ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 1, 2024

Dynamics stability in wireless sensor networks active defensemodel

Prof. D. Raja, Mr. S. Sugavanam, Mrs. K. Janani, Mrs. M. Indra Priya

Professor [1], Associate Professor [2,4], Assistant Professor [3]

raja.d@actechnology.in, sugavanam.s@actechnology.in, kjanani@actechnology.in, indrapriya.m@actechnology.in

Department of CS & BS, Arjun College of Technology, Thamaraikulam, Coimbatore-Pollachi Highway, Coimbatore, Tamilnadu-642 120

Abstract:

Because they are often placed in an open setting, wireless sensor networks—that are extensively used in transportation, industry, and the military—are susceptible to many types of assaults. This paper presents an evolutionary game-theory-based proactive defence model for WSNs, with an emphasis on the node's limited capacity to learn the evolution of rationality from various attacker strategies and execute dynamic strategy adjustments to attain optimal defence. By using this method, we were able to significantly reduce costs (such as energy usage and equipment waste) while simultaneously increasing the nodes' useful life. The whole wireless sensor network may be efficiently deployed by using the suggested approach.

1. Introduction

1.1. Wireless sensor network

A group of interconnected wireless sensor nodes is called a wireless sensor network [1]. A basestation, sometimes called a "gateway," is the central node in a wireless sensor network (WSN) and it communicates with the individual nodes in the network over radio connections. At the wireless sensor node, data is compressed and gathered before being sent directly to the gateway or, if necessary, via additional wireless sensor nodes to the gateway. The gateway link then presents the sent data to the system [2]. The perfect wireless sensor would be part of a network, have a low power consumption, be intelligent and software configurable, gather data quickly, be accurate and dependable over time, be inexpensive to buy and set up, and need little in the way of maintenance. We are really excited about the limitless possibilities of this new technology in a wide variety of fields, such as smart environments, crisis management, healthcare, transportation, entertainment, and the military [3].

Deploying wireless sensor networks in an open, unattended, and potentially hostile environment is not uncommon. Sensor nodes are more susceptible to a wide range of possible assaults from hostile actors due to their inherent power and memory limits [4–7]. Selective forwarding, sinkhole attacks, Sybil attacks, and bogus data injection to disrupt data aggregation are some of the security concerns that wireless sensor networks have been confronting recently [8–12]. When it comes to security,

however, almost everything that's now available is passive; for example, wireless sensor networks only react appropriately when attacked.

after the discovery of assaults. Because of their limited computational and energy resources, wireless sensor networks may not be able to react quickly enough to prevent an attacker from destroying their systems.

1.2. Game theory

Game theory is a branch of applied mathematics that is used in the social sciences, most notably in economics, as well as in the fields of biochemistry, ecology, evolutionary biology, computer science, philosophy, politics, and international relations. The goal of game theory is to provide a mathematical model of how people act in strategic settings, or games, where their own decision-making outcomes are contingent on those of their opponents. The foundation of traditional game theory is the idea that players should be completely rational while solving issues; this implies that players should be self-aware, capable of analytical thinking, have sufficient memory capacity, and be meticulous [13]. Players, according to conventional game theory, should never make a mistake and should always assume that their opponents will do the same.
The high expectations of complete reason in a gaming context make it difficult for players to apply game theory in practice. In the 1900s, Weibull put out the idea of evolutionary game theory in a methodical way. This theory offers a player with limited rationality and the dynamics of the game process, as opposed to the completely rational assumption of classical game theory. In a game with bounded rationality, the player has partial knowledge of the game's state (such as the payout or action strategies) and no idea of the game's overall state (such as these things) [14–16]. No player can hope to discover the perfect strategy after a single game; instead, they must devote many hours to studying the game and practicing their imitations.
A wireless sensor network is defined by its huge number of nodes and the dynamic topology caused by the frequent joining and departing of regular nodes; so, the bounded rationality assumption is applicable to such a network. In reality, sensors can only provide you a partial picture of the network's condition. Obtaining and maintaining the state of the whole network is impractical and counterproductive for resource-constrained wireless sensor networks due to the high amounts of energy and storage used by nodes.

1.3. Wireless sensor network using evolutionary game theory

The article suggests a paradigm for active defence of wireless sensor networks based on evolutionary game theory. As a result of dynamic evolution, nodes may actively and dynamically adapt their defensive measures to deal with various types of attackers. In order to learn, imitate, and simultaneously alter their methods, the nodes must stay in the game until they discover the optimal strategy that suits their interests and needs. Thus, it may save energy and other resources to increase the overall efficiency of wireless sensor networks by extending the life cycle time of network nodes. Here is how the remainder of this paper is structured. We provide the most recent use of game theory to the topic of security for WSNs in Section 2. Section 3 lays forth the framework for wireless sensor network security as an attack-defend game. Section 4 examines the security of

wireless sensor networks via the lens of evolutionary game theory. We provide some numerical explorations in Section 5. Part 6 provides the results and recommendations for further research.

2. Related works

3. Numerous studies have addressed the difficulties associated with wireless sensor network security, with a particular focus on the application of game theory to this increasingly popular area of study. The authors of [17] offered a model for active defence in wireless sensor networks, while those of [18] suggested a model for defensive network security assessment charts, portrayed the attacker and defender in a non-cooperative game, and, finally, used this information to construct a proactive evaluation and active defence model for network security by choosing the best algorithm. For the purpose of active defence and security evaluation of network information systems, many models have been given in [19], such as the defence graph model, the attack-defense taxonomy and cost quantitative technique, and the attack-defense game model. In order to avoid denial of service attacks, the authors of [20] presented two new strategies and reframed the attack-defense issue as a nonzero-sum, non-cooperative game involving a wireless sensor and an attacker. In [21], the study is expanded upon with an emphasis on evaluating the qualities of security enforcement systems that use auction theory to ward against denial-of-service attacks in WSNs. By using game theory to the analysis of commercial information security, the author of [22] finds an equilibrium that takes into account the penalty parameters of both the attacker and the defender.

4. A game theory model of security

Within the framework of a game theory model, we provide a quantitative account of a social scenario whereby several individuals, or players, engage in either cooperative or competitive behaviour. An issue known as collusion might arise when there are more than two participants in the system, since some of the players may conspire with each other. There could be a single step for each participant or several steps in a sequential game. One may encounter a competitive circumstance only once, or they may occur repeatedly. All participants may have complete or partial knowledge of the rules of engagement and the rewards.

Table 1
The attack–defense payoff matrix.

