Mobility-Enabled Topology Control and Routing to Defend MANETs based on Game Theoretic Analysis

Yangming Zhao\(^1,2\), Chunming Qiao\(^2\), Xun Xiao\(^3\), Sheng Zhong\(^4\), Jianping Wang\(^5\), Sheng Wang\(^1\), Shizhong Xu\(^1\)

\(^1\)Key Lab of Optical Fiber Sensing and Communication, Education Ministry of China
University of Electronic Science and Technology of China, Chengdu, P. R. China, 611731
\(^2\)Department of Computer Science and Engineering, SUNY Buffalo, NY, USA, 14260-2500
\(^3\)Centre of System Biology in Max Planck Institute for Molecular Cell Biology and Genetics, D03107 Dresden, Germany
\(^4\)State Key Laboratory for Novel Software, Nanjing University, Nanjing, China, 210046
\(^5\)Department of Computer Science, City University of Hong Kong, Kowloon, Hong Kong SAR

Abstract—This paper aims at enhancing MANET security by leveraging the ability to control the topology, routing and nodal mobility in MANETs. We first model the interaction between an attacker and a defender as a two-player variable-sum game. From the attacker’s point of view, we determine which nodes are worth attacking. By further analyzing the Nash equilibrium solution of the game, we provide useful guidelines to the defender, and design an algorithm to control the topology (enabled by mobility) and routing. Simulation results not only demonstrate that our algorithm can reduce the defender’s payoff loss at a Nash equilibrium, but also show that nodal mobility can bring additional security benefit to the defender.

Index Terms—MANET security; topology control and routing; nodal mobility

I. INTRODUCTION

Mobile ad hoc networks (MANETs) play a vital role in many environments, e.g. in collaborative and distributed computing, disaster recovery, crowd control, and search-and-rescue [1]. Since MANETs work in an open and distributed scenario, they are vulnerable to attacks, such as signal jamming attacks in the physical layer [2], cryptography attacks in the link layer [3], routing attacks and packet forwarding attacks in the network layer [4]. Accordingly, security is an important issue in MANETs. Although security has long been a hot topic in wire-line and wireless networks, these technologies cannot be used in MANETs directly due to their unique characteristics, including an open network architecture which is easier for other nodes to join, the shared wireless medium and their highly dynamic network topology. While an attacker can take advantage of some of these characteristics such as the open network architecture and shared wireless medium, the defender can also take advantage of the ability to control topology and routing, enabled by their wireless medium and nodal mobility in MANETs. This paper aims at providing an insight into how to leverage these characteristics in order to defend attack in MANETs.

Usually, a MANET refers to a multi-hop wireless network formed by a set of mobile nodes. All the nodes in a MANET can communicate directly with some nodes in its range, and with other nodes through forwarding. Sometimes, each of the nodes is purely autonomous and there is no centralized administrator [5-7]. There are also situations where all the nodes in a MANET belong to the same authority and together they pursue the same purpose, such as in rescue operations and military situations. In this paper, we mainly focus on the latter case but our results also provide insight into the former case in terms of which nodes should pay more attention to defend possible attacks and which nodes may not care much about the attacks.

There have been many studies on security issues in MANETs. Some of them proposed concrete schemes to enhance MANET security, such as setting up protection nodes to mitigate the distributed denial-of-service (DDoS) attack [8], designing a smart cryptograph system [9] and modifying existing routing protocols [10], while others focused on analyzing the action of attackers to provide insight to the defender in terms of how to detect attacks [11]. The common shortcoming of these studies is that all of them focused on some specific attacking methods or defending schemes, which have only a limited applicability in practice. More specifically, in realistic situations, there may be interactions between the attacker and the defender. Accordingly, even the most effective defending scheme to counter a specific attack may be exploited by an adaptive attacker. Therefore, modeling and analyzing the interaction between the attacker and defender is necessary to not only guide the MANETs operator at the beginning when a MANET is deployed, but also to provide valuable insights to the operator in terms of how to keep their network safe during its lifetime.

Game theory is a good tool to model the interaction between a sophisticated and rational attacker and a defender. If both the attacker and defender are rational, they should take actions that will bring most benefit to them. When neither attacker nor defender can obtain more benefit by unilaterally changing its strategy, we say the game between the attacker and the defender has reached equilibrium (or a stable state). When we model the interaction between the attacker and defender as a game and solve the equilibrium, the defender can provision its defending resources according to the equilibrium.

Game theory has been widely used to enhance the network security. For example, Xiao et al. [12] and Chen et al. [13] used game theory to analyze the defending resource allocation problem in the network, which are the most related work to this study. Nonetheless, neither of them modeled the situation in MANETs. As a result, one major difference from the previous works is that here, the cost incurred by the defender when a link/node is attacked is no longer constant and, in fact, can be
dynamically changed by the defender. More importantly, previous studies have focused on the analysis of the game, but not on how to utilize the analysis to design topology control and routing algorithms to benefit the defender. In this paper, we not only leverage the configurable topology and routing in MANETs, but also utilize the nodal mobility to enhance the security of MANETs.

The main contributions of our work can be summarized as follows:

- We formulate the interaction between attacker and defender as a two-player variable-sum game. Our analysis shows that not all the nodes are worth attacking, and accordingly, we also determine which nodes should be defended.
- Based on the analysis, we solve the Nash equilibrium of the game and hence yield the payoff of the attacker and defender at the Nash equilibrium.
- We further analyze the solution of the game, and provide three guidelines on how to control the topology and routing in a MANET to reduce the defender’s loss. Although these guidelines are not rigorously proven as theorems, they are backed by solid analysis, rather than simple intuitions.
- We also present an effective topology control and routing algorithm by following the guidelines.
- Simulation results show that our method will enhance the defender’s payoff at equilibrium, and nodal mobility will also bring additional security benefit to the defender.

The rest of the paper is organized as follows. Section II briefly describes the related work and Section III formulates the interaction between the attacker and the defender as a two-player non-zero sum game. In Section IV, we analyze the game and determine which nodes are worth attacking (and defending), and solve the Nash equilibrium of the game. We further analyze the solution of the game to provide guidelines on how to control topology and routing in MANETs, and propose a corresponding algorithm to do so in Section V. Simulation results are presented in Section VI and we conclude this paper in Section VII.

