Computing and Informatics, Vol. 41, 2022, 665–688, doi: 10.31577/cai_2022_3_665

GTA-IDS: GAME THEORETIC APPROACH TO ENHANCE IDS DETECTION IN CLOUD ENVIRONMENT

Komal Singh Gill, Sharad Saxena

Computer Science and Engineering Department
Thapar Institute of Engineering and Technology
Patiala, India, 147004
e-mail: {kgill_phd16, sharad.saxena}@thapar.edu

Anju Sharma

Department of Computational Sciences
Maharaja Ranjit Singh Punjab Technical University
Bathinda, Punjab, India
e-mail: phdanju@gmail.com

Abstract. The Internet of Things (IoT) industry is growing with the high-quality collaboration with Cloud Computing. The data generated by the IoT devices is quite large which can be efficiently stored and processed by the cloud. Further, the scenario like COVID-19 led to an unexpected flood of IoT devices on enabling networks to facilitate online services, which increases the potential threats to the companies fighting to remain operational during the crises. Still, the problem with the IoT devices is their weak security implications because vendors prioritize other factors like energy-saving and efficiency at the cost of security. The Attacker can send malicious requests through the vulnerable IoT device to the network and exploit the cloud in various ways. So, to address this issue, a Game Theoretic Approach to enhance IDS detection (GTA-IDS) in Cloud Environment has been devised that helps the Defender system to be more efficient, accurate in decision-making and save energy. The algorithm based on relative information entropy has been developed to defend against such attacks. The Bayesian Nash Equilibrium (BNE) has been used to make the Defender's strategies and perform actions to maximize its payoffs. The model has been tested on the NSL-KDD dataset and the results have been

compared to the existing techniques. The results show that despite efforts made by the Attacker, the Defender always gets a better gain and ultimately eliminates the attack.

Keywords: Cloud computing, Internet of Things, IDS, information entropy, game theory

1 INTRODUCTION

Cloud computing is a rapidly growing technology used in most of the Information Technology (IT) sector. Many fields like medicine, military, education, politics are leveraging cloud benefits. The features of cloud computing have provided a platform for several other technologies like the Internet of Things (IoT), Big Data. The IoT devices are increasing at a very high pace and are processing that huge amounts of data every minute. And cloud provides many advantages [1]. Nevertheless, the increasing number of devices also poses a threat to the cloud because of security reasons. These devices are not as secure as they should be for safe networking. Most devices have weak credentials that can easily be decoded with a Brute Force attack. Some widgets have factory-set default credentials, and some have no authentication policies. So, these devices can be compromised easily [2]. These can be turned into a huge network of botnets to perform a Distributed Denial of Services (DDoS) [3] attack or can be used to send malicious packets to the cloud. To compromise cloud security, the attackers can find a way to eject a malicious packet into the network through the insecure IoT devices connected to the cloud. There are many other attacks like session hijacking, IP address spoofing, Man-in-the-Middle, network penetration [4]. There are many fields like Telemedicine, smart traffic systems, smart grid, where a small error poses a big problem. For example, in Telemedicine, if the medicine of the patient, the oxygen or blood regulation got altered by some malicious packet, it will have a severe effect on the patient's health [3]. Also, the malware attacks have been increased by 53 % in the last year in India. The analysis shows 3.9 trillion malware attacks in 216 countries worldwide. Another research by SonicWall Capture Labs shows a 30 % rise in IoT malware (32.4 million) in September 2020 [5]. In the past few years, the attacks on IoT devices have proved the need to increase the security of the IoT-Cloud environment. The Mirai attack that occurred in October 2016 is one of the biggest examples of a security attack on IoT devices [6]. With the leak of Mirai code on the internet, the attackers can easily scan the vulnerable devices and attack them to make zombies. These zombies can disrupt the whole system [7]. Furthermore, these IoT devices are connected to the cloud, and because of that, the malware can be propagated through the channel. So, this issue needs to be addressed because modern malware is intelligent and is difficult to detect. To protect the assets of the cloud from the Attacker, there is a need to build a strong defending system. The Defender systems like IDS need

to be more optimized to detect these intelligent malicious packets. The concept of game theory has been used to lower the false positives and increase the detection rate with less energy. The non-zero non-cooperative game has been designed between the Attacker (malicious node) and the Defender system. Both Attacker and Defender use their best strategies to increase their payoffs. By delineating the Bayesian Nash Equilibrium (BNE), the probability of attacking and defending the Asset has been calculated.

1.1 Research Contribution

The novelty of the work is attained by:

- Adding a lightweight proposed module (GTA-IDS) to work parallel with the existing Defender system.
- Assisting the Defender system to work more efficiently by calculating the prior probabilities and payoffs of the risk of the attack.
- Saving energy of the Defender System by activating it only during the times of need. When there is a high risk, GTA-IDS will suggest the Defender start the defending, and when there is no risk, the Defender can rest.

In Section 2, the background of the work has been discussed. The existing game theory models and defending systems have been discussed in Section 3. Section 4 discusses the GTA-IDS. The devised model has been analyzed in Section 5. The results have been shown in Section 6. Section 7 concludes the paper.

2 BACKGROUND

This section discusses the overview of the Game Theory and Game Theory in the IoT-Cloud Environment.

2.1 Game Theory Overview

Game theory is a powerful mathematical approach used to predict and choose strategies to satisfy participating players' self-interest. If the players are competing against themselves, the game is non-cooperative. Otherwise, if they play in coordination for gaining mutual benefits, the game is called the cooperative game. The primary assumption of game theory is that all the players should be rational. So, the actions performed by these players should always be logical and best in their interests [8]. In this work, the two players have been selected. One of the players is the Attacker, which will always try to attack and exploit the resources of the cloud. The Attacker will maximize his Payoff by remaining stealthy, using his least resources, and exploiting the cloud's resources. The other Player, i.e. the Defender, will always try to detect the attack and block the malicious traffic. It leads to forming a non-zero

and non-cooperative game between Attacker and Defender. The essential elements of game theory are shown in Figure 1 and explained below as [9]:

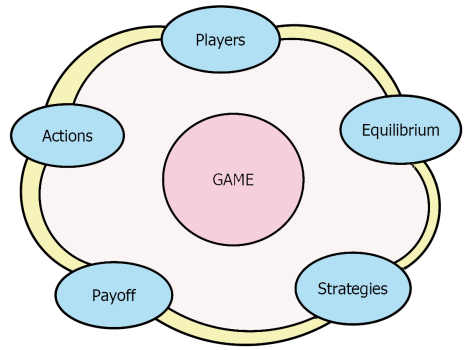

Figure 1. Basic elements of game theory

Players: The player can be a person, company, animal, or any other thing that can interact with surroundings. In this paper, the game is played between the Attacker and the Defender. A set of n players can be represented as $P = \{P_1, P_2, \ldots, P_n\}$, where $n \geq 2$.

Actions: The action is the particular move of the Player which they choose to gain maximum payoff. The action of the attacker is to attack or not to attack, and the Defender is to defend or not to defend. The Player P_i has non-empty action set $A = \{A_1, A_2, \ldots, A_m\}$.

Payoff: After each action performed by the players, they will be rewarded with a negative or positive score called the payoffs and is represented as U. Both players always try to increase their payoffs. If the Attacker successfully attacks without getting caught, the Attacker will gain a positive payoff, and the Defender will gain a negative payoff. The Payoff set containing k payoffs for corresponding strategies can be represented as $U = \{U_1, U_2, \ldots, U_k\}$.