Defender	Attacker	
	Attack	No attack
Deploy	$(R_D - C_D - P_1L, P_1R_A - C_A)$	$(R_D - C_D, 0)$
Not to deploy	$(-P_2L, P_2R_A - C_A)$	$(R_D, 0)$

The players, the strategy spaces, and the reward function are the three main components of a game model. This is the game model expressed in terms of the characteristics of WSNs.
The attackers here are assumed to be nodes with the goal of stealing resources from other nodes in order to increase their own lifespan. Having said that, they aren't evil or self-centred in any way. We have also included a parameter CA to represent their cost to attack in the proposed model. The likelihood of a successful assault increases when a node zeroes in on a single target. So, the likelihood of a successful assault is the only thing that matters when deciding whether an attack is one-to-one or one-to-many based on the number of targets.

4.1. Players

5. There are two groups of players in the game, each with their own unique set of skills and abilities related to the security of wireless sensor networks. One group is the Defenders, who are good at defending the network, and the other group is the Attackers, who are good at launching attacks. Players choose between two roles in the game: defender and attacker.

5.1. Strategy space

Definition 3.1. The probability distribution across a player's pure strategy options, whether some or all of them are used, is called a mixed strategy.

Just like an attacker, a wireless sensor node will evaluate its own resources (power, data transfer rate, and storage space) before deciding whether to implement the security measure. Even more crucially, a hybrid approach that allows the defence to cover ground while the attacker avoids it increases the likelihood of a successful return.

individuals involved. Defence strategy set = SD (deploy security measures, not to deploy security measures) and Attack strategy set = S A (attack, not to attack) are the two sets of strategies in play here.

Payoff function

We say that UD is the Defender's payment function and U A is the Attacker's payment function.

Definition 3.2. The anticipated payoff of a mixed strategy X ∈ Θ is n, given that there exists a pure strategy S = {S1, S2, •••, Sn}.

The function ui(x) might be written as X(s) πi(x) (1).

With k=1,

This is where the i strategy, the k mixed strategy, and the rate of employing this approach are represented by i, k, and X(s), respectively.

The anticipated payoff of this technique is denoted by πi(x) and X(s) is the rate at which it is used.

The following notations are used in this research in accordance with the features of wireless sensor networks.

A player may earn in-game currency known as RD (Reward of Defender) when they successfully transmit data packets. Earnings go up when the importance of the sent data goes down, and vice versa.

Defender's deployment of security measures may result in energy, bandwidth, and other resource consumption, which is represented as CD (Cost of Defender). Because of this, we will pretend that RD is greater than CD.

The compensation obtained from the Attacker via the attack, which may take the form of routing information, documents, or other resources, is denoted as R A (Reward of Attacker).

The cost of an attack, or CA, is the amount that the attacker pays to launch an attack, which may need the use of resources (both physical and digital) and may result in legal repercussions.

When assaulted, the defender is lost, denoted by L.

If the defence decides to implement security measures, the attacker has a 1 in P (Probability 1) chance of successfully launching an attack.

P 2 (Probability 2) is the chance that the attacker will succeed in their attack if the defence does not use any security measures.

The attack-defense payoff matrix is shown in Table 1 and is based on the parameters and assumptions mentioned before.

1.Analysis of the active defense

1.1. Evolutionary stable strategy

Important ideas in evolutionary game theory include the replicator dynamic and evolutionary stable strategy (ESS). Evolutionary stable strategies emphasise the significance of mutation, while the replicator dynamics model links selection with the idea that a subpopulation expands (contracts) when it employs above-average (below-average) strategies [19]. We will assume that the majority of sensor nodes in the initial population follow strategy x, whereas a small subset of nodes ε (0, 1) will follow approach y. Therefore, the odds of an opponent playing the incumbent strategy x and the mutant strategy y, respectively, are 1 ε and ε, when an individual is chosen to play the game. Our tagged person's anticipated payout upon encountering another individual who implements strategy y is defined as u(x, y). This means that in order for a strategy x to be considered evolutionarily stable, its reward must be greater than that of strategy y.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN2454-9940
www.ijasem.org
Vol 18, Issue 1, 2024

$$u\ x, \varepsilon y + (1-\varepsilon)x\ > u\ y, \varepsilon y + (1-\varepsilon)x \quad (2)$$

Definition 4.1. A strategy x is said to be evolutionary stable if for every strategy $y\ /= x$ there exists some $\sigma \in (0,\ 1)$ such that inequality (2) holds for all $\varepsilon \in (0, \sigma)$ [23].

1.2. *Replicator dynamics*

Assumption of innate, pure or mixed strategies by individuals is essential to evolutionary stability. On the other hand, the standard model of replicator dynamics assumes that people can only be taught pure tactics [23]. Based on their consideration of a large population of people trained to the same set of pure strategies K, Taylor and Jonker developed a dynamic selection method called replicator dynamics. Let p(t) = (i∈K) pi(t) represent the whole population, and let p(t) be the number of individuals now programmed to pure strategy i ∈ K. Next, the state of the population is represented by the vector x(t) = (xi(t), •••, xk(t)), where xi(t) represents a portion of the population. If the population is in state x and the average payout is u(x, x), then the anticipated payoff employing pure strategy i is u(si, x). As a result, the replicator dynamic equation =

$$\frac{dx_i}{dt} = u(s_i, x) - u(x, x)\ x_i. \quad (3)$$

It is clear that if strategy i results in a higher payoff than the average level, the population share using i will grow, and vice versa.

1.3. *Analysis*

Take the defensive population as a whole and assume that X% of players use the security measure technique, with 1 X being the percentage of players who do not. We also assume that Y represents the fraction of the attacker population that uses the attack technique, and that 1 Y represents the fraction of the attacker population that does not. Take into consideration that X and Y do not have static values but rather fluctuate over time. The players constantly adapt their tactics by watching other players based on the payout, as we analyse problems on a limited rational framework. Dynamic adjustment is an ongoing process of learning and growth.

1.3.1. *ESS of defenders*

· The expected payoff obtained by employing security measure strategy:

$$E(UD) = Y(R_D - C_D - P_1 L) + (1-Y)(R_D - C_D)$$
$$= R_D - P_1 LY - C_D \quad (4)$$

· The expected payoff obtained by employing no security measure strategy:

$$E(UND) = Y(-P_2 L) + (1-Y)R_D$$
$$= R_D - Y P_2 L - R_D Y \quad (5)$$

· The average expected payoff of the population of defender:

$$E(D) = XE(UD) + (1-X)E(UND)$$
$$= X(R_D - P_1 LY - C_D) + (1-X)(R_D - Y P_2 L - R_D Y) \quad (6)$$

According to Eq. (3), we can get the equation of replicator dynamics for the defender:

$$\frac{dX}{dt} = X\ E(U_D) - E(D)$$
$$= X(1-X)(R_D Y + Y P_2 L - Y P_1 L - C_D) \quad (7)$$

