to The Destination.

Fig. 2. Punishment of Misbehaving Nodes. 50 nodes, 15 sources and 15 misbehaving nodes with the same simulation parameters as the previous. The sources in 2(a) are the misbehaving nodes which transmit packets to the other good nodes. In 2(b), the sources are well-behaving and the destinations are misbehaving. The punishment of a node can be reflected either by the number of packets it does not succeed in transmitting (meaning that it does not manage to construct routes) or by the number of packets that it does not receive because of its isolation.

compared to a scheme without the information distribution. This happens when:

1. Significant amounts of nodes do not have a correct map of their neighbors or there is no sufficient trust relations between the nodes, e.g. too high mobility in a large area, bad connectivity, bad participation, etc.
   The information acceptance is very low in such cases so its effect is negligible.
2. A relatively static network, where only a few arrivals and departures occur or the number of shared neighbors between two neighboring nodes is very low.
   The exchanged ratings do not contribute worthwhile information in such conditions.
3. Frequent packet dropping because of load, collisions, long paths and other network factors that make the system unstable.
   In such circumstances, there are many false positives and the overhead of the rating exchange is bigger than the information contribution.

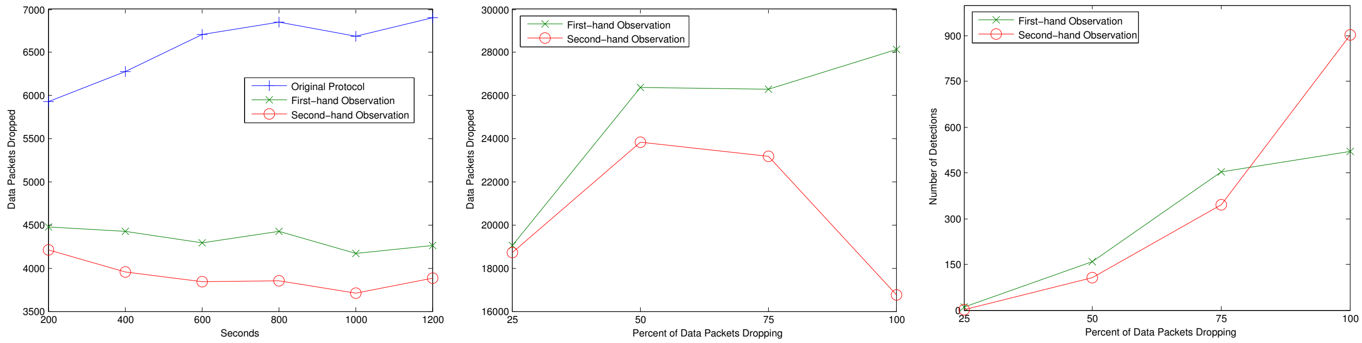
By examination of the throughput (Fig. 1), we can see significant improvements by both first-hand observation method and a reputation system, compared to the original AODV protocol. However, the first-hand observations improve the throughput only locally (the changes in the throughput as the time advances are minor), while the second-hand information gradually affects all the network and causes consistent improvement as time progresses. Note, however, that it takes time for the network to become stable because there is a second chance for every misbehaving node. Similar tendencies can be shown for larger networks with 100 nodes. The advantages of the reputation system when the network is larger are applied less obviously than smaller networks since the system converges more slowly.

We can see the same trend even more prominently when we look at the punishment of misbehaving nodes (Fig. 2). The differences between the schemes are clearer in the punishment graph, since its components are not effected by collisions, malicious dropping and other external causes to packet dropping, as in the throughput graph.

2) Partial Data Packets Dropping: Detecting and punishing gray hole nodes is difficult for several reasons. First, monitoring is limited because of all the collisions and mobility so a strict treatment to nodes with a relatively low rating would probably cause a large amount of false positives, which is undesirable. On the other hand, soft handling of such cases would give the gray holes opportunities to continue with their behavior. In addition, the reputation system effectiveness is limited in case of node discrimination because there are many contradictions between the exchanged ratings. Lastly, the inconsistent behavior requires costly path maintenance to ensure that permanently selected paths remain reliable, since a node can build up a temporary good reputation, be chosen in a route construction, and then misbehave but not beyond a faulty threshold that causes its isolation.

