Early detection and mitigation scheme for internet of things based threats in smart home automation.

EARLY DETECTION AND MITIGATION SCHEME FOR INTERNET OF THINGS BASED THREATS IN SMART HOME AUTOMATION

By

Noxolo Tshwarelo Mahapa

Submitted in partial fulfilment of the requirement of the degree:

Master’s Degree in Engineering (MEng): Engineering: Electrical

Field of Specialization: Telecommunications

In the Department of Electrical Engineering / F’SATI

Faculty of Engineering and the Built Environment,

Tshwane University of Technology

Supervisor: Prof. TO Olwal

April 2024

DECLARATION

"I hereby declare that the dissertation submitted for the degree MEng: Telecommunication, at the Tshwane University of Technology, is my own original work and has not previously been submitted to any other institution of higher education. I further declare that all sources cited or quoted are indicated and acknowledged by means of a comprehensive list of references".

Signature:

[redacted]

Date:

20/4/2024

____

Noxolo Mahapa

ACKNOWLEDGMENT

My heartfelt thanks go to the Almighty God, who has been my strength throughout this work.

My heartfelt gratitude also goes to my supervisor, Prof. Thomas O. Olwal, who contributed, guided, read through, made suggestions, corrected, encouraged, and motivated me to complete this work.

My heartfelt gratitude goes to my son Lesedi for allowing me to steal his precious time with Mommy to finish my studies.

I would also like to express my gratitude to my parents, Alex Mahapa and Selina Skosana, for their unwavering support throughout my studies. To my little sister Portia Miya, niece Luyanda Miya, and Aunt Johannah Selomo, thanks for their help in caring for my son during this study time.

I would also like to thank one of the contributors to this work, Steven Tshehla, for your motivation, mentoring, and support throughout this process. May God bless you richly.

Finally, I would like to thank my employer for providing me with this opportunity by sponsoring my studies.

ABSTRACT

The Internet of Things (IoT) technology and applications that are related to the IoT have witnessed rapid development in recent years. An example of an innovation in the field is the emergence of smart home systems (SHS). These systems encompass a range of internet connected devices, smart home automation systems (SHAS), and dependable energy management systems. Such IoT innovations are accompanied with cyber threats that may impact or threaten the smart home users (SHU). In the year 2022, a total of 112 million cyberattacks targeting IoT devices were recorded on a global scale. In order to address this phenomenon, a game theoretical approach has been adopted in this study in order to provide an early detection and mitigation of IoT based security threats in SHAS. The early detection and mitigation of those IoT-based security threats has been achieved using various game strategies such as pure game theory and mixed game theory techniques. The main objective of the proposed system is to ensure an early automatic response of the detection and mitigation of the threats in the SHAS.

The algorithms and the simulation experimental setup were developed in order to achieve the objective of the study which was to improve the response time on the detection technique and early sending rate response for the mitigation of threats in SHAS. Pure game theory has been reported to be much successful in the early detection of security concerns based on IoT. The application of pure game theory in early detection has shown a slight improvement when compared to the use of a mixed game strategy. Additionally, mixed game theory has shown to be a more effective method for SHAS early mitigation of IoT-based security threats. According to the early mitigation results, adopting mixed game theory can help to mitigate IoT-based security threats before damage is done. The study findings indicate that the utilization of a game theoretical method has the potential to yield a modest enhancement in early detection and mitigation of IoT related risks in SHAS.

Keywords: Detection; Game Theory; Internet of Things (IoT); Mitigation; Security; Smart home.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

GLOSSARY

AM	All Monitor
APIs	Application Programming Interfaces
CH	Cluster Head
CPES	Cyber Physical Embedded Systems
CUSUM	Cumulative Sum
DoS	Denial of Service
DDoS	Distributed Denial of Services
DEDA	Distributed Early Detection Algorithm
DNC	Data Normalization Component
EDMAS	Early Detection and Mitigation Scheme
ESN	Embedded Sensor Network
FAN	Field Area Network
FC	Fusion Component
FMK	Firmware Modification Kit
FSC	Feature Selection Components
HAN	Home Area Network
ICT	Information and Communication Technology
ICMP	Internet Control Message Protocol
ID	Intrusion Detection
IDS	Intrusion Detection System.

IDSaaS	Intrusion Detection System as a Service
IoT	Internet of Things
IoT-IDM	Internet of Things Intrusion Detection Management
IPS	Intrusion Prevention System
IPV	Isolated Payoff Vector
LEDEM	Learning-Driven Detection and Mitigation
MAC	Media Access Control
MIMA	Man in the middle attack
MIAMI-DIL	Minimally Invasive Attack Mitigation via Detection, Isolation, and Localization
MLC	Machine Learning Model
PPS	Packets per Seconds
PPDC	Preprocessing Data Component
SC	Sandbox component
SDN	Software Defined Network
SHA	Smart Home Automation
SH	Smart Home
SHAS	Smart Home Automation System
SHU	Smart Home Users
SVM	Support Vector Machine
TCP	Transmission Control Protocol

1 Chapter 1: Introduction of the study

1.1 Research background/justification

The Internet of Things (IoT) is rapidly becoming an important part of our lives, and its impact can be felt everywhere. The IoT is an innovation that combines a wide variety of intelligent systems, frameworks, devices, and sensors [1]. One such innovation is the concept of smart home systems (SHS) and appliances, which consist of Internet-connected gadgets, smart home automation systems (SHAS), and reliable energy management systems [2]. As a result of the convenience and comfort that SHA delivers, consumers run the danger of a security breach [4]. Such innovation is accompanied with threats and obstacles that may impact or threaten the smart home users (SHU) [3]. As most smart SHU lack understanding and technical expertise regarding the operation and risks of IoT devices, they rarely address security issues [5].

Over 112 million IoT cyberattacks occurred globally in 2022. Prior to this the year 2022, there has been a substantial increase in this statistic, with the number of identified cases reported totalling to 32 million in 2018 [6]. In the most recent recorded year, there was an observed year-on-year growth of 87 percent in the occurrence of hacker events related to IoT. Europe is presently noticing the highest number of incidents directed at IoT devices, with an average of over 70 attacks per company on a weekly basis [7]. Following Europe, the Asia-Pacific (APAC) area encounters an average of 64 attacks, Latin America experiences 48 attacks, and North America witnesses 37 attacks. Notably, North America has observed the largest increase in attacks from the previous year, with a significant rise of 58 percent [74]. In the year 2022, organizations in Africa saw an average of 34 weekly cyber-attacks related to the IoT. In 2023, South African organizations experienced a significant increase in the average cost of data breaches, reaching a record high of R49.45 million. This is an increase of 8% over the previous three years and a 73.0% increase since South Africa was included in the study eight years ago [75].

Several efforts have been undertaken in the literature to solve the various security concerns of IoT devices in SHA which included encryption, firewalls, the privacy of information, data protection, and authentication [8-10]. Despite the implementation of many mechanisms aimed at mitigating security attacks in SHAS, the inherent limitations in the computational capabilities of IoT devices render them vulnerable to such attacks. The Intrusion Detection System (IDS) serves as a firewall for data encryption and other traditional security measures. However, due to the ongoing development of the unprecedented growth scale of the network, IDSs based on traditional pattern matching are no longer effective because they slow down the response time to attacks. Consequently, the use of game theoretical approaches to assist with the early detection and mitigation of IoT-based threats to secure an SHAS. It is now essential to detect and mitigate these threats precisely and in a timely manner. This will expedite the identification of threats on IoT devices as well as the implementation of necessary mitigation measures.

In this study, we r propose an early detection and mitigation of IoT-based threats using the game theoretical approach in IDS. Game theory is an advanced branch of applied mathematics that examines how rational players behave when presented with a combination of limited and shared network resources [12]. The model of game theory represents a game between players who choose to behave cooperatively or non-cooperatively and attempt to maximise their gains by executing strategies based on the cumulative actions of the participants [13]. In game theory, there are a variety of strategies that depend largely on the actions of the players, since they both strive to maximise their own interests and the strength of their defence depends on the actions of both players [14]. The dynamics between the attacker and the defender can be regarded as a game wherein both participants aim to maximize their individual gains. Therefore, each player adjusts their actions in response to the strategies employed by their competitor.

The advantage of applying game theory is that it can be used to investigate the various threats in the IoT system and identify likely measures and expected outcomes for controlling future threats. One additional advantage of employing a game model is its enhanced accuracy in evaluating the benefits of both the attacker and the defender. This enhanced accuracy facilitates a more intuitive comprehension of the many challenges posed by attacks on networks [15]. Based on the systematic conclusion of the game-theoretical method, it is possible to construct robust and dependable protections for IoT-based threats that can identify and block them in time to protect the system from threats. With these defences, game theory could be used to solve the problems that arise when individuals with varying objectives and reasons try to use the SHAS.

1.2 Research problem statement

The IDS consistently consume additional resources within the monitored system, even in the absence of any intrusions. When the components of the intrusion detection system are implemented as individual processes, they can be tampered with. A delay in identifying an intruder may allow them enough time to disable or modify the programs operating on the smart home automation system, making the IDS appear useless or untrustworthy. Based on the literature analysis, there exist limited studies on the security of IoT smart home systems that can effectively detect and mitigate cyber-attacks on home automation networks. Consequently, the need to develop a suitable game theoretical technique in order to enhance the detection and mitigation response time of IDS for IoT technology in home automation systems. Hence, the main purpose of this research is to develop an early detection and mitigation of IoT-based threats in a SHAS using game theory.

1.2.1 Sub-problems

The following are the research sub-problems derived from the problem statement:

- There exists a sizeable amount of delay in IDS when it comes to identifying the IoT based-threats on SHAS. Hence, it is crucial to establish a highly effective early detection IDS using game theory.

- There a sizeable amount of delay in IDS when it comes to minimising the IoT based-threats on SHAS. Hence, it is crucial to establish a highly effective early mitigation IDS using game theory.

1.3 Research hypotheses

The following are the research hypotheses:

- A suitable game theoretical strategy can improve the early detection of the IoT system-based threats in SHA.

- A suitable game theoretical strategy can improve the early mitigation of the IoT system-based threats in SHA.

1.4 Research strategies

In order to address the above-mentioned research sub-problems, the following strategies are adopted in this study:

1.4.1 Literature survey

The literature survey study looks at the detailed overview of the current methods that have been used for the detection and mitigation of IoT based threats in SHA.

1.4.2 System modelling

The modelling of the system was based on the conceptual models derived from the comprehensive literature reviews. The concepts, methods, algorithms, and techniques chosen for this study are analysed and justified here.

1.4.3 Performance or validation of system modelling

The following areas are considered in this study:

- Computation complexity (algorithm implementation).
- Processing and computational capabilities (software level).
- Simulation capabilities (analysis implementation).

1.4.4 Analysis and results

The analysis and the results were compared to establish how the response time of the detection and mitigation scheme compares with those that have already been proposed.

1.5 Delimitations of the study

The delimitations of the study are:

- The study did not use blockchain technology methods for the detection and mitigation of the IoT based threats in SHASs. The blockchain can monitor the data collected by the sensors, blocking their duplication by means of adding inaccurate data. Using blockchain technology, sensors can also transfer data without the need for a trusted third party. However, the main drawbacks of blockchain are its high energy dependence, complicated integration method, and expensive implementation costs.

- The study did not use the software defined network (SDN) method for the early detection and mitigation of the IoT based threats in SHASs. The SDN is a networking model that directs network traffic using software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure. The SDN may enable the collection of network application data, which could aid in the improvement of design of an attack detection algorithm. Due to the more complicated technologies it uses and the specialised management skills required, an SDN could be more difficult to maintain than traditional networking.

- The study will not use any IDS method for the early detection and mitigation of IoT based threats in SHAS. The IDS monitor the routers, firewalls, essential servers, and files and it uses its database to send alerts and trigger alarms. The main drawbacks of the IDS are the false alarm rate, low detection rate, unbalanced datasets, and response time.

- The proposed scheme was limited to the denial of service (DoS) threats and the distributed denial of services (DDoS) only. This is so because it has been found in the literature that these types of threats have to be the most dominant attacks in the IoT-based smart home automation.

1.6 List of publications

This study resulted in a submitted journal article for review and a published conference paper at peer reviewed conference proceeding

Mahapa N. T, Olwal T. O, "Early detection and mitigation of IoT based threats in smart home automation using game theory", under review at Journal of e-Prime Advances in Electrical Engineering, Electronics and Energy 2024.

Mahapa N. T and Olwal T. O, "A game-theoretic approach to the early detection of Internet of Things-based threats in smart home automation" in Proc. IEEE i-COSTE 2023 Conference, held at Fuji, 4- 6 December 2023.

1.7 Outline of dissertation

Chapter 1: Introduction —This chapter covers the introduction to the research, the problem to be researched and the subproblems that need to be addressed. The hypothesis of the envisaged solution and the delimitation of what is not covered.

Chapter 2: Literature review – This chapter provides a thorough examination of the current scholarly literature that is appropriate, up-to-date, and sourced from trustworthy academic publications. This comprehensive study identifies gaps in the relevant research and the conceptualisation of the proposed solution.

Chapter 3: System modelling of early detection and mitigation scheme– this chapter entails the formulation of the research problem and the design of early detection and mitigation scheme for the IoT-based threats in home automation. The modelling of the early detection and mitigation scheme will be based on the conceptual models derived from the comprehensive literature review.

Chapter 4: Performance evaluation – In this chapter, the researcher presents simulations and the technical design of the simulation experiments. The proposed solution or algorithm regarding the early detection and mitigation scheme for IoT-based threats in home automation are validated via computer simulation tests and the results are compared with the results of the existing solutions.

Chapter 5: Conclusion and recommendations– In this chapter, the researcher presents the main results of the study in relation to the study objectives and further recommendations for future work.

1.8 Summary of the chapter

In this chapter, the background and justification of the study were presented. A statement of the study problem, the sub-problems and the hypotheses were outlined. The chapter also furnishes a precursor to the methodology that the study employed and it highlights the contribution that the study makes to the body of knowledge and related real-world applications. In the next chapter, the researcher presents the comprehensive literature review of the related works.

2 Chapter 2: Literature review

2.1 Introduction

Potential IoT security threats and their impact on SHU are on the increase, necessitating that those products such as smart locks, smart refrigerators, and home energy management improve their security measures. An evaluation of the early detection and mitigation conditions in IoT-based SHA environments was conducted, and a technique for determining their security requirements was proposed [16]. It was discovered that the expanded capabilities of SH technology present both original threats and new outcomes for several traditional threats which affects the operations and the availability of the SHS. It is therefore necessary to early detect and mitigate both old and new vulnerabilities that pose threats in SHA environments as early as possible. Several studies based on game theory and its approaches have been discussed in the field of computer network security to model, evaluate, and optimise the performance and efficacy of detection systems in IoT-related technologies [17]. The purpose of this dissertation is not to cover the entire field, but rather to precisely describe in detail the response time for the detection and mitigation approaches used to defend the SHAS from IoT-based threats.

This section comprises subsections introduced in the subproblem, and each subsection offers the user with knowledge pertinent to detecting and mitigating IoT-based threats in smart home automation. Section 2.2 discusses ways of IoT-based threat detection strategies in smart home automation. The strategies for mitigating IoT-based threats in smart home automation are provided in section 2.3. Joint detection and mitigation strategies are described in section 2.4. Section 2.5 discusses the literature related to the theory being proposed in this study. In section 2.6, the chapter summary is presented.

2.2 The detection technique for IoT based in smart home automation

Detection is the process of observing or detecting something of an unexpected character in a particular environment. Detection and effective prevention result from identifying and acting upon signs of risks [18]. Diverse academics have presented techniques for detecting IoT-based threats in various situations [19-21]. Threats and vulnerabilities targeting the availability and the operation of the SHAS are not new; they have been studied for some time, and numerous security measures have been presented [22]. Developing an efficient and effective solution capable of detecting these

IoT-based dangers as early as possible remains a challenge [23]. The following section presents the reviewed literature in the detection of IoT based threats in SHAS using different techniques.