1.3.2. *ESS of attackers*

· The expected payoff obtained by employing attack strategy:

$$E(U_A) = X(P_1 R_A - C_A) + (1-X)(P_2 R_A - C_A)$$
$$= X R_A (P_1 - P_2) + P_2 R_A - C_A \quad (8)$$

· The expected payoff obtained by employing no attack strategy:

$$E(U_{NA}) = 0 \quad (9)$$

· The average expected payoff of the population of attacker:

$$E(A) = Y E(U_A) + (1-Y) E(U_{NA})$$
$$= Y\ X R_A (P_1 - P_2) + P_2 R_A - C_A \quad (10)$$

According to Eq. (2), the equation of replicator dynamics for the attacker can be written as

$$\frac{dY}{dt} = Y\ E(U_A) - E(A)$$
$$= Y(1-Y)\ X R_A (P_1 - P_2) + P_2 R_A - C_A \quad (11)$$

1.4. *Analysis of active defense*

The replicator dynamics system of the attackers and defenders is formed by formulae (7) and (11) according to the preceding study of the evolutionary game. Hence, we may write (X(t), Y(t)) as 0 and 1 and 0 and 1 for any starting points (X(0), Y(0)) that are positive integers. An evolutionary game's dual mix-strategy (X (1 X), Y (1 Y)) corresponds to any point (X, Y) on the replicator dynamics solution curve or attack-defense system. E1(0, 0), E2(1, 0), E3(0, 1), and E4(1, 1) are the five obvious local equilibrium points in a dynamic copy system.

$$0 < \frac{C_A - P_2 R_A}{P_1 R_A - P_2 R_A} < 1$$

and

$$0 < \frac{C_D}{R_D + P_2 L - P_1 L} < 1,$$

$E_5\left(\frac{C_A - P_2 R_A}{P_1 R_A - P_2 R_A}, \frac{C_D}{R_D + P_2 L - P_1 L}\right)$ is an equilibrium point too. Actually, we could know that $0 < \frac{C_D}{R_D + P_2 L - P_1 L} < 1$. $R_D > C_D$ is the

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN2454-9940
www.ijasem.org
Vol 18, Issue 1, 2024

$R_D + P_2$ $L - P$ direct reason for defender to employ the security strategy. Obviously $P_1 L$ P_D $P_2 L - P_1 L$ $> P_1$, so $0 <$ R $+$ CD < 1 is always true. These points of equilibrium represent a defender-attacker evolution game. The stability of the defender-attacker equilibrium is dependent on the comparison of the results of the strategy choices in the game. Even after reaching the equilibrium method, the person continues to fluctuate continually. Here we will examine the evolution game of attacker-defender separately before combining our findings.

(1) Evolutionary stability of the defender.

In replicator dynamics, the defender's equation (6) states that if dX = 0, three possible values may be obtained: X = 0, X = 1, and Y = R + CD. It is only a strategy that can tolerate minute deviations that may be considered an evolutionarily stable approach, according to the notion of evolutionary stability. According to the mathematical "Stability Theory" of differential equations, dX must be smaller than 0 if the deviation causes X to be greater than ESS.

In contrast, dX is considered negative if the departure causes X to be less than ESS.

needs to be greater than zero. During the

The evolutionary stable strategy (ESS) of an evolutionary game is located at the point where the replicator dynamics curve intersects the horizontal axis, with a negative slope of the tangent. This junction is shown in the diagram of the replicator dynamics equation.

The vector field in the open domain must be continuously differentiable for the Liouville formula to be relevant to autonomous differential equations. The degree of divergence at any given place is defined as the point where the trace of

Fig. 1. The phase diagram of replicator dynamics when $Y >$ R $+$ C_D .

matrix Jacobs. Particularly, vector field whose divergence is zero is called no divergence. It could be shown that this feature means that the corresponding flow maintain its volume. Liouville formula shows that the time-derivative of the volume of A exists and equals to the integrals of divergency degree of A.

Intuitively, we can imagine that the asymptotically stable state of vector field whose divergence degree is zero is not tight. If x belongs to X is asymptotically stable, then there is gradually shrinking to the point of a neighborhood of x, which means that as time tends to infinity, the volume of the neighborhood shrinks to zero.

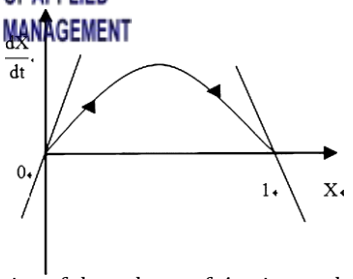
$$div\ \underline{\underline{\phi}}(x) \quad \sum_{i=1}^{k} \frac{\partial\ \underline{\underline{i}}}{\partial x_i}(x) \qquad (12)$$

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 1, 2024



Liouville formula shows that the time-derivative of the volume of A exists and equals to the integrals of divergency degree of A.

$$\frac{dvol[A(t)]}{dt} = \int div\ \boldsymbol{\phi}(x)\ dx \tag{13}$$

Theorem 4.2. *The asymptotically stable state of vector field whose divergence is non-negative is not tight.*

Proof. Here is the formulated version: It is not tight that the asymptotically stable state of the vector field is ϕ: X → R is continuously differentiable (div[ϕ(x)] > 0 is always true), given that X ⊂ Rk is an open domain.
Pretend that the state of % /= A ⊂ X that is asymptotically stable is compact. In this case, the volume of A is an element of R+, and for any xo in the neighbourhood A of X, there is a closure B such that the formulae limt→∞ε(t, xo) → A are true without exception. For any xo that is a member of B, define B(t) as the set of all possible values of ξ(t, xo). For any ε > 0, we can demonstrate that the Hausdorff distance d(x, A)< ε is always true if and only if there exists Tε. Then, as limt approaches infinity, the volume of B(t) equals the volume of A. Voltage[A] < Voltage[B(0)], obviously, < 0. It is not always true for every x ∈ X that div[ϕ(x)] > 0, as stated in Eq. (13).

We take it as read that there is no finite duration during which the set A of distances from any location x ∈ B(t) may remain arbitrarily small. Then, for any value of k, the inequality d[ξ(tk, xk), A] ≥ ε will hold since ε is greater than zero and the time series tk is expanding indefinitely. A convergent subsequence is included in the sequence (xk) as per the Bolzano-Weierstrass theorem. Assuming xk → x∏ for every x∏ ∈ B is a general assumption.

Assuming A is Lyapunov stable, the statement d(ξ(t, xo), A) < ε ∀t ≤ 0 is always valid for any xo in the neighbourhood C of A. A neighbourhood D of A is defined as D ⊂ C and for any integer t∗ that is greater than or equal to 0 and less than or equal to mint, ξ(t, x∗) is a neighbourhood of D. In order for ξ to be continuous, there must be a neighbourhood E such that for every t■, xo ∈ E, ξ(t■, xo) ∈ C. Despite this, the premise [23] is contradicted since tk > t∏ and xk ∈ E are valid for any sufficiently high values of k. Consequently, d(ξ(tk, xk), A)< ε.