The path maintenance involves further issues. For example, when a node detects a neighbor that does not seem to be reliable, and there is not enough evidence for that, there is a greater doubt whether to continue sending through it and take the chance that it is not reliable or to disconnect it, have an overhead of local repairs and take the risk that the packets in its buffer would be deleted because there is no alternative route. In situations of too many disconnections, a good node might be suspected as malicious because it does not find alternative routes.

According to the simulation results (Fig. 3(a)), the monitoring is as effective in partial dropping as in total dropping. However, in contrast to the throughput improvements along the time, as was shown in Fig. 1, there are almost no changes in both systems as the time advances. Figures 3(b) and 3(c) provide some explanation for this. Generally, the forwarding reliability is the major concern of a node. It prefers avoiding misbehaving nodes, rather than waiting for total verification of malicious nodes in order to punish them. Full identification of a misbehaving node requires that its rating be under the

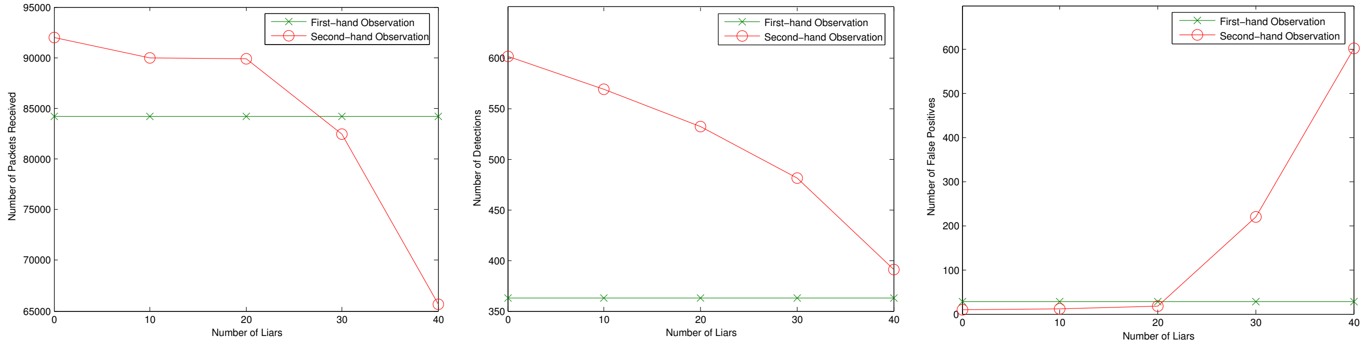


(a) Data Packets Dropped Along the Time. Dropping Probability of 50%.

(b) Data Packets Dropped.

(c) Identifications of Nodes as Misbehaving.

Fig. 3. Partial Data Packets Dropping. Simulation for 1200 seconds, 50 nodes, 15 sources and 15 misbehaving nodes. The traffic parameters are the same as described in Fig. 1. Each misbehaving node transmits all control packets properly. Thus, the 25%, 50%, 75% and 100% dropping probability of data packets result in approximately 18%, 32%, 45% and 78% dropping from the total transmitted packets accordingly. Fig. 3(a) shows the packets dropping along the time. Fig. 3(b) and Fig. 3(c) present the differences between First-hand observation scheme vs. the full reputation system in the various cases of packet dropping. Note, that since there is a second chance, each node can be identified as misbehaving twice. Therefore, the total number of identified misbehaving nodes can be quite large. In addition, because of the avoidance, not all the misbehaving nodes must be identified as bad.



(a) Throughput.

(b) Identifications of Nodes as Misbehaving.

(c) False Positives.

