Control Topology and Routing to Protect Mobile Ad hoc Networks Based on A Game Theoretic Analysis

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 non-zero-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 guidelines to the defender and design algorithms 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 ~~to protect network security~~.**

Index Terms*— *MANET security; topology and routing control; 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, it is vulnerable to attacks, such as signal jamming attack in physical layer [2], cryptography attacks in link layer [3], routing attacks and packet forwarding attacks in 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 its unique characteristic, including an open network architecture which is easier for other nodes to join the network, shared wireless medium and 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 wireless medium and nodal mobility in MANETs. This paper aims at providing an insight in leveraging these characteristics 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 with some nodes in its range directly, and with other nodes through forwarding. Sometimes, each of the node 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 later case but our results also provide insight in the previous 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 deny-of-service (DDoS) attack [8], design a smart cryptograph system [9] and modify 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 provides valuable insights to the operator in terms of how to keep its 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 is the most related work to this study. Nonetheless, neither of them modeled the situation in MANETs, and in fact, both of them assumed that the cost incurred by the defender after each link/node being attacked is constant. In this paper, we will not only leverage the configurable topology and routing in MANETs, but also utilize the nodal mobility to enhance the security of 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.

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

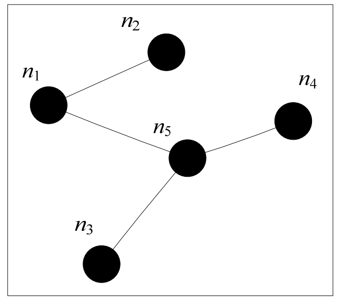
- We formulate the interaction between attacker and defender as a two-player non-zero-sum game. Our analysis shows that not all the nodes are worth attacking, and accordingly, we also determine which nodes should be defended.
- Based on the analysis, we solve the Nash equilibrium of the game and hence 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 MANETs to reduce the defender's loss.
- 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 attacker and 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 MANET, and propose a corresponding algorithm to do so in Section V. Simulations results are presented in Section VI and we conclude this paper in Section VII.

II. RELATED WORK

Many existing studies on MANET security focused on designing specific schemes or countering specific attacks. Mingda et al. [8] took the advantage of high redundancy of MANETs and chooses protection node to share the malicious traffic. Eissa et al. [9] designed a cryptograph system to protect the data integrity in MANETs. And Manel et al. [10] changed the existing routing protocol AODV with the concerning of MANETs security. All these works focused on a specific attacking scenario or protocol and hence are not general enough to be applicable in practice when an attacker is adaptive. In our work, we aim to design a general algorithm/protocol which can be used to protect MANETs in different situations.

Game theory is a good framework to obtain a more general result than only designing specific scheme or protocol. It is not only because that the interaction between an attacker and defender can be explicitly modeled as a game model in natural, but also since the payoff function can be defined to adapt to different scenarios without changing the analyzing. The work in [11] used a game model to study how to allocate defending resource in network to counter malicious attacks. Xiao et al. [12] and Chen et al. [13] did some similar work, which are also related to this study. Though these existing results can be applied to MANETs, they do not take advantage of the nodal mobility which is a unique property in MANETs and may bring additional security benefit to the defender.



Communication pairs and routes	
S/D	Route
$n_1 \to n_2$	$n_1 \to n_2$
$n_1 \to n_5$	$n_1 \to n_5$
$n_3 \to n_4$	$n_3 \to n_5 \to n_4$

Fig.1 An example of MANET with 5 nodes

There are also previous studies, such as [14-19], on the topology and routing control 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 the 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 demand routing in MANETs.

III. PROBLEM FORMULATION

A. Network Model

In this paper, we consider a MANET with N mobile nodes and use $\boldsymbol{T}$ to denote the set of all nodes. For each node i, ~~among its neighbor set, denoted by A_i~~, it can set up direct connections, i.e. inks in the network, with at most K nodes in $\boldsymbol{A}_i$. ~~A_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

$$W_u = \sum_{i,j:u\in P(i,j)} v_{ij} \tag{1}$$

where $P(i,j)$ is the set of node 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 a 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 MANETs, it will allocate defending resources to prevent from such loss. If the attacker

Table 1 Payoff matrix of the game for node i

	Defend	Not defend
Attack	$-C_aW_i$, $-C_pW_i$	W_i-C_aW_i, $-W_i$
Not Attack	0, $-C_pW_i$	0,0

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 attacker will be zero. Note that our work here can be easily extended to cases where each link, instead of a node is attached, 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_p for attacker and defender, respectively. In our work, we assume C_a <<1 and C_p<<1. Otherwise, an attacker may have no incentive to choose a target, nor defender has any incentive to protect its nodes.

Take the MANET in Fig.1 as an example. There are 5 nodes and 3 demand node pairs 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 attacker wants to select node 1 as its target, the attack cost should be C_a ($v_{12}+v_{15}$) and it will get payoff $v_{12}+v_{15}$ if node 1 is not protected. The defender can protect node 1 at cost C_p ($v_{12}+v_{15}$) in case this node being attacked. 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 MANETs so as to minimize the defender's loss or maximize its payoff. It is worth noting that the payoff matrix in Table 1 is only a special case, and our analyzing game-theoretic analysis and general guidelines and conclusions are suitable to all other payoff matrixes.

B. Game Model

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

$$\begin{aligned} U_A &= \sum_i [p_i q_i(-C_a W_i) + p_i(1-q_i)(W_i - C_a W_i)] \\ &= \sum_i p_i W_i (1 - C_a - q_i) \end{aligned} \tag{2}$$

and

$$\begin{aligned} U_D = \sum_i [& p_i q_i(-C_p W_i) - p_i(1-q_i)W_i \\ & -(1-p_i) q_i C_p W_i] \\ = \sum_i & q_i(p_i - C_p)W_i - \sum_i p_i W_i \end{aligned} \tag{3}$$

Therefore, when both the attacker and the defender act attack/defend the targeted MANET, their interactions can be formulated as a two-player non-zero-sum game, $\boldsymbol{G}_A$, as follows:

Player: Attacker, Defender

Strategy space:

Attacker: $S_A = \{p : p \in [0,1]^N, \sum_i p_i \le 1\}$

Defender: $S_D = \{q : q \in [0,1]^N, \sum_i q_i \le 1\}$

Payoff: U_A for attacker and U_D for defender

C. Discussion

The game model we formulated in last subsection can not only be applied to MANETs as in this paper, it is also suitable to any other communication networks if only 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 provide other dimensional defending strategies. 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 in MANETs and it provides more flexibility to control the network topology. Therefore, unique features in MANETs may bring more benefit to defender to protect the networks.

