Research Article

An Evolutionary Game-Based Trust Cooperative Stimulation Model for Large Scale MANETs

Xiao Wang,¹ Yinfeng Wu,¹ Yongji Ren,¹,² Renjian Feng,¹ Ning Yu,¹ and Jiangwen Wan¹,³

¹ School of Instrumentation Science and Opto-Electronics Engineering, Beihang University, Beijing 100191, China
² Department of Command, Naval Aeronautical and Astronautical University, Yantai 264001, China
³ Science and Technology on Communication Information Security Control Laboratory, Jiaxing 314033, China

CorrespondenceshouldbeaddressedtoXiaoWang;wx04508@aspe.buaa.edu.cn

Received 3 April 2013; Accepted 13 May 2013

AcademicEditor: Gurkan Tuna

Copyright © 2013 Xiao Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In order to realize a methodical, effective cooperative stimulation for MANETs and search dynamic trust cooperative stimulation scheme in environment under a high malicious ratio, we have proposed an evolutionary game-based trust cooperative stimulation model for large scale MANETs in this paper. First, the system members’ pluralistic behavior for MANETs has been covered by means of constructing the complete multirisk level strategy space. Then a trust-preferential strategy has been built through trust numerical value mapping technology, which achieves the aim that the malicious action is effectively constrained to avoid a low trust level. Furthermore, the mobility probable parameters and information propagation error matrix are introduced into game model, and the convergence condition between optimum strategy which represents payoff maximization principle and trust-preferential strategy is deduced through evolutionary analyzing finally. Both theoretical analysis and simulation experiments have demonstrated that our model can effectively stimulate cooperation among members and meanwhile be robust under the condition where the environment is harsh under a high original malicious ratio in large scale MANETs.

1. Introduction

With the development of perception theory, ubiquitous computation, and radio technology of multihop, the basic services of large scale mobile ad hoc networks (MANETs) can be autonomously deployed via local backbone nodes (BN), and accomplished by access network nodes (AN). Then the managers of each AN cooperatively upload essential information back to BN, which achieves network managements for large-scale MANETs. Hence, the cooperation among members is the premise for MANETs to provide network services.

However, realizing a methodical and effective scheme for cooperation is facing tougher challenges in MANETs. First, current networks are threatened by a wide range of attacks, such as flooding [1], spoofing [2], wormhole, and Sybil attacks [3], as well as other external attacks [4]. These threats seriously destroy cooperation in MANETs. Furthermore, even if adopting current popular secure mechanism [5, 6] to resist these attacks, due to the own inherent natures of MANETs, including limited available resources, complex deployment environment, exposed communication medium, and intermittent end-to-end links, some normal members may be unwilling to cooperate with others for saving resources to prolong their own network lifetime. The tolerable selfish behavior inevitably interrupts member cooperation of MANETs. For that reason, the exploration and researches on cooperative stimulation scheme for MANETs have been carried out all over the world. Along with current achievements, the cooperative stimulation based on game theory is the most representative. Combining with trust management, distributed system, and key protocol for MANETs, it has effectively stimulated members’ cooperation by game theory for small range of wireless sensor networks and distributed networks. Obviously, the anticipation is clear for game theory as an analytical tool of MANETs: through modeling an independent strategy decision maker, users can control the whole network scene as an acentric control entity and abstract necessary hypothesis to address important problem like other mathematical models [7].
For large scale MANETs, we have found that there are some problems of current game theoretic cooperative stimulation scheme to be solved. First, it is the incompleteness of strategy and payoff space. Current scheme usually defines member’s strategy space simply as “cooperative forwarding, packets dropping” and distributes each action with a payoff value. However in a large scale MANETs with infrastructure mobility, the network action chosen by members is diverse and complicated. The noncooperative actions come from malicious attacks as well as nonmalicious selfish behavior, which is not complete enough by merely describing it as packets dropping. Furthermore the cooperative action is not only the forwarding behavior. According to different network business, it shows various forms of cooperative behavior. Thus a complete strategy space reflecting realistic large scale MANETs and its rational payoff frame must be modeled. Second, it lacks a standard action selection guideline for members. In current game model, network members are modeled as rational and thus naturally selfish individual; they will make any efforts to maximize their payoffs. It is reasonable to assign a higher payoff to cooperation action in order to stimulate members taking cooperative action. In fact, in realistic network, to malicious members, they may more likely launch attacks to get a higher illegal payoff from network collapse. Since large scale MANETs are usually applied for harsh environment monitoring or military detecting, a high malicious ratio is an outstanding feature. As a matter of fact, besides payoff frame reflecting realistic network, an action selection guideline is also needed as scoring system assisting cooperative stimulation scheme based on game theory. Thirdly, the current scheme lacks evolutionary analysis for strategy space using game theory. In fact, the strategy space taken by members is not invariant as the game runs. It may be evolved according to long-term expected benefit or suffering from intrusion of instable strategy. Thus it is necessary to evaluate the evolutionary and convergence performance of each strategy space when using game theory to stimulate the member’s cooperative action. Last but not least, in large scale MANETs, considering the own inherent natures of network, the scheme has to adapt dynamic property as well as propagation error when updating strategy and payoff set.

Aiming at the previous issues, in this paper, we model the transmission process as an evolutionary game and propose a trust cooperative stimulation scheme based on it; our main contributions are summarized as follows.

1. We formulate a transmission evolutionary game defining an abstract concept of level classification in strategy space based on network risk analysis, which can cover the member’s possible network actions under complicated compound attacks in large scale MANETs to enhance the completeness of strategy and payoff space.

2. We construct a trust-preferential expected action space as strategy selection guideline for members through mapping trust management to game theoretical cooperative stimulation, which realizes effective constraint for malicious members obtaining illegal payoffs.

3. We quantitatively analyze the stability and convergence property between our trust-preferential expected action space and payoff maximization-preferential optimum action space and then provide the sufficient and necessary numerical conditions, which can incent members to cooperate with each other.

4. We introduce the mobility probability of members and information propagation error into the formulation of our scheme and make it approach to the realistic large scale MANETs.

2. Related Works

In the literature there are many papers proposing various methods for stimulating members’ cooperation in self-organization networks which can be summarily classified into two schemes: (1) price-based schemes and (2) trust-based schemes. Price-based schemes use the tamper-proof hardware or central billing services to encourage cooperation by rewarding price credits to the cooperative nodes. For example, a cooperation stimulation scheme proposed in [8] employed a virtual currency named Nuglets as price payment for cooperative transmission, later; it was improved in [9] by using price counters. Although price-based schemes can effectively stimulate cooperation among selfish members, the requirement of tamper-proof hardware or central billing service inevitably limits their applications. What is more, the existing works are only fit for traditional multi-hop networks. The price-based schemes depend on end-to-end connections to determine how many prices each member should receive. In MANETs, since end-to-end paths are not guaranteed at all, the existing price-based schemes cannot be used. Regarding this issue, the second method to stimulate cooperation is to adopt trust-based schemes with necessary monitoring, such as CORE [10], CONFIDANT [11], and ARCS [12]. They usually rely on observing the actions of neighbor members and then use mathematical methods such as Dempster-Shafer belief theory to compute the incorporating second-hand information (reports by other nodes) to create a reputation score of members. The trust/reputation score is used for stimulating cooperation because the detected non-cooperative members will be assigned a low score as a penalty to be forced out of the network. However, in realistic dynamic environment of MANETs, for a distributed trust form, the deviating actions of a non-cooperative member are more difficult to be monitored and detected by other members since the connections with the same members are occasional.

Game theory has been widely applied to design and analyze stimulation schemes for wireless network recently. For example, in [13], a Worst Behavior Tit-for-Tat (WBTFT) incentive strategy is proposed to stimulate cooperation at the desired cooperation state, and with perfect monitoring the conditions for the proposed strategy to be subgame perfect are analyzed. In [14], a cooperation stimulation scheme are proposed based on indirect reciprocity game for the scenario where the number of interactions between any pair of players is finite. For large scale wireless networks, Xiao et al. [15]...
proposed a security system that applies the indirect reciprocity principle to combat attacks in wireless networks using the evolutionarily stable strategy concept of game theory. In [16], the authors investigated whether the cooperation among members can improve energy efficiency in ad hoc wireless networks using the behavior-tracking algorithm from game theory, and then the conclusion that the cooperation can reduce power wastage at the same time maximizing the delivery rate is proved.

In addition, further researches have also been made toward mathematically analyzing cooperative stimulation for self-organized wireless network (e.g., MANETs, wireless sensor networks, delay tolerant networks) by using game theory. Zhao et al. [17] proposed a wage-based incentive mechanism for encouraging rational individuals to provide truthful feedbacks. The feedback reporting process in a reputation system was modeled as a reporting game. They also proposed a set of incentive compatibility constraint rules including participation constraints and self-selection constraints. Ze and Haiying [18] analyzed the underlying cooperation of the reputation systems, price-based systems, and a defenseless system through game theory. Based on the results, they proposed an integrated system with a higher performance in terms of the effectiveness of cooperation and selfish node detection. Li et al. [19] showed how game theory can be a tool to analyze the behaviors of every player in role-based trust framework. Considering two types of users, cooperative and malicious, they analyze the strategy sets and payoffs of trust domains and each type of users. Charles et al. [20] investigated when for each node it was cost-effective to freely participate in the security mechanism or protect its privacy according to its own belief in others. The game theoretic framework was used to model trust, and evolutionary game theory was used to capture the dynamic evolution of trust behavior in the network. Also, the studies of cooperative stimulation conditions under correlated equilibrium of coalitional game theoretic approach in ad hoc networks have also been issued in [21–23].