It is clear that ESS values are Y dependent from the study given above. In most instances, we encounter:

Theorem 4.3. *When* $Y > {}_{R} + {}^{CD}$ *, only* $X = 1$ *is the evolutionary stable strategy of evolutionary game of the defender, namely all*

the defenders prefer to the deployment security measure strategy.

Proof. From In Figure 1, which shows the phase diagram of the replicator dynamics equation for the defender, we can see that the horizontal axis and the replicator dynamics curve connect at two locations, X = 0 and X = 1. X = 1, being the sole evolutionary stable strategy, is preferred by all defenders over the deployment security measure approach, since the slope of the tangent at the intersection of X = 0 is positive and negative.

Theorem 4.4. *When* Y *,* *there is no evolutionary stable strategy for the defender.*

$+ {}^{CD}$

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 1, 2024

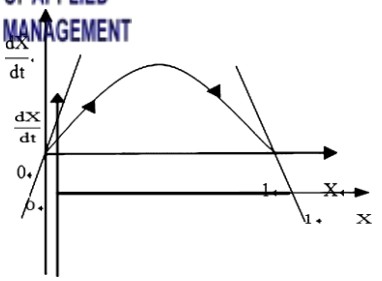


Fig. 2. The phase diagram of replicator dynamics when $Y = R\frac{C_D}{D + P_2L - P_1L}$.

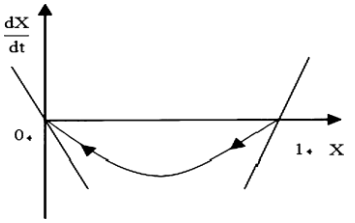


Fig. 3. The phase diagram of replicator dynamics when $Y < {}_{R} + {}^{C_D}$.

Proof. The replicator dynamics curve and the horizontal axis overlap each other, as shown in the phase diagram of replicator dynamics for defence (Fig. 2). There is no stable evolutionary strategy in this scenario because X cannot recover from the minute variation.

Theorem 4.5. *When* $Y < R\frac{C_D}{D + P_2L - P_1L}$, *only* $X = 0$ *is the evolutionary stable strategy of evolutionary game of the defender, namely all*
the defenders prefer to no deployment security measure.

ProofFigure 3 shows the replicator dynamics phase diagram, which shows that the horizontal axis and the replicator dynamics curve connect at two points: X = 0 and X = 1. All defenders prefer not to deploy security measures since the evolutionary stable strategy of the evolutionary game is X = 0, since the slope of the tangent at the point of intersection X = 0 is negative and the slope at the point of intersection X = 1 is positive.

Evolutionary stability of the attacker.

According to the equation of replicator dynamics (10), let $\frac{dY}{dt} = 0$, then we can obtain three values, i.e. $Y = 0$, $Y = 1$, $X = \frac{C_A - P_2R_A}{P_1R_A - P_2R_A}$.

Similarly the values of ESS depend on X, and we have the following three cases as well:

Theorem 4.6. *When* $X > \frac{C_A - P_2R_A}{P_1R_A - P_2R_A}$, *only* $Y = 0$ *is the evolutionary stable strategy of evolutionary game of the attacker, namely all the attackers prefer to no attack strategy.*

Proof. The attacker's replicator dynamics phase diagram (Fig. 4) shows that the horizontal axis and replicator dynamics curve connect at two locations, Y = 0 and Y = 1, respectively. Because the tangent slope at Y = 0 is negative and the tangent slope at Y = 1 is positive, the only stable evolutionary strategy for the attackers in the evolutionary game is Y = 0, meaning they all favour the no attack approach.

Theorem 4.7. *When* $X = \frac{C_A - P_2R_A}{P_1R_A - P_2R_A}$, *there is no evolutionary stable strategy for the attack.*

Proof. From the phase diagram of replicator dynamics for the attacker (Fig. 5), we can see that the curve of replicator dynamics and horizontal axis overlap each other. In this case, Y cannot recover from the minute deviation, and thus it is not the evolutionary stable strategy for the attack. □

Theorem 4.8. *When* $X < \frac{C_A - P_2R_A}{P_1R_A - P_2R_A}$, *only* $Y = 1$ *is the evolutionary stable strategy of evolutionary game for the attacker, namely all the attackers prefer to attack strategy.*

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN2454-9940
www.ijasem.org
Vol 18, Issue 1, 2024

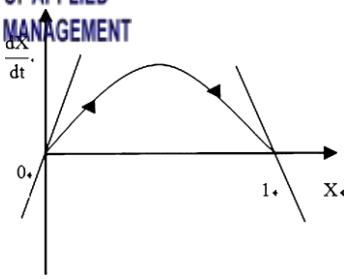


Fig. 4. The phase diagram of replicator dynamics when $X > \frac{C_A - P_2 R_A}{P_1 R_A - P_2 R_A}$.

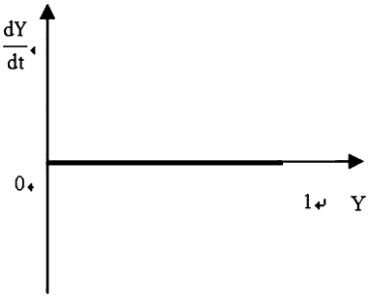


Fig. 5. The phase diagram of replicator dynamics when $X = \frac{C_A - P_2 R_A}{P_1 R_A - P_2 R_A}$.

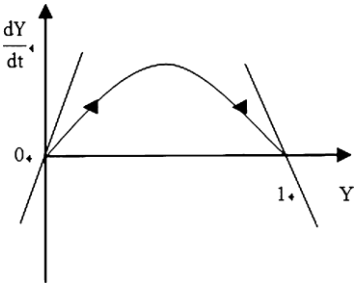


Fig. 6. The phase diagram of replicator dynamics when $X < \frac{C_A - P_2 R_A}{P_1 R_A - P_2 R_A}$.

Proof. Figure 6 shows the attacker's replicator dynamics phase diagram; at the junction of the curve and the horizontal axis, there are two locations, Y = 0 and Y = 1, as can be seen. Given that the tangent slope at Y = 0 is positive and the tangent slope at Y = 1 is negative, the only stable evolutionary strategy for the attacker in the evolutionary game is Y = 1, meaning that all attackers choose this approach.

Active defense of the system.

The ideal scenario, as seen through the lens of wireless sensor networks, is one in which neither the attackers nor the sensor nodes take any security measures. So as to efficiently save energy, storage space, etc., the system should converge to the state (0, 0).

Theorem 4.9. *(0, 0) is the only evolutionary stable of the system strategy if and only if* $P_2 R_A - C_A < 0$.

