Research on Game Model of Wireless Sensor Network Intrusion Detection

Fang Bai[1]
1.Harbin Engineering University
458683836@qq.com

Xiang Yu Liu*[1]
1.Harbin Engineering University
liuxiangyu_@hrbeu.edu.cn

Yu Lin Zhang[1]
1.Harbin Engineering University
2016212130@hrbeu.edu.cn

Da Peng Lang[1,2]
1.Harbin Engineering University
2.Key Laboratory of Network Assessment Technology, CAS
20734980@qq.com

Abstract

Wireless sensor network is widely used in commercial, agricultural, medical and military fields because of its characters of low energetic consumption, flexible configuration, and convenient deployment. However, due to its high requirement to energetic consumption and distribution, wireless sensor network is more vulnerable to be attacked. Therefore, it is more important to integrate intrusion detection system to ensure the node and network security in the wireless sensor network. Based on Game Theory, this paper models the attack and defense process in wireless sensor networks, and improves the Game Model for the intruder's diversified attack methods, so that it can accurately determine the best defensive strategy of the intrusion detection mechanism, to reduce energy consumption and improve detection efficiency; in addition, we also introduce Agent technology to increase the scalability of the system, to improve the problems caused by single point failure, and improve the fault tolerance of the system. Experiments show that the proposed method has a good effect on the scalability and intrusion detection of wireless sensor networks.

1 Introduction

1.1 Wireless Sensor Network

The wireless sensor network is a new generation of sensor networks whose development and application have far-reaching effects on various fields of human life and production. The sensor network consists of a large number of small, inexpensive, and battery-powered sensor nodes with wireless communication and monitoring capabilities. These nodes are densely deployed in the monitoring area for the purpose of monitoring the physical world. Wireless sensor network is a new research direction in information technology. It has extensive application prospects in environmental monitoring, military, homeland security, health care, household, traffic control, community security, forest fire prevention, and target location[1][2].

1.2 Research Status of Intrusion Detection Game Model

Wireless sensor networks may be deployed in extremely harsh geographical environments and lack effective protection. And the first security barriers such as identity authentication and access control built on cryptographic technologies do not ensure the absolute security of wireless sensor networks. As a proactive security protection technology, the intrusion detection system provides the ability to prevent internal and external attacks. Intrusion detection system is an active defense system for network security. As the second line of defense for network security, it plays a vital role in detecting intruders and defending attacks.

In domestic and foreign literature, game theory has been widely applied to IDS to achieve the purpose of ensuring wireless network security. Mutrali[3] established a game theory framework for packet sampling strategies to effectively detect network intrusions. Alpcan[4] proposed a game model of zero and static Markov methods for two game players to detect intrusions, using mathematical analysis to study the optimal strategy solution and assess the defense cost of the nodes. Agah[5] used the non-cooperative game framework to defend against attacks, in which three different schemes were used to find vulnerable nodes in the network and protect it. Up to now, some scholars have proposed solutions to apply game theory to WSN security strategies to reduce energy consumption [6] [7]. But most of them believe that the game is a single process and assume that the attacker has only one choice[8]. On the contrary, repeated attacks always exist in the actual WSN environment, and the attack methods are more diverse [9] [10]. Meanwhile, the adoption of game model will also lead to serious single-point failure. In order to balance the system's detection efficiency and ener-

Acknowledgements: Supported by Open Project Program of key laboratory of network assessment technology, CAS.

International Conference on Embedded Wireless Systems and Networks (EWSN) 2019
25–27 February, Beijing, China

ISBN: 978-0-9949886-3-8

gy consumption, based on the research of the existing sensor intrusion detection game model, this paper analyzes the key problems of IDS, proposes an IDS game model that conforms to the characteristics of sensor networks, and introduces the multi-agent intrusion detection method. The model can reduce the consumption of sensor resources by IDS while protecting the security of the sensor network.

1.3 Analysis of Key Problems Faced by Intrusion Detection Systems

1.3.1 Energy Consumption Problem

The sensor nodes rely on their own battery as an energy supply device. Because of the large number of sensor nodes, large distribution areas, and large geographical differences, they are usually deployed in places with harsh geographical conditions, and it is impossible to provide a sustainable energy supply.

As a security application in sensor network, wireless sensor network intrusion detection systems energy consumption has become an important bottleneck restricting its development. The traditional intrusion detection system structure and method cant be directly applied to wireless sensor networks. It is necessary to design a specific detection architecture to adapt to the low-energy wireless sensor network, which can balance system detection efficiency and node energy consumption.