Fig. 4. Liars Effect. Simulation for 1200 seconds, 50 nodes, 10 nodes as black holes and similar traffic parameters as before. Until they are isolated from the network, the black holes distribute correct information, then their reports are ignored and the liars have a larger effect. After some period of time, when the misbehaving nodes are completely isolated, more than 20 liars are considered as the majority of the running nodes.

faulty threshold of zero with enough evidence (observations). This means that a node is detected and punished only after it drops about 50% or more of the total packets[1]. When the dropping percentage is less than half, there is only avoidance of misbehaving nodes. The avoidance consists of a permanent verification that an active route stays reliable over time and disconnection from the next hop, when its rating decreases beyond some threshold. This disconnection does not involve punishment and isolation, since there is insufficient evidence that the next hop is malicious. However, the node itself prefers not to forward packets through it. The avoidance is effective in increasing path reliability, but because of no punishment, it performs only locally.

Despite this, the reputation system is still better than relying on self-observations due to the additional information contributed for evaluation nodes in the reliability scale. The better avoidance is expressed by a lower rate of data packets that are dropped and by less misbehavior detections. The lower number of detections indicates that the extra information does indeed help it to identify and disconnect unstable nodes before they reach to the faulty threshold.

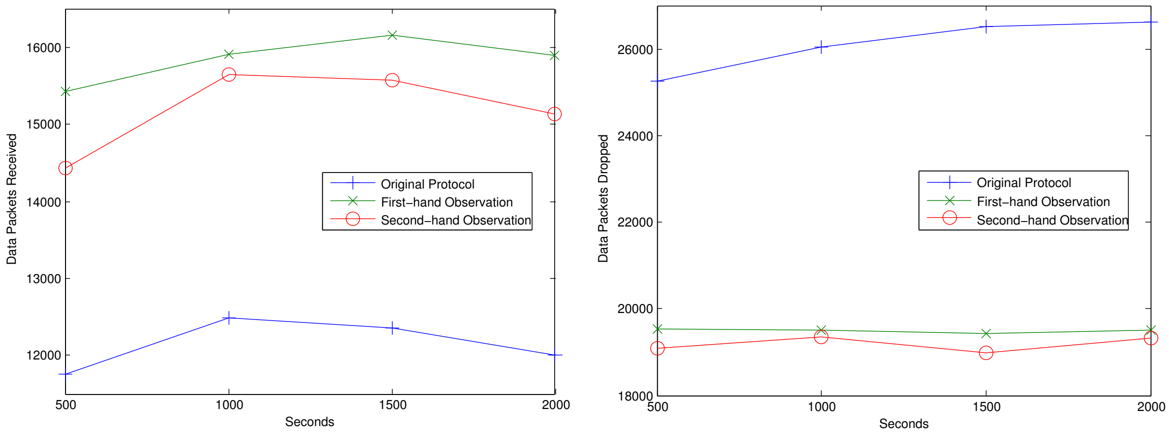
Due to the combination of uncertain ratings, contradictions between nodes and the lack of punishments, the contribution is limited but does still exist. The effectiveness of the reputation system is expressed in its entirety when the behavior is more consistent.

3) Liars: All previous work about robust reputation systems assumed a relatively weak adversary model in which a node either reports extremely negative/positive ratings, random values, inverted values and so on. Our implementation assumes a stronger adversary model in which the liar publishes strategic lies. Those lies are adapted to the ratings that the neighbors hold, in order to be evaluated as trusted and have the ability to adversely affect the other.

The published rating by a liar node is constructed as follows:

- If the average rating received from the neighbors is either extremely good or extremely bad ($\pm 0.5 - 1$), a wrong rating would not significantly affect it, so the liar prefers to publish the average rating in order to increase its trustworthiness.

[1] Our rating system considers both control and data packets with weighting the data packets more than control packets. This does not completely solve the problem since the control packets take a significant part of the packets that are forwarded in the network. An advance solution will change our policy to consider only data packets when it seems that control packets are forwarded well. We leave it for future work.



