This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE SECON 2005 proceedings.

Secure Cooperative Mobile Ad Hoc Networks Against Injecting Traffic Attacks

Wei Yu and K. J. Ray Liu
Department of Electrical and Computer Engineering
and The Institute for Systems Research
University of Maryland, College Park, MD 20742
Email: weiyu, kjrliu@isr.umd.edu

Abstract— **In this paper we investigate how to defend against injecting traffic attacks in cooperative mobile ad hoc networks where nodes belong to the same authority and pursue the common goals. By injecting an overwhelming amount of traffic into the network, the attackers can easily consume good nodes' valuable network resources and reduce the network's lifetime. Since in cooperative mobile ad hoc networks nodes will usually unconditionally forward packets for other nodes, such networks are extremely vulnerable to injecting traffic attacks, especially those launched by inside attackers. In this paper, the possible types of injecting traffic attackers are studied, and a set of mechanisms are proposed to protect cooperative mobile ad hoc network against such attacks. The performance of the proposed mechanisms is analyzed. Both theoretical and experimental bounds are derived, which show that from attackers' point of view, the best strategy is not to launch injecting traffic attacks. Simulation studies have also verified the theoretical analysis.**

I. Introduction

A *mobile ad hoc network* is a group of mobile nodes without requiring centralized administration or fixed network infrastructure. Through cooperatively forwarding packets for each other, nodes in mobile ad hoc networks can communicate with other nodes out of their direct transmission ranges. In many situations, such as military or emergency applications, nodes in an ad hoc network belong to the same authority and pursue the common goals. Under such circumstances, *fully cooperative behavior*, such as unconditionally forwarding packets for each other, can be assumed. We refer to such ad hoc networks as *cooperative ad hoc networks*.

Before ad hoc networks can be successfully deployed, security concerns must be resolved first [1]–[7]. In this paper, we study a class of powerful attacks called injecting traffic attacks. Specifically, attackers inject an overwhelming amount of traffic into the network in attempt to consume valuable network resources, and consequently degrade the network performance, such as causing network congestion and reducing the network's lifetime. Since in cooperative ad hoc networks, nodes will usually unconditionally forward packets for other nodes, such networks are extremely vulnerable to injecting traffic attacks, especially those launched by inside attackers who have gained access to the network.

Roughly speaking, there are two types of injecting traffic attacks that can be launched in cooperative ad hoc networks: *query flooding attack* and *injecting data packet attack* (IDPA). Due to node mobility, nodes in ad hoc networks may need to frequently perform route updates which may require broadcasting query messages. Since in many ad hoc network routing protocols, in general all nodes in the network need to process this query message at least one time, attackers can initiate query messages with a very high frequency to consume valuable network resources, which is called *query flooding attack*. Besides query flooding attacks, attackers can also inject an overwhelming amount of data packets into the network to request other nodes to forward. When other nodes process and forward these packets, their resources will be wasted. Since in general the size of data packet is much larger than the size of query message, and the injection rate of data packets is much higher than the injection rate of query messages, the resources that can be wasted by IDPA are usually much more than by query flooding attacks.

To defend against query flooding attacks, one possible way is to limit the amount of queries that can be initiated by each node in the network. Although this may degrade the network performance in certain degree, such methods can effectively limit the damage that can be caused by query flooding attacks. However, if nodes in the network cannot know other nodes' data packet injection statistics, such as packet injection rate, then it becomes extremely hard (or impossible) to detect whether some nodes are launching IDPA. Fortunately, in cooperative ad hoc networks, since nodes belong to the same authority and pursue the common goals, it is generally true that they can know each other's data packet injection statistics.

In this paper we mainly focus on protecting cooperative ad hoc networks against IDPA, especially those launched by inside attackers. With the reasonable assumption that nodes in the network can know other nodes' statistics about packet injection rate, we propose a set of mechanisms which can effectively detect IDPA, even when attackers can use some advanced transmission techniques such as directional antennas in attempt to avoid being detected. We derive the theoretical upper-bounds for the probability that attackers can successfully launch IDPA without being detected, which shows that from attackers' point of view the best strategy is to conform to their original packets injection rate, that is, the best strategy is not to launch IDPA. Meanwhile, the query flooding attacks are also studied and the tradeoff between limiting query rate and

0-7803-9011-3/05/$20.00 ©2005 IEEE.

system performance is investigated.

The rest of the paper is organized as follows. Section II describes the system model. Section III proposes a set of mechanisms to defend against injecting traffic attacks. The theoretical performance analysis of the proposed mechanisms is presented in Section IV. Simulation results are presented in Section V. Finally, Section VI discusses the related work and Section VII concludes this paper.

II. System Model

This paper considers cooperative mobile ad hoc networks where nodes belong to the same authority and pursue the common goals. Nodes in such networks can be classified into two types: *good* and *malicious*, in which good nodes will unconditionally help those nodes that have not been detected as malicious, while malicious nodes' objective is to maximize the damage they can cause to the system. Each node is equipped with a battery with limited power supply, communicates with other nodes through wireless connections, and can move freely inside a certain area. We assume that good nodes use omnidirectional transmission techniques, such as omnidirectional antennas, but we allow attackers to use directional transmission techniques, such as directional antennas [8] or adaptive beamforming [9], to improve their attacking capabilities.

In the current system model, data packets are generated by certain nodes and delivered to certain destinations with each packet having a specific delay constraint. We call a source-destination (SD) pair to be *legitimate* if this pair is required by the common system goals. For each legitimate SD pair (s, d) in the network, we assume that its average packet injection rate is $\lambda_{s,d}$, and the number of packets that can be injected by this pair into the network until time t is upper-bounded by $f_{s,d}(t)$. Since nodes belong to the same authority and pursue the common goals, we can assume that every node knows all legitimate SD pairs in the network as well as the associated upper-bounds of the packet injection rates.

Attackers can inject an overwhelming amount of packets into the network in attempt to consume other nodes' valuable energy. When other nodes forward these packets, the consumed energy will be wasted. Due to their fully cooperative nature, cooperative ad hoc networks can be extremely vulnerable to injecting traffic attacks. In general, two types of injecting traffic attacks can be launched: injecting data packets attacks (IDPA) and query flooding attacks. For any malicious SD pair (s, d), there are three possible ways to launch injecting data packets attacks:

- *Simple IDPA*: s randomly picks a route to d and injects an overwhelming amount of packets into the network with the rate being much higher than $\lambda_{s,d}$.
- *Long-route IDPA*: s picks a very long route to inject data packets into the network.
- *Multiple-route IDPA*: s picks multiple routes to d and injects traffic into the network through these routes simultaneously. In this way, the attackers can take advantage of advanced transmission techniques, such as directional antenna and beamforming, to avoid being detected, even when some monitoring mechanisms have been employed.

