energies

MDPI

Article

An Active Defense Model with Low Power Consumption and Deviation for Wireless Sensor Networks Utilizing Evolutionary Game Theory

Mohammed Ahmed Ahmed Al-Jaoufi *, Yun Liu and Zhenjiang Zhang

School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China; liuyun@bjtu.edu.cn (Y.L.); zhjzhang1@bjtu.edu.cn (Z.Z.)

* Correspondence: 12119002@bjtu.edu.cn; Tel.: +86-173-1015-3169

Received: 9 April 2018; Accepted: 15 May 2018; Published: 17 May 2018

Abstract: In wireless sensors networks, nodes may be easily captured and act non-cooperatively, for example by not defending forwarding packets in response to their own limited resources. If most of these nodes are obtained by attackers, and an attack by an internal malicious node occurs, the entire network will be paralyzed and not be able to provide normal service. Low power consumption indicates that the rational sensor nodes tend to be very close to the mean; high power consumption indicates that the rational sensor nodes are spread out over a large range of values. This paper offers an active defense model for wireless sensor networks based on evolutionary game theory. We use evolutionary game theory to analyze the reliability and stability of a wireless sensor network with malicious nodes. Adding a defense model into the strategy space of the rational nodes and establishing a preventive mechanism forces the malicious node to abandon the attack and even switch to cooperative strategies. Thus, this paper argues that the stability and reliability of wireless sensor networks can be improved. Numerical experiments were conducted to evaluate the proposed defense model, and these results verified our conclusions based on a theoretical analysis that showed that, compared with the existing algorithms, our approach has lower energy consumption, lower deviation, and a higher probability to quickly switch each node to cooperative strategies.

Keywords: active defense; malicious node; attack; deviation; wireless sensor network security

1. Introduction

A wireless sensor network (WSN) is a network constructed through the self-organization of a large number of sensor nodes. When considering today's network security problems, a significant amount of research is being conducted on the security of wireless sensor networks from different perspectives, with the goal of ensuring that these networks are operating effectively. In terms of security issues, the problems encountered by WSNs and traditional wireless networks can differ greatly based on the characteristics of the individual network.

Since the resources for sensor nodes are limited, processing power, storage space, energy, and other factors can prevent the direct application of effective security protocols and algorithms to wireless sensor networks and result in greater security risks. Qiu et al. [1] proposed an active defense model for WSNs in which the sensor nodes can be dynamic and active, so as to adjust their defensive strategies, thereby achieving an effective defense against different approaches used by attackers.

Chen et al. [2] proposed a mechanism that emphasizes adjustments in the node strategies forwardly and passively to maximize their fitness, thereby forcing the population in the wireless sensor network to ultimately combine into a cooperative state. Hu et al. [3] proposed an adaptive active defense mechanism with low power consumption. This scheme configured some nodes as

monitoring nodes to identify attacks, and when an attacker is identified, the defense system is activated and repairs the damaged node.

Elazouzi et al. [4] introduced a general framework for competitive forwarding in delay-tolerant networks (DTNs) under specific energy constraints and message lifetime requirements in the context of DTNs. In their proposed framework, a basic two-hop relay was used to route packets, and a wireless link becomes available whenever two nodes meet and focus on the probability of delivering a message.

Wu et al. [5] introduced a two-hop routing algorithm and an asymmetric multi-community evolutionary game framework. Their model found each community's unique evolutionary stable strategy (ESS)and provided its existence conditions. Wu et al. [6] proposed an incentive mechanism based on game theory and social networks to determine the availability of packets. Zuo et al. [7] introduced an evolutionary, game-based routing model to eliminate selfish routing behaviors and improve the routing efficiency in peer-to-peer (P2P) networks. The routing behavior of a node was considered a non-cooperative routing game wherein the selfish player routes traffic through a congested and sensitive network. The dynamic behavior of such nodes was studied using the generalized simulation dynamics method.

Feng et al. [8] studied the cooperative mechanism of prefabricated producers based on evolutionary game theory. Their model analyzed the behavioral evolution trends of both parties using evolutionary game theory. Esposito et al. [9] used game theory to promote truth-telling between service providers in smart cloud storage service selection. The dynamic behavior of these nodes was studied using the generalized imitative dynamics approach.

Chen et al. [10] proposed a proactive defense model for wireless sensor networks, in which the node's limited ability to learn the evolution of rationality from different attack strategies of the attacker was emphasized, and the node could dynamically adjust its strategy to achieve the most effective defense. Dynamic evolution means that nodes can be active and dynamic to adjust their defensive strategies to achieve effective defense, according to the attacker's different policies. Bendjima and Feham [11] proposed the use of an intelligent WSN communication architecture based on a multi-agent system (MAS) to ensure optimal data collection. To reduce the size of the MAS, nodes in the network sectors were grouped in such way that, for each MA, an optimal itinerary was established using the least amount of energy with efficient data aggregation within the least amount of time.

Alskaif et al. [12] conducted a survey of game theory to balance wireless sensor networks and provide the required service, while achieving a trade-off between providing the required lifetime and maximizing the lifetime of a network. Guo et al. [13] recommended against various routing attacks on DTNs; the network can reach evolutionary stable strategy (ESS) under special conditions after meeting the evolutionary requirements in the context of DTNs. Evolutionary game theory-based defense schemes can achieve an average delivery ratio, low average transmission delay, and low network overhead in various routing attack scenarios. The initial parameters affect the convergence speed and the final ESS, but the initial ratio of the nodes choosing different strategies only affects the game process.

Li et al. [14] proposed a novel topology link control technique and mitigation attacks in real-time environments. In the proposed approach, a prediction model was constructed using copula functions to predict the peak of a resource through another resource. Al-Jaoufi et al. [15] presented a new model for the selfish node incentive mechanism with a forward game node for wireless sensor networks, and used the incentive mechanism to successfully forward packets while resisting any slight variations.

Therefore, the present incentive model has the following disadvantages [12–14]: (1) with y being the current mechanism, determining the robustness and stability of these mechanisms is impossible due to the lack of analysis when applying strict mathematical theories; (2) the current mechanism enhances the performance of the system, so it can achieve its best performance, but it cannot guarantee that each node can or will achieve the best benefit, so the nodes are still likely to exhibit selfish behaviors; (3) the current model forwarded packets well while resisting any slight variations. However,

the disadvantage is that this model used higher power; it was too late to initiate defensive measures due to the limited ability of power consumption for the defense to compute the nodes [15].

For these reasons, this paper proposes an active defense model for wireless sensor networks to analyze the reliability and stability of a wireless sensor network with malicious nodes. Our model uses game theory to construct prevention strategies for wireless sensor networks, and allows the malicious node to abandon the attack and even cooperate to effectively improve the reliability and stability of those networks.

2. Development and Key Knowledge of Game Theory

In traditional game theory, the participants are often assumed to be completely rational and make decisions based on complete and full information. However, in real network life, participants' full rationality and the conditions wherein complete information is available are difficult to achieve. In any cooperative competition of enterprises, differences exist between participants, and incomplete information can be produced by the obvious complexities of the network environment, the game problem, and the limited rationality of the participants.