Additionally, to assume the attacker having symmetric information as the defender e.g. the MANET topology and demand routing is to provide the worst case performance analysis. We can expect that when the knowledge about the MANETs decreases, the defender will only suffer less payoff losses than the worst case. In next section, we will analyze how to utilize these features in MANETs to counter malicious attacks.

IV. Equilibrium Analysis

As is well known, equilibrium is the key solution concept for a game. In this section, we will solve the game $\boldsymbol{G}_A$ 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/defending in subsection IV.B.

A. Vulnerable Set Analysis

Definition 1: *Vulnerable set*: A set of nodes, denoted by $\boldsymbol{T}_v$, which will be selected as the target by attacker with a positive probability.

By the above definition, for the nodes out of the vulnerable set, the attacker will not select them as targets. Next we first answer the question whether a node will be in the vulnerable set by Theorem 1.

Theorem 1: Any nodes whose value is less than

$$W_{Threshold} = \frac{|\boldsymbol{T}_v|(1-C_a)-1}{(1-C_a)\sum_{i\in T_x}\frac{1}{W_i}} \tag{4}$$

(where $|\boldsymbol{T}_v|$ denotes the total number of nodes in $\boldsymbol{T}_v$), is not in $\boldsymbol{T}_v$.

Proof:

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

Assume that there is a vulnerable set $\boldsymbol{T}_v^{'}$ containing all the nodes with value larger than $W_{Threshold}$, and consider the strategy for the defender

$$q_i^* = 1 - C_a - \frac{|\boldsymbol{T}_v|(1-C_a)-1}{W_i \sum_{i \in T_s^{'}} \frac{1}{W_i}}$$

which satisfies

$$q_i^* \geq 0 \text{ and } \sum_{i \in T_s^{'}} q_i^* = 1$$

If the defender's strategy is $\{q_i\}_{i \in \boldsymbol{T}}$, there must be some node m such that $q_m \leq q_m^*$. Then, we can construct a new strategy for attacker

$$p_i^{'} = \begin{cases} p_m + p_k, i = m \\ 0, i = k \\ p_i, otherwise \end{cases}$$

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

$$\begin{aligned} &\sum_{i \in T} p_i^{'} W_i (1 - C_a - q_i) - \sum_{i \in T} p_i W_i (1 - C_a - q_i) \\ &= p_k W_k (1 - C_a - q_k) - p_k W_m (1 - C_a - q_m) \\ &\leq p_k W_k (1 - C_a - q_k) - p_k W_m \frac{|\boldsymbol{T}_v|(1-C_a)-1}{W_m \sum_{i \in T_s^{'}} \frac{1}{W_i}} \\ &\leq p_k W_k - p_k \frac{|\boldsymbol{T}_v|(1-C_a)-1}{\sum_{i \in T_s^{'}} \frac{1}{W_i}} \\ &\leq 0 \end{aligned}$$

where the first inequality is due to $q_m \leq q_m^*$, the second is because $1 - C_a - q_k < 1$, and the last one is the assumption at the beginning of the proof. All the inequalities are tight if and only if p_k=0. Therefore, this contradicts our assumption and all the nodes with value less than $W_{Threshold}$ will not be selected in $\boldsymbol{T}_v$. ■

In addition to Theorem 1, we also want to ask whether all the nodes whose value is larger than $W_{Threshold}$ 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 3 lemmas which will be used to prove Theorem 2.

Lemma 1 [20]: For a 2-player non-cooperative game, let x and y be mixed strategy for each player. Then x is best response to y if and only if all strategies in the support of x are pure best response to y.

Lemma 2: Assume $W_1 \geq W_2 \geq \cdots \geq W_n$ and

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

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,

$$\begin{aligned} &\frac{(k+1)(1-C_a)-1}{\sum_{i=1}^{k+1} \frac{1}{W_i}} - \frac{k(1-C_a)-1}{\sum_{i=1}^{k} \frac{1}{W_i}} \\ &= \frac{Y - C_a}{X + \frac{1}{W_{k+1}}} - \frac{Y-1}{X} = \frac{(1-C_a)XW_{k+1} - Y + 1}{X(W_{k+1}X+1)} \end{aligned}$$

Consider

$$\begin{aligned} &XW_{k+1}(1-C_a) + Y - 1 \\ &= (1-C_a)W_{k+1}\sum_{i=1}^{k+1} \frac{1}{W_i} - Y + 1 - (1-C_a) \end{aligned} \quad (5)$$

From

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

We know,

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

Therefore,

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

In other words,

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

Lemma 3: Assume $W_1 \geq W_2 \geq \cdots \geq W_n$ if

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

then

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

Proof:

This lemma clearly holds since

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

Theorem 2: All the nodes with value lager than $W_{Threshold}$ will be selected into $\boldsymbol{T}_v$.

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.

On the other hand, we can treat $\boldsymbol{G_A}$ as a 2-player non-cooperative game, in which every node is a pure strategy for attacker/defender. And each player should find a mixed strategy to maximize its payoff.

Assume node m is the node whose value larger than $W_{Threshold}$ but with probability 0 to be attacked at Nash equilibrium, and $W \geq W_m > W_{Threshold}$ is the minimal value associated with the node that is with positive probability to be attacked at the Nash equilibrium, from Lemma 1, there must be

$$0 \leq W_i(1-C_a-q_i) = W_j(1-C_a-q_j)$$

for all $\{i, j \neq m : W_i \geq W, W_j \geq W\}$. Considering the fact that

$$\sum_{i:W_i > W} q_i = 1$$

and solve this equation group, we obtain

$$q_i = 1 - C_a - \frac{M(1-C_a)-1}{W_i \sum_{i\neq m:W_i \geq W} \frac{1}{W_i}}$$

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

In this case, the payoff for attack will be

$$\begin{aligned} U_A &= \sum_{i\neq m:W_i \geq W} p_i W_i (1-C_a-q_i) \\ &= \sum_{i\neq m:W_i \geq W} p_i W_i \{1-C_a-[1-C_a-\frac{M(1-C_a)-1}{W_i \sum_{i\neq m:W_i \geq W} \frac{1}{W_i}}]\} \\ &= \sum_{i\neq m:W_i \geq W} p_i \frac{M(1-C_a)-1}{\sum_{i\neq m:W_i \geq W} \frac{1}{W_i}} \\ &= \frac{M(1-C_a)-1}{\sum_{i\neq m:W_i \geq W} \frac{1}{W_i}} \end{aligned}$$

