A routing defense mechanism using evolutionary game theory for Delay Tolerant Networks

Hang Guo[a], Xingwei Wang[a], Hui Cheng[b], Min Huang[a]
[a]College of Information Science and Engineering, Northeastern University, Shenyang, China
guohang0001@126.com, {wangxw, mhuang}@mail.neu.edu.cn
[b]School of Computing and Mathematical Sciences, Liverpool John Moores University, Liverpool, UK
h.cheng@ljmu.ac.uk

Abstract—Delay Tolerant Networks (DTNs) often suffer from intermittent disruption due to factors such as mobility and energy. Though lots of routing algorithms in DTNs have been proposed in the last few years, the routing security problems have not attracted enough attention. DTNs are still facing the threats from different kinds of routing attacks. In this paper, a general purpose defense mechanism is proposed against various routing attacks on DTNs. The defense mechanism is based on the routing path information acquired from the forwarded messages and the acknowledgment (ACK), and it is suitable for different routing schemes. Evolutionary game theory is applied with the defense mechanism to analyze and facilitate the strategy changes of the nodes in the networks. Simulation results show that the proposed evolutionary game theory based defense scheme can achieve high average delivery ratio, low network overhead and low average transmission delay in various routing attack scenarios. By introducing the game theory, the networks can avoid being attacked and provide normal transmission service. The network can reach evolutionary strategy stable (ESS) under special conditions after evolution. The initial parameters will affect the convergence speed and the final ESS, but the initial ratio of the nodes choosing different strategies can only affect the game process.

Keywords–Delay Tolerant Networks; Evolutionary game; Routing attack; Routing security; Evolutionary strategy stable

1. INTRODUCTION

Delay Tolerant Networks (DTNs) [1] are designed to cope with the challenging conditions in the restricted networks with sparse density, intermittent disruption and limited energy. DTNs can be used in military, industry, transport, monitor, deep space communication and other challenging networks environments [2]. The messages are relayed hop by hop by means of the store-carry-forward mechanism. Importantly, routing is the main challenge in DTNs due to the characteristics of DTNs. The routing techniques in traditional networks cannot work effectively in DTNs since it is extremely difficult to determine the potential end to end path towards the destination [3].

The unique features of DTNs result in unique security challenges [4]. DTNs have features such as multiple hops, self-organization, and no central administration. However, in most cases DTNs are deployed in the open environment, and security problems are tough issues. The security threats of DTNs are different from those of traditional wireless networks because of the unique features, so the traditional methods to deal with network security threats are not necessarily effective and alterations need to be made [5]. As shown in Fig. 1, there are different types of DTNs security problems, and they should be sufficiently considered in different network layers. In the physical layer, the main problems are wireless communication jamming and nodes being compromised. In the link layer, the main problems are collision and wireless resource allocation. In the routing layer, the main problems are the routing attacks and routing security. The various routing attack countermeasures are discussed in this paper.

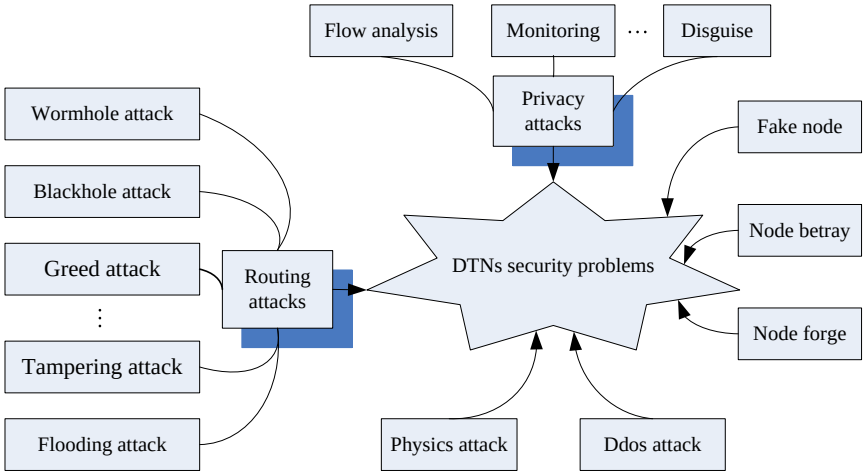

Fig.1 A summary of security problems in DTNs

Packets in DTNs are opportunistically routed towards the destination, making them robust against simple attacks such as packet dropping attacks [6]. However there are still a number of routing attack methods in DTNs. The primary attack methods include wormhole attack, blackhole attack, greed attack, tampering attack and so on. These routing attacks will severely affect the network performance [7]. In this paper, a general solution to deal with routing attacks in DTNs is proposed. First, a proactive defense mechanism is established based on the routing path information and the ACK information. Then, the evolutionary game theory is introduced with the defense mechanism to solve the routing attack problems in DTNs.

The rest of this paper is structured as follows. Section II outlines the current state of routing security in DTNs. In Section III, the defense mechanism is proposed and different strategies of nodes are analyzed in the evolutionary game system. The simulation results under various realistic scenarios are presented in Section IV, followed by the conclusions and future work in the last section.

2. RELATED WORK

The current research on DTNs mostly focuses on routing algorithms [8], and the routing security problems have not attracted enough attention. There are mainly two ways to cope with the routing attacks in DTNs. One is to use different methods to detect malicious nodes and isolate them, and the other is to use incentive mechanism to encourage all the network nodes to participate in the information transmission. Recently the game theory has also been used in the DTNs routing security filed.

