Wireless sensor networks (WSNs) provide network services through the cooperation of sensor nodes, while the basis of cooperation depends on the trust relationships among the nodes. In this paper, we construct an evolutionary game-based trust strategy model among the nodes in WSNs, and we subsequently introduce a strategy adjustment mechanism into the process of game evolution to make up for the deficiency that the replicator dynamic model cannot reflect the requirement of individual strategy adjustments. Afterward, we derive theorems and inferences in terms of the evolutionary stable state through dynamic analyses, providing a theoretical basis for WSN trust management. Furthermore, we verify the theorems and inferences with different parameter values, especially the trust incentive and the upper limit of data retransmission after packets are lost, and both of them are closely related to the evolutionary stable state. The experiments demonstrated that, under certain conditions, the involved nodes can finally reach a stable state of the system by constantly adjusting their trust strategy. At the same time, the speed of evolution of our strategy adjustment mechanism in achieving the stable state is much faster than that of the usual replicator dynamic evolution method.

1. Introduction

Recently, WSNs have developed from a promising research area to a useful technology that is applicable to real-world scenarios. Akyildiz et al. [1] have classified the applications of WSNs as military applications, environmental applications, health applications, home applications, and other commercial applications. In the near future, WSNs that are comprised of small-size, low-power sensor nodes will become an integral part of our lives.

Similar to any computer-related environment, security in WSNs is considered to be nonfunctional but an essential requirement that keeps the complex system available and reliable [2]. In recent years, in addition to the traditional cryptography-based network security technology, trust-based security mechanisms have gradually attracted more attention from academia and industry. The concept of Trust was proposed in a trust management mechanism in WSNs [3–7], and cooperation between the nodes is based on the Trust concept. Studies on the trust strategy and trust evolution process of WSN nodes address an important part of trust management, and they play a significant role in the stability and safety of WSNs. From the perspective of a single node in a WSN, Trust can promote coordination among the nodes and reduce the risk when cooperating with other nodes. From the perspective of the whole WSN, trust management evolves through trust among nodes and improves the cooperation among the nodes as much as possible, following a trust strategy that is based on the payoffs of the nodes. The system could reach a stable state following evolution and maintain normal communication in the network.

Game theory as a mathematical theory tool focuses mainly on the competitive and cooperative relationship of the participants, and it has been widely used in the field of WSN security. In [8], Shen et al. summarized the current research of different types of games in WSN security. Among various methods of game theory, the evolution game
takes the changing trend of the overall population as the research object, where sensor nodes of WSNs are viewed as an individual, and all of the sensor nodes are an overall population. After the continuous evolution of a population, a trust management system guides the individual nodes to make trust decisions that maximize their utilities, and the rate of individuals who choose the strategy that has a higher gain will increase. Conversely, the rate of individuals who choose a strategy that has a lower gain will correspondingly decrease. Thus, the rate of individuals who choose their corresponding strategies remains stable, and the population will finally reach a game equilibrium state. Therefore, it is meaningful for us to study the trust decision model and the evolutionary process of WSNs using evolutionary game theory.

In this paper, we analyze the data retransmission behavior after packets are lost in the communication process of WSNs. Based on this approach, we set up the trust strategy game model, which reflects the gains and losses of the involved nodes. Additionally, we use a new dynamic evolution method that is based on strategy adjustment, to derive and further prove the related theorems and inferences in terms that involve how to use the trust strategy game model for the system to reach a stable state. In the end, we verify the theorems and inferences that are derived following the simulated experiments, and show the advantage of our dynamic evolution method based on strategy adjustment through a comparison with the usual replicator dynamic evolution method. Thus, the rate of individuals who choose the corresponding strategies remains stable, and the population will finally reach a game equilibrium state. Therefore, it is meaningful for us to study the trust decision model and the evolutionary process of WSNs using evolutionary game theory.

The remainder of this paper is organized as follows. In Section 2, we overview related research and focus on the difference between our work and other related studies. In Section 3, we set up the trust strategy game model. In Section 4, we propose a new dynamic evolution method that is based on strategy adjustment. In Section 5, we analyze the evolution process that follows from our dynamic evolution method and we derive and prove the related theorems and inferences about the evolved stable state. In Section 6, the simulation results confirm the conclusions and the advantage of the proposed evolution method is illustrated. Finally, the conclusions are provided in Section 7.

2. Related Work

The process of maintaining security using a trust mechanism in wireless networks can be observed as a process of strategy interaction. The trust decision of a node could affect the trust decision (trust or distrust) of the other nodes and the network state (security or insecurity), where the decision-making process can be explained and analyzed by game theory. Thus, there are many scholars who have studied trust and cooperation of wireless networks using different types of game theory, such as the noncooperation game [9–11], cooperation game [12], Bayesian game [13], and evolutionary game [14–24]. The various branches of game theory have corresponding applications in research on trust for security in wireless networks.

Mejia et al. [11] proposed a trust model that is based on a noncooperative game that uses a bacterial-like algorithm to allow the nodes to quickly learn the appropriate cooperation behavior. Based on cooperative game theory, Palomar et al. [12] proposed a new technique for handling security issues in mobile wireless sensor networks. They defined a game between sensor nodes and concentrated on three fundamental factors: cooperation, reputation, and quality of security, and they proposed a method for calculating the trust degree of nodes based on the amount of cooperation. In [13], Agah et al. developed a model that is based on Bayesian game theory, which is capable of formally explaining the characteristics of ad hoc networks. They further described a simple strategy that enforces cooperation among nodes.

Among the methods of game theory, the evolutionary game becomes a new type of effective method for trust and cooperation of nodes in wireless networks because an evolutionary game has the characteristic of limited rationality. Thus, the dynamic evolutionary game method has been widely used [15–18]. Dong et al. [19] provided a model for the optimization and stability of Internetware systems and improved their credibility with the Wright-Fisher process, which makes the whole system steady for a long time. Komathy et al. [20] analyzed the selfishness of neighboring nodes in MANET and followed a dynamic evolution with a fixed strategy or a random strategy. Finally, their system could reach a cooperation level of the nodes that increased to 100%.

Seredynski and Bouvy [21] addressed the problem of node cooperation in the network using an evolution game that considered the impact of the network size and node type on the cooperation among the nodes. The authors analyzed the specific case in which a reputation system is not present in the network and investigated whether cooperation is dependent on the information type that is used by the trust systems of the network participants.

In the evolutionary game trust model, some work introduced incentives to encourage the nodes to cooperate. Shen et al. [22] introduced incentives for the trust decision problem, for example, a node that obtained additional income by selecting a trust strategy. These authors also studied the dynamic evolution process of trust strategy choice of nodes.
and derived conditions for the evolutionary stable strategy. Chen et al. [23] built a dynamic incentive mechanism to adapt to WSNs based on evolutionary game theory, which enables the selfish nodes to cooperate with one another, to ensure normal network services. Wang et al. [24] proposed an evolutionary game-based trust cooperative simulation model for large-scale MANETs. They constructed a trust-preferential expected action space that effectively confined malicious members to obtaining illegal payoffs. Finally, through evolutionary analysis of a game model, they deduced the convergence condition between the optimum strategy and a trust-preferential strategy.