In most existing studies the modeled game theoretic cooperative stimulation shows a promising incentive effect in the network with a small-range, static topology paradigm. Designing a scheme using game theory towards large scale MANETs is the purpose of this paper. The major difference between this paper and current studies is as follow: (1) we formulate a transmission evolutionary trust game constructing the complete strategy and payoff space to cover the member’s possible network actions under complicated compound attacks in large scale MANETs; (2) we separate trust-preferential strategy from payoff-maximization frame, which can be used as strategy selection guideline by means of numeric mapping technology. It can effectively resist malicious members obtaining illegal payoffs from attacking network; (3) we quantitatively analyze the stability and convergence property of the proposed game model in detail, and then provide the sufficient and necessary numerical conditions which can incent members to cooperate with each other; furthermore, (4) we introduce the mobility probability parameters and information propagation error into the formulation of our scheme and make it approach to the realistic large scale MANETs.

3. Scheme Model

3.1. Information Transmission Scenario. We design the scheme model used in homogenous mobile ad hoc networks consisting of N homogenous randomly mobile nodes. For the convenience of discussing, we make the following assumptions: (1) the underlying channel model adopts disk model in order to abstract asymmetrical information away from the complicated properties of RF. (2) As for information transmitter, the probability that the arbitrary other nodes move away from its communication range or the newly nodes accesses into its communication range is ω.

In our model a typical information transmission scenario is composed of one transmitter, one intended receiver, and several information relay nodes. The transmitter generates the information and sends it to the intended receiver with the help of relay nodes. The node within the communication range of the transmitter can be selected to the relay nodes if it has the optimal link state described by medium congestion level, robustness of route protocol, mobile state prediction, and the health degree of itself. In a similar way, the relay node selects the next relay node and the link route according to the same principle until the generated information successfully gets to the intended receiver. For simplicity of mathematical expression, each node in our model becomes the relay node with the probability μ. In this paper, we use the symbol Φ to indicate whether a node is selected to the relay node. More specifically, Φ = 1 indicates that the node becomes the relay node on the information transmission path while Φ = 0 indicates that this node is only in charge of monitoring the behavior of other nodes and computing their trust value. Then these trust values will be exchanged by neighbor nodes via the cryptographic secure channel.

3.2. Trust Management. In MANETs trust management can effectively resist various internal attacks conducted by compromised internal members. In this paper, to stimulate the cooperation behavior among nodes we design a game model in order to enhance the information transmission throughput which needs a scoring system to evaluate such behaviors. Hence we adopt the trust management to design the scoring system.

More specifically, one node monitors and records various communication factors (i.e., transmission rate, forwarding rate, etc.). Then by means of robust mathematical calculation method (i.e., Bayesian interference, DS evidence theory, fuzzy logic classification, etc.), the quantifiable trust value of each supervised members can be obtained by trust manager via the cryptographic secure channel, which can be regarded as the members’ credible extent.

3.3. Game Model. In this paper, we model the aforementioned information transmission process as a dynamic Bayesian game among all nodes in MANETs. During this game all players who participate in this game make efforts to maximize their own payoffs. That is to say, all nodes in our
game model are deemed as rational players related to game theory.

More specifically, in MANETs, there are three kinds of players which amount to \( n + 2 \) members engaged in our game: a transmitter, an intended receiver, and \( n \) participants within the transmitter’s communication range of the game. At time \( t \), participant \( p_n \) selects one action according to the rational principle from our designed complete strategy space to play the game, denoted as \( a_{p_n}[t] \). Based on the analysis of [24], current malicious nodes in large scale MANETs have gradually changed conventional pure attack modes into purposive strategic attack modes, such as selective forwarding attack, frame flooding, spoof, selfish packet dropping attack, and black hole and Sybil attack. In this paper, unlike present research works which simply build the behavior space composed of cooperative and uncooperative actions, we consider a comprehensive situation of attacks in MANETs. In order to stimulate cooperation among nodes in MANETs when nodes are at risk of aforementioned purposive strategic attacks, we classify and abstract current network attacks into multiple levels and then put them in the behavior space of the game model. The strategy space of our game model is shown in Table 1, where \( \{A_1, A_2, A_3, \ldots, A_L\} \) denotes the attack set classified and abstracted by the risk level. Note that in large scale MANETs the specific attack form corresponding to certain risk level is changing when the network operation goal is different. For example, with regard to the information monitoring network, enhance the energy utility which prolongs the network life time is the most important thing to be considered. Thus the frame flooding attack or the relevant combination of attacks which deteriorate the energy performance should be identified as the high-level risk attacks; another, as for the network that emphasizes the information transmission rate and throughputs such as media ad hoc network, black hole and Sybil attack or the relevant combination of attacks which deteriorate the QoS performance should be identified as the high-level risk attacks. Besides, the elements in behavior set \( \{V, C\} \) denote the action taken by the participant who violates and complies with the cooperation rule respectively. More specifically, to the relay node, \( \{V, C\} \) denotes [selfish, forward]. On the contrary, to the monitoring node, \( \{V, C\} \) denotes [forward, monitor].

The payoff frame is an important factor to model as well as analyze the behavior of players. In our game model after taking one certain strategy from behavior space to participate in the game, each participant obtains a real-time payoff \( R_{p_n}[t] \) with relay indicator \( \Phi \), where \( a_{p_n}[t] \in \{A_1, A_2, \ldots, A_L, V, C\} \). Particularly, as for the information transmitter, at time \( t \) every other player that takes one action \( a_{p_n}[t] \) will produce one instant payoff to it, denoted as \( R_{p_n}[t] \). We use \( [T] \) to stand for the payoff that belongs to the transmitter. Generally speaking, the payoff is composed of two parts; one is the gain from action, and the other is the cost when taking this action. The value obtained by subtracting the cost from the gain means the payoff of taking this action. In this paper, positive payoff means that the participant earns profit from action, while negative payoff means that the participant loses some resources such as energy, throughput. More specifically in our game model, with regard to the participant who takes the cooperation behavior \( C \), both information forwarding (\( \Phi = 1 \)) and channel monitoring (\( \Phi = 0 \)) inevitably consume its own resources; hence \( R_C[\Phi = 1] < R_C[\Phi = 0] \leq 0 \). On the other hand, the information transmitter would earn a profit after taking action \( C \); thus \( R_C[T] > 0 \). Next, with regard to the participants who take action that attacks the network or violates the cooperation rule (denoted as the malicious behavior set \( M = \{a_{p_n}[t] | a_{p_n}[t] \in \{A_1, A_2, \ldots, A_L, V\}\} \), they can earn profits from these actions, so \( R_M[\Phi] > 0 \). In this situation the information transmitter’s benefit is threatened which leads to a negative instant payoff, \( R_M[T] \leq 0 \). In addition, according to a wide range of attacks in MANETs classified by multiple risk levels in our model, the instant payoff satisfies the following conditions for both the transmitter and the game members:

\[
\begin{align*}
R_{A_1}[\Phi] & \geq R_{A_{L-1}}[\Phi] \geq \cdots \geq R_{A_L}[\Phi] \\
& \geq R_{A_1} \{\Phi \} \geq 0 \geq R_V[\Phi] \geq R_C[\Phi], \\
R_C[T] & \geq 0 \geq R_V[T] \geq R_{A_1}[T] \\
& \geq R_{A_2}[T] \geq \cdots \geq R_{A_{L-1}}[T] \geq R_{A_L}[T].
\end{align*}
\]

Note that in our modeled transmission game for MANETs, the strict transmission constraint condition is used. More specifically, the information successfully reaches the intended receiver only if all the participants on transmission path comply with the cooperation rule. Based on this condition, at time \( t \) the total instant payoff for transmitter is the minimum of all the obtained instant payoffs from other nodes, denoted as \( P_T \). Similar to the game participant \( p_n \), its total instant payoff can be expressed as \( P^\Phi_{p_n}[t] = R_{p_n}[t] \). For convenience of understanding the game model, Table 2 lists the symbols as well as their meanings used in this paper.