Strategies: The strategies (S) describe the plan of actions that the players can take. Strategies can be made by the players depending upon the previous actions and their respective payoffs. The attacker strategy is not to get caught by the Defender and transmit the malicious packet within the trusted device. The Defender's strategy will be to detect the packet if there is a change in entropy; otherwise, not to defend because of energy perseverance. The strategies can be represented as a set of l elements $S = \{S_1, S_2, \ldots, S_l\}$.

Equilibrium: The state of the game when each Player's strategy leads to the maximum Payoff for the other Player's strategies. In Nash equilibrium (NE), no player is willing to change the chosen strategy, because no player can choose a better strategy given the choices of the other players. The strategy at the equilibrium can be pure or mixed.

Mathematically a strategic game (G) can be given as:

$$G = (P, (S_j)_{i\epsilon P}, (U_j)_{i\epsilon P}). \tag{1}$$

Here, S_j is the strategy of Player i and U_j is the payoff of that i^{th} Player.

2.2 Game Theory in IoT-Cloud Environment Security

Game Theory has been used as an essential method to predict other players' strategies in the same environment for the past many years. In the Information Technology (IT) sector, especially in cyber security, Game Theory has been used to predict the behavior and strategies of the Attacker. The different types of game models used in IoT-Cloud Environment security have been depicted in Figure 2 and explained in Table 1.

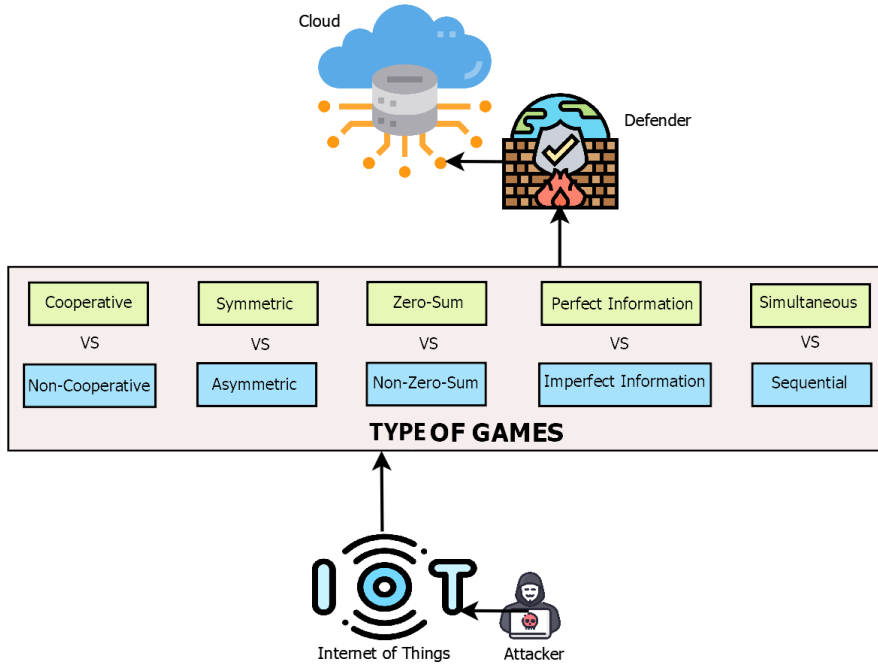

Figure 2. Type of games played between Attacker and Defender in cloud environment

The applicable terms used in this work have been discussed below:

System: In the cloud environment, a system can be a server, a host, software, a process or a device, or a hypervisor controlling the virtual machines.

Type of Games	Description
Cooperative	Players cooperate with each others strategies to achieve their goal.
Non-Cooperative	Attacker and Defender compete against each other to achieve their goal.
Symmetric	Strategies adopted by all the Players are the same.
Asymmetric	Attacker and Defender both have different strategies.
Zero-Sum	One Player gain is the same as the loss of the opponent so that the sum of the payoff is zero.
Non-Zero-Sum	Defender's gain and loss of the Attacker or vice-versa can be different resulting in a non-zero payoff.
Perfect	Players have perfect information about the game being played.
Imperfect	Attacker and Defender do not have common knowledge of the game being played.
Simultaneous	All the Players play simultaneously and do not have known the strategies of other Players.
Sequential	Defender aware of the moves of Attacker who has already adopted a strategy.

Table 1. Types of games

Attacker: Any node that sends malicious data to the cloud for exploiting the resources and for gaining information.

Asset: The System that is most beneficial for the Attacker to attack. In the cloud, the Asset can be a particular server or hypervisor.

Defender: Any software/hardware that can detect and defend the attack. The Defender should defend and analyze the traffic, identify and stop malicious traffic. Firewall and IDS are good examples of a Defender.

3 RELATED WORK

Aslan et al. [10] proposed an intelligent behaviour based malware detection system for cloud computing. The learning-based and rule-based detection engine has been used to separate and determine malware from benign, respectively. The model can detect both the previously known and unknown malware accurately.

Gan et al. [11] developed a dynamic propagation model of malware for cloud security. The Virtual Machines (VM) working in the Infrastructure as a Service (IaaS) architecture have been considered to check the malware. The numerical simulations show that the infection level of the VMs has been reduced by changing the parameters.

Gill et al. [12] proposed a Game-Theoretic Model for IoT-Cloud Environment to enhance the security. The Intrusion Detection System (IDS), including signature and anomaly-based models and honeypots, have been used. The proposed model

predicts the Attacker's strategies and assists the defending System to tackle the attacks more efficiently.

Mardini et al. [13] proposed an approach to enhance the performance of the Internet of Everything in healthcare systems. The IPv6 routing protocol for Low-Power and Lossy-Networks has been used. The set of nodes with everyday tasks connected has been grouped to represent an instance. The two parameters, namely average latency and Packet Delivery Ratio, have been considered. The results show that these parameters have been addressed to enhance the performance of the healthcare system.

Shakeel et al. [14] proposed a protocol to remove collisions from the communication in IoT devices using Multiple Machine Access Learning with Collision Carrier Avoidance (MMALCA) protocol. The regression learning methods have been used to improve the efficiency of (Media Access Control) MAC sync. The performance of the proposed approach has been tested with latency, collision probability, service failure, and resource utilization.

You et al. [15] discussed the four paradigm shifts of communication technology. The first one is to complete the requirement of global coverage. The second is to explore areas like connection density and data rates in detail. The third is to tackle the huge data generated by the users, and the fourth is to strengthen network security. The author justifies that the physical and cyber world boundaries would disappear.

Shen et al. [16] proposed a game-theoretic model for heterogeneous WSNs to diffuse the malware. The Markov chain model with a non-zero-sum game has been designed. The results can be applied to any related theoretical work. A malware detection game has been designed by Xiao et al. [17] for mobile devices offloading based on the cloud. Also, a post-learning-based scheme has been proposed that further enhances the learning capability of the System.

Fan et al. [18] proposed a model to analyze the attack and defense strategy of resource service in cloud applications by using a game-theoretic approach. The game model works on stochastic Petri-nets, which define the behavior of the Attacker and the Defender. An enforcement algorithm is designed to find the possible attack path and enforce strategies according to the path. The simulation results verified that the defense strategy chosen by the Defender quickly tackled the attack.