The methods to detect malicious nodes in DTNs include probabilistic detection, ferry-based detection，reputation-based detection and reference-based detection and so on. Gao et al. [9] propose a probabilistic misbehavior detection scheme. In this scheme, the trusted authority collects every node's routing credentials periodically and judges the nodes' behavior through the information analysis. An intrusion detection system which utilizes the correlation of delivery probability between the nodes is proposed by Kuriakose and Danie [10] to mitigate flood attack in DTNs. Saha [11] et al. propose a table-based strategy to record network history and use this information to detect discrepancies in the behavior of nodes, followed by elimination of those detected as malicious. Chuah et al. [12] propose a message-ferry-based detection method. This scheme assumes that some dependable mobile nodes exist in the network, and these dependable nodes collect the history delivery information of the nodes they encounter, and then the malicious nodes can be distinguished according to the information collected by dependable nodes. Ren et al. [13] take the node's transitivity into consideration and propose a mutual correlation detection scheme. This method can update the transfer probability between the nodes and improve the detection accuracy. Because this type of methods need to use the dependable nodes as ferry nodes, this will lead to extra cost. Meanwhile the efficiency of these methods will decrease in the sparse networks environment. In the reputation-based routing algorithm, Xu et al. [14] propose a secure reputation-based dynamic window scheme. In this scheme, if one node wants to estimate another node's reputation, it should firstly gather all other neighbor nodes' evaluations to this node, and then do the estimation. During the process of routing, the nodes with high reputation will be chosen as relay nodes. Here the reputation can be global or local. The global case will need reliable hardware to spread the reputation, and the local case does not need the support of the hardware. Nagrath et al. [15] design a secure reputation based algorithm that handles flooding attack in distributive and transitive manner, in which it is assumed that the malicious node can flood the network with bogus nodes but is not capable of generating genuine messages. Guo et al. [16] propose a Misbehavior Detection System based on encounter record-based reputation system to protect the security of the hybrid network. In the reference-based DTNs routing algorithm, if one node wants to provide relay service, it should firstly send its reference value to surrounding neighborhood nodes. This reference value is used to certify that the node has taken part in the delivery of messages. Li et al. [17] propose a reference-based method using encounter tickets. Ren et al. [18] propose a reference-based method using packet exchange recording.

The incentive mechanism can improve the performance of DTNs by means of punishment or incentive. Upendra et al. [19] apply the TFT (tit-for-tat) strategy to DTNs. In the scheme, node *A* will forward messages for its neighbor node if the neighbor node has forwarded messages for node *A* and vice versa. Based on the TFT strategy, the author proposes incentive-aware routing protocol which can make the selfish nodes' benefit obey the TFT restriction. Zhu et al. [20] propose a secure credit-based incentive scheme, which uses virtual currency consisting of several layers of information to pay and reward the node that forwards messages in DTNs. The information of virtual currency contains the source node and destination node, the service needed, and the credit value obtained by forwarding the message. The authors subsequently further improve this scheme by permitting relay node to transfer and distribute the virtual currency. Lu et al. [21] propose a practical incentive protocol for DTNs which contains a fair incentive model. The source node will add incentive information to the to-be-sent message to encourage the selfish nodes to forward the message. If the message successfully reaches the destination node, all relay nodes will receive reward from the source node. If the message transmission fails, the relay nodes participating in the forward will achieve the reputation from the trusted agency.

Game theory has been mainly studied and applied in economics, politics and sociology, which has recently emerged as a useful tool in analyzing modern wireless networks since it provides analytical tools to model interactions among entities with conflicting interests that compete for the limited network resources. There is a survey on the game theory used in wireless sensor networks (WSNs) to achieve a tradeoff between maximizing the network lifetime and providing the required service [22]. An active defense model is presented in [23] for the WSNs based on the evolutionary game theory. The game theory is used to deal with the rational providers in the smart cloud storage service selection process. To solve the free-rider phenomenon in the P2P file-sharing applications, Wu et al. [24] propose a Novel Incentive Mechanism (NIM) based on social network and game theory, which can restrain the number of free riders efficiently and encourage the nodes to contribute resources as much as possible. Esposito et al. [25] use the game theory to promote truth-telling ones among service providers in the smart cloud storage service selection. R. azzouzi et al. [26] propose a general framework for competitive forwarding in DTNs under the two hops routing, which focus on the probability to deliver a message, and a utility function is introduced as the difference between a reward unit and the energy cost. Wu et al. [27] introduce an asymmetric multi-community evolutionary game framework and a two-hop routing algorithm. By adopting asymmetric multi-community evolutionary game, the proposed mechanism can find each community's unique evolutionary stable strategy (ESS) and provide the existence conditions. Zuo et al. [28] introduce an evolution game-based routing model to eliminate selfish routing behaviors and improve routing efficiency in P2P networks. The routing behaviors of nodes are considered as a non-cooperative routing game, in which self-interested player's route traffic goes through a congestion-sensitive network. The dynamical behaviors of nodes are studied by adopting a generalized approach of imitative dynamics.

The previous algorithms have taken many factors into consideration regarding the DTNs routing security and put forward a lot of assumptions. However, most of the DTNs are deployed in the challenging network environments, the extra infrastructures required by many security mechanisms are difficult to deploy and operate, for example, the public key infrastructure. Meanwhile, most of the proposed game theory based algorithms just can deal with one specific routing attack mode, or just for one specific routing scheme. In this paper, a general purpose routing defense mechanism that can cope with multiple attack techniques is proposed, which requires no infrastructure support and can be applied to any routing scheme. Due to the lack of transmission opportunity, simply isolating the malicious nodes is not appropriate for DTNs. The evolutionary game theory is introduced to incent as many as possible nodes to participate in communication so as to confront the routing attacks.

3.THE PROPOSED ALGORITHM

The following assumptions have been made in the proposed algorithm.

1. The security of the message is guaranteed by the bundle protocol (BP). Therefore, the content of the message transmitted in the networks is correct and not tampered.