Query flooding attack refers to that attackers issue an overwhelming amount of query messages (e.g., route requests) to request others to process. In general, more nodes in the network will be involved to process and forward route request packets than general data packets, while the size of route request packet is usually much smaller than data packet.

We assume that all nodes in the network are legitimate, no matter whether they are good or malicious. We assume that each node has a public/private key pair, and a node can know or authenticate other nodes' public keys, but no node will disclose its private key to others unless it has been compromised. To keep the confidentiality and integrity of the transmitted content, we assume that each packet will be encrypted and signed by its source when necessary. Without loss of generality, we assume all data packets have equal size.

III. Defense Mechanisms

In such cooperative ad hoc networks, only legitimate SD pairs is allowed to inject data packets and query messages into the network, and the packet injection rates should conform to the legitimate upper bounds. In another words, to detect injecting traffic attack is equivalent to detect those nodes who are not legitimate to inject packets into the network or whose packet injection rates are much higher than their legitimate upper bounds. In this paper, detection of injection traffic attacks is achieved through necessary traffic monitoring, which will be illustrated in the following of this section.

A. Route Discovery and Packet Delivery

In this paper, DSR [10] is adopted as the underlying routing protocol. However, without security consideration, routing protocols can easily become attacking targets. For example, malicious nodes can launch query flooding attacks to waste other nodes' valuable resources. In this paper, the following security enhancements are incorporated into the baseline DSR.

When a source s initiates a route discovery to the destination d, the following format is used for the route request:

$$\{s, d, id_s(s,d), t_s(s,d), seq_s(s,d), BL_s, sig\},$$

where $id_s(s,d)$ is an unique ID specified by s for this request, $t_s(s,d)$ is the time when s issued this request, BL_s is the subset of s's blacklist that has not been broadcasted by s before, $seq_s(s,d)$ is the sequence number associated to the last data packet that s has sent to d, and sig is the signature generated by s based on message $\{s, d, id_s(s,d), t_s(s,d), seq_s(s,d), BL_s\}$. After broadcasting this request, s should increase the value of $id_s(s,d)$ by 1.

After a good node x has received a route request originating from s and targeting on d, x first checks the following conditions:

1) The SD pair (s, d) is legitimate.

2) All signatures are valid;
3) $id_x(s,d) < id_s(s,d)$ and $t_x(s,d) < t_s(s,d)$, where $id_x(s,d)$ is the maximum request sequence number corresponding to the pair (s,d) that x has seen before, and $t_x(s,d)$ is the latest time associated to the route requests issued by pair (s,d) that x has seen before.
4) No nodes appended to the route request packet have been marked as malicious by x.
5) Less than L_{maxhop} intermediate nodes have been appended to the request packet, where L_{maxhop} is a system-level parameter indicating the maximum number of hops that any route is allowed to have in the network.
6) x has not forwarded any request for pair (s,d) in last T_x^{min} interval, where T_x^{min} is the minimum query forwarding interval specified by x to indicate that x will forward at most 1 route request for any legitimate pair in any T_x^{min} interval.

If all the conditions from 1 to 4 are satisfied, we call such a request as a *valid* request, in this situation x will update its record $BL_x(s)$ using the received information BL_s where $BL_x(s)$ is the subset of s's blacklist known by x, assign the value of $id_s(s,d)$ to $id_x(s,d)$, assign the value of $t_s(s,d)$ to $t_x(s,d)$, and assign the value of $seq_s(s,d)$ to $seq_x(s,d)$. If all of the 6 conditions can be satisfied and x is not the destination, x will also append its own address to the request packet, sign and rebroadcast the new request. If the request is not valid, x will discard this request.

Once a source has decided to send a packet to a certain destination using a certain route, a data packet delivery transaction should be started. In this paper, the data packet delivery works as follows. Suppose that node s is to send a packet with payload *msg* and sequence number $seq_s(s,d)$ to destination d through the route R. s first generates two signatures sig_h and sig_b, with sig_h being generated based on message $\{R, seq_s(s,d)\}$ and sig_b being generated based on message $\{R, seq_s(s,d), MD(msg)\}$ where $MD()$ is a digest function such as SHA-1 [11]. The final format of the packet to be sent is as follows:

$$\{R, seq_s(s,d), sig_h, msg, sig_b\}.$$

We refer to $\{R, seq_s(s,d), sig_h\}$ as the *packet header*, and refer to $\{msg, sig_b\}$ as the *packet body*. As to be shown in Section III-B, by also using the signature sig_h, lots of energy can be saved when performing traffic monitoring. Next, s will transmit this packet to the next node on route R (e.g., x), increase $seq_s(s,d)$ by 1, and wait for a receipt to be returned by node x.

When a node (e.g., x) detects that a certain packet is to be transmitted by another node in its neighborhood, x first decodes and checks the packet header. Assume $\{R, seq_s(s,d), sig_h\}$ is the header of the transmitted packet. x needs to continue receiving and decoding the body of the packet only if all of the following conditions are satisfied:

1) x is on the route R.
2) No nodes on route R has been marked as malicious by x.
3) $seq_s(s,d) > seq_x(s,d)$, where $seq_x(s,d)$ is the sequence number of the last packet with the source being s and the destination being d that x has seen.
4) The signature sig_h is valid.
5) Route R has no more than L_{maxhop} hops, where L_{maxhop} is a system-level parameter indicating the maximum number of hops that any route is allowed to traverse in the network.

After x has decided to forward the packet and has successfully received and verified the whole data packet, x will forward the packet to the next node on the route.

B. Traffic Monitoring Mechanisms

In this paper, to detect possible injecting traffic attacks, each good node will keep monitoring its neighbors' transmission activities using the proposed *header watcher mechanism*. Specifically, when a good node x detects that a neighbor is transmitting a data packet, no matter whether x is the target of this transmission or not, x will try to receive and decode the transmitted packet header (e.g., $\{R, seq_s(s,d), sig_h\}$). If the signature of the packet header is valid, x will put the packet header in the set $HL_x(s,d)$, which will be used later to detect whether s has launched injecting traffic attacks.

If all packet headers received by a good node x are recorded, with the increase of x's staying time in the network, more and more storage will be consumed. In this paper, for each legitimate SD pair (s,d) that x knows, only those packet headers received after the last valid route request issued by (s,d) need to be recorded by x. Since the interval between two consecutive route discoveries is usually not long, the storage requirement will become small.