(a) Throughput.

(b) Data Packets Dropped by Misbehaving Nodes.

Fig. 5. Simulation of 500 Nodes. 250 static and the remainder walk on speed of 5-10 m/s. Other parameters are the same as before. The reputation system with second-hand observations has a tiny advantage over the first-hand observation scheme in the number of data packets that are dropped by misbehaving nodes. Conversely, the throughput of the First-hand observation is better over time than the reputation system.

- When the rating is not absolute, a change might affect the status of the node, and a lie could harm one node or more. The liar wishes to pass either the trustworthy test or the deviation test, but since it does not know its trustworthiness by the other nodes, it tries to pass the deviation test. So it takes the average rating and compares it to its own information (the direct observations), then increases or decreases the average rating by half of the deviation test window, in contrast to its own information.
- If no rating is provided by the other nodes, the liar prefers to spread false information, rather than sitting idly, so it modifies its own information by half of the deviation test. The rating is increased when it is negative and is decreased otherwise.

While the deviation test and the trustworthiness prerequisites are enough for simple lies, our scheme requires a consistent majority of good reporters in order to be robust. As it is shown in Fig. 4, the system is very robust and performs well until there is a consistent majority of liars. Too many false positives result in poor performance.

4) Scalability: Generally, the performance of the original AODV protocol without any misbehaving nodes is poor in larger networks. A reasonable assumption is that with large networks there will be some access points and a central management. However, since the scalability property is one of the desired characteristics, networks with 500 nodes were simulated to examine our scheme.

The reputation system was designed from the outset to be scalable and feasible both in large and small networks. Practically speaking, though, it seems that other external factors have greater effects in larger networks.

The main difference between small and large networks is the average path lengths (in our simulation, 3-4 hops in small network vs. 8-13 hops in large network). A long path is more vulnerable to link breaks and requires relatively high control overhead for maintenance. These two conditions, frequent packet dropping, and cost maintenance are major factors in the surprising results we had.

The frequent packet dropping, due to undiscovered routes, unsuccessful local repair and sometimes unreachable destinations, resulted in poor performance when we used the original rating system because of an excessive amount of suspicious and false positives. Consequently, we doubled the number of observations required to detect misbehaving nodes. This, of course, increases the number of dropped packets, but makes the system more stable when the number of false positives is low.

The massive control packets that were forwarded in large networks reached 60% to 70% of the total packets transmitted. This means that black hole detections are very difficult to discover and the system, most of the time, is in state of avoidance. As shown previously, the advantage of the reputation system in such cases, compared to First-hand observation method, is limited.

In contrast to the previous simulation results, when we had a correlation between the number of packets that are dropped by malicious nodes and the throughput, the results in a large network, shown in Fig. 5, differ.

The reputation system cost, which does not significantly effect small networks, is expressed widely within large networks, in terms of transmission price. This means more bandwidth contention and additional collisions. (The extra overhead in terms of CPU processing and memory storage is minor). As one can see in Fig. 5(b), the reputation system manages to suffer less dropped data packets caused by misbehaving nodes. However, the overall number of dropped packets is larger than the corresponding number of the dropped packet when First-hand observation is used (because of network conditions). In such situations, relying on self-observations is better than using the rating exchange.

VI. Conclusions and Future Work

In this paper we show that reputation system on top of AODV has an advantage over schemes that rely only on first-hand observations despite the limited amount of information and the additional problems of AODV versus DSR. This advantage includes both profit and punishment according to the behavior, and works for both partial and complete dropping. The reputation system remained robust against advanced liars as well, when a majority of the nodes are trustworthy. In some circumstances, however, the network conditions have greater effect than the reputation system benefits, as in the case of large networks. In such situations, it is better to rely on self-observations.

Our scheme focuses mainly on partial and complete dropping, but in principle also addresses other patterns of misbehavior in the forwarding phase. It can be improved to dynamically change the rating policy, in order to better handle the different patterns, such as sole consideration of data packets when control packets are forwarded well.

