Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8819545, 9 pages
https://doi.org/10.1155/2020/8819545

Research Article

Intrusion Detection into Cloud-Fog-Based IoT Networks Using Game Theory

Poria Pirozmand,[1] **Mohsen Angoraj Ghafary**,[2] **Safieh Siadat**,[2] **and Jiankang Ren**[3]

[1]*School of Computer and Software, Dalian Neusoft University of Information, Dalian 116023, China*
[2]*Department of Computer Engineering and Information Technology, Payame Noor University (PNU), P.O. Box 19395-4697 Tehran, Iran*
[3]*School of Computer Science and Technology, Dalian University of Technology, China*

Correspondence should be addressed to Safieh Siadat; safieh.siadat@gmail.com

Received 11 April 2020; Revised 25 September 2020; Accepted 27 October 2020; Published 16 November 2020

Academic Editor: Fawad Zaman

The Internet of Things is an emerging technology that integrates the Internet and physical smart objects. This technology currently is used in many areas of human life, including education, agriculture, medicine, military and industrial processes, and trade. Integrating real-world objects with the Internet can pose security threats to many of our day-to-day activities. Intrusion detection systems (IDS) can be used in this technology as one of the security methods. In intrusion detection systems, early and correct detection (with high accuracy) of intrusions is considered very important. In this research, game theory is used to develop the performance of intrusion detection systems. In the proposed method, the attacker infiltration mode and the behavior of the intrusion detection system as a two-player and nonparticipatory dynamic game are completely analyzed and Nash equilibrium solution is used to create specific subgames. During the simulation performed using MATLAB software, various parameters were examined using the definitions of game theory and Nash equilibrium to extract the parameters that had the most accurate detection results. The results obtained from the simulation of the proposed method showed that the use of intrusion detection systems in the Internet of Things based on cloud-fog can be very effective in identifying attacks with the least amount of errors in this network.

1. Introduction

Advances in various technologies like sensors, wireless communications, hidden computing, automatic detection and tracking, extensive Internet access, and distributed services enhance the potential for the integration of intelligent things in our daily lives through the Internet. The convergence of the Internet and intelligent things that can communicate and interact with each other is defined as the Internet of Things (IoT). [1].

However, integrating real-world smart objects with the Internet may pose security threats in many of our daily activities, too [2].

Given the wide range of standards and communication stacks, limited computing power, and the large number of interconnected devices, common security measures against threats cannot effectively operate in Internet of Things (IoT) systems. Accordingly, it is essential to develop certain security solutions by means of mathematical methods and statistical points for the IoT, to make it possible for the users of organizations to carefully analyze and detect all the weaknesses of the system in this way [3].

Due to widespread communication standards and stacks, limited computing power, and a high number of interconnected devices, common security measures against threats cannot be effective in IoT systems. For this reason, it is necessary to develop specific security solutions for the IoT, to allow users of organizations to identify all the weaknesses of the system [3].

Some of the ongoing projects to improve the security of the IoT include methods providing confidentiality of data and authentication, access control within the IoT network,

privacy, and trust between users and things, as well as the implementation of security and privacy policies [Sicari, et al., 2010]. Nevertheless, even with these methods, IoT networks are vulnerable to multiple attacks designed to disrupt and destroy these networks. Thus, one of the required defense methods is to design methods detecting attackers. Intrusion detection systems are for this purpose.

Security concepts are being considered with the rapid growth of IoT technology applications. Concerns are raised about intrusion, privacy, and people's inability to control their personal lives. If people's daily activities are monitored and they produce information outputs, political, economic, and social activities will be affected. The benefits of IoT technology will diminish in case of security breaches, attacks, or malfunctions [4].

Given the security challenges in the virtual world and the emerging technology of the IoT and due to the challenges of infiltrating these systems, it is significant to provide an optimal way to detect intrusion and maintain security in these systems.

Therefore, to deal with intruders and attackers on computer systems and networks, several methods have been developed called intrusion detection methods, responsible for monitoring the events occurring in a computer system or network. In the current study, the following sections are considered to achieve the objectives and provide an efficient mathematical model in intrusion detection systems. The research background is presented in the second section, and the statement of the problem is given in the third section. Modeling and definition of game parameters, information, and the used data are stated in the fourth section. The fifth and sixth sections present the results using the findings obtained, while analyzing, evaluating, and implementing; ultimately, the effective suggestions are presented in the seventh section.