2.2.1 An intelligent security approach using game theory to detect DoS attacks

Yazdankhah *et al.* [24] used game theory to study the security of IoT networks and find Denial-of-Service (DoS) attacks. So far, several ways have been shown to make the IoT more secure. These interventions include light and safe operating systems, scalable methods for alternative control, and new ways to find and stop new threats. It is most important to remember that any kind of attack on a network can cause damage that cannot be fixed by users, devices, things, and their communications. One of the main attacks that attackers use is called a DoS attack. The purpose is to stop services and network communications from working, and most of the time it stops the network from working. The goal of this paper was to use game theory to develop a smart way to protect against DoS attacks in the services of the IoT network.

The important factors at the time of the DoS attacks including energy consumption, latency, and operational throughput were investigated. From an innovation perspective, the research contributions are:

- Classifying and evaluating the denial-of-service attacks in wireless networks.
- Acquiring a suitable equilibrium, based on the Nash equilibrium, to achieve a security balance of the IoT.
- Presenting a smart method for detecting an attack based on game theory.

The signal game can be thought of as a two-player game between the destructive signal transmitter and the node (transmitter/receiver). The equations can be made based on how well each player performs and what their goal is. A player sends out the destructive signal, which stops users from talking to each other by blocking the communication channels in the wireless network and making it impossible to send and receive data in the target channels. The node is a player whose job it is to make the best use of the network channels so that the whole network can do more work. In the game, each player tries to obtain the most money at the end. When one considers the number of strategies in the game and the fact that various strategies could be used to attack at the same time, it is evident that it will be very difficult to reach a deterministic Nash equilibrium.

The suggested method was run through the NS2 simulator to check how well it would work in the network. A comparison was made between the three systems based on their operational throughput, latency, and energy use. Based on game theory, the results of this paper showed that smart methods can perform better than other strategies in terms of energy use (25–30%), latency (10–15%), and operational throughput (10–25%). Figure 2.1 presents an analysis of various types of attacks, namely reactive, random, deceptive, and persistent attacks, in comparison to the no-attack scenario. Resource scarcity is the primary vulnerability of DoS. This could result in a jamming attack, in which the attacker floods the network's several pathways with excessive packets. The functions of persistent, random, deceptive, and reactive are all considered to be attacks. This action disrupts the network by flooding it with unnecessary data packets, causing congestion and hindering the ability of genuine systems to send and receive packets. It has the potential to cause a delay in transmission or completely reject legitimate packets. If there is persistent jamming, the attacker continually releases data at regular intervals. The operational throughput, latency, and energy consumption is evaluated. This analysis considers different time intervals within the sensor network. The investigation was conducted by quantifying three parameters of the sensor network. Despite the approach demonstrating enhanced energy consumption, latency, and operational throughput, it is not practical for the current research. It focuses on only one attack which is the DoS attack and does not cater for a SHAS.

The adoption of game theory as a detection strategy proved to be the most effective choice. One limitation of this approach is its failure to assess response time in identifying potential dangers, limiting its utility in supporting the study.

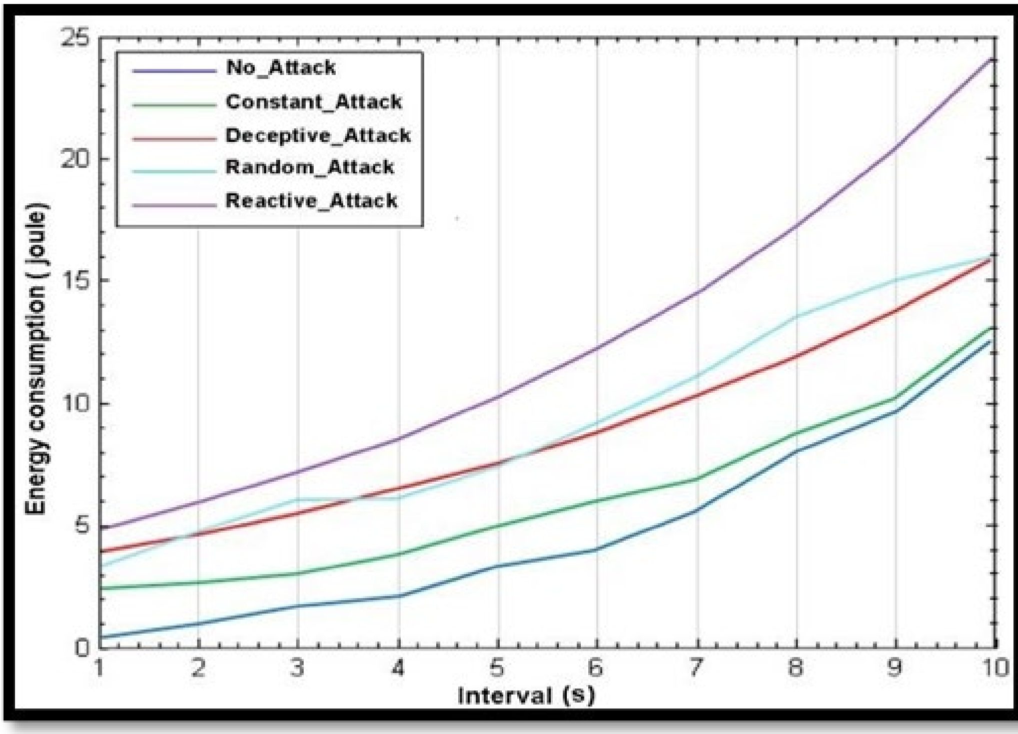

Figure 2.1:Comparison of energy consumption (Proposed vs optimal) [24]

2.2.2 Game Theory Based Collaborative Security Detection for IoT Systems

Wu *et al.* [25] proposed a collaborative method for finding security problems in IoT systems. The researchers noted that many existing IoT systems are not protected against a wide range of malicious attacks. This is so because devices can be accessed from anywhere through a trusted network, and their security protection strategy is still at a low-level stage. As a result of this, the study aimed at finding a way to make the whole system as safe as possible. Considering how the defender and the attacker face off against each other, a game-theoretical analysis framework is made for collaborative security detection. The goal is to make sure that all IoT systems have the most secure protection possible. Each object can collect observations, process them, and then use them to create its own local security profile. Then, the objects share their local profiles with nearby objects and use a fusion scheme to decide how to detect things in real time.

A game model is firstly established to describe how the utilities of the players are affected by their behaviours. In centralised security detection, a central processor is adopted to collect the profiles from the nodes in the entire network and then to make a unified decision based on the fused information. Specifically, the researchers define two events $H0$ and $H1$ by $\{H0$: $\boldsymbol{a} = 0\}$ and $\{H1$:

$\boldsymbol{a} \neq 0\}$. Then, the detection decision of centralised security detection is made by the following testing hypothesis:

$$\frac{1}{N}\sum_{i=1}^{N} x_i \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \delta^c \qquad \text{……………………………….. (2.1)}$$

Table 2.1 represents a summary of the notation used to collaborate this security detection technique. The existence and uniqueness of the Nash equilibrium of the game model with complete consensus are analysed. To analyse the uniqueness of the Nash equilibrium of model *C* with great complexity, Wu *et al*. [25] firstly simplified the problem with the aid of a dimensionality reduction technique. The basic idea is illustrated as follows. Define a function F(*a*) as:

$$F(a) \triangleq \max_{a_1,\cdots,a_N} \mathcal{S}$$
$$s.t. \sum_{i=1}^{N} a_i \; Na, \; a_i \geq 0, \; i = 1, \cdots, N. \qquad \text{………. (2.2)}$$

Then, *F(a)* denotes the maximum-security damage to the network with limited total *Na* resources from the perspective of the attacker only. Then, an iteration-learning-based calculation method is presented to determine the Nash equilibrium. Quantitative analysis is performed for the relationship between the Nash equilibria of the game models in cases of complete and incomplete consensus with an infinite and a finite number of iterations. The results of the simulation considering a DDoS attack are also provided to verify the theoretical results.

The above research showed the detection method for monitoring IoT systems using the game theory. The researcher discovered that the some of the methods adopted in this research can assist in the research to improve the response time for to the detection of the IoT threats in SHA. The drawback to this system is that the detection rate is not determined and the focus does not fall on SHA. The research showed how game theory can be incorporated in the current detection technique.

Symbol	Meaning
N	Number of the IoT nodes
N_i	Neighbourhood set of node I, i=1..., N
x	Detection profile vector, $x= [x_1, \ldots\ldots, x]^T$
$x(m)$	Fused profile vector after m consensus iterations
v	Noises vector in the profiles, $v= [v_1 \ldots v]^T$
C	Consensus matrix, C =[c_{il}]
$\boldsymbol{a}$	Attack resource vector $\boldsymbol{a}= [a_1, \ldots\ldots\ldots, a]^T$
M	Number of iterations for reaching consensus
M^*	Optimal M to maximize the utility of the defender
W_1	Security asset of node I, $I =1, \ldots\ldots, N$
$S(a_1)$	Damage degree to node I, $I = 1, \ldots\ldots, N$
S	Damage to the whole network S =$\sum S(a_i) W_i$
I/C	Game model with incomplete/complete consensus
U_A/U_D	Utilities of the attacker and defender in a game I
U_A^c/U_D^c	Utilities of the attacker/defender in game C

Table 2.1:Summary of notations

2.2.3 Detection of intrusion into Cloud -Fog based IoT networks using game theory

Pirozmand *et al.* [26] used the game theory strategy to find a way to detect intrusions in cloud-fog-based IoT networks. The IoT is a new technology that connects the Internet to smart objects in the real world. However, connecting smart things in the real world to the Internet could pose security risks in many of the actions performed every day. The IoT systems cannot use common security measures against threats because there are so many communication standards and stacks, not enough computing power, and so many devices that are all connected. Due to this reason, it is important to make IoT-specific security solutions so that users of organisations can find all the weak points of a system. So, game theory is used in this study to improve the performance of intrusion detection systems.

In the proposed method, intrusion detection is defined as the process of finding hackers and other people who break into a computer system. Pirozmand *et al.* [26] assumed the interactions between the attacker and the intrusion detection system to be a two-player game, where things change all the time. In game theory, a nonparticipator game is one in which the players cannot talk to each other, make deals, or work together in any way. The main parts of game theory are the players, their actions, their profits, and the information they have about the game.

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 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 results obtained from the simulation of the proposed method showed that the use of intrusion detection systems on the IoT based on cloud-fog, can be very effective in identifying attacks with the least number of errors in this network.

The above method focuses on improving the performance of the IDS in cloud fog and not on SHA. Although their method has shown an improved correct detection rate it is stated that it can be used efficiently in smart systems in real time applications in the future. One limitation of this system is the varying impact of different elements on the players within the suggested game model, which in turn affects the rate of different detection methods and the release rate. Therefore, it may be observed that there is a need for enhancement in the performance of the aforementioned system.

2.2.4 Selfish node detection based on hierarchical game theory in IoT systems

Nobahary *et al.* [27] combined reputation and game theory to locate nodes that exhibit opportunistic and negative behaviour. The major issue of the IoT network is that some nodes do not work together due to the Internet connection of the ‘things'. Multiple-hop data transmission is difficult as selfish nodes send only their data packets. They do not forward the data packets of the neighbours since they want to save energy. Other nodes are malicious; they harm and exploit network facilities. Finding and naming selfish and malevolent nodes eliminate their detrimental impacts. Several methods have been suggested such as the reputation-based strategy, from which nodes receive feedback from other nodes.

The network knows that selfish nodes have worse reputations than the reliable nodes. These systems have a low throughput, and require a large amount of energy as well as allow selfish and malevolent nodes to operate together. The system does not punish or encourage selfish nodes to work with others and it does not give them a second opportunity. Game theory can also uncover selfish nodes. Game theory is an applied mathematical theory that models and analyses situations in which each player strives to win by analysing the strategies of others. Game theory-based methods identify selfish and malicious network nodes using payoffs and incentives. They have fewer false-positives and require less time, supervision, and hardware than other methods.

The game can be formally represented as $G = \{N, A^k, u^k\}$. N represents the total count of nodes within the network. A^k denotes the set of nodes, whereas u^k signifies the set of utility functions, which corresponds to the outcomes generated by players in a single round. The round is designated as round k. To provide additional clarification, let $A^k= [A^k_1, A^k_2..., A^k_n]$ represent the collection of node actions in round k. For instance, A^k_i denotes the action performed by node i during round k. The method under consideration employs a modelling approach that represents the system as a combination of mixed or random strategies. The methodology assigns probabilities to various methods employed by each participant. The field of game theory utilizes punishment and reward processes. In instances where nodes exhibit disruptive behaviour, their data packet transmission power and/or collaborative efforts with other nodes are diminished as a means of retribution and motivation towards fostering cooperation. The improvement of network performance, accuracy, average end-to-end delay, and energy usage can be achieved by the detection of non-cooperative nodes.

False-positive and false-negative rates can also be used to compare algorithms. The performance of the network is considered satisfactory when the values of these metrics are minimized. Additionally, the proposed method exhibits a lower rate of false positives and false negatives compared to earlier detection methods. Figure 2.2 illustrates the data flow in the game theory-based mechanism that encourages selfish nodes on the IoT to cooperate. Evaluation metrics are defined below.

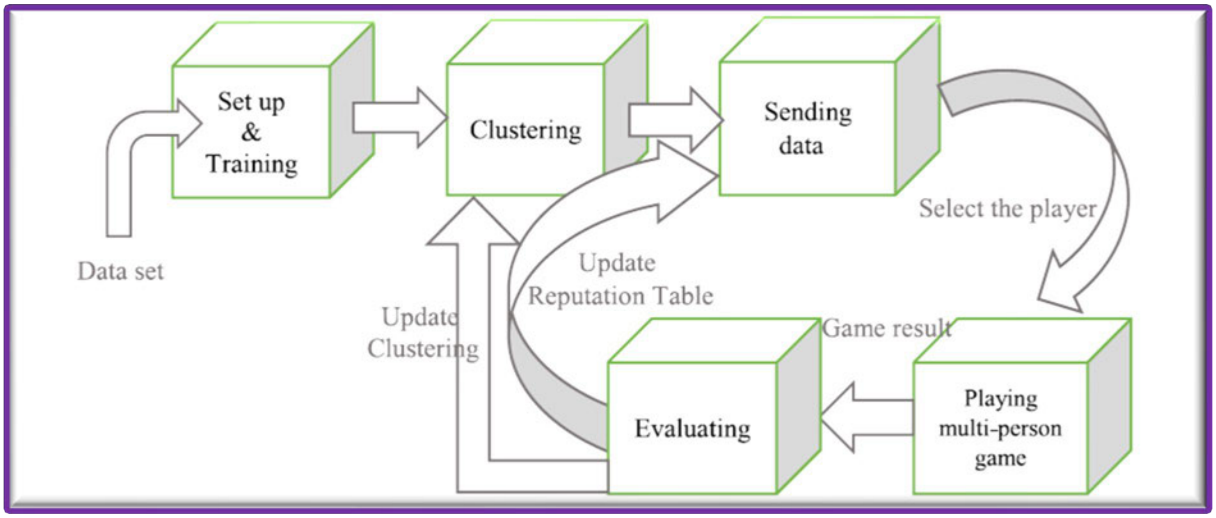

Figure 2.2: General diagram of the proposed mechanism [27]

The detection rate of the selfish node is determined by Equation (2.3).

$$\mathrm{DA} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \quad \text{..................................} \quad (2.3)$$

The false-positive rate (FPR) is calculated using Equation (2.4) and is defined in the following:

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \quad \text{............................} \quad (2.4)$$

$$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{FN} + \mathrm{TP}} \quad \text{............................} \quad (2.5)$$

The parameter is utilized for the assessment of the effectiveness of selfish node detection algorithms. The equation (2.4) defines the false-negative rate as the proportion of selfish nodes incorrectly identified as normal nodes, divided by the total number of selfish nodes detected by the normal node *(FN)* and the number of properly detected nodes (*TP*) in the network.