1.3.2 Improve Performance

As a kind of micro embedded device, the wireless sensor node has its own computing power and storage capacity limit. With the increasing use of wireless sensor network, sensor nodes need to complete the collection and management of monitoring data. At the same time, they need to respond to and process the requests and control commands sent by the aggregation node. All of these have higher requirements on the storage capacity and processing capacity of wireless sensors.

2 Research on Multi-agent Intrusion Detection Model Based on Game Theory

The attacker tries to attack the sensor network node in order to obtain benefits. The intrusion detection system detects the intrusion procedure in order to maintain the normal operation of the system. Obviously, this is a mutually opposing game process. Each time an attacker launches an attack, it will cost a certain amount of resources. If the attack succeeds, it will gain a certain amount of revenue. Each time the intrusion detection system is turned on, it will consume the energy of the node, and the success of the detection will also yield corresponding benefits. Therefore, the network attack and defense process is simulated through the game model. This game model can find the equilibrium solution between the attacker and the intrusion detection system, and solve the energy consumption problem and performance problem faced by the intrusion detection system.

2.1 Modeling Analysis of Static Game Model for Intrusion Detection

XIONG Zi-li et al.[11] proposed a static game model for networked intrusion detection of clustered sensors. The specific process analysis of the game model modeling is as follows:

In the attack and defense model of wireless sensor networks, participants are mainly network attackers (reported as $Attacker$) and intrusion detection systems (reported as $Defender$). Information is completely perceptible to both sides of the game, that is, complete information. Let's write its decision space as Sa and Sd, and its benefit function is denoted as $R_{Attacker}$ and $R_{Defender}$. The equilibrium solution of the model is derived from the analysis of the previous four factors, so that the game model can be simply marked as:

$$G = \{(Defender, Attacker), (Sd, Sa), (R_{Defender}, R_{Defender})\}$$

It is assumed that there are N nodes in the sensor network. These nodes are divided into k clusters according to the clustering routing protocol, which are respectively recorded as $1, 2, \ldots, k$,and the number of nodes in each cluster is $Ni\,(i = 1, 2, \ldots, k)$. This article assumes that an attacker can only attack at most one cluster in each attack. The base station can only select one cluster head to start IDS in each defense. Then for a cluster $k1$ in the network, the attacker has 3 strategies: Either attack the cluster $k1$ (marked as $AS1$); either not attack any cluster (remembered as $AS2$); or select another different cluster $k2$ in the network to attack (marked as $AS3$), that is, $Sa = \{AS1, AS2, AS3\}$. For the defender, there are two strategies to choose from: either to protect the cluster $k1$ (marked as $DS1$) or to choose a different cluster $k2\,(k2 \neq k1)$ for protection (marked as $DS2$), that is, $Sd = \{DS1, DS2\}$. The gains of the two participants IDS and the attacker of the game can be represented by a 2*3 matrix, namely A and B.

In order to determine the benefit function of the attacker and defender, some symbols need to be defined, as follows:

$R(t)$: Benefits of normal operation of sensor network at time t

C_k: Average cost of IDS guard cluster k

S_k: Average cost of IDS for cluster k being successfully attacked

N_K: Number of nodes in the cluster k

$P_k(t)$: The average gain per attack by an attacker

B_k: Attacker's intrusion cost

W:the cost when the attacker waits and decide

Define the attacker's return matrix A and the income matrix of the IDS B:

$$A_{ij} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}$$

$$B_{ij} = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{bmatrix}$$

Among them: a_{11} and a_{21} indicate that the attacker attacks cluster k; a_{13} and a_{23} indicate that the attacker attacks a non-k cluster. $P_k(t) - B_k$ means that the average income of attacking a cluster is subtracted from the average loss of the attack. $b_{11} = R(t) - B_k$ indicates that both the attacker and IDS choose the same cluster for attack and defense respectively. So for IDS, its initial utility value of $R(t)$ minus the defense cost. Other strategy pairs are solved in a similar way.

