To Be Proactive or Not: A Framework to Model Cyber Maneuvers for Critical Path Protection in MANETs

Zhuo Lu
Computer Science
University of Memphis
TN 38152, USA
zhuo.lu@memphis.edu

Lisa Marvel
Army Research Laboratory
Aberdeen Proving Ground
MD 21001, USA
lisa.m.marvel.civ@mail.mil

Cliff Wang
Computer Science
NC State University
Raleigh NC 27695, USA
cliffwang@ncsu.edu

ABSTRACT

Recently, proactive strategies have received much attention as they make a system more dynamic and difficult to predict, therefore reducing the impact of adversary attacks. In this paper, we aim at modeling and evaluating the effectiveness of proactive cyber maneuvers to protect the critical path between a source-destination pair for mission operations in a mobile ad-hoc network (MANET) in the presence of an adversary. We propose a generic framework to analytically model cyber maneuvers and define their associated utilities. With the proposed framework, we develop the optimal solution to maximize the lifetime of the critical path with security assurance. We find that sufficient statistical information in the network is vital for the network defender to be proactive, choose the best cyber maneuvers to protect the critical path, and consequently outperform conventional reactive strategies. We also use simulations to validate the effectiveness of our solution.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection, Data communications*

General Terms

Theory; Design; Security

Keywords

Cyber Maneuvers; Proactive Strategies; Attack, Infection and Defense; Mobile Ad-hoc Networks

1. INTRODUCTION

Recently, proactive strategies have received much attention in cyber defense [1–5]. Instead of following the conventional detect-then-act pattern, proactive defense makes a system more dynamic and difficult to predict, therefore they can significantly reduce the negative impact of attacks even in the presence of the most effective adversary against static systems [5–7]. Proactive strategies can be applied to a number of computer and network systems to actively protect these systems from being compromised.

In this paper, we aim at modeling and evaluating the effectiveness of proactive cyber maneuvers in the scenario of a mobile ad-hoc network (MANET), which is an important infrastructure-less network of mobile wireless devices for military operations. In battlefield scenarios, the success of military operations largely relies on the security and reliability of MANETs. As a MANET is usually deployed in harsh or hostile environments, it must have the capability to counter-react any adversary that attempts to compromise its computer and network systems. However, a MANET is also a resource-limited system with many constraints, such as computing power, bandwidth, and energy [8–11]. Therefore, how to effectively use proactive strategies under different constraints is critical to the success of MANET-based mission operations in the presence of adversaries.

To this end, we consider a typical MANET defense scenario, in which an adversary aims to continuously compromise or infect network nodes by taking advantage of their system vulnerabilities; at the same time, a network defender attempts to patch vulnerable nodes or heal infected nodes such that a critical path between a source and a destination is always secured. In order to ensure such a critical path lasts the longest, the network defender should choose the best cyber maneuver in the cyber domain, such as reactively healing some infected nodes and/or proactively patching some vulnerable nodes that have not yet been infected.

The infection-healing process between a network defender and an adversary in wireless networks has been explored in the literature (e.g., [12–14]). However, most studies focus on comparing the processes between infecting vulnerable nodes and healing infected nodes with the objective to see whether the infection or healing process will eventually dominate in the network. Therefore, a few important questions still remain open in the context of proactive defense in MANETs.

1. Will a critical path last longer if the network defender proactively patches vulnerable nodes instead of trying to heal infected nodes? Is it good to be proactive?

2. What if there are more cyber maneuvers available in the cyber domain, such as partially healing a node to make sure it is secure in routing functions, or completely blocking the node from routing?

3. From the perspective of mission operations, how to provide the best decision to prolong the lifetime of the

MTD'15, October 12, 2015, Denver, Colorado, USA.
© 2015 ACM. ISBN 978-1-4503-3823-3/15/10 ...$15.00.
DOI: http://dx.doi.org/10.1145/2808475.2808479.

critical path based on fine-grained utilities (e.g., costs and benefits) of both proactive and reactive cyber maneuvers that are available to the network defender?

In this paper, we propose a new generic framework to analytically model the utilities (e.g., costs and benefits) of cyber maneuvers in the cyber domain that are available to the network defender. The framework enables us to offer the first study on how to systematically manage both proactive and reactive maneuvers to achieve a mission objective. Based on this framework, we develop the solution to choose the best cyber maneuvers to prolong the lifetime of the critical path. In addition, we use simulations to show that our solution is effective in proactive defense for MANETs. Our contributions in this paper are as follows.

1. We propose a generic framework to analytically model cyber maneuvers and their associated utilities. The new framework enables us to systematically analyze both reactive and proactive cyber maneuvers to protect the critical path in a MANET. Moreover, the framework can be also easily adapted to MANET scenarios with different mission objectives.
2. We find that if the network defender only has the current static information of the network, it may be difficult to proactively patch vulnerable nodes. The best strategy is to defer proactive patching unless we have to (although it does not necessarily mean to avoid being proactive).
3. If sufficient statistical information is available (e.g., the trend of the infection process and network traffic pattern), we find that the network defender can be proactive and choose the best cyber maneuvers to maximize the lifetime of the critical path, hence outperforming conventional reactive strategies.

The remainder of this paper is organized as follows. In Section 2, we state our research problem and specify models. In Section 3, we present our analysis on critical path protection under the proposed framework. In Section 4, we describe our simulation results. Finally, we conclude this paper in Section 5.

2. SYSTEM MODELS

In this section, we describe our problem scenario and system models.

2.1 Problem Scenario and Network Model

We consider a MANET with n nodes, as shown in Fig. 1. There exists an adversary who attempts to compromise mobile nodes by taking advantage of their software vulnerabilities. We call such an attacking process the infection process. There also exists a patching node that wants to make the best decision with a set of available cyber maneuvers (e.g., healing an infected node or patching a node with known vulnerability) to secure a critical path between a particular source-destination node pair. Without loss of generality, we define the following parameters.

