Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 358 – 366

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Adaptive Selection of Cryptographic Protocols in Wireless Sensor Networks using Evolutionary Game Theory

Srishti Arora[1], Prabhjot Singh[b], Dr. Ashok Ji Gupta[1]

[a]*Indian Institute of Technolgy (BHU), Varanasi*
[b]*National Institute of Technology Karnataka, Surathkal*

Abstract

Game theory applies to scenarios wherein multiple players with contrary motives contend with each other. Various solutions based on Game theory have been recently proposed which dealt with security aspects of wireless sensor networks(WSNs). However, the nodes have limited capability of rationality and evolutionary learning which makes it unfavorable to apply conventional game theory in WSNs. Evolutionary Game Theory(EGT) relies on bounded rationality assumption which is in harmony with the wireless sensor networks characteristics. Based on EGT, authors propose an adaptive security model for WSNs for the selection of cryptographic protocols during runtime. The authors formulate this selection in WSNs with the help of an evolutionary game to obtain the evolutionarily stable strategy (ESS) for the system. In this model, the sensor nodes dynamically adapt their defensive strategies to attain the most efficient defense, corresponding to the attackers' varied strategies. Further, the simulations convey that the proposed system converges rapidly to the Evolutionary Stable Strategy. Not only the system converges, but also forms a stable system which was verified by deliberately destabilizing the system. Results show that the nodes quickly return to ESS even after perturbation.

Peer-review under responsibility of organizing committee of the ICISP2015
Keywords: WSNs, Evolutionary Game Theory, Cryptographic Protocols, Selection

1. Introduction

Wireless Sensor Networks (WSNs) is an evolving concept that shows immense opportunities for several futuristic. Wireless Sensor Networks are based on collaborative effort of a large number of tiny sensor nodes, which consist of communicating, sensing and data processing components. Sensor networks usually consist of vast number of sensor nodes which are densely deployed over a range of area. It is not necessary to design or predetermine the position of individual node which makes random deployment in inaccessible terrains feasible. On the other hand, this leads to a constraint, that sensor network protocols and algorithms must exhibit self-organizing capabilities. An additional distinctive feature of sensor networks is the collaborative effort of sensor nodes. Sensor nodes are fitted with an on-board processor and they use their processing abilities to locally carry out simple computations.

*

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.075

The fundamental nature of the attack-defense can be exhibited by mutual strategies of interdependence. Accordingly, WSN security model can be represented by at least two players competing in a challenge to maximize their intended objectives. Game theory can be employed to carry out tactical analysis of the WSN threats produced either by a lone attacker or by a structured group. Game theory[1] was conceived by John von Neumann to mathematically determine optimal strategies for competing adversaries. A contest involves a number of players, all of whom have a choice of moves for the game. The approach a player uses in selecting his moves forms the player's strategy. Payoffs for the various players are the outcomes of the set of strategies selected by them that are governed by the rules; rules and resulting payoffs are articulated in a payoff matrix (normal form games). In classical game theory, all players are required to make their strategic choices based on rationally-determined evaluation of probable outcomes. As a result, it is essential in game theory that each player must make rational choices.

However, evolutionary game theory is based on bounded rationality assumption which is in line with the characteristics of sensor nodes in wireless sensor networks. Frequent topology changes in wireless sensor networks make it infeasible for the sensor nodes to maintain full rationality about the system. Moreover, it is unrealistic and unproductive because wireless sensor networks are generally resource constrained. Dynamic evolution, as suggested in this paper, implies that nodes can be adaptive towards their defense strategies such that nodes can be actively and dynamically modified in order to achieve the effective defense. The significant point in the evolutionary game theory model is that the success of a strategy is not just determined by how good the strategy is in itself, it is a question of how good the strategy is in the presence of other alternative strategies. In Nash equilibrium for a two-player game, the equilibrium is a choice of strategies that tends to prevail once the players have adopted them. Deviation from the strategy pursued by the players at the equilibrium is not considered to be an optimal move in terms of pay-offs. The equivalent notion for evolutionary settings will be that of a genetically-determined strategy that tends to persist once it starts prevailing in a population —an evolutionarily stable strategy[2]. An ESS is a polished or modified form of Nash equilibrium[3]. There are various solutions to WSNs security problems based on Evolutionary Game Theory as mentioned in next section but existing solutions are almost acquiescent defense because of which wireless sensor networks can take appropriate measures only after successful attack detection.