In many IoT contexts, throughput is used as a measure of network performance. The average end-to-end latency refers to the duration required for a packet to go from its originating node to its intended destination. The simulation environment employed in this study is MATLAB, wherein a base station is strategically placed at the centre of each of the four simulated network configurations. When calculating the average throughput, which is the proportion of successfully delivered data packets, an increase of up to 20% is possible, while an improvement of 12% is achieved in the average end-to-end delay.

The results indicate that the proposed methodology successfully detects nodes that exhibit selfish and malicious behaviour, hence mitigating their ability to delay the transmission of data packets, engage in data theft, or deplete network resources such as electricity, battery power, and memory. The approach would have assisted in this research; however, it still does not incorporate the response time and their detection technique is limited to only selfish and malicious nodes.

2.2.5 Game theory based active defense for intrusion detection in CPES

Wang *et al.* [28] suggested a new attack-defence game model to detect malicious nodes via repeated games in this article on intrusion detection (ID). Cyber-Physical Embedded Systems (CPESs) are distributed embedded systems containing actuators and sensors. As embedded sensor networks (ESNs) proliferate, data security from sensors to destinations is a key study field. The ESNs cannot use wired or wireless network security measures due to power, storage, and computing restrictions. The CPESs are rapidly becoming a major computing paradigm for environmental monitoring infrastructure management energy saving and innovation healthcare intelligent traffic control and homeland security.

Embedded and real-time systems are used to merge calculations and physical interactions. Security has usually focused on physical access limitations and software to disable a device if tampering is suspected. Network security challenges are getting more attention as technology advances. The IDSs safeguard modern technologies against data encryption and other standard security techniques. The IDSs based on pattern matching are useless due to the invasion and network expansion.

This problem is addressed by a game-theoretical-based IDS with third-generation intrusion detection pattern matching technology. A game model is superior at evaluating the rewards of an attacker and a defender, which can intuitively explain the infiltration challenges of several networks. If the correct game model is adopted, the rigor and precision of game theory can assist in making the best decision. The other intrusion detection system is unable to evaluate the Nash equilibrium through the game process and determine the optimal strategy. The researcher designed an assault-defensive game model using game theory to identify the optimal attack and defence methods through repeated games.

The model of the attacks-defences game is presented in Figure 2.3. It displays the strategies of the attacker against the defender and their payoffs. Both attackers and defenders are free to pick their own strategies to maximise their respective payoffs. However, when an attacker initiates an attack, defenders must reply promptly and select the appropriate techniques to repel the onslaught. In addition, the IDS must detect threats correctly and precisely by resolving the detection error and detection omission issues. In industrial contexts, ESNs are likely to be assaulted by many types of attacks. Therefore, it was necessary to create new procedures or to change the existing security systems to address these issues.

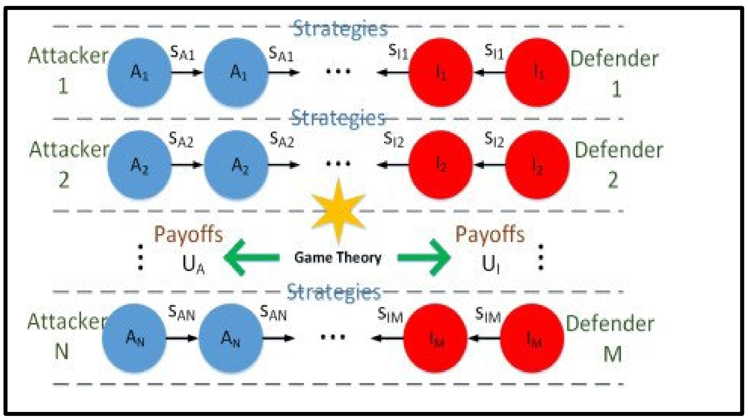

Figure 2.3: A attacker and defender game model [28]

The IDS need to detect the attacks correctly and accurately by solving the error detection and the missing detection problems. The game is defined as G as G _ {{A, I}, {SA, SI}, UA, UI, T}, where {A, I} is the finite collection of players by N _ {1, 2, . . . N}, wherein A _ {$A1$, $A2$, . . . AN} represents the attacker intrusion nodes and I _ {$I1$, $I2$, . . . IM} represents IDS defender defence nodes. {SA, SI} is an offensive and defensive strategy collection of players, wherein SA _ {SA,1, SA,2, . . . SA, N} represents the offensive node strategies, which can launch various types of attack or not. Importantly, error detection and missing detection are taken into consideration in IDSs, where a game tree model is introduced to solve this problem. In addition, pure Nash equilibrium and mixed Nash equilibrium are analysed and their existence is proved.

Simulations indicate that the suggested model can reduce energy usage by up to fifty percent compared to the existing All Monitor (AM) model and enhance the detection rate by up to ten to fifteen percent compared to the existing Cluster Head (CH) monitor model. The ESN intrusion detection model of the repeated game can discover a balance between energy consumption and security based on a game analysis of the tactics of the node behaviours, resulting in greater payoffs than the AM model.

Considering the way, strategies were utilised to increase the detection rate by 10–15% compared to earlier methods, their findings can help improve the detection methodology to obtain the highest detection rate. By increasing the rate of detection and taking attacks into account, smart home automation can achieve greater gains. This research aided the proposed technique to detect threats accurately and in advance.

This research focuses on ID methodologies and proposes a new attack-defence game model for detecting malicious nodes through a repeating game approach. Their approach is very effective and efficient as the IDS used can detect threats correctly and precisely as the detection error and detection omission issues were resolved. This approach can contribute immensely into this research and will be implemented to this research and we will incorporate of main goal which is to improve the response time for the detection of IoT based threats.

2.2.6 DEDA: An algorithm for early detection of topology attacks in IoT systems

The IoT is utilised in several domains, encompassing domestic, industrial, and critical system requirements. These systems include a wide range of applications, such as home settings, transportation networks, power generation facilities, industrial production processes, and healthcare environments. The security of data generated by systems of this nature, as well as the IoT systems themselves, is of utmost importance in these applications. The early detection of potential threats aimed at IoT systems is crucial in order to mitigate the extent of harm caused. In this research article, the authors Karande *et al.* [70] presented a distributed technique aimed at early detection of these threats recognising through the utilisation of predictive descriptor tables. The distributed early detection algorithm (DEDA), which is developed for the detection of topological attacks in the IoT network, operates by strategically deploying monitoring nodes alongside regular nodes to facilitate attack detection. The strategic placement of additional nodes would facilitate the continuous functioning of regular nodes by mitigating the computational and memory load associated with performing detection algorithms on them.

The proposed monitoring nodes will be responsible for overseeing every aspect of data transmission originating from neighbouring IoT nodes; hence, facilitating the construction of a comprehensive descriptor table. Each monitoring node is in the process of generating a partial descriptor table and concurrently maintaining a log of modifications made to the partial descriptor table. The log of modifications and present values is utilised for early anticipation of the descriptor table. The anticipated descriptor table is disseminated among other monitoring nodes. The process involves the collection of aggregate values from the descriptor table that are obtained from other monitoring nodes. The compilation of the anticipated descriptor table will provide a comprehensive overview of the present condition of the system to each monitoring node. Monitoring nodes utilise the anticipated descriptor table in order to identify the existence of the assailant and ascertain the specific node responsible for the attack, as well as the nature of the attack being executed. The dissemination of information regarding the identified attacker is distributed to other nodes in order to facilitate appropriate actions and precautionary measures.

Figures 2.4 below illustrates the accuracy of forecasting the rank and version number of a node in the future. These predictions are based on the historical values recorded in the descriptive table. In addition to the rank and version number, there exist other features that exhibit a higher level of predictability. Furthermore, it is apparent that maintaining an extensive historical record is unnecessary due to the imminent saturation of accuracy. The quick detection of security breaches targeting IoT devices is of utmost importance, and it heavily relies on the misuse of predicted features. The accuracy of recognising the attacker ahead of time is illustrated in Figure 2.5. The ability to accurately predict events far into the future is limited, and so, a decision must be made regarding the trade-off between accuracy and the period of time being predicted while implementing the suggested method. The efficiency of early attack detection has been proved through an extensive simulation study. The algorithm being reviewed demonstrates significant potential for enabling timely detection of threats and mitigating their impact on IoT systems. However, the suggested technique is subject to certain limitations, namely the requirement for additional resources to deploy monitoring nodes and its inability to detect unknown threats. This proposed algorithm will be incorporated in this research using the game theoretical model for detection.

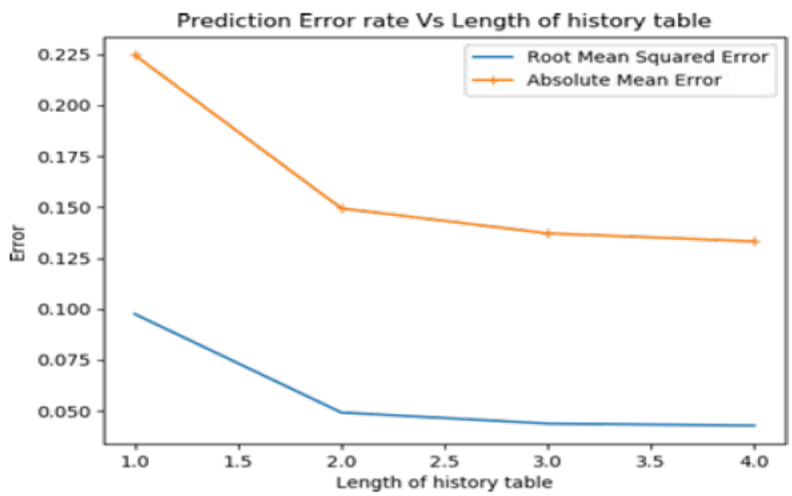

Figure 2.4: Rank of prediction accuracy [70]

(b)

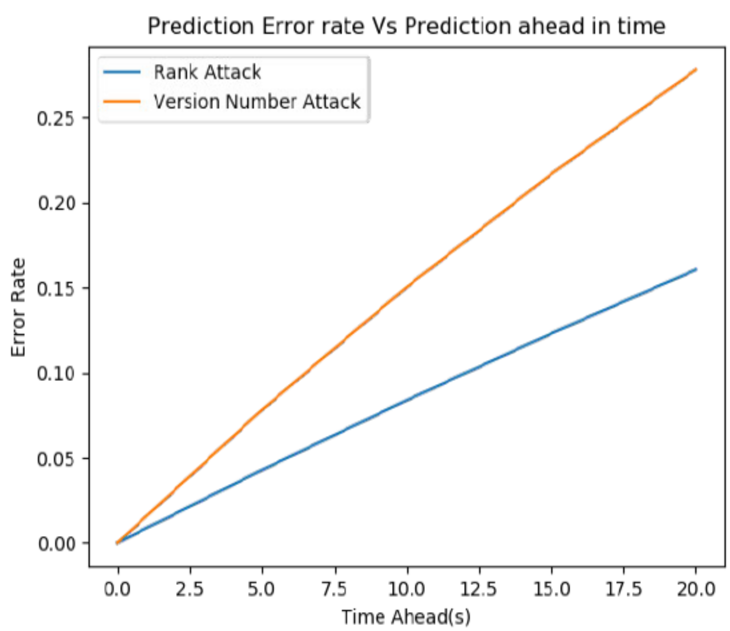

Figure 2.5: Accuracy of attack detection [70]

2.2.7 A collaborative approach to early detection of IoT Botnet

In this study, Giang *et al.* [71] presented a collaborative machine learning model that aims to automate the early identification of IoT Botnet. The suggested model incorporates numerous features that extend beyond the traditional full-time series data-based approaches. The suggested methodology employed a fusion of conventional dynamic characteristics inherent in the IoT Botnet. The aforementioned dynamic aspects are derived from data obtained through the V-Sandbox environment, encompassing network traffic, system call, and system resource utilisation information.

The Sandbox Component (SC) is an essential element that provides a conducive environment for monitoring behaviour and enabling the ELF executable to effectively demonstrate its behaviour.

The pre-processing Data Component (PPDC) is responsible for performing data pre-processing on the data obtained from the Sandbox Component (SC) in order to generate vectorised feature data.

The Data Normalization Component (DNC) refers to the procedure of transforming data obtained from the output of the Pre-processing and Data Cleaning (PPDC) component into a collection of normalised values that are appropriate for utilisation in machine learning algorithms.

The Feature Selection Component (FSC) is responsible for automatically selecting the features that have the most contribution to our prediction variable.

The Machine Learning Classifier Component (MLC) consists of a singular machine learning classifier that is well-suited for the specific output features of the Forward Error Correction (FEC) system.

The Fusion Component (FC) is responsible for integrating the categorisation outcomes generated by individual Machine Learning Components models (MLC).

The dataset holds significant importance in the evaluation of the suggested model. At present, there is a lack of datasets related to the IoT Botnet in a broader context, with a specific shortage of datasets focusing on resource-constrained IoT devices. The benign samples are obtained by extracting firmware images from resource-constrained IoT devices present on the network, including routers, IP cameras, smart lights, and similar devices. The FMK (Firmware Modification Kit) tool is utilised by the writers for this task.

In order to assess the performance outcomes of the suggested methodology, a dataset of 8911 samples was gathered. This dataset consisted of 5023 instances of IoT botnet samples and 3888 instances of benign samples. The implementation was deployed on a server equipped with an Intel Xeon E5-2689 CPU running at a clock speed of 2.6 GHz, and a total of 32 GB of RAM. The installation of V-Sandbox is carried out in accordance with the source code provided by the author on the Github platform [74]. The many machine learning algorithms that were evaluated, including Support Vector Machine, K-Nearest Neighbors, Decision Tree, Random Forest, etc., were implemented using the Python programming language and the Scikit-learn library (Sklearn). The outcomes of these individual machine learning models are collected using the Voting merge function, with the inclusion of Logistic Regression for comparative analysis. There are a total of 64 possible combinations when considering the integration of the four aforementioned common machine learning methods.

A total of 128 outcomes have been assessed to determine the accuracy of the proposed model for detecting IoT Botnet malware, as depicted in Figure 2.6. Based on the obtained results, it can be observed that the Voting function exhibits a higher level of efficiency in comparison to Logistic Regression. Additionally, the combined utilisation of the KNN algorithm for network traffic data, Random Forest for system performance data, and KNN for system call data, referred to as the trilogy KNN + Random Forest + KNN machine learning algorithm, yields the most optimal outcomes with an accuracy of 99.37% as measured by the Area Under the Receiver Operating Characteristic Curve (AUC-ROC).