Proof. *Proof of existence*: According to Eq. (7) and Eq. (11), a Jacobin matrix can be generated which is denoted by J,

$$J = \begin{matrix} (1-2X)(Y R_D + P_2 LY - P_1 LY - C_D) & X(1-X)(R_D + P_2 L - P_1 L) \\ Y(1-Y)(P_1 R_A - P_2 R_A) & (1-2Y)(P_2 R_A - C_A + XP_1 R_A - XP_2 R_A) \end{matrix}$$

Purports to $(0, 0)$ is the evolutionary stable strategy of the system if and only if $det\ J > 0$, $tr\ J < 0$ [21]. Using $(0, 0)$ substitute in the Jacobi matrix J, we have

$$J = \begin{matrix} -C_D & 0 \\ 0 & P_2 R_A - C_A \end{matrix}$$

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 1, 2024

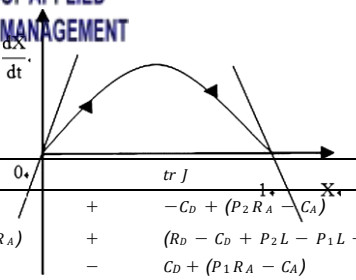


Table 2
The local stability of equilibrium point (EP) of system.

EP (X, Y)	$det\ J$		$tr\ J$		Local stability
$(0, 0)$	$(-C_D) \cdot (P_2 R_A - C_A)$	+	$-C_D + (P_2 R_A - C_A)$	−	ESS
$(0, 1)$	$(R_D - C_D + P_2 L - P_1 L) \cdot (C_A - P_2 R_A)$	+	$(R_D - C_D + P_2 L - P_1 L + C_A - P_2 R_A)$	+	no stability
$(1, 0)$	$C_D \cdot (P_1 R_A - C_A)$	−	$C_D + (P_1 R_A - C_A)$	indefinite	addle point
$(1, 0)$	$(C_D - R_D + P_1 L - P_2 L) \cdot (C_A - P_1 R_A)$	−	$(C_D - R_D + P_1 L - P_2 L) + (C_A - P_1 R_A)$	indefinite	addle point

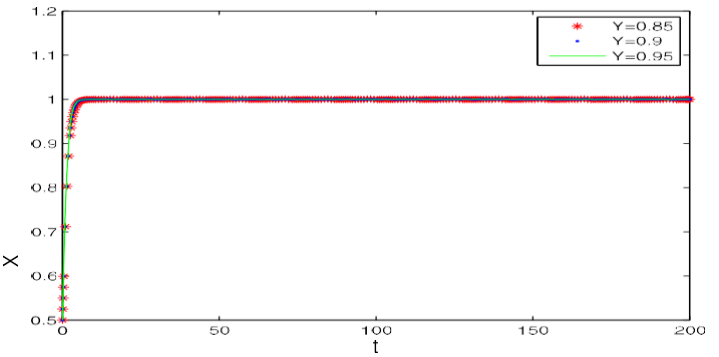


Fig. 7. The ESS of defenders when $Y = 0.9$.

So the determinant of the matrix J is $det\ J = (-C_D)(P_2 R_A - C_A) > 0$, and the track of matrix J is $tr\ J = (-C_D) + (P_2 R_A - C_A) < 0$, finally we can get $P_2 R_A - C_A < 0$.

Proof of unicity: When $(P_2 R_A - C_A) < 0$, $(1, 1)$ and $(0, 0)$ are saddle points, $(0, 1)$ has no stability, so $(0, 0)$ is the only evolutionary stable strategy of system. Table 2 shows the results in details. □

If we set p2 R A CA < 0 according to Theorem 4.9, we will have to either increase the cost of assault CA or decrease the payout of attack R A respectively. Subsequently, defenders may adapt their defensive techniques to effectively counter the attacker's various tactics by being active and dynamic.

2. Numerical evaluation

2.1. Matlab is used to simulate the model in this article. Please see below the list of parameters that were used for the simulation. We normalised all parameters to values in [0, 1] since the measurement units of payout, cost, and loss parameters are different. We will assume that R A = 0.8 × RD and CA = 2 × CD based on the features of wireless sensor networks.

Evolutionary stability of wireless sensor nodes

Set the values of parameters as follows, $R_D = 1$, $C_D = 0.3$, $L = 1$, $P_1 = 0.5$, $X = 0.5$. According to the values of parameters, we can calculate the critical value of deployment security measure and no deployment security measure, then $Y = \frac{C_D}{(R_D + P_2 L - P_1 L)} = 0.2$. Now three simulations with different values of Y are analyzed respectively:

(1) When the value of Y is larger than the critical value, e.g. $Y = 0.85$, $Y = 0.9$, $Y = 0.95$, from Fig. 7, we can see defenders can resist the small deviation from the disturbance and eventually converge to the state of $X = 1$.
(2) When the value of Y equals the critical value, e.g. $Y = 0.2$, from Fig. 8, we can see, the defenders cannot resist the small deviation from the disturbance and also they cannot converge to the state of $X = 1$.
(3) When the value of Y is smaller than critical value, e.g. $Y = 0.05$, $Y = 0.1$, $Y = 0.15$, from Fig. 9, we can see that defenders can resist the small deviation from the disturbance, and eventually converge to the state of $X = 0$.

Now we can come to the conclusion that the theoretical analysis about the defender's ESS is correct.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN2454-9940
www.ijasem.org
Vol 18, Issue 1, 2024

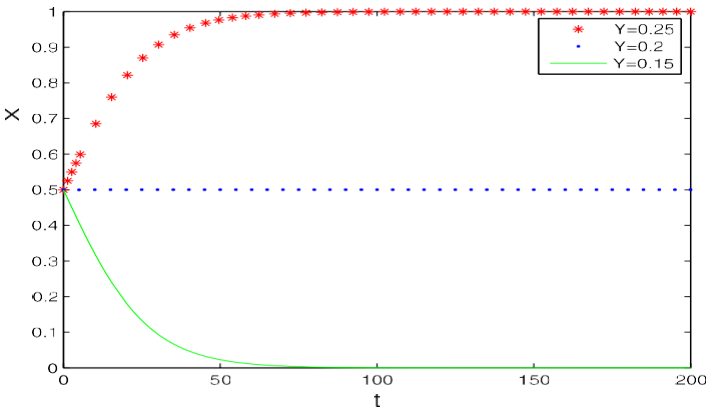


Fig. 8. The ESS of defenders when $Y = 0.2$.

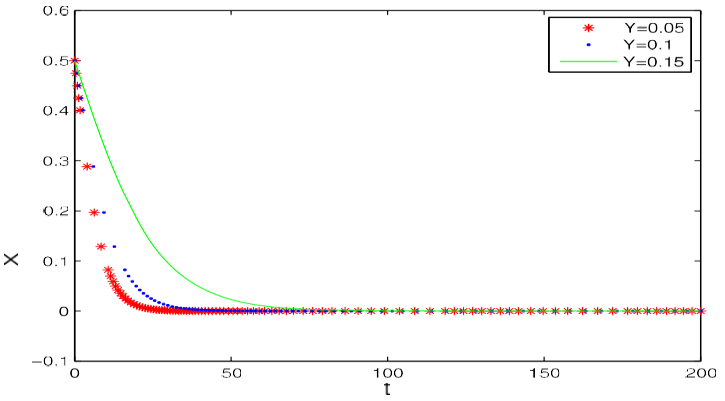


Fig. 9. The ESS of defenders when $Y = 0.1$.