2. Related Works

Over recent years, various papers and methods based on game theory in the field of computer network security have been published to model, analyze, and optimize the performance and efficiency of intrusion detection systems in IoT-related technologies like ad hoc mobile networks ([5]; Mishra et al., 2014), wireless sensor networks (Buton et al., 2016; [6]), cloud computing [7], and physical cyber systems [8].

The report by Moudi et al. [7] provided a variety of intrusions affecting accessibility, confidentiality, and integration in cloud computing. The authors of this reference have divided the intrusion detection system technology used in cloud into three categories: host-based, network-based, and hyper-based systems (virtual machine monitor). Moreover, they have discussed the pros and cons of each protocol and identified challenges to make cloud computing a reliable platform for providing IoT services.

The results of a study by Midi et al. [9] reveal that an intrusion detection system is able to monitor and control multiple communication protocols, a combination of signature rules, and anomaly detection processes.

Buton et al. [10] performed an extensive study of intrusion detection systems in wireless sensor networks and made a comparative analysis between the intrusion detection systems provided for wireless sensor networks given the network architecture and detection methods.

Granjal et al. [11] presented a comprehensive security analysis of several Internet protocols. More specifically, they checked IEEE802.15.4 security issues on low-power wireless regional networks (6LoWPAN), IPv6 routing protocols for low-power and lossy networks (RPL), Datagram Transport Layer Security (DTLS), and constrained application protocols (CoAP).

Goa et al. (2016) addressed a two-step hybrid approach first examining the initial diagnosis of whether or not the data is invasive using the K-means cluster and then, at the second stage, finally diagnosing the closest neighbor using the K algorithm.

Kumar and Dota [5] have examined the intrusion detection methods provided for mobile ad hoc networks through focusing on their detection algorithms. They have introduced a tree classification for intrusion detection methods based on the nature of the processing method used in the detection method.

Walgren et al. (2017) have provided an intrusion detection system for LOWPAN-RPL6 networks able to detect Sinkhole, Sybil, and Selective attacks using a hybrid approach connecting various parameters.

Atli and Jung [12] have developed an intrusion detection system based on the characteristics of the supervisor as well as the use of the leading neural network. Their paper gives a brief overview on ISCX-IDS 2012 and CIC Android. To perform the phase, SVM feature selection has been used with incremental learning; the rankings selected 20 features with the highest ranking out of 43 features in the data set, and then using the neural network, the final diagnosis was 94% to 98.7% accurate.

Shen et al. [13] have provided an optimal framework for demonstrating the potential and practical application of malware repression to protect the privacy of smart things on IoT networks through an intrusion detection system with theoretical calculation of the Bayesian game.

Pagitus et al. (2019) have investigated the security of the IoT, its challenges, threats, and its solutions. After reviewing and assessing the potential threats and determining security measures and requirements in the field of IoT, they have performed a quantitative and qualitative risk analysis examining security threats at each layer.

In their study titled "A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection," Susan and Rayford (2019) have developed a model for IDS distributed with a network of sensors, in addition to suggesting two plans independent from the flexible platform based on game theory techniques. In the presented plan, through implementing participatory game theory, Shapley values have been especially used for analysis and configuration; Nash equilibrium solutions have been obtained by means of analysis method and analyzed for the defined game security.

In their review paper, Hajiheidari et al. (2019) have comprehensively investigated the IDSS in IoT networks. The

research systematically investigates IDSS with a precise classification, considering the common features of IoT tools, analyzes the advantages and disadvantages of these mechanisms and guidelines, and finally presents future trends.

In their study entitled "Deep Learning Approaches for Anomaly- based Intrusion Detection Systems," Arwa et al. (2020) discussed on the efficiency and effectiveness of the proposed methods through analyzing the solutions and experimental studies and by employing the role of deep learning in detecting the intrusion. Deep-learning-based guidelines and identifiers are recommended by identifying the challenges of past research.

Wenjua et al. (2019) have designed a participatory blockchain signature-based intrusion detection model that can be used as a general framework for signature-based IDS for security sharing and reliable database building.

Research efforts on intrusion detection devices for the IoT have started and accelerated. Considering the provided research backgrounds, it is worth noting that the proposed solutions have not investigated the strengths and weaknesses of each method of diagnosis and strategy in depth. Most authors have focused on a few types of IoT attacks and technologies. Ultimately, very simple accreditation strategies have provided the basis for reproducing other proposed approaches.