### 4. Trust Cooperative Stimulation Scheme

In this paper we design a cooperative stimulation scheme for large scale MANETs combining game theory and trust management. On one hand, the equilibrium and stability condition of the aforementioned game model is deduced to grasp and predict the result through figuring out each node’s optimal strategy. What is more, based on solution of game
Table 2: Symbols and notations.

| Symbol | Meaning |
|--------|---------|
| \( N \) | The number of homogenous mobile members |
| \( \omega \) | The probability that the member newly enters or moves away from communication range of transmitter |
| \( \Phi \) | Information relay indicator |
| \( \mu \) | The probability that member is selected as information relay node |
| \( a_{p_n}[t] \) | The action taken by game participant \( p_n \) at time \( t \) |
| \( L \) | Risk classification number of attacks |
| \( R_{p_n}[t]\Phi \) | The instant payoff obtained by participant \( p_n \) with relay indicator \( \Phi \) after taking action \( a_{p_n}[t] \) at time \( t \) |
| \( p_{p_n}^T[t] \) | The total instant payoff obtained by transmitter after taking action \( a_{p_n}[t] \) at time \( t \) |
| \( p_{p_n\Phi}[t] \) | The total instant payoff obtained by participant \( p_n \) with relay indicator \( \Phi \) after taking action \( a_{p_n}[t] \) at time \( t \) |
| \( T_{vector} \) | Trust vector |
| \( \left[N_{i,j}\right]_{(L+2)\times(L+2)} \) | Action decision matrix (used as action selection guideline) |
| \( a_{t}^{\ast} \) | Expected action space |
| \( \Gamma = (\Gamma_A,\Gamma_{A_1},\ldots,\Gamma_v,\Gamma_C) \) | Time factor vector |
| \( \Pi_{i,j}^{\star} \) | The instant trust vector |
| \( \Theta \) | The trust propagation matrix |
| \( \chi_i \) (or \( \varepsilon \)) | The systematic probability of correctly recognizing trust level \( i \) |
| \( \delta \) | The probability that the member becomes the information transmitter |
| \( \overline{A} = \left[\overline{a}_{ij}\right]_{(L+2)\times(L+2)} \) | Optimum action space |
| \( p_{i,j}^\ast \) | The anticipated maximum payoff obtained by participant with trust level \( i \) towards the member with trust level \( j \) |
| \( T_{i,j}^{\Phi R_{p_n}} \) | Trust transfer vector |
| \( p_{i,j}^\Phi \) | The anticipated payoff of participant taking action \( a_{ij} \) |

Table 3: Action-trust-based mapping rule.

| Trust value | Action space | Numeric indicator of trust level |
|-------------|-------------|-------------------------------- |
| \( \frac{L-1}{L+2} \leq T_{value} < \frac{L}{L+2} \) | \( A_1 \) | \( L \) |
| \( \frac{L}{L+2} \leq T_{value} < \frac{L-1}{L+2} \) | \( A_2 \) | \( L - 1 \) |
| \( \frac{L-2}{L+2} \leq T_{value} < \frac{L-3}{L+2} \) | \( A_3 \) | \( L - 2 \) |
| \( \frac{L-3}{L+2} \leq T_{value} < \frac{L-4}{L+2} \) | \( A_4 \) | \( L - 3 \) |
| \( \ldots \) | \( \vdots \) | \( \vdots \) |
| \( \frac{L-2}{L+2} \leq T_{value} < \frac{L-1}{L+2} \) | \( A_{L-1} \) | \( L - 1 \) |
| \( \frac{L}{L+2} \leq T_{value} < 1 \) | \( V \) | \( L + 1 \) |
| \( \frac{L+1}{L+2} \leq T_{value} < 1 \) | \( C \) | \( L + 2 \) |

The symbol in action space (i.e., \( A_1, A_2, \ldots, A_L, V, C \)) corresponding to numerical indicator in the third column can be used to indicate trust level of the member. More specifically, the greater the member's numerical indicator, the higher the trust value it has, the more reliable it belongs to, hence the higher-level cooperative action can be serviced by other members in MANETs.

model, the mathematical relationship between payoff and statistical parameters can be used to guide (stimulate) members to cooperate with each other in order to resist selfish behavior or even high-level risk attacks. On the other hand, by means of trust management mechanism, a uniform frame concerning trust distribution, trust update and behavior selection is constructed by the whole members in the network.

In this section, we mainly introduce the behavior selection frame based on trust management (i.e., each member in MANETs takes action according to its trust value) and propose a trust cooperative stimulation scheme. Trust value records the member's quantified credibility (the higher the member's trust value is, the reliable the member is), and its calculation, distribution, and updating must be accomplished via the cryptographic secure channel. Without permission, members cannot clear or temper trust value optionally. All these paradigms of trust scheme indicate that it is fit for large scale MANETs since the cooperation interactive between two nodes only related to their recorded current trust value. For example, without prior knowledge about whether you cooperated with me before, I can decide to take cooperative action with you only if you have an acceptable trust value for me. It differs from current research about cooperative stimulation based on first-hand in MANETs.

The trust cooperative stimulation scheme contains trust evaluation which is based on our previous works [5], action-trust-based mapping method, game action decision principle, and trust updating frame. In this frame, the higher the member's trust value is, the more likely this member is stimulated to take cooperative action (i.e., \( C \)), which results in spreading the cooperation behavior to the whole network. On the contrary, if the member takes a high-level risk attack behavior for obtaining a short-term positive payoff, its trust value will be rapidly declined which causes cooperative service rejection in terms of scheme rule.

Recall that the behavior space for each node participating in the transmission game is \( \{A_1, A_2, \ldots, A_L, V, C\} \) amounting to \( L + 2 \) elements. To combine trust level with game action, we classify the trust value (ranging from 0 to 1 usually) into \( L + 2 \) trust levels and map each level into the behavior space \( \{A_1, A_2, \ldots, A_L, V, C\} \) linearly as Table 3, which we call action-trust-based mapping method. Consequently, the higher the member's trust level is, the more likely it can get a higher level cooperative action from other members. Note that by means of this mapping method, we can use element in action space to indicate node's trust value (also trust level).

According to original mapping, each node is assigned an original trust level \( j \in \{A_1, A_2, \ldots, A_L, V, C\} \) and a trust
vector \( T_{\text{vector}} = (T_{v_{i_1}}, T_{v_{i_2}}, \ldots, T_{v_{i_L}}, T_{v_{i_C}})^T \), where \( T_{v_i} \) denotes the probability that the node's trust level is \( T_{v_i} \) (\( 0 \leq T_{v_i} \leq 1 \)), 
\( \sum_{j=1}^{L+2} T_{v_{ij}} = 1 \).

After trust mapping, game action decision principle and trust updating frame are the two important parts affecting the performance of the trust cooperative stimulation. More specifically, at single time moment the game action decision principle is designed according to interaction between transmitter with trust level \( i \) and participant with trust level \( j \) shown as matrix \( N_{i,j}^{(L+2) \times (L+2)} \) in the following, where element \( N_{i,j} \) denotes the assigned trust level of the participant who takes action \( i \) (\( i \in \{A_1, A_2, \ldots, A_L, V, C\} \)) towards the transmitter with trust level \( j \) and \( \Phi \) (\( \Phi = 0, 1 \)) is the relay indicator of the participant:

\[
N(\Phi)_{(L+2) \times (L+2)} = \Phi \begin{bmatrix}
A_1(L) & A_1(L) & \cdots & A_1(L) & A_1(L) & A_1(L)
\vdots & \vdots & \cdots & \vdots & \vdots & \vdots
A_2(L-1) & A_2(L-1) & \cdots & A_2(L-1) & A_2(L-1) & A_2(L-1)
C(L+2) & C(L+2) & \cdots & C(L+2) & C(L+2) & V(L+1)
A_1(L) & A_2(L-1) & \cdots & A_L(L) & V(L+1) & C(L+2)
\end{bmatrix}
\]

\[+(1-\Phi)
\begin{bmatrix}
A_1(L) & A_1(L) & \cdots & A_1(L) & A_1(L) & A_1(L)
\vdots & \vdots & \cdots & \vdots & \vdots & \vdots
A_2(L-1) & A_2(L-1) & \cdots & A_2(L-1) & A_2(L-1) & A_2(L-1)
V(L+1) & V(L+1) & \cdots & V(L+1) & V(L+1) & V(L+1)
C(L+2) & C(L+2) & \cdots & C(L+2) & C(L+2) & C(L+2)
\end{bmatrix}
\]

\[= \Phi \begin{bmatrix}
V(L+1) & V(L+1) & \cdots & V(L+1) & V(L+1) & C(L+2)
V(L+1) & V(L+1) & \cdots & V(L+1) & V(L+1) & C(L+2)
\vdots & \vdots & \cdots & \vdots & \vdots & \vdots
V(L+1) & V(L+1) & \cdots & V(L+1) & V(L+1) & C(L+2)
V(L+1) & V(L+1) & \cdots & V(L+1) & V(L+1) & C(L+2)
\end{bmatrix}
\]

\[+ (1-\Phi)
\begin{bmatrix}
C(L+2) & C(L+2) & \cdots & C(L+2) & C(L+2) & C(L+2)
C(L+2) & C(L+2) & \cdots & C(L+2) & C(L+2) & C(L+2)
\vdots & \vdots & \cdots & \vdots & \vdots & \vdots
C(L+2) & C(L+2) & \cdots & C(L+2) & C(L+2) & C(L+2)
C(L+2) & C(L+2) & \cdots & C(L+2) & C(L+2) & C(L+2)
\end{bmatrix}
\]