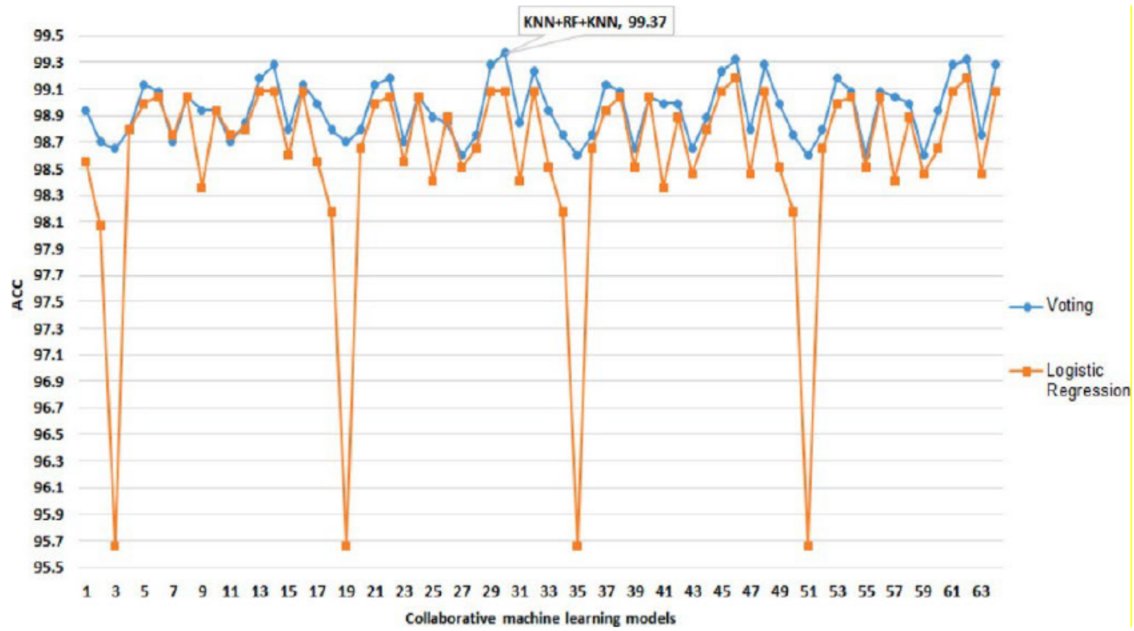

Figure 2.6: Evaluation of the collaborative machine learning algorithms [71]

Table 2.2 summarises the reviewed detection strategies for IoT-based threats utilising game theory. The methodology, aims, and results are summarised in Table 2.2. Although the utilization of diverse game theory strategies enables the achievement of high detection rates and accuracy, there remains potential for further enhancement. The technique described in this study incorporates a comprehensive review of relevant literature and employs a pure game strategy to improve the detection rate and precision of the IoT smart home automation system.

Reference	**Objectives**	**Method**	**Results**	**Drawbacks**
Yazdankhak *et. al.* [24]	To detect the DoS attacks and prevent the problems in the services of network of internet of things.	Signaling game using Nash Equilibrium	Compared to the other strategies, it works better in terms of energy use (25–30%), latency (10–15%), and operational throughput (10–25%).	The adoption of game theory as a detection strategy proved to be the most effective choice. One limitation of this approach is its failure to assess response

				time in identifying potential dangers, limiting its utility in supporting the study.
Wu *et. al.* [25]	A collaborative security detection by considering the confrontation between the defender and the attacker.	Nash Equilibrium	There is a quantitative analysis of how the Nash Equilibriums of the game models relate to each other when there is complete or partial consensus and an infinite or finite number of iterations. The researchers also gave the simulated results that considers a DDoS attack to back up our theoretical results.	One limitation of this system is the lack of a set detection rate, and the emphasis is not placed on smart home automation. The study demonstrated the potential integration of game theory into the existing detection technique.

Pirozmand *et. al*. [26]	To detect the intrusion of attacks in IoT networks in the distributed intrusion detection system.	Dynamic Game Model	The parameters used to evaluate the proposed method are time, correct detection rate, reporting rate and emission rate of the infected smart object.	One limitation of this system is the varying impact of different elements on the players within the suggested game model, which in turn affects the rate of different detection methods and the release rate. Therefore, it may be observed that there is a need for enhancement in the performance of the aforementioned system.
Nobahary *et. al.* [27]	The objective is to identify nodes showing selfish and malicious behaviour by utilizing reputation and game theory.	Reputation and Mixed Game Strategy.	The results indicate that the proposed approach effectively detects self-serving and malicious nodes, thereby mitigating end-to-end data packet latency and minimizing resource consumption by nodes (such as electricity, batteries, memory, etc.).	A key constraint of the proposed methodology is that it affords dangerous and self-interested nodes an increased opportunity to engage in

			A maximum of 20% of data packets successfully reach their intended destination, while the average duration of transmission from the source to the destination is reduced by 12%.	collaboration with other nodes. Furthermore, it fails to quickly remove the nodes from the network. This is due to the fact that as the proportion of such nodes increases, while the network encounters a decrease in performance.
Wang *et. al*. [28]	To identify attacks by detecting anomalous system behaviours.	Repeated Game Approach.	Simulations indicate that the suggested model can reduce energy usage by up to 50% compared to the existing AM model and increase the detection rate by up to 10 to 15% compared to the existing CH monitor model.	The effectiveness and efficiency of the researchers' methodology is evident in the accurate and accurate threat detection achieved by the used IDS, which successfully addressed difficulties related to detection errors

				and omissions. One potential limitation is the necessity of selecting a suitable IDS to enhance the accuracy of false rate detection within the system.
Karande *et. al*. [70]	To early detect any attack targeting the IoT system in order to minimize damages.	DEDA technique	The findings of this study demonstrate that the algorithm provided in this work is successful in proactively detecting attacks.	The limitations of the proposed algorithm associated with deploying monitoring nodes, as well as its inability to identify and detect unknown threats needs to be improved.

Giang *et. al.* [71]	To achieve efficient automation in the early detection of IoT botnets, it is important to consider an extensive number of features.	Machine learning model	The model under consideration demonstrates a level of accuracy equal to 99.37% when evaluated on a dataset consisting of 5023 instances of IoT botnet samples and 3888 instances of benign samples.	The drawback is the time taken by the V sandbox to collect data, affects the efficiency of this system. An improvement is needed for a more efficient system.

Table 2.2: Summary of the reviews on detection techniques

2.3 Mitigation techniques of the IoT based threats in smart home automation

The mitigation plan refers to how the attacks were dealt with and what action was taken immediately to stop any further harm or damage to the system. Most defence mechanisms use countermeasures such as dropping packets, blocking ports, and rerouting traffic, to name a few. The IoT-based threats will always be able to gain access tocertain Internet sites, so it is important to keep an eye on the risks [29]. The network security must find, analyse, and stop the attack as quickly as possible. When an attack is found, the first step is to identify, describe, and measure it. The attack should be found and stopped as soon as possible. To find the best ways to deal with threats, researchers have investigated the use of mathematical and statistical analytics. Routers, firewalls, intrusion prevention systems (IPS), and mitigation systems dedicated to IoT based threats are some of the 27 standard security tools that have been used on most Internet sites for years [30].

Table 2.3 describes the various mitigation approaches that can be utilised to counter IoT-based vulnerabilities in home automation systems [31-37]. It is essential to identify methods used in the literature and to implement them in the proposed solution.

Mitigation techniques	Description	Drawbacks
1. Drop Packets	When one or more of the data packets that are moving through a computer network do not make it to their intended destination, an event known as "packet loss" takes place. The amount of data that can be counted as throughput for a given sender is decreased when there is packet loss since some of the data that is sent is never received [31].	The disadvantage of dropped packets is that it reduces the sender's throughput because some data is never received. When reliable delivery is required, packet loss increases latency because retransmission requires additional time [59].
2. Block Port	Block Port is the practice of an Internet service provider (ISP) to define and block Internet traffic based on a port number and transport protocol combination. This practice is commonly referred to as "blocking ports" [32].	Block port can cause applications to malfunction by preventing them from using the interfaces for which they were designed. It can complicate the application design and development and raise doubts about whether deployed applications will function correctly [60].
3. Redirection	When packets are traveling via a network gateway, such as a router or firewall, network address translation (NAT) will sometimes redirect a	There are many advantages to redirection, including centralized data

	communication request from one address and port number combination to another. This process is known as port forwarding or redirection [33].	storage, easier backups, and increased security. However, it also has disadvantages, including increased server burden, reliance on network connectivity, the possibility of data loss, and increased complexity [61].
4. Control Bandwidth	Control Bandwidth is a feature that can be found in certain software applications as well as hardware devices. This feature gives you the ability to restrict the amount of network bandwidth that the software or hardware can consume [34].	Control Bandwidth is a critical factor that impacts the overall performance and efficiency of your network. Hence, as the bandwidth increases, the ability to respond to high-frequency components in the error signal also amplifies. Noise generally exhibits a dominant presence at higher frequencies, thereby prompting the system to initiate a response to said noise [62].

5. Network reconfiguration	When a transition either puts a port into the forwarding state or transfers a port from the forwarding or learning stages into the blocking state, it is referred to as a shift. A network reconfiguration and topology are the process of changing the network's configuration and topology. To put it another way, a port on an active switch either rises or falls in its status [35].	Insufficient resilience in the system. Propagation of computer malware Challenges in the execution phase. Insufficient operational efficiency [63].
6. Deep packet inspection	Deep packet inspection, also known as packet sniffing, is a type of data processing that involves conducting an in-depth analysis of the data that is being transmitted over a computer network to determine the most appropriate course of action, which may include logging, alerting, blocking, or re-routing the data [36].	The limitation of this methodology lies in its efficacy solely for established assailment's, rather than for prospective attacks yet to be introduced [64].
7. MAC/IP Address changes	It is possible for a computer to hide on a network or mimic another network device by changing its Media Access Control (MAC) address. This allows the computer to avoid access control lists that are stored on servers or routers [37].	MAC address filtering does not leverage the utilisation of encryption mechanisms. There is a shortage of encryption and a lack of safeguards against eavesdropping. MAC address filtering is susceptible to various security

		vulnerabilities, including the known man-in-the-middle (MITM) attacks [65].

Table 2.3: Different types of mitigation techniques in IoT based threats

Unfortunately, there is still a large gap in the application of game theory to the mitigation of IoT-based threats in smart home automation. Table 2.3 outlines the many strategies that have been utilised to counter IoT-based threats. The suggested strategy will contribute to the efficient mitigation of IoT threats in smart home automation by using game theory.

2.4 The detection and mitigation of IoT based threats in smart home automation

Methods of detection and mitigation are set up to identify threats to a system that pose a greater risk to the system than the system itself, and then to eliminate those threats before they can cause any harm. Below is a review of the available literature on the topic of security risks regarding the IoT SHA and the strategies that have been used to identify and counteract them. The first step of the detection and mitigation procedures is to identify potential dangers to the system, and then to eliminate them before they may cause harm. The following literature has evaluated some of the methods used to identify and counteract these vulnerabilities in IoT smart home automation; it is explored in greater detail below.

2.4.1 A host based IoT-IDM framework for smart home using OpenFlow

Nobakht *et al*. [38] explained the IoT-IDM as the name of the proposed framework, which protects smart devices used in the home at the network level. The IoT-IDM keeps an eye on the network activity of smart devices in the home and checks to see if there is anything suspicious or bad activity. Once an intrusion is found, it can also stop the intruder from getting into the victim device right away. The most important thing that this paper adds is a framework for finding computer security attacks on smart objects in home networks and triggering the right defence actions to stop them. It aimed to provide security services by using SDN technology and machine learning techniques. The IoT-IDM framework, which was placed on top of the SDN controller, consists of five key modules: The Device Manager, Sensor Element, Feature Extractor, Detection, and Mitigation. Figure 2.7 shows an overview of the IoT-IDM, including its key modules and how it talks with a typical smart home network. The design of the IoT-modular IDM gives its users the freedom to use custom machine learning techniques for detection based on the signature patterns of known attacks that they have learned.

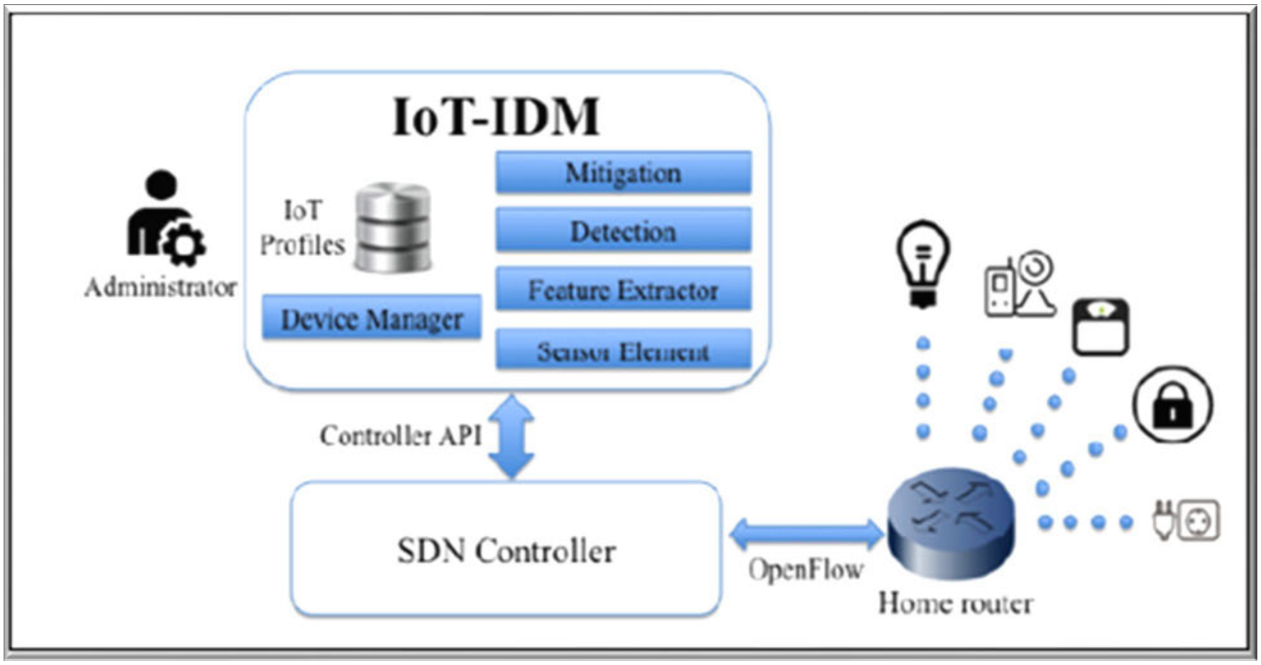

Figure 2.7: IoT-IDM Architecture and a typical smart home network [38]

Based on the results of the test, the linear logistic regression classification model in IoT-IDM predicted that 1201 commands were unauthorised access, of which 69 were false positives. It also said that 561 commands would be allowed access, but 199 of those predictions were False Negative. Based on the obtained outcome, the IoT-IDM successfully detected unauthorized access to the Hue device with a precision rate of 94.25% and a recall rate of 85.05%. In the same manner, when a nonlinear classification model was used, the accuracy of the prediction was 98.53% and the recall was 95.94%. Even though the accuracy of detection depends on the detection algorithm used, this shows that the IoT-IDM can be used. Even though the accuracy of predictions has increased by 98.53% and the rate of predictions has increased by 94.25%, the method and technique used have a flaw. There is still a gap in the manner in which game theory is not being used sufficiently to improve the detection method. Even though the proposed solution was able to find and stop IoT threats in smart home automation using a different method, there is still a hole in the current plan of the researcher to allow the use of game theory to make the detection and stopping of threats more effective.

2.4.2 Dynamic attack detection and mitigation of IoT systems using SDN

Bhunai *et al.* [39] suggested the use of SoftThings, a framework for IoT security based on SDN approaches that enable early detection of abnormal behaviour and better resilience. The enormous volume and heterogeneity of IoT devices increase the likelihood of security problems. There is currently no mechanism to guarantee the security of IoT devices. However, it is essential to provide resilience, continuous monitoring and adaptive decision making. An SDN can effectively handle security threats to IoT devices in a dynamic and flexible manner without imposing any strain on IoT devices; hence addressing these concerns. As illustrated in Figure 2.8, the proposed structure in this paper is hierarchical.