So we can get the income matrix as shown below:

$$R_{Attacker} = \begin{bmatrix} R(t) - C_k & R(t) - C_k & R(t) - C_k - \sum_{i=1}^{N_{k'}} S_{k'} \\ R(t) - C_k - \sum_{i=1}^{N_k} S_k & R(t) - C_k & R(t) - C_{k'} - \sum_{i=1}^{N_{k''}} S_{k''} \end{bmatrix}$$

$$R_{Defender} = \begin{bmatrix} P_k(t) - B_k & W & P_k(t) - B_k \\ P_k(t) - B_k & W & P_k(t) - B_k \end{bmatrix}$$

Therefore, when the network attack and defense sides adopt the strategy pair $(AS1, DS1)$, the game result tends to Nash equilibrium. From the above discussion, you can get the intuition: For IDS, the best strategy is to choose the most appropriate cluster for defense, so that the value is the largest; for the attacker, the best strategy is to choose the most appropriate cluster to attack. Because it is always established, so the attacker is always encouraged to attack.

2.2 Improved Game Model for Diversified Attack Detection Based on Multi-agent Structure

Common network attacks such as DoS attacks [12] can be directly detected by using misuse detection methods. However, new network intrusion methods emerge one after another, and only using the method of intrusion rule matching does not meet the requirements of IDS. Therefore, we also need to use anomaly detection to detect network intrusions. Due to the difference in detection rules between misuse detection and anomaly detection modules, we need to develop a strategy to guide IDS to turn on the correct detection module at the appropriate time.

In addition, the single-point failure problem can occur easily in the sensor network. Once the attacker attacks the abnormal node, the intrusion detection system based on the game model will not work properly. Therefore, we introduce a intrusion detection method based on multi-agent for clustering wireless sensor network, which can effectively solve the single point failure problem of IDS based on game model.

2.2.1 An Improved Method of Agent Intrusion Detection Based on Multi-agent

According to the literature[13], this method uses multiple proxy modules to enhance the availability, security and scalability of IDS by allowing member nodes and cluster heads to perform different tasks. However, this scheme proposed by the author requires that every node should be equipped with monitoring Agent, detection Agent, response Agent and management Agent, which will occupy a large amount of storage space of nodes and cluster heads, and also increase the energy loss of nodes. When the test activities overlap, the detection accuracy will be greatly reduced.

In this regard, we propose an improved method based on multi-agent Agent intrusion detection. In view of the intrusion detection method based on game model, the purpose of introducing multi-agent Agent intrusion detection method is to solve the single-point failure problem. Therefore, the corresponding Agents may not be configured for the member nodes, but only for the cluster heads, so that the cluster heads can effectively find and solve the single point failure problem based on mutual communication. The following describes this improved method in detail:

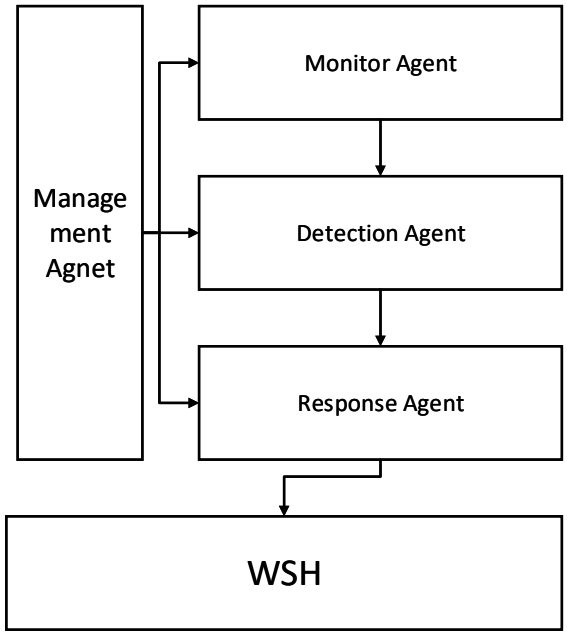

Figure 1. System structure diagram.

The system structure of agent intrusion detection method based on multi-agent is shown in Figure 1.

This method configures a monitoring agent, a detection agent, a response agent and a management agent on each sensor cluster head. The monitoring agent is responsible for monitoring the behavior information of the neighbor cluster heads. After the data is merged and extracted, the information is sent to the detection agent residing on the cluster head, and the detection agent performs the next processing. The detection agent is responsible for analyzing the data information collected by the monitoring agent to determine whether or not intrusion detection occurs. In this part, this paper adopts the intrusion detection method based on game model with the ability to deal with diversified attacks mentioned below. The response agent will activate immediately when the detection agent discovers and judges that an intrusion occurs. And the response agent takes response measures according to the specific situation, such as reducing the trust degree to the suspicious cluster head, cutting off the communication between the other party and itself, updating the communication key, and re-authenticating the identity, etc. The management agent is responsible for managing and maintaining the monitoring agent, detection agent, and response agent, and coordinating their work.