- The set of node indexes is denoted by $\mathcal{N} = \{1, 2, \cdots, n\}$.
- Node 1 is the attacker that moves around in the network, aiming to infect its neighboring nodes. The attacker cannot be healed or patched.

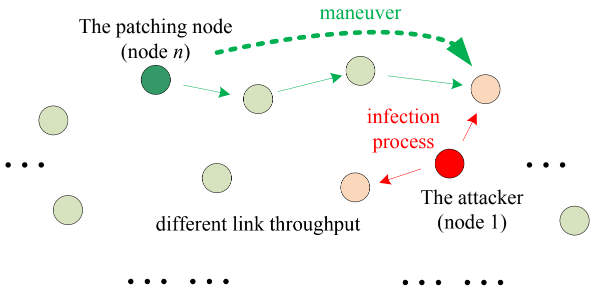

Figure 1: Network and node models.

- Node n is the patching node that can never be infected and aims to secure the critical path by performing cyber maneuvers in the network.
- Nodes 2 to $(n-1)$ are operating nodes in the MANET that can be in different node states, such as infected or patched. These nodes are battery-supplied. Denote by $\mathcal{N}_o = \{2, 3, \cdots, n-1\}$ the set of indexes of all operating nodes.
- The transmission range of each node is $r > 0$, and we say two nodes i and j $(i, j \in \mathcal{N})$ have a network link if they are in each other's transmission range.
- Links can have different throughputs. The link throughput between nodes i and j is denoted by $T_{i,j}$. Apparently, $T_{i,j} = 0$ if there is no network link between nodes i and j. At a particular time, the value of $T_{i,j}$ depends on network setups and topology, such as transmission power and the distance between the nodes.

We assume that the network starts to operate at time 0, when the adversary (i.e., node 1) and the patching node (i.e., node n) start the attack and defense processes, respectively. If a node is infected, it will repeat the same infection process, trying to infect its neighboring nodes.

Our objective is to secure all the nodes on the critical path between the source and the destination for mission operations. In other words, we need to make sure all nodes on the path are not in some "bad" state, which will be defined later.

2.2 Node States and Capabilities

As the network operates, a node will be vulnerable, patched, infected, or in some other states. The state of node i is denoted by $s_i \in \mathcal{S}$, in which $\mathcal{S}$ is the node state space. In the following, we describe an example of the node state space.

$$\begin{aligned} \mathcal{S} = \{&0 : \mathsf{Immune/Patched},\ 1 : \mathsf{Quarantined}, \\ &2 : \mathsf{Blocked},\ 3 : \mathsf{Vulnerable}, \\ &4 : \mathsf{Susceptible},\ 5 : \mathsf{Infected}\}, \end{aligned} \tag{1}$$

where

- Immune/Patched means a node is not vulnerable to compromise/infection or is already patched, therefore it can never be infected by the attacker that takes advantage of the same vulnerability.
- Vulnerable means a node is vulnerable to infection due to software vulnerability.

- Susceptible denotes that a node has an infected neighbor (thus exposed to the attack).
- Infected means the node is infected, thus it is also trying to infect other nodes.
- Quarantined is the state that a node is partially patched so it cannot perform all operations but can be involved in routing messages.
- Blocked is the state that a node is completely blocked by the patching node and will not be actively involved in any operational activity.

For example, $s_2 = 2$ indicates that node 2 is Blocked; and $s_{10} = 5$ means that node 10 is Infected.

It is possible to combine or remove some states, or introduce more states for the state space $\mathcal{S}$. We note that as long as the states and state transitions are well defined, removing or adding states does not affect the formulation of our analytical framework and the subsequent solutions.

Apparently, a node may or may not be involved in mission operations, depending on its state. We define the capability of a node as a function $C(s)$ that maps its state $s \in \mathcal{S}$ to a non-negative value. For example, node i can have a high capability then it is in the Immune/Patched state and a low capability when it is in the Vulnerable state. In addition, we say that a node with Infected state has zero capability; i.e., $C(s) = 0$ when $s = 5$ that corresponds to Infected in (1).

2.3 Cyber Maneuver and Cost Models

Which state a node is in depends on a number of factors, such as mobility, new software vulnerability, and the cyber maneuver performed on it. There are a set of cyber maneuvers available at the patching node that can change a node's state from one to the other. For example, if the patching node decides to patch a vulnerable node, its state will become from Vulnerable to Immune/Patched. However, such a maneuver incurs a cost, e.g., the energy consumed to route patching software from the patching node to the vulnerable node. Thus, we need to define the utilities of maneuvers.

2.3.1 Cyber Maneuvers

In the network, the patching node monitors the states of all nodes and attempts to maneuver them to ensure security. The maneuver space is the set of all potential cyber maneuvers available at the patching node, denoted by $\mathcal{M}$. An example of $\mathcal{M}$ is shown as follows.

$$\begin{aligned}\mathcal{M} = \{&M_0 : \textsf{No Action},\ M_1 : \textsf{Patch},\\ &M_2 : \textsf{Software Heal},\ M_3 : \textsf{Node Block}\},\end{aligned} \tag{2}$$

where

- Patch means the patching node will completely patch a node and change its state to Immune/Patched.
- Software Heal means the patching node will apply a patch to a node to change its state to Quarantined to make it be safely involved in routing.
- Node Block means the patching node will completely block a node.

It is also worth noting that removing or adding maneuvers in the space $\mathcal{M}$ does not affect the generic formulation of our analytical framework and the subsequent solutions. In general, we can define a maneuver $M_m \in \mathcal{M}$ ($m = 0, 1, 2, \cdots, |\mathcal{M}|$) as a function of node state s_i that maps the state of node i to another state. In our example in (2), maneuvers Patch, Software Heal, and Node Block can be denoted by functions M_1, M_2, and M_3 that change s_i to 0, 1, and 2, respectively. And M_0 means no action, satisfying $M_0(s) = s$ for any state $s \in \mathcal{S}$.

We say a maneuver is proactive if it is performed on a node that is neither Infected nor Susceptible, and say it is reactive otherwise.