2. Related Work

Game theory[4] acts upon set-ups where various players with contrary motives compete against each other and hence provides a mathematical model for analyzing WSNs security problems. Effectiveness of the defensive strategy of defender not only depends on his own behavior but also on the attacker's strategy and vice versa. The assumptions of full rationality in conventional game theory[5] require the player to have rational awareness, memory capacity, analytical ability, and precise requirements[6]. Since practically it is not possible for a player to support such high demands of full rationality, the scope of applying game theory is restricted in the existent world. Evolutionary game theory, a concept that mostly relies on the game process dynamics and players with rationality of bounded nature was presented by Weibull in the 20th century. Bounded rationality implies that the player only has the partial knowledge about the game state, such as the action strategies and payoffs[7,8]. The player is not capable of finding the optimal strategy solely with respect to a game. For finding an effective strategy for himself, a player requires continual learning and imitation in the game. The authors in[9] designed a network security risk assessment by modeling attack-defense interactions based on game theoretical which enumerates the threats probability.

An evolutionary game theory approach for an active defense model was presented in[5]. It states that the optimal solution is that the attackers implement no attack strategy, and the sensor nodes implement no security deployment measure strategy. The authors of[5] presents a model which only justifies no attack-no defense state as an ESS. However, existing security solutions are more or less passive defense, which makes wireless sensor networks take appropriate responses only after the attack is detected.

3. System Model and Utility Function

Game theory model usually comprises of three basic elements: pay-off function, players and strategy spaces. According to the characteristics of wireless sensor networks, we build up the game model as follows.

3.1. System Model

We consider a large scale deployment of a wireless sensor network with n nodes, where n >> 1. We assume time is divided into time units called time slots. At the start of each time slot, the players decide which strategy to follow. We assume that each time slot is long enough to facilitate the decision making processes. General composition of system model is players and their strategy space which are discussed as follows:

3.1.1. Players

In accordance with the attributes of wireless sensor network's security, the population of the game players can be classified into two categories: the first one comprises of players with defending capabilities, denoted as Defender; and the other comprises of attacking capabilities, denoted as Adversary, and thus the game players set is represented as (Defender, Adversary). Here players represent the sensor nodes in WSN.

3.1.2. Strategy Space

Considering its residual energy, storage capacity and bandwidth, a wireless sensor node will make a selection regarding deploying either weak or strong security cryptographic protocols. Thus the strategy set of the defender is represented in terms of security deployment $S_D = (strong\ defense, weak\ defense)$. Adversary will take into consideration the cost of attack and the rewards it will gain after the attack and then decide whether to attack or not. Hence, the strategy set of an adversary is represented by $S_A = (attack, no\ attack)$.

3.2. Payoff Function

We assume a number of payoff parameters according to the characteristics of wireless sensor networks. These payoff parameters are computed for each cycle.

- R_D: Reward to defender in case of strong cryptographic protocol.
- C_D: Cost of defense in case of strong cryptographic protocol.
- R_A: Reward to attacker.
- C_A: Cost of attack.
- L : Loss of genuine node in case of successful attack.
- R_U: Reward to sensor node for not being an attacker
- P_S: Probability of a successful attack in case of strong cryptographic protocol.
- P_W: Probability of a successful attack in case of weak cryptographic protocol.
- M_1, M_2: Constant multipliers.

$*$ Cost of defense in case of weak cryptographic protocol is not considered because a weak cryptographic protocol doesn't consume extra resources, and since weak cryptographic protocol is basic requirement for the node to exist in the system, hence no reward to defender.

$* P_S << P_W$

Based on the above parameters and assumptions, we give the Defender - Adversary payoff matrix :

Defender	Adversary	
	Attack	No Attack
Strong Encryption	$M_1[(1-P_S)R_D - C_D] - M_2LP_S, M_2(P_SR_A - C_A)$	$M_1(R_D - C_D), M_2(R_D - C_D)$
Weak Encryption	$M_1R_U - M_2LP_W, M_2(P_WR_A - C_A)$	R_U, R_U

4. Evolutionary Secure Game

In this section, we first give a brief introduction about evolutionary game and then we apply the concepts of evolutionary game theory to our Adaptive Selection of Cryptographic Protocols model. Thereafter, analyzing the replicator equations we derive evolutionarily stable strategy for the same.