Thus far, the basic evolutionary game thoughts have been mostly derived from the research results of Taylor and Jonker [25]. Currently, in evolutionary game theory, the replicator dynamic equation is a dynamic evolution equation with a selection mechanism. The establishment of a replicator dynamic equation is an important symbol-adjusting process of a group behavior. This approach can better reflect and predict the evolution results, but its limitation is obvious. The replicator dynamic studies only the changing trend of the overall group rather than the strategy choice process of individuals. In this paper, we learn the evolutionary dynamics based on the rethinking mechanism from [26] for the strategy choice, and we propose a strategy adjustment mechanism that is based on dynamic evolution. This mechanism designs the choice process of individual strategies, and an individual is likely to change its current strategy at each game. The individual will imitate the opponent’s strategy as its new strategy, and the probability of the new choice strategy depends on the rate of individuals taking this strategy currently. This method accounts for the process of an individual’s strategy choice based on dynamic evolution in such a way as to make up for the deficiency of the replicator dynamic model.

Compared to [22–24], our work is distinguishable in terms of the type of factors in the game and the process of the dynamics. Our ideas derive partly from the trust strategy model [22]; however, considering the data retransmission after the packets are lost, we build a different trust strategy game model and we propose a strategic adjustment mechanism that is introduced into the process of game evolution. As a result, we obtain different theorems compared to [22]. Furthermore, our work focuses centrally on the incentive mechanism for trust decisions of sensor nodes in WSNs, while Chen et al. [23] studied the incentive mechanism for selfish nodes and Wang et al. [24] studied the situation of large-scale MANETs. Overall, our work is different from the related studies described above, and the theorems and inferences on the evolution stable state could provide a theoretic foundation for trust mechanisms of sensor nodes in WSNs.

3. Node Trust Game Model of WSNs

3.1. Network Model

3.1.1. Strategy Description. WSNs adopt mainly the packet retransmission mode; in other words, the data are sent from a source node to the target node by forwarding from other nodes. Each node has two strategy choices: Trust or Distress. In general, a node chooses the strategy Trust, which can help other nodes forward packets in such a way as to enhance its credibility and then obtain the gains. If a node chooses the strategy Distress, it will drop the packets from other nodes to save its energy, but it might not obtain the gains. In such a case, the other nodes will suffer a loss due to the rejection.

To describe this process clearly, we introduce five symbols, as shown in Table 1.

3.1.2. Data Retransmission after Packets Are Lost. Packet loss during the network forwarding process is caused mainly by a network that has unreliable factors, such as weather and the energy of the nodes. In other words, the more unreliable a network is, the more serious the packet loss situation is.

Assume that all of the nodes in the network have the same unreliable factors, and, then, any node will have the same probability of successfully sending the data packet at any one time. Note that the probability is \( q \). When a data packet transmission fails, the nodes trend to retransmit the packet until it forwards the data packet successfully. In general, the system will set a retransmission upper limit and stop retransmitting once the number of times for resending exceeds the upper limit. \( N \) represents the upper limit.

Obviously, the total number of retransmitting data packets obeys a geometrical distribution, when the packet transmission is successful. Because the successful probability of sending the data packet at any one time is \( q \), the successful transmission probability within the retransmission upper limit \( N \) is \( 1 - (1 - q)^N \), which we set as \( \omega \), and usually \( \omega > 0 \) in reality. With one interaction, if the data packet transmission fails, the cost is \( NC \), which we set as \( C_1 \). Otherwise, the cost is \( C_2 \). The expectation for the total number of times for sending the data packets is \( C_2 \), if the data packet transmission is successful within one interaction. Hence, it is easy to derive the probability of the number of transmitting times \( k \).

Consider

\[
P \{ x = k \mid x \leq N \} = \frac{P \{ x = k, x \leq N \}}{P \{ x \leq N \}} = \frac{(1 - q)^{k-1}q}{1 - (1 - q)^N},
\]

Table 1: Symbol descriptions.

| Symbol | Description |
|--------|-------------|
| \( G_T \) | Gain obtained by a sensor node choosing the strategy Trust, which helps other nodes to successfully transfer data packets |
| \( G_C \) | Cooperation gain of a sensor node due to its counterpart choosing the strategy Trust and successfully transferring data packets |
| \( C \) | Cost caused by a sensor node sending its own data packets or forwarding others’ data packets |
| \( L \) | Uncooperative loss of a sensor node due to its counterpart choosing the strategy Distress, and the data packets do not reach the target node |
| \( \alpha T \) | The trust incentive for cooperation, where \( T \) is the trust value of a node, \( \alpha \) is an adjustment factor, and \( \alpha T \geq 0 \) |
Table 2: Payoffs of both interaction nodes choosing the strategy Trust.

| Serial number | A send | A forward | B send | B forward | Probability P | A profit | B profit |
|---------------|--------|----------|--------|-----------|--------------|----------|----------|
| 1             | 1      | 1        | 1      | 1         | \( \omega \) | \( G_T + G_C + \alpha T - 2C_2 \) | \( G_T + G_C + \alpha T - 2C_2 \) |
| 2             | 1      | 1        | 1      | 0         | \( \omega(1 - \omega) \) | \( G_T + \alpha T - 2C_2 - L \) | \( G_C - \alpha T - C_1 - C_2 \) |
| 3             | 1      | 1        | 0      | 1         | 0             | \( - \) | \( - \) |
| 4             | 1      | 1        | 0      | 0         | 0             | \( - \) | \( - \) |
| 5             | 1      | 0        | 1      | 1         | \( \omega(1 - \omega) \) | \( G_C + \alpha T - C_1 - C_2 \) | \( G_T + \alpha T - 2C_2 - L \) |
| 6             | 1      | 0        | 1      | 0         | \( \omega^2(1 - \omega)^2 \) | \( \alpha T - C_1 - C_2 - L \) | \( \alpha T - C_1 - C_2 - L \) |
| 7             | 1      | 0        | 0      | 1         | \( \omega(1 - \omega) \) | \( G_C + \alpha T + C_2 \) | \( G_T + \alpha T - C_1 - C_2 - L \) |
| 8             | 1      | 0        | 0      | 0         | \( \omega(1 - \omega)^2 \) | \( \alpha T - C_1 - L \) | \( \alpha T - 2C_2 - L \) |
| 9             | 0      | 1        | 1      | 1         | \( \omega(1 - \omega) \) | \( G_T + \alpha T - C_1 - C_2 - L \) | \( G_C + \alpha T - C_2 \) |
| 10            | 0      | 1        | 0      | 0         | \( 0 \) | \( - \) | \( - \) |
| 11            | 0      | 1        | 0      | 0         | \( 0 \) | \( - \) | \( - \) |
| 12            | 0      | 0        | 1      | 1         | \( \omega(1 - \omega) \) | \( G_C + \alpha T + C_2 \) | \( G_T + \alpha T - C_1 - C_2 - L \) |
| 13            | 0      | 0        | 0      | 1         | \( \omega(1 - \omega)^2 \) | \( \alpha T - 2C_1 - L \) | \( \alpha T - C_2 - L \) |
| 14            | 0      | 0        | 0      | 1         | \( \omega(1 - \omega)^2 \) | \( \alpha T - 2C_1 - L \) | \( \alpha T - C_2 - L \) |
| 15            | 0      | 0        | 0      | 0         | \( \omega(1 - \omega)^2 \) | \( \alpha T - C_1 - L \) | \( \alpha T - nC - L \) |