Besides the proposed header watcher mechanism, other types of traffic monitoring mechanisms can also be used. The only requirement for these traffic monitoring mechanisms is that they should be able to verify and authenticate the packets being received/listened. In another words, when a node has received a packet, it should know from which node this packet originates. Otherwise, an attacker can easily impersonate good nodes, which can either cause the attacker to flee from being detected, or cause the impersonated good nodes to be mistakenly detected as malicious.

C. Malicious Node Detection

Now we consider the detection of injecting traffic attacks. For each set of packet headers $HL_x(s,d)$ in x's records, x will mark s as malicious if any of the following situations happens:

1) The set $HL_x(s,d)$ is not empty and the SD pair (s,d) is illegitimate.
2) For any header $\{R, seq_s(s,d), sig_h\}$ in $HL_x(s,d)$, R has more than L_{maxhop} hops.
3) x detects that in $HL_x(s,d)$ there are two valid packet headers $\{R, seq_s(s,d), sig_h\}$ and $\{R', seq_s'(s,d), sig_h'\}$ with $seq_x(s,d) = seq_x'(s,d)$ while $R \neq R'$,
4) x detects that there exists a sequence number $seq_s(s,d)$ in $HL_x(s,d)$ with $seq_s(s,d) > f_{s,d}(t)$.

5) Let $\{s, d, id_s(s,d), t_s(s,d), seq_s(s,d), sig\}$ be a valid route request received by x which is issued by s. There is a packet header $\{R, seq'_s(s,d), sig_h\}$ in $HL_x(s,d)$ which is received by x at time $t \leq t_s(s,d)$ with $seq_s(s,d) < seq'_s(s,d)$.
6) x has received a route request from an illegitimate SD pair (s,d).

In all these situations, once a good node x has detected that s has launched injecting traffic attacks, x will also notify other nodes in the network by broadcasting an ALERT message which consists of necessary evidence such as the corresponding packet headers. When other good nodes have received the ALERT message, after verification, they will also mark s as malicious.

After a node has been detected as malicious, one way to punish it is to remove it physically from the network. Since in most situations it is impossible to physically remove a node, in the the proposed system, once a good node v has marked node m as malicious, in the future v will refuse to work with m in any case.

IV. Theoretical Analysis

According to the secure route discovery procedure described in Section III-A, a good node x will only forward at most 1 route request in any time interval T_x^{min} for any legitimate SD pair, and will not forward route requests for any illegitimate SD pairs, therefore the total damage that can be caused by attackers launching query flooding attacks is bounded. Next we analyze the effects of IDPA. Assume that node s is malicious and tries to launch IDPA with d being the destination of the packets injected by s. To avoid being detected immediately, the SD pair (s,d) must be legitimate and d must be malicious too, otherwise, s can be easily detected by d as malicious. According to Section II, there are three possible ways to launch IDPA: simple IDPA, long-route IDPA and multiple-route IDPA.

We first consider *simple IDPA*. According to Section III-A, in order for good nodes to forward packets for s, s has to increase the sequence number $seq_s(s,d)$ by 1 after each packet delivery. Unless all nodes on the selected route are malicious, which makes no sense, the good nodes on route R can easily detect that s is launching IDPA by comparing the received packets' sequence number with $f_{s,d}(t)$ defined in Section III-C. That is, when launching simple IDPA, the attackers can be immediately detected and can cause negligible damage.

If s launches *long-route IDPA*, since much more good nodes will be involved, s can cause similar damage as launching simple IDPA. However, as described in Section III-A, the maximum allowable number of hops per route is bounded by L_{maxhop}, and good nodes will drop all packets with the associated number of hops more than L_{maxhop}. Therefore the damage is upper-bounded by $f_{s,d}(t) L_{maxhop} E_{nergy}$ by time t.

Finally we consider the *multiple-route IDPA*. To avoid being detected immediately, the packet injection rate to each route must conform to $\lambda_{s,d}$, and the selected routes must be node-disjoint, that is, no selected routes should share any common good node except s and d, otherwise, if a good node x lies in more than one route from s to d, it can easily detect whether s and d have launched multiple-route IDPA. Meanwhile, the packets passing through the same route should have different sequence numbers in order for good nodes on the route to forward them. Based on whether s allows packets in different routes to share the same sequence numbers and what transmission techniques s will use, there are three cases:

- Case 1: s dose not allow packets on different routes to share the same sequence numbers. Since $seq_s(s,d) \leq f_{s,d}(t)$ is required to let s avoid being detected immediately, in this case s has no extra gain by comparing with launching simple IDPA.
- Case 2: s allows packets on different routes to share the same sequence numbers, and transmits packets omnidirectionally. Since s's neighbors will keep monitoring s's packets transmission, they can easily detect that some packets sent by s through different routes use the same sequence number, which indicates that s is launching IDPA. Therefore if s can only transmit packets omnidirectionally, s should not launch multiple-route IDPA.
- Case 3: s allows packets on different routes to use the same sequence numbers, and can transmit packets using directional transmission techniques. Since now s's neighbors cannot receive s' transmission not targeting on them, they have little chance to directly detect that s is launching IDPA. However, since good nodes in the network use omnidirectional transmission techniques, the probability that s can successfully launch multiple-route IDPA without being detected still approaches to 0, as to be shown next.

Next we derive the upper-bounds for the probability that s is able to successfully pick n node-disjoint routes to inject data packets without being detected immediately, as illustrated in Case 3. We consider the most general situation that the destination d does not know the exact locations of those nodes within its transmission range, and all d's neighbors are good nodes. Given a node x and a certain area S, we say that x is randomly deployed inside S according to the 2D uniform distribution if for any subarea $S_1 \subset S$ we have $P(x \in S_1 | x \in S, S_1 \subset S) = S_1/S$. Then we have the following theorem.

Theorem 1 *Suppose that N good nodes are independently deployed inside a large area of S according to the 2D uniform distribution. Suppose that all of these N nodes use omnidirectional transmission techniques and r is their common maximum transmission distance. Suppose that the SD pair (s,d) collude to launch IDPA with s using directional transmission technique and s and d not knowing the exact location of the nodes inside d's receiving range (which is r). If the defending mechanisms described in Section III are used by good nodes, then the probability $P(n,r,N)$ that the two attackers can successfully pick n node-disjoint routes to launch* *multiple-route IDPA without being detected immediately is upper-bounded by*

$$P(n,r,N) \leq \left(\frac{3\sqrt{3}}{4\pi}\right)^{\binom{n}{2}} \sum_{k=n}^{N} P_1(k,N) \left(n\left(\frac{3\sqrt{3}}{4\pi}\right)^{\binom{n-1}{2}}\right)^{k-n} . \tag{1}$$

where $P_1(k,N)$ is defined as follows:

$$P_1(k,N) = \binom{N}{k}\left(\frac{\pi r^2}{S}\right)^k \left(1 - \frac{\pi r^2}{S}\right)^{N-k} . \tag{2}$$

Before proving Theorem 1, we first prove the following lemmas.