II. RELATED WORK

Many existing studies on MANET security have focused on designing specific schemes or countering specific attacks. Mingda et al. [8] took advantage of the high redundancy in MANETs and chose protection node to share the malicious traffic. Eissa et al. [9] designed a cryptograph system to protect MANETs and chose protection node to share the malicious traffic. Mingda et al. [8] took advantage of the high redundancy in designing specific schemes or countering specific attacks.

Game theory is a good framework to obtain a more general result than only designing a specific scheme or protocol. This is not only because the interaction between an attacker and defender can be explicitly modeled as a game model but also, since the payoff function can be defined, this method allows us to adapt to different scenarios without changing the fundamental analysis. The work in [11] used a game model to study how to allocate defending resources in a network to counter malicious attacks. Xiao et al. [12] and Chen et al. [13] did some similar works, which are most related to this study. Though both Xiao et al. and Chen et al. modeled the interaction between defender and attacker as a 2-player game, Xiao et al. assumed players would attack/defend links to minimize/maximize the maximal network flow, while Chen et al. used a variable-sum game to model the scenario that players focus on the nodes in the networks. Though these existing results can be applied to MANETs, they do not take advantage of the nodal mobility which is the unique property of MANETs and may bring additional security benefit to the defender.

There are also previous studies, such as [14-19], on the topology control and routing in ad hoc networks. Some of them studied how to improve the QoS in the network [15, 16] or how to save energy in the network [14, 17], while some others studied how to deal with the dynamic topology in MANETs, e.g. to design a safety routing protocol [18] or design dynamic topology to guarantee the network survivability [19].

In short, no work exists on controlling topology and routing in MANETs to enhance network security based on a game theoretic analysis of the interaction between the defender and attacker. To the best of our knowledge, we are among the first to defend malicious attacks by jointly optimizing network topology (enabled by mobility) and routing in MANETs.

III. PROBLEM FORMULATION

A. Network Model

In this paper, we consider a MANET with N-1 mobile nodes. For each node i, it can select at most K nodes among its neighbor set, denoted by N_i, to set up direct connections, i.e. links in the network. N_i is determined by the communication radius of each node and K is determined by the available spectrum, i.e. how many channels can be set up simultaneously by each node. Every two nodes can communicate with each other through a direct connection or via some intermediate nodes.

Hereafter, we refer to traffic or information flows between the nodes in MANETs as "demands". If there exists a traffic demand between node i and node j, we use an importance value v_{ij} to represent the amount of the traffic, information importance and so on. Without ambiguity, we also use v_{ij} to denote the demand from node i to node j. When all the demand routes are fixed, the total value at node u is the sum of the values of all the demands originating from, passing through, or terminating at the node, and can be calculated by

$$W_u = \sum_{i,j \in P(i,j)} v_{ij}$$  \hspace{1cm} (1)

where P(i,j) is the set of nodes on the route of v_{ij}. We say W_u is the value of node u.

In our work, we assume that an attacker can choose one (and only one) node as its target. If the attack is successful, it will obtain all the values associated with the demands traversing this node. Conversely, the defender will lose those values. When the defender realizes that attacks may occur in the MANET, it will allocate defending resources to prevent such
loss. If the attacker chooses node \( u \) as its target and node \( u \) is exactly the node protected by the defender (which presumably provides sufficient protection), the gain of the attacker will be zero. Note that our work here can be easily extended to the cases where each link, instead of a node, is attacked, and where the attacker will be penalized (instead of having a zero gain) when attacking a protected node, for example.

We further assume that costs of attacking and defending a node are proportional to the value of that node. The proportions are \( C_a \) and \( C_d \) for the attacker and the defender, respectively. In our work, we assume \( C_a << 1 \) and \( C_d << 1 \). Otherwise, an attacker may have no incentive to choose a target, nor the defender has any incentive to protect its nodes.

Take the MANET in Fig. 1 as an example. There are 5 nodes and 3 demands in the network. In this MANET, the value of node 1, \( W_1 \), can be calculated as \( v_{12} + v_{15} \) and \( W_5 \) is \( v_{15} + v_{34} \). If the attacker selects node \( i \) as its target, the attack cost would be \( C_a W_i \) and it will get payoff \( W_i \) if node \( i \) is not protected. Accordingly, if node \( i \) is protected, the attacker will have a payoff loss of \( C_a W_i \), and otherwise, it will have a payoff gain of \( W_i - C_a W_i \). On the other hand, the defender can protect node \( i \) at cost \( C_d W_i \) and will have a payoff loss of \( C_d W_i \) whether the node is attacked or not, but if the defender chooses not to defend node \( i \), it will result in a payoff loss of \( W_i \). Table 1 shows the payoff matrix of the (attacker, defender) interaction at node \( i \).

Our problem is how to control the network topology, i.e. set up links in the network, and route demands to protect the MANETs so as to minimize the defender's loss or maximize its payoff. It is worth noting that, although the payoff matrix in Table 1 is a specific case, our game-theoretic analysis and general guidelines and conclusions are suitable to all other payoff matrices.

**B. Game Model**

Based on the network model discussed in the previous subsection, assume that the attacker chooses node \( i \) as its target with probability \( a_i \) and the defender puts its defending resource on node \( i \) with probability \( d_i \), the utility of attacker \( U_A \) and defender \( U_D \) can be calculated as

\[
U_A = \sum_i [d_i \cdot (-C_a W_i) + a_i \cdot (1 - d_i)(W_i - C_a W_i)]
\]

\[
= \sum_i a_i W_i (1 - C_a - d_i)
\]

and

<table>
<thead>
<tr>
<th>Attack</th>
<th>Not Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>( -C_a W_i )</td>
<td>( W_i - C_a W_i )</td>
</tr>
<tr>
<td>( W_i )</td>
<td>( -C_a W_i )</td>
</tr>
</tbody>
</table>

\[
U_D = \sum_i [a_i \cdot d_i \cdot (-C_a W_i) - a_i \cdot (1 - d_i)W_i ] - (1 - a_i) \cdot d_i \cdot C_a W_i
\]

\[
= \sum_i d_i \cdot (a_i - C_a) W_i - \sum_i a_i W_i
\]

It is worth noting that to deal with the case that the defender/attacker may have some probability not to defend/attack, we add a virtual node with value 0 in the network. Also, we use \( T \) to denote the set of all nodes (including real and virtual nodes) in the network. Therefore, when the attacker and the defender attack/defend the targeted MANET, their interactions can be formulated as a two-player variable-sum game, \( G_{M} \), as follows:

- **Player:** Attacker, Defender
- **Strategy space:**
  - Attacker: \( S_a = \{ a : a \in [0, 1], \sum a_i = 1 \} \)
  - Defender: \( S_d = \{ d : d \in [0, 1], \sum d_i = 1 \} \)
- **Payoff:** \( U_A \) for the attacker and \( U_D \) for the defender

**C. Discussion**

The game model we formulated in the last subsection can be applied to not only MANETs as in this paper, but also to any other communication networks once the value of each node is fixed. Accordingly, our work also provides some insight into the security issue of other communication networks. But in MANETs, since the topology and the demand routing can be dynamically controlled, these features can be utilized to further enhance network security. For example we can change the value of a node by varying its connections to the neighboring nodes and the demands passing it, so as to reduce the total payoff loss for the defender. Furthermore, nodal mobility is another unique feather of MANETs and it provides more flexibility in controlling the network topology than power control. Therefore, unique features in MANETs may bring more security benefit to the defender. In Section V, we will analyze how to utilize these features in MANETs to counter malicious attacks.