3. Problem Definition

In fact, intrusion detection is the process of identifying intruders and attackers into information systems. Known as infiltration, these measures are taken aiming at unauthorized access to computer systems. Intruders may be internal or external users. Internal intruders are in fact network users with varying degrees of access trying to increase the level of access and privileges to exploit unauthorized privileges. External intruders are actually users outside the target network trying to gain unauthorized access to system information.

The intrusion detection system includes sensors, an analytical engine, and a reporting system. The sensors are located in different locations or hosts of the network. Their function is to collect network or host data such as traffic statistics, packet headers, and service requests, besides operating system calls, placed in different locations according to network architecture. Sensors send the collected data to the analytical engine, which is responsible for investigating the collected data and detecting the ongoing infiltration with various signature-based, anomaly-based, feature-based, and combination-based approaches. When the analytical engine detects an intrusion, it will equip the reporting system with infiltration information, including intruder detection, intrusion location, and intrusion time and type, and the system will generate an alert for the network manager [Shen & Huang, 2019].

Classified into three strategies: centralized, distributed, and hybrid, in IoT networks, the intrusion detection systems may be placed in different strategies, in one or more specific hosts, or in any physical thing.

In centralized mode, intrusion detection system's agents are deployed in a centralized component, for example, a border router or a dedicated host. However, due to the need for intrusion detection system's agents to collect many data from smart things, this mode establishes a connection between smart things and the border router. In distributed locating strategy mode, intrusion detection systems are placed on each physical thing, which can obviously decline the above connection while increasing the capacity to consume limited resources of smart things. Nevertheless, unlike the two mentioned modes, infiltration detection system's hybrid agents are deployed in nodes or monitoring nodes, for instance, the guard nodes to take the advantage of centralized and distributed strategies and prevent their weaknesses. This strategy may reduce the requirements for communication between smart things and the boundary router and meet more processing capacity [Shen & Huang, 2019].

Figure 1 shows the independent layers, hardware, and software of the agent, as well as how to deploy and influence intrusion detection systems, indicating that intrusion detection systems in cloud fog-based IoT can be located on a border router in one or more dedicated hosts, or in any physical thing [13].

Today, various measures have been taken to establish security, communications, and information exchange in cyberspace, including data encryption, secure protocol design, and the use of firewalls, tracking systems, and intrusion detection prevention systems. In some network security methods like intrusion tracking systems or firewalls, a decision-making process based on certain data is required to set a specific security policy on the network. Various mathematical tools have been used so far to perform such processes in network security systems and optimize them, such as statistical methods of hypothesis testing, decision theory, pattern identification method, machine learning, graph theory, and control theory.

However, since in many security incidents on the network, the attacker is a human being or a smart program, a method is needed that can decide how a smart attacker can make decisions in order to appropriately change the strategy of his attackers in proportion to the precautionary and model countermeasures. Accordingly, in recent decades, some efforts have been made to apply the game theory to network security.

Since game theory was originally created to model and optimize decision-making in situations where a number of smart factors compete or interact with each other, it is a good tool to be used in many issues related to network security. This theory has been so far used in issues like the optimal allocation of resources, the safe design of network topology, and the optimal configuration of intrusion tracking systems, as well as firewalls.

Given the large volume of data faced by an intrusion detection system, the application of a powerful tool able to enable an intrusion detection system to achieve the desired result by exploring the vast amount of network data is inevitable. The use of game-theory-based systems is one of the powerful tools. Game theory has gained great success in solving the optimization of resources and costs in the economic