Lemma 1 *Assume N nodes are independently deployed inside an area of S according to the 2D uniform distribution. For any node x inside subarea $S_1 \subset S$ and for any subarea $S_2 \subset S_1$, we have*

$$P(x \in S_2 | x \in S_1, S_2 \subset S_1 \subset S) = \frac{S_2}{S_1} \tag{3}$$

Proof:

$$\begin{aligned} & P(x \in S_2 | x \in S_1, S_2 \subset S_1 \subset S) \\ = \; & \frac{P(x \in S_2, x \in S_1 | S_2 \subset S_1 \subset S)}{P(x \in S_1 | S_2 \subset S_1 \subset S)} \\ = \; & \frac{P(x \in S_2 | S_2 \subset S)}{P(x \in S_1 | S_1 \subset S)} = \frac{S_2}{S_1}. \end{aligned} \tag{4}$$

That is, the conditional distribution of x in S_1 is independent of S, which is also the 2D uniform distribution. ∎

Lemma 2 *Assume nodes x and y are independently deployed inside a certain area S according to the 2D uniform distribution. Given $x \in S_1 \subset S$ and $y \in S_1 \subset S$, and given any subareas $S_x \subset S_1$ and $S_y \subset S_1$, we have*

$$\begin{aligned} & P(x \in S_x, y \in S_y | x \in S_1, y \in S_1, S_x \subset S_1, S_y \subset S_1) \\ = \; & P(x \in S_x | x \in S_1, S_x \subset S_1) P(y \in S_y | y \in S_1, S_y \subset S_1) \end{aligned} \tag{5}$$

Proof: Since the deployment of x and y are independent of each other, we have

$$\begin{aligned} & P(x \in S_x, y \in S_y | x \in S_1, y \in S_1, S_x \subset S_1, S_y \subset S_1) \\ = \; & P(x \in S_x | x \in S_1, S_x \subset S_1, y \in S_y \subset S_1) * \\ & P(y \in S_y | y \in S_1, S_y \subset S_1, x \in S_1, S_x \subset S_1) \\ = \; & P(x \in S_x | x \in S_1, S_x \subset S_1) P(y \in S_y | y \in S_1, S_y \subset S_1) \end{aligned}$$

That is, the distribution of x and y inside S_1 are independent of each other. ∎

Lemma 3 *Let S be a circular area with o being the center and R being the radius. Assume that node x lies in S and $P(A \in S_1 | A \in S, S_1 \subset S) = \frac{S_1}{S}$. Let $d(x)$ denote the random variable of the distance from x to o, then*

$$P(d(x) = r | x \in S) = \begin{cases} \frac{2r}{R^2} & 0 \leq r \leq R \\ 0 & r > R \end{cases} \tag{6}$$

Proof: For any $0 < r \leq R$, we have

$$P(d(x) = r | x \in S) = \lim_{\Delta \to 0} \frac{\pi r^2 / \pi R^2 - \pi (r - \Delta)^2 / \pi R^2}{\Delta} = \frac{2r}{R^2} \tag{7}$$

For any $r > R$, we have $x \notin S$, which implies $P(d(x) = r | x \in S) = 0$. ∎

Lemma 4 *Let S be a circular area with o being its center and R being its radius. Given that two nodes a and b independently deployed in S according to the 2D uniform distribution, we have*

$$P(|ab| > R | a \in S, b \in S) = \frac{3\sqrt{3}}{4\pi}, \tag{8}$$

where $|ab|$ denote the distance between a and b.

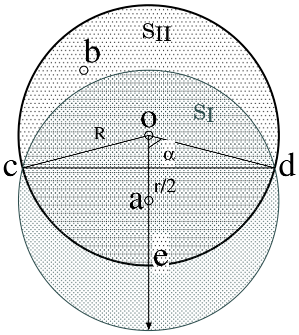


Fig. 1. Illustration

Proof: We use Figure 1 to help illustrating the proof. Let r denote the distance from a to o, let C_o denote the circle with o being the center and R being the radius, and let C_a denote the circle with a being the center and R being the radius. Let c and d be the intersecting points between the two circles C_o and C_a, and let $\alpha = \angle coa = \angle doa$. Let $S_I(r)$ denote the intersecting area inside both circles C_o and C_a with $|oa| = r$, and let $S_{II}(r)$ denote the area of S subtracted by $S_I(r)$. Then we have

$$P(|ab| > R \big| a \in S, b \in S) = \int_0^R \frac{2r}{R^2} \frac{S_{II}(r)}{S} \mathbf{d}r, \tag{9}$$

where (9) comes from Lemma 4. We first calculate $S_I(r)$:

$$S_I(r) = 2\left(R^2 \arccos\frac{r}{2R} - \frac{r}{2}\sqrt{R^2 - (\frac{r}{2})^2}\right), \tag{10}$$

where $\alpha = \arccos(\frac{r}{2R})$. Then $S_{II}(r)$ can be calculated as

$$S_{II}(r) = R^2\left(\pi - 2\arccos\frac{r}{2R} - \frac{r}{R^2}\sqrt{R^2 - (\frac{r}{2})^2}\right). \tag{11}$$

By integrating (11) into (9), we have $P(|ab| > R \big| a \in S, b \in S) = \frac{3\sqrt{3}}{4\pi}$. ∎

Lemma 5 *Assume that n nodes $A = \{a_1, \ldots, a_n\}$ are independently deployed inside a circular area S according to the 2D uniform distribution with R being the radius, then we have*

$$P(|a_i a_j| > R : \forall a_i, a_j \in A) \leq P(|a_1 a_2| > R)^{\binom{n}{2}} \tag{12}$$

Proof:

$$\begin{aligned}
& P(|a_ia_j| > R : \forall a_i, a_j \in A) \\
= \; & P(|a_1a_2| > R, \ldots |a_1a_n| > R, \ldots, |a_{n-1}a_n| > R) \\
= \; & P(|a_1a_2| > R \big| |a_1a_3| > R, \ldots |a_{n-1}a_n| > R) * \\
& P(|a_1a_3| > R, \ldots, |a_{n-1}a_n| > R) \\
= \; & P(|a_1a_2| > R \big| |a_1a_i| > R, |a_2a_i| > R : \forall 3 \leq i \leq n) * \\
& P(|a_1a_3| > R, \ldots, |a_{n-1}a_n| > R)
\end{aligned}$$