2. All the nodes in the network are of bounded rationality and can be classified into two groups, i.e., normal nodes and malicious nodes. The normal nodes get payoff by forwarding the messages. The malicious nodes get payoff by attacking or forwarding the messages, and the payoff by attacking the networks is higher.

3. The payoff of forwarding one message is proportional to the size of the message, and the payoff of every unit is the same.

4. The nodes can retrieve routing path information from the forwarded messages and ACKs in the network.

3.1. The defense mechanism for DTNs

The most important factors affecting the DTNs routing algorithms are the nodes' contacts and the forwarding sequences of the messages. So these two factors are focused on in the defense strategy. In the DTNs, a message will be transferred from the source node to the destination node by store-carry-forward mechanism. Upon successful delivery of a message, an ACK message will be generated and flooded to other nodes. The routing path information such as the source node, the relay nodes, and the destination node can be retrieved from the ACK message. When a node receives a message, it will first search the routing information field of the message. Then the routing information in the message will be analyzed and the nodes' behaviors will be concluded.

Firstly, the routing path data of different nodes is collected from the forwarded messages and the ACKs. When two nodes meet each other, they will exchange the messages carried. The routing information can be retrieved from the message header. The message format is shown in Fig. 2.

Endpoint Identifier	TTL	Routing information	Hop Count	Creation Time	Receiving Time	Bundle Payload

Fig. 2 Format of message

When a message reaches the destination node, the destination node will generate multiple ACK messages and put the whole routing path information into the ACK messages and then flood them into the networks. Thus when one node receives the ACK, it can get the routing path of the message that has been successfully transferred to the destination node.

Secondly, based on the routing information obtained from the forwarded messages and the ACK messages in the networks, the aforementioned nodes can be evaluated. Here two lists are created, one is based on the routing information of the forwarded messages and the other is based on the ACK messages.

In the first list, the nodes that have been recorded in the routing information will be sorted by a certain principle. The principle here is that the node which has participated in more message transmissions will have higher rank in the list. Then a node's participation value by its rank can be achieved. In the second list, the nodes that have been recorded in the ACK messages will also be sorted by the same principle as used in the first list. One value will be calculated for every node appearing in the ACKs.

Finally, every node's total participation value can be calculated by the two values obtained in the above two steps. The P_v is used to denote the total participation value of each node and is defined as below:

$$P_v = \alpha P_r + \beta P_a \tag{1}$$

Here, P_r denotes the participation value obtained from forwarding messages, P_a denotes the participation value obtained from ACK messages, and α and β are the weight coefficients.

The proposed defense strategy is described as follows. When two nodes *a* and *b* meet each other, node *a* which uses defense strategy will first check the P_v value of node *b*. If P_v is smaller than the thresholds value T_p, node *a* will not establish communication with node *b* and will wait for another chance. If P_v is greater than the thresholds T_p, node *a* will establish communication with node *b* and then exchange each other's messages vectors. Then node *a* will decide which messages to be sent to node *b* and sort the messages based on the P_v value of the message's destination node. The defense strategy is formally described in Algorithm 1.

Algorithm 1 The defense strategy

Input: P_v, T_p

1: **Procedure** DefenseStrategy

2: **for** each contact node *i* with defense strategy meeting node *j*

3: **if** $P_v(j) > T_p$ t**hen**

4: establish communication with node *j*.

5: sort the messages $M(i)$ in node i based on the P_v value of the message's destination node.

6: send $M(i)$ in priority order to node j.

7: **else**

8: wait for another chance.

9: **end if**

10: **end for**

11: **end procedure**

Since the path information that one node can collect is limited, the data size in the list is relatively small. The simple Bubble Sort algorithm is used in the sorting process. The algorithm complexity of the above routing defense strategy is $o(n^2)$ where n is the number of nodes.

3.2. The routing defense scheme based on evolutionary game theory

Because of the features of DTNs, the networks may be sparse and there are very few opportunities of making connectivity. The scheme that just simply isolates the malicious nodes is inappropriate. Instead, the malicious nodes especially the selfish nodes should be involved in the message transmission. The key of the problem is to balance the interests between the malicious nodes and the normal nodes, and the game theory is suitable for this purpose.

The Nash equilibrium theory points out that if the balance point exists in a system [29], it indicates that the whole system's interest can achieve optimum at this point. Because the network topology in DTNs is constantly changing and the network nodes are not completely rational, traditional game theory is not suitable for DTNs. However, the evolutionary game theory is appropriate because the dynamics of the evolutionary game and the bounded rationality of the nodes can match the DTNs' features. In the evolutionary game theory, the evolutionary strategy stable (ESS) is used to replace Nash equilibrium. The ESS reflects the convergence status of the network after evolution, and it means that the whole system can return to original stable status when few nodes change their strategies. Therefore, when al1 the nodes are in the ESS condition, the optimum network performance can be guaranteed.

The normal nodes in DTNs should protect themselves from the attack of malicious nodes. So the defense mechanism proposed in Subsection 3.1 is introduced as a strategy for the normal nodes. Certainly, extra network resources will be consumed when the defense strategy is introduced to the routing process. So the balance point should be determined for the nodes to decide whether they need to adopt the defense strategy.

Generally the game model is composed of four factors: players, strategy space, payoff function and evolutionary selection dynamics. The players can be divided into two types of groups. One is the attacker (malicious nodes) group and the other is the defender (normal nodes) group. The parameters of attacker and defender are defined as follows. R denotes the reward of

forwarding one message; C_T denotes the cost of forwarding one message; C_D denotes the cost of defender; C_A denotes the cost of attacker. Normally, $R > C_D$, $R > C_T$, $R > C_A$, $C_D > C_A$, $C_T > C_A$.