4.1. Basic Concept of Evolutionary Game

According to [1,12,13], basic concepts of Evolutionary Game Theory are explained as follows:

4.1.1. Evolutionarily Stable Strategy

In the evolutionary game, each player dynamically adjusts his/her strategy post observing the utilities under different strategies. It is an effective approach for a bunch of players converging towards a stable equilibrium after rounds of strategic interactions, and the observed concluding strategy over the equilibrium is termed as evolutionarily stable strategy (ESS). According to the evolutionary game theory, for a game with N players a strategy profile

$$a^* = (a_1^*, ..., a_N^*)$$

is an ESS if and only if, $\forall a \neq a^*, a^*$ satisfies the follows:

$$U_i(a_i, a_{-i}^*) \leq U_i(a_i^*, a_{-i}^*), \tag{1}$$

$$\begin{aligned} if \quad U_i(a_i, a\_i^*) &= U_i(a_i^*, a_{-i}^*), \\ U_i(a_i, a_{-i}) &< U_i(a_i^*, a_{-i}), \end{aligned} \tag{2}$$

where U_i stands for the payoff of player i and a_{-i} represents the strategies of all players except player i. We can observe that the first condition is the Nash equilibrium (NE) condition, and the second condition guarantees the stability of the strategy. Moreover, we also know that a strict NE is always an ESS.

4.1.2. Replicator Dynamics

In a distributed scheme each node is uncertain about other node's actions and payoffs. In such a situation, to enhance their payoffs, sensor nodes will practice various strategies in each time slot and assimilate from the strategic interactions by applying the technique of understanding-by-building. Since the fraction of total nodes following a certain pure strategy may vary during the process, thus replicator dynamics is used to study such a population evolution. Specifically, let x stands for the proportion of defending nodes using strong encryption scheme and y stands for the proportion of adversary nodes with attack strategy. Applying replicator dynamics, the evolutionary dynamics of x and y are represented by the below differential equations:

$$\dot{x} = \eta(\overline{U}_1 - \overline{U}_x)x, \tag{3}$$

$$\dot{y} = \eta(\overline{U}_3 - \overline{U}_y)y. \tag{4}$$

where $\overline{U}_1$ is the expected payoff of a defending node using purely strong cryptographic protocol, $\overline{U}_x$ is the expected payoff of a defending node using mixed strategy $(x, 1-x)$, $\overline{U}_3$ is the expected payoff of an adversary node with pure intent of attacking, $\overline{U}_y$ is the expected payoff of an adversary node using mixed strategy $(y, 1-y)$, and η is some positive constant which can be used to adjust the rate of convergence. We should note that $\overline{U}_1$ stands for the average payoff of the defending node with purely strong cryptographic protocol, and $\overline{U}_x$ stands for the average payoff of all the defender nodes, if we regard defender nodes and adversary nodes as two populations and the scale of the populations N_1 and N_2 is sufficiently large. Similarly, we can explain $\overline{U}_3$ and $\overline{U}_y$ in this way.

The expected payoff of a node in defender or adversary population using mixed strategy can be written as

$$\overline{U}_x = x\overline{U}_1 + (1-x)\overline{U}_2, \tag{5}$$

$$\overline{U}_y = y\overline{U}_3 + (1-y)\overline{U}_4, \tag{6}$$

where $\overline{U}_2$ is the expected payoff of a defender node using pure strategy of weak cryptographic protocol, and $\overline{U}_4$ is the expected payoff of an adversary node with no intent of attack.