Given $|a_1a_i| > R$ and $|a_2a_i| > R$ for any $3 \leq i \leq n$, we can draw a circle with a_i being the center and R being the radius. To conform to the statement that "$\forall a_i, a_j \in A, |a_ia_j| > R$", both a_1 and a_2 cannot lie inside the intersecting area between this circle and the circle with o being the center. That is, a_1 and a_2 are now restricted in an area of $S' \subset S$ smaller than S. So the probability that $|a_1a_2|$ is larger than R under such restrictions will become smaller than without such restrictions. That is,

$$\begin{aligned}
& P(|a_1a_2| > R \big| |a_1a_i| > R, |a_2a_i| > R) \\
\leq \; & P(|a_1a_2| > R : \forall 3 \leq i \leq n). \qquad (13)
\end{aligned}$$

Following the same arguments we can have

$$P(|a_ia_j| > R : \forall a_i, a_j \in A) \leq \prod_{1 \leq i < j \leq n} P(|a_ia_j| > R). \qquad (14)$$

Since there are total $\binom{n}{2}$ items in the product, and nodes in A are symmetric, we can conclude that (12) holds. ■

Lemma 6 *Assume $n+m$ nodes $\{a_1, \ldots, a_n, b_1, \ldots, b_m\}$ are independently deployed inside a circular area S according to 2D uniform distribution with R being the radius. Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_m\}$, then we have*

$$\begin{aligned}
& P(|a_ib_l| > R \textit{ or } |a_jb_l| > R : \forall a_i, a_j \in A, b_l \in B, i \neq j) \\
\leq \; & \big(nP(|a_1b_1| > R)^{n-1}\big)^m \qquad (15)
\end{aligned}$$

Proof: Let $A_i = A - \{a_i\}$. Given any $b \in B$, to say "$|a_ib| > R$ or $|a_jb| > R : \forall a_i, a_j \in A, a_i \neq a_j$" is equivalent to say "there exists at least one A_i with $|xb| > R$ for any $x \in A_i$", that is,

$$\begin{aligned}
& P(|a_ib| > R \text{ or } |a_jb| > R : \forall a_i, a_j \in A, a_i \neq a_j) \\
= \; & P((|xb| > R : \forall x \in A_1) \text{ or } \ldots \text{ or } (|xb| > R : \forall x \in A_n)) \\
\leq \; & \sum_{i=1}^{n} P(|xb| > R : \forall x \in A_i) \\
= \; & nP(|xb| > R : \forall x \in A_1) \\
\leq \; & nP(|a_1b| > R)^{n-1}
\end{aligned}$$

Due to the symmetry and independence of the m nodes in B, we can concludes that (15) holds. ■

Now Theorem 1 can be proved as follows:

Proof: Let C_d denote the circle with d being the center and r being the radius. For s and d to be able to successfully pick n node-disjoint routes to launch multiple-route IDPA without being detected immediately, they need to pick at least n distinct nodes inside C_d, one for each route, to act as the last intermediate nodes on these routes. Since s and d do not know the exact locations of the nodes inside C_d, these n nodes can only be randomly selected. It is easy to see that the following **three necessary conditions** must be satisfied in order for the attackers to succeed:

C1. There exist at least n nodes inside C_d, otherwise, s and d can never have n node-disjoint routes between them.

C2. Given that there are $k \geq n$ nodes inside C_d, and that s and d are to randomly select n nodes among them to act as the last intermediate node for these n node-disjoint routes, then for any two nodes among the n nodes selected by s and d, no node should lie in the other nodes' transmission range. Otherwise, if any two of the n nodes lie in each other's transmission range, they can easily detect that s is launching multiple-route IDPA.

C3. Given that the n nodes have been selected by s and d, there should exist no other good nodes (nodes excluding the selected n good nodes) which can simultaneously lie in any two of these n nodes' transmission range. Otherwise, if there exist one such node, then it can easily detect that s is launching multiple-route IDPA.

Let $P_1(k, N)$ denote the probability that there are k nodes inside C_d, $P_2(n, r, k)$ denote the probability that the condition C2 can be satisfied given that the n nodes are randomly selected among $k \geq n$ nodes inside C_d, and $P_3(n, r, k, N)$ denote the probability that the condition C3 can be satisfied given there are $k \geq n$ nodes inside C_d and the n nodes have been determined by s and d. It is easy to see that

$$P(n, r, N) \leq \sum_{k=n}^{N} P_1(k, N) P_2(n, r, k) P_3(n, r, k, N). \qquad (16)$$

Since nodes are independently deployed inside S according to the 2D uniform distribution, we can immediately have

$$P_1(k, N) = \binom{N}{k} \left(\frac{\pi r^2}{S}\right)^k \left(1 - \frac{\pi r^2}{S}\right)^{N-k}. \qquad (17)$$

Given that k nodes lie in C_d, according to Lemma 1 and Lemma 2, it is equivalent to say that these k nodes are independently deployed inside C_d according to the 2D uniform distribution. According to Lemma 4 and Lemma 5, we can have

$$P_2(n, r, k) = \left(\frac{3\sqrt{3}}{4\pi}\right)^{\binom{n}{2}}. \qquad (18)$$

To simplify the analysis, we consider a modified version of condition C3: given any two nodes among the selected n nodes, there should exist no other good nodes *inside C_d but not belonging to these n nodes* which can simultaneously lie in these two nodes' transmission range. That is, only a small subset of the applicable nodes are considered. Let $P_3'(n, r, k, N)$ denote the probability that the modified condition C3 can be satisfied given there are $k \geq n$ nodes inside C_d and the n nodes have been determined by s and d, then we must have $P_3(n, r, k, N) \leq P_3'(n, r, k, N)$. According to Lemma 4 and Lemma 6, the probability that the modified condition C3 can be satisfied is upper-bounded by

$$P_3'(n,r,k,N) \leq \left(n \left(\frac{3\sqrt{3}}{4\pi} \right)^{\binom{n-1}{2}} \right)^{k-n} \tag{19}$$

By combining the above results, we can conclude that (1) as well as Theorem 1 holds. ■

Theorem 2 *The probability that two colluding attackers s and d can successfully pick 6 or more node-disjoint routes to launch multiple-route IDPA without being detected immediately is 0.*