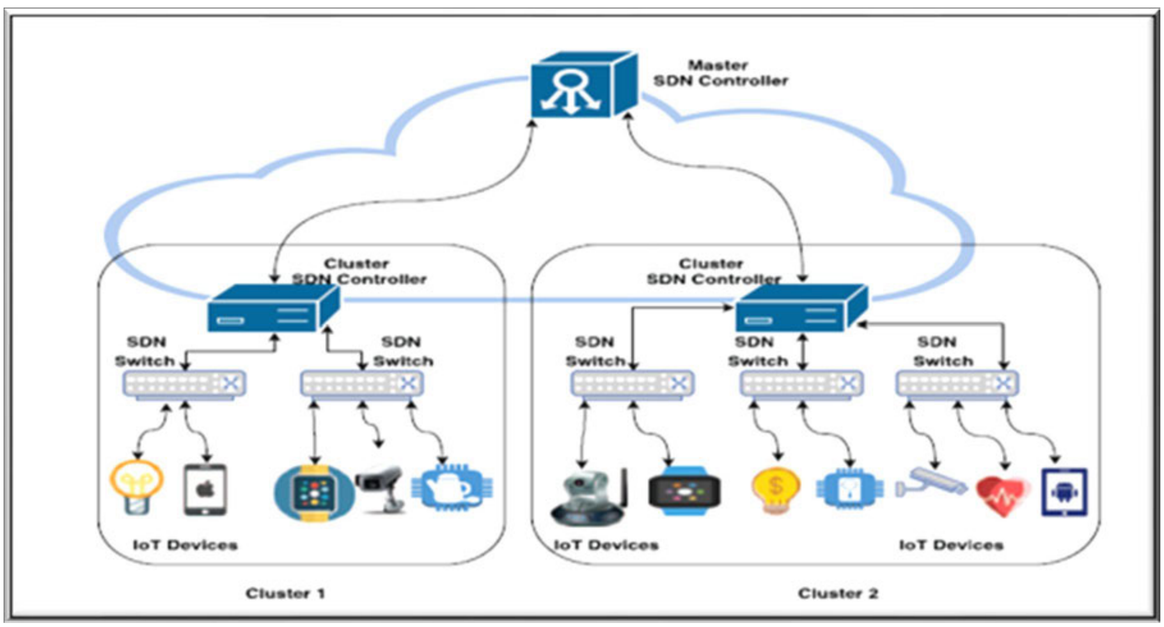

Figure 2.8: SDN based Soft Things framework for anomaly detection in IoT traffic [39]

The advantages of the hierarchical SDN control plane structure are (i) decentralised and scalable network management; and (ii) protection against controller overload (or controller DoS attacks). There are four main parts to the SoftThings framework: (i) Internet of Things devices; (ii) a switch with software-defined networking capabilities; (iii) a cluster SDN controller; and (iv) a master SDN controller. It is expected that each user has access to their own SDN-compatible switch. The switch has security regulations and rules programmed into it. The network of the service provider terminates at the switch.

IoT Devices - Consumers may have several IoT devices in their homes. Some examples of IoT gadgets include security cameras, wearables like smart watches, smart lighting systems, smart appliances like smart refrigerators, smart thermostats, motion detectors, and activity trackers. The SDN-enabled switch serves as the connection point for these gadgets. Each user also has their own identical switch and hardware configuration. Controlled by a cluster of SDN nodes, a subset of users is grouped together geographically. It suggests that there may be a small number of switches in a cluster. Some users of the same telecommunications company may group together in one area. A single SDN controller, dubbed the cluster SDN controller, manages all the nodes in the cluster. In the uppermost tier of the SoftThings architecture, the master SDN controller is owned and operated by the telecom company. This master SDN controller has authority over all other SDN controllers in the cluster. This controller can see everything happening throughout the entire network.

They set up a proof of concept on the Mininet emulator to find strange IoT traffic using a Support Vector Machine (SVM), an algorithm for machine learning, and to then stop attacks. For each scenario, the researcher gave the controller training data that showed how normal traffic flows through the devices and how attacks tend to happen. They mostly thought about three situations: IoT devices are being attacked, hacked IoT devices are being used to launch attacks, and multiple hacked IoT devices are being used to launch a DDoS attack.

Attacks like TCP flooding, ICMP flooding, DDoS, and scenarios with IoT devices have been thought of as both targets and sources of attacks. To find the strange traffic and stop the attack, they used various performance metrics. A machine learning algorithm is used to determine the nature of the activity. So, there may be false alerts. They used precision and recall to determine how well the mechanism to find unusual traffic was working. Both linear and nonlinear SVM were tested to see how well they could find these attacks in various scenarios. Early results show that the proposed SoftThings can detect attacks with about 98% accuracy and stop or slow down the attack flows within a few seconds.

2.4.3 LEDEM of DDoS attack in IoT via SDN cloud architectures

Ravi *et al.* [40] discussed how to stop a DDoS attack that was caused by a malicious wireless IoT on IoT servers. The IoT networks are vulnerable to security breaches, mostly because they do not have many resources. The Distributed Denial-of-Service (DDoS) attack is one type of breach that can cut off a network service to users in different ways, for example, by using up the resources of the server, filling up the bandwidth of the link, and so forth. In critical cases of IoT use, these kinds of DDoS attacks can be a disaster. Their security plan makes use of the cloud and software-defined networks (SDN) to protect IoT servers from DDoS attacks. They have designed a new method called learning-driven detection mitigation (LEDEM), which uses a semi-supervised machine-learning algorithm to find DDoS attacks and stop them. The big ideas of LEDEM are shown in Figure 2.9. It is evident in Figure 2.9 that they use a decentralised SDN with two levels. A local controller oversees each subnetwork domain. The local controllers are linked to a universal controller in the cloud.

There are three parts to the LEDEM:

Data Capture- the gateway for the access points is a switch that can handle OpenFlow. This allows all IoT traffic to go through the OpenFlow switch.

Detection of DDoS- the extracted feature data are fed into the DDoS detection module, which runs on all the local controllers. The researchers used an ML model that was already trained to find DDoSs.

Stopping DDoS- if SDELM detects a DDoS attack, the attack mitigation module is activated, and the set of malicious IoTs is sent to it. The module for stopping attacks is placed in the local controllers.

The researchers tried out LEDEM on the testbed and simulated topology. Subsequently, they compared the results to solutions that are currently considered to be the best. They were able to find DDoS attacks with a better accuracy rate of 96.28%.

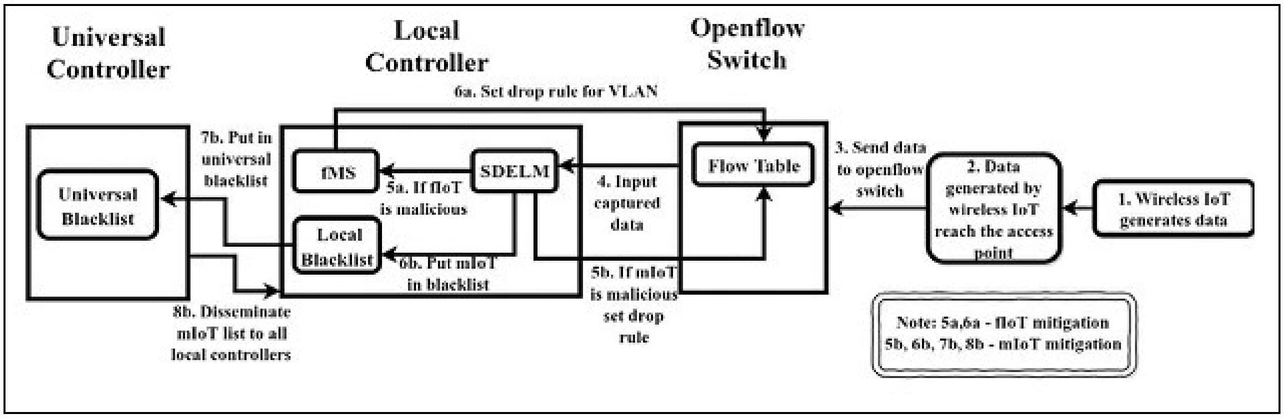

Figure 2.9: LEDEM high level illustration [40]

2.4.4 Timely detection and mitigation of IoT-based cyberattacks in the smart grid

Yilmaz *et al.* [41] proposed a general and scalable way to stop attacks. It is called Minimally Invasive Attack Mitigation via Detection, Isolation, and Localization (MIAMI-DIL). It is based on an online, nonparametric anomaly detection algorithm that is scalable and can find problems quickly. The smart grid infrastructure is always being changed, updated, and improved, which creates new cyber-security challenges that must be dealt with in a successful and satisfactory way for these projects to have a future. The fact that the smart grid can cause physical damage and a chain reaction of power outages makes security breaches much worse. Recent successful Distributed Denial of Service (DDoS) attacks on the Internet, which were made possible by the growth of botnets powered by the IoT show that the smart grid could be the target and likely victim of a similar attack, which could cause millions of people to lose power in a manner that could be catastrophic.

The MIAMI-algorithm DILs for finding anomalies is based on an online, non-parametric approach with a distributed statistical inference method that works well with high-dimensional systems and has a short average delay for detecting anomalies. To keep the control centre from going offline because of data flooding (DoS) or making bad decisions because of fake data, the components under attack should be isolated and their data ignored. This means that the components under attack should be cut off from the data communication infrastructure until the attack is over.

The proposed IDS can find cyberattacks quickly and accurately, and in some cases, it can do so even faster than the best-designed Clairvoyant Cumulative Sum (CUSUM) detector. Their method is much faster than the redundant CUSUM and its more practical version, Generalised CUSUM (G-CUSUM) which estimates the model parameters when finding stealth DoS attacks. As shown in Figure 2.10, the detection method quickly and accurately finds an increase in the mean of the first dimension from 0.1 to 0.5. Simulations show that the proposed method works and can be scaled up.

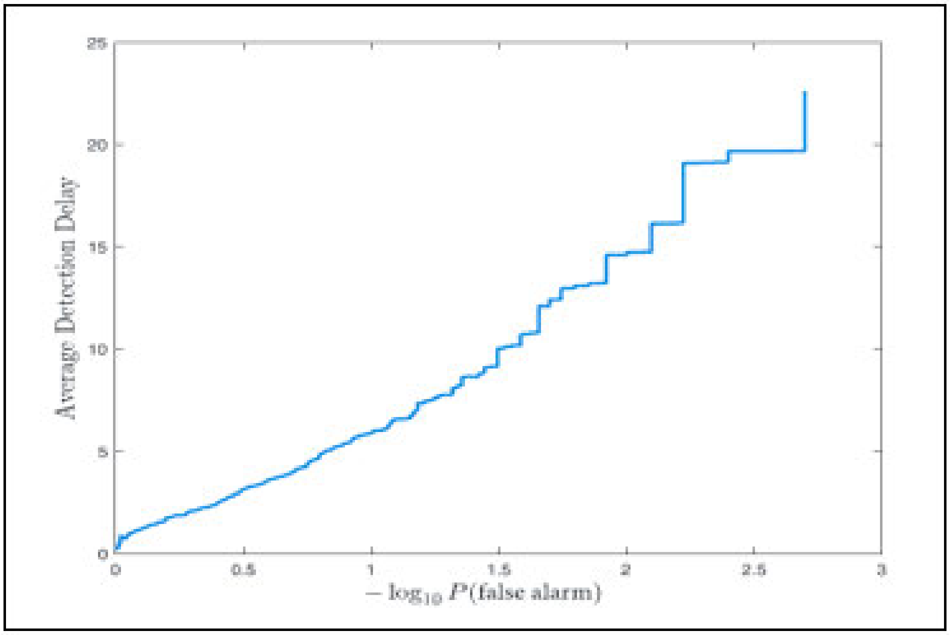

Figure 2.10: The average performance of the proposed detector [41]

2.4.5 A DDoS Attack detection and mitigation with software defined IoT framework

Yin *et al.* [42] proposed an algorithm that uses the cosine similarity of vectors that show the packet-in rate at the boundary SD-IoT switches to find and stop DDoS attacks. The authors also determined the threshold value for the cosine similarity and the length of the vectors. A recent incident involving a DDoS (distributed denial of service) attack revealed the wide range of vulnerabilities in the IoT. In this attack, numerous IoT devices accidentally contributed to the execution of the DDoS attack. The emerging paradigm of software-defined anything (SDx) enables the secure administration of IoT devices. In this article, the researchers provide a general framework for software-defined Internet of Things (SD-IoT) based on SDx.

A controller pool, SD-IoT switches connected to an IoT gateway, and IoT devices comprise the general SD-IoT structure shown in Figure 2.11. The controller pool is constructed with a vertical control structure, which includes a primary control layer and a basic control layer. The simulation outcomes show that the proposed technique quickly controls and mitigates the DDoS attack in IoT and that it is capable of quickly identifying the IoT device from which a DDoS attack originates.

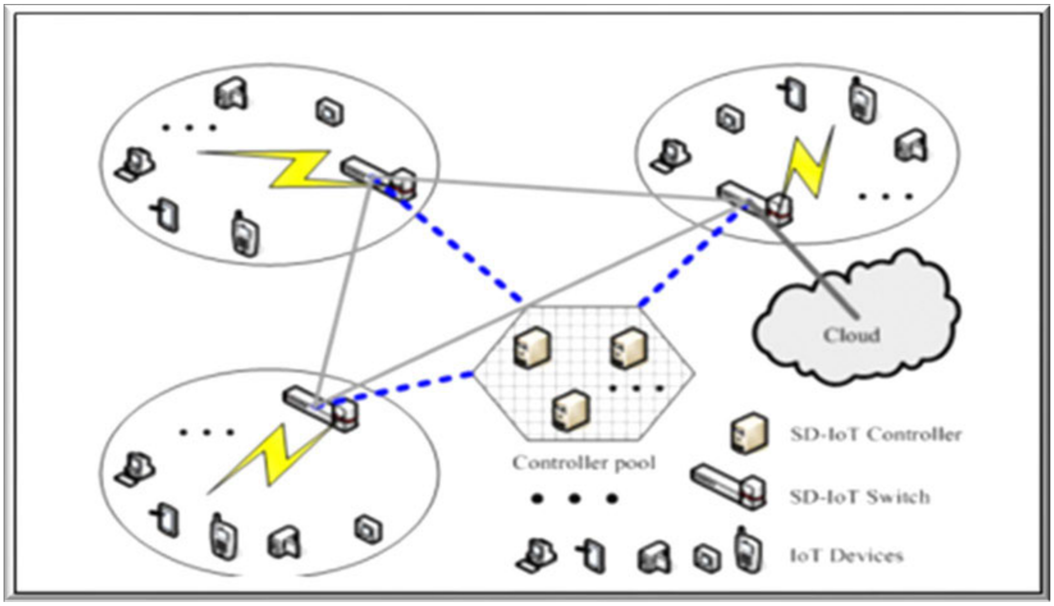

Figure 2.11: SD-IoT Framework [42]

Early detection enables prompt mitigation and isolation of compromised devices in response to attacks. Therefore, the literature study demonstrates that there is still a gap in the early detection and mitigation of IoT-based threats in smart home automation using game theory as there are fewer resource-based problems. While most researchers have tried and tested many strategies for the identification and mitigation of IoT-based dangers, game theory remains untapped. Consequently, the goal of this research is to detect and mitigate these IoT-based vulnerabilities in smart home automation using game theory. The previous reviews have explored in depth the detection of IoT-based risks using game theory, and several of them will serve as references for our game theory-based early detection strategies. There is still a deficiency in mitigation approaches; therefore, it will be most effective to incorporate game theory into the mitigation techniques for IoT-based dangers in smart home automation.

Table 2.4 illustrates the pros and cons of the previously reviewed literature about the detection and mitigation of IoT-based vulnerabilities in smart home automation. It is essential to recognise that game theory is the most effective and efficient way for enhancing the effectiveness of detecting and mitigating these dangers. Therefore, the proposed method will aid in the detection of these at a higher rate.