From matrix \( a_{(L+2) \times (L+2)}^{*} \), for the view of maintaining a higher trust level in this game, this expected strategy space can effectively encourage participants to take cooperative actions.

\[a_{(L+2) \times (L+2)}^{*} = \Phi \begin{bmatrix}
C(L+2) & C(L+2) & \cdots & C(L+2) & C(L+2) & C(L+2)
C(L+2) & C(L+2) & \cdots & C(L+2) & C(L+2) & C(L+2)
\vdots & \vdots & \cdots & \vdots & \vdots & \vdots
C(L+2) & C(L+2) & \cdots & C(L+2) & C(L+2) & C(L+2)
C(L+2) & C(L+2) & \cdots & C(L+2) & C(L+2) & C(L+2)
\end{bmatrix}
\]

Recall that each newly node participating in the game would be assigned a trust vector. Suppose that a new node has a good intention to cooperate with each other; it could be assigned a trust vector \( T_{\text{vector}} = (0, 0, \ldots, 0, 1)^T \). At time \( t+1 \) the action \( i \) (\( i \in \{A_1, A_2, \ldots, A_L, V, C\} \)) taken by participant is recorded by monitoring node. Then according to game action decision principle \( N_{i,j}^{(L+2) \times (L+2)} \), relay indicator \( \Phi \), and the trust level \( j \) of information transmitter, the participant would...
obtain an instant trust level denoted as $I_{t+1}^{i,j} = N_{i,j}(\Phi)$. The trust updating process is triggered as shown in Figure 1.

From Figure 1, the participant’s trust vector at time $t + 1$ is expressed as

$$T_{\text{vector}}(t + 1) = \Theta \left( N_{i,j}(\Phi)T_{\text{vector}}(t) + \left( 1 - N_{i,j}(\Phi) \right) I_{t+1}^{i,j} \right). \tag{4}$$

It is composed of three parts: the first part is instant trust vector

$$I_{t+1}^{i,j} = \begin{bmatrix} 0, \ldots, [1], \ldots, 0 \end{bmatrix}^T$$

The corresponding vector position of $I_t(t+1)$

$$\Theta_{(L+2)\times(L+2)} = \begin{bmatrix}
X_L & \frac{1 - X_L}{L + 1} & \cdots & \frac{1 - X_L}{L + 1} & \frac{1 - X_L}{L + 1} \\
\frac{1 - X_{L-1}}{L + 1} & \frac{1 - X_{L-1}}{L + 1} & \cdots & \frac{1 - X_{L-1}}{L + 1} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
\frac{1 - X_1}{L + 1} & \frac{1 - X_1}{L + 1} & \cdots & \frac{1 - X_1}{L + 1} & \frac{1 - X_1}{L + 1} \\
\frac{1 - X_{L+1}}{L + 1} & \frac{1 - X_{L+1}}{L + 1} & \cdots & \frac{1 - X_{L+1}}{L + 1} & \frac{1 - X_{L+1}}{L + 1} \\
\frac{1 - X_{L+2}}{L + 1} & \frac{1 - X_{L+2}}{L + 1} & \cdots & \frac{1 - X_{L+2}}{L + 1} & X_{L+2}
\end{bmatrix}, \tag{5}$$

where $X_i$ denotes the systematic probability of correctly recognizing trust level $i$.

In this section, we propose a trust cooperative stimulation scheme based on trust-game mapping idea. An expected action matrix $\alpha_{(L+2)\times(L+2)}^*$ (trust-preferential strategy) and the trust updating frame are deduced to guide members tending to cooperation. For the view of maintaining a higher trust level in this game, this scheme can effectively encourage participants to take cooperative actions.

5. Game Theoretic Analysis

In the large scale MANETs, members who take the expected action $\alpha_{(L+2)\times(L+2)}^*$ to select cooperative behavior can maintain a higher trust level (trust-preferential strategy) with themselves. Hence even if the network topology changes dramatically, nodes can also continue to obtain high-level cooperative network services in the new area by means of their high trust level. However in game theory, optimum actions refer to the strategy that receives a highest payoff for all the players. In this section, we mainly study whether the nodes can take the expected trust-preferential strategy also obtain a higher payoff after long-time running of the game? In addition, we adopt the evolutionarily game idea to analyze under which numerical condition can the expected trust-preferential strategy evolve to the payoff-preferential strategy (optimum strategy), that is, evolutionarily stable strategy (ESS).

5.1. Evolutionary Game Theory. Evolutionary game theory provides a new angle of view to research the network cooperative stimulation scheme. It well overcomes the difficulties about rational hypothesis and multiple equilibriums in classical game theory. What is more, it can obtain more accurate results than traditional theory by using evolutionary game theory to research network security and can realistically analyze and explain cooperative motivation. To the best of our knowledge, introducing evolutionary game theory to study the mechanism of cooperative stimulation is a method innovation in MANETs.

In evolutionary game model, if most of the members take ESS, other parts of members’ alternative strategies cannot invade the ESS. First we use the expected trust-preferential action as the original strategy in the game, and then the strategy starts to evolve in terms of the payoff maximum criteria which can deduce the optimum strategy of the game. More specifically, at the original time moment 1, game participant $p_{n}$ takes the action according to the game action
decision matrix \([N_i,j]_{(L+2)\times(L+2)}\) and the expected action matrix \(a_{(L+2)\times(L+2)}\), and the evolutionary process is triggered. At time \(t + 1\), the probability of taking action \(a_{p_n}[t + 1] = i \in \{A_1, A_2, \ldots, A_L, V, C\}\) for node \(p_n\) is denoted as
\[
\Pr\{a_{p_n}[t + 1] = i\} = \frac{\Pr\{a_{p_n}[t] = i\} P_{p_n, i}[t]}{\sum_{j=1}^{L+2} \Pr\{a_{p_n}[t] = j\} P_{p_n, j}[t]},
\]
where \(P_{p_n, i}[t]\) denotes the instant payoff obtained by participant \(p_n\) who takes the action \(i\) at time \(t\). From (7) we can solve the ESS (i.e., optimum strategy space) as well as the corresponding stable trust vector \(\tilde{T}^{\text{vector}}\) of this evolutionary game when taking the expected trust-preferential strategy as original strategy in MANETs.

5.2. Optimum Action Space. We first define matrix \(\tilde{A} = [\tilde{a}_{i,j}]_{(L+2)\times(L+2)}\) as optimum action space, where the element \(\tilde{a}_{i,j} \in \{A_1, A_2, \ldots, A_L, V, C\}\) denotes the instant optimum action taken by participant with trust level \(j\) towards the member with trust level \(i\). Note that taking this instant optimum action the participant should have obtained an anticipated maximum payoff. We use symbol \(P_{i,j}^{\text{max}} = \max_{1 \leq k \leq (L+2)} P_{i,j}^{a_k}\) to denote this anticipated maximum payoff. Consequently, the optimum action should satisfy the following expression:
\[
\tilde{a}_{i,j} = \arg \max_{1 \leq k \leq (L+2)} P_{i,j}^{a_k}.
\]

In our game model, considering the trust updating frame, the trust level of each participant may be transferred at different time moment. Thus we must evaluate the evolutionary optimum action space under the influence of the trust updating process. Recall that in our game the probability of participant selected to the information relay node is \(\mu\). Suppose that each behavior in set \(\{A_1, A_2, \ldots, A_L, V, C\}\) has the same time factor \(\Gamma\). We define trust transfer vector \(\tilde{T}^{T}_{\tilde{T}_{\text{vector}}}\) denoting the transfer probability vector after the participant with trust level \(i\) takes action \(k\) towards the participant with trust level \(j\). Based on trust updating process shown in Figure 1, we can calculate the \(\tilde{T}^{T}_{\text{vector}}\) by the following expression:
\[
\tilde{T}^{T}_{\text{vector}} = \begin{bmatrix} t_{i,j}^{a_{p_n} \mu} [L], & t_{i,j}^{a_{p_n} \mu} [L - 1], & \ldots, & t_{i,j}^{a_{p_n} \mu} [1]; \\
\end{bmatrix}^{\text{T}}\]
\[
= \Theta \left( \Gamma_{\text{vector}}^{\text{T}} + (1 - \Gamma) \right) \times \left( \mu N_{i,j}^{T_{\text{vector}}} (\Phi=1), j \right) + (1 - \mu) N_{i,j}^{T_{\text{vector}}} (\Phi=0), j \right),
\]
where vector element \(t_{i,j}^{a_{p_n} \mu} [k]\) denotes the probability that the trust level of the participant taking action \(k\) towards the participant with trust level \(j\) has transferred from \(i\) to \(l\). Formula (9) takes behavior time factor and relay factor into account, which is embodied by the application of \(\Gamma\) and \(\mu\), respectively.

