Hindawi
International Journal of Antennas and Propagation
Volume 2017, Article ID 8591206, 13 pages
https://doi.org/10.1155/2017/8591206

Research Article

Study on Selfish Node Incentive Mechanism with a Forward Game Node in Wireless Sensor Networks

Mohammed Ahmed Ahmed Al-Jaoufi,[1] Yun Liu,[1] Zhen-jiang Zhang,[1] and Lorna Uden[2]

[1]*School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China*
[2]*School of Computing and Digital Technologies, Staffordshire University, Stoke-on-Trent ST4 2DE, UK*

Correspondence should be addressed to Yun Liu; liuyun@bjtu.edu.cn

Received 4 February 2017; Revised 1 August 2017; Accepted 16 August 2017; Published 8 October 2017

Academic Editor: Francisco Falcone

In a wireless sensor network, some nodes may act selfishly and noncooperatively, such as not forwarding packets, in response to their own limited resources. If most of the nodes in a network exhibit this selfish behavior, the entire network will be paralyzed, and it will not be able to provide normal service. This paper considers implementing the idea of evolutionary game theory into the nodes of wireless sensor networks to effectively improve the reliability and stability of the networks. We present a new model for the selfish node incentive mechanism with a forward game node for wireless sensor networks, and we discuss applications of the replicator dynamics mechanism to analyze evolutionary trends of trust relationships among nodes. We analyzed our approach theoretically and conducted simulations based on the idea of evolutionary game theory. The results of the simulation indicated that a wireless sensor network that uses the incentive mechanism can forward packets well while resisting any slight variations. Thus, the stability and reliability of wireless sensor networks are improved. We conducted numerical experiments, and the results verified our conclusions based on the theoretical analysis.

1. Introduction

A wireless sensor network (WSN) is a wireless network that is constructed via the self-organization of a large number of sensor nodes. Considering the network security problems that exist today, at present, there is a significant amount of research being done on the security of wireless sensor networks from different perspectives with the aim of ensuring that the networks are operating effectively. In terms of security issues, the problems encountered by wireless sensor networks and traditional wireless networks differ greatly and are determined by the characteristics of the individual networks.

Since the resources of sensor nodes are limited, processing power, storage space, energy, and other factors prevent direct application of mature and effective security protocols and algorithms to wireless sensor networks.

Sensor nodes are often deployed in some harsh environments, and, once deployed, they are rarely maintained, and this increases the possibility of nodes being captured. Security issues faced by the wireless sensor network included physical security of nodes, security issues in the link layer, and security issues in the network layer [1–7].

Sensor nodes are usually deployed in numerous unattended nodes; being captured is a security issue, so it is important to discuss how to prevent nodes from being captured in the physical layer. Thus, the main security threats that wireless sensor networks can incur are the interference of the capture [2] and the wireless communication of noise. Once the nodes are captured and become malicious insider nodes, the attacker will transform the nodes and disguise them as legitimate nodes and add them to the wireless sensor network. Then, these malicious nodes can provide services for the attacker, such as intercepting messages, falsifying data, and modifying data. The interference of wireless communication is mainly blocking [3–8], because the sensor nodes of a wireless communication signal spectrum are usually in a frequency band. If an attacker is using the intrusion of external malicious nodes in this band to constantly send useless signals, the node in its transmission radius cannot normally receive data from other nodes. That is to say, only when the

malicious node stops blocking can the nodes in the wireless sensor network transmit normal signal communication.

The main security threat that the link layer can incur is the destruction of data packets in the transmission process, and this can include, for example, collision conflicts, unfair competition, and denial-of-service attacks. The collision conflict [9] occurs mainly when two adjacent sensor nodes send data at the same time; the data will become superimposed and cannot be separated, and the data will be discarded, leading to a decrease in the efficiency of transmission. Unfair competition to the denial-of-service attacks [5] is when attackers modify the priority of the message and then continue to send some high priority messages to occupy the channel. This will prevent normal use of the channel by other nodes and lead to data retention. Because there is no independent routing device in wireless sensor networks, the sensor nodes are used directly for routing. In terms of data-forwarding equipment, there are no special security measures, which makes the security issues associated with any network layer more severe. Security threats faced by the network layer include selective forwarding [6], Sybil attacks [4], black hole attacks [10], and flooding attacks [11]. Selective forwarding attacks mainly refer to malicious nodes of data packets that have the choice of discarding or forwarding, thus reducing the possibility of being found and prolonging the latent time. Witch attacks [4] mainly refer to attackers disguised as malicious nodes with the identity of multiple working false nodes. In this case, the other nodes in the network are mistaken for legitimate nodes, so packets are sent to these nodes, but, in fact, data are collected by the malicious nodes.

Sheng et al. [12] evaluated simulations to demonstrate that protocols provide incentives for nodes to forward packets, and they also discussed the challenging issues in designing incentive-compatible protocols in ad hoc networks; the challenges are overdue to be addressed. At present, solving the problem of selfish nodes in wireless sensor networks mainly includes reputation-based mechanisms and payment mechanisms. However, the existing model primarily concerns the idea of classical game theory to predict node behavior, which is built on a completely rational hypothesis suggested by the participants based on the analysis of the problem and the assumption of fully rational requirements of all participants with rational consciousness, analytic reasoning and recognition judgment ability, memory ability, and accurate behavior, such as the ability to perfect requirements.

Classical game theory emphasizes that participants do not make mistakes in the process of the game; other participants also do not make mistakes and pay attention to the static equilibrium results.

Therefore, the present incentive model has the following disadvantages [12–15]:

(1) It is unable to complete an accurate description of the dynamic evolution of the node strategy, making it impossible to determine the robustness and stability of these mechanisms due to the lack of analysis based on strict mathematical theories.

(2) Current mechanisms assume that every node must have and maintain a global information network, which requires that each node must have a strong cognitive ability and memory space resources. Obviously, this assumption is generally not realistic in wireless sensor networks.

(3) The current mechanism enhances the performance of the system to achieve its best performance, but it cannot guarantee that each node can achieve the best benefit, so the node is still likely to appear to exhibit selfish behavior.

For these reasons, in this paper, we have presented a new model of a selfish node incentive mechanism with a forward game node for wireless sensor networks. The research focused on the selfish nodes in the wireless sensor network that are caused by security issues. Because the nodes that participate and cooperate in the process require the expenditure of energy, storage space, and resources, due to limited resources and selfish behavior, some nodes are not always cooperative. According to game theory analysis, the packet forwarding process is a typical prisoner's dilemma. In the end, all nodes will choose to be noncooperative and refuse to forward packets. Therefore, a conditional cooperation strategy is added to the strategic space of nodes to establish the incentive game model of node forwarding packets, and then the incentive game model is established using evolutionary game theory. To ultimately achieve a good state of cooperation over the whole network, dynamic analysis was performed concerning the stability of stressed nodes through continuous learning in the game, imitation, and trial and error to adjust their strategies to find the most suitable strategy for their own interest. Numerical analysis is used to verify the correctness of our theoretical analysis.

2. Preparation Knowledge of Game Theory

Game theory is a theory that specializes in game strategies and is also known as "theory of games." It is a discipline based on mathematics, and it deals with how a participant will plan to obtain the maximum benefit in a game. One standard game includes nine basic elements, which are as follows:

(1) Participant, also known as "player," means the decision-making body that has the independent decision-making right, independently takes the consequences, and selects the action by self-benefit maximization in a game. The decision-making body can be an individual, but it also can be other groups or organizations. The game with only two players is called a "two-player game." The game with more than two players is called a "multiplayer game." The goal of each player is to maximize self-benefit.

(2) The rules of the game are a set of specifications of the game. They include, for example, the stipulation of participants' action sequences, information obtained when some participant acts, what kind of action can be selected, and what result will be achieved.

(3) Game behavior means the set of all possible strategies or actions of players.

(4) Information of the game is the knowledge of information that is mastered by the player and is helpful in selecting the strategy during the game, especially pertaining to the knowledge of characters and actions for other related players (competitors). The information will be changed as the game progresses or with the variation of time.

(5) Game strategies are the set of all actions that the players can select. Thus, each player can make a decision by stipulating a method, practice in order to ensure maximized self-benefit and guide the actions of the player.

(6) Sequence of game is the continuous sequences that a player chooses during the strategy selections. During all kinds of actual decision activities, all players, or multiple players, sometimes are required to make decisions at the same time so that there are no differences in the sequences. To ensure fair and reasonable play, when a player makes a decision, he or she does not know the decisions of other players.

(7) Earnings of game are the results obtained by the decisions made by a player in the game. It is the function of all players' strategies or actions, and it is the most significant element to each player. All rational players hope that their own earnings can be maximized.

