A Joint Performance-Vulnerability Metric Framework for Designing Ad Hoc Routing Protocols

Andrew Clark*, Rommie Hardy† and Radha Poovendran*
* Network Security Lab (NSL), EE Dept., University of Washington, Seattle, WA, 98195, USA
† Army Research Laboratory, Adelphi, MD, 20783

***Abstract*—When a network is deployed in a hostile environment, different paths between nodes may provide varying levels of resilience to adversarial attack. Therefore, in order to ensure that network services are both timely and secure, both the vulnerability and performance of the path must be taken into account during route selection. However, current routing protocols do not take resilience of intermediate links into account, instead focusing on optimizing use of network resources. In this work, we propose a new class of *resilience-enhanced routing protocols* that incorporate the security of individual communication links when selecting a routing path. To enable resilient path selection, we introduce a *joint performance-vulnerability metric*, which quantifies the cost of a link based on both performance and vulnerability characteristics, so that shortest paths chosen using this metric will be both efficient and resilient to attack. We give an example that measures resilience to key exposure in ad hoc networks and demonstrate the feasibility of our scheme through analysis and simulation.**

I. Introduction

In a wireless ad hoc network, message traffic between distant nodes may be routed through multiple intermediate links. Ad hoc routing protocols have been designed to select routes that make efficient use of network resources. Widely used protocols include Optimal Link-State Routing (OLSR), Dynamic Source Routing (DSR), and Ad hoc On-demand Distance Vector (AODV) routing. A survey of current routing protocols is contained in [1].

When a network is deployed in a hostile environment, the use of multi-hop routing creates new attack options for an adversary. The routing protocol itself may be exploited. An adversary in control of several network nodes may spread false information about the network topology during route selection. This may result in routes that are inefficient or pass through adversarial nodes, potentially leading to eavesdropping or packet loss. Ad hoc routing schemes have been proposed that use authentication checks to prevent unauthorized nodes from interfering with route selection [2], [3].

Even if the routing protocol is executed properly, each intermediate link creates a potential point of adversarial attack. For example, the adversary can carry out a denial-of-service attack by jamming an intermediate link. If messages are decrypted and re-encrypted at each hop, then recovery of the encryption key used by an intermediate link, either through cryptanalysis or physical capture, will allow the adversary to eavesdrop on the communication session. In a heterogeneous network, different intermediate links will have varying levels of resilience to attack. There have been efforts to quantify the impact of these attacks (see for instance [4]). However, many of the current routing protocols focus on optimization of network resources.

In this work, we propose a class of routing protocols that evaluate prospective routes based on both the performance and attack resilience of intermediate links. Using this approach, existing routing protocols can be modified to incorporate attack resilience. Furthermore, optimal routes can be computed efficiently and in a distributed fashion.

As a case study, we apply this approach to reduce vulnerability to key exposure in ad hoc networks. Many lightweight key management protocols (e.g. [5]) use the same keys to secure different communication links. This results in increased vulnerability to key compromise, since capturing a single key (for instance, through node capture) can allow eavesdropping on multiple communication links. For arbitrary key management schemes, we show how efficient paths that are resilient to key exposure can be selected.

Our Contributions: In this work, we make the following contributions:

- Introduce *resilience-enhanced routing protocols*, which choose routes based on a combination of security and performance metrics.
- Propose a framework for designing joint performance-vulnerability metrics, based on combinations of existing performance and vulnerability metrics, that can be used by resilience-enhanced routing.
- Demonstrate the feasibility of our proposed scheme through analytical evaluation and simulation.

The rest of this paper is organized as follows. In Section II, we define our network and adversary models, as well as introduce the formal definition of resilience-enhanced routing. In Section III, we give an overview of performance and vulnerability metrics and propose a joint performance-vulnerability metric. In Section IV we provide analytical and empirical studies of the effectiveness of our metric. Our conclusions and directions for future work can be found in Section V.