Wang et al. [19] studied anti-eavesdropping problems in wireless networks. The Bertrand game has been modeled based on price competition to obtain the best scheme for the friendly jammers. To solve the problem in multichannel jamming, new algorithms have been proposed that provide the optimal strategy of the jammer.

Fadlullah et al. [20] optimized the QoS and security in next-generation heterogeneous networks by game theory. A GT-QoSec framework has been designed to balance the security and QoS parameters. The transition matrices have been considered, and the NE has been obtained in the expected number of steps.

Li et al. [21] designed a differential game model of IDS in cloud computing. This work leads to deciding the optimal strategies by the IDS for the defense of the cloud resources by theoretical foundations of the game theory. La et al. [22]

presented a game model in honeypot enabled networks for IoT. The Bayesian game of incomplete information has been modeled, and the equilibrium has been calculated for the one-shot game and repeated games. The Defender used the mixed strategy to decide whether to deploy a honeypot to keep the energy level optimum and the Attacker's success rate low. Wang et al. [23] proposed a game model to detect infected nodes by using IDS as a Defender. The defending Player re-evaluates the previous outcomes to make the next strategy better.

The IDS has been improved by decreasing the missing and error detection rates. The results show a decrease in energy usage and an increase in detection rate. Cheng [24] designed a non-cooperative differential game model between IDS and attackers in Wireless Sensor Networks (WSN). The sensor has been clustered in this model, and each cluster head node is assigned with the IDS.

The optimal strategies that increase the payoffs of the IDS have been obtained. Wang et al. [25] proposed a game model which is dynamic to defend the network from the DDoS attack. Algorithms have been given to adjust the offensive and defensive strategy from the scenarios studied. The proposed model has increased the detection rate of the firewall and the QoS of legal users.

Bedi et al. [26] developed a defense mechanism inspired by game theory to defeat the DDoS attack. The attacker player in the game creates multiple bots and generates enormous traffic, leading to congestion in the network. The Defender has to set its strategies to configure the firewall to block the rogue traffic.

Spyridopoulos et al. [27] investigated different permutations by which attacker can perform DDoS or DoS attack. A framework based on game theory has been designed to defend against the DoS/DDoS attacks. The traffic, number of zombies, rate of host victimization have been considered the main parameters. The simulated environment has replicated the analytical parameters to test the accuracy of the designed framework.

Moosavi et al. [28] proposed a game-theoretic framework for robust intrusion detection in WSN. The non-zero-sum discounted incomplete information stochastic games have been considered to design the framework. The game parameters and the players' payoffs have been designed to tackle the security problems in WSNs.

The discussion of the above-stated work of different researchers clearly shows the influence of game theory in network security. The game theory can be applied in any environment like WSNs, Cloud, IoT to analyze the security complications. The addition of the game-theoretic module helps the researchers increase the detection accuracy and lower the false positives rates and the energy consumption of the defending System.

4 GAME THEORETIC APPROACH TO ENHANCE IDS DETECTION IN CLOUD ENVIRONMENT (GTA-IDS)

The GTA-IDS model has been proposed to protect the cloud environment from the malicious packets ejected through the IoT devices. This scenario has been depicted

in Figure 3.

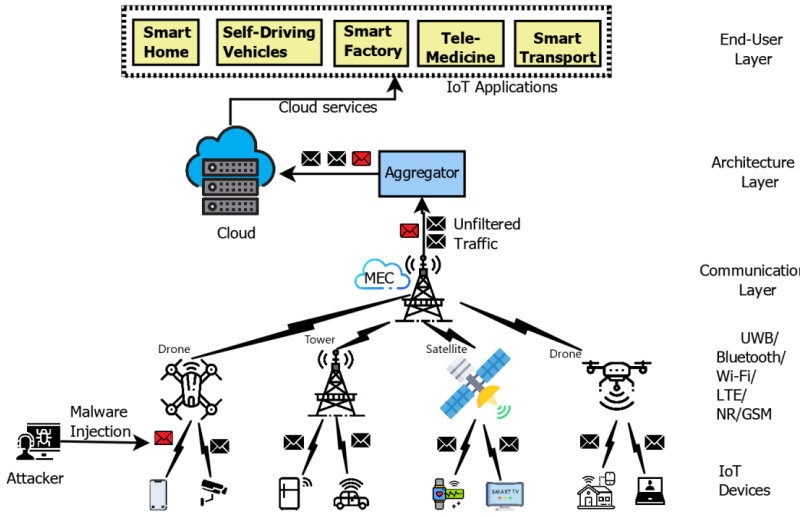

Figure 3. An attacker inserting malware in cloud environment

The communication can be done via satellites, drones, towers, GSM, LTE technologies. The Attacker attacks the vulnerable IoT devices with malicious packet (depicted in the red packet), and the malicious packet travels through the communication channel to the cloud servers.

The Defender system always needs to work efficiently and accurately with minimum energy requirements. The false positives of the Defender should be very low, and the true positive number should be high [12]. To make the Defender system more efficient, a game-theoretic model has been designed based on a non-zero non-cooperative game. This model uses probabilistic Defending strategies based on the Nash Equilibrium of the game. The model allows the Defender to detect the malicious packet as early as possible. Also, the Defender will only defend when there is a chance of malicious activity, thus increasing efficiency. The interaction between two players, namely malicious node (P_a) and Defender (P_d) has been designed in this game model. The names malicious node and Attacker have been used interchangeably in this paper. The malicious node has two pure strategies [*Attack*, *Not-Attack*]. The Defender has two strategies, namely [*Defend*, *Not-Defend*]. However, the strategy of the normal node is [*Not-Attack*]. It can be represented as Figure 4.

The Defender has no prior knowledge about the maliciousness of the nodes. So, the game of imperfect information can be mathematically given as: $G = (P, S, U)$ [29] where:

- $P = P_a, P_d$ are the two participating and competitive players, namely the At-

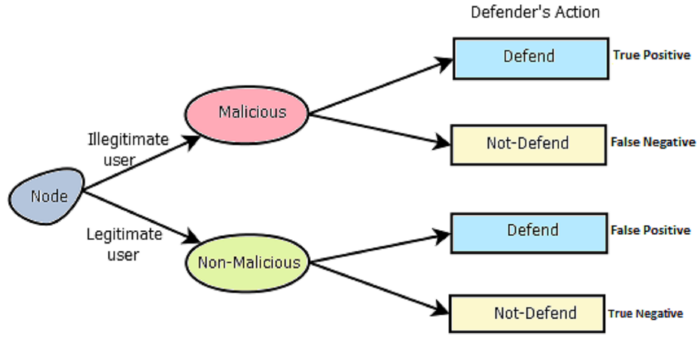

Figure 4. A figure depicting actions of both players in GTA-IDS

tacker and the Defender, respectively.

- $S = S_a X S_d$ is the strategy space of the game where strategies of the Attacker have been represented as S_a and strategies of the Defender are given by S_d.
- $U = U_a X U_d$ are the payoffs gained by the Attacker and the Defender by their strategy space S. U_a is the Payoff of the malicious node with S_a and U_d is the Payoff gained by the Defender with strategy S_d. The other parameter used in the game model has been represented in Table 2.