Game theory specializes in game strategies; it is also known as the "theory of games". Game theory is a discipline based on mathematics that deals with how a participant will plan to obtain maximum benefit in a game. Each standard game includes nine basic elements: participants, rules of the game, game behavior, information, game strategies, sequence of the game, earnings of the game, the results of the game, and equilibrium. Nash equilibrium is a very important concept in any game algorithm. It is a set of policies for a group of participant policies, and any participant who individually changes that strategy will be compromised. Nash equilibrium, therefore, corresponds to having a stable game result. Once the result of this game is attained, no participant has the motivation to change their own strategy [15].

3. Active Defense Model Based on Evolutionary Game Theory

The active defense model is based on procedural behavior, independent analysis, and the judgment of the real-time protection of a WSN. The model simultaneously provides accurate and automatic identification of attackers and monitoring of program behavior, as well as automatic extraction of feature values, visual display monitoring information, and other characteristics. Active defense is both a type of technology and a technical system composed of a variety of technologies that provide an active defense function for a wireless sensor network by using the rational nodes of these technologies. Active defense organically combines the rational nodes, provides coordination, and allows complete security of the wireless sensor network.

In statistics and probability theory, deviation shows how much variation or dispersion exists from the average or expected value. A low deviation indicates that the data points tend to be very close to the mean; high deviation indicates that the data points are spread out over a large range of values [16]. Thus, to determine the results, we considered three kinds of defensive strategies in the simulations: (1) rational nodes without choosing defense; (2) half of the rational nodes choosing defense; and (3) all of rational nodes choosing defense. The architecture of the model systems is shown in Figures 1–3.

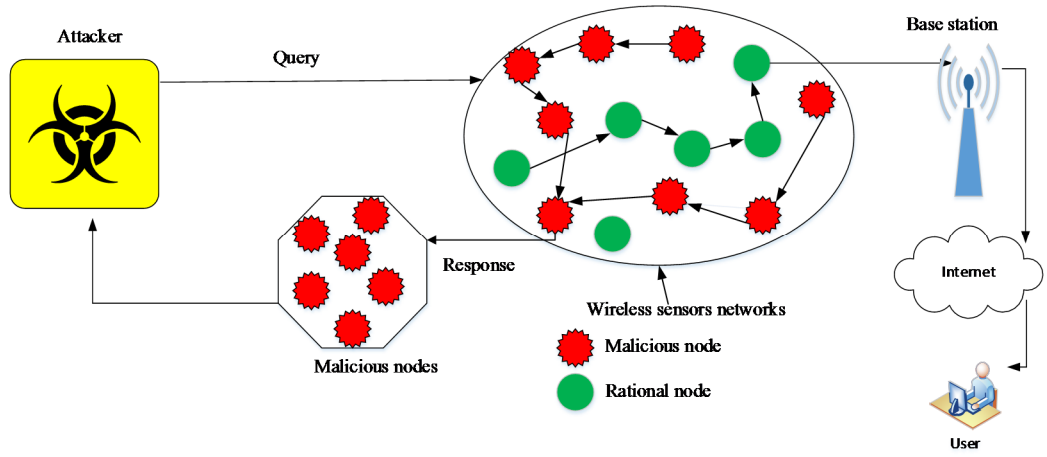

Figure 1. The architecture of rational nodes without choosing defense.

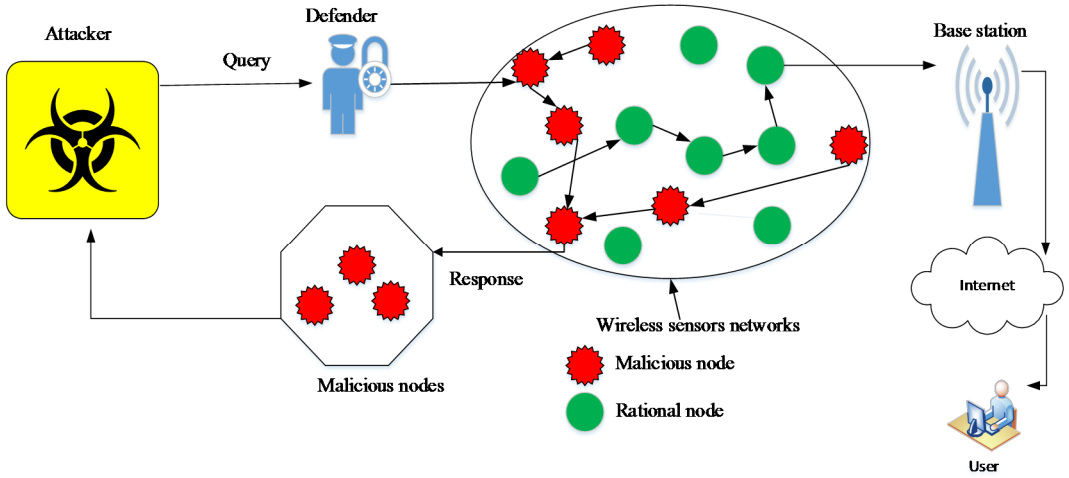

Figure 2. The architecture for half of the rational nodes choosing defense.

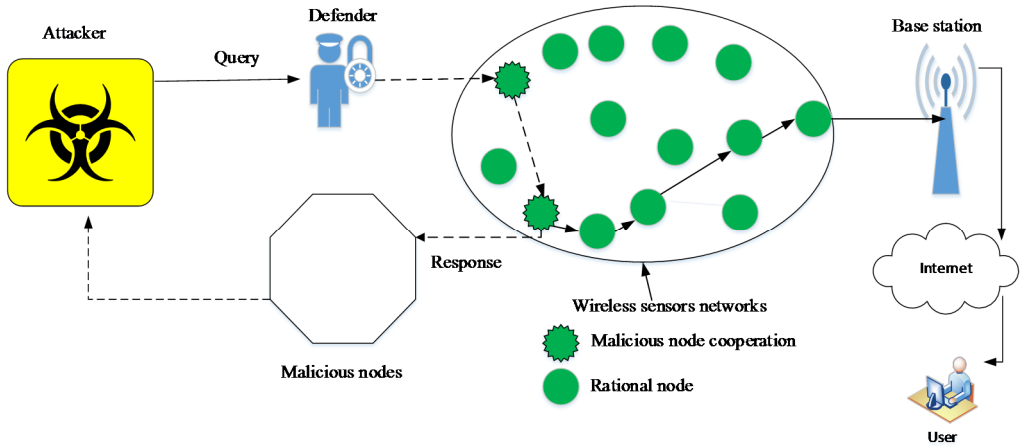

Figure 3. The architecture for all rational nodes choosing defense.

Figures 1–3 show that our goal considered improving security while reducing the deviations for wireless sensor networks. Figure 1 shows that when the rational nodes do not choose defense, the attacker very easily captured nodes and acted non-cooperatively, and capturing the rational nodes resulted in higher power consumption. Figure 2 shows that when the half of the rational nodes choose

defense, then the attacker does not easily capture the nodes and acts non-cooperatively, and taking the rational nodes takes more time with a lower power consumption. Figure 3 shows that when all rational nodes choose defense, then it is difficult for the attacker to capture nodes and act non-cooperatively, and taking the rational nodes occurs quickly with a much lower power consumption.