II. Problem Statement

In this section, we introduce our communication and adversary models and provide the definition of a resilience-enhanced routing protocol.

A. Network Model

We assume a network of N nodes, indexed by the set $V = \{1, \ldots, N\}$. The nodes are deployed over an area

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Joint Performance-Vulnerability Metric Framework for Designing Ad Hoc Routing Protocols	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Army Research Laboratory,Adelphi,MD,20783**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

When a network is deployed in a hostile environment different paths between nodes may provide varying levels of resilience to adversarial attack. Therefore, in order to ensure that network services are both timely and secure, both the vulnerability and performance of the path must be taken into account during route selection. However, current routing protocols do not take resilience of intermediate links into account instead focusing on optimizing use of network resources. In this work, we propose a new class of resilience-enhanced routing protocols that incorporate the security of individual communication links when selecting a routing path. To enable resilient path selection, we introduce a joint performance-vulnerability metric which quantifies the cost of a link based on both performance and vulnerability characteristics, so that shortest paths chosen using this metric will be both efficient and resilient to attack. We give an example that measures resilience to key exposure in ad hoc networks and demonstrate the feasibility of our scheme through analysis and simulation.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**6**	

TABLE I
NOTATION USED IN THIS PAPER

Notation	Definition
V	Set of network nodes
N	Number of nodes
$\mathcal{A}$	Network deployment region
x_i	Location of node with index i
r	Node radio range
G_g	Geometric network graph
$\mathcal{K}$	Key pool
f	Key distribution function
$\mathcal{P}(\mathcal{K})$	Set of subsets of $\mathcal{K}$
P	Key pool size
m	Number of keys held by each node
$\mathcal{K}_i$	Set of keys held by node i
G_k	Key graph, defining set of nodes that share keys
G	Combined geometric/key graph, defining set of nodes capable of secure communication
S	Vulnerability metric
L	Cost metric
g	Joint performance-vulnerability metric
ETX	Expected number of packet transmissions
τ	Vulnerability threshold

$\mathcal{A} \subset \mathbf{R}^2$, with node i at position $x_i \in \mathcal{A}$. Two nodes are capable of communicating over a direct wireless channel if they are within each other's radio range r. Based on this assumption, the network has a *geometric* graph structure $G_g = (V, E_g)$, where for any $i, j \in V$, we have $(i, j) \in E_g$ if and only if $||x_i - x_j||_2 \leq r$.

Due to the computational overhead associated with public key cryptography, we assume that nodes communicate with secret keys drawn from a key pool $\mathcal{K}$ according to a key distribution function $f : V \to \mathcal{P}(\mathcal{K})$, where $\mathcal{P}(\mathcal{K})$ is the set of subsets of $\mathcal{K}$. Two nodes $i, j \in V$ are capable of communicating securely only if they share at least one cryptographic key, i.e. if $f(i) \cap f(j) \neq \emptyset$. This induces a *key graph* $G_k = (V, E_k)$, where $(i, j) \in E_k$ if and only if $f(i) \cap f(j) \neq \emptyset$.

The intersection of these two graph structures provides the set of nodes that are capable of secure communication. Hence we say that the network has graph structure $G = (V, E)$, where $E = E_k \cap E_g$.

B. Adversary Model

We assume an adversary that is *active*, *mobile*, and *resource-constrained*. By active, we mean that the adversary is capable of both passive eavesdropping and physically capturing nodes. Once a node is captured, the adversary gains access to its secret keys.

As time progresses, the network will perform updates by adding new nodes, revoking compromised keys, and updating nodes with new keys. We assume that, due to resource constraints, the adversary cannot compromise a large subset of the network between updates. The adversary's mobility enables it to monitor links throughout the network and gain knowledge of the network and routing topologies. This, combined with knowledge of the network protocols used, allows the adversary to eavesdrop on any communication that is unencrypted or encrypted using compromised keys.