2.3.2 Cost Models

Because all operating nodes are battery-supplied in the MANET, we consider the energy as the major cost for cyber maneuvers.

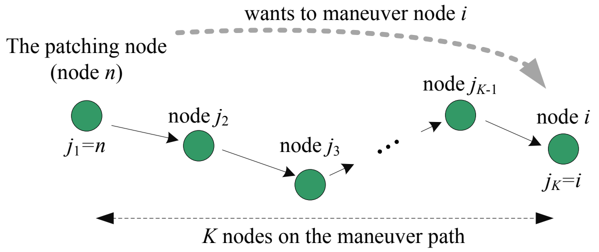
wants to maneuver node i
The patching node (node n)
j_1=n
node j_2
node j_3
node $j_{K\text{-}1}$
node i
j_K=i
K nodes on the maneuver path

Figure 2: The maneuver path from nodes n to i: there are K nodes with indexes j_1, j_2, $\cdots$, j_K.

For any cyber maneuver $M_m \in \mathcal{M}$ on node i, the patching node (i.e., node n) has to forward the maneuver data to the destination node i. As shown in Fig. 2, assume that there are K nodes on the maneuver path from nodes n to i, and denote indexes of the K nodes by j_1, j_2, $\cdots$, j_K (apparently $j_1 = n$ and $j_K = i$). Also denote the size of the data by b_m. Then, the total energy cost for node j_k to receive the data from the previous hop j_{k-1} and forward the data to the next hop j_{k+1} on the maneuver path can be written as

$$e_{m,j_k} = b_m(P_{rx}/T_{j_{k-1},j_k} + P_{tx}/T_{j_k,j_{k+1}}), \tag{3}$$

for $k = 2, 3, \cdots K - 1$, where P_{tx} and P_{rx} are the transmit and receive powers, respectively; and T_{j_{k-1},j_k} is the link throughput between nodes j_{k-1} and j_k.

Also denote by e_m the energy consumption of node i applying the maneuver; then, the energy cost of node i is

$$e_{m,j_K} = b_m P_{rx}/T_{j_{K-1},i} + e_m. \tag{4}$$

Finally, the overall energy cost of maneuver M_m from nodes n to i is

$$c_{m,i} = \Sigma_{k=2}^{K} e_{m,j_k}. \tag{5}$$

Denote by E_j the remaining energy available at node j ($j \in \mathcal{N}_o$). We say that maneuver M_m is energy-feasible if and only if

$$e_{m,j_k} \leq E_{j_k} \tag{6}$$

for all k. In other words, the remaining energy of each node on the maneuver path must be larger than the energy consumption of performing this maneuver.

2.4 Maximizing Lifetime of Critical Path

Our objective is to maximize the lifetime of the critical path between the source and the destination in the MANET.

Assume that there are Y nodes on the critical path, and denote indexes of these nodes by x_1, x_2, $\cdots$, x_Y (which take values in the set of indexes of operating nodes $\mathcal{N}_o$), where node x_1 is the source and node x_Y is the destination. Besides maximizing the lifetime of such a critical path between nodes x_1 and x_Y, there also exist many other objectives to achieve. For example,

- All nodes on the path must not be infected;
- The overall capability of the path (i.e., the sum of capabilities of all nodes on the path) should be maximized;
- The overall capability of the network (i.e., the sum of capabilities of all nodes in the network) should be maximized;
- The cost to protect such a path should be minimized.

Unfortunately, all the objectives cannot be met at the same time. For example, if we want to maximize the overall capability, we should always patch all nodes to make them completely secure; on the other hand, if we want to maximize the lifetime, we should not always patch because patching costs energy, and accordingly reduces the lifetime of a node. Therefore, we formulate the problem as an optimization with multiple constraints in the next section.

3. FORMULATION AND ANALYSIS

In this section, we formulate the problem and present our solutions.

3.1 Protecting Critical Path based on Current Network View

We first consider the scenario that the patching node only has the current view of network status (e.g., link throughputs, node states, critical path info), but does not predict the future based on statistical information (e.g., how nodes may be geometrically distributed and statistically infected).

3.1.1 Formulation

At a particular time, when a state change of node q is reported (e.g., node q is infected), the patching node (i.e., node n) will decide whether to maneuver node q.

As shown in Fig. 3, the critical path consists of Y nodes: x_1, x_2, $\cdots$, x_Y; and the maneuver path is from nodes n to q, different from the critical path from nodes x_1 to x_Y.

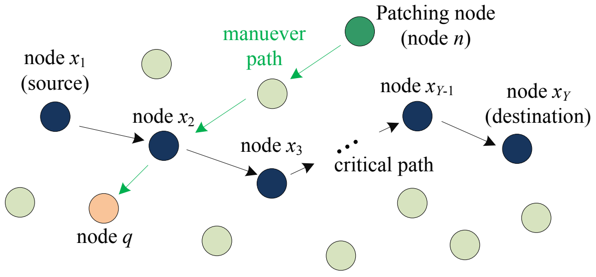

Figure 3: The patching node will decide whether to patch node q in a network with a critical path from nodes x_1 to x_Y.

The primary objective is to maximize the lifetime of this critical path. Since the patching node cannot predict the future, the only factor pertaining to the lifetime of the path is the remaining energy of the node with minimum energy on the path. If the battery of the node dies, the critical path will not exist. In addition, we also need to make sure all nodes on the path are operational and not infected after maneuver; i.e., the state of each node should be in the "good" state space $\mathcal{S}^* = \{\textsf{Immune/Patched}, \textsf{Quarantined}, \textsf{Vulnerable}\}$. Note that state Susceptible should not be allowed after maneuver, because it indicates that a node has been exposed to infected nodes and will soon become infected, thereby compromising the security of the critical path.