Ref.	Objectives	Method	Results
Nobakht *et al.* [38]	To provide a network-level protection for smart devices deployed in home environments.	Host Based OpenFlow	According to the data, the IoT-IDM effectively detected unauthorized access to the Hue system with a precision rate of 94.25% and a recall rate of 85.05%. Similarly, the prediction precision was 98.53% and the prediction recall was 95.94% when a non-linear classification model was used.
Bhunai *et.al.* [39]	To address the issues of security threats that could lead to DDoS.	Software Defined Network (SDN)	The results show that this framework can detect IoT attacks with a 98% accuracy.
Ravi *et.al.* [40]	To tackle the DDoS attack triggered by malicious wireless IoT on IoT servers.	SDN cloud architecture	In detecting DDoS attacks, they improved their accuracy rate to 96.28%.
Yilmaz *et.al.* [41]	To timely detect and mitigate cyber security challenges on a smart grid.	Minimally Invasive Attack Mitigation via Detection, Isolation, and Localization (MIAMI-DIL)	Based on an online and nonparametric anomaly detection algorithm that is scalable and capable of detecting anomalies in real time. We demonstrate the efficacy and scalability of the proposed approach using simulations as a proof-of-concept.
Yin *et.al.* [42]	To detect and mitigate DDoS attack.	SDN Framework	The proposed algorithm performed well, and the framework was modified to improve IoT security with heterogeneous and vulnerable devices.

Table 2.4: Comparison of detection and mitigation methods

2.5 Insights on the desired game theory method

This research examines the application of game theory to IoT-based threats in SHA. The initial purpose of game theory was to resolve issues between economic entities [43, 44]. Various IoT applications have used game theory in recent years because it delivers robust solutions. An IoT system is a multi-entity system in which each entity is either a sensor with varying sensing capabilities or a user with varying decision-making skills. Game theory provides the right concepts and techniques for dealing with several interacting entities, with the goal of maximizing the utility of each entity [75]. This article outlines how game theory is used in resource management [45]–[48], task scheduling [49], node selection [50], quality of service [51], and network security [52].

The game relies on background information, environmental conditions and constraints, individuals, and groups. and implement strategies from their respective possible strategy sets and obtain corresponding results or benefits simultaneously or successively, once or many times [75]. Game theory provides a few models and techniques for analysing the interactions between various entities. Multiple strategies are employed to maximize utility [53]. This section provides game model classifications:

Cooperative game theory: refers to a type of game where participants form coalitions instead of participating in individual competition. This characteristic raise consideration related to the creation of parties and the distribution of payoffs [54].

Non-cooperative game theory: is a game that focuses on the interactions of economic players who are rationally pursuing their own objectives. The most well-known non-cooperative game is the strategic game, in which only available strategies and the results of a succession of decisions are considered [55].

The fundamental elements of the game are used to characterize the game player: strategies, payoff, action, information, order, and equilibrium [56]. These characteristics are defined as follows: A player is a decision-maker in a game whose goal is to maximize their objective function, utility level, or benefit function by selecting actions or strategies. Strategies constitute the plans of action and basic rules of the players [75]. In the game, there are two types of strategies: pure strategy and mixed strategy. Pure strategy refers to the action plan from which the players can choose; it includes the action rules of the players within the provided information structure [57]. The return of participants after they make decisions in the game is referred to as the payoff. It is determined by the strategy or behaviour of all the players. Action refers to the gathering of all possible player strategies or actions [58]. The above discussion demonstrates the application of game theory to the IoT and constitutes a summary and analysis of existing game methods from the perspective of resource management.

The game is dependent on the underlying contextual data, the present environmental factors, the implemented limitations, as well as the actions and interactions of both individuals and groups. They select and execute strategies from their respective sets of possible strategies and achieve corresponding outcomes or advantages concurrently or repeatedly, either once or multiple times. This research explains the basic components of the game by expanding upon its nature, encompassing the player, strategies, payoff, action, information, order, and equilibrium [66]. These elements are defined in the following manner.

A player, in the context of a game, refers to the individuals responsible for making decisions with the goal to optimizing their objective function, utility level, or benefit function through the selection of actions or strategies. The player can be an individual or a collective entity such as a manufacturer or a platform. Once the game rules have been established, all participants shall be considered to have equal status. It is imperative that any entity involved in the game adhere to the predetermined set of regulations [67].

Strategies encompass the thoroughly devised course of actions undertaken by the players, serving as the guiding principles for their operational actions within the established framework of rules and regulations. In the realm of game theory, two distinct strategies are encountered: i) pure strategy, which entails a predictable course of action; and ii) mixed strategy, which involves a probabilistic approach to decision-making. Pure strategy refers to the predetermined course of action that the participants may elect, in accordance with the prescribed regulations, within the confines of the provided information framework [68].

In essence, it refers to the selection of actions that the player needs to undertake given the corresponding conditions [75]. The player's strategy set comprises all the alternative strategies. The relationship between team members and task requesters can be effectively represented as a game-theoretic model within the domain of mobile collaboration.

Two distinct approaches exist for players, namely trusted and untrusted. For individuals engaged in the game, the set of pure strategies is defined as (reliable, or "unreliable. Every participant selects a strategy si from their respective strategy set; $s = \{s1, s2,... si,... sn\}$ represents the combination of strategies for n players. Let si represent the set of strategies for worker i. Therefore, *si* can be expressed as (trusted, or "untrusted. The proposed approach involves capturing the various configurations of players, excluding player i, denoted as *si* = {*s1, s2,..., si1, si+1,..., sn*}.

The mixed strategy of participant I can be defined as a probability distribution over his set of pure strategies. The participants stochastically select the pure strategy based on this probability distribution during their decision-making process. In the aforementioned mobile crowdsourcing game model, the crowd workers opt for a trusted strategy with a probability of 60% and an untrusted strategy with a probability of 40%. This combination of strategies is referred to as the mixed strategy employed by the crowd workers [69].

Payoff refers to the returns obtained by participants following their decision-making process within the game. It is a function of the strategic or behavioural characteristics of all the participants. A utility function is commonly used to quantify the payoff that players receive from different combinations of strategies. The objective of the players in the game is to optimize their utility function by selecting suitable strategies [75].

The Nash equilibrium is a fundamental concept within the realm of game theory. According to their individual payoffs, it represents a stable equilibrium in a strategic game where no player has a unilateral incentive to deviate. Both pure strategy and mixed strategy Nash equilibria can be characterized and delineated within the realm of game theory. A strategic game possesses the potential to exhibit multiple Nash equilibria [71]. It has been empirically demonstrated that any game featuring a discrete quantity of participants, wherein each participant possesses a finite set of pure strategies to select from, will inevitably possess at least one Nash equilibrium.

Action pertains to the assemblage of all conceivable methodologies or operations of participants.

2.6 Chapter summary

This study considered various studies on the early detection and mitigation of IoT-based threats in SHAS. Given the background presented in the study, it is worth noting that the proposed solutions do not discuss the response time of detection for each diagnostic approach and strategy in detail. Most authors have concentrated on the detection and mitigation techniques employed in other environments, with only a few exceptions focusing on SHA and response time. On the one hand, the proposed detection strategies above yielded good results but suffer from the early detection time requirement, which is to activate the IDS as early as possible to detect threats. Only a few have used other techniques to solve the early detection of those IoT-based threats in different environments. The game-theoretic approach, on the other hand, is the most appropriate technique for solving the early detection and mitigation of IoT-based threats in smart home automation because it provides a variety of collections of validated mathematical methods for multi-player strategy making and uses different forms to capture the interaction of players in detecting and mitigating threats. As a result, the focus of this research falls on the early detection and mitigation of IoT-based threats in smart home automation using game theory to provide efficiency, reliability, and availability as soon as possible while avoiding damage to the home system.

3 Chapter 3: System modelling for early detection and mitigation scheme

3.1 Introduction

In chapters 1 and 2, an overview of the IoT SHAS as well as the security threats were shown. In this chapter, we look at and explain why we chose the ideas, methods, and techniques we did for this study. Modelling and simulation are important for researchers because they let them test whether the design requirements are met by using virtual experiments instead of real ones. The conceptual models that emerge from the thorough literature reviews in Chapter 2 will be used to build the models of the system. A distributed approach to estimating the response time of detection and mitigation techniques for IoT-based threats in SHAS is considered. The most important contribution of this research is a better means to improve the response time, or the time the system takes to detect and mitigate IoT-based threats against smart appliances in home networks.

The primary contribution this research makes is devising a suitable method to improve the response time or the time the system takes to detect and mitigate IoT-based threats against smart appliances in home networks. A game-theoretical approach is employed to demonstrate the response time needed to detect and mitigate those malicious threats. Therefore, in this research, the aim is to provide the following prevention:

- The detection technique using both pure and mixed game theory will ensure that the threats are automatically detected timeously.
- The mitigation technique using both mixed and pure game theory will ensure that those threats are automatically blocked and prevent access to the system as early as possible.
- The proposed technique prompts an early response that is robust, effective, efficient, accurate, and reliable.

3.2 Modelling of the proposed system

It is critical to detect and mitigate IoT-based threats as early as possible in SHAS. Lights, temperature sensors, security camera systems, and smart appliances are all controlled by a SHAS. These devices and sensors are linked to the Internet, and they can easily become targets for threats. Figure 3.1 illustrates the implementation roadmap of the scheme that would assist with the early detection and mitigation of IoT-based threats. The four steps in Figure 3.1 describe the process that will be followed, which is the gathering of information, then identifying the threats, activating the detection technique, and, lastly, mitigating the threats. Our main development approach focused on the early response of the detection technique and the early response to mitigate those IoT-based threats.

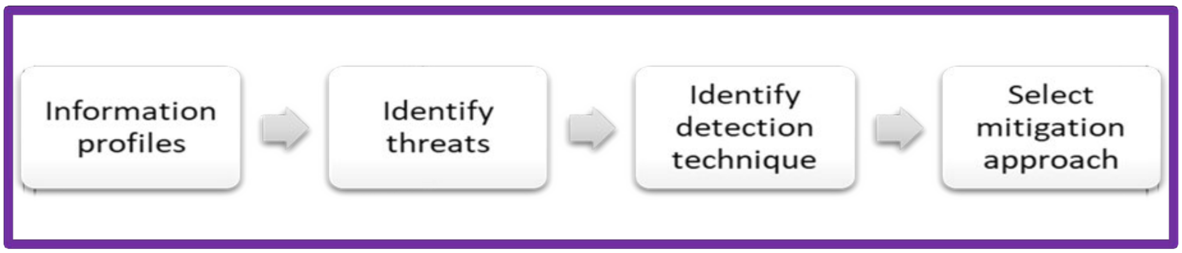

Figure 3.1: Implementation roadmap of the scheme

By integrating numerous smart sensors and Internet-enabled hardware devices into the home, this system will be able to collect and store data regarding all user activities. The IoT gateway, which is a device capable of aggregating and processing sensor data prior to transmitting it to Internet servers, is thus critical. Because they lie at the confluence of edge devices (sensors and actuators) and the Internet, IoT gateways are vulnerable to both classic IP threats and traditional attacks against wireless sensor networks.

The primary purpose of this model is to monitor various activities, illegal access, and information sharing in IoT technologies and to construct a game-theoretic model to assist with the early response time to identify the threats in the IoT SHS. With the emphasis placed on the detection and mitigation of these IoT-based threats, the emphasis will be placed on early detection to avoid delays. The system would be able to provide security services remotely, and end-users of IoT-enabled SHS should not be required to perform such laborious activities. To solve this difficulty, the researcher proposes employing an approach based on pure game theory and mixed game theory that will aid in the timely detection and mitigation of these IoT threats. As demonstrated below, the game-theoretical approach to network security and privacy beats conventional approaches in numerous ways.

- Most traditional security systems, whether preventative (e.g., firewall) or reactive (e.g., anti-virus software), rely purely on heuristics. Nonetheless, using proven mathematics, game theory may explore security decisions in a systematic manner.
- Researchers can create defence mechanisms for robust and reliable cyber systems against selfish behaviours (or attacks) by malicious users or nodes based on the analytical results of the game.

3.3 Early detection of IoT based threats using pure game strategy

As mentioned in Chapter 1, communication networks are becoming more popular as privacy and security become more important. The game-theory approach is often used to improve communication security. This means that IoT-based threats that could affect the availability of the home system to home users need to be identified as early as possible and dealt with accordingly.

In this first part, the manner in which pure game theory strategies can be used to detect IoT-based threats as early as possible is discussed. The intelligent IDS is used in this system. Game theory is used to improve the ability of the system to find IoT-based threats early in the SHAS. The IDS serves as the safeguarding mechanism for data encryption and other conventional security protocols, ensuring the integrity and protection of cutting-edge technological advancements. The operational principles of an IDS can be examined in a tripartite order. Figure 3.2 depicts a simplified schematic representation describing the operational principles of an IDS. The diagram shows a step by step approach of the operation of the IDS. The data traffic monitors the traffic for suspicious activity then alerts the host/network-based sensor to confirm and identify the suspicious threats. After the host/network-based sensor has identified the threat then it sends it to the feature extraction to identify the type of threats using the pattern signature. Then the anomaly detection will send an alert then the threat has been detected. The game-theory-based IDS will efficiently resolve this issue as it represents the most recent third-generation intrusion detection pattern matching technology, effectively adhering to the requirements of the currently available IDSs.

Game theory is employed to formulate a quantitative framework that summarizes the dynamics of actions and decisions within strategic conditions. Upon detection of an intrusion by the detection system, it shall immediately initiate a response mechanism aimed at mitigating potential system damages. In the realm of single-stage attacks, the endeavour to identify the optimal countermeasure by the defenders in response to a detected attack and the subsequent maximization of payoffs can be framed as a significant problem of majorization. One additional rationale for employing a game model lies in its enhanced precision when evaluating the payoff of both the attacker and the defender. This increased accuracy facilitates a more intuitive comprehension of the various situations arising from network intrusions. Moreover, by virtue of the diligence and precision inherent in game theory, an optimal selection can be attained in contrast to alternative methodologies, provided that the appropriate game model is formulated.

When formulating the model for this particular system, two distinct entities with conflicting objectives are considered: the attacker and the defender. The system is under the purview of the defender, who typically assumes the role of a system administrator. The critical objective of the defender is to protect the SHS against possible threats by identifying them earlier before they might compromise its operational continuity. On the contrary, the attacker can be characterized as a malicious opponent whose objective is to compromise the integrity of the SHS. Utilizing empirical data derived from real-world security incidents, a comprehensive model that characterizes the complex interaction between the attacker and the safeguarding entity is established.

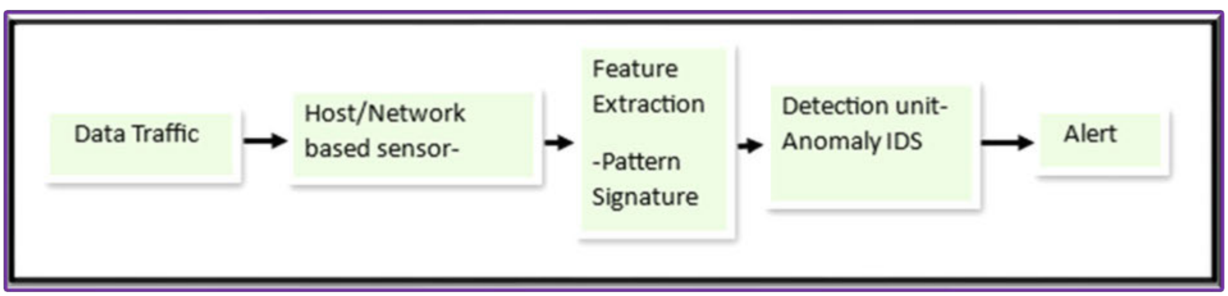

Figure 3.2: Simplified schematic diagram of operational diagram

The study makes use of the monitor, device manager, and detector, which constitute the three parts of the detection scheme. The monitor is used to keep an eye on the traffic. The information from the monitor will be managed by the device manager, who will make sure that only the necessary information gets through. The detector will then be used to find the unwanted information.