C. Resilient Routing

We propose the use of metrics that can be used to jointly evaluate vulnerability and performance of a given link. The end-to-end performance-security characteristics of a path can then be described as the sum of the link metric values, allowing the use of standard shortest-path routing protocols.

We now give the definition of a *joint performance-security metric*. First, we define the following general notions of a cost metric and a vulnerability metric.

Definition 1: A function $L : E \to \mathbf{R}_{\geq 0}$ is a *link cost metric* if, for some cost criteria and two links $l, l' \in E$, we have $L(l) \geq L(l')$ if and only if l has higher cost than l'.

Cost metrics may be based on the delay incurred by using a communication link, the energy cost of making a transmission, or the effect of using a link on network throughput. In this work, the two performance metrics we will consider are *hop count* and *link quality*, to be defined in the following section.

Definition 2: A function $S : E \to \mathbf{R}_{\geq 0}$ is a *link vulnerability metric* if, for some security criteria and two links $l, l' \in E$, we have $S(l) \geq S(l')$ if and only if l has higher security than l'.

In this work, we will consider the *link key vulnerability metric* (LKVM) of the link, defined in the following section, as our link security metric. Based on these definitions, we define a class of metrics that jointly evaluate vulnerability and performance.

Definition 3: A function $g : E \to \mathbf{R}_{\geq 0}$ is a *joint performance-vulnerability metric* with respect to a link performance metric L and a link vulnerability metric S if and only if, for any links $l, l' \in E$, we have $L(l) \leq L(l')$ and $S(l) \geq S(l')$ implies that $g(l) \leq g(l')$.

This definition states that a performance-vulnerability metric is well-defined if the metric value *decreases* with decreasing vulnerability and *increases* with increased cost. Based on this definition, paths with the shortest length according to a performance-vulnerability metric will have minimal cost and a high security value. In this work, we consider performance-vulnerability metrics that are defined in terms of existing cost and vulnerability link metrics.

Definition 4: A routing protocol is said to be a *resilience-enhanced routing protocol* with respect to a joint performance-security metric g if the routes produced by the protocol are shortest paths with respect to g. That is, for any nodes $i, j \in V$, a path $\pi = (i = i_0, i_1, \ldots, i_k = j)$ generated by the protocol satisfies

$$\sum_{l=1}^{k} g((i_{l-1}, i_l)) \leq \sum_{l=1}^{k'} g((i'_{l-1}, i'_l)) \tag{1}$$

for any path $\pi' = (i = i'_0, i'_1, \ldots, i'_{k'} = j)$

By basing our criteria for optimality on shortest paths, we can integrate these metrics into existing routing protocols. Note that this definition is made possible by the definition of

the joint performance-vulnerability metric; links with lower performance-vulnerability metric values will have higher security and lower cost.

III. Proposed Resilient Routing Scheme

In this section, we give our proposed joint performance-vulnerability metric and show how this motivates a straightforward resilient routing scheme.

A. Threshold Link Metric

Definition 5: Let $G = (V, E)$ be the network graph structure. Let S be a vulnerability metric and let L be a cost metric. Then the *threshold performance-vulnerability metric* $g : E \to \mathbf{R}_{\geq 0}$ is given by

$$g(l) = \begin{cases} L(l), & S(l) > \tau \\ \infty, & \text{else} \end{cases} \tag{2}$$

We denote this as the *threshold* metric because links with vulnerability metric exceeding a certain threshold are considered by the routing protocol, while links below the threshold are given infinite cost weight, and will therefore be ignored. This requires minimal extra computation compared to performance metrics alone.

This metric is based on the idea that, since compromise of a single link will lead to the capture of all traffic passing through that link, the overall security of a path will be governed by the security of its weakest link. Guaranteeing a certain security level for a path is therefore equivalent to placing a lower bound on the security of the weakest link.

The metric provides a framework for combining existing performance and vulnerability metrics into a form suitable for routing protocol design. Computation will depend on the performance and vulnerability metrics used. We now describe the performance and vulnerability metrics considered in this work.