Before we establish the game model for the malicious behavior of nodes, we must make the following assumptions concerning a wireless sensor network:

- Assumption 1: Infinite sensor network nodes are limited, and each node has a routing forwarding function. The parameters of the defender and the attacker can be defined as follows: R denotes the reward for forwarding one message, C_A denotes the cost of the attacker, C_D denotes the cost of the defender, $D_{f,half}$ denotes half the rational nodes choosing defense, and $D_{f,all}$ denotes all the rational nodes choosing defense. In this current effort, we assumed that the value of half the rational nodes choosing defense was 0.33, and the value of all the rational nodes choosing the defenders was 1. Normally, $D_{f,all} > D_{f,half}$.
- Assumption 2: is widely used to design defensive strategies for rational sensor nodes and protocol implementation in WSNs [17]. There are two kinds of nodes in the network: (1) defender nodes (rational nodes), and (2) attacker nodes (malicious nodes). The latter type refers to nodes in the network after capture with all packets having the same size as the malicious node. The node will successfully forward a packet, and the benefits are the same as those for the proceeds of the R units.

Applying the three basic elements of the game model—the participant, the strategy space, and the profit matrix—the game model for a wireless sensor network node was established as follows:

1. Participants: According to the features of the security of a wireless sensor network, the participants in the game can be divided into two different populations: (1) a population composed of rational nodes, mainly through forwarding packets to obtain benefits (the rational nodes); and (2) a population composed of malicious nodes (denoted the malicious nodes), so that the population system is a group of strategic behaviors. These populations can gain revenue by launching attacks or by forwarding packets, with the former having a larger payoff than the latter.
2. Strategy Space: The rational node has two kinds of cooperation strategies: (1) rational node cooperation (R_c), and (2) rational node non-cooperation (R_{nc}). Cooperation is the behavior of the node when it is forwarding a packet, which is the behavior of a node loss packet; then, its strategy set is recorded as $S_1 = \{R_c, R_{nc}\}$. A malicious node has three different strategies: (1) malicious node cooperation (M_c); (2) attacker (A_t); and (3) malicious node non-cooperation (M_{nc}). This strategy set is recorded as $S_2 = \{M_c, A_t, M_{nc}\}$.
3. Profit Matrix: According to the characteristics of wireless sensor networks, C_A represents the resource (e.g., energy or bandwidth) being consumed by the malicious node to attack the behavior, and C_R indicates that the node is forwarding the resource consumed by a forwarded packet, normally $C_R > C_A$. This profit matrix is divided into two kinds of nodes as shown in Table 1.

Table 1. Profit matrix for forwarding packets.

Malicious Node / **Rational Node**	**Cooperative**	**Attacker**	**Non-Cooperative**
Cooperative	$R - C_R, R - C_R$	$-C_R, R - C_A$	$-C_R, 0$
Non-cooperative	$0, -C_R$	$0, -C_A$	$0, 0$

The profit matrix above shows that, after a finite number of games, both kinds of nodes in a wireless sensor network choose the non-cooperative strategy, and that strategy combination {non-cooperative, non-cooperative} becomes the Nash equilibrium solution of the finite repetition

game. If the network is in this non-cooperative equilibrium state, the network will be paralyzed and unable to provide normal service, thus providing an unsatisfactory result.

In the current research, a new defensive strategy was added to the rational node strategy to limit the attack behavior of the malicious node. This new strategy makes the malicious node unprofitable, and the malicious node thus can no longer attack and cooperate. Furthermore, it allows the network to provide normal service and promotes the higher performance of the network.

When the rational node adds a new defensive strategy, it has three possible strategies: cooperative, non-cooperative, and defender (D_f). The strategy space, $S_1 = \left\{R_c, R_{nc}, D_f\right\}$, as well as both sides of the game profit matrix are shown below in Table 2.

Table 2. Profit matrix for active defensive strategies.

Malicious Node / Rational Node	Cooperative	Attacker	Non-Cooperative
Cooperative	$R - C_R, R - C_R$	$-C_R, R - C_A$	$-C_R, 0$
Non-cooperative	$0, -C_R$	$0, -C_A$	$0, 0$
Defender	$R - C_D, R - C_R$	$R - C_D, -C_A$	$-C_D, 0$

We assume here that the nodes in wireless sensor networks use rational node strategies, i.e., R_c, R_{nc}, and D_f for x_{Rc}, x_{Rnc}, and x_{D_f}, respectively, where $x_{Rc} + x_{Rnc} + x_{D_f} = 1$. It appears that $x_1 + x_2 + x_3 = 1$. We assume that the malicious nodes' strategies are used, i.e., M_c, M_{nc}, and A_t for y_{Mc}, y_{Mnc}, and, y_{At} respectively, wherein $y_{Mc} + y_{Mnc} + y_{At} = 1$, and it appears that $y_1 + y_2 + y_3 = 1$. The strategies of the rational nodes and malicious nodes are defined as follows:

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

As the defender has three strategies gleaned from the strategy space $S_1 = \left\{R_c, R_{nc}, D_f\right\}$, the profit matrix of the defender and attacker are defined as A and B, respectively:

$$A = \begin{bmatrix} R - C_R & -C_R & -C_R \\ 0 & 0 & 0 \\ R - C_D & R - C_D & -C_D \end{bmatrix} \tag{2}$$

$$B = \begin{bmatrix} R - C_R & R - C_A & 0 \\ -C_R & -C_A & 0 \\ R - C_R & -C_A & 0 \end{bmatrix} \tag{3}$$

Replicator dynamics describe a dynamic selection process, as proposed by Taylor and Jonker [18]. At time t, let $p_i(t)$ be the number of individuals who are currently programmed to the strategy $i \in K$, and let $p(t) = \sum_{i \in K} p_i(t)$ be the total population.

Then, the associated population state can be in defined as the vector $z_i(t) = (z_i(t), \ldots, z_k(t))$, where each component $z_i(t)$ is the population share, i.e.,$z_i(t) = p_i(t)/p(t)$. The term $u(z, z)$ is defined as the average payoff of the population, and the term $u(s_i, z)$ is defined as the expected payoff using strategy i. The replicator dynamics in the evolutionary game can thus be expressed as:

$$\frac{dz_i}{dt} = [u(s_i, z) - u(z, z)]z_i \tag{4}$$

According to Equations (1)–(4), the replicator dynamic equations of the blurred vision game for defenders and attackers are divided into two replicator dynamic equations, as follows:

$$\frac{dx_h}{dt} = \left[\sum_{k\in S_2} a_{hk}y_k - \sum_{j\in S_1}\sum_{k\in S_2} x_i a_{jk} y_k\right] x_h \tag{5}$$

$$\frac{dy_k}{dt} = \left[\sum_{h\in S_2} b_{hk}x_h - \sum_{j\in S_2}\sum_{k\in S_1} y_i b_{hj} x_h\right] y_k \tag{6}$$

where h, k, j = 1, 2, 3 and a, b are the corresponding elements of the A and B matrices. Thus, the replicator dynamic equations for $x_1, x_2, x_3, y_1, y_2, y_3$ are computed as:

$$\frac{dx_1}{dt} = \left[x_1y_1 - x_1^2y_1 - x_1x_3(y_1+y_2)\right]R - (x_1 - x_1^2)C_R + x_1x_3C_D \tag{7}$$