In the following discussion, we will first assume that the attacker has symmetric information as the defender e.g. the complete MANET topology and demand routing. This is to provide the worst case performance analysis from defender’s point of view. We can expect, which is also verified through simulation, that when the attacker has less knowledge about the MANETs, the defender will have less payoff losses than that in the worst case.

**IV. EQUILIBRIUM ANALYSIS**

In this section, we will solve the game \( G_{M} \) defined in the previous section by investigating its Nash Equilibrium. Intuitively, not all the nodes in the network are worth attacking, e.g. a node whose value is less than the attacking cost.
Accordingly, we first answer the following question: whether all the nodes in a MANET have the potential to be a target of the attacker? If not, which nodes have the potential to be attacked? Based on such analysis, we solve the game without further considering the nodes that are not worth attacking.

V. EQUILIBRIUM ANALYSIS

In this section, we will solve the game $G_M$ defined in the previous section by investigating its Nash Equilibrium. Intuitively, not all the nodes in the network are worth attacking, e.g. the node value is less that the attacking cost. Accordingly, we first answer the question in subsection IV.A that whether all the nodes in MANET have the potential to be a target of the attacker? If not, which nodes have the potential to be attacked? Based on this analysis, we solve the game without considering the nodes that are not worth attacking in subsection IV.B.

A. Vulnerable Set Analysis

**Definition 1**: Vulnerable set: A set of nodes, denoted by $T_v$, which will be selected as the target by the attacker with a positive probability at some Nash equilibrium.

By the above definition, for the nodes out of the vulnerable set, the attacker will not select them as targets. Next we will study which nodes will be in $T_v$ by the following theorems.

**Theorem 1**: Any nodes whose value is less than

$$W_{\text{Threshold}} = \frac{|T_v|(1-C_a) - 1}{(1-C_a)\sum_{i\in T_v} W_i}$$

(where $|T_v|$ denotes the total number of nodes in $T_v$), is not in $T_v$.

**Proof**:

We prove this theorem by contradiction. Assume that the value of a node $k$ is less than $W_{\text{Threshold}}$ but be selected as the attacker’s target with probability $a_{k} > 0$.

Assume that there is a vulnerable set $T_v$ containing all the nodes with value larger than $W_{\text{Threshold}}$ and consider the strategy for the defender

$$d'_k = 1 - C_a - \frac{|T_v|(1-C_a) - 1}{W\sum_{i\in T_v} W_i}$$

which satisfies

$$d'_k \geq 0 \text{ and } \sum_{k=1}^{n} d'_k = 1$$

If the defender’s strategy is $\{d'_k\}_{k=1}^n$, there must be some node $m$ such that $d'_m \leq d'_a$. Then, we can construct a new strategy for attacker

$$a'_i = \begin{cases} a_m + a_k, i = m \\ 0, i = k \\ a_i, \text{ otherwise} \end{cases}$$

Now, the payoff difference associated with the two strategies will be

$$\sum_{i\in T} a'_i W_i(1-C_a - d'_i) - \sum_{i\in T} a_i W_i(1-C_a - d_i)$$

$$= a_i W_i'(1-C_a - d_i) - a'_i W_i'(1-C_a - d'_a)$$

$$\leq a_i W_i'(1-C_a - d_i) - a'_i W_i'(1-C_a - d'_a)$$

$$\leq a_i W_i'(1-C_a - d_i) - a'_i W_i'(1-C_a - d'_a)$$

$$\leq a_i W_i'(1-C_a - d_i) - a'_i W_i'(1-C_a - d'_a)$$

$$\leq 0$$

where the first inequality is due to $d'_m \leq d'_a$, the second is because $1-C_a - d_i < 1$, and the last one is the assumption at the beginning of the proof. All the inequalities are tight if and only if $a_k = 0$. Therefore, this contradicts our assumption and all the nodes with value less than $W_{\text{Threshold}}$ will not be selected in $T_v$.

In addition to Theorem 1, we also want to ask whether all the nodes whose value is larger than $W_{\text{Threshold}}$ will be selected as the attacker’s target with positive probability. This question is answered by Theorem 2. Before introducing Theorem 2, we first give out 2 lemmas which will be used to prove Theorem 2.

**Lemma 1**: Assume $W_i \geq W_j \geq \cdots \geq W_k$ and

$$W_i \geq \frac{k(1-C_a) - 1}{(1-C_a)\sum_{i=1}^{k} \frac{1}{W_i}}$$

for $i = 1, \cdots, n$, then

$$\frac{(k+1)(1-C_a) - 1}{(1-C_a)\sum_{i=1}^{k+1} \frac{1}{W_i}} \geq \frac{k(1-C_a) - 1}{(1-C_a)\sum_{i=1}^{k} \frac{1}{W_i}}$$

for $k = 1, \cdots, n-1$

**Proof**:

To simplify the representation, let

$$X = \sum_{i=1}^{k} \frac{1}{W_i} \text{ and } Y = k(1-C_a)$$

Then,

$$\frac{(k+1)(1-C_a) - 1}{(1-C_a)\sum_{i=1}^{k+1} \frac{1}{W_i}} = \frac{\frac{1}{X} + \sum_{i=1}^{k} \frac{1}{W_i}}{X + \frac{1}{W_{k+1}}}$$

$$= \frac{Y - C_a - Y - 1}{X + \frac{1}{W_{k+1}}} = \frac{X}{X(W_{k+1} + 1)}$$

Consider

$$XW_{k+1}(1-C_a) + Y - 1$$

$$= (1-C_a)W_{k+1} \sum_{i=1}^{k+1} \frac{1}{W_i} - Y + 1 - (1-C_a)$$

From

$$W_i \geq \frac{(k+1)(1-C_a) - 1}{(1-C_a)\sum_{i=1}^{k+1} \frac{1}{W_i}}$$

We know,
Therefore,

\[(5) \geq (k+1)(1-C_a) - 1 - Y + C_a = 0\]