B. Link Performance Metrics

Two link performance metrics that are commonly used by existing routing protocols are *hop count* and *link quality*, defined as follows. Hop count is equal to the number of intermediate links in a path, and is therefore equivalent to the length of a path when each link has a uniform weight of 1.

In a wireless network where channel characteristics vary between links, hop count may not be an appropriate metric, since messages sent over lossy links will need to be retransmitted, leading to high resource cost in spite of low hop count. In this case, the ETX metric, which is equal to the expected number of transmissions involved in sending a packet, can be used [6]. The ETX metric for link (A, B) is given by $1/(p_A p_B)$, where p_A is the packet delivery probability for the $A \to B$ link and p_B is the packet delivery probability for the $B \to A$ link. These probabilities can be estimated by the nodes forming the link through the use of periodic probe packets.

C. Vulnerability Metric

The vulnerability metric considered in this paper evaluates the resilience of a link to key compromise. For more information, see [7].

During a node capture attack, keys that appear with great frequency in the network will be captured first by an adversary. The frequency of key reuse will be a function of the key distribution scheme used. Hence the security of a communication link will depend both on the number of keys used and the number of times that each key is reused by the network.

Definition 6: Let $l = (i, j)$ be a communication link. Let $f : V \to \mathcal{P}(\mathcal{K})$ be a key distribution mapping, and let $\mathcal{K}_i := f(i)$ and $\mathcal{K}_{ij} = \mathcal{K}_i \cap \mathcal{K}_j$. Let $X_1, X_2, \ldots, X_l, \ldots$ be integers selected uniformly at random from V, and let $\mathcal{C}_s = \bigcup_{l=1}^{s} \mathcal{K}_{X_l}$. We define random variable T_k to be $\min\{s : k \in \mathcal{C}_s\}$ and T_{ij} to be $\max\{T_k : k \in \mathcal{K}_{ij}\}$. The metric $S(l)$ is given by $\mathbf{E}(T_{ij})$.

Intuitively, this metric can be stated in the following way. Suppose we draw nodes from the network at random and with replacement, adding the keys recovered at each round to a pool of recovered keys. Then the metric is given by the expected time to gather all keys securing the link.

Given limited information about the key distribution scheme used, it is possible for two nodes to compute their LKVM value. However, due to space constraints, we omit discussion of this computation.

D. Proposed Joint Metric

We define the joint performance-vulnerability metric used in this work to be

$$g(l) = \begin{cases} ETX(l), & S(l) > \tau \\ \infty, & \text{else} \end{cases} \tag{3}$$

In a routing protocol based on this metric, two nodes first compute their vulnerability metric value. If the value does not exceed the pre-arranged threshold, the nodes do not form any connections; otherwise, they proceed as in a conventional routing protocol. The performance of the scheme will depend heavily on the choice of threshold, giving the network owner the ability to tune the performance and security characteristics of the system. In Section IV, we discuss the effect of the threshold value on performance, which can inform the choice of threshold.

IV. Performance Evaluation

In this section, we analyze the proposed joint performance-vulnerability metric. First, using random graph theory, we derive a bound on the probability of connectivity as a function of the security threshold. Second, we present simulation results showing the effect that resilient routing has on connectivity, hop count, ETX, and resistance to attack.

A. Analytical Evaluation

We make the following assumptions. First, we assume that nodes are deployed uniformly at random over area A. Second, we assume that each node is given a set of m keys chosen uniformly at random from a pool of size P, as in

[5]. This scheme was chosen because it has been shown to achieve network connectivity with low overhead[1]. Under these assumptions, the geometric graph defined in Section II becomes a *Euclidean random graph*, while the key graph can be modeled as the random graph $G(n,p)$, where p is equal to $Pr(S > \tau)$.

As a preliminary, we have the following lemma.