$$\frac{dx_2}{dt} = -[x_1x_2y_1 + x_2x_3(y_1+y_2)]R - x_1x_2C_R + x_2x_3C_D \tag{8}$$

$$\frac{dx_3}{dt} = \left[x_3(y_1+y_2) - x_1x_3y_1 - x_3^2(y_1+y_2)\right]R + x_1x_3C_R - (x_3 - x_3^2)C_D \tag{9}$$

$$\frac{dy_1}{dt} = \left[(x_1+x_3)y_1 - y_1^2(x_2+x_3) - x_1y_1y_2\right]R - (y_1 - y_1^2)C_R + y_1y_2C_{\mathrm{A}} \tag{10}$$

$$\frac{dy_2}{dt} = \left[x_1y_2 - y_1y_2(x_1+x_3) - x_1y_2^2\right]R - (y_2 - y_2^2)C_R + y_1y_2C_{\mathrm{R}} \tag{11}$$

$$\frac{dy_3}{dt} = -[(x_1+x_3)y_1y_3 + x_1y_2y_3]R - y_1y_3C_R + y_2y_3C_{\mathrm{A}} \tag{12}$$

Thus, we applied the game theoretic analysis tool to produce the security of a wireless sensor network. The following theorems are provided to achieve that result. First, based on the characteristics of WSNs, the active defense model of node forwarding packets was established. Second, using evolutionary game theory to analyze the dynamics and stability of the active defense model and for the networks to achieve good collaboration, emphasis was placed on the nodes of the game through continuous learning, imitation, and trial and error to determine their strategies to find the most suitable strategy for their own interests.

Theorem 1. *In wireless sensor networks that consist of N nodes with a small probability of having a population of sensor nodes, lower cost (C_D) and a mutation probability approach of zero based on the active defense strategies, the defensive strategy (D_f) is considered to be evolutionarily stable.*

Proof. Based on the theorem of evolutionary stability, if strategy i is evolutionarily stable, 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 the arbitrary condition $i \neq j$. The profit matrix in Table 2 suggests that the defensive strategy requires $a_{22} > a_{12}$ and $a_{22} > a_{32}$ to meet the definition of an evolutionary game, so that the defensive strategy is evolutionarily stable and exhibits a strict Nash equilibrium. □

Theorem 2. *If the deviation value is zero and the average-medium defensive strategy has the same value, and the variation probabilities and composition of sensor nodes are fewer in wireless sensor networks, the population system then converges and uses defensive strategies and the malicious node in order to cooperate.*

Proof. Based on the theorem of a population system that converges, in order for the malicious node to cooperate, it must meet the following two conditions: (1) the deviation value ≤ 0 and (2) average value = medium value, so that the population system is evolutionarily stable and exhibits a strict Nash equilibrium. □

Accordingly, using Theorem 2 from the previous analysis, we can obtain the following propositions:

Proposition 1. *When strategy $R_c \neq 0$, strategy $R_{nc} \neq 0$, and strategy $D_f = 0$ after a period of an evolutionary game, the nodes in the wireless sensor networks eventually choose strategy M_{nc}. At this point, the population system is unable to continue in a stable state.*

Proof. Based on the proposition of the population system being in an unstable state, if the strategy without defense is ($D_f = 0$), the nodes in the wireless sensor networks eventually choose strategy M_{nc}. Thus, after the nodes choose strategy M_{nc}, the population system is unable to continue in the stable state that is shown in Figure 4. □

Proposition 2. *When strategy $R_c \neq 0$, strategy $R_{nc} \neq 0$, and strategy $D_{f,half} \neq 0$, and half of the rational nodes in the wireless sensor networks choosing the defensive strategy are in the system after a period of time for evolution, the nodes in the wireless sensor networks eventually choose strategy M_c. At this point, the population system is able to continue in a stable state.*

Proof. Based on the proposition of the population system being in a stable state, if the strategy is $D_{f,half} \neq 0$ for half the rational nodes when choosing defense, the nodes in the wireless sensor networks eventually choose strategy M_c. Thus, after the nodes choose strategy M_c, the population system is able to continue in a stable state, as shown in Figure 5. □

Proposition 3. *When strategy $R_c = 0$, strategy $R_{nc} = 0$, and strategy $D_{f,all} \neq 0$, and all the rational nodes in the wireless sensor networks choosing a defensive strategy are in the system after a period of time for evolution, then the nodes in the wireless sensor networks eventually choose strategy M_c. At this point, the population system is in a stable state.*

Proof. Based on the proposition that the population system is in a stable state, if the strategy $D_{f,all} \neq 0$ when all the rational nodes choose defense, the nodes in the wireless sensor networks eventually choose strategy M_c, thus after the nodes choose strategy M_c, the population system is in a stable state, as shown in Figure 8. □

Proposition 4. *When strategy $R_c \neq 0$, strategy $R_{nc} = 0$, and strategy $D_{f,all} \neq 0$, and all the rational nodes that appear in the wireless sensor networks choose the defensive strategy, in the system, after a period of time for evolution, the nodes in the wireless sensor networks eventually choose strategies M_c and R_c. At this point, the population system converges and adopts a stable state.*

Proof. Based on the proposition that the population system converges and adopts a stable state, if the strategy $D_{f,all} \neq 0$ for all rational nodes when choosing defense is adopted, along with the strategy $R_c \neq 0$, the nodes in the wireless sensor networks will eventually choose strategies M_c and R_c. Thus, after the nodes choose strategies M_c and R_c, the population system is in a stable state, as shown in Figure 10. □

4. Modeling Simulation and Analysis

Modeling and simulation experiments were performed using the MATLAB mathematical tool version 2016a. The assumptions for the wireless sensor network were as follows. Due to different measurement standards for the profit and the cost of the nodes, all the participants' parameters were standardized with values in the range of [0,1]. Given $R = 1.0$, $C_R = 0.4$, $C_A = 0.3$, and $C_D = 0.5$, a mathematical model was established using Equations (7)–(12).

4.1. Rational Nodes Not Choosing Defense and Half the Rational Nodes Choosing Defense

The simulation results for the state of the wireless sensor population when $(x, y) = (x_1, x_2, x_3, y_1, y_2, y_3) = (0.5, 0.5, 0, 0.33, 0.33, 0.33)$ and $(0.33, 0.33, 0.33, 0.33, 0.33, 0.33)$ are shown below in Figures 4 and 5, respectively.