Description	**Symbol**
Resources consumed by Defender	E_{ds}
Detection rate of Defender	λ
False Positive rate of Defender	σ
Value of the Asset to be protected	ψ
Malicious node	d
Number of nodes used by attacker	z
Timestamp	T_a
User ID of Trusted nodes	T_{id}
Threshold value of entropy (High)	TH_h
Threshold value of entropy (Low)	TH_l
Change in Entropy	CiE

Table 2. Nomenclature

The parameters used in this model are explained as follows. The energy or the resources consumed by the Defender while defending the traffic is represented as E_{ds}. If the Defender is at rest, this factor will be zero. The detection rate i.e., the true positive rate, or the accuracy of the Defender has been defined by λ. The false-positive rate means the Defender identified the legitimate node as a malicious node and blocked it. It is given by σ. The value of λ and σ lies between 0 and 1 i.e. λ, $\sigma \in [0, 1]$. The Asset the Defender needs to protect can be a hypervisor,

a server, software, or any other helpful entity of the cloud. The Asset's value should always be greater than the resources consumed by the Defender and more significant than the resources exhausted on the attacker side. Suppose the asset value is lower than the resources consumed by the Defender. In that case, it will not prevent the attack as, ultimately, it is gaining a low value (players are rational in game theory). Otherwise, the Attacker and the Defender will continuously lose the game whenever he attacks, similarly to the case with the Defender. The attacking or malicious nodes have been represented by d. The number of malicious nodes used by the Attacker is given by z. The time for which the node keeps on sending malicious packets is given by T_a. Some IoT Devices connected with the cloud are put in the trust category. These devices are assumed to meet the security requirements needed to be connected with the cloud. The id of these trusted devices has been given by T_{id}. To calculate the entropy of the information changed, the relative entropy or Kullback Leibler distance formula has been used [30]. It is given by:

$$D(P||Q) = \sum_i p_i \log\left(\frac{p_i}{q_i}\right) \tag{2}$$

where Q is the distribution calculated on the legitimate set of traffic, P is the distribution that can be of the malicious form. If the value of p_i is greater than q_i, the value of logarithm will be greater than 1, resulting in a higher value of total. So, a threshold value has been placed, which is given by TH_h and TH_l, if the Change in Entropy (CiE) increases by TH_h, the packet will be treated as malicious and will directly be blocked. If the value lies between TH_h and TH_l, the packet propagation to the network will be decided on anomaly and signature tests. If the value is below TH_l, traffic will simply be forwarded to the cloud network.

The algorithm based on information entropy has been given by Algorithm 1.

The architecture of the proposed model has been depicted in Figure 6. The packet is entered into the defending System comprising Entropy Module, GTA-IDS, and the Intrusion Detection System (IDS). In the Entropy Module, the packet is captured at the capture layer. The information entropy of the packet is calculated at the calculation layer, and as shown in Figure 5, the decision is taken at the process layer. According to the decision made by the Entropy Module, the packet is passed to the GTA-IDS Model. Firstly all the parameters are initialized according to the values the payoffs of the Attacker and the Defender are calculated. At Equilibrate, the Nash Equilibrium (NE) is calculated. The decision is further passed to the IDS to start the signature-based module, anomaly-based module, or to rest.

The payoff matrices of both players have been given in Table 3. Table 3 shows the relation between malicious node and the Defender. All the possible combination of events (*Attack*, *Defend*), (*Attack*, *Not-Defend*), (*Not-Attack*, *Defend*) and (*Not-Attack*, *Not-Defend*) have been discussed.

After building the game model, there is a need to analyze this model to compute the Nash Equilibrium (NE). At NE, both the players will have the best strategies

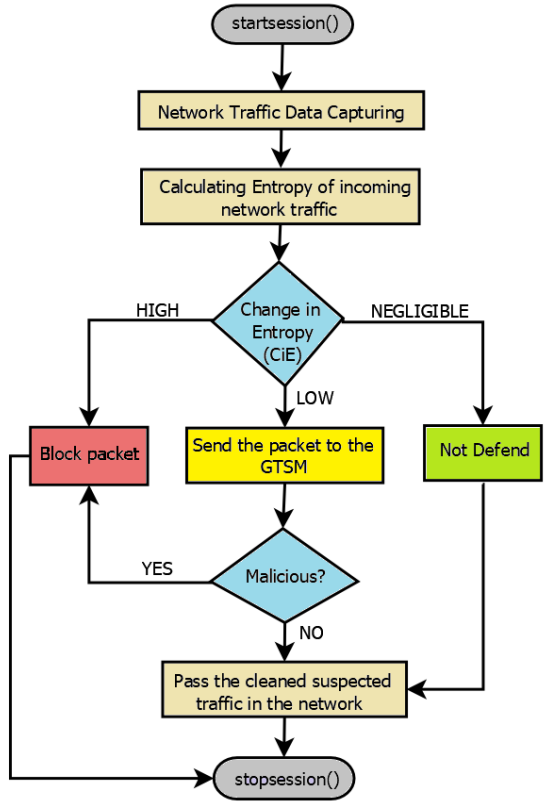

Figure 5. Attack defending strategy process

	Defend	**Not-Defend**
Attack	$(T_aE_{ds} - 2\lambda)\psi - zd, (2\lambda - E_{ds})\psi - T_aE_{ds}$	$(\psi - zd)T_a, -T_a\psi$
Not-Attack	$0, (-\sigma\psi - E_{ds})T_a$	$0, 0$

Table 3. Payoff matrix of malicious node and Defender

and the best payoffs.

	Defend	**Not-Defend**
Not-Attack	$0, (-\sigma\psi - E_{ds})T_a$	$0, 0$

Table 4. Payoff matrix of normal node and Defender

Algorithm 1 GTA-IDS Algorithm

Input: Packet entering the defending system
Output: Non-Malicious packets entering the cloud
startsession()
if $T_{id} == True_{id}$ **then** ▷ $True_{id}$ is the authenticated id in Database
return Pass
else if $CiE > TH_h$ **then**
return Fail
else if $(CiE < TH_h)$ and $(CiE > TH_l)$ **then**
    initialize GTA-IDS module
    if $(Packet! = Signature) \,||\, (Packet! = existbehaviour)$ **then**
return Fail
    end if
else
return Pass
end if
stopsession()

5 GTA-IDS ANALYSIS

The purpose of payoffs shown in Table 3 is to increase the probability of the Defender successfully detecting the attack. We assume there is some initial belief of maliciousness of node and is given by p_0. So, $(1 - p_0)$ is the initial belief of a non-malicious node. The observations made from Figure 7 have been discussed below with the help of different cases:

Case 1: The node is malicious and it chose its pure strategy as *Attack*. The pure strategies of the Defender are *Defend* and *Not-Defend*. The payoffs of Defender in this case are given in Equations (3) and (4):

$$U(Defend) = p_0[(2\lambda - E_{ds})\psi - T_a E_{ds}] - (1 - p_0)[(\sigma\psi + E_{ds})T_a], \quad (3)$$

$$U(Not\text{-}Defend) = -p_0 T_a \psi. \quad (4)$$

If the Defender chooses to Defend, it will result in true positive means this strategy will gain the Defender. The Defender successfully prevents the asset from getting damaged. If the Defender chooses the strategy *Not-Defend*, then it will lose the asset, and the attacker will be completely in gain.