Additional mechanisms to support QoS and to increase the fairness in the network are possible areas for future research. Our work is dedicated to AODV, but can be adopted to other routing algorithms as well as to sensor networks.

References

[1] L. Buttyfin and J. Hubaux. Report on a working session on security in wireless ad hoc networks, November 2002.

[2] J. Hubaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In *Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, CA, USA, October 2001.

[3] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang. Security in mobile ad hoc networks: Challenges and solutions. *IEEE Wireless Communications*, 11:2–11, February 2004.

[4] P. Obreiter, B. König-Ries, and M. Klein. Stimulating cooperative behavior of autonomous devices - an analysis of requirements and existing approaches. In *Second International Workshop on Wireless Information Systems (WIS2003)*, Angers, France, April 2003.

[5] M. Conti, E. Gregori, and G. Maselli. Cooperation issues in mobile ad hoc networks. In *Proceedings of the 24th International Conference on Distributed Computing Systems Workshops (ICDCSW'04)*, Tokyo, Japan, March 2004.

[6] S. Buchegger and J. 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)*, Switzerland, June 2002.

[7] P. Michiardi and R. Molva. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proceedings of The 6th IFIP Communications and Multimedia Security Conference*, pages 107–121, Portorosz, Slovenia, September 2002.

[8] S. Bansal and M. Baker. Observation-based cooperation enforcement in ad hoc networks, July 2003.

[9] L. Buttyán and J. P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. *MONET*, 8(5):579–592, October 2003.

[10] P. Michiardi and R. Molva. A game theoretical approach to evaluate cooperation enforcement mechanisms in mobile ad-hoc networks. In *Proceedings of Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt'03)*, SophiaAntipolis, France, March 2003.

[11] Aodv homepage. http://moment.cs.ucsb.edu/AODV/aodv.html.

[12] C. E. Perkins, E. M. Belding-Royer, and S. R. Das. Ad hoc on-demand distance vector (AODV) routing. Rfc 3561, IETF, July 2003.

[13] E. M. Belding-Royer and C. E. Perkins. Evolution and future directions of the ad hoc on-demand distance vector routing protocol. *Ad hoc Networks Journal*, 1(1):125–150, July 2003.

[14] J. Broch, D. B. Johnson, and D. A. Maltz. The dynamic source routing protocol for mobile ad hoc networks. Internet draft, IETF, July 2004.

[15] E. Royer and C. Toh. A review of current routing protocols for ad-hoc mobile wireless networks. *Mobile Wireless Networks. IEEE Personal Communications*, pages 46–55, April 1999.

[16] M. Conti, E. Gregori, and G. Maselli. Towards reliable forwarding for ad hoc networks. In *Proceeding of Personal Wireless Communications (PWC 2003)*, pages 790–804, Venice, Italy, September 2003.

[17] P. Dewan, P. Dasgupta, and A. Bhattacharya. On using reputations in ad hoc networks to counter malicious nodes. In *Proceedings of the 10th International Conference on Parallel and Distributed Systems (ICPADS 2004)*, Newport Beach, CA, USA, July 2004.

[18] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Mobile Computing and Networking (MOBICOM)*, pages 255–265, 2000.

[19] S. Buchegger and J. Y. Le Boudec. Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks. In *Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing*, Spain, 2002. IEEE Computer Society.

[20] S. Buchegger and J. Y. Le Boudec. The effect of rumor spreading in reputation systems for mobile ad-hoc networks. In *Proceedings of WiOpt '03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, Sophia-Antipolis, France, March 2003.

[21] S. Buchegger and J. Y. Le Boudec. A robust reputation system for mobile ad hoc networks. Technical Report IC/2003/50, EPFL-DI-ICA, July 2003.

[22] S. Buchegger. *Coping With Misbehavior in Mobile Ad-hoc Networks*. PhD thesis, Swiss Federal Institute of Technology (EPFL), April 2004.