In other words,

\[
\frac{(k+1)(1-C_a) - 1 - k(1-C_a) - 1}{(1-C_a)\sum_{i=1}^{k+1} \frac{1}{W_i}} \geq 0
\]

**Lemma 2:** Assume \(W_i \geq W_2 \geq \cdots \geq W_n\) if \(W_{k+1} \geq \frac{k(1-C_a) - 1}{(1-C_a)\sum_{i=1}^{k+1} \frac{1}{W_i}}\) then

\[
W_{k+1} \geq W_i
\]

**Proof:**

This lemma clearly holds since

\[
W_{k+1} \geq \frac{(k+1)(1-C_a) - 1}{(1-C_a)\sum_{i=1}^{k+1} \frac{1}{W_i}} \geq \frac{k(1-C_a) - 1}{(1-C_a)\sum_{i=1}^{k+1} \frac{1}{W_i}}
\]

**Theorem 2:** All the nodes with value larger than \(W_{\text{Threshold}}\) will be selected into \(T_i\).

**Proof:**

It is obvious that if attacker does not attack a node with value \(W\), it will not select a node with value less than \(W\) as its target. Otherwise, the attack can easily put all the probability on attacking node with less value to the node with larger value, and then its payoff will increase. Accordingly, defender will not put its defending resource on these nodes whose value is less than \(W\) at Nash equilibrium.

Assume node \(m\) is the node whose value larger than \(W_{\text{Threshold}}\) but with probability 0 to be attacked at Nash equilibrium, and \(W_i \geq W_{m} > W_{\text{Threshold}}\) is the minimal value associated with the node that is with positive probability to be attacked at the Nash equilibrium, since every strategy adopted should bring equal payoff to the player at Nash equilibrium [20], there must be

\[
0 \leq W_i(1-C_a - d_i) = W_j(1-C_a - d_j)
\]

for all \(i,j \neq m : W_i \geq W_j\). Considering the fact that

\[
\sum_{i \in S: W_i > W} d_i = 1
\]

and solve this equation group, we obtain

\[
d_i = 1 - C_a - \frac{M(1-C_a) - 1}{W_i} \sum_{i \in S: W_i > W} \frac{1}{W_i}
\]

where \(M\) is the size of set \(\{i \neq m : W_i \geq W\}\).

In this case, the payoff for attack will be

\[
U_d = \sum_{i \in S: W_i > W} a_iW_i(1-C_a - d_i)
\]

\[
= \sum_{i \in S: W_i > W} a_iW_i[1-C_a - (1-C_a - \frac{M(1-C_a) - 1}{W_i} \sum_{i \in S: W_i > W} \frac{1}{W_i})]
\]

\[
= \sum_{i \in S: W_i > W} a_i \frac{M(1-C_a) - 1}{W_i} \sum_{i \in S: W_i > W} \frac{1}{W_i}
\]

\[
= M(1-C_a) - 1 \sum_{i \in S: W_i > W} \frac{1}{W_i}
\]

If attacker shifts its target to node \(m\), which is not defended at this time, its payoff should be

\[
(1-C_a)W \geq (1-C_a)W_{\text{Threshold}}
\]

\[
= M(1-C_a) - 1 \sum_{i \in S: W_i > W} \frac{1}{W_i}
\]

The first inequality is due to the assumption \(W > W_{\text{Threshold}}\), and the second one can be obtained from Lemma 1 and Lemma 2. This inequality means that there is a strategy for attacker to increase its payoff and such strategy cannot be at Nash equilibrium. Accordingly, all nodes with value larger than \(W_{\text{Threshold}}\) will be attacked with positive probability at Nash equilibrium.

From Theorem 1 and Theorem 2, we know that all the nodes with value larger than \(W_{\text{Threshold}}\) will be the attacker’s target with positive probability will not be attacked if its value less than \(W_{\text{Threshold}}\). But how about the nodes whose value is exactly \(W_{\text{Threshold}}\)? This question will be answered by Theorem 3.

**Theorem 3:** Whether or not the attacker selects the nodes with values equal to \(W_{\text{Threshold}}\) will not change its payoff.

**Proof:**

Assume \(W_1 \geq W_2 \geq \cdots \geq W_i \geq W_{k+1}\), and

\[
W_{k+1} = \frac{(k+1)(1-C_a) - 1}{(1-C_a)\sum_{i=1}^{k+1} \frac{1}{W_i}}
\]

(6) means that \(W_{k+1} = W_{\text{Threshold}}\).

From the proof of Theorem 2, we know that if attacker only selects the first \(k\) nodes as target with positive probability, its utility will be

\[
\frac{k(1-C_a) - 1}{\sum_{i \in S: W_i > W} \frac{1}{W_i}}
\]

while its payoff will be

\[
\frac{(k+1)(1-C_a) - 1}{\sum_{i \in S: W_i > W} \frac{1}{W_i}}
\]

if it puts positive attack probability on all the \(k+1\) nodes. From (6), we know

\[
(1-C_a)W_{k+1} \frac{k}{\sum_{i \in S: W_i > W} \frac{1}{W_i}} + (1-C_a) = (k+1)(1-C_a) - 1
\]
That is
\[ W_{k+1} = \frac{k(1-C_a) - 1}{(1-C_a) \sum_{i=1}^{k} \frac{1}{W_i}} \]
Therefore,
\[ \frac{k(1-C_a) - 1}{\sum_{i=1}^{k} \frac{1}{W_i}} = \frac{(k+1)(1-C_a) - 1}{\sum_{i=1}^{k+1} \frac{1}{W_i}} \]

From above three theorems, we can easily get following theorem:

**Theorem 4:** A node is in \( T_v \) if and only if its value is larger than \( W_{\text{threshold}} \).

It should be noted that we still do not know the number of nodes in \( T_v \) neither is the value \( W_{\text{threshold}} \).

We propose following theorem.