Hence, we propose the following optimization problem for the patching node to decide which maneuver it should choose.

$$\begin{aligned}
\underset{\text{choose maneuver } M_m}{\text{maximize:}} \quad & \min\{E_{x_y} - e_{m,x_y}\}_{y\in[1,Y]} && (7)\\
\text{subject to} \quad & s^*_{x_y} \in \mathcal{S}^* \text{for all } y \in [1,Y], && (8)\\
& \Sigma_{y=1}^{Y} C(s^*_{x_y})/Y \geq C^*_{path}, && (9)\\
& \Sigma_{i=2}^{n-1} C(s^*_i)/Y \geq C^*_{network}, && (10)\\
& c_{m,q} \leq c^*, && (11)\\
& M_m \text{ is energy-feasible}, && (12)
\end{aligned}$$

where s^*_i denotes the capability of node i after the maneuver.

The main objective (7) in our optimization approach is to maximize the remaining energy of the node with minimum energy on the critical path such that the lifetime can be maintained as long as possible.

The first constraint (8) is to ensure that after maneuver, the state of each node on the critical path must be in the "good" state space $\mathcal{S}^* = \{\textsf{Immune/Patched}, \textsf{Quarantined}, \textsf{Vulnerable}\}$.

The second constraint (9) is to make sure the average capability of nodes on the critical path is larger than a given threshold C^*_{path}, depending on the requirements of a mission.

The third constraint (10) requires that the average capability of nodes in the network is larger than a given threshold $C^*_{network}$, because the overall network should also be fairly secured in addition to protecting the critical path.

The four constraint (11) is used to limit the cost of a maneuver within an upper bound c^*. In other words, we cannot spend too much energy to maneuver a node.

The last constraint (12) is to ensure that all nodes on the maneuver path have enough energy to perform the maneuver; i.e., (6) holds.

3.1.2 Solution

We only need to choose a maneuver $M_m \in \mathcal{M}$ to solve (7). A solution can be obtained by augmenting from the first constraint to the last constraint, and from the maneuver with the minimum cost (i.e., No Action) to the one with the maximum cost (i.e., Patch or Software Heal).

The solution is illustrated in Algorithm 1. The basic idea of Algorithm 1 is straightforward: we should always attempt to use the maneuver with the minimum cost to maximize the lifetime of the critical path. This indicates that No Action is always preferred if it satisfies the optimization conditions.

3.1.3 Generic Case of Maneuvering Multiple Nodes

The optimization approach in (7) only considers how to maneuver a single node q in the network. It is straightfor-

Algorithm 1 : Optimization based on Current View.

```
Given: Arrange maneuver set $\mathcal{M}$ in the order from maneuvers with lowest cost to highest cost.
repeat
  Get the next maneuver $m$ from $\mathcal{M}$;
  Compute the overall cost $c_{m,q}$;
  if $M_m(S_{x_y}) \notin \mathcal{S}^*$for some $y \in [1, Y]$ then
    continue;
  end if
  if $c_{m,q} > c^*$ or not energy-feasible then
    fail;
  end if
  Compute path capability $C^{est}_{path} = \Sigma^Y_{y=1} C(s^*_{x_y})$;
  Compute network capability $C^{est}_{network} = \Sigma^{n-1}_{i=2} C(s^*_i)$;
  if $C^{est}_{path} \geq C^*_{path}$ and $C^{est}_{network} \geq C^*_{network}$ then
    output the optimal maneuver $m$;
  end if
until All maneuvers are iterated.
```

ward to extend the solution to a generic case in which at a particular time, how can the patching node decide to maneuver a set of nodes $q_1, q_2, \cdots, q_Z$ in the network such that the lifetime of the critical path is maximized with capability and energy guarantees, as shown in Fig. 4.

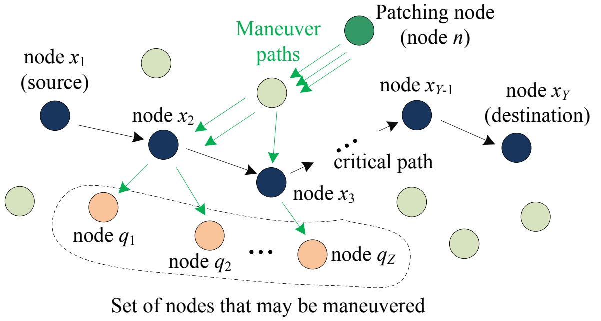

Figure 4: The patching node will decide whether to patch a set of nodes (q_1, q_2, $\cdots$, q_Z) in a network with a critical path from nodes x_1 to x_Y.

We need to modify the main objective (7) and the constraints (11) and (12) in the optimization formulation with single maneuver. In particular, given all nodes q_1, q_2, $\cdots$, q_Z that may need maneuvers, we formulate the problem in the following.

$$\underset{\substack{\text{choose } M_{m_z} \text{ on node } q_z \\ \text{for all } z \in [1, Z]}}{\text{maximize:}} \quad \min\{E_{x_y} - e_{m,x_y}\}_{y \in [1,Y]} \tag{13}$$

$$\text{subject to} \quad s^*_{x_y} \in \mathcal{S}^* \text{for all } y \in [1, Y], \tag{14}$$

$$\Sigma^Y_{y=1} C(s^*_{x_y})/Y \geq C^*_{path}, \tag{15}$$

$$\Sigma^{n-1}_{i=2} C(s^*_i)/Y \geq C^*_{network}, \tag{16}$$

$$\Sigma^Z_{z=1} c_{m,q_z}/Z \leq c^*, \tag{17}$$

$$M_{m_z} \text{ is energy-feasible}, \tag{18}$$

where constraint (17) denotes that the average cost to maneuver a set of nodes should be limited within an upper bound c^*. An augmentation solution similar to Algorithm 1 can be immediately applied to solve (13). That is, a solution can be similarly obtained by augmenting from the maneuver with the minimum cost (i.e., No Action) to the one with the maximum cost (i.e., Patch or Software Heal).

The theoretical indication behind (13) is that we intend to defer cyber maneuver (i.e., choose No Action) as much as possible unless we have to act (when the constraints do not hold), given only the current view of the network without predicting the future. Because we know that we cannot predict the future, satisfying the current and waiting to see the next time is always the best solution to minimize the energy cost and maximize the lifetime of the critical path.