(8) Results are the set of elements in which the analysts of a game are interested.

(9) Equilibrium refers to the combination of optimum strategies and actions of all players. In the equilibrium of game theory, Nash equilibrium, one type of strategy combination is a situation faced by all players when other players do not change their strategies because they have found the best strategy to use.

3. Incentive Gaming Model for Selfish Behaviors of Nodes

3.1. Problem Descriptions of Selfish Nodes. Wireless sensor networks provide normal network services through cooperation among nodes, but in the process of cooperation, the nodes consume energy, storage space, and other resources. Therefore, some nodes will choose selfish, noncooperative behavior due to limited resources, which will seriously affect the performance of the entire network. In order to analyze the problem of selfish nodes, we make the following assumptions about wireless sensor networks:

(1) Wireless sensor networks are composed of N nodes; each node has a routing and a forwarding function.

(2) Each node has a selection of two strategies; one is cooperatively forwarding data packets, and the other is noncooperative in that data packets are not forwarded.

(3) All packets have the same size, and the energy consumed by the node forwarding a packet is equal.

Table 1: Profit matrix of forwarding packets.

	Cooperative	Noncooperative
Cooperative	R-C	-C
Noncooperative	R	0

Table 2: Profit matrix of incentive mechanism.

	Strategy C	Strategy D	Strategy CC
Strategy C	C	-C	R-C
Strategy D	0	0	0
Strategy CC	-C_C	-C_C	R-C-C_C

(4) If the nodes are selected to cooperatively forward packets, they will get R units of profit and consume C units of resources; if the nodes are selected for noncooperative forwarding of packets, the profit is 0; if one node is selected for a cooperative strategy and another node is selected for a noncooperative strategy, the node selected for the cooperative strategy has a profit of 0 and consumes C units of resources. The profit obtained by selecting the nodes for noncomparative strategy will be R, and $R > 2C$. From the above assumptions, we can obtain the profit matrix shown in Table 1.

3.2. Establishment of the Incentive Model. The packet forwarding process of a node is a typical prisoner's dilemma. Ultimately, all nodes choose the strategy of not forwarding the data packets, which will paralyze the network. Therefore, we propose a new conditional cooperation strategy to encourage nodes to be cooperative, and the game model of incentive is made as follows.

(1) Participants in the Game. The N nodes and the population that has N nodes between nodes describe a symmetric game. That is, all nodes have the same strategy space, and the profit matrix is the same.

(2) Participants of the Strategy Space. Each node has three strategies, that is, cooperative (C), noncooperative (D), and conditional cooperative (CC). The cooperative strategy can be understood as a selfless node that will always forward packets for other nodes that have noncooperative strategies. In the conditional cooperative strategy, nodes are qualified for cooperation with other nodes that have been working together. Based on the conditions of cooperative strategy, a cooperative node carries forward packets, while a noncooperative node does not forward packets.

(3) Participant's Profit Matrix. There are three profit matrices in the strategic space of the participant. The profit matrix is a 3 × 3 matrix, recorded as $A = [a_{ij}]$, where $j = 1, 2, 3$; a_{ij} shows the profit of node i when a game is played between a node with i strategy and one with j strategy. Cc in profit matrix A shows the cost for a node with CC strategy and the specific profit matrix, as shown in Table 2.

4. Analysis of Incentive Mechanism Based on the Evolutionary Game

4.1. Dynamic Analysis of Incentive Mechanism. We assume that the nodes in wireless sensor networks adopt strategies C, D, and CC for x_C, x_D, and x_{CC}, respectively, where $x_C + x_D + x_{CC} = 1$. It seems that $x_1 + x_2 + x_3 = 1$. In order to facilitate the following analysis, strategies C, D, and CC, are referred to as strategies 1, 2, and 3; thus, x_C, x_D, and x_{CC} are recorded as x_1, x_2, and x_3, respectively. The strategy distribution of the whole population at a certain time is denoted as follows:

(1) Expected profit of node i:

$$W_i(X) = \sum_{j=1}^{3} x_j a_{ij} = (AX)_i. \tag{1}$$

(2) Average profit of populations:

$$\overline{W}(X) = \sum_{I=1}^{3} x_i W_i(x) = X \cdot AX. \tag{2}$$

(3) Replicator dynamics equation:

$$\frac{dx_i}{dt} = \left(W_i(X) - \overline{W}_i(X)\right) x_i = \left((AX)_i - X \cdot AX\right) x_i. \tag{3}$$

In accordance with the analyses above, the replicator dynamics equation of each strategy is calculated as follows:

(1) Expected profit of strategy 1 (C):

$$W_1(X) = (x_1 + x_3) R - (x_1 + x_2 + x_3) C. \tag{4}$$

(2) Expected profit of strategy 2 (D):

$$W_2(X) = x_1 R. \tag{5}$$

(3) Expected profit of strategy 3 (CC):

$$\begin{aligned} W_3(X) = {} & (x_1 + x_3) R - (x_1 + x_3) C \\ & - (x_1 + x_2 + x_3) C_c. \end{aligned} \tag{6}$$

(4) Expected profit of populations:

$$\begin{aligned} \overline{W}(X) = {} & \left[(x_1 + x_3)^2 + x_1 x_2\right] R \\ & - \left[(x_1 + x_3)^2 + x_1 x_2\right] C \\ & - \left[x_1 x_3 + x_2 x_3 + x_3^2\right] C_c. \end{aligned} \tag{7}$$

(5) Replicator dynamics equation of strategy 1 (C):

$$\begin{aligned} \frac{dx_1}{dt} = {} & \left[x_1^2 + x_1 x_3 - x_1 (x_1 + x_3)^2 - x_1^2 x_2\right] R \\ & + \left[x_1 (x_1 + x_3)^2 + x_1^2 x_2 - x_1^2 - x_1 x_2 - x_1 x_3\right] C \\ & + \left[x_1^2 x_3 + x_1 x_2 x_3 + x_1 x_3^2\right] C_c. \end{aligned} \tag{8}$$

(6) Replicator dynamics equation of strategy 2 (D):

$$\begin{aligned} \frac{dx_2}{dt} = {} & \left[x_1 x_2 - x_2 (x_1 + x_3)^2 - x_1 x_2^2\right] R \\ & + \left[x_2 (x_1 + x_3)^2 + x_1 x_2^2\right] C \\ & + \left[x_2^2 x_3 + x_1 x_2 x_3 + x_{12} x_3^2\right] C_c. \end{aligned} \tag{9}$$

(7) Replicator dynamics equation of strategy 3 (CC):

$$\begin{aligned} \frac{dx_1}{dt} = {} & \left[x_3^2 + x_1 x_3 - x_3 (x_1 + x_3)^2 - x_1 x_2 x_3\right] R \\ & + \left[x_3 (x_1 + x_3)^2 + x_1 x_2 x_3 - x_1 x_3 - x_3^2\right] C \\ & + \left[x_1 x_3^2 + x_2 x_3^2 + x_3^2 - x_1 x_3 - x_2 x_3 - x_3^2\right] C_c. \end{aligned} \tag{10}$$

4.2. Stability Analysis of Incentive Mechanism. First, according to the characteristics of wireless sensor networks, the incentive game model of node forwarding packets is established. Second, using evolutionary game theory to analyze the dynamics and stability of the incentive game model and for networks to achieve good collaboration, emphasis is placed on nodes of the game through continuous learning, imitation, and trial and error to find the most suitable strategy that meets their interest and the demands of the strategy.

Theorem 1. *In a wireless sensor network consisting of N nodes, when lower cost and mutation probability approach zero based on the condition of cooperation strategies, strategy D is considered as evolutionarily stable.*

Proof. According to the theorem of evolutionary stability, if a strategy i is evolutionary stable, then it must meet the following two conditions: (1) $a_{ii} > a_{ji}$ and (2) if $a_{ii} = a_{ji}$, then $a_{ij} > a_{jj}$ for arbitrary condition $i \neq j$. The profit matrix in Table 2 suggests that strategy D requires $a_{22} > a_{12}$ and $a_{22} > a_{32}$ to meet the definition of an evolutionary game, so strategy D is evolutionary stable and exhibits a strict Nash equilibrium. □

According to the previous analysis, we can obtain the following lemmas.