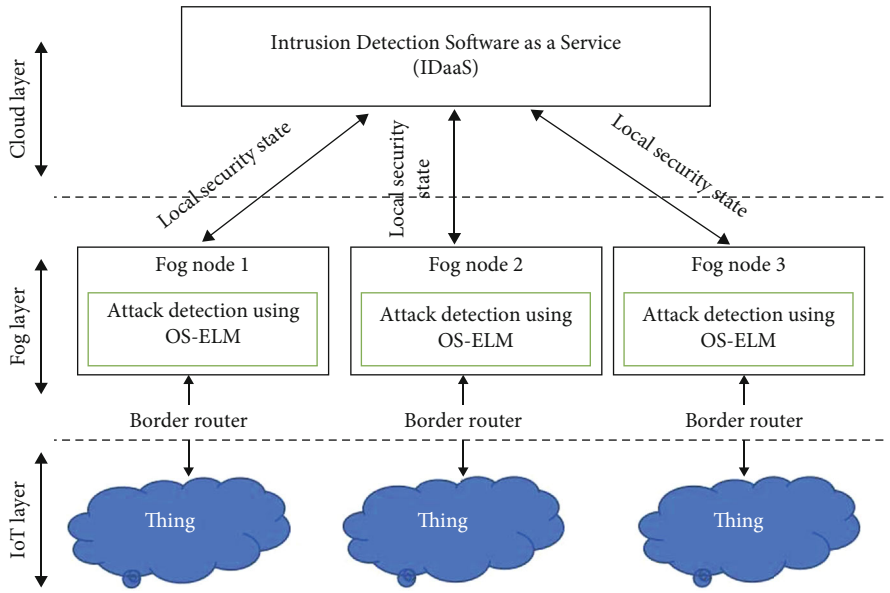

Figure 1: Infrastructures of intrusion detection system for cloud fog-based IoT networks.

field. Accordingly, in recent years, it has been considered by researchers in other fields, too [14].

Game theory is based on the behavior of each player, and it can be based on cooperation or noncooperation in a participatory game [14].

In recent years, the provision of mathematical inferences for wireless networks has become very popular by means of game theory methods. Since game theory is a natural and flexible tool for studying the intelligent and decision-making users, the interaction and cooperation of automated users in wireless networks may be examined with this tool [Pavlidou & Pavlidov, 2010]. Hence, if the issue of security and intrusion detection is investigated from the perspective of game theory, common points between this issue and the models may be gained in this theory.

Detection tools and placement strategy are among important specifications of intrusion detection systems. The studied and analyzed papers point to a general consensus indicating that the game theory and finding the best solution through Nash equilibrium are the most important tools to detect attacks against intrusion detection systems in IoT. However, although the game models proposed to detect IoT intrusion attacks have many similarities, they fundamentally differ from each other in the scope of attack detection. Despite lots of potential attacks against IoT networks, the proposed game model for the intrusion detection system is capable of detecting more attacks simultaneously.

In the proposed model, a mathematical pattern is presented to detect more classes of attacks and correct detection rate and to minimize incorrect detection rate using game theory.

Considering research gap in other studies, in the proposed model, we put emphasis on the lowest amount of error and it can be observed that by considering the dissemination rate parameter and the possibility of the next infraction for a smart object, which is an effective indicator on a smart object behavior, the error and time problem is significantly taken into account and resolved. This way, the smart sensor series detect the attacking smart object *faster and more accurately* and avoid malware dissemination in the IoT network layers.

In the present study, we aimed to model the interactions between attackers and the intrusion detection system as a dynamic two-player game. In game theory, nonparticipatory game is a game in which players may not exchange or negotiate with each other and reach an agreement or form a coalition in any way.

The selection and use of nonparticipatory game are due to the nature of the interactions between the intrusion detection system and the IoT network subsystems. These interactions are indeed a dynamic game with complete information, in which the intrusion detection system is uncertain about the type of player's performance.

4. Information and Data

The main elements in game theory include players, actions, profits, and information, all of which are known as the rules of the game.

The objective in modeling using game theory is to design a situation based on the rules of the game in order to determine what will happen in a specific situation. Game theory is based on the behavior of each player, and players strive to increase their profits in the game and make decisions called strategies [Behounek, 2016]. Accordingly, game theory may be defined as the science of modeling and investigating decision-making systems.

In the current study, dynamic game modeling is defined based on time, completely and strategically according to the information, and the following two conditions have been observed and considered in the proposed model:

(1) Players are fully aware of all the parameters and rules of the game

(2) At least one of the players is unaware of the strategy of the other player; hence, the first player first makes his move, then the second player chooses his move when he is aware of the selected move (operator) of the first player

Defining the players and determining their preferences through the profit function are two of the key elements in describing the game. In the proposed game model, the player is a potential attacker and the other player, the defender of the intrusion detection system.

(i) Players: $\mathcal{N} = \{\text{possible attacker, intrusion detection system}\}$

(ii) First player strategy: $\mathcal{S}_1 = \{\text{attack, no attack}\}$

(iii) Second player strategy: $\mathcal{S}_2 = \{\text{alert by detection, no alert}\}$

Given the provided definitions, we consider the intrusion detection system with the network of sensors $S = \{S_1, S_2, \cdots, S_p\}$, where the sensors are defined as an operating software, reporting the possible attacks in the large subsystem of IoT using a variety of signature-based, anomaly-based, feature-based, and hybrid-based approaches. Alerts reported by the intrusion detection system may be displayed as a set of subsystems, including computer programs or network components, as well as the independent processes distributed across multiple hosts as $A = \{a_1, a_2, \cdots, a_M\}$ which are the target of an attacker. We define the set $T = \{t_1, t_2, \cdots, t_K\}$ as a set of recorded recognizable threats that each member of the set represents a possible intrusion. The properties of one of the T elements can be described by assigning it to one or more classes of the function between $\{F_1, F_2, \cdots\}$ that each class of the function F represents a common property of its members.