Second, we solve the game payoff \(P_{i,j}^{a}\) obtained by participant \(p_n\) with trust level \(i\) towards the participant taking optimum action \(a_{i,j}\) with trust level \(j\). If \(p_n\) takes action \(a_{i,j}\), its instant payoff at time \(t\) can be denoted as \(\mu P_{p_n, a_{i,j}}^{\Phi=1} [t] + (1 - \mu) P_{p_n, a_{i,j}}^{\Phi=0} [t]\). In addition, consider the dynamics of MANETs, suppose that the probability of the node staying in the local area or moving to the new area is \(\omega\), and the stable trust vector \(\tilde{T}_{\text{vector}}\) does not change as time goes on; we can calculate the instant payoff obtained by nonrelay participant \(p_n\) as
\[
\mu P_{p_n, a_{i,j}}^{\Phi=1} [t] + (1 - \mu) P_{p_n, a_{i,j}}^{\Phi=0} [t] + \omega \sum_k \tilde{T}_{i,j}^{T_{\text{vector}}} P_{k,j}.\]

On the other hand, if \(p_n\) faces the information transmitter, similarly, its instant payoff can be calculated by
\[
(1 - \mu) P_{p_n, a_{i,j}}^{\Phi=0} [t] + \mu P_{p_n, a_{i,j}}^{\Phi=1} [t] + \omega \sum_k \tilde{T}_{i,j}^{T_{\text{vector}}} P_{k,j}.\]

To sum up, we define the probability that the node becomes the information transmitter in the game is \(\delta\) consequently the game payoff \(P_{i,j}^{a}\) can be expressed as
\[
P_{i,j}^{a} = (1 - \delta) \left( \mu P_{p_n, a_{i,j}}^{\Phi=1} [t] + (1 - \mu) P_{p_n, a_{i,j}}^{\Phi=0} [t] \right) + \omega \sum_k \tilde{T}_{i,j}^{T_{\text{vector}}} P_{k,j}.\]

Thirdly, we give the expression of stable trust vector \(\tilde{T}_{\text{vector}}\) when the game evolves to the ESS. According to trust updating frame, when taking probability \(\mu\) and relay indicator \(\Phi\) of the participant \(p_n\) into account, the stable trust vector \(\tilde{T}_{\text{vector}}\) can be expressed by
\[
\text{\bar{T}}_{\text{vector}} = \Theta \Gamma \text{\bar{T}}_{\text{vector}} + (1-\Gamma) \begin{pmatrix}
\sum_{i=1}^{L+2} \sum_{j=N_{i,j}(\Phi=0)=0}^{L} \bar{T}_{i,j} \bar{T}_{i,j} \\
\vdots \\
\sum_{i=1}^{L+2} \sum_{j=N_{i,j}(\Phi=0)=L}^{L+2} \bar{T}_{i,j} \bar{T}_{i,j}
\end{pmatrix} + (1-\mu) \begin{pmatrix}
\sum_{i=1}^{L+2} \sum_{j=N_{i,j}(\Phi=0)=0}^{L} \bar{T}_{i,j} \bar{T}_{i,j} \\
\vdots \\
\sum_{i=1}^{L+2} \sum_{j=N_{i,j}(\Phi=0)=L}^{L+2} \bar{T}_{i,j} \bar{T}_{i,j}
\end{pmatrix},
\]

(13)

where \(\sum_{i=1}^{L+2} \sum_{j=N_{i,j}(\Phi=0)}^{L} \bar{T}_{i,j} \bar{T}_{i,j}\) denotes the probability that the trust level of participant (with relay indicator \(\Phi\)) who takes optimum action \(\bar{a}_{i,j}\) transfers to level \(k\). Based on previous analysis, the optimum action space has been modeled into a Markov decision process.

Combining (9), (12), and (13), the proposed optimum action space \(\bar{a}_{i,j}\) and its corresponding stable trust vector \(\text{\bar{T}}_{\text{vector}}\) of the evolutionary game can be solved by iterative numerical method.

5.3. Relationship between Optimum and Expected Action and Its Convergence Condition. So far by means of evolutionary game theory we have deduced the ESS of the payoff-preferential strategy (optimum strategy) when taking the expected trust-preferential strategy as the original dominant action. In this section, we continue to study the convergence condition of this game, which is depicted as the paradigm that the ESS of the game converges to the original strategy. Meanwhile, we deduce and give the numerical relationship between optimum and expected action and its convergence condition.

If our evolutionary game converges, the original dominant strategy \(a_{i,j}^{*}\) will evolve to be the optimum strategy \(\bar{a}_{i,j}\); that is, \(\bar{a}_{i,j} = a_{i,j}^{*}\). According to (3), we have

\[
\begin{bmatrix}
\bar{a}_{i,j}^{(\Phi)} \\
\bar{a}_{i-1,j}^{(\Phi)} \\
\vdots \\
\bar{a}_{i,j}^{(\Phi)} \\
\bar{a}_{i+1,j}^{(\Phi)} \\
\bar{a}_{i,j+1}^{(\Phi)} \\
\bar{a}_{i,j+2}^{(\Phi)}
\end{bmatrix}_{(L+2)\times(L+2)} = \begin{bmatrix}
\bar{a}_{i,j}^{(\Phi)} \\
\bar{a}_{i,j}^{(\Phi)} \\
\vdots \\
\bar{a}_{i,j}^{(\Phi)} \\
\bar{a}_{i,j}^{(\Phi)} \\
\bar{a}_{i,j}^{(\Phi)} \\
\bar{a}_{i,j}^{(\Phi)}
\end{bmatrix}_{(L+2)\times(L+2)}
\]

\[
\begin{bmatrix}
V(L+1) \\
V(L+1) \\
\vdots \\
V(L+1) \\
C(L+2)
\end{bmatrix} + (1-\Phi)
\begin{bmatrix}
V(L+1) \\
V(L+1) \\
\vdots \\
V(L+1) \\
C(L+2)
\end{bmatrix} = \Phi
\]

(14)

For the convenience of deducing, suppose that all the probability of correctly recognizing trust level in trust propagation matrix \(\Theta\) is the same, and \(\chi_{i} = \epsilon\); we also have

\[
\Theta(L+2) = \begin{bmatrix}
\epsilon & 1-\epsilon & 1-\epsilon & \cdots & 1-\epsilon \\
1-\epsilon & \epsilon & 1-\epsilon & \cdots & 1-\epsilon \\
1-\epsilon & 1-\epsilon & \epsilon & \cdots & 1-\epsilon \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1-\epsilon & 1-\epsilon & 1-\epsilon & \cdots & \epsilon \\
L+1 & L+1 & L+1 & \cdots & \epsilon
\end{bmatrix}
\]

(15)

**Proposition 1.** Given the trust level \(1 \leq j \leq (L+2)\) and \(1 \leq m \leq (L+1)\), the following expression is obtained:

\[
P_{(L+2),j} - P_{m,j} = \frac{\delta \mu (P_{L+2,j}^{\pi} - P_{L+1,j}^{\pi}) (L+1)}{(L+1) (1-\omega \delta) - \omega (1-\delta) (L\epsilon - 1)}.\]

(16)

**Proof.** According to (9), (14), and (15), the difference of two trust transfer vectors from optimum action strategy is

\[
\text{\bar{T}}_{m,j}^{\bar{a}_{i,j}} - \text{\bar{T}}_{m,j}^{\bar{a}_{i,j}} |_{(L+2),j} = \text{\bar{T}}_{m,j}^{\bar{a}_{i,j}} - \text{\bar{T}}_{m,j}^{\bar{a}_{i,j}} |_{(L+2),j} = \Theta \Gamma (I_{m,j}^{\text{vector}} - I_{m,j}^{(L+2)})
\]

(17)
Note that in the remainder of this paper we use $V[x]$ to denote the $x$th element of vector $V$. Combining (12), (14), and (17), we can obtain

$P_{m,j} - P_{L+2,j}T_{m,kl} = P_{m,j} - P_{L+2,j}$

$= (1 - \delta)\omega\sum_{k} \left[ \left( T_{m,kl}^T[k] - T_{L+2,kl}^T[k] \right) \right] T_{m,k}P_{k,l}$

$+ \delta \left( (1 - \mu) \left( p_{m,kl}^{T(1)}(0) - p_{L+2,kl}^{T(1)}(0) \right) + \mu \left( p_{m,kl}^{T(1)}(1) - p_{L+2,kl}^{T(1)}(1) \right) \right)$

$+ \omega \sum_{k} T_{m,k} \left( P_{m,j} - P_{L+2,j} \right)$

$= (1 - \delta)\omega\sum_{k} \left[ \left( T_{m,kl}^T[k] - T_{L+2,kl}^T[k] \right) \right] T_{m,k}P_{k,l}$

$+ \delta \left( \mu \left( p_{m,kl}^{T(1)} - p_{L+2,kl}^{T(1)} \right) + \omega \sum_{k} T_{m,k} \left( P_{m,j} - P_{L+2,j} \right) \right)$

$= \delta \mu \left( p_{m,kl}^{T(1)} - p_{L+2,kl}^{T(1)} \right) + \omega \left( \delta + (1 - \delta) \Gamma \left( \frac{L - 1}{(L + 1)} \right) \right)$

$\times \sum_{k} T_{m,k} \left( P_{m,j} - P_{L+2,j} \right).$

(18)