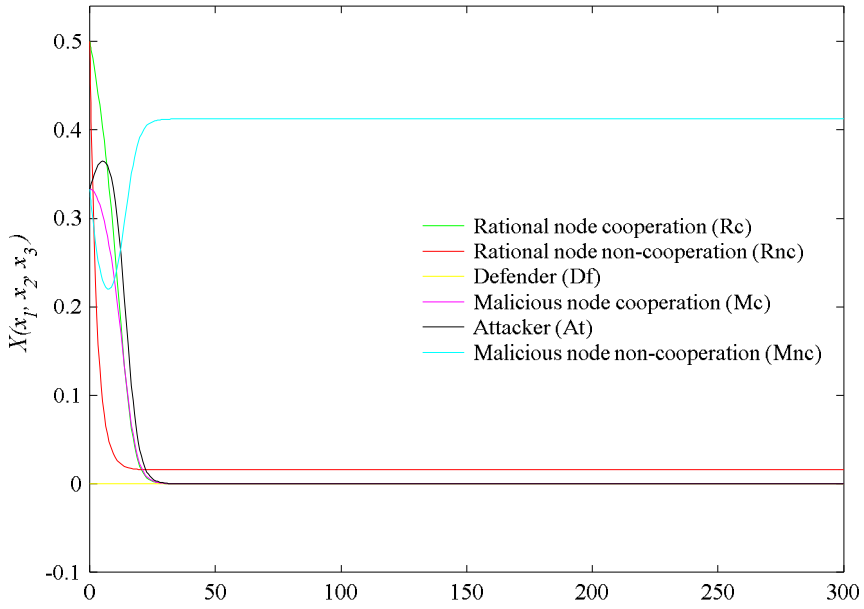

Figure 4. The rational nodes not choosing defense.

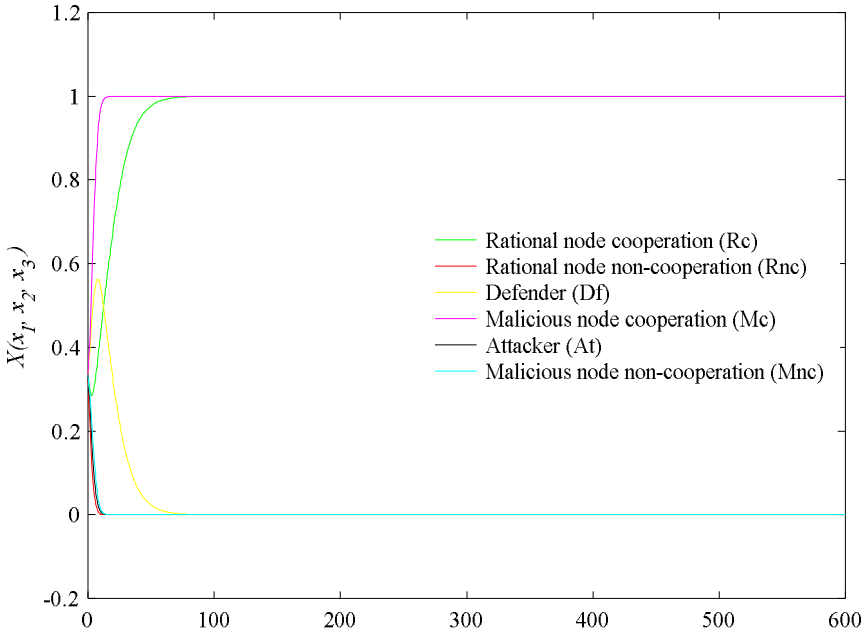

Figure 5. Half the rational nodes choosing defense.

When the rational nodes in wireless sensor networks are without defensive strategies, the simulation result in Figure 4 indicates that the nodes of the wireless sensor network choose strategy M_{nc} after an evolutionary game is performed for a period of time. In Figure 5, to determine the simulation results, we believed that wide area wireless sensor networks would appear and the range would increase up to 600, showing that, in this part of the simulation, when half the rational nodes in the wireless sensor networks choose defensive strategies in the system after a period of time for evolution, the nodes of the wireless sensor network will choose strategy M_c in this state. As long as little variation occurs in the node, the population system will choose strategy R_c. At this point, the population system continues in a stable state.

The results of the statistical analysis of all the data in Figures 4 and 5 are provided below in Tables 3 and 4, respectively.

Table 3. Statistical analyses of strategies R_c, R_{nc}, D_f, M_c, A_t, and M_{nc}.

	X	R_c	R_{nc}	D_f	M_c	A_t	M_{nc}
Minimum Value	0.00	0.00	0.02	0.00	0.00	0.00	0.22
Maximum Value	300	0.50	0.50	0.00	0.33	0.36	0.41
Average Value	116.3	0.05	0.04	0.00	0.04	0.04	0.39
Medium Value	95.03	0.00	0.02	0.00	0.00	0.00	0.41
Mode	0.00	0.00	0.02	0.00	0.00	0.00	0.22
Deviation	94.09	0.13	0.08	0.00	0.09	0.11	0.05
Range	300.0	0.50	0.48	0.00	0.33	0.36	0.19

Table 4. Statistical analyses of strategies R_c, R_{nc}, D_f, M_c, A_t, and M_{nc}

	X	R_c	R_{nc}	D_f	M_c	A_t	M_{nc}
Minimum Value	0.00	0.28	0.00	0.00	0.33	0.00	0.00
Maximum Value	600	1.00	0.33	0.56	1.00	0.33	0.33
Average Value	294.7	0.96	0.00	0.03	0.99	0.00	0.00
Medium Value	294.5	1.00	0.00	0.00	1.00	0.00	0.00
Mode	0.00	1.00	0.00	0.00	0.33	0.00	0.00
Deviation	177.1	0.13	0.02	0.11	0.06	0.03	0.03
Range	600.0	0.72	0.33	0.56	0.67	0.33	0.33

From the statistical analyses shown in Tables 3 and 4, we used these experiments in 0/300/116.3/95.03/0/94.09/300 rows and 0/600/294.7/294.5/0/177.1/600 rows to obtain more meaningful data. These data are presented below in Figures 6 and 7, respectively.

From the results in Figure 6, when all the values of the nodes' defender strategies D_f were zero, all nodes of the wireless sensors network chose strategy M_{nc}. In Figure 7, the range increased up to 600, and D_f was able to resist small variations; the nodes of the wireless sensors network then chose strategy M_c. The average medium values in Figure 6 are 0 and 0.4, whereas they are 0.03 and 0 in Figure 7. The results of the average medium values in each case were not smooth and steady. These conclusions are verified in Figures 4 and 5, respectively. Propositions 1 and 2 were also verified.

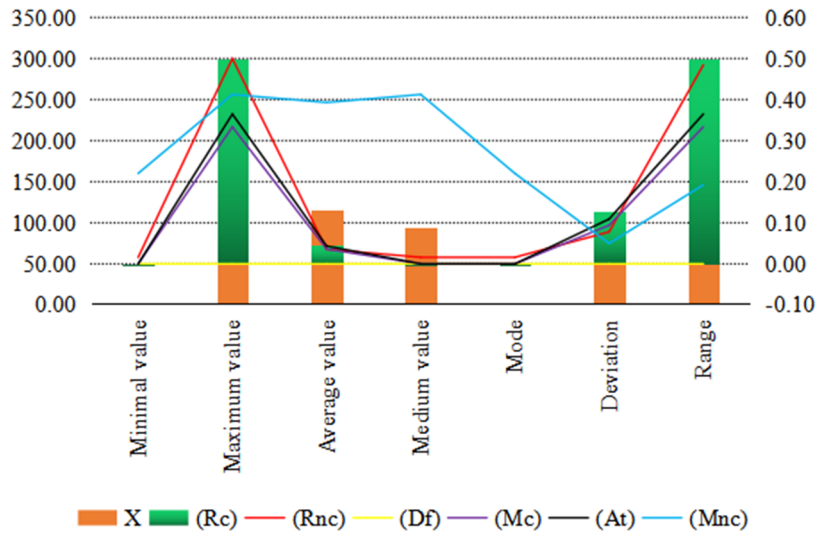

Figure 6. Analyses of rational nodes without defender strategies.