In order to be able to detect more than one intrusion by the sensors, by mapping from the S set to the $T \cup \{0\}$ set, the sensor output vector $d = \{d_1, d_2, \cdots, d_L\}$ is defined, so that $L \geq P$. The element i, the output vector associated with the $s_j \epsilon S$ sensor, in the form of $d_1(s_j)$, is equal to one, if the sensor has detected the possible intrusion of $T_k \epsilon T$; otherwise, $d_1(s_j) = 0$.

Given the above argument and since each smart sensor may report a maximum of one of any possible intrusions, we will have

$$d_i(s_k) \neq d_j(s_k), \quad \perp i, j, k > 0 s_k \epsilon S, \tag{1}$$

$$\text{Unless, } d_1(s_k) \neq d_j(s_k). \tag{2}$$

Now, using the definitions and hypotheses of the game, the matrix of the M system is defined by describing the relationship between the output vector of the sensor j and the subsystem i as the matrix (3):

$$M_{i,j} = \begin{cases} 1, & \text{if the sensor } j \text{ alerts for intrusion } i, \\ 0, & \text{if the sensor } j \text{ does not alert for intrusion } i. \end{cases} \tag{3}$$

In Figure 2, the parameters t_1, t_2, and t_3 are as threat targets of subsystems 1, 2, and 3 by the attacker; nt_1 and nt_2 identify the operator of not attacking by the attacker; a_1, a_2, and a_3 warnings show the intrusion detection system alerts for relevant subsystems; and na_1 and na_2 indicate an alert from the intrusion detection system.

The tree modeled in Figure 2, representing an example of the proposed game with two information sets and three subsystems, may be studied by a reversible method. In the first set of information, where the threat t_1 defined by the attacker targets the first subsystem, or does nothing (nt_1), the whole applications of the intrusion detection system are an alert report for the first subsystem with a_1 identifier or not sending an alert with a_2 identifier. Consequently, using the game tree, Figure 2 and definitions may be employed to show the matrix of 2×2 games and how the strategies work in Table 1.

Always $\alpha, \beta \geq 0$.

The parameters Q_{IDS} and Q_{Attack} defined in Table 1 represent the values of the profit function of each player and similar rows and columns like the matrix, performance, strategy spaces of the players, the intrusion detection, and attack system. The $-\alpha_h$ value is the gain of the intrusion detection system for the target detection alert report. On the other hand, α_f and α_m indicate the costs of the detection system for false alarms and attack loss. The cost of β_h shows the penalty for the attacker, and $-\beta_s$ shows the gain of an undetected intrusion.

As a result, strategies of the player's intrusion detection system depend on the relative values of α_f and α_m and false alerts and the cost of losing an attack and threat. If $\alpha_f > \alpha_m$, then the intrusion detection system will not have an alert ($n\alpha$ identifier), and in the other case, if $\alpha_f > \alpha_m$, then the intrusion detection system will always specify an alert (α identifier).

5. Finding the Best Response and Analyzing the Nash of the Game

The study of Nash equilibrium existence in a game has two advantages. First, if we have a game with Nash equilibrium assumptions, we can hope that the attempt to find balance will be successful. The second and the more important is that the existence of equilibrium indicates that the game is compatible with the mode-space solution. Moreover, the equilibrium existence for a family of games allows us to study their properties without finding them explicitly or being faced with the risk of studying an empty collection.

The presence of Nash equilibrium in the Q_{IDS} matrix is investigated. We develop the results by considering strategies similar to those players defined in the form of probability distributions on the space of certain strategies. It is supposed that P_1 and $1 - P_1$ are the probabilities of the t_1 and nt_1 strategies of the attacking player and that q_1 and $1 - q_1$ are the

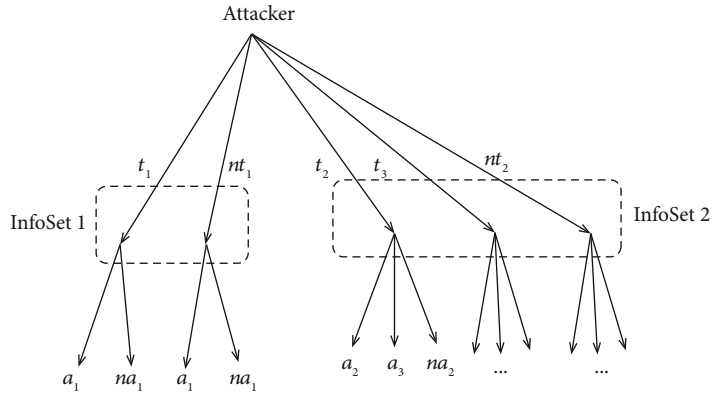

Figure 2: The extended form of the game with 2 information sets and 3 subsystems.