Because $P_{m,j} - P_{L+2,j}$ is independent with value $i$, the above (18) can be rewritten as

$P_{m,j} - P_{L+2,j} = \delta \mu \left( p_{m,kl}^{T(1)} - p_{L+2,kl}^{T(1)} \right)$

$\times \left( (1 - \omega \delta) - \omega (1 - \delta) \Gamma \left( \frac{L - 1}{(L + 1)} \right) \right) \sum_{k} T_{m,k} \left( P_{m,j} - P_{L+2,j} \right).$

(19)

Thus we can get the conclusion of Proposition 1. \hfill \Box

According to Proposition 1, we can infer that the participant with trust level $m$ (less than the highest level $L + 2$) would obtain a lower bound of the payoff after taking the expected trust-preferential strategy:

$P_{L+2,j} - \frac{\delta \mu \left( p_{m,kl}^{T(1)} - p_{L+2,kl}^{T(1)} \right) \left( L + 1 \right)}{(L + 1)(1 - \omega \delta) - \omega (1 - \delta) \Gamma \left( \frac{L - 1}{(L + 1)} \right)}.$

(20)

The mechanism of cooperative stimulation by using the expected trust-preferential strategy is depicted as follows: no matter how low the participant’s trust level is or which attribute (transmitter, receiver, relay node, and monitor) the participant belongs to, the expected trust-preferential strategy can stimulate it to cooperate with other members to obtain needed payoff to be serviced by the network.

**Theorem 2.** The sufficient condition that the proposed evolutionary game model can converge is

$$P_{1}^{\Phi} - P_{L+2}^{\Phi} < \frac{\omega(1 - \Gamma) (L - 1) \delta \mu \left( p_{L+2}^{T(1)} - p_{L+1}^{T(1)} \right)}{(L + 1)(1 - \omega \delta) - \omega(1 - \delta) \Gamma \left( \frac{L - 1}{(L + 1)} \right)},$$

$$\Phi = 0, 1, \quad \epsilon > \frac{1}{L + 2}.$$  

(21)

**Proof.** First, consider the situation that the participant with trust level $i$ faces the participant with the highest trust level $(L + 2)$ and relay indicator $\Phi = 1$. To inquire the expected behavior matrix $a_{i,j}^\Phi$, it should take the expected action shown as $\hat{a}_{i,j}^\Phi(\Phi = 1) = L + 2$. So for arbitrary action indicator $m < L + 2$, we have $P_{L+2}^{\Phi(1)}(L+2) - P_{L+2}^{\Phi(1)=m} > 0$. Again after combining (12), we can deduce the following equation:

$$P_{L+2}^{\Phi(1)=L+2} - P_{L+2}^{\Phi(1)=m}$$

$$= (1 - \delta) \left( \mu \left( p_{L+2}^{\Phi(1)} - p_{L+2}^{\Phi(1)=m} \right) \right)$$

$$+ \omega \sum_{k} \left( \left( l_{L+2}^{\Phi(1)} \right)[k] \right) \hat{T}_{k}P_{k,l} > 0.$$

(22)

Combining (2), (9), and (22), we have

$$\mu \left( p_{L+2}^{\Phi(1)} - p_{L+2}^{\Phi(1)=m} \right)$$

$$\times \left( (1 - \omega \delta) - \omega (1 - \delta) \Gamma \left( \frac{L - 1}{(L + 1)} \right) \right) \sum_{k} T_{m,k} \left( P_{m,j} - P_{L+2,j} \right).$$

(23)

Taking (17) into the above (23), we can obtain

$$\left( p_{m}^{\Phi(1)} - p_{L+2}^{\Phi(1)=m} \right) < \omega (1 - \Gamma) \left( \frac{L - 1}{L + 1} \right) \sum_{k} T_{m,k} \left( P_{m,j} - P_{L+2,j} \right).$$

(24)
Thus,
\[
P_{\Phi=1}^{\Phi=1} - P_{L+2}^{\Phi=1} < \frac{\omega (1 - \Gamma) (L - 1) \delta \mu (P_{L+2}^{\Phi} - P_{L+1}^{\Phi})}{(L + 1) (1 - \omega \delta) - \omega (1 - \delta) \Gamma (L - 1)}.
\]

(25)

Because of $P_{L+2}^{\Phi} \geq P_{L+1}^{\Phi}$ and $P_{L+2}^{\Phi=1} \leq P_{L+1}^{\Phi=1}$, the above formula can also indicate that $\epsilon > 1/(L + 2)$.

Second consider the situation that the participant with trust level $i$ faces the participant with the highest trust level $(L + 2)$ and relay indicator $\Phi = 0$. Similar to the above case with $\Phi = 1$, according to (14), (12) can be rewritten as
\[
P_{i,L+2}^{\Phi=1}(0)=(L+2) - P_{i,L+2}^{\Phi=1}[m] > 0.
\]

(26)

Combining (2), (9), and (26), we have
\[
(1 - \mu) (P_{L+2}^{\Phi=1} - P_{m}^{\Phi=1}) > \omega \sum_{k,l} \left( \begin{array}{c}
t^{a_{i,L+2}(0)=(L+2)}[k] - t^{a_{i,L+2}(0)=m}[k] \\
(P_{m}^{\Phi=0} - P_{(L+2)}^{\Phi=0})
\end{array} \right) \overline{T}_{i,j} P_{k,j}.
\]

(27)

Because of $1 \leq m \leq L + 1$, taking (17) into the above formula, we can obtain
\[
(P_{1}^{\Phi=0} - P_{L+2}^{\Phi=0}) < \omega (1 - \Gamma) \left( \frac{L - 1}{L + 1} \right) (P_{L+2,j}^{\Phi} - P_{L+1,j}^{\Phi})
\]

(28)

To sum up, we can get the conclusion of Theorem 2 when the participant with trust level $i$ faces the participant with the highest trust level $(L + 2)$.

Next we have to consider the situation that the participant with trust level $i$ faces the participant with the trust level $j < (L + 2)$ and relay indicator $\Phi = 1$. In this situation, it should take the expected action shown as $\overline{a}_{i}(\Phi = 1) = L + 1$. (1) For action indicator $m < L + 1$, we have $P_{i,j}^{a_{i}(1)=(L+1)} - P_{i,j}^{a_{i}(1)=m} > 0$. According to (12), we can deduce that
\[
P_{i,j}^{a_{i}(1)=(L+1)} - P_{i,j}^{a_{i}(1)=m} > (1 - \delta) \left( \frac{\mu (P_{L+1}^{a_{i}(1)}) - P_{L+1}^{a_{i}(1)})}{m} + \omega \sum_{k,l} \left( \begin{array}{c}
t^{a_{i}(1)=(L+1)}[k] - t^{a_{i}(1)=(L+2)}[k] \\
(P_{m}^{\Phi=1} - P_{(L+2)}^{\Phi=1})
\end{array} \right) \overline{T}_{i,j} P_{k,j} \right) > 0.
\]

(29)

Simplifying it, we have
\[
\mu (P_{L+1}^{\Phi=1} - P_{m}^{\Phi=1}) > \omega \sum_{k,l} \left( \begin{array}{c}
t^{a_{i}(1)=(L+1)}[k] - t^{a_{i}(1)=(L+2)}[k] \\
(P_{m}^{\Phi=0} - P_{(L+2)}^{\Phi=0})
\end{array} \right) \overline{T}_{i,j} P_{k,j}
\]

(30)

Hence,
\[
(P_{m}^{\Phi=0} - P_{m}^{\Phi=1}) < \omega (1 - \Gamma) \left( \frac{L - 1}{L + 1} \right) (P_{L+2,j}^{\Phi} - P_{m}^{\Phi})
\]

(31)

Because of $1 \leq m \leq L$, taking (17) into the above, we can obtain:
\[
(P_{1}^{\Phi=0} - P_{L+1}^{\Phi=0}) < \omega (1 - \Gamma) \left( \frac{L - 1}{L + 1} \right) (P_{L+2,j}^{\Phi} - P_{L+1,j}^{\Phi})
\]

(32)

In the same situation, (2) for action indicator $m = L + 2$, the expected action participant should take is still shown as $\overline{a}_{i}(\Phi = 1) = L + 1$. So we have $P_{i,j}^{a_{i}(1)=(L+1)} - P_{i,j}^{a_{i}(1)=(L+2)} > 0$ and the following expression:
\[
P_{i,j}^{a_{i}(1)=(L+1)} - P_{i,j}^{a_{i}(1)=(L+2)} > (1 - \delta) \left( \frac{\mu (P_{L+1}^{a_{i}(1)}) - P_{L+1}^{a_{i}(1)})}{m} + \omega \sum_{k,l} \left( \begin{array}{c}
t^{a_{i}(1)=(L+1)}[k] - t^{a_{i}(1)=(L+2)}[k] \\
(P_{m}^{\Phi=1} - P_{(L+2)}^{\Phi=1})
\end{array} \right) \overline{T}_{i,j} P_{k,j} \right) > 0.
\]