2.2. The evolutionary stability of attackers

The following is how you may set the parameters: The critical value of attack and the absence of attack may be determined by X~C A −p2 R A 0 1, where R A is 0.8, CA is 0.6, and P 2 is 0.5. Here we have a look at three separate simulations, each with a unique value of X:
The relation p1 R A − p2 R A is defined in (1).Figure 10 shows that the attackers are able to withstand the little departure from the disturbance and converge to the state of Y~0 when the value of X is greater than the critical value, for example, X~0.75, X 0.8, and X 0.85.

At critical values of X (e.g., X = 0.05, X = 0.1, or X = 0.15), as shown in Figure 11, attackers are unable to withstand even a minor deviance from the disturbance and so cannot converge to a stable state.

(3) As shown in Figure 12, attackers are able to withstand the little departure from the disturbance and converge to the state of Y = 1 when the value of X is lower than the critical value, for example, X = 0.03, X = 0.05, or X = 0.07.
In conclusion, the simulation findings show that the theoretical analysis of the attacker's ESS was valid.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN2454-9940
www.ijasem.org
Vol 18, Issue 1, 2024

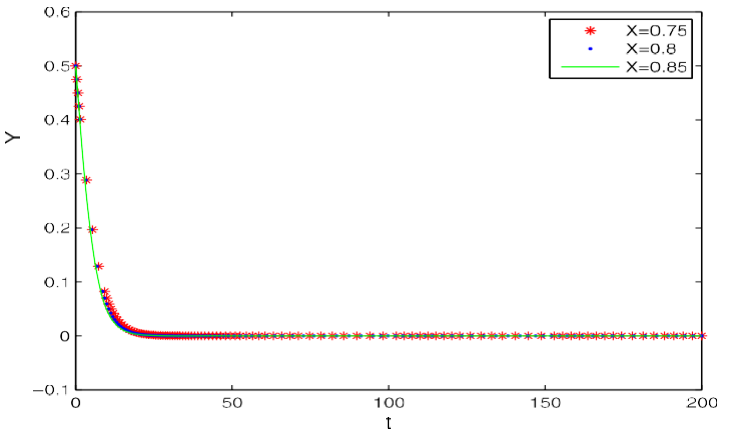


Fig. 10. The ESS of attackers when $X = 0.8$.

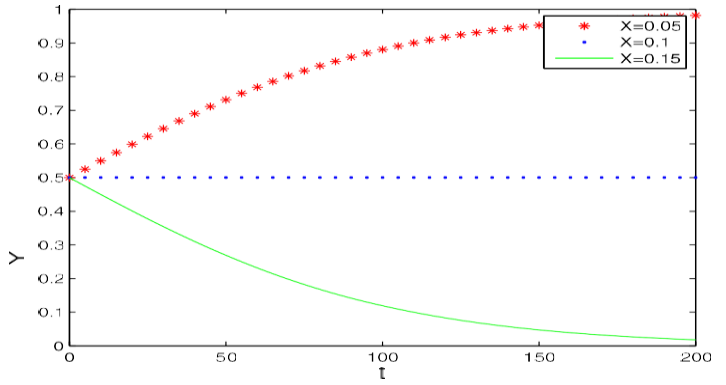


Fig. 11. The ESS of attackers when $X = 0.1$.

2.3. Evolutionary stability of the system of attack–defense

There is no stability among attackers and defenders (9.3.1).
Parameter values should be set as follows: The variables are as follows: RD = 1, CD = 0.3, L = 0.7, P 1 = 0.3, P 2 = 0.8, X = 0.5, R A = 0.8, CA = 0.6.
The attackers and wireless sensor nodes are in an unstable attack-defense cycle when P 2 R A > CA, as shown in Fig. 13. It wreaks havoc on resource-constrained wireless sensor nodes. Instead of making reasonable and timely plans for security, we can only choose a strategy at random, which reduces the efficacy of defence.

All parties involved, including attackers and defenders, are stable at 9.3.2.

The following changes are made to the parameter values and the value of CD in accordance with Theorem 4.9: 1 for RD and 0.4 for CD,

R A = 0.8, CA = 0.8, X = 0.5, P 1 = 0.3, P 2 = 0.8, L = 0.7, and Y = 0.5.

Figure 14 illustrates that attackers will have a harder time launching successful attacks when wireless sensor nodes increase the Security Defence level, which in turn increases the deployment security measures. As a result, the cost of attacks will exceed the benefits gained from them, meaning that R A < CA. The findings of the simulation indicate that wireless

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN2454-9940
www.ijasem.org
Vol 18, Issue 1, 2024

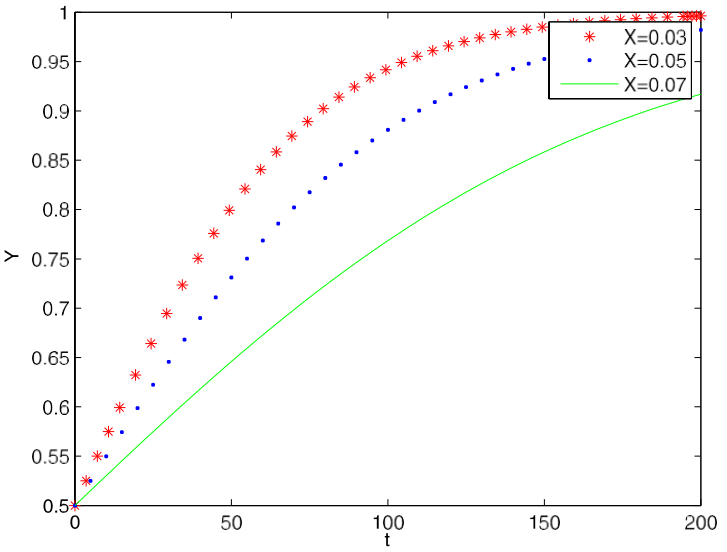


Fig. 12. The ESS of attackers when $X = 0.05$.