[23] P. Michiardi and R. Molva. Preventing denial of service and selfishness in ad hoc networks. In *Working Session on Security in Ad Hoc Networks*, Lausanne, Switzerland, June 2002.

[24] P. Michiardi and R. Molva. Simulation-based analysis of security exposures in mobile ad hoc networks. In *European Wireless Conference*, 2002.

[25] P. Ning and K. Sun. How to misuse aodv: A case study of insider attacks against mobile adhoc routing protocols. In *Proceedings of the 4th Annual IEEE Information Assurance Workshop*, June 2003.

[26] W. Wang, Y. Lu, and B.K. Bhargava. On vulnerability and protection of ad hoc on-demand distance vector prototol. In *Proceedings of International Conference on Telecommunication (ICT)*, 2003.

[27] C.Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt. A specification-based intrusion detection system for aodv. In *Proceedings of the ACM workshop on Security of ad hoc and sensor networks (SASN '03)*, Fairfax, Virginia, October 2003.

[28] H. Yang, X. Meng, and S. Lu. Self-organized network-layer security in mobile ad hoc networks. In *Proceedings of the ACM workshop on Wireless security (WiSE '02)*, USA, September 2002.

[29] M. Just, E. Kranakis, and T. Wan. Resisting malicious packet dropping in wireless ad hoc networks. In *Proceedings of ADHOCNOW'03*, Montreal, Canada, October 2003.

[30] A. Jósang and R. Ismail. The beta reputation system. In *15th Bled Conference on Electronic Commerce*, Bled, Slovenia, June 2002.

[31] A. Jósang, S. Hird, and E. Faccer. Simulating the effect of reputation systems on e-markets. In *Proceedings of the First International Conference on Trust Management*, Crete, May 2003.

[32] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman. Reputation systems. *Commun. ACM*, 43(12):45–48, 2000.

[33] S. Y. Ni, Y. C. Tseng, Y. S. Chen, and J. P. Sheu. The broadcast storm problem in a mobile ad hoc network. In *MobiCom '99: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, pages 151–162, Washington, USA, August 1999.

[34] S. Mueller, R. P. Tsang, and D. Ghosal. Multipath routing in mobile ad hoc networks: Issues and challenges. In *MASCOTS Tutorials*, 2003.

[35] S.J. Lee and M. Gerla. AODV-BR: Backup routing in ad hoc networks. In *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2000)*, Chicago, IL, September 2000.

[36] M. K. Marina and S. R. Das. On-demand multipath distance vector routing in ad hoc networks. In *Proceedings of IEEE International Conference on Network Protocols (ICNP)*, November 2001.

[37] Z. Ye, S. V. Krishnamurthy, and Satish K. Tripathi. A framework for reliable routing in mobile ad hoc networks. In *Proceedings IEEE INFOCOM 2003*, San Franciso, CA, USA, 2003.

[38] A. Murthy P. Sambasivam and E. M. Belding-Royer. Dynamically adaptive multipath routing based on aodv. In *Proceedings of the 3rd Annual Mediterranean Ad hoc Networking Workshop (MedHocNet)*, Bodrum, Turkey, June 2004.

[39] GloMoSim. http://pcl.cs.ucla.edu/projects/glomosim.

[40] S. J. Lee, E. M. Belding-Royer, and C. E. Perkins. Scalability study of the ad hoc on-demand distance vector routing protocol. *International Journal on Network Management*, 13(2):97–114, March-April 2003.

[41] H. Hellbrück and S. Fischer. Towards analysis and simulation of ad-hoc networks. In *Proceedings of the 2002 International Conference on Wireless Networks (ICWN02)*, pages 69–75, USA, June 2002.

[42] J. Yoon, M. Liu, and B. Noble. Random waypoint considered harmful. In *Proceedings IEEE INFOCOM 2003*, San Franciso, CA, USA, 2003.