(33)
Simplifying above formula, we have

\[ \mu(P_{L+1}^\Phi - P_{L+1}^\Phi = 1) > \omega \sum_k \sum_l (t_{i,j}^{(1)} = (L+2)) [k] - t_{i,j}^{(1)} = (L+1)) [k] \tilde{T}_{i,j} P_{k,l} \]

\[ = \omega \sum_k \Theta(1-\Gamma) \sum_l (t_{i,j}^{N_{L+1}}(\Phi = 1) - t_{i,j}^{N_{L+1}}(\Phi = 1)) [k] \tilde{T}_{i,j} P_{k,l} \]

\[ = \omega (1-\Gamma) \left( \sum_l \tilde{T}_{i,j} \left( P_{j,l} - P_{(L+2),j} \right) \right). \]

(34)

Hence,

\[ (P_{L+2}^\Phi - P_{L+1}^\Phi) < \omega (1-\Gamma) \left( \frac{L-1}{L+1} \right) (P_{(L+2),j} - P_{j,l}) \]

\[ = \omega (1-\Gamma) \frac{(L-1)\delta \mu (P_{L+2}^T - P_{L+1}^T)}{(L+1)(1-\omega \delta) - \omega (1-\delta) \Gamma (L-1)}. \]

(35)

Last, consider the situation that the participant with trust level \( i \) faces the participant with the trust level \( j < (L+2) \) and relay indicator \( \Phi = 0 \). Similar to the above proof procedure, we can obtain the following two expressions:

\[ P_{L+2}^{\Phi = 0} - P_{L+1}^{\Phi = 0} < \frac{\omega (1-\Gamma) (L-1) \delta \mu (P_{L+2}^T - P_{L+1}^T)}{(L+1)(1-\omega \delta) - \omega (1-\delta) \Gamma (L-1)}. \]

(36)

To sum up, we considered all the situations and deduced (25), (28)–(36), which can support and verify the conclusion of Theorem 2. If the parameters of our proposed stimulation scheme are set to satisfy Theorem 2, the transmission game of Theorem 2. If the parameters of our proposed stimulation scheme are set to satisfy Theorem 2, the transmission game.

6. Simulation

6.1. Simulation Setup. In this part, we conduct extensive simulations to evaluate the network performance of our proposed stimulation model. All simulations are conducted in randomly generated MANETs. 5000 members are randomly deployed in a 10000 m x 10000 m region. The Medium Access Control (MAC) layer protocol implements the IEEE 802.11 DCF with a four-way handshaking mechanism. The default link bandwidth is 2 Mb/s. DSR is adopted as route protocol. The maximum transmission range is 100 m. In our simulated MANET, each node is moving according to the random waypoint model: a node randomly chooses a destination within the circle and moves forward to the destination at a velocity uniformly chosen in 0.5 m/s, 2.5 m/s. When arriving at the destination, the node will choose a new location and a new speed to move on.

Table 4 lists the default settings of stimulation scheme.

| Parameter | Default value setting |
|-----------|-----------------------|
| \( N \)   | 5000                  |
| \( \omega \) | 0.4                  |
| \( \mu \)  | 0.5                   |
| \( \delta \) | 0.25                  |
| \( L \)    | 3                     |
| \( \Gamma \) | (0.5, 0.5, 0.5, 0.5) |
| \( \chi_i \) (or \( \varepsilon \)) | 0.75               |

Table 4: Default parameter settings.

To evaluate the network transmission performance of our proposed cooperative stimulation scheme in large scale MANETs, a proportion of malicious members who give priority to take attack action from strategy space on the basis of payoff maximization will be mixed up with normal members at the initial time, that is, original malicious ratio (i.e., we mainly set the ratio at 0%, 20%, 40%, and 60% in simulation). More specifically, take wireless medium network for instance in simulation; a 3-level attack set is provided for malicious members to make decisions; \( A_1 \) means frame flooding attack, \( A_2 \) means black hole attack, and highest risk of \( A_3 \) means packets dropping attack. Then the following indexes are measured for evaluating network performance.

(1) Cooperative Population: it is defined as the ratio between the total number of members taking cooperative action and that of all members in MANETs.

(2) Average Payoffs: it is defined as the mean value payoffs obtained by all members in MANETs after each round of the game.

(3) Transmission Success Ratio (TSR): it is defined as the ratio between the total number of successfully forwarded packets and that of packets scheduled to be sent.

(4) Normalized Network Throughput (NNT): it is defined as the ratio between the number of valid packets (or bits) which make them through the network per time unit and that of total network packets, which can be depicted as the data activity of MANETs.
In our evolutionary game, each simulation is evolved 500 times to estimate these indexes. What is more, the evolutionary stable status and game convergence performance are also measured to verify our trust cooperative stimulation scheme.

6.2. Simulation Results. Figure 2 compares the overall effect of evolutionary cooperative population under various kinds of malicious ratio using our trust cooperative stimulation scheme. From Figure 2 we can see that as the cooperation game goes on, the network cooperative population, which takes strategy $C$, is all increased significantly during 500 game rounds under original malicious ratio at 0%, 20%, 40%, and 60%. This is because nodes could take cooperation strategy to obtain a higher trust level in the frame of cooperative stimulation scheme in order to strive for continuous network services. In addition, the simulation parameter setting meets the condition of Theorem 2; namely, the game model exists evolutionary stable status and convergence point. According to the simulation results, after the evolutionary game is played 439 rounds the evolutionary stable status (ESS) comes and the cooperative population cannot fluctuate wildly. More specifically, when original malicious ratio of network is at 0%, 20%, 40%, and 60%, respectively, the cooperative population is increased from 62.3%, 45.8%, 36%, and 19.6% to 94.3%, 83.9%, 78.6%, and 72.4% at ESS point. Even if there is small proportion of network members engaged in malicious attacking after ESS, the stable status of cooperative population is not invaded by malicious strategy. These simulation results prove that our proposed scheme can stimulate cooperation behavior among network members under a high malicious ratio as well as promote ratio of population participating in cooperative transmission so as to maintain normal services of MANETs.

Figure 3 shows the comparison of the cooperative population using our proposed stimulation scheme and the method not using stimulation scheme under original malicious ratio at 0%, 20%, 40%, and 60%, which are shown Figures 3(a), 3(b), 3(c), and 3(d), respectively. Note that in MANETs, especially in large scale MANETs, if there are more than 70% of network members refusing to cooperate with others, the network transmission service is suspended. Without loss of generality
the round number of the game which corresponds to the point of 30% of cooperative population is defined as network lifetime. From Figure 3, we can see that the network lifetime is effectively prolonged by improving cooperative population far above 30% using stimulation scheme compared with the other method. More specifically, under original malicious ratio at 0%, 20%, 40%, and 60% the network lifetime is 129 rounds, 63 rounds, 23 rounds, and 19 rounds, respectively, by using the method without stimulation scheme. While using our scheme, until the end of 500 rounds of the simulation, the network services are still maintained by large crowd of cooperative population (94.3%, 83.9%, 78.6%, and 72.4% when it comes to ESS). It can be inferred that in large scale MANETs (member number exceeds 5000) as well as high malicious ratio (>50%), our scheme still has a better performance.

Recall that in our proposed cooperative stimulation scheme, the time factor of the action space plays a role in coupling current and accumulated trust level of the members in MANETs; hence it contributes to the improvement in cooperative performance of the network. In order to verify and evaluate the impact of the time factor on cooperative population and convergence rate of the proposed evolutionary game, a series of simulations have been conducted. Figure 4 shows the result of the two kinds of settings of the time factor; one is time factor for each action at 0.5; that is, the updated trust level of the members is equal-weighted by the current value of trust level and that of accumulated value. The other one is time factor optimally by hierarchically weighting different action element; that is, the higher the risk level corresponding to action element, the smaller its time factor is set. By using hierarchical setting of time factor, the updated trust value by taking the higher risk action relies less on accumulated value. On the contrary, because of the larger value of time factor corresponding to beneficial action, the updated trust value relies more on accumulated value. Thus once the member takes action with a higher risk level, its trust level will be reduced immediately as punishment, and while taking actions that do not threaten the network, its reduction rate of trust level slows down with the increase of coupling degree. From Figure 4, we can see that, adopting the equal-weighted setting of time factor ((0.5, 0.5, 0.5, 0.5, 0.5)), the game gets into the ESS at the point of 439 game rounds and the cooperative population at this time remains 78.6% under original malicious rate at 40%. While in the same circumstances, not only the convergence rate, but also the cooperative population is superior to the previous result by using optimal hierarchical setting of time factor ((0.3, 0.2, 0.1, 0.4, 0.5)) whose value is 361 rounds and 87.3%, respectively. To sum up, the hierarchical setting method can be regarded as user interface which adjusts the risk level of various actions in our scheme.