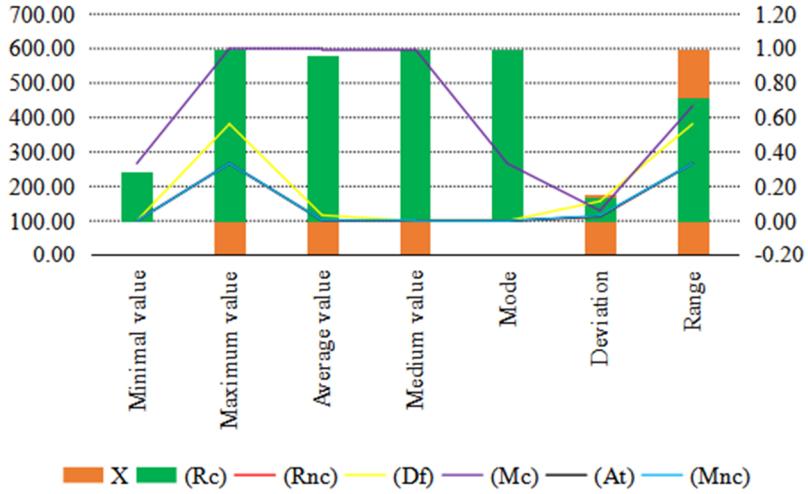

Figure 7. Analyses half of rational nodes when choosing defender strategies.

4.2. All Rational Nodes Choosing Defense

For the simulation results for the state of the wireless sensor population, we considered that all the rational nodes choosing defense were divided into two kinds of defensive strategies: (1) the all rational nodes strategy, which is zero; and (2) the all rational nodes strategy, which is not zero. The results when $(x, y) = (x_1, x_2, x_3, y_1, y_2, y_3) = (0, 0, 1, 0.001, 0.5, 0.49)$ are shown in Figure 8.

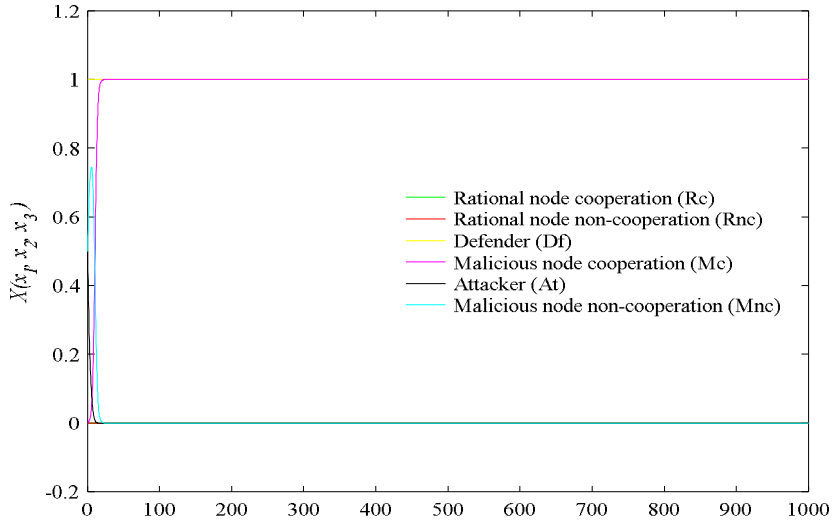

Figure 8. All rational nodes choosing defender strategies and $R_c = 0$.

In Figure 8, to determine the simulation results, wide area wireless sensor networks appeared, the range increased up to 1000, and the rational nodes strategy was zero. The simulation results showed that when all the rational nodes in a wireless sensor network choose a defensive strategy in the system after a period of time for evolution, the malicious node chose the cooperative strategy. In this state, as long as little variation exists in the node, the population system will choose strategy M_c, but when the medium average value of strategies M_c, A_t, and M_{nc} are not at equilibrium, the model always chose strategy D_f, and the defender cannot become zero for low power consumption. Each node is not guaranteed to achieve the best benefit. Thus, the stability and reliability of the network is improved. The results of the statistical analysis of the data in Figure 8 are provided in Table 5.

Table 5. Statistical analyses of strategies R_c, R_{nc}, D_f, M_c, A_t, and M_{nc}.

	X	R_c	R_{nc}	D_f	M_c	A_t	M_{nc}
Minimum Value	0.00	0.00	0.00	1.00	0.00	0.00	0.00
Maximum Value	1000	0.00	0.00	1.00	1.00	0.50	0.75
Average Value	482.7	0.00	0.00	1.00	0.97	0.01	0.02
Medium Value	481.4	0.00	0.00	1.00	1.00	0.00	0.00
Mode	0.00	0.00	0.00	1.00	0.00	0.00	0.00
Deviation	298.5	0.00	0.00	0.00	0.14	0.04	0.10
Range	1000	0.00	0.00	0.00	1.00	0.50	0.75

From the statistical analyses shown in Table 5, the range increased up to 1000. We used these experiments in the 0/1000/482.7/481.4/0/298.5/1000 rows to gain more meaningful data, which are presented in Figure 9.

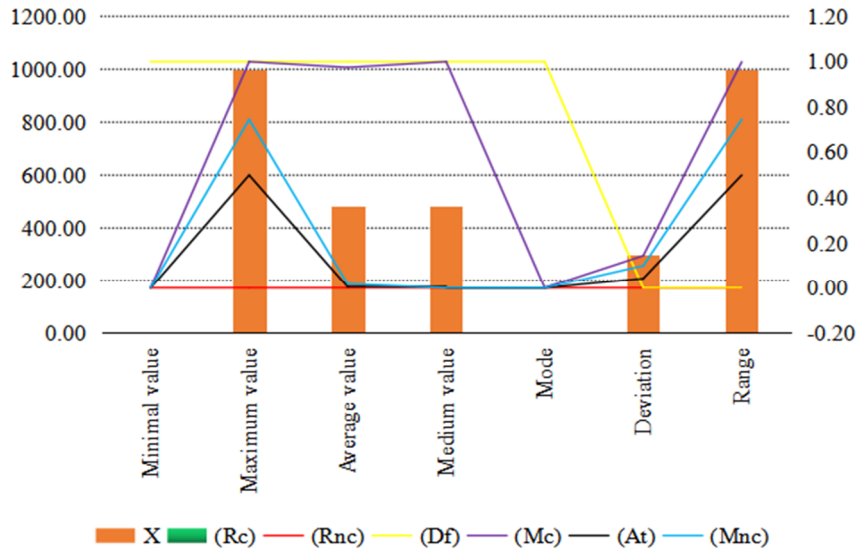

Figure 9. Analyses of when all rational nodes choose defender strategies.

Figure 9 shows that the range increased up to 1000, and when all the values of the nodes' choosing defender strategies D_f were nonzero, all the rational nodes of the wireless sensors network chose strategy M_c. Also, when the deviation X = 298.5 occurred, the result of that deviation was zero in the D_f nodes strategy. However, when the average medium values in the node strategy M_c were 0.97 and 1, the average medium values in each case were smooth and steady, but each node did not achieve the best benefit. This conclusion is verified in Figure 8; Proposition 3 was also verified. The results when $(x, y) = (x_1, x_2, x_3, y_1, y_2, y_3) = (0.001, 0, 1, 0.001, 0.5, 0.49)$ are shown in Figure 10.