Substituting 5 and 6 back to 3 and 4, we have

$$\dot{x} = \eta x(1-x)(\overline{U}_1 - \overline{U}_2), \tag{7}$$

$$\dot{y} = \eta y(1-y)(\overline{U}_3 - \overline{U}_4). \tag{8}$$

4.2. Replicator Dynamics of Security Model

Using the Defender - Adversary payoff matrix, the expected payoff of a defender node using pure strategy of strong cryptographic protocol or weak cryptographic protocol can be computed respectively by

$$\overline{U}_1 = M_1(R_D - C_D) - yP_S(M_1R_D + M_2L) - xs \tag{9}$$

$$\overline{U}_2 = y(M_1R_U - M_2LP_W - R_U) + R_U - (1-x)w \tag{10}$$

where, s and w are loss in inter-cluster communication due to hindrance by cryptographic protocols and $s, w > 0$.

According to Defender-Adversary payoff matrix, the expected payoff of an adversary node using pure strategy of participation with intent of Attack or No Attack can be computed respectively by

$$\overline{U}_3 = M_2(P_WR_A - C_A) - xM_2R_A(P_W - P_S) \tag{11}$$

$$\overline{U}_4 = xM_2(R_D - C_D - R_U) + R_U \tag{12}$$

$$\dot{x} = \eta x(1-x)[y\{M_2L(P_W - P_S) + (1-M_1)R_U - M_1P_SR_D\} + M_1(R_D - C_D) - R_U - (s+w)x + w] \tag{13}$$

$$\dot{y} = \eta y(1-y)[M_2(P_WR_A - C_A) - xM_2\{R_A(P_W - P_S) + (R_D - C_D) - R_U\} - R_U] \tag{14}$$

4.3. Analysis of Evolutionarily Stable Strategy

At equilibrium, we have $\dot{x} = 0$ and $\dot{y} = 0$. According to 13 and 14, we get the possible equilibria:

$$(0,0), (0,1), (1,0), (1,1)$$

$$(x^+, 0) = \left(\frac{M_1(R_D - C_D) - R_U + w}{s+w}, 0\right)$$

and (x^*, y^*) where

$$x^* = \frac{M_2(P_WR_A - C_A) - R_U}{M_2\{R_A(P_W - P_S) + (R_D - C_D) - R_U\}}, \text{ and}$$

$$y^* = \left[\frac{\{M_2(P_WR_A - C_A) - R_U\}(s+w)}{M_2\{R_A(P_W - P_S) + (R_D - C_D) - R_U\}} + R_U - w - M_1(R_D - C_D)\right]\frac{1}{M_2L(P_W - P_S) + (1-M_1)R_U - M_1P_SR_D} \tag{15}$$

According to the evolutionary game theory [12], equilibrium of the replicator dynamics is an ESS if and only if it is a locally asymptotically stable point in a dynamic system.

Since 13 and 14 is a non-linear dynamic system, by analyzing Jacobian matrix (J) of the replicator dynamics equations, we examine whether the equilibrium's are ESSs. For the same, we require:

$$J = \begin{pmatrix} \frac{\partial \dot{x}}{\partial x} & \frac{\partial \dot{x}}{\partial y} \\ \frac{\partial \dot{y}}{\partial x} & \frac{\partial \dot{y}}{\partial y} \end{pmatrix} = \eta \begin{pmatrix} J_{11} & J_{12} \\ J_{21} & J_{22} \end{pmatrix}$$

For the model described above, $J_{11}, J_{12}, J_{21}, J_{22}$ are listed as

$$J_{11} = (1-2x)[y\{M_2L(P_W - P_S) + (1-M_1)R_U - M_1P_SR_D\} + M_1(R_D - C_D) - R_U - (s+w)x + w] - x(1+x)(s+w), \tag{16}$$

$$J_{12} = x(1-x)\{M_2L(P_W - P_S) + (1-M_1)R_U - M_1P_SR_D\}, \tag{17}$$

$$J_{21} = -y(1-y)M_2\{R_A(P_W - P_S) + (R_D - C_D) - R_U\} and \tag{18}$$

$$J_{22} = (1-2y)[M_2(P_WR_A - C_A) - xM_2\{R_A(P_W - P_S) + (R_D - C_D) - R_U\} - R_U] \tag{19}$$

And the asymptotical stability implies that $det(J) > 0$ and $tr(J) < 0$ i.e. ,

$$det(J) = J_{11}.J_{22} - J_{12}.J_{21} > 0, \tag{20}$$

$$tr(J) = J_{11} + J_{22} < 0. \tag{21}$$

Before analyzing the equilibria we will first try to explain the physical significance of the equilibrium:

$*$ Equilibrium (x^+, y^+) signifies that the system will converge to a state where x^+ proportion of the defenders will choose strong encryption strategy and y^+ proportion of the adversaries will choose not to attack.