Lemma 2. *When strategy $C \neq 0$, strategy $D \neq 0$, and strategy $CC = 0$ and after a period of an evolutionary game, the nodes in wireless sensor networks eventually choose strategy D and are able to resist small variations. At this point, the group is able to continue in a stable state.*

Lemma 3. *When strategy $C \neq 0$, strategy $D = 0$, and strategy $CC \neq 0$ and after a period of an evolutionary game, the nodes in wireless sensor networks are selected by strategy C. However, the population is not stable in this state as long as there is little variation in the node. Then, the node selects strategy C, which eventually chooses strategy D. At this point, the group continues to be in a stable state.*

Lemma 4. *When strategy $C = 0$, strategy $D \neq 0$, and strategy $CC \neq 0$, there are three kinds of situations:*

(1) When strategy (CC) > cost for node (*Cc*)/(units of profit (*R*) − units of resources (*C*)), *after a period of an evolutionary game, the wireless sensor network node R-C chooses strategy CC. However, the population in this state is unstable as long as there is a small variation in the nodes. Then, the nodes will select strategy CC, which will choose strategy C and then choose strategy D. Eventually, all nodes in a population are grouped in strategy D, and this group will sustain a steady state.*

(2) When strategy (CC) = cost for node (*Cc*)/(units of profit (*R*)−units of resources (*C*)), *population selection strategy D and strategy CC of nodes exist at the same time, but the population in this state is unstable as long as there is a small variation. Strategy D of nodes will eventually lead to strategy CC, and this group will sustain a steady state.*

(3) When strategy (CC) < cost for node (*Cc*)/(units of profit (*R*) − units of resources (*C*)), *after a period of an evolution game, the nodes in the wireless sensor network ultimately choose strategy D and can resist small variations, so the group will continue to be in a stable state.*

Theorem 5. *In a P2P system with a small probability of population variation and a fixed number of nodes, when the cost approaches zero based on the conditional cooperation strategy, the nodes in the population spend most of their time on conditional cooperation strategies and cooperation strategies [16].*

Lemma 6. *Accordingly, Theorem 5 can be launched for a fixed number of sensor nodes, and the composition and variation probabilities of nodes are less in a wireless sensor network when the deviation value and the conditions of cooperation strategy of cost (C_C) are zero, so the population converges and adopts strategies CC and C.*

5. Modeling and Analysis

Modeling and simulation experiments were performed using the MATLAB mathematical tool. The assumptions about the wireless sensor network are as follows. Due to different measurement standards for the profit and cost of nodes, all participant parameters were standardized with values in the range of $[0, 1]$. Given $R = 1.0$ and $C = 0.4$, a mathematical model was produced according to (8)–(10).

(1) The simulation results of the state of the wireless sensor population when $Cc = 0.1$ for $x = (0.5, 0.5, 0)$ and $x = (0.5, 0.5–0.0001, 0.0001)$ are shown in Figures 1 and 2, respectively.

Figures 1 and 2. The simulation results in Figure 1 indicate that nodes of the wireless sensor network chose strategy *D* after an evolutionary game was performed for a period of time. In Figure 2, the system's population can manage slight variation and sustain a stable state.

For the statistical analysis of all data in Figures 1 and 2, the statistics are provided in Tables 3 and 4, respectively.

Based on the statistical analyses from Tables 3 and 4, we used these experiments in 0/100/36.65/25.43/0/30.2/100 and 0/100/36.65/25.43/0/30.2/100 rows to get more meaningful data, which are presented in Figures 3 and 4, respectively.

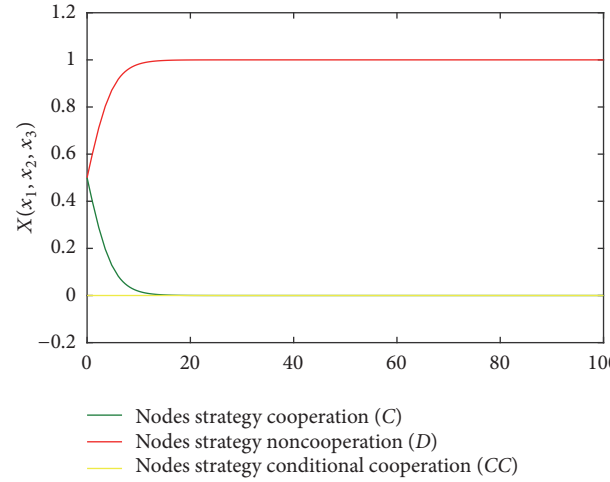

Figure 1: The state of population when $x = (0.5, 0.5, 0)$.

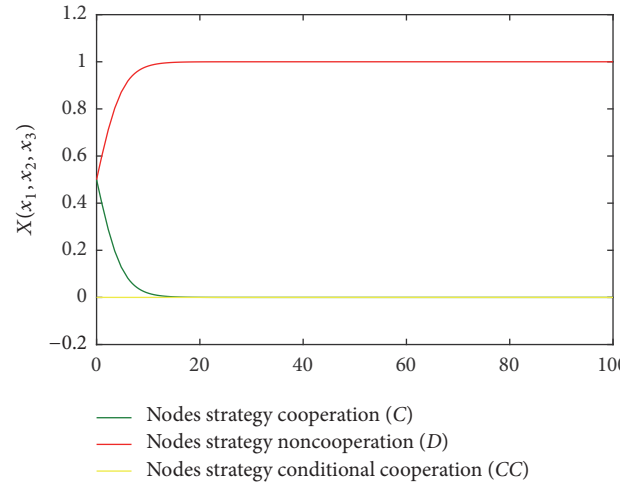

Figure 2: The state of population when $x = (0.5, 0.5–0.0001, 0.0001)$.

Table 3: The statistical analyses of strategies *C*, *D*, and *CC*.

	X	*C*	*D*	*CC*
Minimal value	0	$-1.08E-06$	0.5	0
Maximum value	100	0.5	1	0
Average value	36.64	0.03626	0.9637	0
Medium value	25.43	$3.82E-05$	1	0
Mode	0	$-1.08E-06$	0.5	0
Deviation	30.19	0.1073	0.1073	0
Range	100	0.5	0.5	0

From the results in Figure 3, when all of the values of the nodes strategy conditional cooperation (*CC*) were zero, and *CC* in Figure 4 was able to resist small variations, we see that all nodes of the wireless sensors network (WSN) have chosen strategy *D*, and when the values of average-medium values in

Table 4: The statistical analyses of strategies C, D, and CC.

	X	C	D	CC
Minimal value	0	$-1.08E-06$	0.4999	$4.56E-09$
Maximum value	100	0.5	1	0.0001
Average value	36.65	0.03626	0.9637	$1.88E-05$
Medium value	25.43	$3.81E-05$	1	$7.87E-06$
Mode	0	$-1.08E-06$	0.4999	$4.56E-09$
Deviation	30.2	0.1073	0.1073	$2.56E-05$
Range	100	0.5	0.5001	0.0001

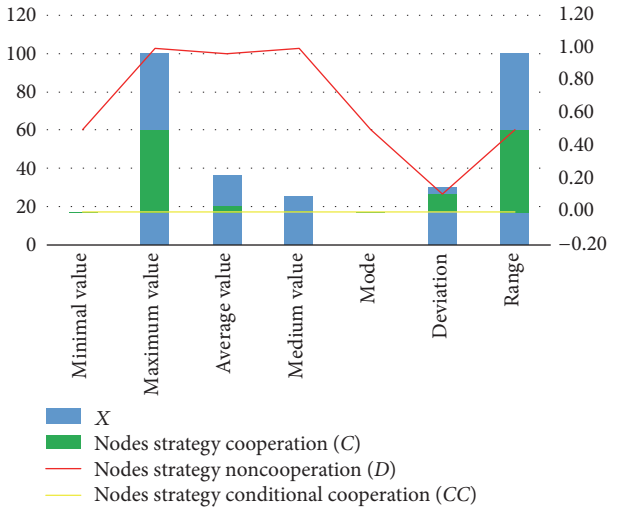

Figure 3: The state of population when X = (0, 100, 36.64, 25.43, 0, 30.19, 100).

Figure 3 were 36.64 and 25.43 and in Figure 4 were 36.65 and 25.43, the results of the average-medium values in each case were not smooth and steady. Therefore, Figures 1 and 2 and Lemma 2 were verified.

(2) When Cc = 0.1 and x = (0.5, 0, 0.5) and (0.5–0.0001, 0.0001, 0.5), the simulation results of the state wireless sensor population were as shown in Figures 5 and 6, respectively.

Figures 5 and 6. The simulation results in Figure 5 show that, in the system after a period of time for evolution, the nodes of the wireless sensor network will choose strategy C, whereas Figures 5 and 6 show that a node in the population system will choose strategy C. Figure 6 indicates that the population is not stable in this state as long as there is little variation in the node. The node then selects strategy C, which eventually chooses strategy D. At this point, the group continues to be in a stable state. The corresponding statistics of all data in Figures 5 and 6 are provided in Tables 5 and 6, respectively.