Case 2: The pure strategy of Defender is *Defend*, the payoffs of the attacker for strategy *Attack* and *Not-Attack* is given in Equations (5) and (6), respectively:

$$U(Attack) = p_0[(T_a E_{ds} - 2\lambda)]\psi - zdT_a, \quad (5)$$

$$U(Not\text{-}Attack) = 0. \quad (6)$$

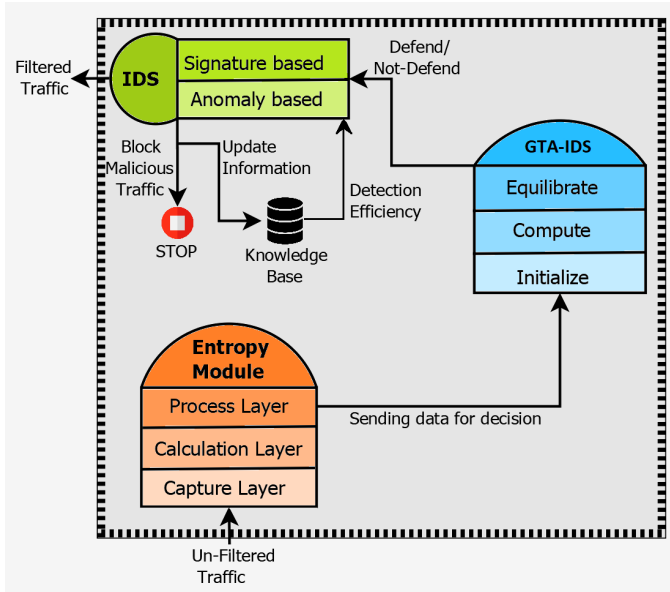

Figure 6. Architecture of GTA-IDS model

$U(Attack)$ represents the profit of the attack gained by the attack and exploiting the asset. If the attacker chooses the strategy *Not-Attack*, neither it will lose nor gain anything. So, the payoff in this case will be 0.

Case 3: When the malicious node has chosen its strategy as *Attack*, the Defender will choose its pure strategy *Defend*.

If $U(Defend) > U(Not\text{-}Defend)$: If Defender plays its *Defend* strategy, the node will stop attacking because for getting caught every time. Hence, in this case, the Defender and Attacker keep on changing strategy, so it does not follow NE.

If $U(Defend) < U(Not\text{-}Defend)$: the Defender chooses *Not-Defend* and then the Attacker strategy will always be Attack which follows the NE.

Case 4: If the malicious node chooses *Not-Attack* strategy, the beneficial move for the Defender is to *Not-Defend*. But if the Defender tends to chose the *Not-Defend* strategy, the attacker changes its strategy to *Attack*. Thus, this case will also not follow NE.

So, in some cases, there does not exist any NE. So, we need to find the mixed strategy NE. Let the attacking probability of the malicious node be p. Thus, $(1-p)$ is the probability of not-attacking. Similarly, q is the probability of defending the Asset, and $(1-q)$ is the probability for not defending. From Figure 7, the net

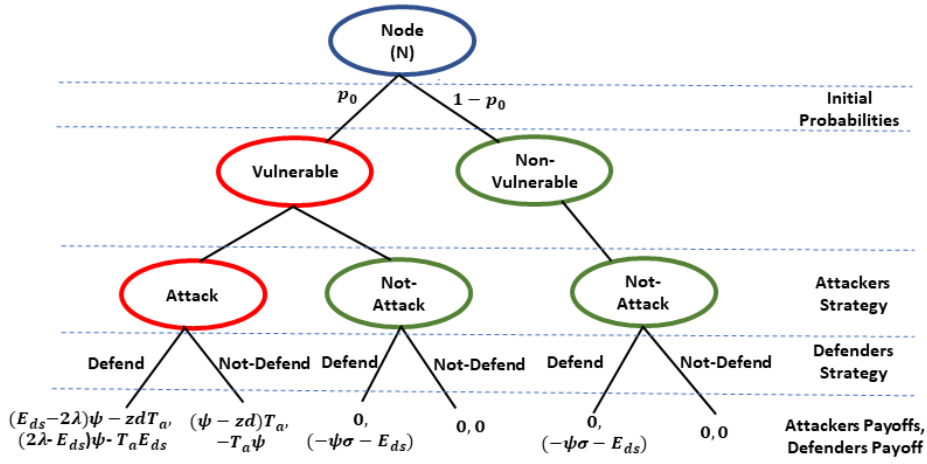

Figure 7. An extensive game model between Defender and malicious node

payoffs can be deduced as:

$$U(Defend) = pp_0[(2\lambda - (E_{ds})\psi - T_aE_{ds}] - (1-p)p_0[(\sigma\psi - E_{ds})T_a] - (1-p)[(\sigma\psi - E_{ds})T_a], \quad (7)$$

$$U(Not\text{-}Defend) = -pp_0T_a\psi. \quad (8)$$

For the malicious node, the payoffs for strategies *Attack* and *Not-Attack* are:

$$U(Attack) = p_0[q((T_aE_{ds} - 2\lambda)\psi - zdT_a) + (1-q)((\psi - zd)T_a)], \quad (9)$$

$$U(Not\text{-}Attack) = 0. \quad (10)$$

For the sake of Equilibrium, we equate $U(Defend)$ and $U(Not\text{-}Defend)$ and probability for attack (p) comes out to be:

$$p = \frac{\sigma\psi T_a + E_{ds}T_a}{[2\lambda - E_{ds} + T_a(\sigma+1)]p_0\psi} \quad (11)$$

and the probability of defending is:

$$q = \frac{zd - \psi T_a}{\psi(T_aE_{ds} - 2\lambda - T_a)}. \quad (12)$$

So, to gain maximum payoffs, a malicious node will attack with probability p and Defender will Defend with probability q.

The analysis of the game model by the above equations clearly shows that there does not exist any pure strategy Nash Equilibrium. However, there exists a mixed strategy Bayesian Nash Equilibrium (BNE) in which strategies depend upon the probability. The probability of the malicious node and the Defender has been calculated. To find out the best strategy for the Attacker and Defender during the [*Attack*, *Defend*] scenario, a MATLAB simulation environment has been done. The values of the parameters have been varied randomly to understand the best strategy of the players.

Figure 8 shows the payoffs of the Defender on the Y-axis and time elapsed (in seconds) on X-axis. This screenshot of the simulation is taken when the Attacker attacks the System with short breaks. The payoffs above zero show that the attack is not being performed at that particular time. Because of that, the Defender conserves the energy and thus gets a positive payoff. The negative Payoff shows the depletion of the resources and the energy used by the Defender to confront the attack.

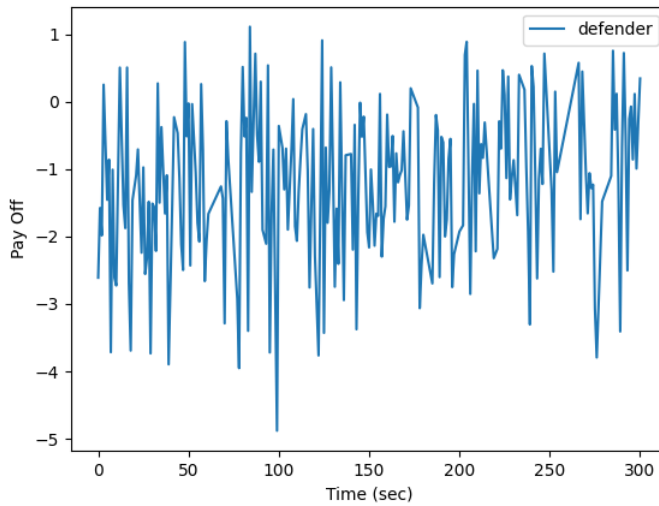

Figure 8. The graph showing Defender's payoff

In Figure 9, the payoffs of the attacker shows a great dip in the negative region in terms of $le16$. This dip clearly shows that the attacker looses badly whenever he/she is trying to compromise the security. The short gap between the graph shows where the attacker is not attacking.

