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.