3.2 Protecting Critical Path based on Statistical Information

The solution to (13) is generic for protecting the critical path given only the current view of the network. Essentially, it tends to perverse the energy consumption on the critical path, while maintaining the required security and capability levels. Therefore, such a solution appears to be not proactive, but reactive to protect the critical path.

Given some statistical information in the network, it is in fact feasible to proactively prolong the lifetime of the critical path. In other words, if we can predict how the network behaves statistically in the future, we can have a better cyber maneuver strategy than the previous one.

3.2.1 Formulation

In what follows, we describe the strategy to protect the critical path with statistical information. In MANETs, any network event is always a random event due to node mobility, traffic pattern and randomness of wireless channels. Therefore, a critical path between the source and destination that exists currently does not mean it will exist in the future. Therefore, we denote by A_τ the event that there still exists a critical path between the source and the destination in the network after time duration τ. Then, our objective to maximize the probability that such a critical path still exists, i.e., to maximize $\mathbb{P}(A_\tau)$.

As a result, we can write our solution as

$$\underset{\substack{\text{choose } M_{m_z} \text{ on node } q_z \\ \text{for all } z \in [1, Z]}}{\text{maximize:}} \quad \mathbb{P}(A_\tau) \tag{19}$$

$$\text{subject to} \quad s^*_{x_y} \in \mathcal{S}^* \text{for all } y \in [1, Y], \tag{20}$$

$$\Sigma^Y_{y=1} C(s^*_{x_y})/Y \geq C^*_{path}, \tag{21}$$

$$\Sigma^{n-1}_{i=2} C(s^*_i)/Y \geq C^*_{network}, \tag{22}$$

$$\Sigma^Z_{z=1} c_{m,q_z}/Z \leq c^*, \tag{23}$$

$$M_{m_z} \text{ is energy-feasible}, \tag{24}$$

where constraints (20)–(24) are the same as constraints (14)–(18) in the solution with only current view. The reason is that although we aim to obtain the highest chance of protecting the critical path in the future, we have to make sure that the current critical path is still protected and operational. Accordingly, we have the same constraints to meet the requirements of security and costs for the current time.

3.2.2 Approximate Solution

The analytical modeling related to $\mathbb{P}(A_\tau)$ in the context of wireless networks with random mobility has been widely investigated in the literature (e.g., [15–17]). In particular, a wireless network with a random node distribution can be modeled as a random geometric graph, and $\mathbb{P}(A_\tau)$ is a function of node density, mobility model, and network size. In general, it is mathematically intractable to find the analytical solution to $\mathbb{P}(A_\tau)$. However, it has been shown to be increasingly proportional to the node density (which is defined as the number of nodes divided by the network area) [17–19]. Thus, maximizing $\mathbb{P}(A_\tau)$ is equivalent to maximizing the "future" node density (after time duration τ). In our scenario, the node density is equivalent to the average number of "good" nodes that can still participate in routing to form a critical path between the source and the destination divided by the network area. As the network area is always fixed, maximizing $\mathbb{P}(A_\tau)$ is equivalent to maximizing the average number of "good" nodes in the network after time duration τ.

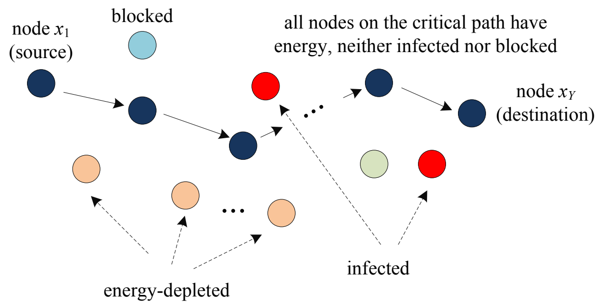
node x_1
(source)
blocked
all nodes on the critical path have
energy, neither infected nor blocked
node x_Y
(destination)
energy-depleted
infected

Figure 5: After time duration τ, all nodes on the critical path must have still energy, at the same time neither infected nor blocked.

It is important to note that a "good" node is one that (i) is neither infected, (ii) nor blocked, and (iii) still has remaining energy to operate. As shown in Fig. 5, the three conditions guarantee that a "good" node can be involved in secure routing to form a critical path. Thus, in the following, we aim at finding out the average number of "good" nodes in the network after time duration τ. To this end, we need to use the some statistical information to predict such a number. In particular, we use the following information that is generally considered known or predictable for some MANET scenarios in the literature.

- Energy depletion model. Energy usage is generally determined by traffic patterns in wireless networks. Therefore, it has been shown possible to build an energy depletion model in existing studies (e.g., [20–22]). For node j, we model its probability of energy depletion after time duration τ as a function $p_d(E_j, \tau)$, where E_j is the current remaining energy. In addition, $p_d(E_j, \tau)$ is a decreasing function of E_j and increasing function of τ, satisfying
$$\lim_{E_j \to 0} p_d(E_j, \tau) = 1, \text{and} \lim_{\tau \to \infty} p_d(E_j, \tau) = 1.$$
If we randomly choose a node from all nodes in the network, the probability that it is energy-depleted after time duration τ can be denoted as
$$p_{\text{depleted}} = \sum_{j \in \mathcal{N}_o} p_d(E_j, \tau)/|\mathcal{N}_o|. \tag{25}$$

- Infection propagation model. In a network scenario where an adversary wants to infect other mobile nodes, the average infection propagation speed has been shown at most linearly increasing over time [23]. This result enables us to approximate the average number of nodes that have been infected in the network as a quadratic function of time τ, i.e., $n_m(1 + \beta\tau^2)$, where n_m is the number of node that still remain infected after current maneuver, and β is a constant infection factor. Thus, if there are currently n_m infected nodes in the network, after time duration τ, the probability of a node being infected in the network is approximated as
$$p_{\text{infected}} \approx \max\left(1, n_m(1 + \beta\tau^2)/n\right). \tag{26}$$