If the defense strategy is not employed, the attacker can choose from three strategies: attack (A), cooperation (C) and non-cooperation (NC). So the strategy space $S_A = \{A, C, NC\}$. The defender group can choose cooperation strategy or non-cooperation strategy, so the strategy space of defender $S_D = \{C, NC\}$. In this situation, all the network nodeswill choose non-cooperation strategy after a finite number of gaming [30]. The strategy profile $\{NC, NC\}$ will be the ESS solution for the game. However the networks cannot provide basic forwarding service in this situation.

In order to avoid the above-mentioned dilemma, the defense strategy (D) proposed in previous subsection is introduced to restrict the attack behavior of malicious nodes. By this way, the attack behavior will be unprofitable and this will prompt the malicious nodes to cooperate with others. Then the network can work properly and the performance will be improved. Because the defender has three strategies from the strategy space $S_D = \{C, NC, D\}$, the payoff matrixes of the defender and the attacker are defined as A and B respectively:

$$A = \begin{bmatrix} R-C_T & R-C_T & 0 \\ -C_T & -C_A & 0 \\ R-C_T & -C_A & 0 \end{bmatrix} \tag{2}$$

$$B = \begin{bmatrix} R-C_T & -C_T & -C_T \\ 0 & 0 & 0 \\ R-C_D & -C_D & -C_D \end{bmatrix} \tag{3}$$

Assume that the proportions of the normal nodes that choose cooperation, non-cooperation and defense strategies are x_1, x_2 and x_3 separately, and the proportions of the malicious nodes that choose cooperation, attack and non-cooperation strategies are y_1, y_2 and y_3 separately, then $x_1, x_2, x_3, y_1, y_2, y_3$ will satisfy:

$$\begin{cases} x_1 + x_2 + x_3 = 1 \\ y_1 + y_2 + y_3 = 1 \end{cases} \tag{4}$$

Replicator dynamics describe a dynamic selection process, which is proposed by Taylor and Jonker [31]. At time t, let $p_i(t)$ be the number of individuals who are currently programmed to strategy $i \in K$, and let $p(t) = \sum_{i \in K} P_i(t)$ be the total population. Then the associated population state is defined as the vector $z(t) = (z_i(t) \ldots, z_k(t))$, where each component $z_i(t)$ is the population share, i.e., $z_i(t) = p_i(t) / p(t)$. The $u(z, z)$ is defined as the average payoff of the population and the $u(s_i, z)$ is defined as the expected payoff using strategy i. The replicator dynamics in evolutionary game can be expressed as:

$$\frac{dz_i}{dt} = [u(s_i, z) - u(z, z)]z_i \tag{5}$$

Based on Eq. (2), (3), (4), (5), the overall dynamic replication equations for defenders and attackers can be derived:

$$\begin{cases} f(x_h) = \dfrac{dx_h}{dt} = [\sum\limits_{k \in S_A} a_{hk} y_k - \sum\limits_{j \in S_D} \sum\limits_{k \in S_A} x_j a_{jk} y_k] x_h \\ f(y_k) = \dfrac{dy_k}{dt} = [\sum\limits_{h \in S_D} b_{hk} x_h - \sum\limits_{j \in S_A} \sum\limits_{k \in S_D} y_j b_{kj} x_k] y_k \end{cases} \tag{6}$$

Here h, k, j = 1, 2, 3; a and b are the corresponding elements of the matrixes A and B. So the dynamic replication equations for $x_1, x_2, x_3, y_1, y_2, y_3$ can be listed as below:

$$\begin{aligned} f(x_1) &= [x_1 y_1 - x_1^2 y_1 - x_1 x_3 (y_1 + y_2)] R - (x_1 - x_1^2) C_T + x_1 x_3 C_D \\ f(x_2) &= -[x_1 x_2 y_1 + x_2 x_3 (y_1 + y_2)] R - x_1 x_2 C_T + x_2 x_3 C_D \\ f(x_3) &= [x_3 (y_1 + y_2) - x_1 x_3 y_1 - x_3^2 (y_1 + y_2)] R + x_1 x_3 C_T - (x_3 - x_3^2) C_D \\ f(y_1) &= [(x_1 + x_3) y_1 - y_1^2 (x_1 + x_3) - x_1 y_1 y_2] R - (y_1 - y_1^2) C_T + y_1 y_2 C_A \\ f(y_2) &= [x_1 y_2 - y_1 y_2 (x_1 + x_3) - x_1 y_2^2] R - (y_2 - y_2^2) C_T + y_1 y_2 C_A \\ f(y_3) &= -[(x_1 + x_3) y_1 y_3 + x_1 y_2 y_3] R + y_1 y_3 C_T + y_2 y_3 C_A \end{aligned} \tag{7}$$

As part of the theoretical analysis, the following theorems are derived.

Theorem 1: if one point is the equilibrium point of the game system, it should meet the following equation:

$$\frac{dz_i}{dt} = 0 \tag{8}$$

For the proposed evolutionary game model, the possible equilibrium points can be calculated from Eq. (7) and (8), and the results are shown as follows: ($x_1, x_2, x_3, y_1, y_2, y_3$) = (1,0,0,1,0,0), (1,0,0,0,1,0), (1,0,0,0,0,1), (0,1,0,1,0,0), (0,1,0,0,1,0), (0,0,0,0,0,1), (0,0,1,1,0,0), (0,0,1,0,1,0), (0,0,1,0,0,1). Certainly not all the equilibrium points are ESS points, but every ESS point must be the equilibrium point.