Lemma 1: Let τ be the security threshold. Then the probability that the vulnerability metric for a link will satisfy $S(l) > \tau$ is bounded by

$$Pr(S(l) > \tau) \geq \sum_{t=1}^{m} (1 - p_\tau^t) \binom{P}{t} \frac{\binom{P-t}{m-t}\binom{P-m}{m-t}}{[\binom{P}{m}]^2} \quad (4)$$

where p_τ is given by

$$p_\tau = \sum_{k=\lceil \frac{N}{\tau} \rceil}^{N} \binom{N}{k} \left(\frac{m}{P}\right)^k \left(1 - \frac{m}{P}\right)^{N-k} \quad (5)$$

Proof: Let $l \in E$, and suppose $l = (i,j)$. Define event ξ_τ to be $\{S(l) > \tau\}$. Then $Pr(S(l) > \tau)$ is given by

$$Pr(\xi_\tau) = \sum_{t=1}^{m} Pr(\xi_\tau || \mathcal{K}_{ij}| = t) Pr(|\mathcal{K}_{ij}| = t) \quad (6)$$

Now, if $|\mathcal{K}_{ij}| = t$, suppose $\mathcal{K}_{ij} = \{k_1, \ldots, k_t\}$. Then from the discussion following Definition 6,

$$S(l) = \mathbf{E}(\max\{T_{k_1}, \ldots, T_{k_t}\}) \quad (7)$$

where T_{k_i} is the number of captures until key k_i has been recovered. Due to Jensen's Inequality, we can write

$$\mathbf{E}(\max\{T_{k_1}, \ldots, T_{k_t}\}) \geq \max\{\mathbf{E}(T_{k_1}), \ldots, \mathbf{E}(T_{k_t})\} \quad (8)$$

Since the key distribution is random, the $\mathbf{E}(T_{k_a})$'s are themselves random variables. The value of $\mathbf{E}(T_{k_a})$ will be equal to N/N_{k_a}, where N_{k_a} is the number of nodes that have been issued key k_a. We then have

$$\begin{aligned} Pr(\xi_\tau || \mathcal{K}_{ij}| = t) &= Pr(\mathbf{E}(\max\{T_{k_1}, \ldots, T_{k_t}\}) > \tau) \\ &\geq Pr(\max\{\mathbf{E}(T_{k_1}), \ldots, \mathbf{E}(T_{k_t})\} > \tau) \\ &= 1 - Pr(\mathbf{E}(T_{k_1}) \leq \tau, \ldots, \mathbf{E}(T_{k_t}) \leq \tau) \\ &= 1 - Pr(\mathbf{E}(T_{k_1}) \leq \tau)^t \end{aligned}$$

Since we assume that keys are independently distributed. Now $\{\mathbf{E}(T_{k_1}) \leq \tau)\}$ is equivalent to $\{N/N_{k_1} \leq \tau\}$, which can be rewritten as $\{N_{k_1} \geq N/\tau\}$. N_{k_1} is a binomial random variable, and so the probability of this event, p_τ, is denoted by

$$p_\tau = \sum_{k=\lceil \frac{N}{\tau} \rceil}^{N} \binom{N}{k} \left(\frac{m}{P}\right)^k \left(1 - \frac{m}{P}\right)^{N-k} \quad (9)$$

Now, it remains to calculate $Pr(|\mathcal{K}_{ij}| = t)$. This is the probability that two nodes share exactly k keys; since each node's set of keys is chosen independently at random, this is given by

$$\binom{P}{t} \frac{\binom{P-t}{m-t}\binom{P-m}{m-t}}{[\binom{P}{m}]^2} \quad (10)$$

Combining these results gives the desired bound. ∎

This lemma gives a bound on the probability that two nodes will satisfy the security requirements for establishing a connection. Based on this, we can use the random graph structure of the network to find the probability that secure paths can be found.