With the two statistical models, we can derive the average number of "good" nodes in the network after time duration τ. Specifically, the probability p_{good} for a node being "good" is the probability that it is (i) not infected, and (ii) not blocked, and (iii) not energy-depleted. The probability of a node being blocked can be written as
$$p_{\text{blocked}} = n_b/|\mathcal{N}_o|, \tag{27}$$
where n_b is the number of nodes whose state is blocked after current maneuver. Given (25), (26), and (27), we obtain
$$\begin{aligned} p_{\text{good}} &= (1 - p_{\text{infected}})(1 - p_{\text{blocked}})(1 - p_{\text{depleted}}) \\ &\approx \min\left(0, 1 - \frac{n_m(1 + \beta\tau^2)}{n}\right)\left(1 - \frac{n_b}{|\mathcal{N}_o|}\right) \\ &\quad \left(1 - \frac{\sum_{j \in \mathcal{N}_o} p_d(E_j, \tau)}{|\mathcal{N}_o|}\right). \end{aligned} \tag{28}$$

Finally, the original maximization objective (19) can be approximated as
$$\underset{\substack{\text{choose } M_{m_z} \text{ on node } q_z \\ \text{for all } z \in [1, Z]}}{\text{maximize:}} \qquad p_{\text{good}}|\mathcal{N}_o|, \tag{29}$$
where p_{good} is given in (28), $\mathcal{N}_o$ is the set of indexes of all operating nodes, i.e., $\{2, 3, \cdots, n-1\}$ as aforementioned, and $|\mathcal{N}_o| = n - 2$ is the number of operating nodes in the network.

Combining objective (29) and constraints (20)–(24) yields the final solution to find the best cyber maneuver with statistical information. It is worth mentioning that the best maneuver is found by iterating over all possible maneuver space to maximize (29). This indicates that given sufficient information, it is feasible to find the best proactive strategy to maintain a critical path between the source and destination. Compared with the previous case in which we should defer proactive strategies with only the information of the current view of the network, statistical information provides us the opportunity to be proactive; i.e., we should be proactive as long as the maximization objective in (19) is achieved, which will be further validated in simulations in the Section 4.

4. SIMULATION RESULTS

In this section, we use numerical simulations to validate the effectiveness of our solutions.

4.1 Setups

We set up a MANET with the following configurations.

- Network size. The network is on a 1000-meter by 1000-meter region.
- Node setups. Each node has a transmission range of 100 meters, and is uniformly distributed on the network with independent mobility.

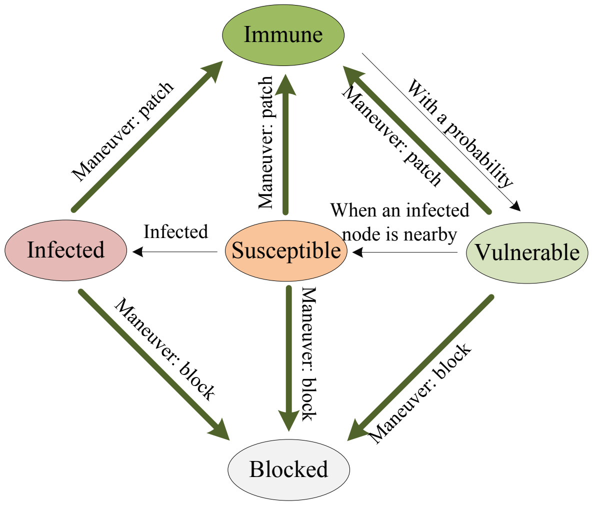

Figure 6: The state and maneuver space with transitions used in simulations.

- Energy mode. The energy consumption of each node is a linear function of the number of traffic transmissions of each node.
- Critical path. We randomly choose two nodes as the source and the destination, and protect the critical path between them. The critical path is chosen to be the shortest path on which forwarding nodes are not infected, blocked, nor energy-depleted.
- Attack and defense. There exists an adversary in the network that attempts to infect other nodes as long as they meet. There also exists a patching node aiming to make the best decision to maneuver other nodes in the network in order to maximize the lifetime of the critical path between the source and the destination.
- Measure of time. The time is slotted in the network, and wireless transmissions happen at the beginning of each time slot. The simulation starts at slot 0, and all nodes are initially in the Vulnerable state.

In addition, the node state space and cyber maneuvers with state transitions used in simulations are illustrated in Fig. 6. As Fig. 6 shows, we consider the scenario in which a node is immune when it is patched, but it can become vulnerable again in the next time slot with a probability because of some new vulnerability and the adversary's new strategy. A vulnerable node will become susceptible when it is exposed to an infected node, will then become infected in the next time slot unless a patch is applied. We also considered three maneuvers in simulations: No Action, Patch, Node Block as shown in Fig. 6.

The values of node capability are specified in Table 1. The threshold of C^*_{path} is set to be 2.5, which means that the average capability of nodes on the critical path must be greater than 2.5 in the network.

4.2 Protecting Critical Path based on Current View

We first evaluate the performance of the optimal strategy for cyber maneuvers based only on the current view of the network. Fig. 7 shows the average capability of nodes on the critical path over time. As all nodes start with the state of Vulerable, we observe in Fig. 7 that the average capability is 2 at time 0, and starts to drastically increase. This is because the capability threshold is 2.5 and accordingly maneuvers have to be performed on some nodes on the critical path to make sure the average capability is greater than 2.5. As time goes, more nodes are infected or become susceptible, cyber maneuvers will be triggered if the average capability shows the tendency to go below the threshold 2.5.

Table 1: Capability values used in simulations.