Table 3: Payoffs of one of the interaction nodes choosing the strategy Trust.

| Serial number | A send | A forward | B send | Probability P | A profit | B profit |
|---------------|--------|----------|--------|--------------|----------|----------|
| 1             | 1      | 1        | 1      | \( \omega \) | \( G_T + \alpha T - 2C_2 - L \) | \( G_C - C_2 \) |
| 2             | 1      | 1        | 0      | 0             | \( - \) | \( - \) |
| 3             | 1      | 0        | 0      | \( \omega(1 - \omega) \) | \( \alpha T - C_2 - C_1 - L \) | \( -L - C_2 \) |
| 4             | 1      | 0        | 0      | \( \omega(1 - \omega) \) | \( \alpha T - C_2 - L \) | \( -L - C_1 \) |
| 5             | 0      | 1        | 1      | \( \omega(1 - \omega) \) | \( G_T + \alpha T - C_1 - C_2 - L \) | \( G_C - C_2 \) |
| 6             | 0      | 0        | 1      | 0             | \( - \) | \( - \) |
| 7             | 0      | 0        | 0      | \( \omega(1 - \omega) \) | \( \alpha T - 2C_1 - L \) | \( -L - C_2 \) |
| 8             | 0      | 0        | 0      | \( \omega(1 - \omega)^2 \) | \( \alpha T - C_1 - L \) | \( \alpha T - nC - L \) |

The corresponding expectation is as follows:

\[
C_2 = E(x) = \sum_{k=1}^{N} k \cdot P \{ x = k \mid x \leq N \} = \frac{qC}{1 - (1 - q)^N} \sum_{k=1}^{N} k \cdot (1 - q)^{k-1}. \tag{2}
\]

To simplify the progression \( \sum_{k=1}^{N} k \cdot (1 - q)^{k-1} \), we can easily obtain

\[
\sum_{k=1}^{N} k \cdot (1 - q)^{k-1} = \frac{1 - (N + 1)(1 - q)^N + N(1 - q)^{N+1}}{q^2}. \tag{3}
\]

Thus, there exists

\[
C_2 = E(x) = \frac{qC}{1 - (1 - q)^N} \cdot \frac{1 - (N + 1)(1 - q)^N + N(1 - q)^{N+1}}{q^2}. \tag{4}
\]

and taking \( \omega = 1 - (1 - q)^N \) into \( E(x) \), we derive

\[
C_2 = E(x) = \frac{\omega - Nq + Nq\omega}{q\omega} \cdot C. \tag{5}
\]

3.2. Trust Game Model. When the WSN nodes interact with one another, each node can choose either the strategy Trust or the strategy Distrust. The network usually has unreliable factors, which lead to a failure when sending a data packet to other nodes; thus, the nodes could interact with one another by two types of strategies, which could result in different gains. The different conditions on transmitting the packets are discussed as follows.

For Tables 2, 3, 4, and 5, we give an explanation of each symbol: \( P \) represents the probability that each event occurs, 1 and 0 means success and failure, respectively, and “—” means an impossible event in real life, regardless of its payoffs.

3.2.1. Both Interaction Nodes Choose the Strategy Trust. When two nodes A and B interact, each node has two actions, namely, send and forward. In addition to, due to the unreliable factors in the network, each action has two possible results, either success or failure. As shown in Table 2, there are 16
different events in all. This table shows the probability of each event occurring and the gains of the nodes.

We can see that, in Table 2, when two interactive nodes both choose the strategy Trust, the expected payoff of each node is the summary of multiplying each probability by its corresponding payoff. Thus, the total payoff is equal for the nodes A and B; that is, \(\omega\) corresponds payoff. Thus, the total payoff is equal for the nodes A and B; that is, the summary of multiplying each probability by its corresponding payoff. Thus, the total payoff is equal for the nodes A and B; that is, the summary of multiplying each probability by its corresponding payoff. Thus, node A of each node is also the summary of multiplying each probability by its corresponding payoff. Thus, node A

| Serial number | A send | B send | Probability P | A profit | B profit |
|---------------|--------|--------|---------------|----------|----------|
| 1             | 1      | 1      | \(\omega\)    | \(-C_2 - L\) | \(-C_2 - L\) |
| 2             | 1      | 0      | \(\omega(1 - \omega)\) | \(-C_2 - L\) | \(-C_1 - L\) |
| 3             | 0      | 1      | \(\omega(1 - \omega)\) | \(-C_2 - L\) | \(-C_2 - L\) |
| 4             | 0      | 0      | \((1 - \omega)^2\) | \(-C_1 - L\) | \(-C_1 - L\) |

### Table 4: Payoffs of both interactive nodes choosing the strategy Distrust.

| Trust          | Distrust                        |
|----------------|---------------------------------|
| \(\omega^2G_T + \omega^2G_C + \omega^2L + \alpha T\) | \(\omega^2G_T + \alpha T - (1 - \omega^2)C_1 - (\omega + \omega^2)C_2 - L\) |
| \(-\omega^2G_C - \omega^2L - (1 - \omega)C_1 - \omega C_2 - L\) | \(-1(1 - \omega)C_1 - \omega C_2 - L\) |

### Table 5: Matrix of payoffs.

3.2.2. One of the Interacting Nodes Chooses the Strategy Trust. When two nodes A and B interact, and, in that interaction, A chooses the strategy Trust while B chooses the strategy Distrust, A has two actions, send and forward, while B has only the action send. As shown in Table 3, there are 8 different events in all. We can see that when only one node chooses the strategy Trust between the interactive nodes, the expected payoff of each node is also the summary of multiplying each probability by its corresponding payoff. Thus, node A choosing the strategy Trust can obtain the payoff of \(\omega^2G_T + \omega^2G_C + \omega^2L + \alpha T - (1 - \omega^2)C_1 - (\omega + \omega^2)C_2 - L\), while B choosing the strategy Distrust can obtain the payoff of \(\omega^2G_C + \omega^2L - (1 - \omega)C_1 - \omega C_2 - L\).

3.2.3. Both Interactive Nodes Choose the Strategy Distrust. If both of the two interactive nodes A and B choose the strategy Distrust, then nodes A and B have only one action left, which is send. As shown in Table 4, there are 4 different events in all. We can see the probability of each event occurring and the payoffs of the nodes.

According to Table 4, when both of the two interactive nodes choose the strategy Distrust, the expected payoff of each node is also the summary of multiplying each probability by its corresponding payoff. Thus, the total payoff is equal for the nodes A and B; that is, \(-C_2 - L\).