For the statistical analysis of all data in Figures 5 and 6, the respective statistics are provided in Tables 5 and 6.

From the statistical analysis of all values in Tables 5 and 6, we used these experiments in 0/100/46.98/47.85/0/31.27/100 and 0/100/47.97/51.73/0/26.54/100 rows to get more meaningful data, which are presented in Figures 7 and 8, respectively.

In Figure 7, when all of the values of the nodes (D) were zero, the nodes (D) in Figure 8 were able to resist small

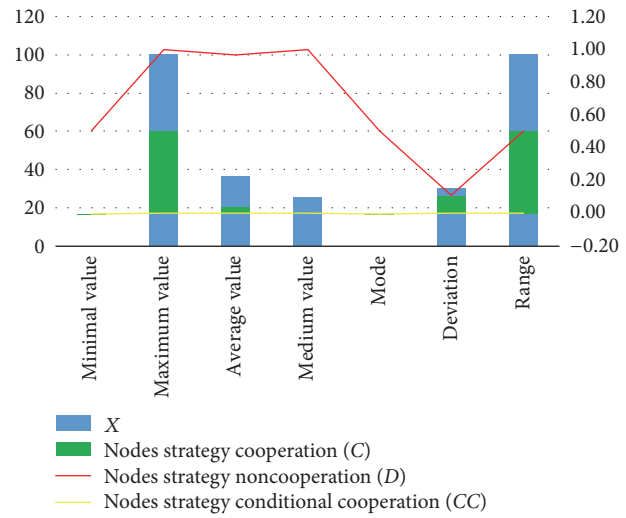

Figure 4: The state of population when X = (0, 100, 36.64, 25.43, 0, 30.2, 100).

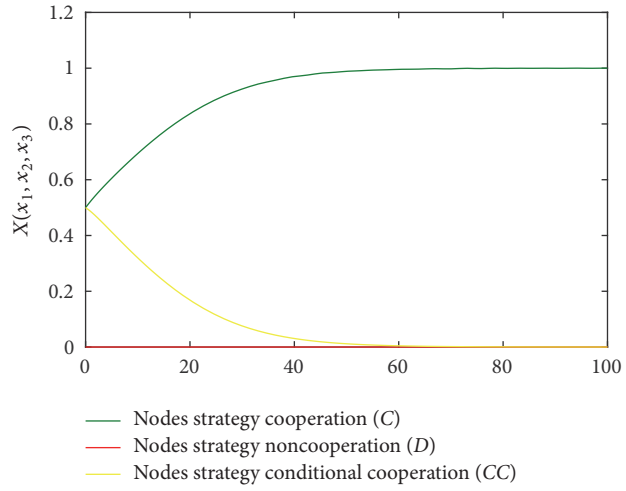

Figure 5: The state of population when x = (0.5, 0, 0.5).

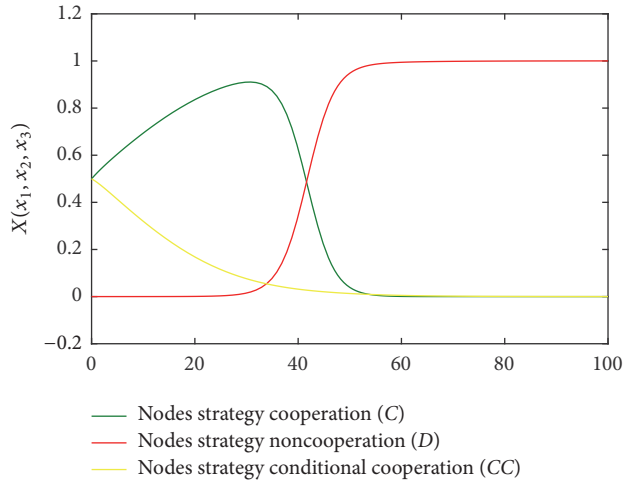

Figure 6: The state of population when x = (0.5–0.0001, 0.0001, 0.5).

Table 5: The statistical analyses of strategies C, D, and CC.

	X	C	D	CC
Minimal value	0	0.5	0	$8.08E-05$
Maximum value	100	1	0	0.5
Average value	46.98	0.8877	0	0.116
Medium value	47.85	0.9854	0	0.0144
Mode	0	0.5	0	$8.08E-05$
Deviation	31.27	0.1614	0	0.1668
Range	100	0.5002	0	0.4999

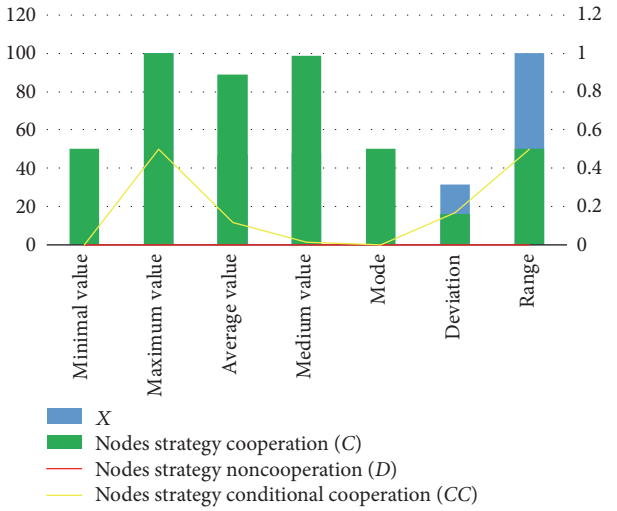

Figure 7: The state of population when X = (0, 100, 46.98, 47.85, 0, 31.27, 100).

variations; we see that all nodes of the WSN have chosen strategy C, and, in Figure 8, they have chosen strategy D, so the deviation in this case increased to 0.357. Thus, Figures 5 and 6 and Lemma 3 were verified.

(3) The simulation results of the state wireless sensor population when $Cc = 0.1$ and $x = (0, 0.5, 0.5)$ and (0.0001, 0.5, 0.5–0.0001) are displayed in Figures 9 and 10, respectively.

Figures 9 and 10. The simulation results in Figure 9 show that, after a period of time for evolution, the system and the nodes of a wireless sensor network will select strategy CC. Figure 10 indicates that the population in this state is unstable as long as there is a small variation in the nodes. Then, the nodes will select strategy CC, which will choose strategy C and then choose strategy D. Eventually, all nodes in a population are grouped in strategy D, and this group will sustain a steady state. Statistical analyses of the data in Figures 9 and 10 are shown in Tables 7 and 8, respectively.

From the statistical analyses of all of the values in Tables 7 and 8, in this case, we can see the range in Table 8, increasing up to 300 rows, and we used these experiments in 0/100/36.64/24.53/0/30.02/100 and 0/300/130.2/139.4/0/86.78/300 rows to get more meaningful data, which are presented in Figures 11 and 12.

Based on Figures 11 and 12, when all values of the nodes (C) were zero, as well as the nodes (C) in Figure 12, in this

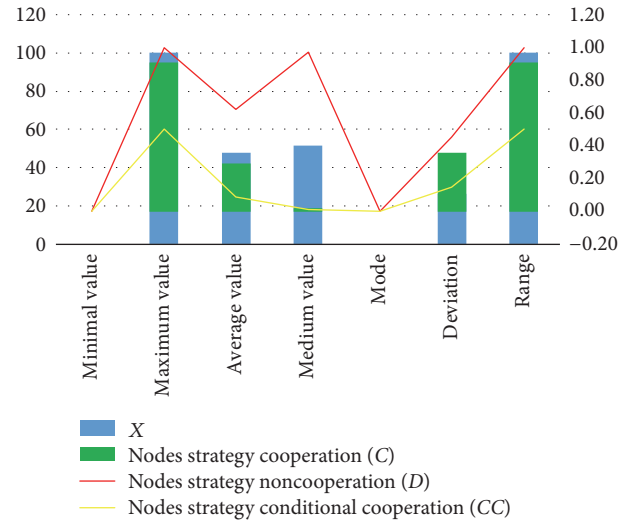

Figure 8: The state of population when X = (0, 100, 47.97, 51.73, 0, 26.54, 100).