Proof: For the attackers s and d (assuming s is the source and d is the destination) to simultaneously pick 6 routes to launch multiple-route IDPA, it needs to pick 6 nodes within d's receiving range, that is, the circular area C_d with d being the center and r the radius. Let $A = \{a_1, a_2, a_3, a_4, a_5, a_6\}$ denote the set of 6 selected nodes by s and d that lies inside C_d. One necessary condition for the attackers to succeed is that for any $a_i, a_j \in A$, we must have $|a_i a_j| > r$ for any $a_j \in A$ and $a_j \neq a_i$. Now we show that it is not achievable. If there exist $a_i, a_j \in A$ with $\angle a_i d a_j = 0$, then we must have $|a_i a_j| \leq r$. Next we only need to consider the situations that for any $a_i, a_j \in A$, $\angle a_i d a_j \neq 0$. For each node $a_i \in A$, we draw a radial originated from d and passing a_i, and let a_i' be the intersecting point between the radial da_i and the circumference of the circle C_d. Any two radials will partition the circular area C_d into two sectors. We say a sector is *singleton* if none of the nodes in A lie inside this sector (including the arc but excluding the two radials). It is easy to say that the 6 nodes will partition the circle into 6 singleton sectors. To satisfy the above necessary condition, the angle of each singleton sector should be more than $\pi/3$: if the angle of a singleton section is no more than $\pi/3$, let a_i be the node on one side of this sector, and a_j be the node on the other side of this sector, then for any point x that lies in the segment da_i' and any point y that lies in the segment da_j', we must have $|xy| \leq r$. Since we have 6 singleton sectors, and each singleton sector has an angle of more than $\pi/3$, the summed angle is more than 2π, which contradicts the fact that a circle is 2π. Given this conclusion, it is trivial to show that more than 6 routes is also not achievable. ■

We have also evaluated through experiments the upper-bounds of the success ratio for two colluding attackers s and d to launch multiple-route IDPA with s using directional transmission technique. Given a rectangular area of $20r \times 20r$, we put d in the center of the area. At each round of experiment, we independently deploy $400r^2\rho$ nodes inside the area according to 2D uniform distribution and randomly pick n nodes inside d's receiving range, where ρ is referred to as the node density. We say (s, d) may succeed only if all of the three necessary conditions presented in the proof of Theorem 1 are satisfied. For each configuration of route number n and node density ρ, 10^7 experiments have been conducted, and the upper-bounds are obtained as the ratio of total success number over the total number of experiments.

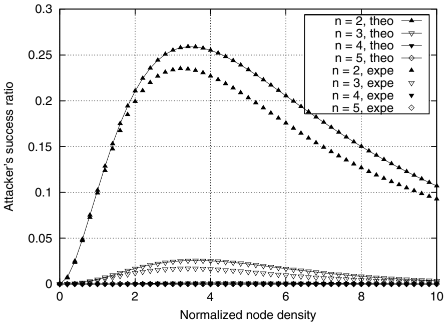


Fig. 2. Upper bounds of attackers' success probability

Both experimental and theoretical upper-bounds are plotted in Figure 2, where "theo" denotes the theoretical upper-bounds obtained using (1), "expe" denotes the experimental upper-bounds obtained through experiments described above, and "n" denotes the number of node-disjoint routes to be picked by the malicious SD pair (s, d). In Figure 2, the normalized node density is defined as the average number of nodes inside an area of πr^2. Since both the theoretical and experimental upper-bounds corresponding to $n = 4$ and $n = 5$ are almost equal to 0 across all illustrated node densities (e.g., for $n = 4$, all values are less than 2×10^{-3}), the four curves associated to $n = 4, 5$ have almost overlapped into one single curve, which is the lowest curve illustrated in Figure 2. For $n = 2, 3$, we can see that the success ratio increases first with the increase of node density until it arrives at a peak, then decreases with the further increase of node density, which is consistent with (1). The reason is as follows: with the increase of the node density, the probability P_1 that the condition C1 can be satisfied increases monotonically from 0 to 1, the probability P_2 that the condition C2 can be satisfied keeps unchanged, while the probability P_3 that the condition C3 can be satisfied decreases monotonically from 1 to 0, and when ρ is small, the value of P_1 dominates the bound, while when ρ is large, the value of P_3 dominates the bound. From Figure 2 we can also see that there exist gaps between theoretical results and experimental results. The reason is that when we calculate the probability of condition C3 being satisfied, only a subset of applicable nodes have been considered, which make the theoretical upper-bounds a little bit looser (higher) than the experimental upper-bounds.

The above upper bounds are evaluated based on a fixed topology, that is, the set of links $E(t)$ keeps unchanged for all time index t. However, due to node mobility, $E(t)$ will change over time t, therefore s needs to frequently update routes. Then after several route updates, the probability that s still has not been detected as malicious will be very small. For example, assume that each route update is independent, after 5 times of route updates, even for $n = 2$, the probability that s has not been detected as malicious is less than 0.06%. That is, attackers has negligible chance to flee. In summary, when the malicious SD pair (s, d) tries to launch IDPA, to avoid being detected and to maximize the damage, the optimal strategy is to use only one route to inject data packets by conforming to

TABLE I

SIMULATION PARAMETERS

Number of Good Nodes	100
Number of Malicious Nodes	0-50
Maximum Velocity (v_{max})	10 m/s
Average Pause time	300 seconds
Dimensions of Space	1500m × 1500m
Maximum Transmission Range	300 m
Average Packet Inter-Arrival Time	1 seconds
Data Packet Size	1024 bytes
Link Bandwidth	1 Mbps

both the maximum hop number L_{maxhop} and the legitimate rate $\lambda_{s,d}$, which is equivalent to say that the optimal strategy is not to launch IDPA.

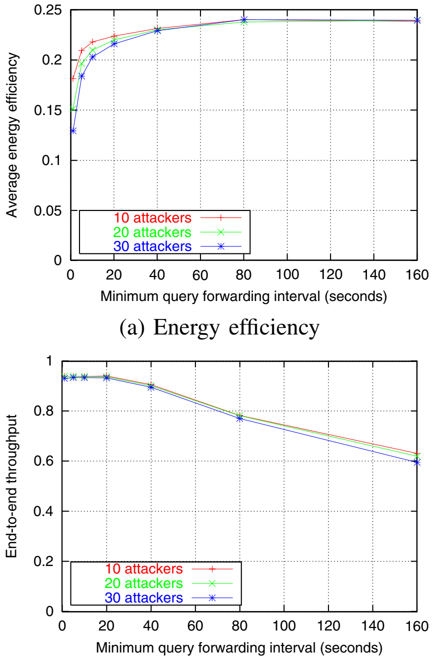
Besides injecting traffic by themselves, attackers may also impersonate good nodes to launch injecting traffic attacks in attempt to avoid being detected as well as let those impersonated good nodes being mistakenly detected as malicious. Next we analyze the effects of possible impersonation attacks that can be launched by attackers. In the proposed mechanisms, the only way that an attacker m can impersonate a good node s who has not been compromised is to first record the packets that s has transmitted, then later forwards/broadcasts these packets. Specifically, there are two situations:

- Situation 1: m recorded a query packet issued by s at time t and rebroadcast it at time $t_1 > t$. However, since this query packet has been seen by all other nodes in the network due to the flooding nature of query message, no nodes will further process this query packet.
- Situation 2: m recorded a data packet issued by s at time t and forwarded it at time $t_1 > t$. However, since nodes on the route associated to this data packet will only process this packet at most one time, forwarding this packet at time t_1 by m cannot cause damage to other nodes.