Theorem 2: if one equilibrium point is the ESS point, it should meet the following condition:

$$\begin{cases} Trace(J) < 0 \\ Det(J) > 0 \end{cases} \tag{9}$$

Here matrix J is the Jacobi matrix of the game system. The $Trace(J)$ is defined to be the sum of the elements on the main diagonal of matrix J and the $Det(J)$ is defined to be the determinant of matrix J.

$$J = \begin{bmatrix} \dfrac{\partial f(x_1)}{\partial x_1} & \dfrac{\partial f(x_1)}{\partial x_2} & \cdots & \dfrac{\partial f(x_1)}{\partial y_3} \\ \dfrac{\partial f(x_2)}{\partial x_1} & \dfrac{\partial f(x_2)}{\partial x_2} & \cdots & \dfrac{\partial f(x_2)}{\partial y_3} \\ \vdots & \vdots & \ddots & \vdots \\ \dfrac{\partial f(y_3)}{\partial x_1} & \dfrac{\partial f(y_3)}{\partial x_2} & \cdots & \dfrac{\partial f(y_3)}{\partial y_3} \end{bmatrix}$$

Theorem 3: when $C_T > C_D$, all the normal nodes will choose defense strategy and all the malicious nodes will choose cooperation strategy after the evolution ends. In other words, the point (0, 0, 1, 1, 0, 0) is the only evolutionary strategy stable point for the system.

Proof:

First, the existence is proved as below.

According to Eq. (8), the following equation can be derived:

$f_{x_1}(0,0,1,1,0,0) = 0$

And at this point,

$Trace(J) = -5R + 3C_D - C_A$

$Det(J) = (R - C_D)^2 (R - C_T)^2 (R + C_T + C_A)(C_T - C_D)$.

$\because \quad R > C_T, \quad R > C_D,$

$\therefore \quad Trace(J) < 0$.

If $C_T > C_D$, $Det(J) > 0$.

So the point (0, 0, 1, 1, 0, 0) is one of the evolutionary strategy stable points for the system.

Second, the uniqueness is proved as below.

At points (1, 0, 0, 0, 0, 1), (0, 1, 0, 0, 0, 1), (0, 1, 0, 1, 0, 0), (0, 1, 0, 0, 1, 0), (0, 1, 0, 0, 1, 0), (0, 0, 1, 0, 0, 1), $Det(J) = 0$.

At point (1, 0, 0, 0, 1, 0), $Trace(J) = -R + 2C_A + C_T - C_D$, $Det(J) = -C_T^2 (R - C_A)(R - C_T)(R + C_T - C_D)(C_T - C_A) < 0$.

At point (1, 0, 0, 1, 0, 0), $Trace(J) = -3R + C_T$, $Det(J) = -(R - C_T)^2 (R + C_T - C_D)(C_T - C_D)R < 0$.

At point (0, 0, 1, 0, 1, 0), $Trace(J) = -2R + 2C_A - C_T + C_D$, $Det(J) = -C_T C_A (R^2 - C_D^2)(R + C_T - C_D)(R + C_A - C_T) < 0$.

Therefore, the point (0, 0, 1, 1, 0, 0) is the only ESS point in this system.

Theorem 4: when $C_T < C_D$, all the nodes will choose cooperation strategy after the evolution ends. In other words, the point (1, 0, 0, 1, 0, 0) is the only evolutionary strategy stable point for the system.

***Proof*:** It is similar to the proof process in Theorem 3.

According to Theorem 3 and Theorem 4, when the cost of forwarding messages is higher than the cost of defending, all the normal nodes in the network will choose defense strategy and all the malicious nodes will choose cooperation strategy eventually after the evolution. However, if the cost of forwarding message is higher than the cost of defending, all the nodes will choose cooperation strategy in the end.

4. SIMULATION AND ANALYSIS

The simulation experiments are implemented by the ONE simulator [32]. The ONE is superior in supporting DTNs compared to the NS2, OMNET++ and DTNSim. The ONE allows users to create scenarios based upon different synthetic movement models and real-world traces and offers a framework for implementing routing and application protocols. It is able to interact with other programs and data sources.

The representative routing scheme Spray and Focus (SAF) and map-based movement model are implemented in the simulation. The proposed scheme will be carried out in different situations and compared with the SRSnF strategy. In the experiments, the network having no malicious nodes is named NM, and the network having malicious nodes but no defense mechanism is named HMND, and the network having malicious nodes and defense mechanism is named HMD. Twenty malicious nodes are randomly chosen from 200 nodes, and the attack methods include blackhole attack, wormhole attack and greed attack. The whole simulation time is 45000 seconds and the warm-up time is 1000 seconds. The detailed parameter settings are summarized in Table 1.

TABLE 1 Simulation parameters

Parameter	Setting
Simulation area	10, 000 × 8, 000 m
Node storage	50 M
Node bandwidth	2 Mbps
Node velocity	0.5 ~ 1.5 m/s
Transmission radius	20 m
Message size	0.5 ~ 1 M
Generation interval	15 ~ 45 s
Message TTL	3, 600 s
Energy per Node	10000 mA/h
Scanning Energy:	10 mA/h
Transmission Energy	20 mA/h

The performance metrics used in the evaluation are message average delivery ratio (ADR), message average transmission delay (ATD), and network overhead ratio (NOR). The ADR is defined as the average ratio of the messages successfully delivered to the destination to the total messages, and the ATD is defined as the average time between when a message is generated by the source node and when it is received by the destination, and the NOR is defined as the ratio of the messages forwarded to the messages successfully delivered. The proposed defense mechanism and the applied evolutionary game theory in DTNs will be evaluated in terms of these metrics. The influence on the algorithm brought by different parametr values will

be investigated. The initial proportions by which the nodes choose different strategies are also important factors which will be investigated as well.