Substituting the equilibria points in 20 and 21 using 16, 17, 18, 19, we can examine whether they are ESSs.

Before we start analyzing the equilibria, we should note that since both x and y are proportions, therefore

$$0 < x < 1 \quad and \quad 0 < y < 1$$

We checked for (x^*, y^*) calculated in 15 because it is the most expected state for a real time system and we observed that (x^*, y^*) is an ESS, as it satisfies following conditions : $0 < x^* < 1$; $0 < y^* < 1$; $det(J) > 0$; $tr(J) < 0$, if parameters are set accordingly. For all the other equilibria, we can similarly derive conditions for parameter setting in order to achieve an ESS.

5. Simulation Results

We conducted simulations to verify the effectiveness of our analysis. Firstly, we simulated the proposed model via NetLogo to show its effectiveness to reach ESS and to show the relationship between the ESS and the benefit multiplier. Then, we verified the stability of the ESS by simulation. Finally, impact of η (step-size) on rate of convergence of equilibrium by simulating against various values of η is discussed.

5.1. Convergence to ESS

In all simulations, the common parameters setting are as follows:

$R_D = 30$, $C_D = 10$, $R_A = 50$, $C_A = 20$, $L = 10$, $R_U = 10$, $P_S = 0.2$, $P_W = 0.8$ $s = 40$ $w = 2$.

Since the metrics of cost, loss parameters and pay-off are different, we normalized all parameters to lie in range $[0, 1]$.

Fig 1. represents the color scheme followed in population graphs plotted below. By population, we mean the number of nodes following that strategy. Using the proposed model, all the nodes update their strategies. Values of benefit multipliers M_1 and M_2 are adjusted to see which ESS they converge to. In below figures, we show the convergence of the population when initial population is chosen as $(59, 15)$ corresponding to total population of $(100, 50)$. Thus, initial probability (x_0, y_0) is set as $(0.59, 0.30)$ and the benefit multipliers (M_1, M_2) are varied to see which ESS the system will converge to.

In Fig 2. , we observe that when $(M_1, M_2) = (0.2, 0.5)$ the system converges to ESS $(x^*, y^*) = (0, 0)$, which means all the adversaries choose not to Attack and defender nodes adhere to weak encryption strategy.

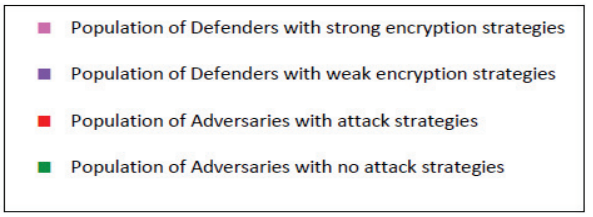
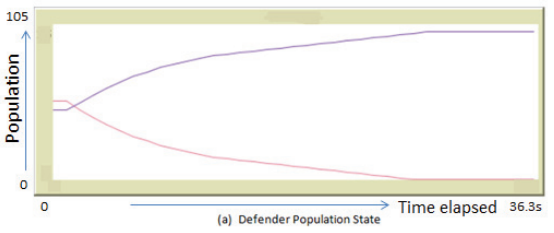