In summary, impersonation attack cannot cause further damage to good nodes in the network.

V. SIMULATION STUDIES

We use an event-driven simulator to simulate mobile ad hoc networks. Nodes are randomly deployed inside a rectangular area, and each node moves according to the *random waypoint* model [10]: a node starts at a random position, waits for a duration called the *pause time* that is modeled as a random variable with exponential distribution, then randomly chooses a new location and moves toward the new location with a velocity uniformly chosen between 0 and v_{max}. When it arrives at the new location, it waits for another random pause time and repeats the process. The physical layer assumes that two nodes can directly communicate with each other successfully only if they are in each other's transmission range. The MAC layer protocol simulates the IEEE 802.11 Distributed Coordination Function (DCF) with a four-way handshaking mechanism [12]. Some simulation parameters are listed in Table I.



(a) Energy efficiency

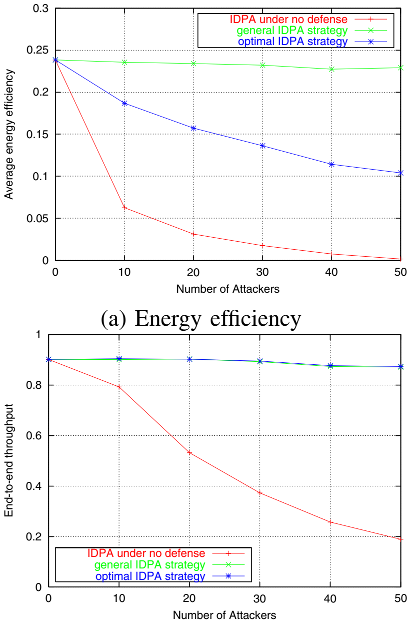
(b) End-to-end throughput

Fig. 3. Limiting route request rate vs. system performance

In the simulations, 50 good nodes are selected as the packet generators, and each will randomly pick a good node to send packets, therefore the total number of SD pairs are 50. For each malicious node who launches injecting traffic attacks, it will randomly pick another malicious node who also launches injecting traffic attacks as the destination to inject packets. For each malicious node who launches routing disruption attacks, it will not inject traffic to the network. All SD pairs (good or malicious) are set to be legitimate, and for each pair, packets are generated according to a Poisson process with a pre-specified traffic rate known by all nodes, where the average packet inter-arrival time is 1 second. For malicious nodes who launch injecting traffic attacks, they will increase the average packet injection rate by 10 times. Also, all data packets have the same size.

In our simulations, each configuration has been run 20 independent rounds using different random seeds, and the result are averaged over all the 20 rounds. For each round, the simulation time is set to be 5000 seconds. When we calculate the energy efficiency, only transmission energy consumption has been considered, one reason is that transmission energy consumption plays a major role in overall energy consumption, and another reason is that receiving energy consumption may vary dramatically over different communication systems due to their different implementations. However, both data and route request packets have been considered. We assume that the transmission energy needed per data packet is normalized to be 1.

We first investigate the tradeoff between limiting the route request rate and system performance. Although the performance also depends on other factors such as the mobility pat-



(a) Energy efficiency

(b) End-to-end throughput

Fig. 4. Effects of IDPA under different configurations

tern, the number of nodes in the network, the average number of hops per route, etc., to better illustrate the tradeoff between limiting the route request rate and system performance, the other parameters are set to be fixed. However, similar results can also be obtained by changing these parameters.

Fig. 3 illustrates the tradeoff between limiting the route request rate and network performance. In this set of simulations, all malicious nodes will only inject route request packets and will not inject any data packets or launch routing disruption attacks. We assume that all good nodes have the same minimum route request forwarding interval denoted by T^{min}, but all malicious nodes will set their route request rate to be 1 per second. From Fig. 3(a) we can see that with the increase of T^{min} from 1 to 80 seconds, the energy efficiency of good nodes also increases, and keeps almost unchanged from 80 to 160 seconds. The reason is that when T^{min} is small, attackers can waste good nodes' energy through injecting a lot of route request packets to request others to forward. Fig. 3(b) shows that with the increase of T^{min} from 1 second to 20 seconds, the end-to-end throughput of good nodes keeps almost unchanged, while with the increase of T_{min} from 80 seconds to 160 seconds, the end-to-end throughput of good nodes drops almost linearly. These results also motivate us to pick T^{min} to be 40 seconds in the following simulations.

Fig. 4 shows the simulation results under various types of IDPA. In Fig. 4, "IDPA under no defense" denotes the case that attackers launched simple IDPA and the underlying system has not launched any defending mechanism; "general IDPA strategy" denotes the case that attackers launch IDPA but the mechanisms described in Section III have been launched, where both multiple-route IDPA and long-route IDPA have been simulated; "optimal IDPA strategy" denotes the case that attackers will use only one route to inject data packets which conforms both to the maximum hop number $L_{maxhop} = 10$ and to the legitimate maximum packet injection rate and the mechanisms described in Section III have been launched.

From Fig. 4(a) we can see that when there is no defending mechanisms for IDPA, even simple IDPA can dramatically degrade the energy efficiency of good nodes. When the defending mechanisms described in Section III are employed, from attackers' point of view, launching IDPA has no any gain in decreasing the energy efficiency of good nodes. However, if attackers apply the optimal IDPA strategy, they can still degrade the energy efficiency of good nodes. From Fig. 4(b) we can see that without employing necessary defending mechanisms, with the increase of the number of attackers, even simple IDPA can dramatically degrade the end-to-end throughput of good nodes due to the congestion they caused. When the defending mechanisms described in Section III are employed, launching IDPA has almost no effects on the performance of good nodes' end-to-end throughput.

VI. Related Work

To secure ad hoc networks, the first step is to prevent attackers from entering the network through secure key distribution and secure route and neighbor discovery, such as [1], [5], [6], [13]–[17]. In [1], Zhou and Haas investigated distributed certificate authorities in ad hoc networks using threshold cryptography. In [4], Hubaux et al. developed the idea of self-organized public-key infrastructure similar to PGP in the sense that public-key certificates are issued by the users. The difference with PGP is that in their system, certificates are stored and distributed by the users. In [18], Capkun et al. discussed how to build security associations with the help of mobility in mobile ad hoc networks.