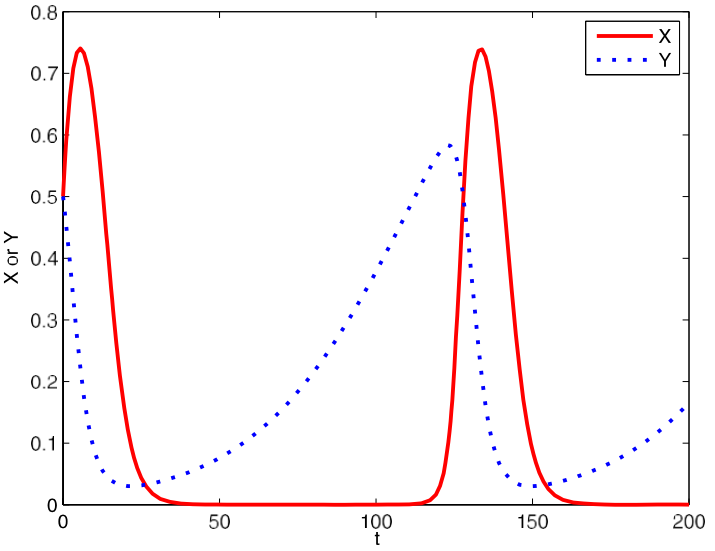


Fig. 13. The ESS of system when $P_2 R_A > C_A$.

an evolutionary steady state is achieved by both the sensor nodes and the attackers. Based on this, the theoretical analysis presented in Section 3 of this study about the evolutionary stability of attacker-defender is supported. Nodes in resource-constrained wireless sensor networks may dynamically alter their defensive cost in response to the values of data to be sent, as the attack is real and objective. Because of this, attackers will find wireless sensor networks to be a safer alternative, since the costs of an attack will outweigh the benefits of a successful assault. In this way, wireless sensor nodes may protect specific targets, reduce energy consumption, and remain operational for a longer period of time inside the network.

9.3.1 An effect of P 1 on the ESS convergence rate

To begin, set the parameters to the following values: The significance levels are P=0.1, P=0.3, and P= 0.5. From Figure 15, we may deduce that the success probability of an assault, P1, has no effect on the rate of accessing ESS. No matter how high the assault's success probability is, the utility of the attacker is always negative since the rewards of a successful attack are always less than the cost of an attack. Accordingly, if the assailant is being rational, then refraining from attacking is the wisest course of action.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 1, 2024

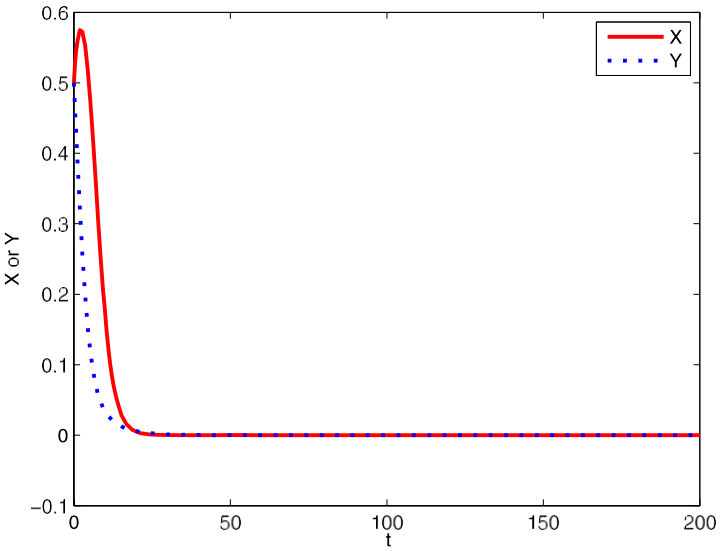


Fig. 14. The ESS of system when $P_2 R_A < C_A$.

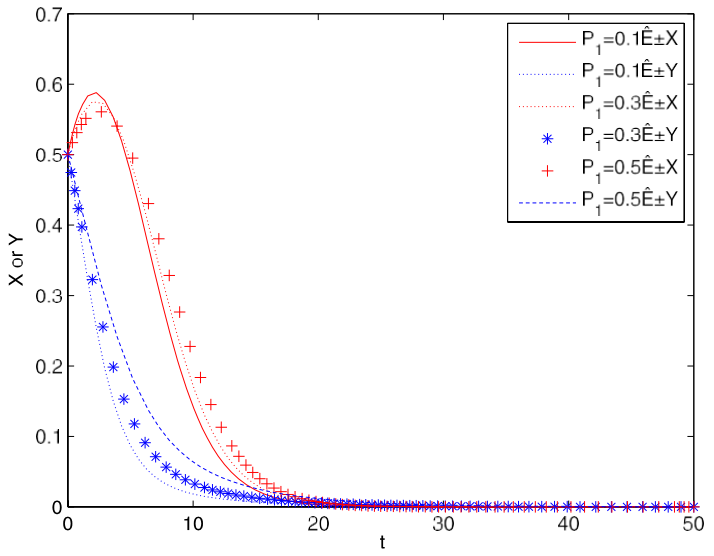


Fig. 15. The ESS of system when the different value of P_1.

2.3.1. Different values of P_2 affect the convergent rate of ESS

P 2 = 0.1, P 2 = 0.3, and P 2 = 0.5 are the parameter values that should be set.
The rates at which the attacker and the defender attain ESS are directly proportional to the magnitude of p2, as seen in Figure 16. This lines up with the idea that if the defence opts out of using security measures, the attack has a good chance of succeeding. Even though it should be able to pay the cost CA, an attacker can more easily gain the R A with a greater p2. For this reason alone, the attacker will choose this attack approach. In other words, if the defence decides not to use security measures, it is the greatest option for the attacker.

9.3.2. The convergence rate of ESS is affected by different values of X and Y.

X = 0.8 and Y = 0.8; X = 0.3 and Y = 0.3; X = 0.8 and Y = 0.3; and finally, X = 0.3 and Y = 0.8 represent the values of the parameters.

According to Figure 17, the attacker's rate of achieving ESS regarding wireless sensor networks decreases as the initial probability of the attacker choosing the deployment security measure strategy increases, and the reverse is also true for attackers choosing attack strategies.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 1, 2024

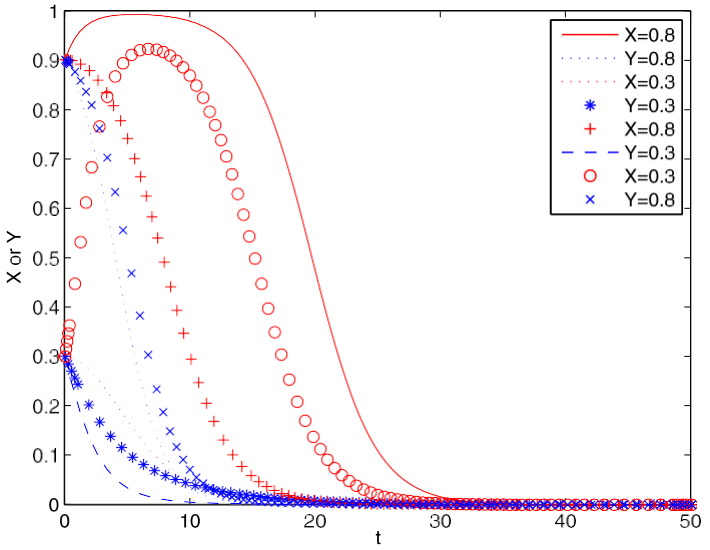


Fig. 16. The ESS of system when the different value of P_2.