Fig. 1: Color Description



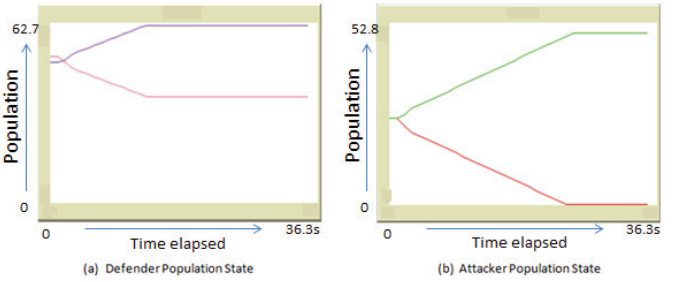


Fig. 3: Population State when $(M_1, M_2) = (1.2, 1.5)$, ESS$(0.37, 0)$

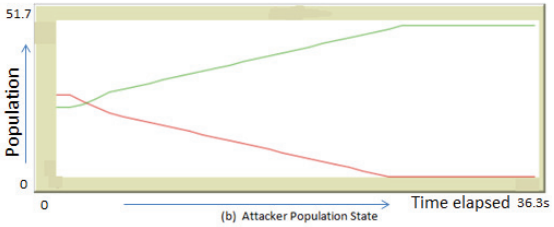


Fig. 2: Population State when $(M_1, M_2) = (0.2, 0.5)$ ESS$(0, 0)$

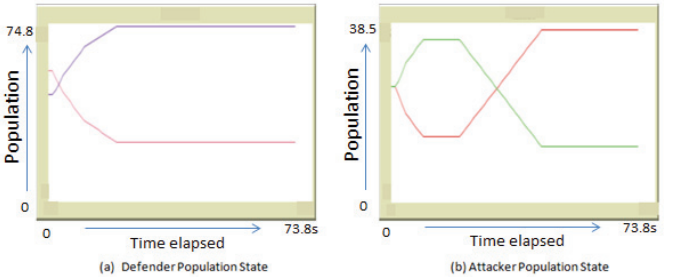


Fig. 4: Population State when $(M_1, M_2) = (0.8, 2.6)$, ESS$(0.25, 0.74)$

Consider Fig 2, Fig 3, Fig 4, Fig 5, Fig 7, it can be clearly observed that as value of M_1 (benefit multiplier for defender) increases, value of x increases i.e. defenders tend to choose strong encryption scheme. But since value of x does not depend solely on M_1 (considering equation 9 and 10) after the value of M_2 decreases beyond a certain limit it decreases x, which is clearly deducible on comparing fig 3 and fig 6, i.e. if the benefit multiplier for adversary decreases, tendency of defender to choose a strong encryption decreases.

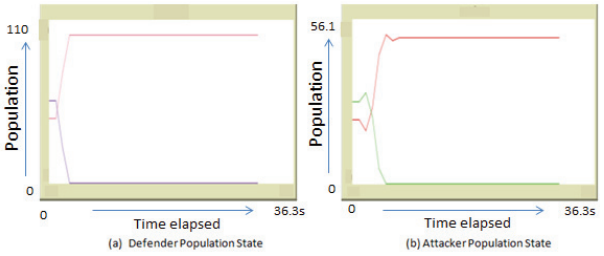


Fig. 5: Population State when $(M_1, M_2) = (13.2, -8)$ ESS$(1, 1)$

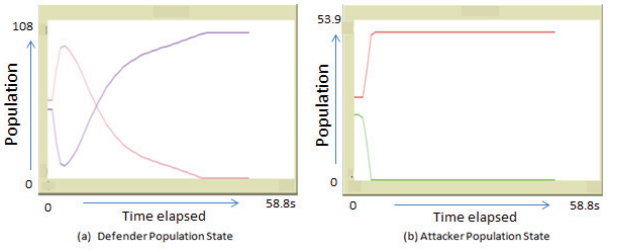


Fig. 6: Population State when $(M_1, M_2) = (8, -8)$, ESS$(0, 1)$

Value of y, i.e. tendency of an adversary to attack is independent of M_1 and depends only on M_2 (equation 11 and 12). Consider Fig 2, Fig 3, Fig 4, Fig 7,, after value of M_2 increases beyond a certain limit, value of y increases with M_2 i.e. once a min. value of benefit multiplier M_2 is reached, tendency of an adversary to attack increases. But as can