The set (X, Y) = (x_1, x_2, x_3, y_1, y_2, y_3) denotes the proportions by which the nodes choose different strategies, and the detailed definition is shown in Subsection 3.2. Because the measurement standard is different under different conditions, the normalized standard is used and the game parameter values are between [0, 1]. It is assumed that R=1.0 and C_A=0.1 in the simulation. In Subsection 4.1 and 4.2, C_T = 0.4, C_D = 0.2, and in Subsection 4.3, C_T = 0.2, C_D = 0.4.

4.1. Equal initial proportions

In this case, at the beginning of the simulation, (X, Y) is set to be (1/3, 1/3, 1/3, 1/3, 1/3, 1/3). This means that different strategies will be chosen by the nodes in equal opportunities. These values will vary during the game process. Fig. 3 shows the percentage variation of the nodes choosing different game strategies during the game process. The simulation results are shown in Figs. 4-6.

Intuitively, the malicious nodes will conduct attacks in order to maximize their own interests, and then some normal nodes will change their strategies from cooperation to defense in order to reduce the loss. Meanwhile some other malicious nodes will turn to the cooperation strategy after evolution and learning. The majority of the nodes are normal nodes, so some of the normal nodes will alternate their strategies between defense and cooperation, and a few of them will apply non -cooperation when most of their contacts are malicious nodes. However, the evolutionary tendency is that almost all normal nodes choose the defense strategy and all the malicious nodes choose the cooperation strategy. Therefore the network can run properly.

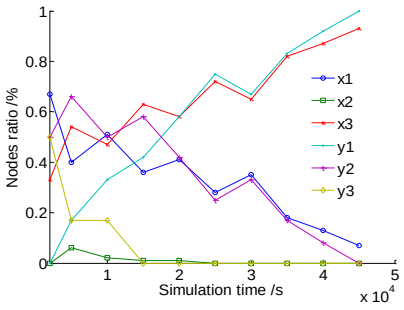

Fig. 3 Nodes ratio in game process

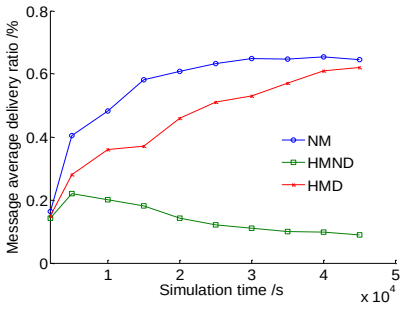

Fig. 4 Message average delivery ratio

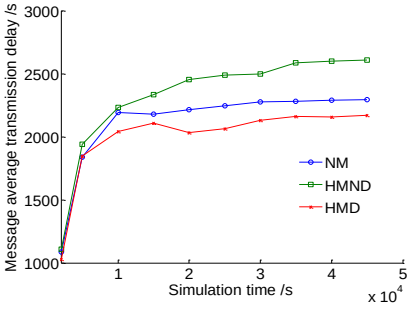

Fig. 5 Message average transmission delay

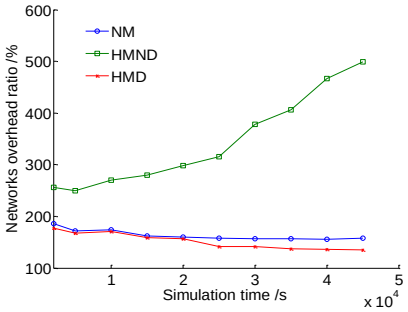

Fig. 6 Network overhead ratio

As shown in Fig. 4, the message average delivery ratio falls drastically when there are some malicious nodes in the network and the network lacks safety measures. The defense mechanism can protect the normal nodes against different routing attacks. The message average delivery ratio increases following the game process. In Fig. 5, the routing attack has no significant impact on the message average transmission delay. The reason is that the DTNs are opportunistic networks and the delay is mainly related to the TTL of the message and the contact frequencies. However, the network overhead ratio is affected by the routing attack severely as shown in Fig. 6. The reason is that the malicious nodes drop many messages in the message forwarding process. But the defense mechanism and the game process alleviate this influence by decreasing the network overhead ratio slightly.

4.2. Half of normal nodes choosing defense and half ofmalicious nodes choosing attack initially

In this case, at the beginning of the simulation, (X, Y) is set to be (1/4, 1/4, 1/2, 1/4, 1/2, 1/4). Firstly half of the normal nodes choose the defense strategy and the rest of them choose the cooperation strategy or the non-cooperation strategy with equal opportunity. Fig. 7 shows the percentage variation of the nodes choosing different game strategies during the game process in this case. The simulation results are shown in Figs. 8-10.

As shown in Fig. 7, the malicious nodes choose the cooperation strategy at a quicker speed after evolution and learning than the speed in the previous case, and the normal nodes alternate their strategies between cooperation and defense. In the end, all the normal nodes choose the defense strategy and all the malicious nodes choose the cooperation strategy in order to maximize their own interests after evolution and learning. Thereafter, normal nodes choose the defense strategy all the time, so the malicious nodes have no opportunity to attack and have to choose the cooperation strategy eventually. The network finally converges to the equilibrium state where normal nodes defend and malicious nodes cooperate. The network can provide normal transmission service without being attacked.