In Figure 10, to determine the simulation results, wide area wireless sensor networks appeared, the range increased up to 10,000, and the rational nodes strategy was nonzero. In the system, after allowing a period of time for evolution to elapse, the malicious node chose the cooperative strategy to maximize its interests because the rational node chose defensive measures. Thus, the malicious node can multiply inorganically, and the malicious node will always choose the cooperative strategy. The final network converges into the equilibrium state of malicious node cooperation and all the rational nodes choose defense, so the wireless sensor network can effectively avoid the attacker behavior of the malicious node. In this state, as long as little variation exists in the node, the population system will choose strategy R_c. When the medium average value of strategies M_c, A_t, and M_{nc} are at equilibrium, the strategy D_f becomes to zero for low power consumption. The final network converged to the equilibrium state of the malicious node cooperation and rational node cooperation,

thus improving the stability and reliability of the network. The statistical analyses of all these data is shown in Figure 10, and the statistics are provided in Table 6.

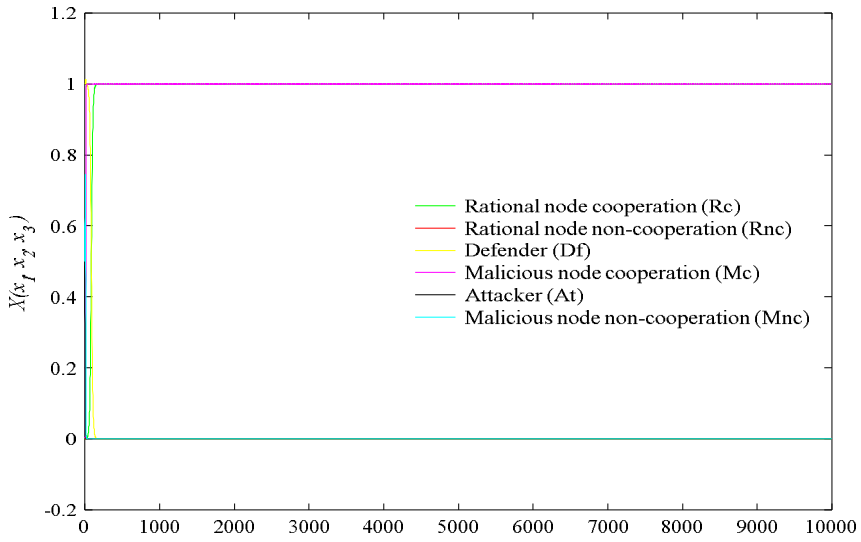

Figure 10. All rational nodes choosing defender strategies and $R_c \neq 0$.

Table 6. Statistical analyses of strategies R_c, R_{nc}, D_f, M_c, A_t

	X	R_c	R_{nc}	D_f	M_c	A_t	M_{nc}
Minimum Value	0.00	0.00	0.00	9.881×10^{-3}	0.00	0.00	0.00
Maximum Value	10,000	1.00	0.00	1.01	1.00	0.50	0.74
Average Value	4952.0	0.98	0.00	0.02	1.00	0.00	0.00
Medium Value	4951.0	1.00	0.00	0.00	1.00	0.00	0.00
Mode	0.00	1.00	0.00	9.881×10^{-3}	0.00	0.00	0.00
Deviation	2917.0	0.13	0.00	0.13	0.06	0.02	0.04
Range	10,000	1.00	0.00	1.01	1.00	0.50	0.74

Using the statistical analyses shown in Table 6, the range increased up to 10,000. We used these experiments in the 0/10,000/4952/4951/0/2917/10,000 rows to gather more meaningful data, which are presented in Figure 11.

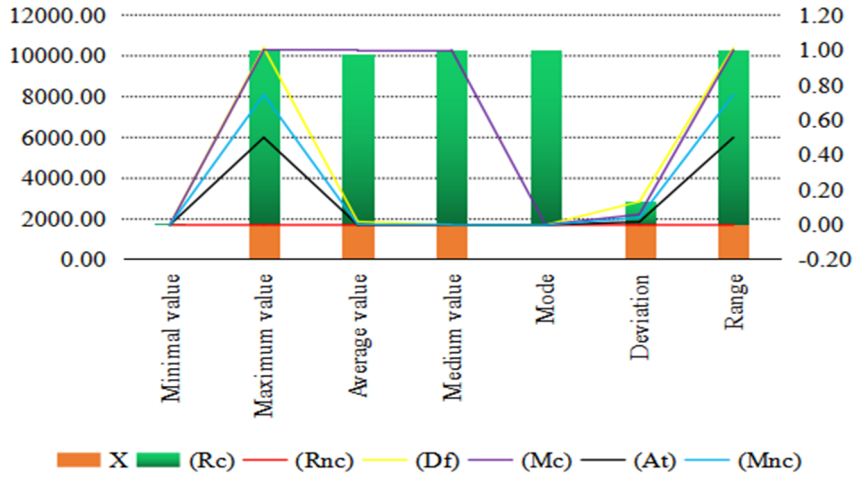

Figure 11. Analyses all of rational nodes when choosing defender strategies.

In Figure 11, the range increased up to 10,000, and when all the values of the node defender strategy D_f and rational nodes strategy were nonzero, all nodes of the wireless sensors network chose strategies M_c and R_c. When the deviation X = 2917 in Figure 11 occurred, the result of that deviation was zero in the nodes strategy M_c. The average medium values in the node strategy M_c in each case were one, and in the nodes strategies A_t and M_{nc}, they were zero. The results of the average medium values in each case were both smooth and steady. This conclusion is verified in Figure 10; Proposition 4 is also verified.

5. Discussion

In Figure 11, when all the rational nodes chose defense, the deviation value was zero and the average medium defensive strategy had the same value, and the variation probabilities and composition of sensor nodes were fewer in the wireless sensor networks. The population system then converged and used defensive strategies against the malicious node in order to oblige it to cooperate. Compared with previous studies [12–14], in which the system performance could not guarantee that each node can achieve the best benefit, the node is still likely to appear to exhibit selfish behavior. Also, the system is unable to complete an accurate description of the dynamic evolution of the node strategy, preventing the determination of 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 reports in that we added a new defensive strategy between the rational nodes of the WSN, and these rational nodes can be cooperative by then forwarding defense packets efficiently and resisting small variations.

Compared to the previous literature [19–21], in which game theory and dynamic programming were used to model a multiple-period, attacker–defender, resource allocation, and signaling game with incomplete information, attacks are deflected to an asset or deferred altogether with our method, or the assets are made less valuable to the attacker. As a result, we generally recommend that defensive investments be disclosed. However, disclosure cannot always be optimal in practice, because otherwise there is no role for secrecy and/or deception in defensive investments.

Our research results indicated that our approach is faster and can be optimal in practice, with lower power consumption and fewer deviations. Compared with Al-Jaoufi et al. [15], the disadvantages are outlined in Table 7 below.

Table 7. Compared with Al-Jaoufi et al. [15].