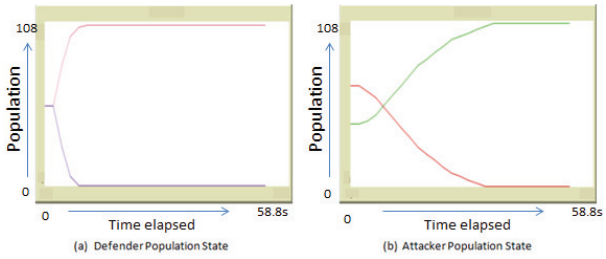


Fig. 7: Population State when $(M_1, M_2) = (12, 0.5)$, ESS$(1, 0)$

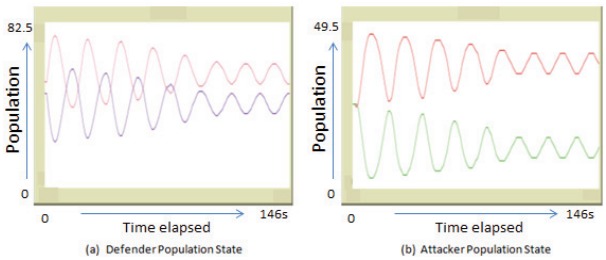


Fig. 8: Population State when $(M_1, M_2) = (6, -5)$

be seen from equation 11 and 12, value of y depends on x up to a certain extent. If value of x reaches a certain point and M_2 is negative, then decrease in M_2 increases y i.e. even if benefit multiplier of adversary is negative and if value of x is high (a lot of strongly encrypted defenders) tendency to attack increases (Fig 3, Fig 4, Fig 5).

5.2. Stability of ESS

In order to verify the stability of ESS, we let system converge to ESS (0.28, 0.74) taking $(M_1, M_2) = (0.6, 2.3)$ and then let it deviate from ESS by intentionally setting $(x, y) = (0.26, 0)$ in Fig. 10 but it can be seen both x and y quickly return to ESS after perturbation.

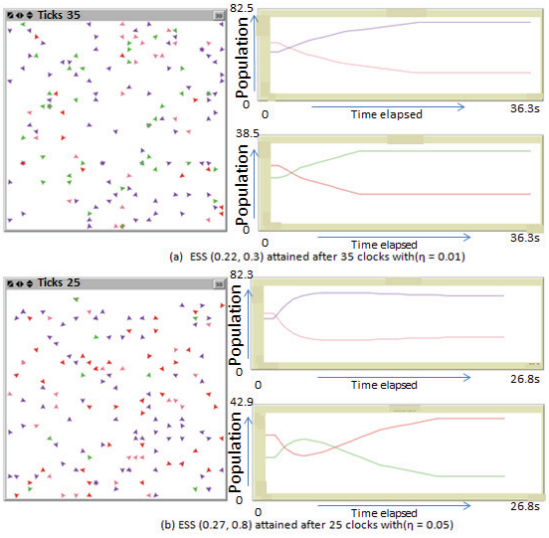


Fig. 9: Impact of η (Step-size) on Convergence Rate of ESS

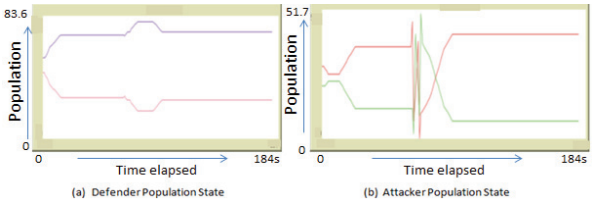


Fig. 10: Stability of ESS with $(M_1, M_2) = (0.6, 2.3)$

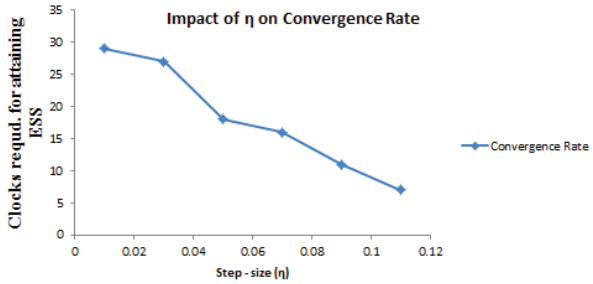


Fig. 11: Impact of η (Step-size) on Convergence Rate of ESS

5.3. Impact of η (Step Size)

To study impact of η on ESS various simulations were conducted by fluctuating the value of η and setting other parameter values as constant. Fig. 11, the plot between Convergence Rate and Step-Size is the outcome of those simulations. By analyzing the plot, we can clearly observe that Convergence Rate is directly proportional to Step-Size. We also observed that in case value of Step-Size is too high, there are chances that system will skip that particular ESS since step-size was too high and may further converge to a new ESS.