Table 1: Parametric description of similar strategies of the first database.

	t_1	β_h	$-\beta_s$		t_1	$-a_h$	α_m
Q_{Attack}	nt_1	0	0	Q_{IDS}	nt_1	a_f	0
		a_1	na_1			a_1	na_1

probabilities of the strategies a_1 and na_1 of the intrusion detection system. Pair (P^*, q^*) proposes a noncooperative Nash equilibrium solution for 2×2 matrix game operator $(Q_{\text{Attack}}, Q_{\text{IDS}})$ provided that the inequalities (4) and (5) hold true given the fundamental theorem of Nash equilibrium.

$$p_1^*(\beta_h q_1^* - \beta_s(1 - q_1^*)) \le p_1(\beta_h q_1^* - \beta_s(1 - q_1^*)), \quad (4)$$

$$p_1^* a_m + q_1^*\left[a_f - (a_f + a_h + a_m)p_1^*\right] \le p_1^* a_m + q_i\left[a_f - (a_f + a_h + a_m)p^*\right], \quad (5)$$

where $0 \le p_1, q_1 \le 1$. The only solution for the set of inequalities presented as the parameters of the best response is to form a unique Nash equilibrium of the game obtained through

$$p_1^* = \frac{a_f}{a_f + a_h + a_m}, \quad (6)$$

$$p_1^* = \frac{B_s}{B_h + B_s}. \quad (7)$$

In addition, the equilibrium costs of the attacker Q^*_{Attack} and the intrusion detection system Q^*_{IDS} for the designed subsystem matrix of Table 1 are obtained from

$$Q^*_{\text{Attack}} = [p_1^*(1 - p_1^*)]Q_{\text{Attack}}[q_1^*(1 - q_1^*)]^T, \quad (8)$$

$$Q^*_{\text{IDS}} = [p_1^*(1 - p_1^*)]Q_{\text{IDS}}[q_1^*(1 - q_1^*)]^T. \quad (9)$$

Given the Nash equilibrium equations (6) and (7) and the best response parameters of the (8) and (9) equations, the likelihood that the attacker will attack and target the first subsystem at the Nash equilibrium point is reduced by a decrease in a_f since the lower the cost of not reporting an alert to the intrusion detection system, the more likely it is to set an alert and trap the attacker. Then, of course, increasing a_n and a_m plays a key role for the attacker, and $-\beta_s$ the likelihood that the intrusion detection system will detect an alert is affected by the attacker's gain from successful intrusion.

The parametric analysis for the second set of information is examined by establishing a relationship between costs in subsystems two and three and in the form of a 2×2 matrix in Table 2.

In Table 2 α_d and $-\beta_d$ are the deception costs for the intrusion detection system and attack. It can be assumed that $\alpha_d > \alpha_m$ and $\beta_d > -\beta_s$ since the lack of alert of the intrusion detection system is much more costly than the lack of attack, and the attacker disrupts the security mechanisms by deceiving the intrusion detection system. Let us assume that $\bar{p}_1$, $\bar{p}_2$, and $1 - \bar{p}_1 - \bar{p}_2$ are the probabilities of t_2, t_3, and nt_2 strategies of the attacker, and assume that $\bar{q}_1$, $\bar{q}_2$, and $1 - \bar{q}_1 - \bar{q}_2$ are the probabilities of the a_1, a_2, and na_2 strategies. The intrusion detection systems' operating strategy is presented with relative values such as

$$\bar{p}_1^* = \bar{p}_2^* = \frac{a_f}{2a_f + 2a_m + a_{h-}a_d}, \quad (10)$$

$$\bar{q}_1^* = \bar{q}_2^* = \frac{\beta_f}{2\beta_s + \beta_h - \beta_d}, \quad (11)$$

if $\beta_d < \beta_{h\beta_d<\beta_h}$ and $a_d < 2a_f + 2a_m + a_{ha_d<2a_f+2a_m+a_h}$. Finally, the Nash equilibrium strategy of the intrusion detection system may be presented in the form of

$$\begin{cases} \dfrac{a_1 \text{ with probability } q_1^*}{na_1 \text{ with probability } q_2^*}, \text{ InfoSet 1,} \\ a_2 \text{ with probability } \bar{q}_1^* \\ a_3 \text{ with probability } \bar{q}_2^* \quad \text{, InfoSet 2.} \\ na_1 \text{ with probability } 1 - \bar{q}_1^* - \bar{q}_2^* \end{cases} \quad (12)$$