The first stage shown in Figure 3.3, is the monitoring stage that monitors the development of the information profiles and then identify the information containers. This stage will keep an eye on the network to gather information about it that will be used to feed the detection algorithm, which is based on a pure game theory strategy algorithm and calculations. The information profile process sets clear limits for an asset and figures out what kind of security is needed. After that, all the places where an asset is kept, moved, or worked on are found. Smart homeowners should also figure out where these assets are used, how to obtain them, and who oversees them.

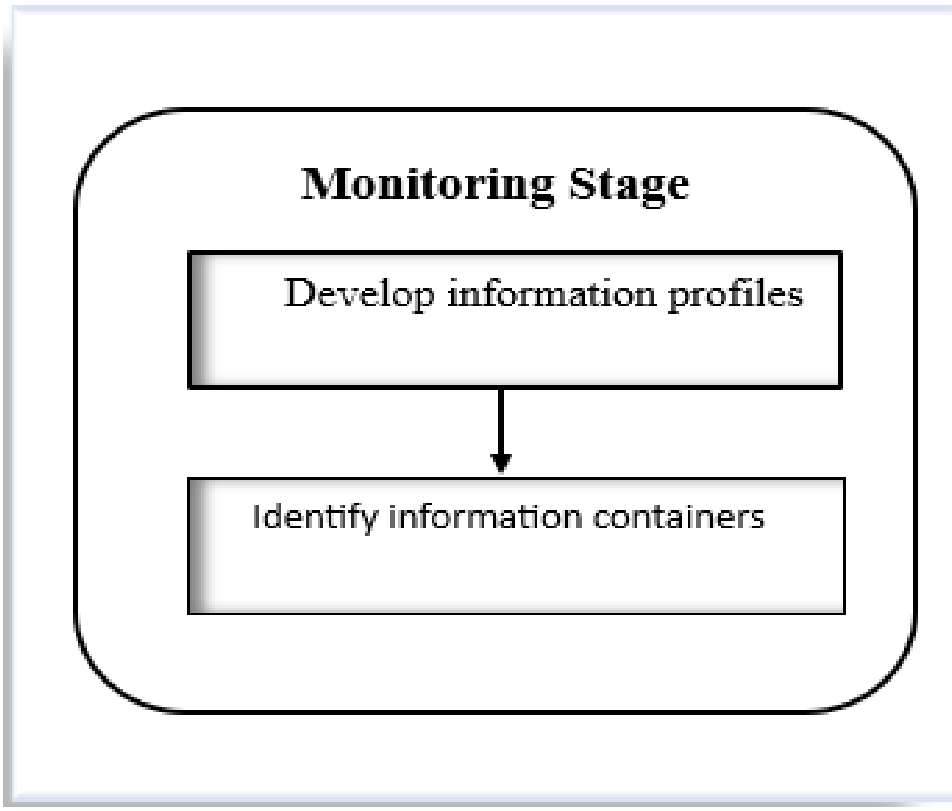

Figure 3.3: The schematic operation monitoring stage

The second stage is the device manager, which will take care of all the information coming from the detector and make sure that it is correct and what the home system needs. Pure game theory will be used to enhance the utility of every device in the IoT SHS network. Using the pure game theory strategy, the third stage, which is the detector, is also used as a detection unit to find all the unwanted information or threats. Figure 3.4 presents a simple diagram of how the detection unit works. The detection technique will be figured out using a pure game theory-based algorithm and a detection unit that uses a pure game theory application. The network traffic of an IoT device that has been registered is picked up by the sensor element and used to extract features. Since all the traffic is available, the user can choose which fields to pull out. The features are the most important parts of network traffic. To define them, it is necessary to know a lot about the hosts and the kinds of attacks that could occur.

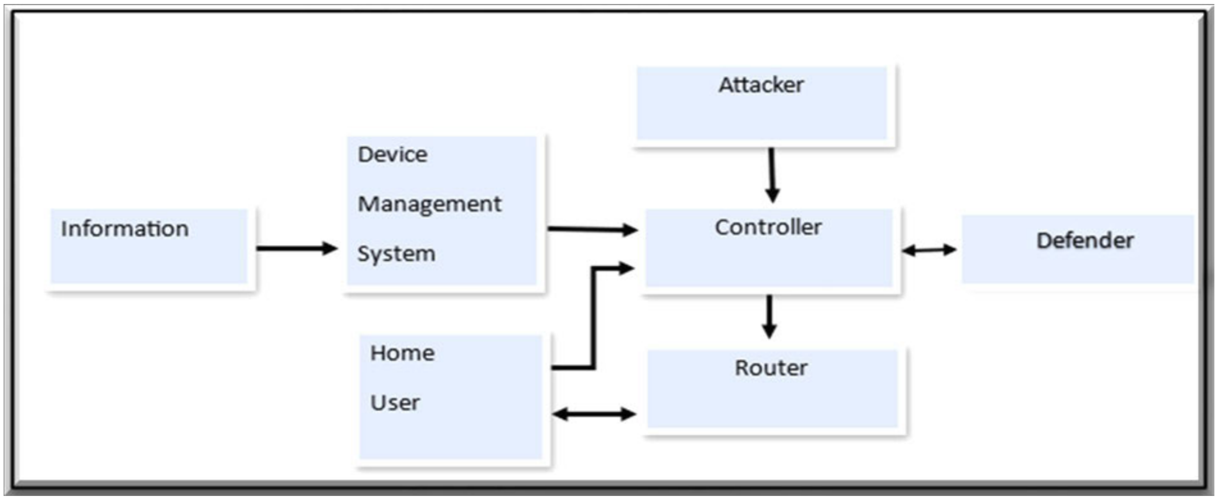

Figure 3.4: An overview architect of the Detection method

In game theory, the main elements are players, actions, strategy, and information, all of which are known as the rules of the game. The proposed strategy considers the following conditions:

- The players must know all the parameters and rules of the game.
- The first player must be unaware of the plan of the second player, as the second player will first study the strategy of the first player and then choose a strategy to counteract the first player.

The following are some of the potential applications of game theory:

- It is a means to figure out the best strategy in a competitive situation using numbers.
- It lets players change their plans based on what other people are doing in the game.
- Nodes in a network are independent and can make their own choices based on what is best for them.
- Game theory gives us the right tools to look at how each player acts and behaves.

The game strategies will be made based on the results of the players, which will be shown as probability distributions in the space of specific strategies. Figure 3.5 describes the architecture of the IDS and SHAS. The figure depicts the threats as nodes with a level of vulnerability that attackers can exploit, while the router functions as the SHAS server. The server automatically allocates IP addresses to all nodes connected to the home network and the controller have sufficient strength to efficiently handle all incoming packets within the network. The approach of pure game theory would be used to help with the detection method to make sure that threats are found quickly and correctly. In SHA, the pure game strategy will be used to quickly identify IoT-based threats. In a pure game strategy, players apply a strategy that produces the best results. Therefore, because it is necessary to detect IoT-based threats as early as feasible, selecting the best strategy will assist us in accomplishing our objective. Pure game strategy produces excellent outcomes for players.

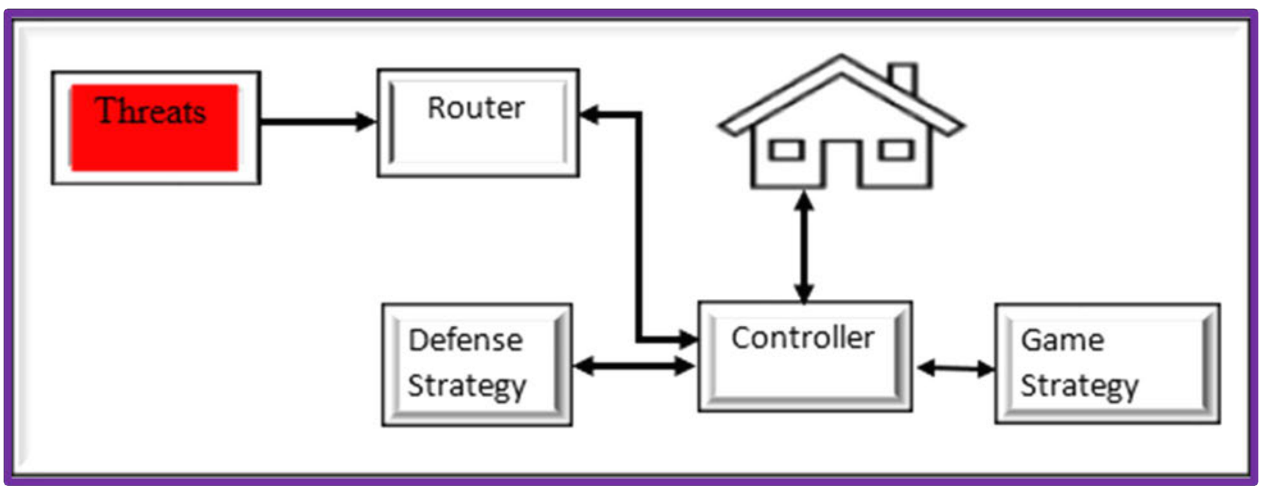

Figure 3.5: An architecture for game theory

Key terms in pure game theory

The main goal of the defender is to quickly recognize threats emerging from the IoT within the SHS, ensuring that the availability and functionality of the SHAS remain uninterrupted. The primary aim of the defense strategy is to enhance the efficiency of detecting and responding to potential threats by employing game theory-based IDS. Nonetheless, the motives of the attacker often remain undisclosed. Therefore, we shall examine a possible scenario in which the primary aim of the attacker is to compromise the security objective of the defense. Therefore, pure game theory will be used to assist with the early detection of those IoT-based threats in SHAS.

The game was perceived as a game involving two players: the attacker, representing possible threats, and the defender node, responsible for shielding the SHAS from the attacker and aiding in prompt detection response. The person responsible for the attack acts as a barrier to the users of the SHS system, hindering their ability to gain access. The role of the defender is to effectively detect and mitigate possible threats in IoT systems, with the objective of stopping unauthorized access to the SHAS by the attacker.

The primary aspect of game theory involves determining and defining the parameters. Player 1 will demonstrate the attacker, particularly the threats relating to the IoT. On the other hand, player 2 will represent the defender, acting as the detector responsible for activating the IDS to detect threats early. To achieve our objective of early detection, this will aid in enhancing the response time to the IDS.

- Set of players: N
- Players: N_A= Possible threats (Attackers), N_D = Detection Unit (Defender) $\{N_A, N_D\}$
- Strategies: Attacker strategies M_a and Defender strategies M_d
- Attacker nodes : Q
- Defender nodes: P
- Payoffs of attackers action: H_a
- Payoffs of defenders action: H_d
- Time required for monitoring: T_p
- The potential point of attackers action: G_w
- The potential point of starting the IDS: G_m
- The loss of attacked node: G_i
- The probability of attacking: δ_i
- The probability of defending: σ_i

The pure game theoretical technique is utilized for early detection. The game consists of two primary components: the controller, who assumes the role of the defender, and the intruders or threats, who act as the attackers. The defender must possess the capacity to analyse and comprehend the surrounding environment. The controller is responsible for overseeing the data generated by each smart home device within its home router and transmitting a signal to the IDS in the case of a system attack. The time t will be used to calculate the duration it takes for the defender to transmit a signal to the IDS indicating the potential presence of an unauthorized entity within the system. The response time formula will be derived below, considering the formulation of both defender and attacker strategies.

The game is defined as the following:

$$\text{Game} = N, (M_{\text{dNd}})_{t\in \text{N}}, (P_{\text{Nd}})_{t\in \text{N}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3.1)$$

$$\text{Game} = N, (M_{\text{aNa}})_{t\in \text{N}}, (Q_{\text{Na}})_{t\in \text{N}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3.2)$$

Various players are likely to have distinct preferences for game strategies which are:

$$M = \{M_{\text{a}}^{\text{Tp}}, M_{\text{d}}^{\text{Tp}}\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3.3)$$

The potential attacker's nodes can choose to prevent from launching an attack upon the activation of the IDS by the defender. Every player in the game needs to achieve a certain goal and those goals needs to be achieved using a particular strategy. The goal of the defender is to early activate the IDS for early detection of the IoT based threats and can be defined as G_{i}^{Tp}, which i is the number of nodes in the system. The goal of the attacker is to include the attacker's attack $\text{G}_{\text{a}}^{\text{Tp}}$, and the attackers not attacking G_w^{Tp} .

The strategy for player N_{d} is defined as:

$$M_{dNd}= [M_{dNd}(\text{t}(0)), M_{dNd}(\text{t}(1)), \ldots\ldots\ldots M_{dNd}(T_P)] \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (3.4)$$

The strategy for player N_{a} is defined as:

$$M_{aNa}=[M_{aNa}(\text{t}(0)), M_{aNa}(\text{t}(1)), , \ldots\ldots\ldots M_{aNa}(T_P)] \ldots\ldots\ldots\ldots \ldots\ldots \quad (3.5)$$

After defining the game and the strategy we defined the payoff of each player:

$$\mathbf{U_a} = \sum_{Tp=1}^{\infty} \sum_{i} * G_i{}^{Tp} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3.6)$$

We calculate the payoffs and strategy for the defender to see that it can timely activate the IDS when an attacker is on the system, and the IDS can act as quick as possible to respond.

$$\sum_{Tp=1}^{\infty} * \sum_{i} Gi^{Tp} < P_a - \sum_{Tp=1}^{\infty} * \sum_{i} G_a{}^{Tp} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3.7)$$

The IDS is then activated using the following game formula:

$$\mathbf{PN_d} = \sum_{t=0}^{Nd}(1-\delta)/\sum_{t=0}^{Na} \delta^{t}\mathrm{N_a} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3.8)$$

$$= \sum_{t=0}^{Nd} 1 - \sum_{t=0}^{Nd} \delta/\sum_{t=0}^{Na} \delta^{t}\mathrm{N_a}$$

$$\mathbf{PN_d} \geq \mathbf{PN_a} \ \textit{for all } t' \epsilon \Delta^{t}$$

When the IDS detects an attack, it will take action to limit any potential damage that the attacker might cause to the system. The process of determining the most efficient defensive response to a detected attack and maximizing payoffs is a major problem for single-stage attacks. The best game strategy can be obtained by analysing the Nash equilibrium through the game process.

Now, to determine the response time in the system, the following formula will be formulated to assist with improving the defender's response time. We have deployed additional nodes into the game system to aid with the early response time for the activation of the detection unit towards the attacker's action.

$$\mathbf{F(t)} = \sum_{t=0}^{Md} * \sum_{t=0}^{Ma} (N_{\mathrm{d}}/N_{\mathrm{a}}) \quad \ldots\ldots\ldots\ldots\ldots \quad (3.9)$$

After an attacker has acted, the defender decides what to do depending on information from the monitoring system. Only if the defender fails to respond properly does the action of an attacker result in a transition to the intended state. The attacker is required to return to the default state once the defender responds to the observed action.

3.3.1 Threat detection algorithm

To provide a better understanding, the algorithm for solving the problem is discussed in this section. The proposed algorithm for the detection of a threat attack in IoT smart home systems will work by placing monitoring nodes to normal nodes for the detection of an attack.

Step 1: Determine the plans of the attacker.

Step 2: Check the strategy of the defenders, while keeping in mind that an attacker can act.

Step 3: In the game, the attacker decides how to use attack resources based on how the defender defends. The goal is to find any intruder in the home system as early as possible.

Step 4: The losses of the attacker come from the person who gets into the system without permission and does more damage to the user.

Step 5: When the home system is attacked, the defender tries to respond as early as possible with the defence resource to minimise the damage sooner.