6. Discussion

The EGT based security model for dynamic selection of cryptographic protocols is an effective approach to design an evolutionarily stable WSN system in order to attain the most efficient and optimal defense. The sensor nodes dynamically select the defense strategy they want to follow in order to reach an evolutionarily stable state. The idea of using Evolutionary game theory over other theories was given more weightage owing to resource constraints, less centralization and limited rational capabilities associated with the sensor nodes deployed in the wireless sensor networks.

Currently the simulation is done with NetLogo which is more of a generic simulator, planned future work include creating a patch for NS2 network simulator so that the implementation could be verified in close to its practical application. Moreover, so far we have developed a mathematical model which depends on parameter settings to achieve an ESS, probing deeper can further lead to close mapping with real attack-defense scenario.

7. Conclusion

Heterogeneous environment conditions, frequent topology changes, resource constraints and increased demand has made wireless sensor networks a favorable choice for security attacks. For the above said reason, one policy fits all doesn't seems to be an efficient and reliable solution for the problem. Wireless sensor networks have many aspects in common with biological behaviors such as decision making, cooperation and dependence on energy conservation policies. Thus we proposed an adaptive selection of cryptographic protocols during runtime using paradigms of evolutionary game by classifying protocols into strong and weak. This paper aims to curb security issues in wireless sensor networks by proposing an adaptive approach and therefore it introduces an evolutionary game model to study mutual interactions between attackers and defenders. Further solving replicator dynamics equations of the proposed game we derived various ESSs. From simulation and theoretical results, we observed that by adjusting the constant multipliers, the population states of the network will converge to the desired ESS which is robust defense against invaders. The simulation results are in line with our theoretical analysis and support the practicality and effectiveness of the proposed model, where system converges rapidly to the ESS. Not only it converges, it also forms a stable system which was verified by deliberately destabilizing the system.

References

1. J.W Weibull, *Evolutionary Game Theory*, MIT Press, 1995.
2. David Easley and Jon Kleinberg, *Chapter 7,Evolutionary Game Theory from the book Networks, Crowds, and Markets: Reasoning about a Highly Connected World*, Cambridge University Press, 2010.
3. Ezio Vailati, *A very short intro to evolutionary game theory*, Southern Illinios University Edwardsville.
4. Shigen Shen, Guangxue Yue, Qiying Cao, *A Survey of Game Theory in Wireless Sensor Networks Security*, JOURNAL OF NETWORKS, VOL. 6, NO. 3, MARCH 2011.
5. Yihui Qiu, Zhide Chen, Li Xu, *Active Defense Model of Wireless Sensor Networks Based on Evolutionary Game Theory*, 978-1-4244-3709-2/10/ 2010 IEEE.
6. Von N, John, Oskar M, *Theory of games and economic behavior*, Princeton, NJ: Princeton University Press, pp. 36-39, 1994.
7. J. Hofbauer and K. Sigmund, *Evolutionary game dynamics*, American Mathematical Society, Vol 40 No. 4, pp. 479-519, 2003.
8. Fudenberg D, Levned K, *The theory of learning in games*, Cambridge, Mass MIT Press, pp. 167-169, 1998
9. Wei He, Chunhe Xia, Haiquan Wang, Cheng Zhang, et al, *A game theoretical attack-defense model oriented to network security risk assessment*, 2008 International Conference on Computer Science and Software Engineering, pp. 498-504, 2008.
10. Jiang Wei, Fangbin Xing, et al, *Evaluating network security and optimal active defense based on attack-defense game theory*, chinese journal of computers, Vol. 32 No. 4, 2009.
11. A. Agah, S. K. Das and K. Basu, *Preventing DoS attack in Sensor and Actor Networks: A Game Theoretic Approach*, IEEE International Conference on Communications (ICC), Seoul, Korea, pp. 3218-3222, 2005.
12. R. Cressman, *Evolutionary Dynamics and Extensive Form Games*, Cambridge MA: MIT Press, 2003.
13. D. Monderer and L. Shapley, *Potential Games," Games and Economic Behavior*, MIT Press, 1996.