If compared the payoffs of the Defender and the Attacker closely on the same graph, as shown in Figure 10, it can be observed that the Payoff of the Defender is almost stable around zero. Still, the Payoff of the Attacker is fluctuating at a high rate but in a negative direction. This means the Attacker is trying its best with different parameters and methods each time but is not winning.

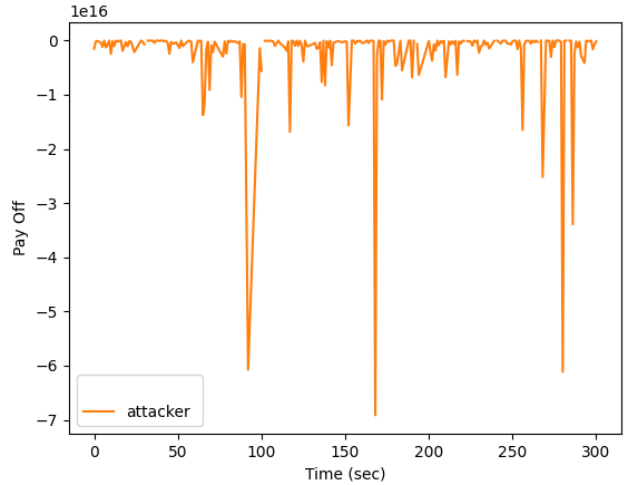

Figure 9. The graph showing Attacker's payoff

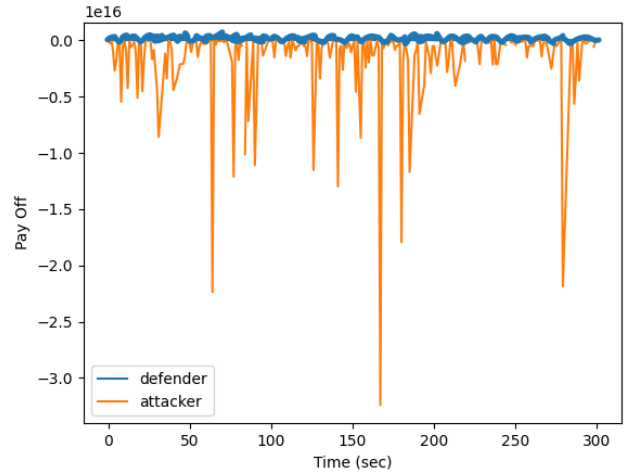

Figure 10. The graph showing Attacker's and Defender's payoff

So, from the graphs, it is clear that the Attacker's payoffs are lower than the Defender's. The Defender's strategy is to use minimum energy and minimize the attacking time, while the Attacker's strategy to gain maximum Payoff is to increase the attacking time and use fewer devices. Also, the best Payoff for the Attacker is to attack the cloud with probability p, and the Defender should Defend the cloud with probability q to gain maximum Payoff.

6 RESULTS AND DISCUSSIONS

GTA-IDS has been tested on real dataset NSL-KDD and the results have been compared with other existing techniques like NIDS [31], AS-IDS [32] and Hybrid [33]. NSL-KDD dataset is an enhanced version of the KDDCUP '99 dataset. This dataset composes of training and testing dataset with 125 973 and 22 544 records. Each NSL-KDD record has 41 features (e.g., protocol type, Logged in, and Duration, etc.). These features are represented as numeric, nominal, and binary, defined as continuous or discrete, and labelled as normal or attack. The NSL-KDD dataset has been divided into four classes. The types of attack considered to test the model are DoS, probe, R2L, U2L. The normalisation of the dataset has been achieved by the Z-score. After the normalisation, the three models, Gradient Boosting Machine (GBM), Random Forest, and Deep Learning have been trained using Machine Learning (ML). After training with these models, the Detection Rate (DR) and the False Positive Rate (FPR) of the IDS have been calculated. The values of the DR and the FPR have been tested on the the GTA-IDS model. The Payoffs of the Defender have been calculated from the DR and FPR values that are further delineated from the NSL-KDD Dataset.

Technique	Model	Detection Rate	False Positive Rate (in %)	Payoff
NIDS [31]	KNN	0.71	2.27	0.66
	CNN	0.7	2.25	0.7
	C4.5	0.76	3.88	0.58
	IBK	0.71	2.28	0.22
AS-IDS [32]	AS-IDS	0.96	3.4	0.72
Hybrid [33]	Hybrid	0.94	0.77	0.69
GTA-IDS	GBM	0.995	0.07	0.84
	RF	0.97	0.05	0.75
	DNN	0.997	0.06	0.81

Table 5. Comparative analysis of GTA-IDS with existing techniques

Table 5 shows the comparative analysis of GTA-IDS with the existing techniques. GTA-IDS performed well with a detection rate and payoff value of 99.5 and 0.84, respectively. The FPR is also the lowest out of all techniques with the value of 0.05. Figure 11 shows the graphical representation of the payoffs of the Defender respective to its Detection Rate.

The trend clearly shows the payoff value increases and decreases with the increase and decrease of the DR. In other words, Payoff gained by the Defender is directly proportional to the DR of the Defender. It shows that the DR and payoff of the GTA-IDS is highest as compared to the other methods. Also, with the addition of the GTA-IDS, the DR and the Payoff of the Defender increases gradually. Figure 12 shows the relation of False Postive Rate and the Payoff of the Defender has also been plotted. With the GTA-IDS module, the values of the FPR swiftly decreases. This leads to the increase in the Payoff of the Defender.

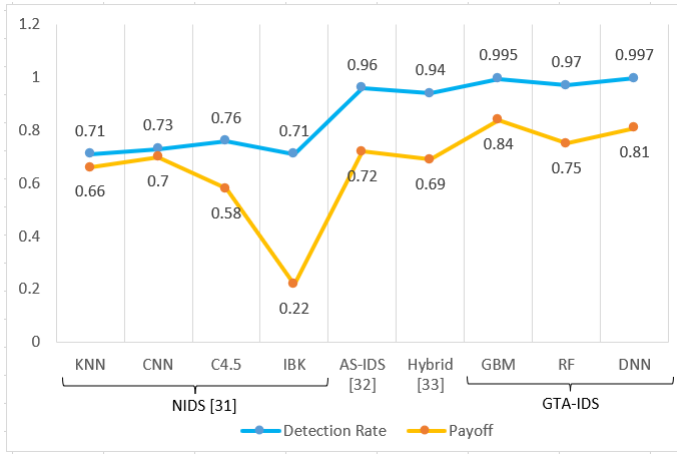

Figure 11. Graph showing Defender's Payoff with the Detection Rate

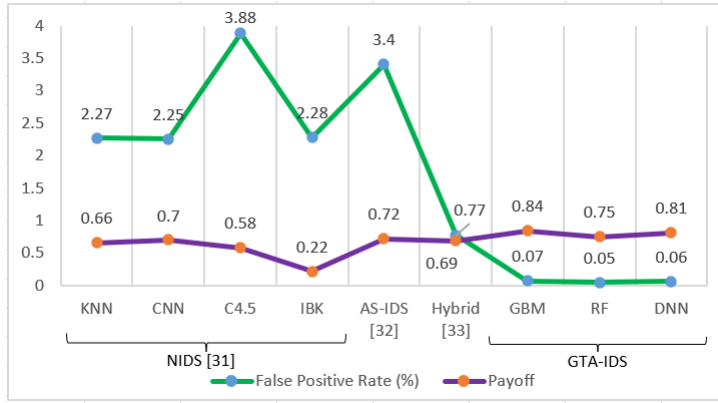

Figure 12. Graph showing Defender's Payoff with the False Positive Rate

Figure 13 shows the comparison of the proposed model GTA-IDS with other models. The bars of the graphs clearly shows the GTA-IDS performs better than other techniques in every parameter. The clubbing of GTA-IDS module with the IDS not only increases the Detection Rate and the Payoffs but also decreases the FPR of the IDS.