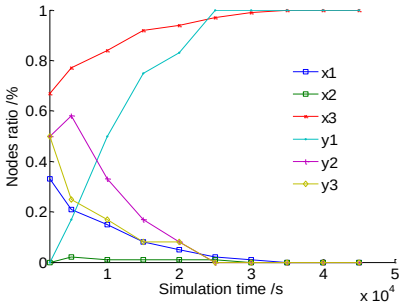

Fig.7. Nodes ratio in game process

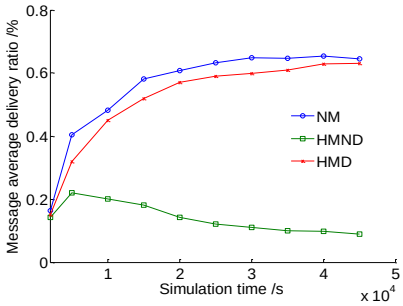

Fig. 8 Message average delivery ratio

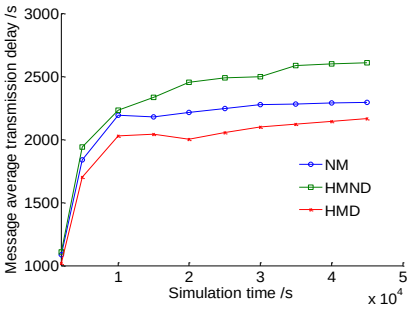

Fig. 9 Message average transmission delay

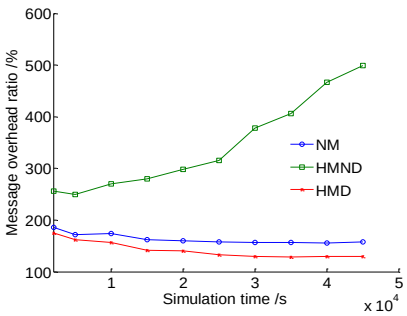

Fig. 10 Network overhead ratio

The simulation results regarding the message average delivery ratio, message average transmission delay and network overhead ratio are shown in Figs. 8-10 separately. The results are similar to the results in the first case. The difference between them mainly lies in the changing speed. In this situation, the message average delivery ratio increases more quickly because the malicious nodes cooperate with other nodes more quickly. The message average transmission delay is approximately the same as in the first case because the delay has barely any relationship with the routing attack. The network overhead ratio is a bit lower because more attacks will create more messages being dropped.

4.3. Changing the game parameters

In this case, at the beginning of the simulation, (X, Y) is set to be (1/4, 1/4, 1/2, 1/4, 1/2, 1/4). The initial percentages of the nodes choosing different strategies are the same as in Subsection 4.2, and the difference is that $C_T = 0.2$ and $C_D = 0.4$. The simulation results are approximately the same as shown in the previous case except the ratios of the nodes choosing different strategies in the game process. Because the ESS point is (1, 0, 0, 1, 0, 0) now, nearly all the nodes choose the cooperation strategy eventually as shown in Fig. 11.

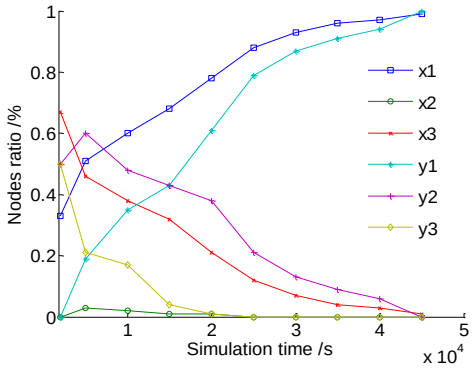

Fig.11. Nodes ratio in game process

Our simulation results can be summarized as follows. First, without the defense mechanism, the routing attacks will obviously decrease the message delivery ratio and network overhead ratio in DTNs. Second, the general defense mechanism can prevent the routing attacks remarkably. Third, with the defense mechanism, using the evolutionary game theory can incent the attackers participating in the message transmission process and thereby improve the network performance. Fourth, different

initial parameters may result in different ESS. Different initial percentages of nodes choosing different strategies will affect the game process, but after evolution and learning the nodes will converge to the same ESS eventually.

5. CONCLUSION AND FUTURE WORK

In this paper, first a general purpose defense mechanism is proposed for Delay Tolerant Networks based on the routing information acquired from the messages forwarded by the relay nodes and the ACKs generated by the destination nodes. Then the proposed mechanism is applied with the evolutionary game theory to form a routing defense scheme which encourages the nodes not to attack but to cooperate with others. The evolutionary process is analyzed and the ESS of the game in different cases is obtained. Simulation results show that the proposed scheme can effectively deal with various routing attack issues and make the malicious nodes participate in the normal data transmission. We plan to carry out the future research work in two directions. One is to investigate other promising intelligent methods and malicious nodes routing attack models. The other is to further expand the mechanism to opportunistic networks.

ACKNOWLEDGMENTS

This work was supported in part by the National Natural Science Foundation of China under Grant No. 61070162, 71071028, 60802023, and 70931001.

REFERENCES

[1] Fall K, Farrell S. DTN: an architectural retrospective. IEEE J.sel.areas Commun, 2008, 26(5): 828-836.

[2] Voyiatzis A G, Voyiatzis A G. A Survey of Delay- and Disruption-Tolerant Networking Applications. Journal of Internet Engineering, 2012, 5: 331-344.

[3] Jin-Shu Su, Qiao-Lin Hu, Zhao B K, et al. Routing Techniques on Delay/Disruption Tolerant Networks[J]. Journal of Software, 2010, 21(1): 119-132.

[4] Gao L, Yu S, Luan T H, et al. Privacy Protected Routing in Delay Tolerant Networks [M]. Springer briefs in Computer Science, 2015: 69-79.

[5] Wen Ding, Cai Ying, Li zhuo. Research on resistance to internal node attack in DTN[J]. Journal of Beijing Information Science and Technology University, 2013, 28(3): 57-63.

[6] Burgess J, Bissias G D, Corner M D, et al. Surviving attacks on disruption-tolerant networks without authentication[C]//In Proc. of MobiHoc' 07, 2007: 61-70.

[7] Choo F C, Chan M C, Chang E C. Robustness of DTN against routing attacks[C]//In Proc. of Communication Systems and Networks (COMSNETS), 2010 Second International Conference on IEEE, 2010: 1-10.