### Definition 1. The WSNs node trust game is a 4-tuple \(\mathbb{R}(W, N, S, U)\), where

1. \(W\) is a population that is composed of a very large number of individuals (sensor nodes in WSNs);
2. \(N\) is the set of individuals who are in the same population \(W\);
3. \(S\) is the set of strategies, and \(S = \{s_1, s_2\} = \{\text{Trust}, \text{Distrust}\}\);
4. \(U\) is a payoff matrix that is formed from the utilities of the game between the two individuals, and its value is shown in Table 5.

### 4. Strategy Adjustment Based on the Evolutionary Game

In this section, we introduce the dynamic evolution method for adjusting the strategies, to make up for the deficiency in the replicator dynamic. During the process of evolution, each individual in the game constantly adjusts the current strategy in such a way as to enable the individual to modify its current strategy with a certain probability.

Let \(S = \{s_1, s_2, \ldots, s_k\}\) be a pure strategy set, and each strategy can be chosen by individuals. Let a vector \(x_i = [x_{i1}, x_{i2}, \ldots, x_{ik}]\) be the overall situation, where \(x_i\) is the probability of choosing the strategy \(i \in S\); \((i, j)\) denotes a game for two individuals who are choosing the strategies \(i\) and \(j\), and the probability of this game is \(x_i x_j\). After playing a game, the two individuals learn from each other and rethink the current strategy and its benefits, and, then, they each observe the other’s strategy and benefits. If the opponent’s payoff is better than that of its own, then the node would change its strategy into the opponent’s strategy with a certain probability. Let \(p_i^j(x)\) be the transition probability from strategy \(i\) to \(j\).

Therefore, after a game \((i, j)\), the state becomes \((i, i)\) through learning with the probability \((1 - p_i^j(x))p_i^j(x), (j, i)\) with the probability \(p_i^j(x)p_i^j(x), (j, j)\) with the probability \(p_i^j(x)(1 - p_i^j(x)), (i, j)\) with the invariant probability \((1 - p_i^j(x))(1 - p_i^j(x)).\) For the first situation \((i, i)\), one more node that chooses the strategy \(i\) is added, while the number of nodes that choose the strategy \(j\) is one less. For the third situation, \((j, j)\), the number of nodes that choose the strategy \(i\) is one less and one more for nodes that choose the strategy \(j\). On the second and fourth cases \((j, i)\) and \((i, j)\), the number of nodes that choose the strategies \(i\) and \(j\) does not change, and, thus, the ratio of the number of individuals who
choose the strategy does not change. It can be concluded that, after the individuals learn from each other and adjust their strategies, the dynamic equation for the ratio of the number of individuals who choose strategy \( i \) is

\[
F(x_i) = x_i \cdot \sum_{j \in S} \left[ (1 - p_j^i(x)) \cdot p_j^i(x) - p_j^i(x) \right] \cdot (1 - p_j^i(x)) \right] 
= x_i \cdot \sum_{j \in S} [p_j^i(x) - p_j^i(x)] . \tag{6}
\]

When the two nodes play a game once, one of the nodes will compare its gain with the other’s. If the gain from its strategy is less than that of the other node’s gain, then the first node will adjust its strategy to be the other node’s strategy. In contrast, it will use its own strategy. We introduce the trust strategy adjustment mechanism in such a game.

Based on the analysis above, we use a probabilistic method to quantify the strategy adjustment.

**Definition 2** (see [26]). In the WSNs node trust game, when the nodes that choose the pure strategy \( i \) play games with the nodes that choose the pure strategy \( j \), the probability \( p_j^i(x) \) of adjusting the pure strategy \( i \) to the pure strategy \( j \) is defined as \( m \cdot u(j, x) - n \cdot u(i, x) \), where \( m > 0, n > 0, \) and \( 0 < m \cdot u(j, x) - n \cdot u(i, x) < 1 \). Here, \( u(i, x) \) means the total benefit expectation of choosing the pure strategy \( i \) under situation \( x \).

In Definition 2, \( m \cdot u(j, x) - n \cdot u(i, x) \) is the probability of strategy adjustment, which guarantees its value in a reverse way with its own benefit \( u(i, x) \) and in a positive way with the opposite benefit \( u(j, x) \).

### 5. Trust Game Model Analysis

**5.1. Evolution Dynamics Analysis.** Because the stable state \( x^* \) of the evolutionary game possesses stability, in this state, it will eventually revert back to the \( x^* \) state even if there are a small number of mutations. According to the nature of stability of the equilibrium point of differential equations, the evolutionary stable state \( x^* \) requires the satisfaction of (6), where the function value of \( x^* \) equals 0, and the derivative of \( x^* \) is less than 0; in other words, \( F(x^*) = 0 \) and \( F'(x^*) < 0 \).

According to Definitions 1 and 2 and (6), the dynamic equation for the individual proportion of choosing the strategy Trust is derived as follows:

\[
F(x_1) = x_1 \cdot x_2 \cdot \left[ (m \cdot u(s_1, x) - n \cdot u(s_2, x)) - (m \cdot u(s_2, x) - n \cdot u(s_1, x)) \right] , \tag{7}
\]

where \( x_1 \) and \( x_2 \) represent an individual proportion of choosing the strategies Trust and Distrust, respectively, and the equation \( x_1 + x_2 = 1 \) is satisfied. For ease of expression, we denote \( x_1 \) as \( \bar{x} \). Let \( u(s_1, x) \) be \( u_1(\bar{x}) \), and let \( u(s_2, x) \) be \( u_2(\bar{x}) \). In fact, \( u_1(\bar{x}) \) and \( u_2(\bar{x}) \) represent the total benefit expectations for the nodes that have the strategies of Trust and Distrust, respectively. Therefore,

\[
u_1(\bar{x}) = \bar{x} \cdot \left[ \omega^2 G_T + \omega^2 C_C + \omega^2 L + \alpha T - (1 - \omega^2) C_1 - (\omega + \omega^2) C_2 - L \right] + (1 - \bar{x}) \cdot \left[ \omega^2 G_T + \alpha T - (1 - \omega^2) C_1 - \omega C_2 - L \right]
\]

\[
u_2(\bar{x}) = \bar{x} \cdot \left[ \omega^2 G_C + \omega^2 L - (1 - \omega) C_1 - \omega C_2 - L \right] + (1 - \bar{x}) \cdot \left[ -(1 - \omega) C_1 - \omega C_2 - L \right]. \tag{8}
\]

Place (8) and (9) into (7), and let (7) equal 0; then,

\[
\begin{align*}
F(\bar{x}) &= \bar{x} \cdot (1 - \bar{x}) \cdot \left[ (m \cdot u_1(\bar{x}) - n \cdot u_2(\bar{x})) - (m \cdot u_2(\bar{x}) - n \cdot u_1(\bar{x})) \right] \\
&= \bar{x} \cdot (1 - \bar{x}) \cdot (m + n) \cdot \left[ u_1(\bar{x}) - u_2(\bar{x}) \right] \\
&= \bar{x} \cdot (1 - \bar{x}) \cdot (m + n) \cdot \left[ \omega^2 G_T + \alpha T - (1 - \omega^2) C_1 - \omega C_2 - L \right]. \tag{9}
\end{align*}
\]

It is easy to obtain the two solutions to the equation: \( \bar{x}_1 = 0 \) and \( \bar{x}_2 = 1 \). In other words, the evolutionary game yields two evolutionary stable states: \( \bar{x}_1^* = 0 \) and \( \bar{x}_2^* = 1 \).