7 CONCLUSION

IoT devices are increasing all over the world. However, these IoT devices lack security implications. The devices connected to the cloud can be a massive opportunity for the Attacker to compromise the cloud. The malicious packet can be transmitted

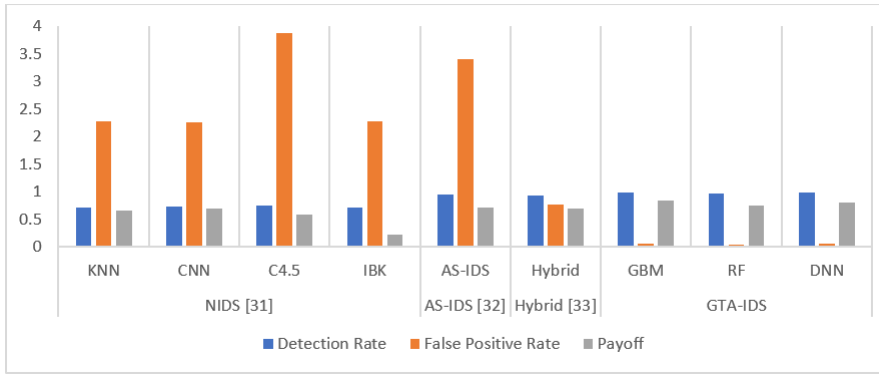

Figure 13. Graph comparing GTA-IDS model with other models

through the insecure IoT device in the cloud network. To make the Defender more efficient and accurate, a game-theoretic model (GTA-IDS) has been devised based on non-zero-sum non-cooperative game theory. The two players, malicious node and Defender, compete against each other to gain maximum Payoff. The game model has been analyzed after specifying the players' payoffs. The analyses show that there exists no pure strategy Nash Equilibrium. However, a mixed strategy Bayes Nash Equilibrium (BNE) has been reached. The probability by which an attacker should attack and a Defender should defend has been calculated. The graphs have been plotted against the payoffs of the two players. The best strategy for the Attacker is to use fewer nodes and increase the time for the attack. The Defender's best strategy is to minimize the energy cost and the attack timing. Further, the model has been applied to the NSL-KDD dataset and results have been compared with NIDS, AS-IDS and Hybrid. With the addition of the GTA-IDS module, the detection rate of the IDS comes to be 99.5 % and FPR comes to be 0.07 % which is better than the existing techniques. This game model can further be extended to a multi-level game.

REFERENCES

[1] Stergiou, C.—Psannis, K. E.—Kim, B. G.—Gupta, B.: Secure Integration of IoT and Cloud Computing. Future Generation Computer Systems, Vol. 78, 2018, pp. 964–975, doi: 10.1016/j.future.2016.11.031.

[2] Conti, M.—Dehghantanha, A.—Franke, K.—Watson, S.: Internet of Things Security and Forensics: Challenges and Opportunities. Future Generation Computer Systems, Vol. 78, 2018, No. 2, pp. 544–546, doi: 10.1016/j.future.2017.07.060.

[3] Gill, K. S.—Saxena, S.—Sharma, A.: Taxonomy of Security Attacks on Cloud Environment: A Case Study on Telemedicine. 2019 Amity International Con-

ference on Artificial Intelligence (AICAI 2019), IEEE, 2019, pp. 454–460, doi: 10.1109/AICAI.2019.8701363.

[4] Gill, K. S.—Sharma, A.: IDPS Based Framework for Security in Green Cloud Computing and Comprehensive Review on Existing Frameworks and Security Issues. 2015 International Conference on Computing, Communication and Security (ICCCS), IEEE, 2015, pp. 1–6, doi: 10.1109/CCCS.2015.7374153.

[5] SonicWall: New Sonicwall Research Finds Aggressive Growth in Ransomware, Rise in IoT Attacks. `https://bit.ly/3o88pmm`.

[6] Antonakakis, M.—April, T.—Bailey, M.—Bernhard, M.—Bursztein, E. et al.: Understanding the Mirai Botnet. 26th USENIX Security Symposium (USENIX Security 17), 2017, pp. 1093–1110.

[7] Akhtar, M. W.—Hassan, S. A.—Ghaffar, R.—Jung, H.—Garg, S.—Hossain, M. S.: The Shift to 6G Communications: Vision and Requirements. Human-Centric Computing and Information Sciences, Vol. 10, 2020, No. 1, Art. No. 53, doi: 10.1186/s13673-020-00258-2.

[8] Wu, H.—Wang, W.: A Game Theory Based Collaborative Security Detection Method for Internet of Things Systems. IEEE Transactions on Information Forensics and Security, Vol. 13, 2018, No. 6, pp. 1432–1445, doi: 10.1109/TIFS.2018.2790382.

[9] Liang, X.—Xiao, Y.: Game Theory for Network Security. IEEE Communications Surveys and Tutorials, Vol. 15, 2013, No. 1, pp. 472–486, doi: 10.1109/SURV.2012.062612.00056.

[10] Aslan, Ö.—Ozkan-Okay, M.—Gupta, D.: Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment. IEEE Access, Vol. 9, 2021, pp. 83252–83271, doi: 10.1109/ACCESS.2021.3087316.

[11] Gan, C.—Feng, Q.—Zhang, X.—Zhang, Z.—Zhu, Q.: Dynamical Propagation Model of Malware for Cloud Computing Security. IEEE Access, Vol. 8, 2020, pp. 20325–20333, doi: 10.1109/ACCESS.2020.2968916.

[12] Gill, K. S.—Saxena, S.—Sharma, A.: GTM-CSec: Game Theoretic Model for Cloud Security Based on IDS and Honeypot. Computers and Security, Vol. 92, 2020, Art. No. 101732, doi: 10.1016/j.cose.2020.101732.

[13] Mardini, W.—Aljawarneh, S.—Al-Abdi, A.: Using Multiple RPL Instances to Enhance the Performance of New 6G and Internet of Everything (6G/IoE)-Based Healthcare Monitoring Systems. Mobile Networks and Applications, Vol. 26, 2020, pp. 952–968, doi: 10.1007/s11036-020-01662-9.

[14] Shakeel, P. M.—Baskar, S.—Fouad, H.—Manogaran, G.—Saravanan, V.—Xin, Q.: Creating Collision-Free Communication in IoT with 6G Using Multiple Machine Access Learning Collision Avoidance Protocol. Mobile Networks and Applications, Vol. 26, 2020, pp. 969–980, doi: 10.1007/s11036-020-01670-9.