[8] Gao L, Yu S, Luan T H, et al. Routing Protocols in Delay Tolerant Networks[M]. Springer briefs in Computer Science, 2015: 19-34

[9] Gao Zhaoyu, Zhu Haojin, Du Suguo. et al. Pmds: a probabilistic misbehavior detection scheme in DTN[C]//In proc. of IEEE International Conference on Communications, ICC 2012: 4970-4974.

[10] Kuriakose, Divya, Daniel, David. Effective defending against flood attack using stream-check method in tolerant network[C]//In proc. of Green Computing Communication and Electrical Engineering (ICGCCEE), 2014 International Conference on IEEE, 2014: 1-4.

[11] Saha S, Verma R, Sengupta S, et al. SRSnF: A Strategy for Secured Routing in Spray and Focus Routing Protocol for DTN[M]. Advances in Computing and Information Technology, Springer Berlin Heidelberg, 2012: 159-169.

[12] Chuah M, Yang P, Han J. A Ferry-based Intrusion Detection Scheme for Sparsely Connected Ad Hoc Networks[C]//In Proc. of Mobile and Ubiquitous Systems, Annual International Conference on IEEE, 2007: 1-8.

[13] Ren Y, Chuah M C, Yang J, et al. MUTON: Detecting Malicious Nodes in Disruption-Tolerant Networks[C]//In Proc. of Wireless Communications & Networking Conference IEEE, 2010: 1-6.

[14] Xu Zhong, Jin Yuan, Shu Weihuan, et al. SreD: a secure reputation-based dynamic window scheme for disruption-tolerant networks[C]//In proc. of 2009 IEEE Military Communications Conference, MILCOM 2009, 2009: 1-7.

[15] Nagrath P, Aneja S, Purohit G N. Defending flooding attack in Delay Tolerant Networks[C]//In Proc. of 2015 International Conference on Information Networking (ICOIN)IEEE Computer Society, 2015: 40-45.

[16] Guo Y, Schildt S, Pougel T, et al. Mitigating Blackhole attacks in a hybrid VDTN[C]//In Proc. of 2014 IEEE 15th International Symposium on IEEE Computer Society, 2014: 1-6.

[17] Li Feng, Wu Jie, Avinash Srinivasan. Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets[C]In Proc. of IEEE INFOCOM, 2009: 2228-2236.

[18] Ren Yanzhi, Miiu Choo Chuan, Yang Jie, et al. Detecting blackhole attacks in disruption-tolerant networks through packet exchange recording[C]//In Proc. of 2010 IEEE International Symposium on "A World of Wireless. Mobile and Multimedia Networks", WoWMoM 2010. 2010: 1-6.

[19] Upendra Shevade, Song Han Hee, Qiu Lili, et al. Incentive-aware routing DTNs[C]//In proc. of 16th IEEE International Conference on Network Protocols, ICNP08. 2008: 238-247.

[20] Zhu Haojin, Lin Xiaodong, Lu Rongxing, et al. A secure incentive scheme for delay tolerant networks[C]//In proc. of 3rd International Conference on Communications and Networking in China, ChinaCom 2008: 23-28.

[21] Lu R, Lin X, Zhu H, et al. Pi: A practical incentive protocol for delay tolerant networks[J]. Wireless Communications IEEE Transactions on, 2010, 9(4): 1483-1493.

[22] Alskaif T, Zapata M G, Bellalta B. Game theory for energy efficiency in Wireless Sensor Networks: Latest trends[J]. Journal of Network & Computer Applications, 2015: 33–61.

[23] Yihui Qiu; Zhide Chen; Li Xu, Active Defense Model of Wireless Sensor Networks Based on Evolutionary Game Theory[C]//In proc. of Wireless Communications Networking and Mobile Computing (WiCOM), 2010: 23-25.

[24] Wu T Y, Lee W T, Guizani N, et al. Incentive mechanism for P2P file sharing based on social network and game theory[J]. Journal of Network & Computer Applications, 2014, 41(3): 47–55.

[25] Esposito C, Ficco M, Palmieri F, et al. Smart Cloud Storage Service Selection Based on Fuzzy Logic, Theory of Evidence and Game Theory[J]. IEEE Transactions on Computers, 2015, in press. (1): 1-1.

[26] El-Azouzi, Rachid, De Pellegrini, et al. Evolutionary forwarding games in Delay Tolerant Networks[C]//In Proc. of Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2010 Proceedings of the 8th International Symposium on IEEE, 2010: 76-84.

[27] Wu D, Cao J, Ling Y, et al. Routing Algorithm Based on Multi-Community Evolutionary Game for VANET[J]. Journal of Networks, 2012, 7(7): 1106-1115.

[28] Fang Z, Wei Z. An Evolutionary Game-Based Mechanism for Routing P2P Network Flow among Selfish Peers[J]. Journal of Networks, 2014, 9(1): 10-17.

[29] Wang Chengjun, Gong Zhenghu, Tao Yong, et al. CRSG: A congestion control routing algorithm for security defense based on social psychology and game theory in DTN[J]. Journal of Central South University, 2013, 20(2): 440-450.

[30] Agah A, Das S K, Basu K. Preventing DoS attack in sensor and actor networks: a game theoretic approach[C]//In proc. of IEEE International Conference on Communications, 2005: 3128-3222.

[31] Taylor P D, Jonker L B. Evolutionarily Stable Strategies and Game Dynamics[J]. Mathematical Biosciences, 2010, 40(78): 145--156.

[32] Ari Keränen, Jörg Ott, Teemu Kärkkäinen. The ONE simulator for DTN protocol evaluation[C]//In Proc. of the Second International Conference on Simulation Tools and Techniques, Rome, Italy: ACM, 2009: 1-10.