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

$$\begin{aligned} (1-C_a)W &> (1-C_a)W_{Threshold} \\ &= \frac{|\boldsymbol{T}_v|(1-C_a)-1}{\sum_{i\in T_v} \frac{1}{W_i}} > \frac{M(1-C_a)-1}{\sum_{i\neq m:W_i \geq W} \frac{1}{W_i}} \end{aligned}$$

The first inequality is due to the assumption $W > W_{Threshold}$, and the second one can be obtained from Lemma 2 and Lemma 3. 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 $W_{Threshold}$ 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 $W_{Threshold}$ will be the attacker's target with positive probability while with 0 probability to be at[illegible]d if its value less than $W_{Threshold}$. But how about the nodes whose value is exactly $W_{Threshold}$?

Theorem 3: Whether or not attacker select the nodes with values equal to $W_{Threshold}$ will not change its payoff.

Proof:

Assume $W_1 \geq W_2 \geq \cdots \geq W_k \geq W_{k+1}$, and

$$W_{k+1} = \frac{(k+1)(1-C_a)-1}{(1-C_a)\sum_{i=1}^{k+1} \frac{1}{W_i}} \tag{6}$$

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

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

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

while its payoff will be

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

if it puts positive attack probability on all the k+1 nodes.

From (6), we know

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

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: The vulnerable set is formed by all the nodes whose value is larger than $W_{Threshold}$.

It should be noted that we still do not know the number of nodes in $\boldsymbol{T_s}$, neither is the value $W_{Threshold}$. To solve this problem, we propose following theorem.

Theorem 5: Assume $W_1 \geq W_2 \geq \cdots \geq W_N$, if

$$W_N > \frac{N(1-C_a)-1}{(1-C_a)\sum_{i=1}^{N} \frac{1}{W_i}}$$

then $\boldsymbol{T_v}=\boldsymbol{T}$. Otherwise, let k be the minimal index that satisfy

$$W_k > \frac{k(1-C_a)-1}{(1-C_a)\sum_{i=1}^{k} \frac{1}{W_i}} \text{ and } W_{k+1} \leq \frac{(k+1)(1-C_a)-1}{(1-C_a)\sum_{i=1}^{k+1} \frac{1}{W_i}}$$

then $\boldsymbol{T}_v = \{i \mid i \leq k\}$

Proof:

The proof Theorem 4 is skipped due to it is similar to Lemma 1 in [13]. ■

B. Nash Equilibrium

Based on the analysis in the previous subsection, we have known that only the nodes in $\boldsymbol{T}_v$ may be with a positive probability. Accordingly, let $\{p_i^*\}$ and $\{q_i^*\}$ denote the strategy of the attacker and the defender at Nash equilibrium, respectively. There is

$$p_i^* = q_i^* = 0 \text{ for all } i \notin \boldsymbol{T}_v \quad (7)$$

As to the nodes in T_s, according to Lemma 1, we have

$$W_i(1-C_a-q_i^*) = W_j(1-C_a-q_j^*) \quad (8)$$

and

$$(p_i^*-C_p)W_i = (p_j^*-C_p)W_j \quad (9)$$

for all $i, j \in \boldsymbol{T}_v$. In addition to (7)-(9), since we have

$$\sum_{i\in T_s} p_i^* = 1 \text{ and } \sum_{i\in T_s} q_i^* = 1$$

this forms an equation system where the solution is

$$p_i^* = \begin{cases} C_p + \dfrac{1-|\boldsymbol{T}_v|C_p}{W_i \sum_{i\in T_s} \frac{1}{W_i}}, & i \in \boldsymbol{T}_v \\ 0, & i \notin \boldsymbol{T}_v \end{cases} \quad (10)$$

and

$$q_i^* = \begin{cases} 1-C_a - \dfrac{|\boldsymbol{T}_v|(1-C_a)-1}{W_i \sum_{i\in T_s} \frac{1}{W_i}}, & i \in \boldsymbol{T}_v \\ 0, & i \notin \boldsymbol{T}_v \end{cases} \quad (11)$$

Theorem 6: The Nash equilibrium for the game $\boldsymbol{G_A}$ is that the defender and the attacker choose nodes to allocate (defending and attacking) resources with probability values given by p^* and q^* in (10) and (11) respectively.

Proof:

To prove Theorem 5, we should show:

1. $p_i^* \geq 0$ and $q_i^* \geq 0$ for all i
2. $W_i(1-C_a-q_i^*) \geq W_j(1-C_a)$ for $i \in T_s$ but $j \notin \boldsymbol{T}_v$
3. $(p_i^*-C_p)W_i \geq -C_pW_j$ for $i \in T_s$ but $j \notin \boldsymbol{T}_v$.

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

Now, we prove the above 3 items one by one:

1. For node $i \in \boldsymbol{T}_v$

$$C_p + \frac{1-|\boldsymbol{T}_v|C_p}{W_i \sum_{i\in \boldsymbol{T}_v} \frac{1}{W_i}} = \frac{1}{W_i \sum_{i\in \boldsymbol{T}_v} \frac{1}{W_i}} (C_pW_i \sum_{i\in \boldsymbol{T}_v} \frac{1}{W_i} + 1 - |\boldsymbol{T}_v|C_p)$$

$$\geq \frac{1}{W_i \sum_{i\in \boldsymbol{T}_v} \frac{1}{W_i}} (\frac{C_p|\boldsymbol{T}_v|(1-C_a)-C_p}{1-C_a} + 1 - |\boldsymbol{T}_v|C_p)$$

$$= \frac{1}{W_i \sum_{i\in \boldsymbol{T}_v} \frac{1}{W_i}} \frac{1-C_a-C_p}{1-C_a}$$

Since we assume C_a<<1 and C_p<<1 in our work, $p_i^* \geq 0$.

$$1-C_a - \frac{|\boldsymbol{T}_v|(1-C_a)-1}{W_i \sum_{i\in \boldsymbol{T}_v} \frac{1}{W_i}}$$

$$\geq 1-C_a - [|\boldsymbol{T}_v|(1-C_a)-1]\frac{(1-C_a)}{|\boldsymbol{T}_v|(1-C_a)-1}$$

$$\geq 0$$

Hence, $q_i^* \geq 0$

2.