[15] You, X.—Wang, C. X.—Huang, J.—Gao, X.—Zhang, Z. et al.: Towards 6G Wireless Communication Networks: Vision, Enabling Technologies, and New Paradigm Shifts. Science China Information Sciences, Vol. 64, 2021, No. 1, Art. No. 110301, doi: 10.1007/s11432-020-2955-6.

[16] Shen, S.—Huang, L.—Zhou, H.—Yu, S.—Fan, E.—Cao, Q.: Multistage Sig-

naling Game-Based Optimal Detection Strategies for Suppressing Malware Diffusion in Fog-Cloud-Based IoT Networks. IEEE Internet of Things Journal, Vol. 5, 2018, No. 2, pp. 1043–1054, doi: 10.1109/JIOT.2018.2795549.

[17] Xiao, L.—Li, Y.—Huang, X.—Du, X.: Cloud-Based Malware Detection Game for Mobile Devices with Offloading. IEEE Transactions on Mobile Computing, Vol. 16, 2017, No. 10, pp. 2742–2750, doi: 10.1109/TMC.2017.2687918.

[18] Fan, G.—Chen, L.—Yu, H.: A Game Theoretic Method to Model and Analyze Attack-Defense Strategy of Resource Service in Cloud Application. Concurrency and Computation: Practice and Experience, Vol. 29, 2017, No. 12, Art. No. e4131, doi: 10.1002/cpe.4131.

[19] Wang, K.—Yuan, L.—Miyazaki, T.—Guo, S.—Sun, Y.: Antieavesdropping with Selfish Jamming in Wireless Networks: A Bertrand Game Approach. IEEE Transactions on Vehicular Technology, Vol. 66, 2017, No. 7, pp. 6268–6279, doi: 10.1109/TVT.2016.2639827.

[20] Fadlullah, Z. M.—Wei, C.—Shi, Z.—Kato, N.: GT-QoSec: A Game-Theoretic Joint Optimization of QoS and Security for Differentiated Services in Next Generation Heterogeneous Networks. IEEE Transactions on Wireless Communications, Vol. 16, 2017, No. 2, pp. 1037–1050, doi: 10.1109/TWC.2016.2636186.

[21] Li, Z.—Xu, H.—Liu, Y.: A Differential Game Model of Intrusion Detection System in Cloud Computing. International Journal of Distributed Sensor Networks, Vol. 13, 2017, No. 1, doi: 10.1177/1550147716687995.

[22] La, Q. D. S.—Quek, T. Q.—Lee, J.—Jin, S.—Zhu, H.: Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things. IEEE Internet of Things Journal, Vol. 3, 2016, No. 6, pp. 1025–1035, doi: 10.1109/JIOT.2016.2547994.

[23] Wang, K.—Du, M.—Yang, D.—Zhu, C.—Shen, J.—Zhang, Y.: Game-Theory-Based Active Defense for Intrusion Detection in Cyber-Physical Embedded Systems. ACM Transactions on Embedded Computing Systems, Vol. 16, 2016, No. 1, Art. No. 18, doi: 10.1145/2886100.

[24] Cheng, Z. M.: A Differential Game Model Between Intrusion Detection System and Attackers for Wireless Sensor Networks. Wireless Personal Communications, Vol. 90, 2016, No. 3, pp. 1211–1219, doi: 10.1007/s11277-016-3386-6.

[25] Wang, Y.—Ma, J.—Zhang, L.—Ji, W.—Lu, D.—Hei, X.: Dynamic Game Model of Botnet DDoS Attack and Defense. Security and Communication Networks, Vol. 9, 2016, No. 16, pp. 3127–3140, doi: 10.1002/sec.1518.

[26] Bedi, H.—Shiva, S.—Roy, S.: A Game Inspired Defense Mechanism Against Distributed Denial of Service Attacks. Security and Communication Networks, Vol. 7, 2014, No. 12, pp. 2389–2404, doi: 10.1002/sec.949.

[27] Spyridopoulos, T.—Karanikas, G.—Tryfonas, T.—Oikonomou, G.: A Game Theoretic Defence Framework Against DoS/DDoS Cyber Attacks. Computers and Security, Vol. 38, 2013, pp. 39–50, doi: 10.1016/j.cose.2013.03.014.

[28] Moosavi, H.—Bui, F. M.: A Game-Theoretic Framework for Robust Optimal Intrusion Detection in Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security, Vol. 9, 2014, No. 9, pp. 1367–1379, doi:

10.1109/TIFS.2014.2332816.

[29] Subba, B.—Biswas, S.—Karmakar, S.: A Game Theory Based Multi Layered Intrusion Detection Framework for Wireless Sensor Networks. International Journal of Wireless Information Networks, Vol. 25, 2018, pp. 399–421, doi: 10.1007/s10776-018-0403-6.

[30] Zhang, Q.—Li, M.—Deng, Y.: Measure the Structure Similarity of Nodes in Complex Networks Based on Relative Entropy. Physica A: Statistical Mechanics and Its Applications, Vol. 491, 2018, pp. 749–763, doi: 10.1016/j.physa.2017.09.042.

[31] Belgrana, F. Z.—Benamrane, N.—Hamaida, M. A.—Chaabani, A. M.—Taleb-Ahmed, A.: Network Intrusion Detection System Using Neural Network and Condensed Nearest Neighbors with Selection of NSL-KDD Influencing Features. 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS), IEEE, 2021, pp. 23–29, doi: 10.1109/IoTaIS50849.2021.9359689.

[32] Otoum, Y.—Nayak, A.: AS-IDS: Anomaly and Signature Based IDS for the Internet of Things. Journal of Network and Systems Management, Vol. 29, 2021, No. 3, Art. No. 23, doi: 10.1007/s10922-021-09589-6.

[33] Depren, O.—Topallar, M.—Anarim, E.—Ciliz, M. K.: An Intelligent Intrusion Detection System (IDS) for Anomaly and Misuse Detection in Computer Networks. Expert Systems with Applications, Vol. 29, 2005, No. 4, pp. 713–722, doi: 10.1016/j.eswa.2005.05.002.

Komal Singh Gill is currently pursuing his Ph.D. from Thapar Institute of Engineering and Technology (TIET), Punjab. He has completed his B.Tech. in computer science and engineering from Lovely Professional University in 2014. He completed his M.Tech. in computer science and applications in 2016 from TIET, Punjab. His research interests include network security, cloud computing, and game theory.

Sharad Saxena received his Ph.D. (CSE) in 2012 and M.Tech. (CSE) in 2009. He authored more than 54 international publications and is a member of societies like IEEE, ACM, IAENG, CSI, and ISRD. He has guided 15 M.Tech. dissertations and four Ph.D. till date. His research interest includes wireless sensor networks and IoT. Presently he is working as Associate Professor in the Department of Computer Science and Engineering at Thapar Institute of Engineering and Technology, Patiala, Punjab, India.

Anju Sharma is working as Assistant Professor in the Department of Computational Sciences, MRSPTU, Bathinda. Her research interests include smart grid computing, cloud computing, IoT, and fog computing. She has varied numbers of publications in international journals and conferences of repute. She is Senior Member of International Association of Computer Science and Information Technology (IACSIT) and a professional member of ACM India, IEEE. She is an active member (TCM and reviewer) of various conferences.