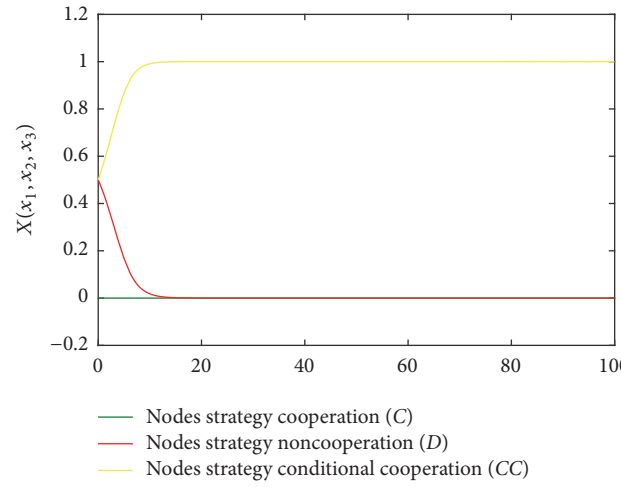

Figure 9: The state of population when x = (0, 0.5, 0.5).

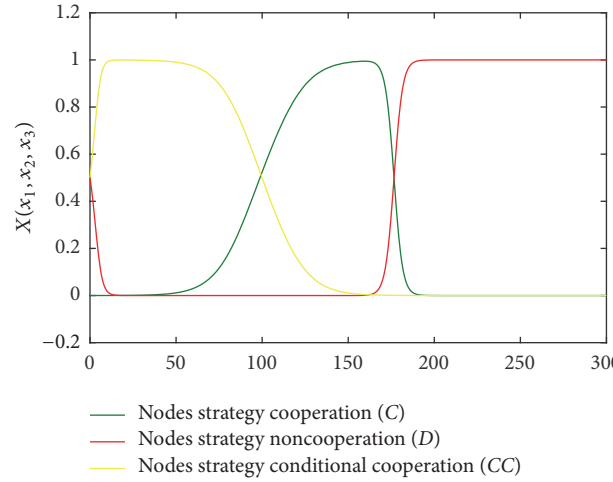

Figure 10: The state of population when x = (0.0001, 0.5, 0.5–0.0001).

Table 6: The statistical analyses of strategies C, D, and CC.

	X	C	D	CC
Minimal value	0	$-8.85E-08$	$9.10E-05$	$9.89E-05$
Maximum value	100	0.9106	1	0.5
Average value	47.97	0.2909	0.6236	0.0884
Medium value	51.73	0.0204	0.9687	0.01126
Mode	0	$-8.85E-08$	$9.10E-05$	$9.89E-05$
Deviation	26.54	0.357	0.4545	0.1473
Range	100	0.9106	1	0.4999

Table 7: The statistical analyses of strategies C, D, and CC.

	X	C	D	CC
Minimal value	0	0	$-6.201e-07$	0.5
Maximum value	100	0	0.5	1.001
Average value	36.64	0	0.03597	0.9682
Medium value	24.53	0	$1.286e-05$	1
Mode	0	0	$-6.201e-07$	0.5
Deviation	30.02	0	0.105	0.101
Range	100	0	0.5	0.5006

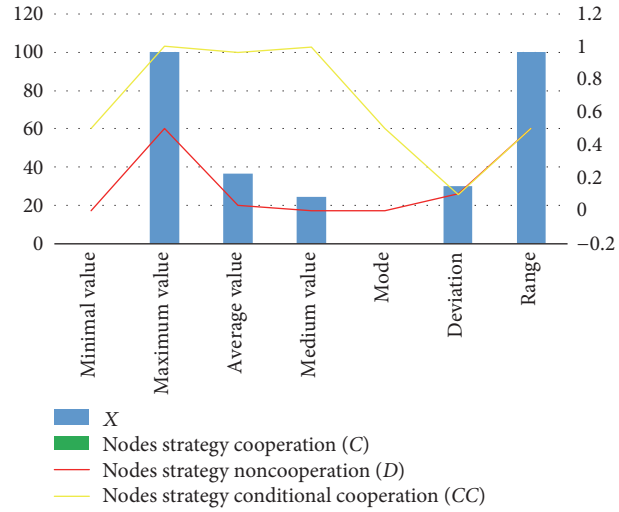

Figure 11: The state of population when $X = (0, 100, 36.64, 24.53, 0, 30.0, 100)$.

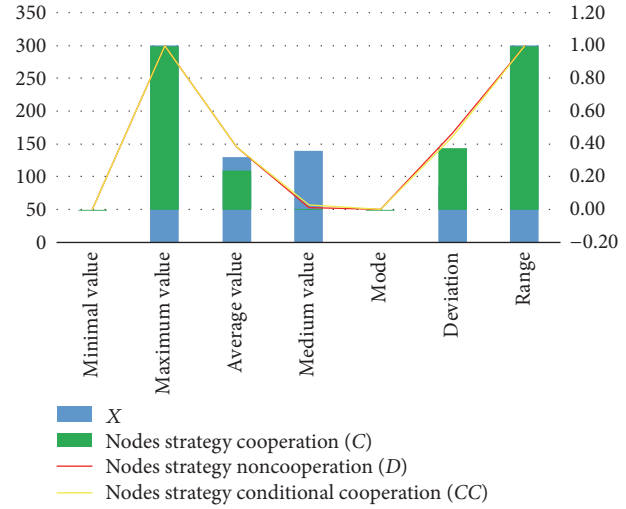

Figure 12: The state of population when $X = (0, 300, 130.2, 139.4, 0, 86.78, 300)$.

case, the range value increased to 300 and was able to resist small variation; we see that all nodes of WSN in Figure 11 chose the strategy CC and then D, and in Figure 12 they chose the strategy CC, so the deviation in this case increased to 0.444 of 0.101 in CC. Therefore, data in Figures 9 and 10 were verified as well as Lemma 4_(1).

(4) When $Cc = 0.1$ and $x = (0, 0.833, 0.166)$ and $(0.0001, 0.833, 0.166–0.0001)$, the simulation results of the state wireless sensor population are displayed in Figures 13 and 14, respectively.

Figures 13 and 14. The simulation results in Figure 13 indicate that nodes of the wireless sensor network can choose strategy CC after an evolutionary game of the system is performed for a period of time. Figure 14 suggests that the nodes choose strategy D as long as there is a slight variation in the system population, so, subsequently, strategy CC is chosen, and, finally, all of the nodes choose strategy CC. Statistical analyses of the data in Figures 13 and 14 are presented in Tables 9 and 10, respectively.

From the statistical analyses in Tables 9 and 10, we used these experiments in 0/100/45.98/40.59/0/24.3/100 and 0/100/45.52/40.75/0/25.36/100 rows to get more meaningful data, which are presented in Figures 15 and 16, respectively.

From Figures 15 and 16, when all values of the nodes (C) in Figure 15 were zero, we see that all nodes of WSN in each case have chosen strategy CC, so the deviation in this case increased to 0.279 of 0.254 in CC, and this group will sustain a steady state. These conclusions were verified in Figures 13 and 14, respectively, and Lemma 4_(2) was also verified.

(5) When $Cc = 0.1$ and $x = (0, 0.857, 0.142)$ and $(0.0001, 0.857–0.0001, 0.142)$, the simulation results of the state wireless sensor population are displayed in Figures 17 and 18, respectively.

Figures 17 and 18. The simulation results in Figure 17 suggest that nodes of the wireless sensor network can choose strategy CC after an evolutionary game of the system is performed

Table 8: The statistical analyses of strategies C, D, and CC.

	X	C	D	CC
Minimal value	0	$-5.96E-07$	$-3.53E-07$	$3.44E-09$
Maximum value	300	0.9946	1	0.9995
Average value	130.2	0.2403	0.3812	0.383
Medium value	139.4	0.001984	0.01049	0.03015
Mode	0	$-5.96E-07$	$-3.53E-07$	$3.44E-09$
Deviation	86.78	0.3729	0.4648	0.4441
Range	300	0.9946	1	0.9995

Table 9: The statistical analyses of strategies C, D, and CC.

	X	C	D	CC
Minimal value	0	0	$-9.494e-07$	0.1667
Maximum value	100	0	0.8333	1
Average value	45.98	0	0.1469	0.87
Medium value	40.59	0	0.0003978	0.9999
Mode	0	0	$-9.494e-07$	0.1667
Deviation	24.3	0	0.2739	0.2544
Range	100	0	0.8333	0.8333

Table 10: The statistical analyses of strategies C, D, and CC.

	X	C	D	CC
Minimal value	0	$1.734e-06$	$-1.056e-06$	0.1666
Maximum value	100	0.00279	0.8333	1
Average value	45.52	0.0002201	0.1561	0.8577
Medium value	40.75	$1.067e-05$	0.0003766	0.9993
Mode	0	$1.734e-06$	$-1.056e-06$	0.1666
Deviation	25.36	0.0005504	0.2933	0.2798
Range	100	0.002788	0.8333	0.8334

Table 11: The statistical analyses of strategies C, D, and CC.