$$W_i(1-C_a-q_i^*) = \frac{|\boldsymbol{T}_v|(1-C_a)-1}{\sum_{i\in \boldsymbol{T}_v} \frac{1}{W_i}} \geq (1-C_a)W_j$$

The inequality is due to the fact that $j \notin \boldsymbol{T}_v$, so that

$$W_j \leq \frac{|\boldsymbol{T}_v|(1-C_a)-1}{(1-C_a)\sum_{i\in \boldsymbol{T}_v} \frac{1}{W_i}}$$

3.

$$(p_i^*-C_p)W_i + C_pW_j = \frac{1-|\boldsymbol{T}_v|C_p}{\sum_{i\in \boldsymbol{T}_v} \frac{1}{W_i}} + C_pW_j$$

$$\geq \frac{W_j}{|\boldsymbol{T}_v|}(1-|\boldsymbol{T}_v|C_p) + C_pW_j = \frac{|\boldsymbol{T}_v|}{W_j} > 0$$

The first inequality is due to the fact that $W_j \leq W_i$ for all $i \in \boldsymbol{T}_v$. In other words,

$$(p_i^*-C_p)W_i \geq -C_pW_j$$ ■

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

$$\begin{cases} U_A = \dfrac{|\boldsymbol{T}_v|(1-C_a)-1}{\sum_{i\in \boldsymbol{T}_v} \frac{1}{W_i}} \\ U_D = \dfrac{(1-|\boldsymbol{T}_v|)(1-|\boldsymbol{T}_v|C_p)}{\sum_{i\in \boldsymbol{T}_v} \frac{1}{W_i}} - C_p \sum_{i\in \boldsymbol{T}_v} W_i \end{cases} \quad (12)$$

It should be noted that if U_A may be less than 0, it indicates that it is not worth launching attacks as a rational attacker. For the defender, it thus indicates that current network is safe and in low risks.

V. Topology and Routing Control

Due to the flexible topology and routing in MANETs, we can optimize the value of each node to protect MANETs by configuring the MANET topology and demand routing so that the values lost 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 so that the losses can be minimized.

A. Guidelines to Defend a MANET

Guideline 1: To protect MANETs, we should reduce the node values even if it may increase the node number in $\boldsymbol{T}_v$.

Ideally, we want to make the attacker's payoff to be negative, i.e.

$$\frac{|\boldsymbol{T}_v|(1-C_a)-1}{\sum_{i\in \boldsymbol{T}_s}\frac{1}{W_i}} \le 0$$

That is $|\boldsymbol{T}_v|(1-C_a)<1$, which is almost impossible in realistic networks, since it requires $|\boldsymbol{T}_v|=0$ when $C_a<<1$. When $|\boldsymbol{T}_v|\ge 1$, we should maximize U_D at Nash equilibrium.

Since $C_p<<1$, $1-|\boldsymbol{T}_v|C_p \approx 1$

$$U_D = \frac{1-|\boldsymbol{T}_v|}{\sum_{i\in \boldsymbol{T}_v}\frac{1}{W_i}} - C_p\sum_{i\in \boldsymbol{T}_v} W_i \qquad (13)$$

If one more node is to be add into $\boldsymbol{T}_v$ due to the value reduction of some node, say the node enter into $\boldsymbol{T}_v$ is node k, the node reducing value is node l whose new value is $W_l^{'}<W_l$, U_D will be

$$U_D^{'} = \frac{1-(|\boldsymbol{T}_v|+1)}{\sum_{i\ne l, i\in \boldsymbol{T}_v}\frac{1}{W_i}+\frac{1}{W_k}+\frac{1}{W_l^{'}}} - C_p\Big(\sum_{i\ne l, i\in \boldsymbol{T}_v} W_i + W_k + W_l^{'}\Big)$$

The payoff difference between before and after node k enters into $\boldsymbol{T}_v$ is

$$U_D^{'} - U_D = \frac{1-|\boldsymbol{T}_v|-1}{\sum_{i\ne l, i\in \boldsymbol{T}_v}\frac{1}{W_i}+\frac{1}{W_k}+\frac{1}{W_l^{'}}} - \frac{1-|\boldsymbol{T}_v|}{\sum_{i\in \boldsymbol{T}_v}\frac{1}{W_i}} - C_p(W_k + W_l^{'} - W_l)$$

$$= \frac{-|\boldsymbol{T}_v|\Big(\sum_{i\ne l, i\in \boldsymbol{T}_v}\frac{1}{W_i}+\frac{1}{W_l}\Big) - (1-|\boldsymbol{T}_v|)\Big(\sum_{i\ne l, i\in \boldsymbol{T}_v}\frac{1}{W_i}+\frac{1}{W_k}+\frac{1}{W_l^{'}}\Big)}{\sum_{i\in \boldsymbol{T}_v}\frac{1}{W_i}\Big(\sum_{i\ne l, i\in \boldsymbol{T}_v}\frac{1}{W_i}+\frac{1}{W_k}+\frac{1}{W_l^{'}}\Big)}$$

$$-C_p(W_k + W_l^{'} - W_l)$$

Since the value reduce incur the entrance of node k into $\boldsymbol{T}_v$, there must be

$$\frac{|\boldsymbol{T}_v|(1-C_a)-1}{(1-C_a)\Big(\sum_{i\ne j, i\in \boldsymbol{T}_v}\frac{1}{W_i}+\frac{1}{W_l}\Big)} \approx \frac{|\boldsymbol{T}_v|-1}{\sum_{i\ne j, i\in \boldsymbol{T}_v}\frac{1}{W_i}+\frac{1}{W_l}} \ge W_k$$

That is

$$(|\boldsymbol{T}_v|-1)\frac{1}{W_k} \ge \sum_{i\ne j, i\in \boldsymbol{T}_v}\frac{1}{W_i}+\frac{1}{W_l}$$

Then,

$$-|\boldsymbol{T}_v|\Big(\sum_{i\ne l, i\in \boldsymbol{T}_v}\frac{1}{W_i}+\frac{1}{W_l}\Big) - (1-|\boldsymbol{T}_v|)\Big(\sum_{i\ne l, i\in \boldsymbol{T}_v}\frac{1}{W_i}+\frac{1}{W_k}+\frac{1}{W_l^{'}}\Big)$$

$$= (|\boldsymbol{T}_v|-1)\Big(\frac{1}{W_k}+\frac{1}{W_l^{'}}\Big) - |\boldsymbol{T}_v|\frac{1}{W_l} - \sum_{i\ne l, i\in \boldsymbol{T}_v}\frac{1}{W_i}$$

$$\ge (|\boldsymbol{T}_v|-1)\Big(\frac{1}{W_l^{'}}-\frac{1}{W_l}\Big) \ge 0$$

Based on the assumption $C_p<<1$, we can ignore the term

$$-C_p(W_k + W_l^{'} - W_l)$$

Therefore, $U_D^{'} - U_D > 0$. In other words, if C_a does not make $\boldsymbol{T}_v$ to be an empty set, we should minimize the total value in the network.