**Theorem 5:** Assume \( W_i \geq W_j \geq \cdots \geq W_N \), if
\[ W_N > \frac{N(1-C_a) - 1}{(1-C_a) \sum_{i=1}^{N} \frac{1}{W_i}} \]
then \( T_v = T \). Otherwise, let \( k \) be the minimal index that satisfy
\[ W_k > \frac{k(1-C_a) - 1}{(1-C_a) \sum_{i=1}^{k} \frac{1}{W_i}} \quad \text{and} \quad W_{k+1} \leq \frac{(k+1)(1-C_a) - 1}{(1-C_a) \sum_{i=1}^{k+1} \frac{1}{W_i}} \]
then \( T_v = \{ i \mid i \leq k \} \).

The proof Theorem 5 is skipped and can be found in [13].

**A. Nash Equilibrium**

Based on the analysis in the previous subsection, only the nodes in \( T_i \) may be attacked with a positive probability. Accordingly, let \( \{ a^*_i \} \) and \( \{ d^*_i \} \) denote the strategy of the attacker and the defender, i.e. the probability to allocate attacking and defending resources at node \( i \) respectively. There is
\[ a^*_i = d^*_i = 0 \quad \text{for all} \quad i \notin T_v \quad (7) \]

As to the nodes in \( T_v \), according to the best response lemma [20], we have
\[ W_i (1-C_a - d^*_i) = W_j (1-C_a - d^*_j) \quad (8) \]
and
\[ (a^*_i - C_a) W_i = (a^*_j - C_a) W_j \quad (9) \]
for all \( i, j \in T_v \). In addition to (5)-(7), since we have
\[ \sum_{u \in T_v} a^*_u = 1 \quad \text{and} \quad \sum_{u \in T_v} d^*_u = 1 \]
this forms an equation system where the solution is
\[ a^*_u = \begin{cases} 
C_a + \frac{|T_v|}{W_i} |C_a - 1|, & i \in T_v \\
0, & i \notin T_v 
\end{cases} \quad (10) \]
and
\[ d^*_u = \begin{cases} 
1 - C_a - \frac{|T_v|}{W_i} |C_a - 1|, & i \in T_v \\
0, & i \notin T_v 
\end{cases} \quad (11) \]

**Theorem 6:** The strategy given by (10) and (11), i.e. attacker chooses node \( i \) as its target with probability \( a^*_i \) while defender allocates defending resources at node \( i \) with probability \( d^*_i \), is a Nash equilibrium for the game \( G_M \).

**Proof:**

To prove Theorem 6, we should show:
1. \( a^*_i \geq 0 \) and \( d^*_i \geq 0 \) for all \( i \)
2. \( W_i (1-C_a - d^*_i) \geq W_j (1-C_a) \) for \( i \in T_v \) but \( j \notin T_v \)
3. \( (a^*_i - C_a) W_i \geq C_a W_j \) for \( i \in T_v \) but \( j \notin T_v \).

Item 1 is required by the definition of strategy space, while items 2 and 3 are used to guarantee that each player’s strategy is the best response to the other player’s strategy.

Now, we prove the above 3 items one by one:
1. For node \( i \in T_v \),
\[ C_d + \frac{|T_v|}{W_i} |C_d| = \frac{1}{W_i} \left( C_d \sum_{j \in T_v} \frac{1}{W_j} + 1 - |T_v| |C_d| \right) \geq \frac{1}{W_i} \left( C_d |T_v| (1-C_a) + 1 - |T_v| |C_d| \right) \]
\[ = \frac{1}{W_i} \frac{1 - C_a - C_d}{1 - C_a} \]
Since we assume \( C_a << 1 \) and \( C_d << 1 \) in our work, \( a^*_i \geq 0 \).
\[ 1 - C_a - \frac{|T_v|}{W_i} |C_a - 1| \geq 0 \]
Hence, \( d^*_i \geq 0 \)
2. \[ W_i (1-C_a - d^*_i) = \frac{|T_v|}{W_i} |C_a - 1| \geq (1-C_a) W_j \]
The inequality is due to the fact that \( j \notin T_v \), so that
\[ W_j \leq \frac{|T_v| |1 - C_a|}{1 - C_a} \sum_{i \in T_v} \frac{1}{W_i} \]
\[(a'_i - C_d)W_i + C_dW_j = \frac{1}{\left| \mathcal{T}_i \right|} \sum_{i \in \mathcal{T}_i} W_i - C_d \sum_{i \in \mathcal{T}_i} W_i \]

\[\geq \frac{W_j}{\left| \mathcal{T}_j \right|} (1 - |\mathcal{T}_i|)C_d + C_dW_j = |\mathcal{T}_i| > 0\]

The first inequality is due to the fact that \(W_j \leq W_i\) for all \(i \in \mathcal{T}_i\).

In other words,

\[(a'_i - C_d)W_i \geq -C_dW_j\]

Now, the payoff of each player at Nash equilibrium can be easily calculated:

\[
U_a = \left| \mathcal{T}_i \right| (1 - C_d) \sum_{i \in \mathcal{T}_i} W_i
\]

\[
U_D = (1 - |\mathcal{T}_i|) (1 - |\mathcal{T}_j|)C_d \sum_{i \in \mathcal{T}_i} W_i
\]

(12)

In our network model, \(W_i\) is determined by the network topology and demand routing. Accordingly, both \(U_a\) and \(U_D\) are functions of \(W_i\). For a defender, it can try to maximize its payoff (minimize loss) at Nash equilibrium by controlling network topology and demand routing to vary \(W_i\). In the next section, we will study how a defender should control network topology and demand routing to maximize its payoff.

VI. TOPOLOGY AND ROUTING CONTROL

Due to the flexible topology and routing in MANETs, we can optimize the value of each node to protect the MANET by configuring the its topology and demand routing so that the defender’s loss can be minimized. In subsection V-A, we first present some guidelines gained by analyzing the defender’s payoff at Nash equilibrium. After that, in subsection V-B, we design an algorithm to control the MANET topology and demand routing to maximize its payoff.

A. Guidelines to Defend a MANET

In this subsection, we will present some guidelines on how to control the topology and demand routing to reduce the defender’s loss. It should be noted that due to some approximations, these are just guidelines not theorems and hence they are not rigorously proved also.

Guideline 1: To protect MANETs, we may reduce the values of nodes in \(\mathcal{T}_i\), even if it will bring another node into \(\mathcal{T}_i\).