In previous systematic simulations, all parameters are set to satisfy Theorem 2. When the transmission game gets into ESS, the optimum strategy space converges to the expected strategy space which can also make members obtain maximum payoff. In the following simulation, we need to evaluate another important index which mainly drives members to take which actions, that is, average payoff, and verify the effect of Theorem 2 in this paper. As can be shown in Figure 5, we compared 4 action spaces in our game, which are optimum action space (payoff-preference), expected action space satisfying Theorem 2 (convergent trust-preference), expected action space not satisfying Theorem 2 (nonconvergent trust level-preference), and expected action space not satisfying Theorem 2 with a hierarchical time factor (optimal attack classification). From the simulation result, under original malicious ratio at 50%, the optimum action space has the highest average payoffs during each round of the game (the average value of payoffs obtained by 5000 members is greater than 0.6 and grows top to 0.92). By contrast, the average payoffs of the other 3 action spaces are lower than optimum action space (about 0.4–0.8). On the other hand when members take optimum strategy, the cooperative population of the network does not increase in spite of the maximizing members’ payoffs. This is because that the strategy driven by obtaining maximized payoff principle is always attack, that is, violating to cooperate with each other. As a consequence, as shown in Figure 5(b), taking optimum strategy would reduce the cooperative population (as curve 1). According to our inference in this paper, expected strategy (trust-preference) can effectively stimulate members to cooperate with others, but it cannot bring members a satisfying payoff (as curve 4). To solve this problem, if parameters are set to satisfy Theorem 2, it can not only stimulate members to cooperate with others, but also increase average payoff of the whole network (as curves 2, 3). Moreover the strategy which is set to include hierarchical time factor performs better than that without hierarchical time factor (see curve 2), which well verifies the simulation result above.

To extend our theoretical game model to the application of realistic MANETs, there are 2 important indexes referring to network transmission service, transmission success rate (TSR) and normalized network throughput (NNT), which must be measured. So finally we conduct afterwards simulation to evaluate TSR and NNT using the proposed
cooperative stimulation scheme comparing to that using traditional multihop transmission scheme in large scale MANETs. The bar chart of Figure 6 shows the simulation result, where A, B, C, and D denote the member number of the network 2500, 5000, 7500, and 10000, respectively. From Figure 6, we can see that due to the increase of the cooperative population by using stimulation scheme, the TSR has been increased from 79% to 84% as the network member number ranges from 2500 to 10000. On the contrary, under original malicious ratio at 40% by using traditional multi-hop scheme the TSR drops dramatically from 71% to 42% which results in lacking of cooperation among network members. Then to

the index NNT which reflects the active degree of network information, as a matter of fact, a higher NNT means larger accommodation of data stream of MANETs. From Figure 6, the NNT has been effectively maintained from 62% only down to 54% with the growth of the network scale. But in the same situation, by using traditional multi-hop scheme the NNT has been reduced dramatically from 59% to 35%. Therefore, our proposed cooperative stimulation scheme can effectively serve date transmission in large scale MANETs with a higher malicious ratio.

7. Conclusion

In this paper, we have investigated an evolutionary game theoretic trust cooperative stimulation scheme for large scale MANETs to incent members to take cooperative actions with each other so as to maintain cooperative performance. By means of constructing the complete multirisk level strategy and payoff space and building trust-preferential strategy, the malicious action can be effectively constrained to a low trust level. Then through evolutionary analysis of game model, the convergence condition between optimum strategy which represents payoff maximization principle and trust-preferential strategy is deduced. Furthermore, the mobility probability parameters and information propagation error are also introduced into our scheme, which makes it approach to the realistic large scale MANETs. Both theoretical analysis and simulation experiments have demonstrated that although a gap may exist between the game model and reality, the game-theoretic approach can still provide thoughtful insights and helpful guidelines when stimulating members to cooperate with each other from multirisk level of purposive strategic attack in large scale MANETs. The proposed scheme can effectively stimulate cooperation among members and meanwhile be robust under the condition where the environment is harsh under a high original malicious ratio in large scale MANETs.
Acknowledgment

This work is supported by the National Natural Science Foundation of China under Grants nos. 61001138 and 61201317.

References

[1] H. Kim, R. B. Chitti, and J. Song, "Novel defense mechanism against data flooding attacks in wireless ad hoc networks," IEEE Transactions on Consumer Electronics, vol. 56, no. 2, pp. 579–582, 2010.

[2] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," IEEE Wireless Communications, vol. 14, no. 5, pp. 85–91, 2007.

[3] M. S. Fallah and M. Mouzarani, "A game-based sybil-resistant strategy for reputation systems in self-organizing MANETs," Computer Journal, vol. 54, no. 4, pp. 537–548, 2011.

[4] A. Alireza, T. Helen, and V. Athanasios, "A survey of security challenges in cognitive radio networks: solutions and future research directions," Proceedings of the IEEE, vol. 100, no. 12, pp. 3172–3186, 2012.

[5] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory," Sensors, vol. 11, no. 2, pp. 1345–1360, 2011.

[6] A. Rehan, K. Turgay, and G. V. Raju, "EML-Trust: an enhanced machine learning based reputation system for MANETs," Ad Hoc Networks, vol. 10, no. 3, pp. 435–457, 2012.

[7] H. Y. Shi, W. L. Wang, N. M. Kwok, and S. Y. Chen, "Game theory for wireless sensor networks: a survey," Sensors, vol. 12, no. 7, pp. 9055–9097, 2012.

[8] L. Blazevic, L. Buttyan, S. Ćapkun, S. Giordano, J. P. Hubaux, and J. Y. Le Boudec, "Self-organization in mobile ad hoc networks: the approach of terminodes," IEEE Communications Magazine, vol. 39, no. 6, pp. 166–173, 2001.

[9] L. Buttyán and J. P. Hubaux, "Stimulating cooperation in self-organizing mobile Ad Hoc networks," Mobile Networks and Applications, vol. 8, no. 5, pp. 579–592, 2003.

[10] P. Michiardi and R. Molva, "CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proceedings of the 6th Joint Working Conference on Communications and Multimedia Security (IFIP TC6/TC 11), pp. 107–121, 2002.

[11] S. Buchegger and J. Y. Le Boudec, "Performance analysis of the CONFIDANT protocol (Cooperation of nodes: fairness in dynamic ad-hoc networks)," in Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '02), pp. 226–236, June 2002.

[12] W. Yu and K. J. Ray Liu, "Attack-resistant cooperation stimulation in autonomous Ad Hoc networks," IEEE Journal on Selected Areas in Communications, vol. 23, no. 12, pp. 2260–2271, 2005.

[13] B. Niu, H. Jiang, and H. V. Zhao, "A cooperative multicast strategy in wireless networks," IEEE Transactions on Vehicular Technology, vol. 59, no. 6, pp. 3136–3143, 2010.

[14] Y. Chen and K. J. R. Liu, "Indirect reciprocity game modelling for cooperation stimulation in cognitive networks," IEEE Transactions on Communications, vol. 59, no. 1, pp. 159–168, 2011.

[15] L. Xiao, Y. Chen, W. S. Lin, and K. J. R. Liu, "Indirect reciprocity security game for large-scale wireless networks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 4, pp. 1368–1380, 2012.

[16] D. A. Maurizio, O. Francesco, and R. S. Pietro, "Can cooperation improve energy efficiency in ad hoc wireless networks?" Computer Communications, vol. 35, no. 14, pp. 1707–1714, 2012.

[17] H. Zhao, X. Yang, and X. Li, "An incentive mechanism to reinforce truthful reports in reputation systems," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 951–961, 2012.

[18] L. Ze and S. Haiying, "Game-theoretic analysis of cooperation incentive strategies in mobile Ad Hoc networks," IEEE Transactions on Mobile Computing, vol. 11, no. 8, pp. 1287–1303, 2012.

[19] L. Li, W. Cai, L. Liang, and L. Fan, "Design and analysis of Bayesian game in role based trust management," in Proceedings of the IEEE International Conference on Information Theory and Information Security (ICITIS’10), pp. 394–398, December 2010.

[20] A. K. Charles, P. Niki, and M. Kia, "Game theoretic modeling and evolution of trust in autonomous multi-hop networks," in Proceedings of the IEEE International Conference on Communications (ICC ‘11), Kyoto, Japan, June 2011.

[21] D. Wu, Y. Cai, and J. Wang, "Cooperation policy selection for energy-constrained Ad Hoc networks using correlated equilibrium," IEEE Communications Letters, vol. 16, no. 3, pp. 349–351, 2012.

[22] T. Chen, L. Zhu, F. Wu, and S. Zhong, "Stimulating cooperation in vehicular ad hoc networks: a coalitional game theoretic approach," IEEE Transactions on Vehicular Technology, vol. 60, no. 2, pp. 566–579, 2011.

[23] W. Yu and K. J. R. Liu, "Secure cooperation in autonomous mobile ad-hoc networks under noise and imperfect monitoring: a game-theoretic approach," IEEE Transactions on Information Forensics and Security, vol. 3, no. 2, pp. 317–330, 2008.

[24] F. Li, Y. Yang, and J. Wu, "Attack and flee: game-theory-based analysis on interactions among nodes in MANETs," IEEE Transactions on Systems, Man, and Cybernetics B, vol. 40, no. 3, pp. 612–622, 2010.
Submit your manuscripts at
http://www.hindawi.com