**Theorem 3.** If \( \omega^2 G_T + \alpha T - (1 - \omega^2) C_1 - \omega^2 C_2 > 0 \), then \( \bar{x}_2^* = 1 \) is the evolutionary stable state of the WSNs trust game.

**Theorem 4.** If \( \omega^2 G_T + \alpha T - (1 - \omega^2) C_1 - \omega^2 C_2 < 0 \), then \( \bar{x}_1^* = 0 \) is the evolutionary stable state of the WSNs trust game.

**Proof.** To prove that \( x^* \) is an evolutionary stable state, according to the judgment theorem of stability for the ordinary differential equation, we could equally prove the solution of \( F(x^*) = 0 \) and \( F'(x^*) < 0 \).

Because \( \bar{x}_1^* = 0 \) and \( \bar{x}_2^* = 1 \) are calculated from (10), we have, thus, \( F(\bar{x}_1^*) = 0 \) and \( F(\bar{x}_2^*) = 0 \).

Taking the derivative of \( F(\bar{x}) \) in (10), we obtain

\[
F'(\bar{x}) = (1 - 2\bar{x}) \cdot (m + n) \cdot \left[ \omega^2 G_T + \alpha T - (1 - \omega^2) C_1 - \omega^2 C_2 \right]. \tag{11}
\]

Taking \( \bar{x}_1^* \) and \( \bar{x}_2^* \) into (11), we obtain

\[
\begin{align*}
F'(\bar{x}_1^*) &= (m + n) \cdot \left[ \omega^2 G_T + \alpha T - (1 - \omega^2) C_1 - \omega^2 C_2 \right] \\
F'(\bar{x}_2^*) &= -(m + n) \cdot \left[ \omega^2 G_T + \alpha T - (1 - \omega^2) C_1 - \omega^2 C_2 \right]. \tag{12}
\end{align*}
\]

According to Definition 2, it is easy to know that \( m + n > 0 \). When \( \omega^2 G_T + \alpha T - (1 - \omega^2) C_1 - \omega^2 C_2 > 0 \), we can obtain \( F'(\bar{x}_1^*) > 0 \) and \( F'(\bar{x}_2^*) < 0 \) following (12). According to the
stability of the equilibrium point of the differential equations, \( x_2^* = 1 \) is the evolutionary stable state of the WSNs trust game, and, then, Theorem 3 is proved.

When \( \omega^2G_T + \alpha T - (\omega - \omega^2)C_1 - \omega^2C_2 < 0 \), we can obtain \( F'(\tilde{x}_1^*) < 0 \) and \( F'(\tilde{x}_2^*) > 0 \), which follow from (12). According to the stability of the equilibrium point of the differential equations, \( \tilde{x}_1^* = 0 \) is the evolutionary stable state of the WSNs trust game; thus, Theorem 4 is proved.

Under the conditions of Theorem 3, only the Nash equilibrium can be used to choose a trust strategy for both sides; this equilibrium is strictly a dominant and stable evolution. In other words, regardless of what strategy node B will choose, the total income for node A choosing the Trust strategy is always greater than that of choosing the Distrust strategy. Regardless of what the initial state is for all of the nodes, the network will eventually reach a stable state in which all of the nodes choose a Trust strategy through evolution.

Under the conditions of Theorem 4, only the Nash equilibrium can be used to choose a Distrust strategy for both sides; this equilibrium is strictly a dominant and stable evolution. In other words, regardless of what strategy node B chooses, the total income for node A choosing the Distrust strategy is always greater than that of choosing the Trust strategy. Regardless of what the initial state is for all of the nodes, the network will eventually reach a stable state in which all of the nodes choose a Distrust strategy through evolution.

5.2. Trust Model Analysis. To ensure the security and stability of the WSNs and to improve the mutual trust among the nodes, we can adjust the controllable parameters in the WSNs’ trust mechanisms to satisfy the conditions of Theorem 3 and avoid the conditions of Theorem 4. After we take \( C_1 \) and \( C_2 \) from Section 3.1.2 into \( \omega^2G_T + \alpha T - (\omega - \omega^2)C_1 - \omega^2C_2 \), through derivation, we can obtain the following:

\[
\omega^2G_T + \alpha T - (\omega - \omega^2)C_1 - \omega^2C_2 = \omega^2G_T + \alpha T - \omega^2 \left( \frac{Nq + N\omega}{q\omega} \right) C_1 = \omega^2 \left( \frac{G_T - C}{q} \right) + \alpha T,
\]

(13)

where \( \omega = 1 - (1 - q)^N \). In general, \( G_T, C, \) and \( q \) are related to the environment and can be regarded as constants.

From (13), we know that \( \omega^2G_T + \alpha T - (\omega - \omega^2)C_1 - \omega^2C_2 \) is related to the retransmission upper limit \( N \) and the trust incentive degree \( \alpha T \). It is easy to generate the following inferences.

**Inference 1.** Improving the trust incentive \( \alpha T \) contributes to achieving an evolutionary stable state \( \tilde{x}_2^* = 1 \).

**Proof.** If the trust incentive \( \alpha T \) is improved, then \( \omega^2G_T + \alpha T - (\omega - \omega^2)C_1 - \omega^2C_2 \) becomes larger. When \( \alpha T \) is improved to a suitable value for \( \omega^2G_T + \alpha T - (\omega - \omega^2)C_1 - \omega^2C_2 > 0 \) that satisfies the conditions of Theorem 3, it can allow networks to achieve an evolutionary stable state \( \tilde{x}_2^* = 1 \). Inference 1 is then proved.

**Inference 2.** When \( G_T - (C/q) > 0 \), \( \tilde{x}_2^* = 1 \) is an evolutionary stable state of the WSNs trust game.

**Proof.** When \( G_T - (C/q) > 0 \), for \( \omega^2 > 0 \) and \( \alpha T \geq 0 \), we obtain \( \omega^2G_T + \alpha T - (\omega - \omega^2)C_1 - \omega^2C_2 = \omega^2(G_T - (C/q)) + \alpha T > 0 \), which satisfies the conditions of Theorem 3. Therefore, the networks can achieve an evolutionary stable state of \( \tilde{x}_2^* = 1 \). Inference 2 is thus proved.

**Inference 3.** When \( G_T - (C/q) < 0 \) and \( \alpha T > qC - q^2G_T \), if we reduce the retransmission upper limit \( N \), this step can benefit the networks in achieving an evolutionary stable state of \( \tilde{x}_2^* = 1 \).