Since \(C_d < 1\), \(1 - |\mathcal{T}_i| C_d = 1\), and hence we have

\[U_D = \frac{1 - |\mathcal{T}_i|}{\sum_{i \in \mathcal{T}_i} W_i} - C_d \sum_{i \in \mathcal{T}_i} W_i\]

(13)

Say a node \(k\) enters into \(\mathcal{T}_i\) after node \(l\)’s value has been reduced. Assume that node \(l\)’s new value is \(W'_l < W_l\), the defender’s new payoff will be

\[U'_D = \frac{1 - (|\mathcal{T}_i| + 1)}{\sum_{i \in \mathcal{T}_i} W_i + 1 - \frac{1}{W_k} + \frac{1}{W'_l}} - C_d \left( \sum_{i \in \mathcal{T}_i} W_i + W_k + W'_l \right)\]

The change in the payoff after node \(k\) enters into \(\mathcal{T}_i\) is thus

\[U_D - U'_D = \frac{1 - |\mathcal{T}_i| - 1}{\sum_{i \in \mathcal{T}_i} W_i + 1 - \frac{1}{W_k} + \frac{1}{W'_l}} - C_d \left( \sum_{i \in \mathcal{T}_i} W_i + W_k + W'_l \right)\]

\[- |\mathcal{T}_i| \left( \sum_{i \in \mathcal{T}_i} W_i + 1 - \frac{1}{W_k} + \frac{1}{W'_l} \right) - (1 - |\mathcal{T}_j|) (\sum_{i \in \mathcal{T}_i} W_i + 1 - \frac{1}{W_k} + \frac{1}{W'_l})\]

\[-C_d \left( W_k + W'_l - W_l \right)\]

Since node \(k\) will be in \(\mathcal{T}_i\) after node \(l\)’s value has been reduced, there must be

\[|\mathcal{T}_i| \left( 1 - C_d \right) - 1 \geq \sum_{i \in \mathcal{T}_i} W_i + 1 - \frac{1}{W_k} + \frac{1}{W'_l} \]

That is

\[(|\mathcal{T}_i| - 1) \left( \frac{1}{W_k} - \frac{1}{W'_l} \right) \geq 0\]

Then,

\[- |\mathcal{T}_i| \left( \sum_{i \in \mathcal{T}_i} W_i + 1 - \frac{1}{W_k} + \frac{1}{W'_l} \right) - (1 - |\mathcal{T}_j|) (\sum_{i \in \mathcal{T}_i} W_i + 1 - \frac{1}{W_k} + \frac{1}{W'_l})\]

\[= (|\mathcal{T}_i| - 1) (\frac{1}{W_k} - \frac{1}{W'_l}) - |\mathcal{T}_j| \left( \frac{1}{W_k} - \sum_{i \in \mathcal{T}_i} W_i \right)\]

\[\geq (|\mathcal{T}_i| - 1) \left( \frac{1}{W_k} - \frac{1}{W'_l} \right) \geq 0\]

Based on the assumption \(C_d < 1\), we can ignore the term

\[-C_d \left( W_k + W'_l - W_l \right)\]

Therefore, \(U_D - U'_D > 0\). In other words, we should minimize the node value in \(\mathcal{T}_i\), without considering if it will enlarge the size of \(\mathcal{T}_i\).

To show how Guideline 1 works, we give the following example:

Example 1: Consider 3 nodes, \(A, B\) and \(C\), in the network whose initial values are 3, 3 and 1 respectively and for simplicity, assume \(C_d = 0.05\). There is a demand from \(A\) to \(C\), and it has two route options. The first one is \(A \rightarrow C\), while the second one is \(A \rightarrow B \rightarrow C\). If the first option is chosen, the value of each node will be 4, 3 and 2, and \(|\mathcal{T}_i| = 3\). If the second option is chosen, the values will be 4, 4 and 2, and \(|\mathcal{T}_i| = 2\). From Guideline 1, we know that the first option would be better. In fact, under the first option the defender’s payoff will be \(-24/13 \approx -2.29\) at the Nash equilibrium, while it will be \(-2.4\) under the second option.

Guideline 2: When the number of nodes in \(\mathcal{T}_i\) and the sum of their value are both fixed, we may try to make the value of the nodes in \(\mathcal{T}_i\) approximately equivalent (e.g. by doing load balanced routing).

When \(|\mathcal{T}_i|\) is fixed,
The first option is to place it at a node in \( T_v \) following discussion therefore will focus on two other options: defender will not risk losing any additional values. The second is to place it at node \( \mathcal{D} \) because by doing so, the right choice for the defender because by doing so, the nodes not in \( T_v \) may be the better choice.

Assume that value \( W \) should be placed into the network. Obviously, if \( W \) is so small that after placing it at a node \( k \) which is currently not in \( T_v \), \( W_k \) will still be less than \( \theta \) (i.e. \( k \) will still remain outside of \( T_v \)), then placing \( W \) at node \( k \) is the right choice for the defender because by doing so, the defender will not risk losing any additional values. The following discussion therefore will focus on two options: The first option is to place it at a node in \( T_v \), say node \( i \), while the second is to place it at node \( k \) which is currently not in \( T_v \) but will be after \( W \) is placed at node \( k \). In addition to our assumption \( C_j \ll 1 \), we will consider the payoff difference between two similar situations (caused by placing value at different nodes), so that \( C_j \) may have little impact on the result and we just ignore \( C_j \) for simplicity. Then the defender’s payoffs associated with these two options are

\[
U_i = \frac{1 - |T_i|}{\sum_{i \in T_i} W_i + \frac{1}{W_i} + W} \quad \text{and} \quad U_2 = \frac{|T_v|}{\sum_{i \in T_i} W_i + \frac{1}{W_i} + W}
\]

respectively. Then

\[
(\sum_{i \in T_i} \frac{1}{W_i} + \frac{1}{W_i} + W)(\sum_{i \in T_i} \frac{1}{W_i} + \frac{1}{W_i} + W)(U_1 - U_2) = \sum_{i \in T_v} \frac{1}{W_i} + |T_v| - 1 \cdot \frac{1}{W_i} - (|T_v| - 1) \cdot \frac{1}{W_i} + W)
\]

If \( W_k \) is very small and \( W \) is in the same order of magnitude of \( W_k \), we have

\[
W_k + W = \frac{|T_v| - 1}{\sum_{i \in T_v} W_i}
\]

and then

\[
(15) = T_v \cdot (\frac{1}{W_i + W} - \frac{1}{W_i}) < 0
\]

which means that \( W \) should be placed at the node not in \( T_v \). On the other hand, if \( W >> W \), we have

\[
W_i + W > \frac{|T_v| - 1}{\sum_{i \in T_v} W_i} \quad \text{and} \quad \frac{1}{W_i + W} = \frac{1}{W_i}
\]

then

\[
(15) \Rightarrow |T_v| \cdot (\frac{1}{W_i + W} - \frac{1}{W_i}) = 0
\]

which means the value should be placed at the nodes in \( T_v \).