Theorem 1: Let $\rho = \frac{N}{A}$, the density of the network graph. The probability that there exists a path between any two nodes that does not violate the vulnerability threshold is bounded below by

$$e^{-Ne^{-\rho p' \pi r^2}} \quad (11)$$

where p' is the bound on $Pr(S(l) > \tau)$ derived in the previous lemma.

Proof: A result due to Penrose [8] states that, in a geometric random graph, the connectivity and minimal degree of the network will be equal with probability 1 as the network size increases asymptotically. As a corollary, the probability that a graph is connected is equal to the probability that the minimum degree of the graph is at least 1.

In a geometric random graph, the distribution of nodes behaves as a two-dimensional Poisson process. Hence we have

$$Pr(\text{ k nodes in a region of size } A') = e^{-\rho A'} \frac{(\rho A')^k}{k!} \quad (12)$$

Now, in order for two nodes to share a link in the overall graph G, the link between them must be above the vulnerability threshold. Under the i.i.d. assumption, this occurs independently with probability $p = Pr(S(l) > \tau)$ for each link. The number of nodes in a region of size A' capable of communicating with a given node becomes a Poisson random variable with parameter $p\rho A'$.

In our case, the region of interest is the radio range of a given node, which is a disc of radius r. Thus we have that, for any node i, the degree D_i of the node satisfies

$$Pr(D_i = k) = e^{-\rho p \pi r^2} \frac{(\rho p \pi r^2)^k}{k!} \quad (13)$$

and so the probability that the degree of a node is at least one is

$$Pr(D_i \geq 1) = 1 - Pr(D_i = 0) = 1 - e^{-\rho p \pi r^2} \quad (14)$$

If we assume that the degrees of the nodes are independent, we have that the probability that all N nodes have minimum degree at least one is

$$(1 - e^{-\rho p \pi r^2})^N \approx e^{-Ne^{-\rho p \pi r^2}} \quad (15)$$

Now, note that this formula increases as p increases. Since we have $p > p'$, we have the desired result. ∎

This theorem allows us to determine whether a key distribution scheme with given parameters will result in a connected graph for a certain security threshold.

[1]Note that the definition of S takes the number of keys securing a link into account when evaluating vulnerability, and hence can be used for arbitrary key distributions as well.

TABLE II
LIST OF SIMULATION PARAMETERS

Parameter	Description	Setting
N	Number of nodes	200
A	Deployment area	2400x2400m
r	Radio range	400m
P	Size of key pool	765, 368, 256
m	Size of each node's set of keys	30
τ	Vulnerability threshold	Varies from 1 to $N/2$
α	Path-loss exponent	2

B. Simulation

To demonstrate the feasibility of resilience-enhanced routing, we present simulation results that describe the behavior of the threshold routing scheme.

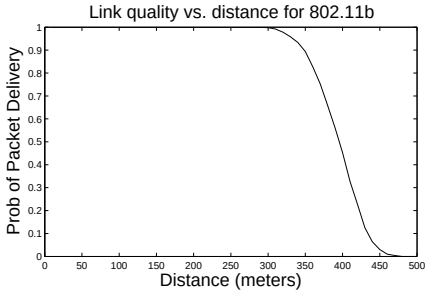

Fig. 1. Link quality as a function of distance for free-space path-loss model

1) Simulation Setup: A network of 200 nodes deployed in a random static topology was simulated using Matlab.

In order to estimate the link quality characteristics, preliminary simulations were performed in ns-3. The goal was to find the packet delivery probability (i.e. link quality) as a function of the distance d between two nodes. Two nodes were initialized at a distance d apart. The environment was assumed to have free-space path loss, i.e., $P_{rx} = P_{tx}d^{-\alpha}$.

When modeling wireless networks, it is typically assumed that $2 \leq \alpha \leq 7$. In this work, we choose $\alpha = 2$. The transmit power was set at 0 dBm, while the receiver sensitivity was set at -85 dBm. The simulation parameters were based on the 802.11b standard. The packet delivery probability was estimated by broadcasting 1000 packets from the sender and counting the number of packets received at the destination. Using these values, the link quality-distance curve in Figure 1 was found. The curve displays near-perfect packet delivery up until a range of roughly 300 meters, followed by a linear decay to 0.