For ease of presentation, make the following notation and definition:

H: The number of cluster heads involved in communication in sensor network

L: The trust between cluster heads, each cluster head stores the trust degree of the neighbor cluster head, $0 < L < 1$

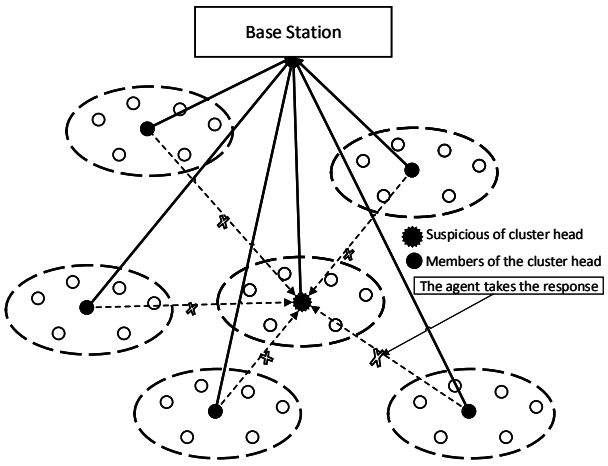

Figure 2. Response agent takes the response.

α: The threshold of trust depends on the security requirements of the network in the actual application. The higher the level of network security is , the larger the value of α is, which is generally considered to be the value $0 < \alpha < 0.5$

β: The percentage of trust reduction, $0 < \beta < 1$. The value is related to the number of cluster heads.

Every time cluster head k' receives a query report on cluster head k, k' reduces its trust rate on cluster head k by a certain percentage. If let X represents the trust of cluster head $k$after k' receiving $x(2 < x < H)$ query reports, it can be described as follows:

$$L_x = (1-\beta^H)(1-\beta^{H-1})...(1-\beta^{H+1-X})L_0$$

When $L < \alpha$, the node concludes that the cluster head is a malicious node and will take corresponding response measures. Here, the node actively cuts off the connection with the cluster head and refuses to communicate with the cluster head. Figure 2 shows the situation in which the neighbor cluster head receives a certain number of challenge reports so that its trust in the cluster head is reduced below α.

2.2.2 Constructing a Diversified Attack Detection Game Model

For a fixed cluster k, the attacker has two strategies: choose common attacks, such as DoS attacks(marked as a_1). Or choose a new type of attack (marked as a_2). IDS also has two strategies: use misuse detection module (marked as d_1); or use Anomaly detection module (marked as d_2). Then there are four kinds of game strategies: $(d_1,a_1);(d_1,a_2);(d_2,a_1);(d_2,a_2)$.

Now, set the average detection accuracy of common network attacks using misuse detection methods to n. And set the average detection accuracy of the new attack using the anomaly detection method to m. According to the definition of misuse detection and anomaly detection, we can judge that the accuracy of using the abnormal detection method to detect common attack and using the misuse detection method to detect new attack is zero.

When selecting a policy, the attacker chooses to use the common attack method to attack, and the defender uses the misuse detection method for intrusion detection. Then we can get the total benefit function of the attacker and the defender respectively:

$$\begin{aligned} &R_{11}(Attacker) = (1-n)(p_k(t)-B_k) - nB(k) \\ &= P_k(t) - B_k - np_k(t) - nB_k + nB_k \\ &= P_k(t) - B_K - np_k(t) \end{aligned}$$

$$\begin{aligned} &R_{11}(Attacker) = (1-n)(p_k(t)-B_k) - nB(k) \\ &= P_k(t) - B_k - np_k(t) - nB_k + nB_k \\ &= P_k(t) - B_K - np_k(t) \end{aligned}$$

Similarly, we can get the total benefit function of the attacker and defender in the other three sets of strategies. After sorting out, we can get the bivariate benefit matrix of the game:

$$X = \begin{bmatrix} P_k(t) - B_K - nP_k(t) & P_k(t) - B_k \\ P_k(t) - B_k & P_k(t) - B_K - nP_k(t) \end{bmatrix}$$

$$Y = \begin{bmatrix} R(t) - C_k - P_k(t) + nP_k(t) & R(t) - C_k - P_k(t) \\ R(t) - C_k - P_k(t) & R(t) - C_k - P_k(t) + mP_k(t) \end{bmatrix}$$