	X	C	D	CC
Minimal value	0	0	0.8571	0.000381
Maximum value	100	0	1.076	0.1429
Average value	53.64	0	1	0.05883
Medium value	55	0	1.037	0.0356
Mode	0	0	0.8571	0.000381
Deviation	30.97	0	0.07996	0.05804
Range	100	0	0.2186	0.1425

for a period of time. Figure 18 shows that nodes that chose strategy CC can choose strategy D as long as there is any slight variation in the system population, so, subsequently, strategy D is the chosen profit, and, finally, all nodes choose strategy D. Statistical analyses of the data in Figures 17 and 18 are presented in Tables 11 and 12, respectively.

From the statistical analyses in Tables 11 and 12, we used these experiments in 0/100/53.64/55/0/30.97/100 and 0/100/50.08/50.87/0/33.37/100 rows to get more meaningful data, which are presented in Figures 19 and 20, respectively.

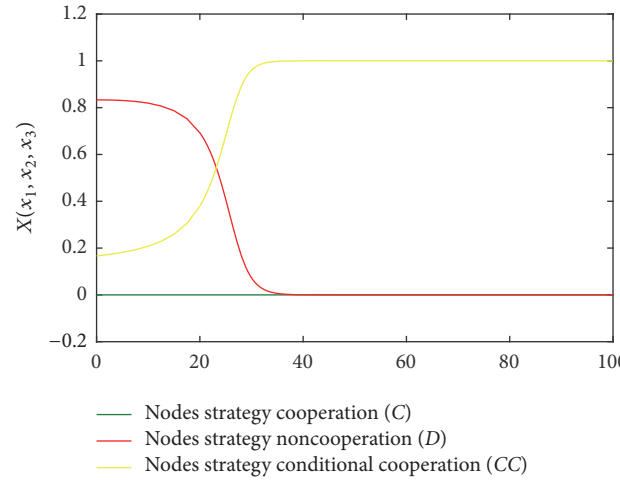

Figure 13: The state of population when $x = (0, 0.833, 0.166)$.

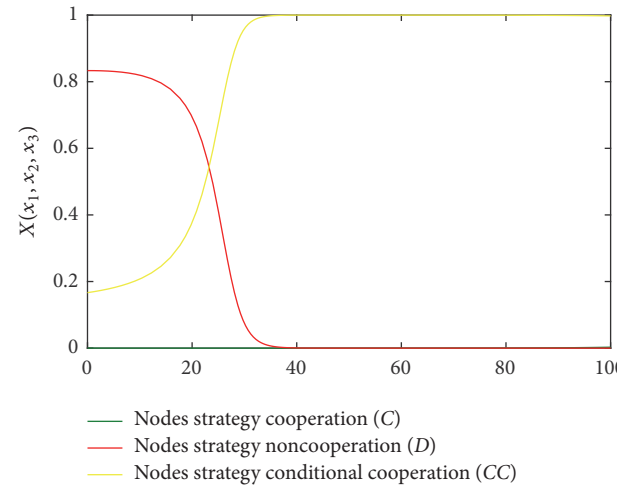

Figure 14: The state of population when $x = (0.0001, 0.833, 0.166–0.0001)$.

Based on Figures 19 and 20, when all values of the nodes (C) in Figure 19 were zero and the nodes (C) in Figure 20 were able to resist small variation, we see that all nodes of WSN in each case have chosen strategy D, so the group will continue to maintain a stable state. These observations were verified in Figures 17 and 18, and Lemma 4_(3) was also verified.

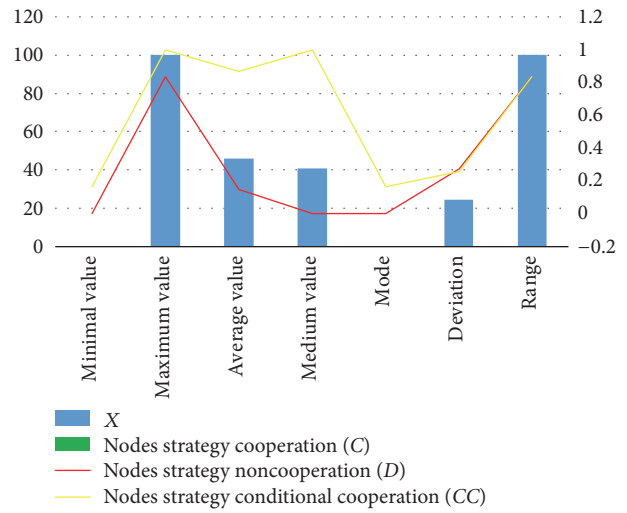

Figure 15: The state of population when X = (0, 300, 130.2, 139.4, 0, 86.78, 300).

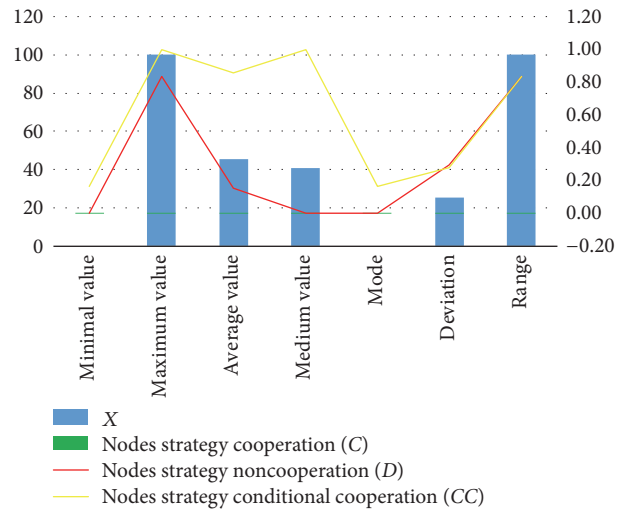

Figure 16: The state of population when X = (0, 300, 130.2, 139.4, 0, 86.78, 300).

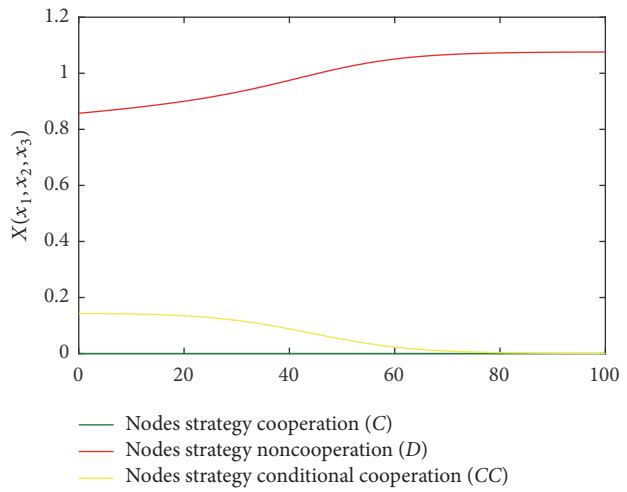

Figure 17: The state of population when x = (0, 0.857, 0.142).

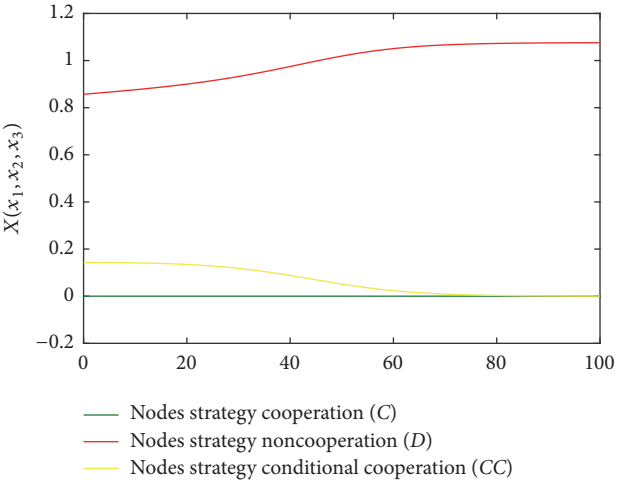

Figure 18: The state of population when x = (0.0001, 0.857–0.0001, 0.142).

Table 12: The statistical analyses of strategies C, D, and CC.

	X	C	D	CC
Minimal value	0	$-4.31E-07$	0.857	0.0003808
Maximum value	100	0.0001	1.076	0.1429
Average value	50.08	$6.88E-06$	0.9888	0.0657
Medium value	50.87	$1.30E-07$	1.023	0.04841
Mode	0	$-4.31E-07$	0.857	0.0003808
Deviation	33.37	$1.90E-05$	0.08613	0.06108
Range	100	0.0001004	0.2187	0.1425

Table 13: The statistical analyses of strategies C, D, and CC.