Based on these results, the node range was set at 400m, roughly the point when $Pr(error) = 0.5$. Nodes were deployed uniformly at random in a 2400m x 2400m square area. Keys were then chosen independently at random and distributed to the nodes according to the scheme of [5], with key pool sizes $P = 765$, 378, and 256, and key ring size $m = 30$. A summary of the simulation parameters can be found in Table II.

During each trial, a random network topology was generated and the vulnerability metric values were calculated. 50 pairs of nodes were chosen at random and the hop count and link quality of the shortest paths between them were computed as τ, the security parameter, varied from 1 (representing minimal security) to $N/2$ (the maximum possible value). For each value of τ, the values of hop count and link quality were averaged over all the node pairs. Also, the percentage of the randomly chosen pairs for which a path exists was computed. The average over all trials was then plotted.

The level of security afforded by each routing scheme was also analyzed. For each value of τ and each pair of nodes, the number of random captures needed to compromise the path between the nodes was estimated via Monte Carlo methods. The average over all paths was then computed; these values were then averaged over all trials and plotted.

2) Simulation Results: Figure 2a summarizes the effect of varying the threshold on the network connectivity. For each key pool size, we see that the connectivity remains high until a certain value of τ (which we will denote τ_c) is reached, at which point there is a precipitous drop in connectivity. Explicitly, we define τ_c by

$$\tau_c = \max\{\tau : P_{connect}(\tau) > 0.9\} \tag{16}$$

As Figure 2b shows, the average hop count between randomly chosen points increases as the threshold τ increases. This is to be expected, since the number of valid links is strictly decreasing in τ. This requires selecting routes that are more indirect, but are composed of more secure links. In Figure 2d, we see that increasing τ results in an increase in the number of captures required by the adversary to compromise the traffic between source and destination – roughly 25% more captures for $P = 368$ and 20% more captures for $P = 756$. Thus, even below τ_c, there is a trade-off between performance and security.

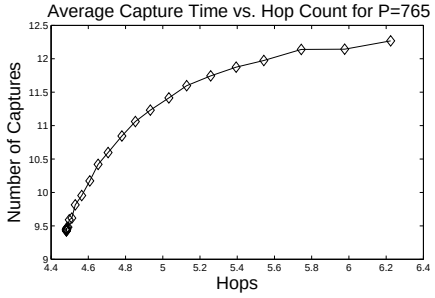

Fig. 3. Trade-off between hop count and resilience to node capture. Eventually, taking longer and more secure paths ceases to provide an improvement in security.