Table 2: Parametric description of similar strategies of the second information set.

t_2	β_h	β_d	β_s
Q_{Attack}			
t_3	$-\beta_d$	$-\beta_h$	$-\beta_s$
nt_2	0	0	0
	a_2	a_3	na_2
t_2	$-\alpha_h$	α_d	α_m
Q_{IDS}			
t_3	α_d	$-\alpha_h$	α_m
nt_2	α_f	α_f	0
	a_2	a_3	na_2

Always $\alpha, \beta \geq 0$.

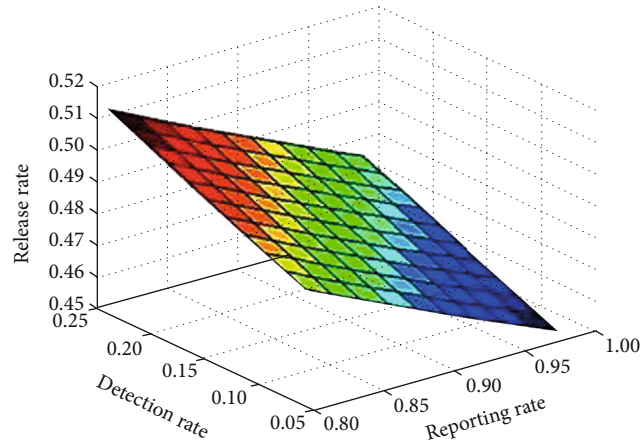

Figure 3: Release rate of an aggressive smart object based on the parameters of detection rate and reporting rate.

6. Evaluation and Validation of the Proposed Game Model

Today's intrusion detection system's architecture is a passive information-processing model.

Nevertheless, with the abundance and complexity of security attacks, intrusion detection systems cannot distinguish between the real intentions and target of the attackers. To correctly identify and detect the target of an attack, intrusion detection systems must be able to process the attack information in the text. Through establishing a network of sensors in the system and by a theoretical analysis of the game's sensor output data, the attacker's behavior, intention, and target may be modeled. In addition, due to the flexibility of the proposed game model, not only attacks targeting the specific parts of the network but also single targets such as processes distributed across multiple physical subsystems may be detected. Besides modeling the attacker's behavior and intention, the game's theoretical framework may be employed in order to analyze and model the response process of the intrusion detection system through calculating the relationship between security succession and statistical points. The response and reaction of the intrusion detection system vary from a simple alert setting to a high-cost reconfiguration of the system, including shutting down relatively less important services in the system.

In this section, the theoretical framework of the proposed game is first validated by performing numerical experiments in MATLAB software environment and augmentation, and to investigate and explain the Nash equilibrium of the numerical samples, in mixed and behavioral strategies, the attacker's vector with application of t_1, t_2, t_3, nt_1nt_2 and the intrusion detection system's vector with application of $[a_1, a_2, a_3, na_1na_2]$ were related; and the Nash equilibrium was calculated according to equations (6), (7), (10), and (11). Then, by entering the proposed game model into the IoT using cloud-fog-based IDSaaS, a potential application is presented.

As the intrusion detection system and the potential attacker interact and play in several different strategies in the proposed game model, the game results are observed and recorded at each stage. We present and calculate some statistical points from these results.

The optimal smart thing rate criteria as an attacker have been considered by choosing release and the possibility of subsequent infection. The reason for choosing this criterion may determine the effective parameters on the behavior of a smart thing in the network, as well as the principles of timely judgment about whether the attacker's smart thing is infected or not.

The parameters of various game strategies have been specifically evaluated in software experimentation, although if the values of these parameters are logically changed, similar trends towards statistical points can be reached. Thus, given the parameters of different strategies, it is believed that the following numerical results are helpful for showing the characteristics of the proposed game model and they can be easily reproduced for more specific situations.