	X	C	D	CC
Minimal value	0	0.02433	$-7.34E-07$	0.1169
Maximum value	1000	0.8712	0.7232	0.9712
Average value	487.3	0.4024	0.02033	0.5788
Medium value	457.2	0.3863	$2.29E-14$	0.5841
Mode	0	0.02433	$-7.34E-07$	0.1169
Deviation	288.7	0.2636	0.09514	0.265
Range	1000	0.8468	0.7232	0.8543

(6) When Cc = 0.01, 0.0001, and 0.000001 and x = (0.33, 0.33, 0.33), (0.33, 0.33, 0.33), and (0.33, 0.33, 0.33), the simulation results of the state wireless sensor population are displayed in Figures 21, 22, and 23, respectively.

Figures 21, 22, and 23. Simulation results from Figures 21, 22, and 23 suggest that the cost of nodes based on the excitation strategy tends to be 0. In this case, the range increased up to 1000, and the values of C, D, and CC were nonzero; the population converged gradually from the original unstable state via three exit strategies to a state where cooperative and excitation strategies are available.

The statistics of all data in Figures 21, 22, and 23 are shown in Tables 13, 14, and 15, respectively.

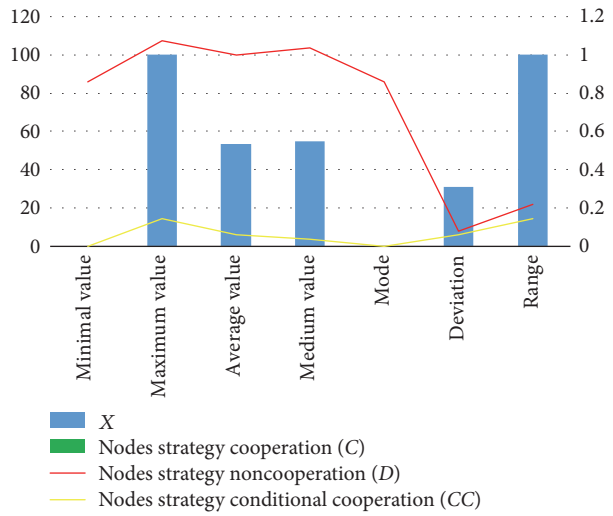

FIGURE 19: The state of population when X = (0, 100, 53.64, 55, 0, 30.97, 100).

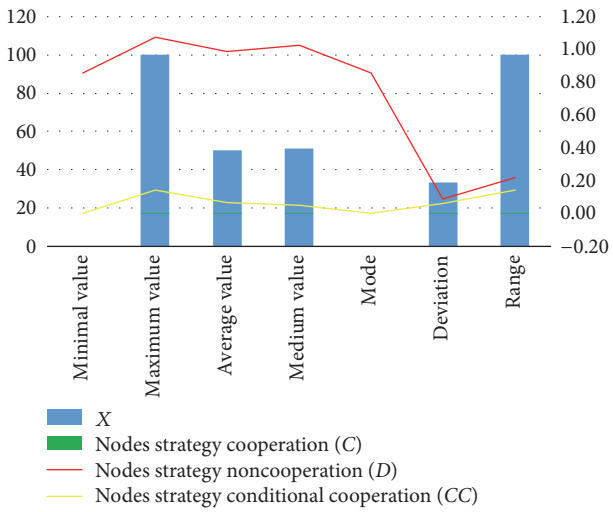

FIGURE 20: The state of population when X = (0, 100, 53.64, 55, 0, 30.97, 100).

TABLE 14: The statistical analyses of strategies C, D, and CC.

	X	C	D	CC
Minimal value	0	0.2454	$-2.66E-07$	0.33
Maximum value	1000	0.33	0.33	0.7526
Average value	492.1	0.2548	0.003945	0.7412
Medium value	490.7	0.2545	$2.72E-59$	0.7452
Mode	0	0.2454	$-2.66E-07$	0.33
Deviation	294.4	0.006238	0.03134	0.03559
Range	1000	0.08463	0.33	0.4226

From the statistical analyses in Tables 13, 14, and 15, in each case, we can see the range in Tables 13, 14, and 15; the range increased up to 1000 rows, and we used these experiments in 0/1000/487.3/457.2/0/288.7/1000, 0/1000/492.1/490.7/0/294.4/1000, and 0/1000/492.5/491.3/0/294.7/1000

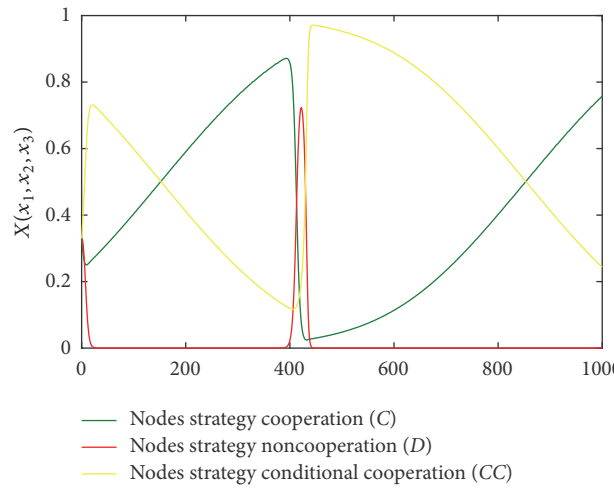

FIGURE 21: The state of population when C_C = 0.01 and x = (0.33, 0.33, 0.33).

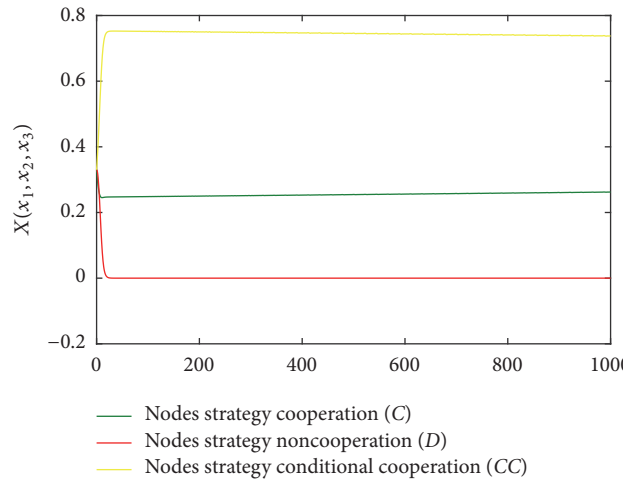

FIGURE 22: The state of population when C_C = 0.0001 and x = (0.33, 0.33, 0.33).

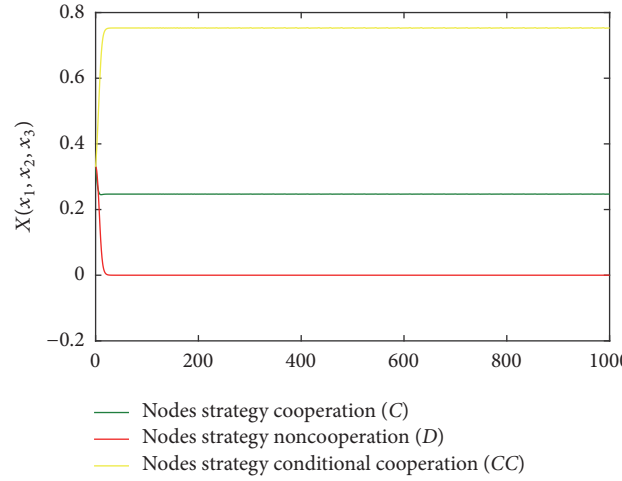

FIGURE 23: The state of population when C_C = 0.000001 and x = (0.33, 0.33, 0.33).

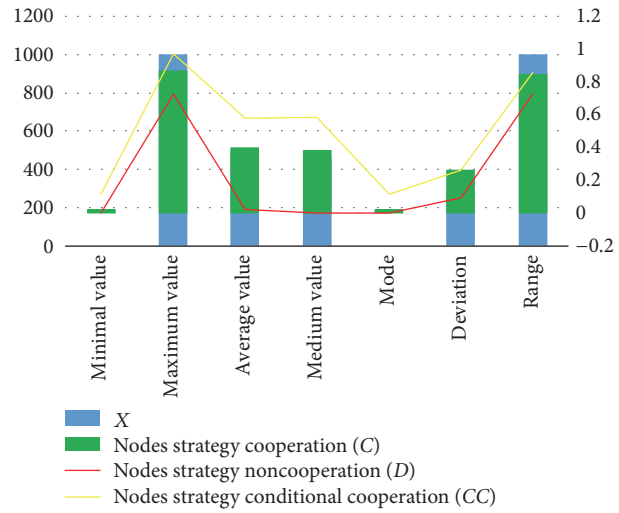

Figure 24: The state of population when X = (0, 1000, 487.3, 457.2, 0, 288.7, 1000).