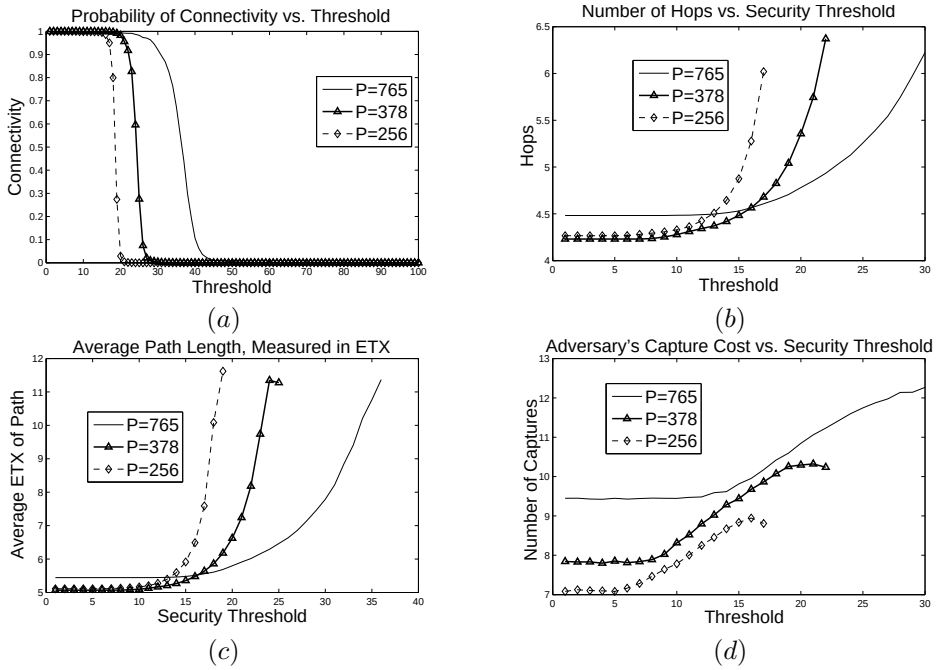

Fig. 2. Plots of network performance and security as a function of the vulnerability threshold. Plots are based on ensemble averages over 50 random network realizations. (a) Effect of increased threshold on the probability that two random nodes will be connected. Note the rapid drop as $\tau > \tau_c$. (b) Effect of threshold on hop count. Hop count increases as fewer and fewer links meet vulnerability metric criteria. (c) Effect of threshold on the ETX metric. As with hop count, there is an increase as τ exceeds the threshold. (d) Effect of threshold on the security level, measured as the average number of random captures required to compromise a path. Increasing the security threshold results in more resilient paths.

This trade-off is further examined in Figure 3, which is a plot of security level vs. hop count, with each point representing a different value of τ between 1 and τ_c. The shape of the curve suggests that increasing the threshold results in "diminishing returns," as decreases in performance result in smaller gains in security. This is because even though the individual links in the path may be more secure, having to make additional hops increases the number of possible points of attack. These effects can also be seen in Figure 2c, which shows the effect of the vulnerability threshold on the ETX metric.

These plots also show the effect of changing the key distribution parameters on the performance of the system. We see that for a larger key pool, the vulnerability metric values are higher, resulting in connectivity even for higher values of τ. Furthermore, the paths chosen are more resilient to node capture. This is to be expected, since when keys are distributed independently and at random, it will take more random captures to cover the entire key pool. Furthermore, Figure 2b shows that we do not pay a significant price in routing performance for the extra security afforded by a large key pool.

V. Conclusions and Future Work

In this paper, we have considered the problem of designing routing protocols that choose routes that are resilient to adversarial attack. In order to do so, we have defined a link weight that jointly describes the performance and security of a communication link. We have shown that this weight can be used to design shortest-path routing protocols that are efficient, as measured by traditional performance metrics.

Two directions for future work are as follows. First, metrics that measure resilience to other types of attack will be proposed. Second, new types of performance-vulnerability metrics other than the threshold metric presented here may be appropriate for other attacks or network settings. Hence a goal of future work will be to find new ways of jointly representing cost and vulnerability for a link or path.

References

[1] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 325–349, 2005.

[2] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proceedings of the 10th IEEE International Conference on Network Protocols*, 2002, pp. 78–89.

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[4] P. Tague, D. Slater, J. Rogers, and R. Poovendran, "Evaluating the Vulnerability of Network Traffic Using Joint Security and Routing Analysis," *IEEE Transactions on Dependable and Secure Computing*, pp. 111–123, 2008.

[5] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*. ACM, 2002, pp. 41–47.

[6] D. Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," *Wireless Networks*, vol. 11, no. 4, pp. 419–434, 2005.

[7] A. Clark and R. Poovendran, "A Metric for Quantifying Key Exposure Vulnerability in Wireless Sensor Networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference*, 2010.

[8] M. Penrose, "On k-connectivity for a geometric random graph," *Random structures and Algorithms*, vol. 15, no. 2, pp. 145–164, 1999.