The parameters used to evaluate the proposed method in this research are time, correct detection rate, reporting rate, and emission rate of the infected smart object. The faster intelligent sensors can detect and report an attacking smart object, the faster the propagation rate converges over time t , which prevents malware (attacker) from spreading across layers of the Internet of Things.

Obviously, a higher detection rate and a higher reporting rate (alert) allow IDSaaS to more easily trap an attacking smart object, which in turn, as shown in Figure 3, causes the malware in attacking smart object makes less effort to propagate, which reduces the propagation rate.

In addition, lower reporting rates mean that attacker detection rates are reduced and the privacy of IoT networks cannot be adequately protected for research purposes, so it can be concluded that an attacker is a smart object. Release at a higher rate means that the intrusion detection system is less likely to detect that attacker. As expected, the actual implementation trends in Figure 3 confirm the analysis presented.

However, different factors have different impacts on the players in the proposed game model, affecting the rate of different detection strategies and the release rate.

Table 3: Comparison of the proposed model with the other three models.

	Security threats coverage	Emphasized detection method	Type of game model	Complexity of protocol and architecture	Scalability
The proposed model	Noncooperative game	Combined	Common attacks in IoT networks and wireless sensors	Low	Yes
Susan and Rayford (2019)	Noncooperative game	Signature-based	Threats in mobile ad hoc networks	Moderate	Yes
Wenjua et al. (2019)	Cooperative game	Signature-based	Dissemination of malware, to protect privacy in IoT networks	High	Yes
Shen et al. [13]	Cooperative game	Combined	Dissemination of malware, to protect privacy in IoT networks	Moderate	Yes

Table 3 includes a comparison of the proposed model with the three models in other articles.

7. Conclusions

In the present study, a strategic, dynamic, and complete game model has been defined to detect the intrusion of attacks in IoT networks in the distributed intrusion detection system. An analytical research of the game in the form of 2×2 matrix subgames and finding the best response parameters in Nash equilibrium bring valuable insights for the attacker and the behavior of intrusion detection. Furthermore, the simple assumptions proposed to achieve analytical results may be easily expanded to achieve more realistic scenarios, and smart intrusion detection system, defined as a software agent, reports attacks on the large subsystems of IoT using a variety of signature-based, anomaly-based, feature-based, and hybrid approaches.

Thus, it can be stated that given the equilibrium solutions and costs of each subgame in the presented matrices, the intrusion and attack detection systems specify the performance of their strategies. Furthermore, compared to a related work, the distinguishing feature and the used innovation are the presentation of a game model to detect attacks on the IoT between sensor's nodes and the platform server used to detect more attacks, correct detection rates, and minimize wrong detection rate.

Consequently, it is important to note that other common security measures, as well as the implementation of privacy, cannot be directly applied to IoT technologies. Therefore, the development of specific security solutions such as intrusion detection systems is essential to allow users and organizations to identify and repair all weaknesses and attacks in their system. Further, this method has been used in smart systems efficiently in the future in real-time applications.

Data Availability

Data are available on request through contacting safieh .siadat@gmail.com.

Conflicts of Interest

The author declare that they have no conflicts of interest.

References

[1] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[2] E. Borgia, "The Internet of things vision: key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1–31, 2014.

[3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[4] D. Jin, "Application of IOT in electronic commerce," *Journal of Digital Content Technology and its Application*, vol. 6, 2012.

[5] S. Kumar and K. Dutta, "Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges," *Security and Communication Networks*, vol. 9, no. 14, pp. 2484–2556, 2016.

[6] A. Abduvaliyev, A. S. K. Pathan, Jianying Zhou, R. Roman, and W.-C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1223–1237, 2013.

[7] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.

[8] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyberphysical systems," *ACM Computing Surveys*, vol. 46, no. 4, pp. 1–29, 2014.

[9] D. Midi, A. Rullo, A. Mudgerikar, E. Bertino, and Kalis, "Kalis — A system for knowledge-driven adaptable intrusion detection for the Internet of things," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pp. 656–666, Atlanta, GA, USA, June 2017.

[10] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 266–282, 2014.

[11] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[12] B. G. Atli and A. Jung, "Online feature ranking for intrusion detection systems," 2018, http://arxiv.org/abs/1803.00530.

[13] S. Shen, L. Huang, H. Zhou, S. Yu, E. Fan, and Q. Cao, "Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in fog-cloud-based IoT networks," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1043–1054, 2018.

[14] T. Ramesh and S. Shaleni Priya, "A review on game theory based congestion control in wireless sensor network," *Journal of Network Communications and Emerging Technologies*, vol. 8, no. 4, 2018.