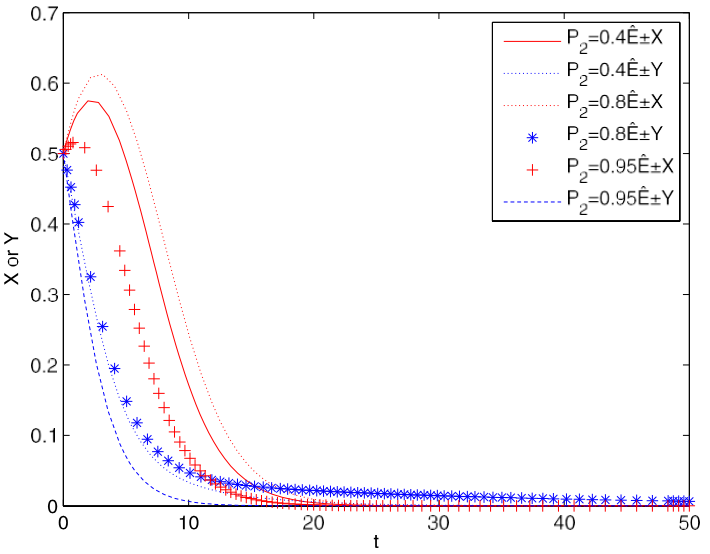


Fig. 17. The ESS of system when the different values of X and Y.

3. Conclusion

In this study, we provide an evolutionary game-theory-based active defence model for WSNs. Instead of relying on the completely rational premise of classical game theory, this active defence model calls for sensor nodes that exhibit limited rationality and game process dynamics. As such, it meets the requirements for wireless sensor network nodes. Since the topology is always changing, the sensor nodes that need to know the network's status and keep it updated take a lot of power and space. For wireless sensor networks with limited resources, it seems to be both impractical and useless. Nevertheless, nodes may actively and dynamically adapt their defensive methods to effectively counter the attacker's various policies via dynamic evolution. The application of evolutionary game theory to wireless sensor networks has shown to be an effective tool. The widespread use of wireless sensor networks is inevitable given the proliferation of new standards-based networks and the ongoing development of low power systems, both of which make possible a plethora of hitherto impractical applications.

Acknowledgments

This work was supported by Natural Science Foundation of Fujian Province (2012J01252); Fujian Province University-Industry Cooperation of Major Science and Technology Project (2011H6008); National Natural Science Foundation (61072080, 11171086); Fujian development and reform commission high technical [2013] 266; Fujian Normal University Innovative Research Team (No. IRTL1207).

References

[1] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister, System architecture directions for networked sensors, in: ASPLOS, November 2000.
[2] J.S. Wilson, Wireless sensor networks: principles and applications (Chapter 22).
[3] John A. Stankovic, Wireless sensor networks, University of Virginia, Charlottesville, VA, 22904.
[4] Tahir Naeem, Kok-Keong Loo, Common security issues and challenges in wireless sensor networks and IEEE 802.11 wireless mesh networks, Internat. J. Digital Content Technol. Appl. 3 (1) (2009) 89–90.
[5] Mark Luk, Ghita Mezzour, Adrian Perrig, Virgil Gligor, MiniSec: a secure sensor network communication architecture, in: Proceedings of the Sixth International Conference on Information Processing in Sensor Networks, IPSN 2007, 2007.
[6] A. Perrig, J. Stankovic, D. Wagner, Security in wireless sensor networks, Commun. ACM 47 (6) (2004).
[7] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, Security in wireless sensor networks: issues and challenges, in: International Conference on Advanced Computing Technologies, 2006, pp. 1043–1045.
[8] J. Newsome, E. Shi, D. Song, A. Perrig, The Sybil attack in sensor networks: Analysis and defenses, in: IPSN '04, Berkeley, CA, 2004.
[9] S. Zhu, S. Setia, S. Jajodia, P. Ning, An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks, in: IEEE Symposium on Security and Privacy, Berkeley, CA, 2004.
[10] A. Wood, J. Stankovic, Denial of Service in Sensor Networks, IEEE Computer Society, September 2002, pp. 54–62.
[11] Sami S. Al-Wakeel, Saad A. Al-Swailem, PRSA: a path redundancy based security algorithm for wireless sensor networks, in: WCNC 2007 Proceedings, pp. 4159–4163.
[12] A.D. Wood, J.A. Stankovic, G. Zhou, DEEJAM: defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks, in: Fourth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON, San Diego, CA, 2007.
[13] J. von Neumann, O. Morgenstern, Theory of Games and Economic Behavior, Princeton University Press, Princeton, NJ, 1994, pp. 36–39.
[14] J. Hofbauer, K. Sigmund, Evolutionary game dynamics, Bull. Am. Math. Soc. 40 (4) (2003) 479–519.
[15] L. Samuelson, Evolutionary Games and Equilibrium Selection, MIT Press, 1997.
[16] D. Fudenberg, K. Levned, The Theory of Learning in Games, Mass MIT Press, Cambridge, 1998, pp. 167–169.
[17] Yihui Qiu, Zhide Chen, Li Xu, Active defense model of wireless sensor networks based on evolutionary game theory, in: 6th International Conference on Wireless Communications Networking and Mobile Computing, WiCOM, 2010, pp. 1–4.
[18] Wei He, Chunhe Xia, Haiquan Wang, Cheng Zhang, et al., A game theoretical attack–defense model oriented to network security risk assessment, in: 2008 International Conference on Computer Science and Software Engineering, 2008, pp. 498–504.
[19] Jiang Wei, Fangbin Xing, et al., Evaluating network security and optimal active defense based on attack–defense game theory, Chin. J. Comput. 32 (4) (2009).
[20] A. Agah, S.K. Das, K. Basu, Preventing DoS attack in sensor and actor networks: a game theoretic approach, in: IEEE International Conference on Communications, ICC, Seoul, Korea, 2005, pp. 3218–3222.
[21] A. Agah, S.K. Das, K. Basu, Enforcing security for prevention of dos attack in wireless sensor networks using economical modeling, in: Proceedings of 2nd IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, MASS, Washington, DC, 2005.
[22] Wei Sun, Xiangwei Kong, Dequan He, et al., Information security game analysis with penalty parameter, Internat. Symp. Elect. Commerce Sec. 8 (2008) 453–456.
[23] J.W. Weibull, Evolutionary Game Theory, MIT Press, 1995.