Guideline 2: When the number of nodes in $\boldsymbol{T}_v$ and the sum of their value are both fixed, we should try to make the value of the nodes in $\boldsymbol{T}_v$ approximately equivalent.

When $|\boldsymbol{T}_v|$ is fixed,

$$U_D = \frac{1-|\boldsymbol{T}_v|}{\sum_{i\in \boldsymbol{T}_v}\frac{1}{W_i}} - C_p\sum_{i\in \boldsymbol{T}_v} W_i \ge \frac{1-|\boldsymbol{T}_v|}{|\boldsymbol{T}_v|^2}\sum_{i\in \boldsymbol{T}_v} W_i - C_p\sum_{i\in \boldsymbol{T}_v} W_i \qquad (14)$$

The inequality is due to Cauchy-Schwarz inequality

$$\sum_{i\in \boldsymbol{T}_v}\frac{1}{W_i}\sum_{i\in \boldsymbol{T}_v} W_i \ge |\boldsymbol{T}_v|^2 \text{ and } 1-|\boldsymbol{T}_v|<0$$

The equation is held only when all the value of nodes in $\boldsymbol{T}_v$ are equivalent. (14) is not only coupled with Guideline 1 that we should minimize the value of each node in $\boldsymbol{T}_v$, but also further motivates us to minimize the total value of nodes in $\boldsymbol{T}_v$.

Guideline 3: If a value ~~should~~ be increased ~~at some node,~~ we need to determine where to place this value accordingly to its magnitude. If the value is at the same magnitude as the nodes in $\boldsymbol{T}_v$ or even much larger, we should use the node in $\boldsymbol{T}_v$. Otherwise, the nodes out of $\boldsymbol{T}_v$ may be the better choice.

~~Consider there is a~~ value W should be placed into the network ~~(In realistic MANET, we are to determine the route/relaying of a demand)~~. The first option is to place it ~~on~~ a node in $\boldsymbol{T}_v$, say node l, while the second is to place it ~~on~~ node k out of $\boldsymbol{T}_v$ but incur the entrance of node k into $\boldsymbol{T}_v$. For simplicity, we set $C_a=C_p=0$, then the defender's payoff associated with these two option are

$$U_1 = \frac{1-|\boldsymbol{T}_v|}{\sum_{i\ne l, i\in \boldsymbol{T}_v}\frac{1}{W_i}+\frac{1}{W_l+W}} \text{ and } U_2 = \frac{-|\boldsymbol{T}_v|}{\sum_{i\in \boldsymbol{T}_v}\frac{1}{W_i}+\frac{1}{W_k+W}}$$

respectively. Then

$$\Big(\sum_{i\ne l, i\in \boldsymbol{T}_v}\frac{1}{W_i}+\frac{1}{W_l+W}\Big)\Big(\sum_{i\in \boldsymbol{T}_v}\frac{1}{W_i}+\frac{1}{W_k+W}\Big)(U_1-U_2)$$
$$= \sum_{i\ne l, i\in \boldsymbol{T}_v}\frac{1}{W_i}+|\boldsymbol{T}_v|\frac{1}{W_l+W}-(|\boldsymbol{T}_v|-1)\frac{1}{W_l}-(|\boldsymbol{T}_v|-1)\frac{1}{W_k+W} \qquad (15)$$

If W_k is very small and W is ~~at~~ the same order of magnitude of W_l, ~~there is~~

$$W_k + W \approx \frac{|\boldsymbol{T}_v|-1}{\sum_{i\in \boldsymbol{T}_v}\frac{1}{W_i}}$$

and then

$$(15) \approx |\boldsymbol{T}_v|\Big(\frac{1}{W_l+W}-\frac{1}{W_l}\Big) < 0$$

W should be placed ~~to~~ the node out of $\boldsymbol{T}_s$. If $W_l>>W$, ~~there are~~

$$W_k + W > \frac{|\boldsymbol{T}_v|-1}{\sum_{i\in \boldsymbol{T}_v}\frac{1}{W_i}} \text{ and } \frac{1}{W_l+W} \approx \frac{1}{W_l}$$

then

$$(15) > |\boldsymbol{T}_v|\Big(\frac{1}{W_l+W}-\frac{1}{W_l}\Big) \approx 0$$

the value should be placed ~~to~~ the nodes in $\boldsymbol{T}_v$.

Algorithm 1: Connection and Routing control in MANET

Input: Moving area of each node $\{\boldsymbol{S}_i\}$ and its communication radius $\{r_i\}$, value of each demand $\{v_{ij}\}$
Output: All connections in the MANET $\boldsymbol{C}=\{c_{ij}\}$, route for each communication $\boldsymbol{P}=\{P_{ij}\}$
Initialize: $\boldsymbol{C}\leftarrow\Phi$, $\boldsymbol{P}\leftarrow\Phi$

```
1:  Sort all the communications in non-increasing order in terms of their value
2:  for each communication 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 auxiliary graph G=<N, E>, where each node in G present an MANET node if e_ij∈E if and only if j∈ A_i.
6:      Set weight on G (Detail in Algorithm 2)
7:      P_ij=ShortestPath(G, v_ij)
8:      P←P∪P_ij
9:      for all e_ij∈P_ij do
10:         if c_ij ∉C then
11:             C←C∪c_ij
12:         end if
13:     end for
14: end for
15: return C, P
```