In order to get the defender's defensive strategy, we need to set the defender's probability of performing misuse detection to be r, and the probability of performing anomaly detection is 1-r. The probability of an attacker using a common attack method is s, and the probability of using a new attack mode is 1-s. What we want to know is that how much r and s are respectively, the attacker and defender have the largest value of the benefit function. The total benefit function of the attacker and the defender can be obtained according to the bivariate matrix we have obtained:

$$R_{Defender} = R(t) - C_K - P_k(t)[1 - nrs - (1-r)(1-s)m]$$

$$R_{Attacker} = [1 - nrs - (1-r)(1-s)m]P_k(t) - B_k$$

2.2.3 Nash Equilibrium Analysis

Now we carry out Nash equilibrium analysis for the total benefit function of the attacker and the defender, and the solving process is as follows:

Differentiate $R_{Defender}$ on r get $[(n+m)s - m]P_k(t) = 0$. that is, $s = \frac{m}{n+m}$.

Similarly, differentiate $R_{Attacker}$ on s get $[(m-(n+m)r]P_k(t) = 0$. that is, $r = \frac{m}{n+m}$.

Get the defender's strategy $T_{Defneder}$ and Attacker's strategy $T_{Attacker}$ are: $T_{Defneder} = (\frac{m}{n+m}, \frac{n}{n+m})$, $T_{Attacker} = (\frac{m}{n+m}, \frac{n}{n+m})$.

That is, both of the attacker and the defender use the $\frac{m}{n+m}$ probability to attack in a common way and detect it by misuse detection method. And both of the attacker and the defender use the $\frac{n}{n+m}$ probability to attack in a new way and detect it by anomaly detection method.

The above $T_{Defneder}$ and $T_{Attacker}$ are the Nash equilibrium solutions of defenders and attackers. When r and s take a value of $\frac{m}{n+m}$, defenders and attackers gain maximum.

3 Experimental Verification

In the range of 150m*150m, 120 nodes are randomly deployed, and the initial energy of each node is set to 0.6J,

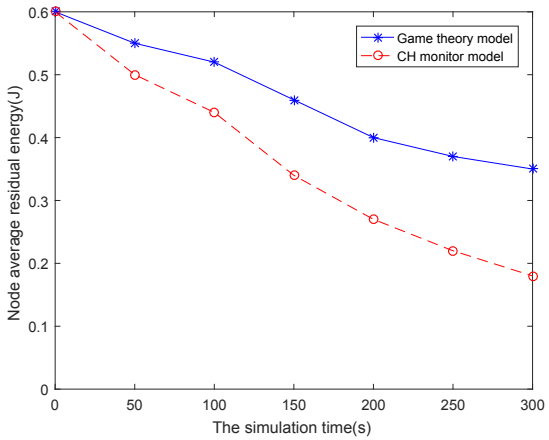

Figure 3. Energy consumption diagram.

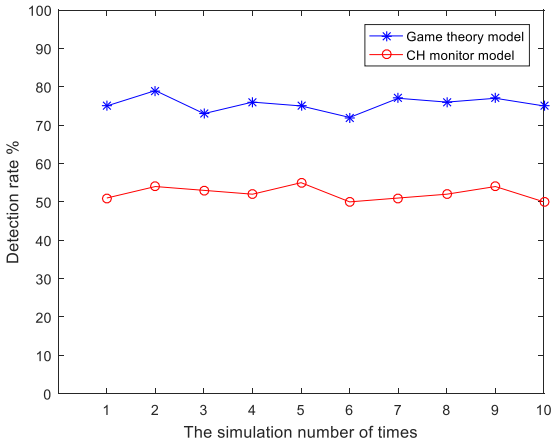

Figure 4. Detection performance diagram.

the node cannot be moved once deployed, and the simulation maintained for 5 minutes. During the experiments, the multi agent of attack and defense game model improved in this paper is introduced to compare the intrusion detection capabilities, and the energy consumption is compared with the full monitoring detection model.

Literature[14] believed that 70% of the energy of wireless sensor networks were used for data transmission. However, data transmission relies on wireless broadcasting, and reducing usage of wireless communication means decreasing energy consumption. In the processes of experiments, the energy consumption of the intrusion detection system based on the game model greatly reduced compared to the intrusion detection system of the full monitoring mode. As shown in Figure 3, at the beginning of the test, the average residual energy of the nodes is the initial value, 0.6J. With the increase of time, the energy consumption of the two detection systems has changed significantly; when the time is 300s, energy consumption of the improved system was reduced by 41% than the monitoring system. Therefore, the multi-agent based multi-attack detection game model effectively solves the problem of efficiency detection and energy consumption.