Immune:	4
Vulnerable:	2
Susceptible:	1
Infected:	0
Blocked:	0

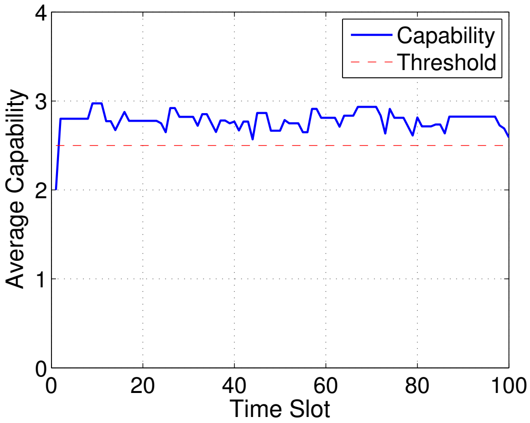

Figure 7: The average capability of nodes on the critical path over time with the optimal strategy based only on current view of network status.

One important observation that we obtain from Fig. 7 is that the average capability almost always remains right above the threshold. In addition, there are many maneuvers performed over time (each increase of the average capability in Fig. 7 means a maneuver is performed). Intuitively, the reason is that given current view, the strategy is to always defer a maneuver unless we have to; and even when we perform a maneuver, we always perform the maneuver with minimum energy cost, which results in a minimum number of nodes being patched. This means that more and more nodes will be infected over time while the minimum number of nodes are in fact patched. As time goes, the infection speed is eventually larger than the patching speed. Therefore, the impact of infected nodes becomes overwhelming, and cyber maneuvers have to be frequently performed.

4.3 Protecting Critical Path based on Statistical Information

We then evaluate the performance of the optimal strategy for cyber maneuvers based on statistical information of the network. Similar to Fig. 7, Fig. 8 depicts the average capa-

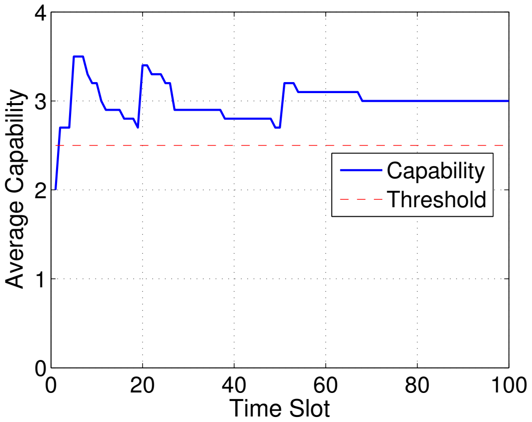

Figure 8: The average capability of nodes on the critical path over time with the optimal strategy based on statistical information of the network.

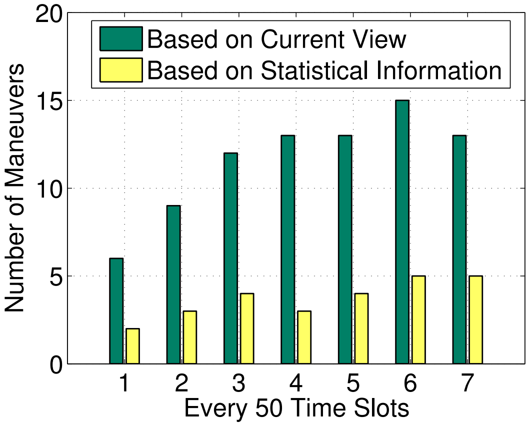

Figure 9: Comparisons of the numbers of cyber maneuvers based on current view and statistical information in every 50 time slots after the network starts at time 0.

bility of nodes on the critical path over time. It is noted in Fig. 8 that the average capability is 2 at time 0, and starts to drastically increase, then is further boosted to a higher value of capability. In addition, there are fewer cyber maneuvers than those in Fig. 7. This is because given statistical information, we are able to choose the best strategy that could also benefit the future. Such a strategy will not lead to the overwhelming effect of the infection speed greater than the patching speed in the previous case. The best maneuver based on statistical information may cost more energy from the perspective of the current view, but it shows the optimality in a long run.

4.4 Comparisons between Results of Current View and Statistical Information

We compare the two strategies based on current view and statistical information in Figs. 9 and 10.

Fig. 9 compares the numbers of cyber maneuvers between current view and statistical information in every 50 time slots after the network starts at time 0. It is evident to see that the strategy based on statistical information leads to much fewer cyber maneuvers than that based on current view. Fig. 10 compares the lifetimes of the critical path between current view and statistical information. It is observed from Fig. 10 that the statistical-information lifetime is substantially greater than the current-view lifetime.

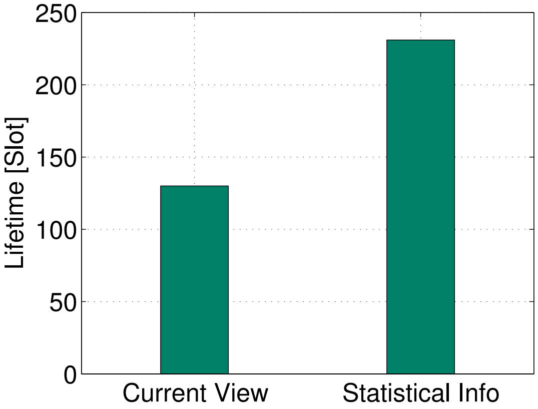

Figure 10: Comparisons of the lifetimes of the critical path between two nodes based on current view and statistical information. The critical path will not exist when we cannot find nodes with sufficient capability and energy to form such a path in the network.

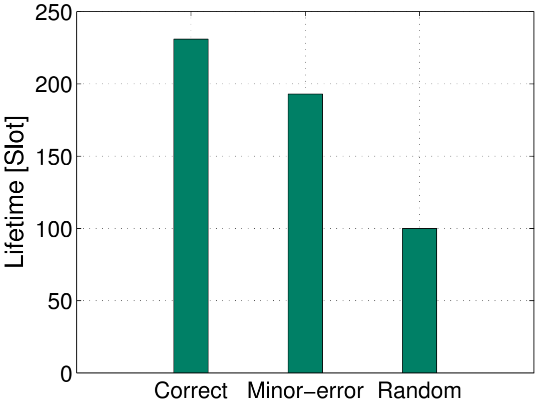

Figure 11: Comparisons of the lifetimes of the critical path based on (i) completely correct statistical information, (ii) information with minor (10%) error and (iii) randomly wrong information.