**Proof.** When \( G_T - (C/q) < 0 \), there is a reward mechanism; that is, \( \alpha T > 0 \). If we reduce the retransmission limit \( N \), then \( \omega = 1 - (1 - q)^N \) becomes smaller, while \( \omega^2(G_T - (C/q)) + \alpha T \) becomes larger. If we reduce \( N \) to a minimum value \( 1 \) and put \( \alpha T > qC - q^2G_T \), then

\[
\omega^2 \left( \frac{G_T - C}{q} \right) + \alpha T > q^2 \left( \frac{G_T - C}{q} \right) + qC - q^2G_T = 0.
\]

From (13), we obtain

\[
\omega^2G_T + \alpha T - (\omega - \omega^2)C_1 - \omega^2C_2 = \omega^2 \left( \frac{G_T - C}{q} \right) + \alpha T > 0,
\]

(15)

which satisfies the conditions of Theorem 3; the networks can then achieve an evolutionary stable state \( \tilde{x}_2^* = 1 \). Inference 3 is thus proved.

5.3. Comparison with Replicator Dynamics. Replicator dynamics are one of the dynamic evolution methods in evolutionary game theory; the replicator dynamic equation is described as follows:

\[
F(x_i) = x_i \cdot [u(i, x) - \overline{u}(x, x)],
\]

(16)

where \( x_i \) is the probability of choosing strategy \( i \), \( u(i, x) \) means the total benefits expectation of choosing the pure strategy \( i \), and \( \overline{u}(x, x) \) represents the average payoff of the individuals.

We put (8) and (9) into (16). It is easy to obtain the game model of Definition 1, according to which the replicator dynamic equation allows the system to dynamically evolve; the dynamic equation in which the individuals choose the strategy Trust is

\[
F(\overline{x}) = \overline{x} \cdot (1 - \overline{x}) \cdot \left[ \omega^2G_T + \alpha T - (\omega - \omega^2)C_1 - \omega^2C_2 \right].
\]

(18)
Compared with (10) and (18), (10) is the same as (18) when \( m + n = 1 \). Therefore, the replicator dynamics can be viewed as a special case of the dynamic evolution method based on the strategy adjustments.

Comparing (10) and (18), the dynamic equation expresses the speed of the dynamic evolution. There are three cases. (1) The evolution speed of (10) is faster than that of (18) when \( m + n > 1 \); thus, our model converges to the steady state much faster than the replicator dynamics; (2) the evolution speed of (10) is less than that of (18) when \( m + n < 1 \); thus, the replicator dynamic converges much faster than our model; (3) when \( m + n = 1 \), the two methods have the same convergence speed.

Overall, we can derive that the convergence speed to the steady state is much faster in the evolution method than in the replicator dynamic as long as \( m + n > 1 \).

### 6. Simulation Experiments

The experimental environment is Matlab 7. The experimental content is divided into three parts.

1. The first part is the verification of the evolution stable experiment, including the verification of Theorems 3 and 4 and Inference 2.
2. The second part is to study the factors that have an effect on the evolutionary stable speed, including the verification to Inferences 1 and 3.
3. The third part is the experiments that compare the dynamic evolution method based on strategy adjustment and replicator dynamics.

#### 6.1. Experiment on the Evolutionary Stability

The experiment verifies the conclusions about the evolutionary stable state which are drawn by Theorems 3 and 4 and Inference 2.

We set the parameters of the first group and second group to meet the conditions of Theorem 3, the third group and fourth group to meet the conditions of Theorem 4, and the fifth group and sixth group to meet the conditions of Inference 2. The results of the trust evolution of the WSN nodes were observed under the 6 groups of parameters. The experiment data settings are shown in Table 6. The experimental results are shown in Figures 1–3.

In Figure 1, the solid curve and dotted curve correspond to the first group and second group of the experimental data in Table 6, respectively. We can verify that the experimental data values from the first group and second group meet the conditions of Theorem 3 and Definition 2, respectively. As seen from Figure 1, when the initial value of the dynamic equation (10) of the sensor nodes trust evolution is 0.01, that is, when the rate of the sensor nodes choosing strategy Trust is 1% in the WSNs, the first group (solid curve) after playing 340 times and the second group (dotted curve) after playing approximately 50 times converge to 1. In other words, the rate of the sensor node of the final choice strategy Trust is stable at the point \( \bar{x}_2^* = 1 \). The results of the two experimental groups show that \( \bar{x}_2^* = 1 \) is the evolutionary stable strategy of the WSNs trust game. Therefore, Theorem 3 is verified.

In Figure 2, the solid curve and dotted curve correspond to the third group and fourth group of the experimental data in Table 6, respectively. We can verify that the experimental data values from the third group and fourth group meet the conditions of Theorem 4 and Definition 2, respectively. As seen from Figure 2, when the initial value of the dynamic equation (10) of the sensor nodes trust evolution is 0.99, that is, when the rate of the sensor nodes choosing strategy Trust is 99% in the WSNs, the third group (solid curve) after playing 200 times and the fourth group (dotted curve) after playing approximately 450 times converge to 0. In other words, the rate of the sensor node of the final choice strategy Trust is stable at the point \( \bar{x}_1^* = 0 \). The results of the two experimental
groups show that \( x^*_1 = 0 \) is the evolutionary stable strategy of the WSNs trust game. Therefore, Theorem 4 is verified.

In Figure 3, the solid curve and dotted curve correspond to the fifth group and sixth group of the experimental data in Table 6, respectively. We can verify that the experimental data values from the fifth group and sixth group meet the conditions of Inference 2 and Definition 2, respectively. As seen from Figure 3, when the initial value of the dynamic equation (10) of the sensor nodes trust evolution is 0.01, that is, when the rate at which the sensor nodes choose the strategy \( Trust \) is 1% in the WSNs, the fifth group (solid curve) after playing 57 times and the sixth group (dotted curve) after playing approximately 87 times converge to 1. In other words, the rate of the sensor node for the final choice strategy \( Trust \) is stable at the point at which \( x^*_2 = 1 \). The results of the two experimental groups show that \( x^*_2 = 1 \) is the evolutionary stable strategy of the WSNs trust game. Therefore, Inference 2 is verified.

### Table 6: Experimental data (1).

| Serial number | \( q \) | \( G_T \) | \( G_C \) | \( L \) | \( C \) | \( m \) | \( n \) | \( N \) | \( \alpha T \) |
|---------------|--------|--------|--------|-----|------|-----|-----|-----|--------|
| Group 1       | 0.8    | 3      | 4      | 4   | 5    | 0.2 | 0.23| 7   | 4      |
| Group 2       | 0.8    | 9      | 2      | 4   | 7    | 0.4 | 0.3 | 7   | 3      |
| Group 3       | 0.8    | 5      | 3      | 4   | 7    | 0.2 | 0.23| 7   | 3      |
| Group 4       | 0.8    | 3      | 4      | 4   | 5    | 0.2 | 0.23| 7   | 3      |
| Group 5       | 0.8    | 8      | 7      | 4   | 2    | 0.11| 0.12| 5   | 3      |
| Group 6       | 0.8    | 6      | 5      | 4   | 2    | 0.11| 0.12| 5   | 2      |

6.2. Verification Experiments on the Effect of Convergence Speed. In this section, we explore the two important influencing factors on the evolutionary stable state: the trust incentives \( \alpha T \) and the retransmission upper limit \( N \). The experimental data are shown in Table 7. The experiment varies the value of \( \alpha T \) and maintains the values of the other parameters, by using the data from the first and second group to meet the conditions of Theorem 3 and Definition 2. Additionally, it varies the value of \( N \) and maintains the values of the other parameters by using the third group to meet the conditions of Theorem 3 and Definition 2, and it maintains the values of the last two groups to meet the conditions of Theorem 4 and Definition 2. The experimental results are shown in Figures 4 and 5.