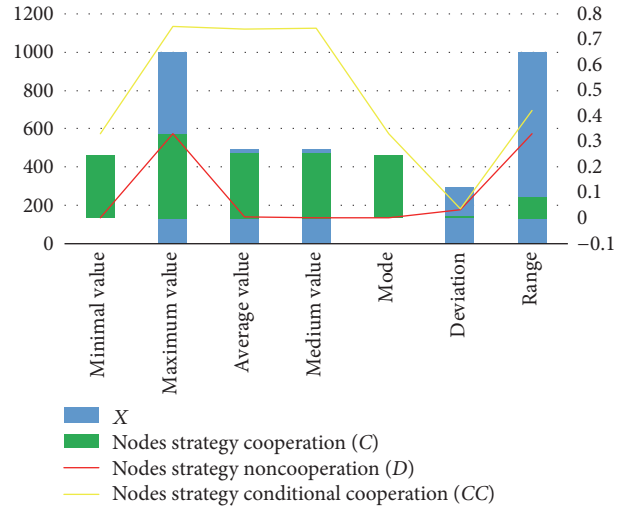

Figure 25: The state of population when X = (0, 1000, 492.1, 490.7, 0, 294.4, 1000).

Table 15: The statistical analyses of strategies C, D, and CC.

	X	C	D	CC
Minimal value	0	0.2453	$-2.68E-07$	0.33
Maximum value	1000	0.33	0.33	0.7538
Average value	492.5	0.2474	0.003944	0.7485
Medium value	491.3	0.247	$4.44E-58$	0.7529
Mode	0	0.2453	$-2.68E-07$	0.33
Deviation	294.7	0.004958	0.03134	0.0362
Range	1000	0.0847	0.33	0.4238

rows to get more meaningful data, which are presented in Figures 24, 25, and 26, respectively.

In the case of Figures 24, 25, and 26, the range increased up to 1000, and the values of C, D, and CC were nonzero; first, when the deviation (X = 288.7) in Figure 24 occurred, the

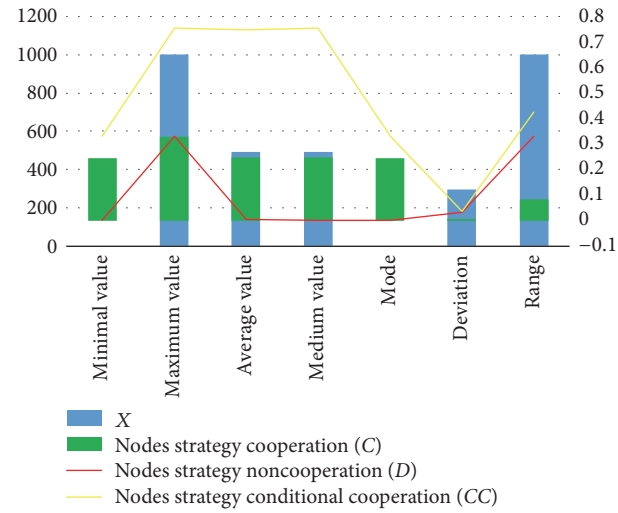

Figure 26: The state of population when X = (0, 1000, 492.5, 491.5, 0, 294.7, 1000).

result of the deviation was small in nodes strategy D, only 0.095, but in the same case, in the nodes strategies C and CC, it is not a better result, since the deviation values were 0.263 and 0.265. Second, when the deviations were X = 288.7, X = 294.7 in Figures 25 and 26, the results of the deviation were small in nodes strategy C, 0.006 and 0.004, and in the same case, in the nodes strategies D and CC, it is also a better result, given that the deviation values in each case were only 0.031 and 0.036, and in the same case, the average and medium values of nodes strategies D and CC were only 0.003 and 0.74. So, the values in Figures 25 and 26 were smooth and steady. These statements are verified in Figures 21, 22, and 23, respectively, and Lemma 6 was also verified.

6. Discussion

In Figures 24, 25, and 26, when the average and medium values are smooth and steady, the malicious node attack noncooperative behavior occurs and leads to all of the nodes having the safety problem of noncooperative behavior. First, according to the characteristics of wireless sensor networks, the incentive game model of node forwarding packets was established. Second, evolutionary game theory was used to analyze the dynamics and stability of the incentive game model, with emphasis on nodes of the game through continuous learning, imitation, and trial and error to adjust their strategies to find the one most suited to their own interest and demands of the strategy, finally resulting in the network's achieving good collaboration. There are many limitations in the current approaches [13–15] to wireless sensor network systems. Most of the nodes in a network exhibit selfish behavior. Also, current approaches are unable to complete an accurate description of the dynamic evolution of the node strategy, making it impossible to determine the robustness and stability of these mechanisms due to the lack of analysis based on strict mathematical theories. Our research results indicated that our approach is faster and the best among all

recent papers in that it added a new condition of cooperation between the nodes of the WSN and that these nodes can be cooperative and can then forward packets efficiently and resist small variations. Our analyses were the first among all recent papers to indicate that the performance of the WSN could be enhanced due to its stability and reliability; in the same case, the deviations of only 0.031 and 0.036 existed in nodes strategy noncooperation and nodes strategy conditional cooperation, respectively, as shown in Figures 25 and 26. Thus, the time is much shorter because the deviation is very small.

7. Conclusion

In this paper, we proposed a dynamic cooperative incentive mechanism that is suitable for wireless sensor networks based on the evolutionary game theory, simulation, and trial and error. According to the characteristics of wireless sensor networks, the mechanism can be used to determine strategies that are consistent with their own requirements. As indicated by the simulation results, the wireless sensor network uses an incentive mechanism that allows network nodes to forward data packets efficiently. The system is able to resist any slight variations so that the network maintains good operating conditions, meaning that the stability and reliability of wireless sensor networks have been improved.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: security protocols for sensor networks," in *Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '01)*, pp. 189–199, July 2001.

[2] C. Hartung, "Node compromise in sensor network: the need for Secure System," Tech. Rep. CU-CS-988-04, 2005.

[3] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, 2006.

[4] J. Newsome et al., "The Sybil attack in sensor network analysis and defenses," in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Network*, 2004.

[5] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[6] B. Yu and B. Xiao, "Detecting Selective forwarding attacks in wireless sensor network," in *Proceedings of the 2nd International Workshop on Security in System and Network*, 2006.

[7] F. Hu and N. K. Sharma, "Security considerations in ad hoc sensor networks," *Ad Hoc Networks*, vol. 3, no. 1, pp. 69–89, 2005.

[8] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *Proceedings of the 26th IEEE International Conference on Computer Communications, IEEE INFOCOM '07*, pp. 1307–1315, May 2007.

[9] S. Datema, *A Case Study of Wireless Sensor Network Attacks [M.S. thesis]*, Parallel and Distributed System Group, Faculty of Electrical Engineering, Mathematics, and Computer Science, Delft University of Technology, Delft, Netherlands, 2005.

[10] E. C. Ngai, J. Liu, and M. R. Lyu, "On the intruder detection for sinkhole attack in wireless sensor networks," in *Proceedings of the 2006 IEEE International Conference on Communications, ICC '06*, pp. 3383–3389, July 2006.

[11] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113–127, May 2003.

[12] Z. Sheng, L. E. Li, Y. G. Liu, and Y. R. Yang, "On designing incentive compatible routing and forwarding protocols in wireless ad-hoc networks," *Wireless Networks*, vol. 13, no. 6, pp. 799–816, 2007.

[13] G. Cui, M. Li, Z. Wang et al., "Analysis and evaluation of incentive mechanisms in P2P networks: a spatial evolutionary game theory perspective," *Concurrency and Computation Practice and Experience*, vol. 27, no. 12, pp. 3044–3064, 2015.

[14] K. Lu and S. Wang, "A reward-and-punishment aware incentive mechanism in P2P networks," in *Proceedings of the 12th International Conference on Fuzzy Systems and Knowledge Discovery, FSKD '15*, pp. 2049–2053, August 2015.

[15] D.-P. Qu, X.-W. Wang, and M. Huang, "Selfish node detection and incentive mechanism in mobile P2P networks," *Journal of Software*, vol. 24, no. 4, pp. 887–899, 2013.

[16] Y. Wang, A. Nakao, A. V. Vasilakos, and J. Ma, "P2P soft security: on evolutionary dynamics of P2P incentive mechanism," *Computer Communications*, vol. 34, no. 3, pp. 241–249, 2011.