We can conclude from Figs. 9 and 10 that if we are aware of the statistical information in the network, we can be proactive and use the optimal strategy for cyber maneuvers, which leads to substantial improvement over the current-view performance.

Note that the statistical information in the network may not be always available or may even have errors. To show how such information mismatch affects the performance, we evaluate in Fig. 11 the performance of proactive strategies based on three different types of information: (i) completely correct statistical information, (ii) information with minor (10%) error, and (iii) randomly wrong information.

It is observed from Fig. 11 that information with minor error and randomly wrong information will both lead to shorter lifetime because of inappropriate patching and energy wasting. In particular, in the randomly wrong case, the lifetime is even shorter than the current-view case as shown in Fig. 10. Thus, it is also concluded that correct statistical information is the key to the effectiveness of proactive cyber maneuvers.

5. CONCLUSIONS

In this paper, we provided the first study on modeling and evaluating the effectiveness of proactive cyber maneuvers to protect the critical path in MANETs. We proposed a generic framework to analytically model cyber maneuvers and define their associated utilities. We developed the optimal solution to maximize the lifetime of the critical path with security assurance. We found that sufficient statistical information in the network is vital for the network defender to be proactive, choose the best cyber maneuvers to protect the critical path, and outperform conventional reactive strategies.

Our future work includes more systematic organizations of node states, cyber maneuvers, and maneuvers-induced state transitions, as well as discussion of more optimization objectives.

Acknowledgement

The research in this paper is supported by NSF CNS-1464114. The views and conclusions contained in this paper are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on.

6. REFERENCES

[1] P. Beraud, A. Cruz, S. Hassell, and S. Meadows, "Using cyber maneuver to improve network resiliency," in *Proc. of MILCOM*, 2011, pp. 1121–1126.

[2] S. Jajodia, A. K. Ghosh, V. Subrahmanian, V. Swarup, C. Wang, and X. S. Wang, *Moving Target Defense II.* Springer, 2013.

[3] D. Torrieri, "Cyber maneuvers and maneuver keys," in *Proc. of MILCOM.* IEEE, 2014, pp. 262–267.

[4] Z. Lu, C. Wang, and M. Wei, "On detection and concealment of critical roles in tactical wireless networks," in *Proc. of MILCOM*, Oct. 2015.

[5] Z. Lu and C. Wang, "Network anti-inference: A fundamental perspective on proactive strategies to counter flow inference," in *Proc. of IEEE INFOCOM*, Apr. 2015.

[6] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "Spatiotemporal address mutation for proactive cyber agility against sophisticated attackers," in *Proc. of ACM MTD*, Nov. 2015.

[7] P. Beraud, A. Cruz, S. Hassell, J. Sandoval, and J. J. Wiley, "Cyber defense network maneuver commander," in *Proc. of IEEE ICCST*, 2010, pp. 112–120.

[8] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, *Mobile ad hoc networking.* John Wiley & Sons, 2004.

[9] S. Singh, M. Woo, and C. S. Raghavendra, "Power-aware routing in mobile ad hoc networks," in *Proceedings of ACM MobiCom*, 1998, pp. 181–190.

[10] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security.* Springer, 2007, pp. 103–135.

[11] X. Cheng, M. Cardei, J. Sun, X. Cheng, L. Wang, Y. Xu, and D.-Z. Du, "Topology control of ad hoc wireless networks for energy efficiency," *IEEE Transactions on Computers*, vol. 53, no. 12, pp. 1629–1635, 2004.

[12] M. Khouzani, S. Sarkar, and E. Altman, "Maximum damage malware attack in mobile wireless networks," *IEEE/ACM Transactions on Networking*, vol. 20, no. 5, pp. 1347–1360, 2012.

[13] M. Khouzani, S. Sarkar, and E. Altman, "Dispatch then stop: Optimal dissemination of security patches in mobile wireless networks," in *Proc. of IEEE CDC*, 2010, pp. 2354–2359.

[14] M. Khouzani, S. Sarkar, and E. Altman, "Optimal control of epidemic evolution," in *Proc. of IEEE INFOCOM*, 2011, pp. 1683–1691.

[15] A. E. Gamal, J. Mammen, B. Prabhakar, and D. Shah, "Throughput-delay trade-off in wireless networks," in *Proc. of IEEE INFOCOM*, vol. 1, 2004.

[16] R. Groenevelt, P. Nain, and G. Koole, "The message delay in mobile ad hoc networks," *Performance Evaluation*, vol. 62, no. 1, pp. 210–228, 2005.

[17] L. Sun and W. Wang, "On distribution and limits of information dissemination latency and speed in mobile cognitive radio networks," in *Proc. of IEEE INFOCOM*, 2011, pp. 246–250.

[18] M. Franceschetti, O. Dousse, D. N. Tse, and P. Thira, "Closing the gap in the capacity of wireless networks via percolation theory," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 1009–1018, 2007.

[19] I. Glauche, W. Krause, R. Sollacher, and M. Greiner, "Continuum percolation of wireless ad hoc communication networks," *Physica A: Statistical Mechanics and its Applications*, vol. 325, no. 3, pp. 577–600, 2003.

[20] W. R. Heinzelman, A. Sinha, A. Wang, and A. P. Chandrakasan, "Energy-scalable algorithms and protocols for wireless microsensor networks," in *Proc. of IEEE ICASSP*, vol. 6, 2000, pp. 3722–3725.

[21] X. Wu, G. Chen, and S. K. Das, "On the energy hole problem of nonuniform node distribution in wireless sensor networks," in *Proc. of IEEE MASS*, 2006, pp. 180–187.

[22] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey," *Ad hoc networks*, vol. 7, no. 3, pp. 537–568, 2009.

[23] Z. Lu, W. Wang, and C. Wang, "How can botnets cause storms? understanding the evolution and impact of mobile botnets," in *Proc. of IEEE INFOCOM*, Apr. - May 2014.