	Al-Jaoufi et al. [15]	**This Paper**
Number of Strategies	3	Increased up to 6
Rang Number	1000	Increased up to 10,000
Equilibrium State	The average medium values in the non-cooperative nodes strategy were 0.003944 and 4.44×10^{-58}, and nodes strategy conditional cooperative were 0.7485 and 0.7529.	The average medium values in malicious node cooperation for each case were only 1, and in the attacker nodes strategies and malicious node non-cooperation were each only zero.
Power Consumption	Higher power consumption because the model always chooses the conditional cooperative nodes strategy.	Lower power consumption, only after malicious nodes cooperation, attacker, and malicious nodes non-cooperation equilibrium state, the defender strategies are close to zero.
Deviations	When the deviation X = 294.7, the result of the deviation was small in the non-cooperative nodes, given that the deviation value was 0.031.	When the deviation X = 2917 in Figure 11 occurred, the result of that deviation was zero in the attacker nodes strategy, which is a better result given that the deviation value was 0.02.

Our analyses were the best among all recent reports, indicating that the performance of the WSNs could be enhanced due to its stability and reliability. The deviations were 0.13, 0.06, and 0.02 in rational

node cooperation, malicious node cooperation, and attacker nodes, respectively, as shown in Figure 11. Thus, using our method the time requirement was much shorter with very low power consumption because the deviation was very small.

6. Conclusions

The microscopic behavior of malicious nodes in wireless sensor networks was studied for this paper and corresponding strategies were offered. A defense strategy based on evolutionary game theory was proposed and a model was developed. In particular, Section 4.2 shows that malicious node cooperation (M_c) can be an equilibrium strategy when the average medium values have the same value, which was only one, and the attacker nodes strategies (A_t) and malicious node non-cooperation (M_{nc}) values were only zero. In those cases, the final result required low power consumption. Only after malicious node cooperation (M_c), and attacker (A_t) and malicious node non-cooperation (M_{nc}) equilibrium states, were the defender (D_f) strategies close to zero.

The simulation results show that all the malicious nodes in the network chose to cooperate, so that the network remains in good working condition, meaning that the stability and reliability of the wireless sensor networks improved.

Author Contributions: M.A.A.A.-J. has conceived, designed, performed the experiments, and wrote this paper; Y.L. gave valuable suggestions; Z.Z. organized the paper. All authors revised the paper.

Acknowledgments: The authors would like to thank the editors and reviewers for their insightful comments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Qiu, Y.; Chen, Z.; Xu, L. Active defense model of wireless sensor networks based on evolutionary game theory. In Proceedings of the Wireless Communications Networking and Mobile Computing (WiCOM), Chengdu, China, 23–25 September 2010; pp. 23–25.
2. Chen, Z.; Qiu, Y.; Liu, J.; Xu, L. Incentive mechanism for selfish nodes in wireless sensor networks based on evolutionary-game. *Comput. Math. Appl.* **2011**, *62*, 3378–3388. [CrossRef]
3. Hu, Y.; Li, R. Adaptive active defense mechanism in wireless sensor networks. In Proceedings of the International-Symposium on Instrumentation and Measurement, Sensor Network and Automation, Toronto, ON, Canada, 23–24 December 2013; pp. 8–13.
4. El-Azouzi, R.; De Pellegrini, F.; Kamble, V. Evolutionary forwarding games in delay tolerant networks. In Proceedings of the Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), Avignon, France, 31 May–4 June 2010; pp. 76–84.
5. Wu, D.; Cao, J.; Ling, Y.; Liu, J.; Sun, L. Routing algorithm based on multi-community evolutionary game for VANET. *J. Netw.* **2012**, *7*, 1106–1115. [CrossRef]
6. Wu, T.Y.; Lee, W.T.; Guizani, N.; Wang, T.M. Incentive mechanism for P2P file sharing based on social network and game theory. *J. Netw. Comput. Appl.* **2014**, *41*, 47–55. [CrossRef]
7. Zuo, F.; Zhang, W. An evolutionary game-based mechanism for routing P2P network flow among selfish peers. *J. Netw.* **2014**, *9*, 10–17. [CrossRef]
8. Feng, T.; Tai, S.; Sun, C.; Man, Q. Study on Cooperative Mechanism of Prefabricated Producers Based on Evolutionary Game Theory. *Math. Probl. Eng.* **2017**, *2017*, 1–6. [CrossRef]
9. Esposito, C.; Ficco, M.; Palmieri, F.; Castiglione, A. Smart Cloud Storage Service Selection Based on Fuzzy Logic, Theory of Evidence and Game Theory. *IEEE Trans. Comput.* **2016**, *65*, 2348–2362. [CrossRef]
10. Chen, Z.; Qiao, C.; Qiu, Y.; Xu, L.; Wu, W. Dynamics stability in wireless sensor networks active defense model. *J. Comput. Syst. Sci.* **2014**, *80*, 1534–1548. [CrossRef]
11. Bendjima, M.; Feham, M. Architecture of an MAS-Based Intelligent Communication in a WSN. *Int. J. Distrib. Sens. Netw.* **2015**, *2015*, 1–12. [CrossRef]
12. AlSkaif, T.; Zapata, M.G.; Bellalta, B. Game theory for energy efficiency in wireless sensor networks: Latest trends. *J. Netw. Comput. Appl.* **2015**, *54*, 33–61. [CrossRef]

13. Guo, H.; Wang, X.; Cheng, H.; Huang, M. A routing defense mechanism using evolutionary game theory for Delay Tolerant Networks. *Appl. Soft Comput.* **2016**, *38*, 469–476. [CrossRef]
14. Li, J.; Hu, H.P.; Ke, Q.; Xiong, N. A Novel Topology Link-Controlling Approach for Active Defense of a Node in a Network. *Sensors* **2017**, *17*, 553. [CrossRef] [PubMed]
15. Al-Jaoufi, M.A.A.; Liu, Y.; Zhang, Z.; Uden, L. Study on Selfish Node Incentive Mechanism with a Forward Game Node in Wireless Sensor Networks. *Int. J. Antennas Propag.* **2017**, *12*, 1–13. [CrossRef]
16. Standard Deviation. STANDS4 LLC, 2018. Available online: http://www.symbols.com/symbol/standard-deviation (accessed on 13 March 2018).
17. Sohrabi, K.; Gao, J.; Ailawadhi, V.; Pottie, G.J. Protocols for self-organization of a wireless sensor-network. *IEEE Pers. Commun. Mag.* **2000**, *7*, 16–27. [CrossRef]
18. Taylor, P.D.; Jonker, L.B. Evolutionarily stable strategies and game dynamics. *Math. Biosci.* **2010**, *40*, 145–156. [CrossRef]
19. Zhuang, J.; Bier, V.M.; Alagoz, O. Modeling Secrecy and Deception in a Multiple-period Attacker-Defender Signaling Game. *Eur. J. Oper. Res.* **2010**, *203*, 409–418. [CrossRef]
20. Jose, V.R.R.; Zhuang, J. Technology adoption, accumulation, and competition in multi-period attacker-defender games. *Mil. Oper. Res.* **2013**, *18*, 33–47. [CrossRef]
21. Shan, X.; Zhuang, J. Reliability Engineering and System Safety, 2017. Available online: http://dx.doi.org/10.1016/j.ress.2017.03.022 (accessed on 1 April 2018).