Figure 4 gives the effect of the trust incentives on the trust evolution. The solid curve and dotted curve correspond to the experimental data of the first group (\( \alpha T = 5 \)) and second group (\( \alpha T = 4 \)) in Table 7, respectively. The experiment varies the value of \( \alpha T \) and maintains the value of the other parameters. The two groups of experimental data meet the conditions of Theorem 3 and Definition 2. In Figure 4, when the initial value is set to 0.01 in the dynamic evolution equation (10), the dotted line shows that the system will reach the evolutionary stable state \( x^*_2 = 1 \) after iterating 340 times when \( \alpha T = 4 \), while the solid line shows that it must iterate 150 times to reach the same stable state when \( \alpha T = 5 \).

Obviously, the speed of the curve of \( \alpha T = 5 \) is faster than that of the curve \( \alpha T = 4 \) when converging to the stable state in Figure 4. The results of the two experimental groups show that, under the same conditions, the greater the trust incentive is, the faster the network can reach the evolutionary stable state. Therefore, Inference 1 is verified.

### Table 7: Experimental data (2).

| Serial number | \( q \) | \( G_T \) | \( G_C \) | \( L \) | \( C \) | \( m \) | \( n \) | \( N \) | \( \alpha T \) |
|---------------|--------|--------|--------|-----|------|-----|-----|-----|--------|
| Group 1       | 0.8    | 3      | 4      | 4   | 5    | 0.2 | 0.23| 7   | 5      |
| Group 2       | 0.8    | 3      | 4      | 4   | 5    | 0.2 | 0.23| 7   | 4      |
| Group 3       | 0.8    | 5      | 3      | 4   | 7    | 0.2 | 0.23| 1   | 3      |
| Group 4       | 0.8    | 5      | 3      | 4   | 7    | 0.2 | 0.23| 3   | 3      |
| Group 5       | 0.8    | 5      | 3      | 4   | 7    | 0.2 | 0.23| 5   | 3      |

### Figure 3: Trust evolution curve (3).

### Figure 4: Trust evolution curve in terms of \( \alpha T \).
The following experiment is verified by the effect of the upper limit retransmission \( N \). In Figure 5, the curves correspond to the experimental data of the last three groups in Table 7; the data in the three groups varies the value of \( N \) and maintains the values of the other parameters.

The experimental data of the last two groups correspond to the trust evolution curve of \( N = 3 \) and \( N = 5 \), respectively, which meet the conditions of Theorem 4, Definition 2, and Inference 3. In the trust evolution dynamic evolution equation (10), we use the same initial value of 0.01. We can see that the speed of the curve that corresponds to \( N = 5 \) is faster than the curve that corresponds to \( N = 3 \), when converging to the evolutionary stable state. The experiment results imply that, under the same conditions, the smaller the upper limit of the retransmission \( N \), the slower the convergence speed of the evolutionary stable state at \( \bar{x}_1^* = 0 \).

In Figure 5, the solid curve of \( N = 1 \) corresponds to the third group of data, which meets the conditions of Theorem 3, Definition 2, and Inference 3, and it reaches the evolutionary stable state at \( \bar{x}_1^* = 1 \).

Comparing the experimental results of the three groups of data under the same conditions, we know that if the upper limit retransmission \( N \) is smaller, the conditions of Theorem 3 are easily met and the steady state at \( \bar{x}_2^* = 1 \) is easy to reach. Therefore, Inference 3 is verified.

6.3. Experimental Comparison with the Replicator Dynamic.
In this section, we set the same initial values and compare our dynamic evolution based on strategy adjustment following the dynamic equation (10) and the replicator dynamic method according to the replicator dynamic equation (18). Then, we analyze the effect of the convergence speed toward the steady state using the two different evolution methods.

The experimental data are shown in Table 8: the first, third, fourth, and sixth groups of data for our method of dynamic evolution are based on strategy adjustment, and the second and fifth groups of data are based on the replicator dynamics. Through the previous analysis of Section 5.3, the replicator dynamics are a special case of our dynamic evolution method and are based on strategy adjustment, and the replicator dynamic evolution equation (18) is unrelated to the values of \( m \) and \( n \); thus, we ignore the values of \( m \) and \( n \). The experimental results are shown in Figures 6 and 7, respectively.

In Figure 6, the curves \( a, b, \) and \( c \) correspond to the experimental data in the first, second, and third groups of Table 8, respectively. They meet the conditions of Theorem 3. Moreover, the data of the first and third groups satisfy the conditions of Definition 2, which implies that these three curves will finally reach the evolutionary stable state at \( \bar{x}_2^* = 1 \). In Figure 7, the curves \( d, e, \) and \( f \) correspond to the experimental data in the last three groups in Table 8, respectively, which meet the conditions of Theorem 4. Additionally, the data of the fourth and sixth groups meet the conditions of Definition 2, in such a way that all of the curves will reach the evolutionary stable state at \( \bar{x}_1^* = 0 \).

In Figure 6, curve \( b \) is the trust evolution curve, which meets the condition \( m + n = 1 \) of the strategy adjustment method. Following the conclusion in Section 5.3, this curve is also the replicator dynamic trust evolution curve. Here,
In Figure 7, we can see that the convergence speeds in the curves $a$, $b$, and $c$ converge to the steady state $\tilde{x}_2^* = 1$. The experimental results show that when $m + n > 1$, the convergence speed of the evolution strategy that is based on dynamic adjustment is greater than the convergence speed of the replicator dynamic method. When $m + n < 1$, the convergence speed of our method is less than that of the replicator dynamic method.

In Figure 7, curve $e$ is the trust evolution curve, which meets the condition $m + n = 1$ of the strategy adjustment method. Following the conclusion in Section 5.3, this curve is also the replicator dynamic trust evolution curve. Here, $d$ is the trust evolution curve, which satisfies the condition $m + n > 1$ of the strategy adjustment method. Additionally, $f$ is the trust evolution curve, which satisfies the condition $m + n < 1$ of the adjustment method. Comparing the three curves in Figure 7, we can see that the convergence speeds of the curves $d$, $e$, and $f$ converge to the steady state $\tilde{x}_2^* = 0$, and we can draw the same results as those from Figure 6.