In summary, we have shown that in order for a defender to reduce losses, it first considers reducing the value of each node in \( T_v \). Further, without increasing the total value and the node number in \( T_v \), evenly distributing the values among the nodes in \( T_v \) to achieve a load balance is a good objective to pursue. Last but not least, the defender should also route each new demand according to its value.

B. Topology and Demand Routing Control Algorithm

Based on the Guideline 1 discussed in the previous subsection and (14), a defender may first reduce the total value of nodes in \( T_v \) to reduce its value lost. In the following discussion, to simplify presentation, we also let \( T_v \) represent a subnetwork consisting of the nodes in \( T_v \).

The total value of nodes in \( T_v \) is

\[
\sum_{i \in T_v} W_i = \sum_{i \in T_v} \sum_{j \in \mathcal{D}(i,j)} v_{ij}
\]

where \( H_i \) is the number of nodes in \( T_v \), on the path from node \( i \) to node \( j \). Motivated by the rearrangement inequality [21], we

\[
\text{Algorithm 1: Topology Control and Routing in MANET}
\]

**Input**: Moving area of each node \( \mathcal{S}_i \) and its communication radius \( \mathcal{R}_i \), value of each demand \( \{v_{ij}\} \)

**Output**: All connections in the MANET \( C=\{c_{ij}\} \), route for each demand \( P=\{P_{ij}\} \)

**Initialize**: \( C=\emptyset, P=\emptyset \)

1: Sort all the demands in a non-increasing order in terms of their value
2: for each demand \( v_{ij} \) do
3: Every node moves towards node \( i \) without cutting down connections in \( C \).
4: Calculate Neighbor set of each node \( \{A_i\} \)
5: Construct an auxiliary graph \( G=(N, E) \), where each node in \( G \) present an MANET node if \( c_{ij} \in E \) if and only if \( j \in A_i \).
6: Set weight on each link in \( G \) (Detail in Algorithm 2)
7: \( P_{ij}=\text{ShortestPath}(G, v_{ij}) \)
8: \( P=\emptyset \cup P_{ij} \)
9: for all \( c_{ij} \in P_{ij} \) do
10: if \( c_{ij} \in C \) then
11: \( C=\emptyset \cup c_{ij} \)
12: end if
13: end for
14: end for
15: return \( C, P \)
can find a path with fewer nodes in \( T_v \) for the demands with larger value and assign a path with relatively more nodes in \( T_v \) for the demands with smaller value.

From Guideline 2, without increasing the total value of nodes in \( T_v \), balancing the value of each node in \( T_v \) is the way to further reduce the defender’s loss. To that end, all the demands should be distributed in \( T_v \) evenly. Therefore, we can determine routing of all the demands in MANETs one by one so that the demands routed later can balance the value of each node in \( T_v \) based on the path of demands routed.

Based on the discussion above, the algorithm to control MANET topology and demand routing is shown in Algorithm 1. The key idea of Algorithm 1 is to route all the demands on the auxiliary graphs one by one and determine the MANET topology base on the routing result. We now introduce the details of the algorithm as follows.

First of all, as shown in Line 1, our algorithm sorts the demand in a non-increasing order in terms of their value, which considers routing the demand with the larger value with the higher priority.

For every demand \( v_j \) sorted above, we first move all other nodes towards node \( i \) one by one to provide node \( i \) more relaying choices without interrupting those connections already built. Then, an auxiliary graph \( G \) containing all the available paths to \( v_j \) is constructed. After that, we set weight on each link in \( G \) based on the guidelines discussed in the previous subsection, and find the shortest path on \( G \) for \( v_j \). When finishing one demand routing, we update all information of the MANET including its path set \( P \) and connection set \( C \) as shown in Line-8 and Line 9-13 respectively. Once all the demands are routed, the algorithm returns the connection and routing configurations for the MANET.

Now we introduce how to determine the weight setting as mentioned in Line 6 of Algorithm 1 in detail since it is the key step affecting how resilient the MANET will be to attacks. Following the guidelines presented in the previous subsection, the total demand to weight of each link, \( w_{ij} \) in \( G \) for \( v_j \) is shown in Algorithm 2. Though the defender always wants to minimize its loss, the spectrum constraint cannot be violated, i.e. at most \( K \) connections can be set up at any node \( i \). Therefore, those nodes that have already had \( K \) connections should be excluded (Line 2-4). In order to minimize the total value in \( T_v \), we set the weight of a link ending at a node in \( T_v \) to the sum of all the demand values plus the value of its ending node. The first term in the weight leads the path of \( v_j \), to be the minimal hop first in \( T_v \) while the second term is used to balance the value of nodes in \( T_v \) (Line 5-7). If a node’s value will be less than \( W_{\text{Threshold}} \) even it relays \( v_j \), this node can be used with little cost. Accordingly, we only set a small weight to the links ending at these nodes (Line 8-10). Otherwise, we should set weight to links according to Guideline 3. When \( W_{\text{Threshold}} \) is much larger than the value of demand being routed, we set large weight to the link ending at nodes out of \( T_v \) so as to force \( v_j \) to use the nodes in \( T_v \). If the value of \( v_j \) is less than \( W_{\text{Threshold}} \) we should reduce the weight of links ending at nodes out of \( T_v \) to make \( v_j \) be relayed by the nodes out of \( T_v \) (Line 11-14).

VII. Simulation

In this section, we will evaluate the performance of our proposed method to reduce the defender’s loss. Firstly, we will compare our topology and routing control method with the minimal hop method in subsection VI-A. In subsection VI-B, we will evaluate the security benefit brought by the nodal mobility. We will also discuss the impact of routing information to the defender’s payoff in subsection VI-C.

In our simulation, we randomly allocate some nodes in an area with the size of 2km×2km, set the communication radius of each node to be 400m and assume each node can set up at most 4 connections to other nodes. All the demand values in the network are evenly distributed between 0 and 100.