The detection performance of the multi-agent based intrusion detection game model was evaluated. The simulation experiment was repeated 10 times, the experimental conditions are the same, and recorded the detection rate of each detection model. Changed the experimental conditions, the simulation of the cluster head node performed the IDS attack and defense game model, also 10 times, and recorded the detection rate of the simulation experiment. The comparison of the detection performance of the two models was shown in Figure 4.

It can be seen from the figure that the detection rate of the cluster head CH performing the IDS game model[15] was between 50% and 60%, and the detection rate was about 55% in most cases, and the detection performance is unstable. The detection rate of multi-agent based multi-attack detection game model proposed in this paper was between 70% and 80%, The detection rate is relatively stable and the model showed higher security performance.

4 Conclusions

On account of huge applicable value of wireless sensor networks, the related network intrusion problems are attracting more and more attention. Most of the existing intrusion detection systems at home and abroad only have a high detection rate for specific attack methods, and seems powerless for other attacks, and easy to take place problem of a single point of failure. The intrusion detection system increases the system's energy consumption while protecting the system. In this paper, we focused on the intrusion detection algorithm in wireless sensor networks, and combined game theory and non-cooperative complete information static game principle, to construct the intrusion detection model in wireless sensor networks. The multi-agent based intrusion detection method was introduced and improved. The effectiveness of the new model was verified through simulation experiments.

Game theory and multi-agent technology also provide feasible new ideas and new technologies for the research of many key issues in various of aspects of wireless sensor network security. Both of them are significant and bright research directions.

5 References

[1] Hai-Fei Si, Zhong Yang, and Jun Wang. Review on research status and application of wireless sensor networks [j]. *Journal of Mechanical & Electrical Engineering*, 1:006, 2011.

[2] Zhi-ling Ren, Guang-quan Zhang, Dong Lin, Zhong-bao Zhang, and Xing Zhao. Review on application of wsns. *Transducer and Microsystem Technologies*, 37:1–3, 2018.

[3] Murali Kodialam and TV Lakshman. Detecting network intrusions via a sampling: a game theoretic approach. In *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, volume 3, pages 1880–1889. IEEE, 2003.

[4] Tansu Alpcan and Tamer Basar. An intrusion detection game with limited observations. In *Proceedings of the 12th Int. Symp. on Dynamic Games and Applications*, 2006.

[5] Afrand Agah, Sajal K Das, Kalyan Basu, and Mehran Asadi. Intrusion detection in sensor networks: A non-cooperative game approach. In *null*, pages 343–346. IEEE, 2004.

[6] Hossein Jadidoleslamy. Designing an agent-based intrusion detection system for heterogeneous wireless sensor networks: Robust, fault tol-

erant and dynamic reconfigurable. *International Journal of Communications, Network and System Sciences*, 4(08):523, 2011.

[7] Chi-Ming Wong, Chih-Fong Chang, and Bih-Hwang Lee. A simple time shift scheme for beacon broadcasting based on cluster-tree ieee 802.15. 4 low-rate wpans. *Wireless personal communications*, 72(4):2837–2848, 2013.

[8] Knut Ovsthus, Lars M Kristensen, et al. An industrial perspective on wireless sensor networksa survey of requirements, protocols, and challenges. *IEEE communications surveys & tutorials*, 16(3):1391–1412, 2014.

[9] Jamal N Al-Karaki and Ahmed E Kamal. Routing techniques in wireless sensor networks: a survey. *IEEE wireless communications*, 11(6):6–28, 2004.

[10] Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. Wireless sensor networks: a survey. *Computer networks*, 38(4):393–422, 2002.

[11] Lansheng Han, Man Zhou, Wenjing Jia, Zakaria Dalil, and Xingbo Xu. Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model. *Information Sciences*, 2018.

[12] Maryam Mohi, Ali Movaghar, and Pooya Moradian Zadeh. A bayesian game approach for preventing dos attacks in wireless sensor networks. In *Proceedings of the 2009 WRI International Conference on Communications and Mobile Computing*, pages 507–511, 2009.

[13] Xue Tingmei and Shi Zhiqiang. Multi-agent based intrusion detection system for wireless sensor networks. *system*, 8:9, 2012.

[14] Hasan Çam, Suat Ozdemir, Devasenapathy Muthuavinashiappan, and Prashant Nair. Energy efficient security protocol for wireless sensor networks. In *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*, volume 5, pages 2981–2984. IEEE, 2003.

[15] Michael Krishnan. Intrusion detection in wireless sensor networks. *walrandpc. eecs. berkeley. edu/228S06/Projects/KrishnanProject. pdf*, 2006.