### 7. Conclusions

A WSN’s trust management is an important aspect of WSN security. In this paper, we study WSN node trust decisions and trust evolution problems using evolutionary game theory. Based on the interaction cooperation of the sensor nodes, we consider the data retransmission after packets are lost and the trust incentive mechanism and we build an evolutionary game model that is closer to the reality of WSNs. Moreover, we propose an evolution method that is based on a dynamic adjustment strategy, to make up for the deficiency of the replicator dynamic method, which cannot show the trust decision process of the individuals. Through the analysis of dynamic evolution, we draw the conditions of reaching a steady state and analyze the factors that affect the convergence speed, and, finally, we compare the evolution speed of our method with that of the replicator dynamics. Last, the conclusions are proved effectively and feasibly by several experiments.

The results of this paper reveal the evolution dynamics rules of trust decision-making and trust evolution of WSNs; we could further calculate the trust values of the sensor nodes based on this evolution method-based strategy adjustment in subsequent work, and the trust management model that we propose provides a theoretical basis for the security of WSNs.

### Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

### Acknowledgment

This work was supported by the National Natural Science Foundation of China under Grant no. 61272034.

### References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” Computer Networks, vol. 38, no. 4, pp. 393–422, 2002.

[2] S. Shen, Y. Li, H. Xu, and Q. Cao, “Signaling game based strategy of intrusion detection in wireless sensor networks,” Computers & Mathematics with Applications, vol. 62, no. 6, pp. 2404–2416, 2011.

[3] G. Han, J. Jiang, L. Shu, J. Niu, and H. Chao, “Management and applications of trust in Wireless Sensor Networks: a survey,” Journal of Computer and System Sciences, vol. 80, no. 3, pp. 602–617, 2014.

[4] Y. Ren, V. I. Zadorozhny, V. A. Oleshchuk, and F. Y. Li, “A novel approach to trust management in unattended wireless sensor networks,” IEEE Transactions on Mobile Computing, vol. 13, no. 7, pp. 1409–1423, 2014.

[5] G. P. Gupta, M. Misra, and K. Garg, “Energy and trust aware mobile agent migration protocol for data aggregation in wireless sensor networks,” Journal of Network and Computer Applications, vol. 41, no. 1, pp. 300–311, 2014.

[6] R. Feng, S. Che, and X. Wang, “An incentive mechanism based on game theory for trust management,” Security and Communication Networks, vol. 7, no. 12, pp. 2318–2325, 2014.

[7] Y. Ren, V. I. Zadorozhny, V. A. Oleshchuk, and F. Y. Li, “A novel approach to trust management in unattended wireless sensor networks,” IEEE Transactions on Mobile Computing, vol. 13, no. 7, pp. 1409–1423, 2014.

[8] S. Shen, G. Yue, Q. Cao, and F. Yu, “A survey of game theory in wireless sensor networks security,” Journal of Networks, vol. 6, no. 3, pp. 521–532, 2011.

[9] M. Seredynski, P. Bouvry, and M. A. Klopotek, “Modelling the evolution of cooperative behavior in ad hoc networks using a game based model,” in Proceeding of the IEEE Symposium on
Computational Intelligence and Games (CIG '07), pp. 96–103, Honolulu, Hawaii, USA, April 2007.

[10] K. Komathy and P. Narayanasamy, “Trust-based evolutionary game model assisting AODV routing against selfishness,” Journal of Network and Computer Applications, vol. 31, no. 4, pp. 446–471, 2008.

[11] M. Mejia, N. Peña, J. L. Muñoz, O. Esparza, and M. A. Alzate, “A game theoretic trust model for on-line distributed evolution of cooperation in MANETs,” Journal of Network and Computer Applications, vol. 34, no. 1, pp. 39–51, 2011.

[12] E. Palomar, A. Alcaide, A. Ribagorda, and Y. Zhang, “The Peer’s Dilemma: a general framework to examine cooperation in pure peer-to-peer systems,” Computer Networks, vol. 56, no. 17, pp. 3756–3766, 2012.

[13] A. Agah, S. K. Das, and K. Basu, “A game theory based approach for security in wireless sensor networks,” in Proceedings of the 23rd IEEE International Conference on Performance, Computing and Communications (IPCCC '04), pp. 259–263, Phoenix, Ariz, USA, April 2004.

[14] A. Urpi, M. Bonuccelli, and S. Giordano, “Modeling cooperation in mobile ad hoc networks: a formal description of selfishness,” in Proceedings of the Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, pp. 3–5, INRIA Sophia-Antipolis, Valbonne, France, March 2003.

[15] J. J. Jaramillo and R. Srikant, “A game theory based reputation mechanism to incentivize cooperation in wireless ad hoc networks,” Ad Hoc Networks, vol. 8, no. 4, pp. 416–429, 2010.

[16] G. Yin, Y. Wang, Y. Dong, and H. Dong, “Wright-Fisher multi-strategy trust evolution model with white noise for Internetware,” Expert Systems with Applications, vol. 40, no. 18, pp. 7367–7380, 2013.

[17] G. Yin, Y. Wang, Y. Dong, and H. Dong, “Wright-Fisher multi-strategy trust evolution model with white noise for Internetware,” Expert Systems with Applications, vol. 40, no. 18, pp. 7367–7380, 2013.

[18] M. Mejia, N. Peña, J. L. Muñoz, O. Esparza, and M. Alzate, “DECADE: distributed emergent cooperation through ADaptive evolution in mobile ad hoc networks,” Ad Hoc Networks, vol. 10, no. 7, pp. 1379–1398, 2012.

[19] K. Komathy and P. Narayanasamy, “Secure data forwarding against denial of service attack using trust based evolutionary game,” in Proceedings of the IEEE 67th Vehicular Technology Conference (VTC '08), pp. 31–35, Singapore, May 2008.

[20] K. Komathy and P. Narayanasamy, “Study of co-operation among selfish neighbors in MANET under evolutionary game theoretic model,” in Proceedings of the International Conference on Signal Processing, Communications and Networking (ICSCN '07), pp. 133–138, Chennai, India, February 2007.

[21] M. Seredynski and P. Bouvry, “Analysing the development of cooperation in MANETs using evolutionary game theory,” Journal of Supercomputing, vol. 63, no. 3, pp. 854–870, 2013.

[22] S. G. Shen, X. Ma, H. Jiang, W. Li, and Q. Y. Cao, “Evolutionary game theory based trust strategy model and dynamics analysis in wireless sensor networks,” Control and Decision, vol. 27, no. 8, pp. 1133–1138, 2012.

[23] Z. Chen, Y. Qiu, J. Liu, and L. Xu, “Incentive mechanism for selfish nodes in wireless sensor networks based on evolutionary game,” Computers and Mathematics with Applications, vol. 62, no. 9, pp. 3378–3388, 2011.

[24] X. Wang, Y. Wu, Y. Ren, R. Feng, N. Yu, and J. Wan, “An evolutionary game-based trust cooperative stimulation model for large scale MANETs,” International Journal of Distributed Sensor Networks, vol. 2013, Article ID 245017, 16 pages, 2013.

[25] P. D. Taylor and L. B. Jonker, “Evolutionarily stable strategies and game dynamics,” Mathematical Biosciences, vol. 40, no. 1-2, pp. 145–156, 1978.

[26] J. W. Weibull, Evolutionary Game Theory, MIT Press, Cambridge, Mass, USA, 1995.