Algorithm 2: Set weight for demand routing

Input: Auxiliary graph $\boldsymbol{G}$, the demand to be routed v_{uv}, the number of connections can be set up by one node K.
Output: Weight on each link $\{w_{ij}, e_{ij}\in\boldsymbol{E}\}$
Initialize: Calculate $V=\sum v_{ij}$, W_i for all nodes based on the demands already routed, $W_{Threshold}$ and $\boldsymbol{T}_s$. Predefine M=10;

```
for each e_ij in G do
    if node i or node j is with K connections and c_ij∉C then
        w_ij←inf, continue;
    end if
    if j∈T_s then
        w_ij←V+W_j, continue;
    end if
    if W_Threshold>W_j+v_uv then
        w_ij←σ, continue;
    end if
    if W_Threshold>Mv_uv then
        w_ij←2V
    else w_ij←σ
    end if
end for
return {w_ij}
```

In summary, we have ~~known~~ that ~~when we control the network topology and demand routing~~ to reduce losses, ~~we should~~ first consider reducing the value ~~lost~~ of each node in $\boldsymbol{T}_v$. Without increasing the total value and the node number in $\boldsymbol{T}_v$, ~~value~~ balance is ~~the~~ objective to pursue. Last but not least, ~~we~~ should also route each demand according to its value.

B. Topology and Demand Routing Control Algorithm

Based on the guidelines analyzed in the previous subsection, first choice is to reduce the value of each node in $\boldsymbol{T}_v$. Though this purpose is hard to pursue since reducing the value of one node may incur the value increasing of other nodes, motivated by (14), we can try to reduce the total node value in $\boldsymbol{T}_v$. Without increasing the total node value in $\boldsymbol{T}_v$, the value balance in the subnetwork formed by the nodes in $\boldsymbol{T}_v$ (If there is no ambiguity, we say $\boldsymbol{T}_v$ instead of the subnetwork formed by the nodes in $\boldsymbol{T}_v$ for short hereafter.) should be pursued to further optimize the defender's payoff.

The total value of nodes in $\boldsymbol{T}_s$ is

$$\begin{aligned}\sum_{u\in\boldsymbol{T}_v} W_u &= \sum_{u\in\boldsymbol{T}}\sum_{i,j:u\in P(i,j)} v_{ij} \\ &= \sum_{i,j}\sum_{u:u\in P(i,j)} v_{ij} \\ &= \sum_{i,j} H_{ij} v_{ij}\end{aligned}$$

where H_{ij} is the node number on the path from node i to node j in $\boldsymbol{T}_v$. Motivated by the rearrangement inequality [21], we can find a shorter path for the demand with large value while assign a relative longer path for the demand with small value. In this way, the total value of nodes in $\boldsymbol{T}_v$ can be minimized.

To balance the value in $\boldsymbol{T}_v$, we should distribute the demand in the $\boldsymbol{T}_v$ evenly. Therefore, we can determine routing of all the demands in MANETs one by one based on how previous communicate routed.

Based on the discussion above, our 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 auxiliary graphs one by one and determine the MANET topology base on the routing result.

Before routing demands, we first sort all the demands in a non-increasing order in terms of their values. In this case, demands with larger values will be routed first, so that they can choose a path with least nodes in $\boldsymbol{T}_v$.

When we route demand v_{ij} in the MANET, we first move all other nodes towards node i one by one to provide node i more relaying choices. It should be noted that the moving of each node should not affect the connections that have been set up for the previous demands. After that, the neighbor set of each node can be updated and then we can construct an auxiliary graph $\boldsymbol{G}$ to route the demand, in which each edge presents a connection option. Then, we set weight to the auxiliary graph in order to lead the demand to the desirable route. According to the path of each demand, we can update the path set and the connection set for the MANET as shown in Line 8 and Line 9-13, respectively. Once all the demands can be specified a routing of their own, the algorithm returns the connections and routing configurations for the MANET.

Obviously, the weight setting is the key step which determines the performance of Algorithm 1. Following the guidelines present in the previous subsection, the detail to set weight on $\boldsymbol{G}$ for v_{ij} is shown in Algorithm 2, where w_{ij} is the weight set to edge (i, j) on $\boldsymbol{G}$. Though minimal losses is pursued, we should first guarantee the spectrum constraint is satisfied, i.e. a node cannot set up new connections once it has already set up K connections (refer to Line 2-4). In order to minimize the total value in $\boldsymbol{T}_v$, we set the weight of links ending at a node in $\boldsymbol{T}_v$ close to the sum of all the demand value, which leads the path of each demand to be minimal hop first in $\boldsymbol{T}_v$. Also, we plus the node value on the weight to balance the value in $\boldsymbol{T}_v$, Since in this case, the node with less value will be used first if multiple path is with the same hop (Line 5-7). If a node is out of $\boldsymbol{T}_v$ and will not enter into $\boldsymbol{T}_v$ even it relays the demand being routed, it can be used with little cost. Accordingly, we can only set a small weight to the links connecting to these nodes (Line 8-10). Otherwise, we should set weight to links under the Guideline 3 discussed in previous subsection. When $W_{Threshold}$ is much larger than the value of demand being routed, we set large weight to the link connecting to nodes out of $\boldsymbol{T}_v$ and lead demand to use the node in $\boldsymbol{T}_v$. If the value of demand being routed is less than $W_{Threshold}$,, we should reduce the weight of such link to make demand be relayed by the nodes out of $\boldsymbol{T}_v$ (Line 11-14).