A. Performance of Our Topology and Routing Control Method

In this subsection, we evaluate the performance of our topology control and routing method on enhancing the defender’s payoff in MANETs with different numbers of nodes. The simulation results are shown in Fig.2. All the points in the graphs are the defender’s payoff at Nash equilibrium. When studying how the defender’s payoff changes with the node number in MANETs, we set the demand number is 2 times of the node number (i.e. keep the demand density constant), while we set the node number to be 200 when we study the relationship between the defender’s payoff and the demand number. We also set that each node can move in a circle centered at its original location with radius of 200m and \( C_a=C_d=0.005 \). As a benchmark, we also test the scheme that the defender uses the path with minimal hop to route its demands.

From the simulation, we can see that the defender’s payoff will decrease with the increase of nodes/demands number. That is because there are more demands and larger value in the network. Therefore, the defender may lose more payoffs when

<table>
<thead>
<tr>
<th>Algorithm 2: Set weight for demand routing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input:</strong> Auxiliary graph ( G ), the demand to be routed ( v_{aw} ), the number of connections can be set up by one node ( K ).</td>
</tr>
<tr>
<td><strong>Output:</strong> Weight on each link ( {w_{ij} \in E } )</td>
</tr>
<tr>
<td><strong>Initialize:</strong> Calculate ( V=\sum_{v_j} W_j ) for all nodes based on the demands already routed, ( W_{\text{Threshold}} ) and ( T_v ). Predefine a large number ( M );</td>
</tr>
<tr>
<td>1: for each ( e_{ij} ) in ( G ) do</td>
</tr>
<tr>
<td>2: if node ( i ) or node ( j ) is with ( K ) connections and ( e_{ij} \notin C ) then</td>
</tr>
<tr>
<td>3: ( \sigma \leftarrow \text{inf} ), continue;</td>
</tr>
<tr>
<td>4: end if</td>
</tr>
<tr>
<td>5: if ( e_{ij} \notin T_v ) then</td>
</tr>
<tr>
<td>6: ( w_{ij} \leftarrow V+W_j ), continue;</td>
</tr>
<tr>
<td>7: end if</td>
</tr>
<tr>
<td>8: if ( W_{\text{Threshold}} \geq W_j ) then</td>
</tr>
<tr>
<td>9: ( w_{ij} \leftarrow \sigma ), continue;</td>
</tr>
<tr>
<td>10: end if</td>
</tr>
<tr>
<td>11: if ( W_{\text{Threshold}} \geq M_{vaw} ) then</td>
</tr>
<tr>
<td>12: ( w_{ij} \leftarrow 2V )</td>
</tr>
<tr>
<td>13: else ( w_{ij} \leftarrow \sigma )</td>
</tr>
<tr>
<td>14: end if</td>
</tr>
<tr>
<td>15: end for</td>
</tr>
<tr>
<td>16: return ( {w_{ij} } )</td>
</tr>
</tbody>
</table>
it does not catch the attacker. Another reason for this observation is that more nodes in the network will increase the difficulty to catch the attacker in the network, and hence a larger network will incur more value losses to defender.

More importantly, no matter what the node/demand number is in the MANET, controlling the topology and routing through our method will lose fewer payoffs compared with the case that all the demands are routed in the minimal hop path.

Another observation from the results is that the more demands in the MANET, the larger performance improvement will be brought by our topology control and routing method. The reason is that more demands will bring larger optimization space, resulting in performance improvement.

B. Performance Improvement Brought by Nodal Mobility

In this subsection, we evaluate the security benefit of nodal mobility on defending the attack. Intuitively, if node $i$ can move when it wants to set up a connection, there will be more nodes which can be selected as its relaying nodes and there will be greater optimization space for the defender to reduce its payoff loss. At first, we take the case that every node in the network cannot move (i.e. set $\gamma=0$ for all $i$) as a baseline to study the benefit brought by nodal mobility in different size networks. We also set $C_a=C_d=0.005$, each node can move in a circle with radius 200m as in subsection VI-A and the simulation results are shown in Fig.3.

In Fig.3(a), we find that the nodal mobility will increase the defender’s payoff from about 28.63% to 32.09% in networks with different node number. When the network size is relatively large, there will be more performance improvement than in the small size networks. It is again because that there will be greater optimization space when the network size is relatively larger and there are more demands in the network.

In Fig.3(b), similar results with Fig.3(a) can be yielded. More demands will result in more value losses to defender, but the more demands in the network, the larger performance improvement there will be, due to the larger optimization space. In our simulation, nodal mobility will bring about 16.53% to 34.98% performance improvement to defender.

In addition, we also study the impact of each defender’s maximum moving distance. We do this simulation in a MANET with 200 nodes and 400 demands. With different maximum moving distance for each node, the defender’s payoff and the total distance all nodes moving are shown in Fig.4. In this figure, we see that a longer moving distance for each node will help to reduce the defender’s payoff loss but increase the total moving distance. When the maximum moving...
distance exceeds a threshold (500m in our simulation), a larger maximum distance will not bring benefit to the defender since there remains no optimization space that can be seized by the node’s movement.

C. Impact of Routing Information

In subsection III-C, we have discussed that our method can guarantee the defender’s worst case performance by assuming the attacker has the information of demand routing. In this subsection, we will study how much security benefit the defender can get from hiding demand routing information by simulation.

When the attacker has no information on the demand routing, it also does not know the value of each node. Accordingly, it can only randomly choose a node as its target. On the other hand, the defender does not know whether the attacker knows the demand routing information. Therefore, it will stick to the strategy at Nash equilibrium to guarantee its worst case performance.

In this situation, the defender’s payoff is shown in Fig. 5. One observation is that compared with the case that the attacker has no demand routing information, the defender will suffer from much larger payoff loss if the attacker knows all the demand routing information. Another observation is that without demand routing information, the attacker cannot bring a significant larger payoff loss to the defender when the network size increases. The reason is that attack cannot seek the most valuable node to attack without knowing the value of each node. Both observations suggest that hiding the demand routing information is necessary for defender to reduce its payoff loss.

VIII. Conclusion

In this paper, we formulated the interaction between the attacker and the defender in MANETs as a two-player variable-sum game. Based on the analysis of this game, we identified the nodes that are worth attacking and solved the game. Inspired by the Nash equilibrium, we summarized some important defending guidelines for the topology control and demand routing in the MANET. Based on these guidelines, we also proposed an algorithm to reduce the defender’s loss under attack. Simulations show that our algorithm can reduce the defender’s loss at Nash equilibrium and the nodal mobility can also bring benefit to defender. We also find that hiding the demand routing information is also an efficient method to reduce the defender’s loss.

References


