Journal of Computer and System Sciences 80 (2014) 1534–1548

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Dynamics stability in wireless sensor networks active defense model

Zhide Chen [a,c], Cheng Qiao [b], Yihui Qiu [a], Li Xu [a,c,*], Wei Wu [a,c]

[a] School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, 350007, China
[b] Shenzhen Institute of Advanced Technology, Chinese Academy of Science, Shenzhen, 518055, China
[c] Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou, 350007, China

ARTICLE INFO

Article history:
Received 28 January 2013
Received in revised form 21 August 2013
Accepted 10 April 2014
Available online 18 April 2014

Keywords:
Wireless sensor networks
Evolutionary
Game theory
Active defense

ABSTRACT

Wireless sensor networks, which are widely used in military, industrial and transportation fields, are vulnerable to various kinds of attacks, since they are mostly deployed in a relatively open environment. Based on the evolutionary game theory, this paper proposes a proactive defense model for wireless sensor networks, in which we emphasize that the node has a limited ability to learn the evolution of rationality from different attack strategies of the attacker, and can dynamically adjust their strategies to achieve the most effective defense. Following this approach, the cost (e.g., energy consumption and wastage of machinery) has been greatly saved and the life cycle of the nodes has been extended as well. By employing the proposed model, the whole wireless sensor network can be implemented in an effective way.

1. Introduction

1.1. Wireless sensor network

A wireless sensor network is a collection of nodes organized into a cooperative network [1]. A wireless sensor network (WSN) generally consists of a basestation (or "gateway") that can communicate with a number of wireless sensors via radio links. Data is compressed and collected at the wireless sensor node, then transmitted to the gateway directly or, if required, uses other wireless sensor nodes to forward data to the gateway. The transmitted data is then presented to the system by the gateway connection [2]. The ideal wireless sensor is networked, consuming very little power, smart and software programmable, capable of fast data acquisition, reliable and accurate over the long term, costs little to purchase and install, and requires no real maintenance. This new technology is exciting in unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces [3].

Wireless sensor networks are commonly deployed in an open, unmanned, and even enemy environment. In addition, because of the inherent power and memory limitations of sensor nodes, it is more vulnerable to a variety of potential attacks from malicious adversaries [4–7]. Recently, the security problems wireless sensor networks facing are selective forwarding, sinkhole attacks Sybil attacks and false data injection to disrupt data aggregation, etc. [8–12]. However, nearly all of the existing security solutions are passive defenses, i.e., wireless sensor networks make appropriate responses only

* Corresponding author.

http://dx.doi.org/10.1016/j.jcss.2014.04.020
0022-0000/

after attacks are detected. Apparently, it would be too late for wireless sensor networks with limited resources in energy and computing power, for the attacker may have wrecked the system before the system takes any action.

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 biology (particularly evolutionary biology and ecology), engineering, political science, international relations, computer science, and philosophy. Game theory attempts to mathematically capture behavior in strategic situations, or games, in which an individual's success in making choices depends on the choices of others. Traditional game theory is based on the fully rationality of player to analysis problems, which require the player having rational awareness, analytical reasoning ability, memory capacity, and accuracy requirements [13]. Conventional game theory emphasizes that players must not make mistakes and believe that other players also will not make mistakes through the process of the game at any times.

Due to the player is unable to meet the high demands of such fully rationality in the real environment, the application of game theory is limited in the real world. Weibull proposed the concept of evolutionary game theory systematically in the nineties of the 20th century, which abandons fully rational assumption of the classical game theory and proposes the player with bounded rationality and dynamics of the game process. Bounded rationality assumption means that the player only knows a part of knowledge of the state of the game, and is impossible to know the overall state of the game, such as the payoff, action strategies [14–16]. The player needs to learn and imitate the game continually before finding the best strategy for himself/herself, it is impossible to obtain the optimal strategy by playing the game only once.

Bounded rationality assumption satisfies the characteristics of a wireless sensor network, since a wireless sensor network is composed of a large number of nodes, the joining and leaving of regular nodes makes topology changes constantly. Actually, sensors only know part of the state in the network. For resource-constrained wireless sensor networks, it is unrealistic and unproductive to obtain and maintain the state of the entire network, as nodes need to consume a large amount of energy and storage.

1.3. Wireless sensor network using evolutionary game theory

Based on evolutionary game theory, the paper proposes an active defense model for wireless sensor networks. Dynamic evolution means that nodes can actively and dynamically adjust their defensive strategies in order to achieve the active defense, according to the attackers' different strategies. The nodes need to remain in the game during the process of learning, imitation and try to adjust their strategies at the same time, and ultimately find the best strategy for their own interests and demands. Therefore it can save the energy and other resources to extend the life cycle time of nodes in the network and the effectiveness of the whole wireless sensor networks would be greatly improved.

The rest of this paper is organized as follows. In Section 2, we introduce the latest application of game theory in the field of wireless sensor networks security. In Section 3, we define the attack–defend game model of wireless sensor networks security. Wireless sensor networks security on the principle of evolutionary game theory is analyzed in Section 4. In Section 5, we give some numerical investigations. Conclusions and future works are given in Section 6.

2. Related works

For the security challenges of wireless sensor networks, many research has been done, especially the way of using game theory to analyze wireless sensor networks which becomes a hot topic. An active defense model of wireless sensor networks has been provided in [17], while in [18], authors proposed a defense for network security assessment chart model, modeled network attacker and defender as two sides of a non-cooperative game, and finally built up proactive network security evaluation and an active defense model by selecting the optimal algorithm. Several models have been presented in [19] including defense graph model, attack–defense taxonomy and cost quantitative method, and attack–defense game model to evaluate the security of network information systems and perform active defense. Authors of [20] formulated the attack–defense problem as a two-player, nonzero-sum, non-cooperative game between an attacker and a wireless sensor, and proposed two novel schemes for preventing denial of service. The work has been extended in [21], which focuses on the assessment of the properties of security enforcement mechanisms using auction theory to prevent the DoS attacks in wireless sensor networks. In [22], based on the game theory, the author analyzes information security in the commerce, and achieves the equilibrium according to the penalty parameters of the defender and attacker.

3. A game theory model of security

Under a game theory model, we provide a mathematical description for a social situation in which two or more individuals, or players, either compete or cooperate with each other. With more than two players there may come up with a problem called collusion where some players collude with each other in the system. Game may involve several sequential steps or one step for each player. Competitive situations may be repeated or be faced only once. Information concerning the rules of engagement and the payoffs may be known to all players or imperfectly known to some.