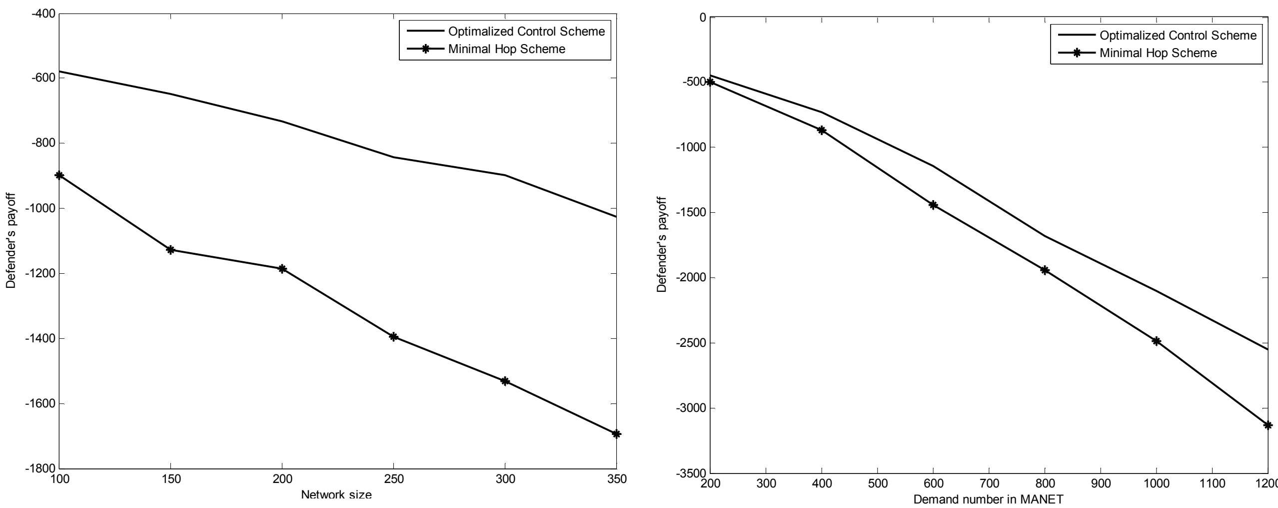
VI. SIMULATION

In this section, we evaluate the performance to defend attacks of our proposed method in MANETs. Firstly, we will compare our topology and routing method with the minimal hop method in subsection VI.A. In subsection VI.B, we will evaluate the benefit brought by the mobility of each node in MANETs. We will also discuss the impact of defending cost 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, each node can set up channels to the nodes within 400m and can set up channels to at most 4 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

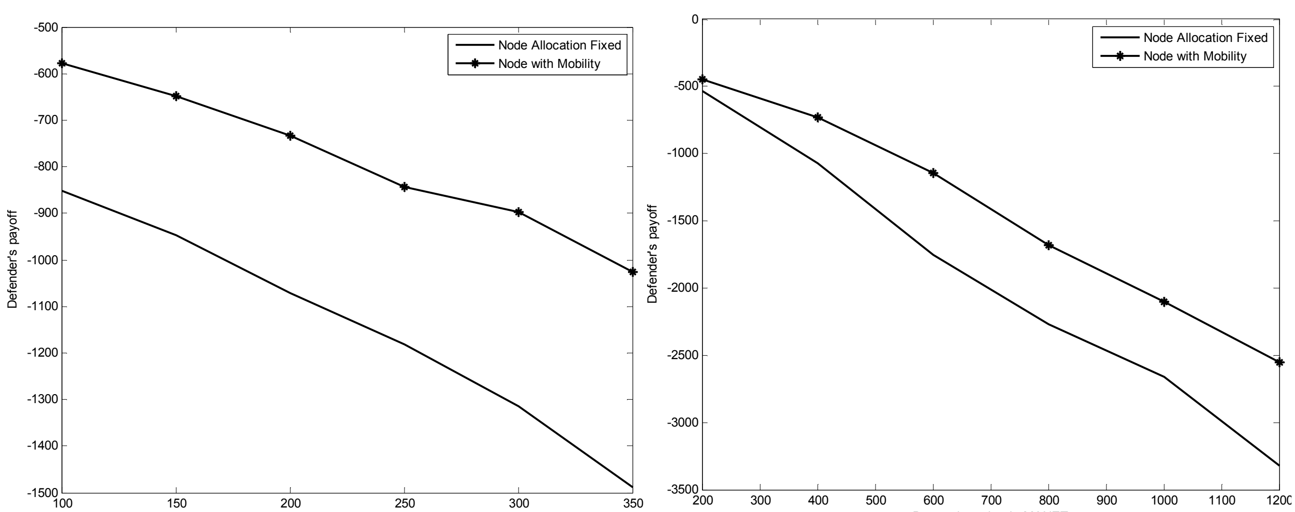
In this subsection, we evaluate the performance of our topology and routing control method on enhancing the payoff of defender in MANETs with different number of nodes. The



(a) Algorithm performance vs. network size

(b) Algorithm performance vs. demand number

Fig. 2 Performance of connection and routing control



(a) Defender's payoff vs. network size

(b) Defender's payoff vs. demand number

Fig. 3 Benefit brought by nodal mobility 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 change 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 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 100m and C_a=C_p=0.005. As a benchmark, we also test the scheme that defender only use the path with minimal hop to route its demand.

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, defender may loss more payoffs when it does not catch the attacker.

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

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

B. Performance Improvement brought by nodal mobility

In this subsection, we evaluate the 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 can be selected as its relaying nodes and there will be larger optimization space for defender to reduce its payoff loss. At first, we take the case that every node in the network cannot move (i.e. set r_i=0 for all *i*) as a baseline to study the benefit brought by nodal mobility in different size network. We also set C_a=C_p=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 reduce defender's loss 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 that in the small size network. It is also because that there will be more optimization space when the network size is relatively larger and more demands in the network.

In Fig.3(b), similar results with Fig.3(a) can be yielded. Nodal mobility will bring about 16.53% to 34.98% performance improvement to defender and the more demand in the network, the larger performance improvement there will be, due to the larger optimization space.

On the other hand, 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 distance all nodes moving are shown in Fig.4. In this figure, we see that 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 excess a threshold (500m in our simulation), longer maximum distance will not bring benefit to defender since there remains no optimization space that can be seized by node's movement.

C. Impact of Routing Information

In subsection IV.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. But there remains an interesting question that how much benefit defender can get from attacker's lack of demand routing information. In this subsection, we study this question 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, so that we assume each node is with the same probability to be attacked. On the other hand, defender does not know whether attacker knows demand routing information. Therefore, it will stick to the strategy it should choose at Nash equilibrium.