Besides injecting traffic attacks, routing disruption attacks can also be severe threats to ad hoc networks, which refer to that attackers attempt to cause legitimate data packets to be routed in dysfunctional ways, and consequently cause packets to be dropped or extra network resources to be consumed. Papadimitratos and Haas [13] proposed a secure routing protocol for mobile ad hoc networks that guarantees the discovery of correct connectivity information over an unknown network in the presence of malicious nodes. Sanzgiri et al. [14] considered a scenario that nodes authenticate routing information coming from their neighbors while not all the nodes on the path will be authenticated by the sender and the receiver. Hu, Perrig and Johnson [5] proposed Ariadne, a secure on-demand ad hoc network routing protocol, which can prevent attackers or compromised nodes from tampering with uncompromised routes that (only) consist of uncompromised nodes. In [6], [16], they describe how to defend rushing attacks through secure neighbor discovery and how to apply packet leashes to defend against wormhole attacks. Later, Capkun and Habaux investigated secure routing in ad hoc networks in which security associations exist only between a subset of all pairs of nodes [19]. Aad et al. [7] studied DoS resilience in ad hoc networks, where two attacks are studies: black hole and JellyFish. Yu et al. [20] proposed a general framework to defend against routing disruption attacks in ad hoc networks.

Once attackers have entered the network, the schemes based on secure key distritbuting and secure route discovery will become ineffective. In these situations, schemes based on monitoring traffic in the network can be used to detect malicious nodes and to confine the damage, such as [2], [3], [21]–[24]. Initial work using these mechanisms was proposed by Marti et al [3]. They considered the case that nodes agree to forward packets but fail to do so, and proposed two tools that can be applied upon source routing protocols: *watchdog* and *pathrater*. However, this system suffers some problems. First, many attacks can cause a malicious behavior not being detected, such as ambiguous collisions, receiver collisions, limited transmission power, collusion, and partial dropping, and malicious nodes can easily propagate false information to slander good nodes. In [21], [25], the authors extended the ideas in [3], and allowed the reputation to propagate throughout the network. However, since these schemes still rely on watchdog, they also suffer the same types of problems as [3]. Furthermore, once reputation is allowed to propagate, attackers can also collude to frame up or blackmail other nodes. In [2], Zhang and Lee discussed intrusion detection in wireless ad hoc networks. They examined the vulnerabilities of a wireless ad hoc network, then introduced multi-layer integrated intrusion detection and response mechanisms. However, they have not described specific mechanisms to secure ad hoc networks.

Some other related work appeared in [22]–[24], where instead of cooperative ad hoc networks, the authors considered the scenario that nodes in the network are selfish which are not willing to forward packet on the benefits of other nodes. They propose schemes to stimulate cooperation among selfish nodes based on credit system or game theory. However, those schemes cannot handle the situations with the presence of malicious nodes, whose objective is to maximize the damage they cause to the network, instead of maximize their own benefits obtained from the network.

VII. Conclusion

In this paper we have studied the possible injecting traffic attacks that can be launched in cooperative ad hoc networks, and proposed a set of mechanisms to defend against such attacks. Both query flooding attacks and injecting general data packets attacks have been investigated. Furthermore, for injecting general data packets attacks, the situations that attackers may use some advanced transmission techniques, such as directional antennas or beamforming, to avoid being detected have also been studied. Our theoretical analysis has shown that when the proposed mechanisms are used, the best strategy for attackers is not to launch injecting traffic attacks. Extensive simulation studies have also agreed with our theoretical analysis.

Acknowledgments

This work was supported in part by the Army Research Office under URI Award No. DAAD19-01-1-0494.

References

[1] L. Zhou and Z. Haas, "Securing Ad Hoc Networks," *IEEE Network Magazine*, vol. 13, no. 6, pp. Nov./Dec., 1999.

[2] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks," in *MobiCom 2000*, Boston, MA, USA, Aug. 2000.

[3] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in *Mobicom 2000*, August 2000, pp. 255–265.

[4] J. P. Hubaux, L. Buttyan, and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks," in *MobiHOC 2001*, May 2001.

[5] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," in *MobiCom 2002*, Atlanta, GA, USA, Sep. 2002.

[6] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," in *WiSe*, San Diego, CA, USA, Sep. 2003.

[7] I. Aad, J. P. Hubaux, and E. Knightly, "Denial of service resilience in ad hoc networks," in *ACM MobiCom*, Philadelphia, PA, September 2004.

[8] J. D. Kraus and R. J. Marhefka, *Antennas: for All Applications*, McGraw-Hill, New York, 3rd edition, 2002.

[9] S. Haykin, *Adaptive Filter Theory*, Prentice Hall, Sep. 2001.

[10] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing," In *Moible Computing*, edited by Tomasz Imielinski and Hank Korth, chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.

[11] "Secure Hadh Standard," Federal Information Processing Standards Publication 180-1, 1995.

[12] IEEE Computer Society LAN MAN Standards Committee, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-1007," The Institue of Electrical and Electrics Engineers.

[13] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad hoc Networks," in *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, Jan 2002.

[14] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," in *Proceedings of the International Conference on Network Protocols (ICNP)*, Nov. 2002.

[15] M. G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," in *WiSe*, Sep. 2002.

[16] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," in *IEEE Infocom*, 2003.

[17] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," *Ad Hoc Networks Journal*, vol. 1, pp. 175–192, 2003.

[18] S. Capkun, J.-P. Hubaux, and L. Buttyan, "Mobility Helps Security in Ad Hoc Networks," in *MobiHOC 2003*, Annapolis, Maryland, USA, June 2003.

[19] S. Capkun and J.-P. Hubaux, "BISS: Building Secure Routing out of an Incomplete Set of Security Associations," in *WiSe*, San Diego, CA, USA, Sep. 2003.

[20] W. Yu, Y. Sun, and K. J. R. Liu, "HADOF: Defense against routing disruptions in mobile ad hoc networks," in *IEEE INFOCOM*, Miami, FL, March 2005.

[21] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol," in *Mobihoc*, 2002, pp. 226 – 236.

[22] L. B. and J.-P. Hubaux, "Stimulating Cooperation in Self-organizing Mobile Ad Hoc Networks," *Mobile Networks and Applications*, vol. 8, no. 5, pp. 579 – 592, Oct. 2003.

[23] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks," in *INFOCOM 2003*, 2003.

[24] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in Wireless Ad Hoc Networks," in *IEEE INFOCOM*, 2003.

[25] P. Michiardi and R. Molva, "Core: a COllaborative REputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," in *IFIP - Communications and Multimedia Security Conference*, 2002.