In this situation, the defender's payoff is shown in Fig. 5. From this figure we can see that defender will suffer from a much larger payoff loss if attack has demand routing information than the case that attacker has no demand routing information. Another observation is that without demand

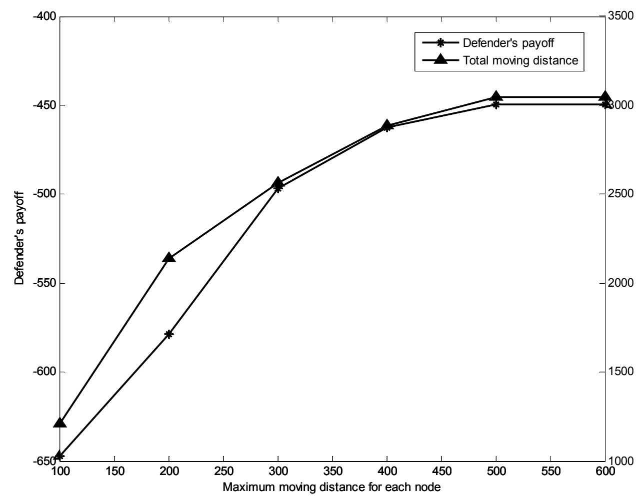


Fig. 4 Impact of maximum moving distance of each node

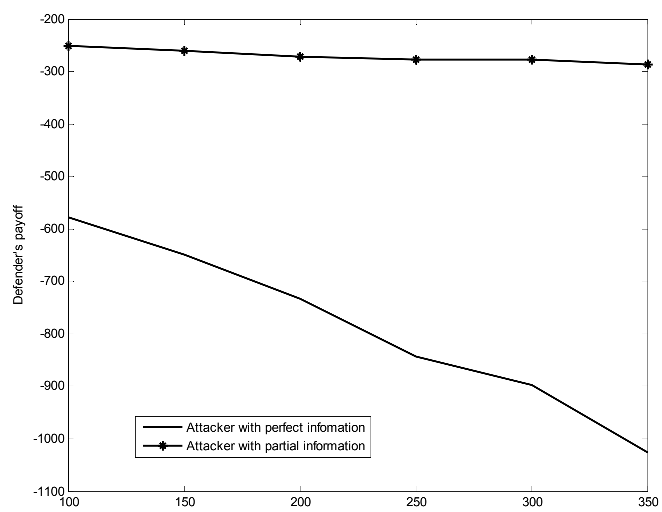


Fig.5 Impact of routing information

routing information, attacker cannot bring significant larger payoff loss to 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 to protect the demand routing information is also an efficient method to counter malicious attack.

VII. Conclusion

In this paper, we formulated the interaction between the attacker and the defender in MANETs as a two-player non-zero-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 defender's loss under attacking. 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 hide the demand routing information is also an efficient method to reduce defender's loss.

References

[1] Liqiang Zhao; Jie Zhang; Kun Yang; Hailin Zhang, "Using Incompletely Cooperative Game Theory in Mobile Ad Hoc Networks," *Communications, 2007. ICC '07. IEEE International Conference on* , vol., no., pp.3401,3406, 24-28 June 2007

[2] Hao Yang; Haiyun Luo; Fan Ye; Songwu Lu; Lixia Zhang, "Security in mobile ad hoc networks: challenges and solutions," *Wireless Communications, IEEE* , vol.11, no.1, pp.38,47, Feb 2004

[3] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," ACM MOBICOM, 2001.

[4] M. Zapata, and N. Asokan, "Securing Ad Hoc Routing Protocols," ACM WiSe, 2002.

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

[6] W. Yu and K. J. R. Liu, "Attack-Resistant Cooperation Stimulation in Autonomous Ad Hoc Networks," IEEE J. Select. Areas Commun.: Autonomic Communication Systems, vol. 23, pp. 2260–2271, Dec. 2005.

[7] Z. Ji, W. Yu, and K. J. R. Liu, "An optimal dynamic pricing framework for autonomous mobile ad hoc networks," in Proc. IEEE INFOCOM'06, Barcelona, 2006.

[8] Minda Xiang; Yu Chen; Wei-Shinn Ku; Zhou Su, "Mitigating DDoS Attacks Using Protection Nodes in Mobile Ad Hoc Networks," *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE* , vol., no., pp.1,6, 5-9 Dec. 2011

[9] Eissa, T.; Razal, S.A.; Ngadi, M.A., "Enhancing MANET Security Using Secret Public Keys," *Future Networks, 2009 International Conference on* , vol., no., pp.130,134, 7-9 March 2009

[10] Manel Guerrero Zapata. 2002. Secure ad hoc on-demand distance vector routing. *SIGMOBILE Mob. Comput. Commun. Rev.* 6, 3 (June 2002), 106-107.

[11] Feng Li; Yinying Yang; Jie Wu, "Attack and Flee: Game-Theory-Based Analysis on Interactions Among Nodes in MANETs," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on* , vol.40, no.3, pp.612-622, June 2010

[12] Xun Xiao; Minming Li; Jianping Wang; Chunming Qiao, "Optimal resource allocation to defend against deliberate attacks in networking infrastructures," *INFOCOM, 2012 Proceedings IEEE* , vol., no., pp.639-647, March 2012

[13] Lin Chen; Leneutre, J., "A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks," *Information Forensics and Security, IEEE* Transactions on , vol.4, no.2, pp.165,178, June 2009

[14] Zeki Bilgin, Bilal Khan, and Ala Al-Fuqaha. 2010. Using connection expansion to reduce control traffic in MANETs. In *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference* (IWCMC '10). ACM, New York, NY, USA, 534-538.

[15] Ratica, J.; Dobos, L., "Mobile Ad-Hoc Networks Connection Admission Control Protocols Overview," Radioelektronika, 2007. 17th International Conference , vol., no., pp.1,4, 24-25 April 2007

[16] Erik Nordström, Per Gunningberg, and Christian Tschudin. 2004. Comparison of forwarding strategies in internet connected MANETs. *SIGMOBILE Mob. Comput. Commun. Rev.* 8, 4

[17] Agarwal, S.; Katz, R.H.; Krishnamurthy, S.V.; Dao, S.K., "Distributed power control in ad-hoc wireless networks," Personal, Indoor and Mobile Radio Communications, 2001 12th IEEE International Symposium on , vol.2, no., pp.F-59,F-66 vol.2, Sep/Oct 2001

[18] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. 2005. Ariadne: a secure on-demand routing protocol for ad hoc networks. *Wirel. Netw.* 11, 1-2 (January 2005), 21-38.

[19] Fei Xing, Wenye Wang, "On the Survivability of Wireless Ad Hoc Networks with Node Misbehaviors and Failures," IEEE Transactions on Dependable and Secure Computing, vol. 7, no. 3, pp. 284-299, July-September, 2010

[20] John Nash, "Non-Cooperative Games", *The Annals of Mathematics*, Second Series, Volume 54, Issue 2, 286-295, Sep. 1951.

[21] G.H.Hardy, J. Littlewood, and G. Plya, Inequalities. Cambridge University Press, 1952