The following is the algorithm for detection of IoT based threat:

Algorithm 1: Implementation of early detection pure game model

1.Inputs: N_a, N_a, M_a, M_d, H_a, H_d, $T_p = \infty$ // define the inputs

2. Outputs: Best Response Time T.

3. Repeat{

4. If $G_w^{Tp} \geq Pa - G_a^{Tp}$ // attackers not attack

5. Else

6. Find the active $P=\{P_1, P_2, \ldots \ldots P_n\}$ of attackers and $Q= \{Q_1, Q_2, \ldots \ldots Q_{n+1}\}$ of defenders

7. Observe action Q> and P>

8. }

9. If all attackers follow recommendation{

10. Recommend action $P > Ma=\{Ma1, Ma2, \ldots \ldots Man\}$ and $Q > Md=\{Md1, Md2, \ldots Mdn\}$

11. Md increase, Ma decrease

12. Else

13. Md decrease, Ma Increase

14. }

15. Time T start, end

16. Start= T_P

17. {

18. For T_p=0, T_p=10ms, T_p++

19. {

20. $G_w^{Tp} \leq Pa - G_a^{Tp}$ // attack is attacking

21. $\boldsymbol{F(T_P)} = \sum_{t=0}^{Md} * \sum_{t=0}^{Ma} (N_d/N_a)$ // Activating the defender nodes

22. }

23. End= T_p++

24. }

25. }

Algorithm 1: Compute Pure Game Theory for Detection

Mixed game strategy in early detection:

In this section, the symbols δi, σi, (1-δi), and (1-$\sigma 1$) are employed to denote the probabilities associated with various events. Specifically, δi represents the probability of node i initiating the Intrusion Detection System (IDS), σi represents the probability of an attack occurring, (1-δi) represents the probability of the IDS not being initiated in a timely manner, and (1-σ1) represents the probability of no attack taking place. Hence, the payoffs of mixed strategies can be considered comparable to the payoffs of pure strategies in the game, as determined by the weighted average probability.

Attackers mixed strategy is

$$H_a = \sum_{Tp=1}^{\infty} \sum_{i} * (((Pa - Ga)(1 - \delta\, i))\sigma i + (-Ua)\delta i\sigma i + Gi(1\text{-}\sigma\text{i})) \ldots\ldots\ldots \quad (3.10)$$

$$= \sum_{Tp=1}^{\infty} \sum_{i} * (((Pa - Ga)(1 - \delta i))\sigma i - Ua\delta i\sigma i + Gi(1 - \sigma i))$$

Defenders mixed strategy is

$$H_d = \sum_{Tp=1}^{\infty} \sum_{i} * ((Ua - Gi)(1 - \delta i)\sigma i + (Ua - Gm)\delta i\sigma i + Ua(1 - \delta i)(1 - \sigma i) + (Ua - Gm)\delta i(1 - \sigma i)) \ldots\ldots\ldots \quad (3.11)$$

$$= \sum_{Tp=1}^{\infty} \sum_{i} * Gi\delta i\sigma i + Gi - Gm\delta i - Gi\sigma i$$

When defenders mixed strategy starts the IDS and δi goes larger the probability of being early detected by the IDS also increases, and the attacker's payoffs will reduce. The defender's main goal is to ensure that an attack is early detected before it can even access the SHAS. The attacker's best strategy is to increase the attacker's best probability in order to gain access to the SHAS, but the defender's probability is to increase the speed of the nodes in order for the IDS to perform the early detection as efficient as possible. The algorithm below clearly outlines the early detection methodology utilized for the mixed game theory.

The following is the algorithm for Mixed Game theory:

Algorithm 2: Implementation of early detection mixed game model

---

1.Inputs: σ_i, δ_i, T_p // define inputs

2. Output: Response time

3. Repeat {

4. If $G_w \geq P_a - G_a$ // Attackers are not attacking

5. Observe action P and G

6. Else

8. δi increases, σi decreases

9. Else

10.δi decreases, σi increases

11. End If

12. End If

13. $t \leftarrow t+1$ }

Algorithm 2: Mixed Game strategy

3.4 Early mitigation of IoT based threats using pure game theory strategy

In this section, the main objective is to create a system that will mitigate the IoT-based threats as early as possible in SHAS using both pure and mixed game theory strategies in order to determine which one performs better. The mitigation module assists in limiting access to the SHAS and ensuring that threats can be removed in real time, prior to any harm occurring. The mitigation strategy was validated using MATLAB computation tool. This tool provides relevant function toolboxes for effective computational capability required in this aspect of the problem.

The pure game theory strategy depends on an algorithm that directs malicious threats that attempt to enter the IoT SHAS by either blocking them or eliminating them. The mitigation module assists in limiting access to the SHAS and ensuring that threats can be removed in real time, prior to any harm occurring.

The researchers evaluated the most effective approach for playing a pure game matrix and demonstrated how pure game-theory defence mechanisms could assist. The model of mitigation is displayed in Figure 3.6. Home users, attackers, a switch, a router, and a firewall comprise the components of this model to defend against IoT-based threats. The most crucial aspects of the mitigation model are the attackers and the firewall. The attackers will attempt to transmit threats to the SHAS in a manner that prevents home users from utilizing it. The attacker attempts to determine the best rate for sending packets, while the defender must configure the firewall to block IoT-based threats while allowing real packets through.

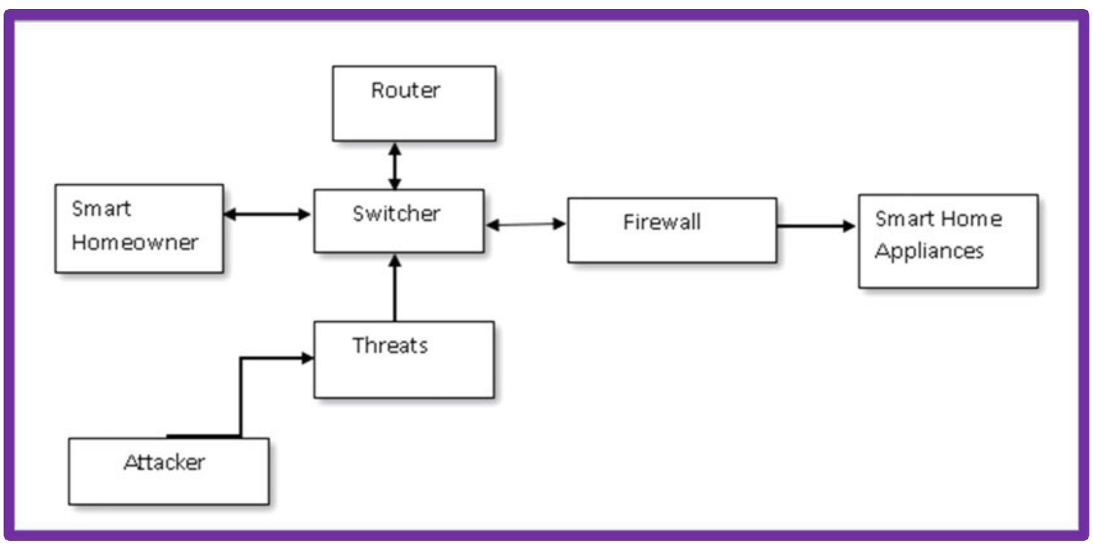

Figure 3.6: Mitigation model

Pure game theory for mitigation

The parameters of the pure gameType equation here. theory is defined below. The potential threats are defined as player 1 which is the attacker, and the defender will be player 2 which is the firewall.

- Players: N= *{Possible threats (Attackers)*N_1*, Firewall (Defender)*N_2*}*
- Strategies: *Attack strategy* C_A*, Defender strategy* C_D
- Sending rate*:* R= *{time, no Alert}*
- Block time: T_b
- $N_A = \{N_{A1}, N_{A2}, \ldots\ldots\ N_{A,N}\}$ for the attacker nodes.
- $N_D = \{N_{D1}, N_{D2}, \ldots\ldots\ N_{D,N}\}$ for the defender nodes.
- Payoff node for attacker *Q*
- Payoff node for defender *P*

Pure game matrix for the response time to block the intruder is as follows:

$$\begin{pmatrix} a11 & a12 \\ a21 & a22 \end{pmatrix}$$

In a pure game strategy, a matrix game, a mitigation strategy that can block intruders from accessing the SHAS must be created. When using this approach, it is presumed that Q denotes the proportion of time during which the attacker player N_1 employs the attack strategy N_A , whereas (1 - N_A) represents the proportion of time during which he employs the defender strategy N_D. Similarly, N_D and (1 –N_D) denote the proportion of time during which the defender player N_2 employs method in eq. (3.12) and in eq. (3.13) accordingly.

$$N_A = \frac{a22 - a12}{(a11 = a22) - (a12 + a21)} \tag{3.12}$$

$$N_D = \frac{a22 - a21}{(a11 + a22) - (a12 + a21)} \tag{3.13}$$

The expected value of the game N, as perceived by players, is determined by solving the matrix.

$$N = \frac{a11a22 - a12a21}{(a11+a22)-(a12+a21)} \tag{3.14}$$

The payoff for a pure game may always be represented by a n x m matrix, where player N_A has m possible strategies and player N_D has n possible strategies. Every pure game strategy possesses a distinct numerical value denoted as N.

$$R_A = \sum_{tb}^{n} N_{Atb} \tag{3.15}$$

$$R_D = \sum_{tb=1}^{n} N_{Dtb} \tag{3.16}$$

The last task of this pure game strategy that will assist with early detection is to break the game matrix down into two sub-matrices, one representing the payoffs for each player. The payoff matrix player one is named cN1d which is the attacker strategy.

$$N_A q = [\ 4\ 9;\ 0\ 3] \tag{3.17}$$

$$N_D p = [3\ 2;\ 5\ 1] \tag{3.18}$$

The above matrices will determine the best sending rate strategy that will show the early mitigation of the IoT based threats.

Algorithm3: Implementation of early mitigation pure game model

---

1. Input: $N_A, N_D, N, N_Aq, N_Dp, t_b, C_A, C_D, T_b=\infty$
2. Output: Sending rate, block time
3. $T_b = \infty$;
4. {
5. If $(N_A \neq N_D)$
6. Status = $N_D(t_b)$;
7. $N_D = \sum_{tb=1}^{n} N_{Dtb}$
8. Calculate sending rate;
9. }
10. Else if status is “Attacked”
11. N_{D++};
12. Drop packets
13. Else
14. Status $\neq N_A$

15. allow the packets to pass”
16. End if
17. “allow the rest of the packets up to $m+n$””
18. }

Algorithm 3: Compute Pure Game Theory for Mitigation.

Mixed game mitigation strategy

In a mixed game strategy Nash equilibrium is introduced to assist with the mitigation technique of IoT based threats in SHAS. A Nash equilibrium is a term used to describe a stable state in a game where no player has a reason to change their strategy. An option to using Nash equilibrium is to employ the backward induction approach. During a game, each player strategically selects acts that maximize their own potential gain, while also considering the logical choices made by other participants. A player's strategy includes a complete set of actions to be taken in every possible game situation. This is because changing strategies could result in decreased pay-offs, assuming all players are following the prescribed strategy. The added parameters to the game are the following:

- The probability of attack: u_A
- The probability of defender: y_D

The defender which defense against the attacker uses the drop packets technique which is suitable to mitigate the system from being attacked. The defender observes the information about the attack and decides which action to choose. Y_D denotes the probability for the defender over the action payoff node p, u_A denotes the probability distribution for the sender strategy over the action. The sending rate is then observed.

Defenders payoff is calculated using the following equation:

$$a11yd1 + a12yd2 + \cdots . + a1nydn \leq N \tag{3.19}$$

$$a21yd1 + a22yd2 + \cdots + a2nyn \leq N$$

$$yd1 + yd2 + \cdots + ydn = 1$$

The sum of probabilities must be equal to 1 where $y1, y2, \dots yn \geq 0$.

Algorithm 4:Implementation of early mitigation mixed game model

1. Inputs: y_D, u_A, T_b // define inputs
2. Output: Response time, block time
3. Repeat {
4. If $y_D \geq N_D$ // Attackers are not attacking"
5. "allow the packets to pass"
6. **Else**
7. $y_D \leq N_A$ //Attackers are attacking
8. "block the packets"
9. Observe T_b;
10. **Else**
11. $u_A \leq N_D$ //Defender allow block
12. "calculate sending rate"
13. End If
14. $t \leftarrow t_b+1$ }

Algorithm 4: Compute Mixed Game Theory for Mitigation

3.5 Chapter summary

In this chapter, the steps to conduct this research were provided. It has been demonstrated that the game theoretical model was applied to detect IoT-based threats in home automation early and the importance of game theory to mitigate such threats was explained. The game theory method is useful because it models how each player acts and which strategies they use as well as how they interact with each other. Most detection and defence methods have not yet been fully put into place in networked environments, so one cannot rely on them completely. The above method, on the other hand, has worked well to solve the smaller problems that have been raised.

4 Chapter 4: Performance evaluations

4.1 Introduction

In Chapter 3, the research method that was used to answer the subproblems was explained. This method was compiled into a game scheme that showed all the players, their strategies, and the nature of their usefulness. The researcher was able to confidently calculate the best detection response rate and the sending rate to help block the threats before the expected time. This shows how the strategies of a player depend on the strategies of the other players in the game. Since a theoretical model cannot yield the right answers, MATLAB was used to run this model. In this chapter, the proposed method is evaluated and compared with other methods that are similar in a few ways. The approach considers the criteria for evaluation, the simulation, and a comparison of the reviewed literature.

4.2 Computer simulations

A computer simulation is the use of computer software to model "real-world" processes, systems, and events. Simulation is the process of constructing a computational representation of the underlying theoretical logic that connects simplified worlds. MATLAB was utilized to aid in the simulation of the proposed designs. MATLAB is a programming environment with its own programming language that specializes in scientific numerical computing, modelling, algorithm design, computer simulations, data analysis and presentation, signal measurement and processing, control system designs, and data analysis and presentation. The two objectives tested are outlined below.

The first objective was to incorporate a suitable game theoretical strategy that can improve the early detection of the IoT system-based threats in SHA. A pure and mixed game theory strategies were chosen to assist with the detection technique for early response time after a thorough literature review. Through calculations and algorithms, the pure and mixed game theoretical strategies were utilized to analyse and model the response time in IDS for the IoT based threats in SHA. The purpose of this objective was to identify an optimal game theory strategy that can effectively enhance the early response time in IDS. The second objective was to incorporate a suitable game theoretical strategy that can improve the early mitigation of the IoT system-based threats in SHA.

A thorough evaluation and investigation were conducted to identify an appropriate mitigation technique that can be incorporated into the early mitigation of IoT-based threats in SHA. To achieve the intended results for the SHAS, both pure and mixed game-theoretical strategies were implemented to assess the appropriate early mitigation of the IoT based threats using different mitigation techniques.

In the simulation, two game theoretical model will be simulated and the following results are expected: i) detection response time; and ii) the sending rate for the mitigation. The simulation platform was established in order to assess the impact of the game theoretic IDS based on real network models. In the event of an unexpected attack on the SHAS, the IDS employs an ideal defence strategy to prevent damage to the system's operation and ensure its availability is secured. This is achieved through the responsive actions of the IDS engine. The proposed solution aims to enhance the response time of the IDS and firewall in both detecting and mitigating attacks. By adjusting the defender variables that were computed in the third chapter, there will be an improvement in the system's response time. Therefore, it will assist the system with a better response time. The outcomes of the early detection and mitigation game theory model are then analysed and compared with existing literature-related models. Finally, performance comparisons with the detection response time and the sending rate are demonstrated. These two simulations will aid in a proper understanding of the developed game schemes.

4.3 Early detection of IoT system-based threats in SHAS using game theory

4.3.1 Introduction

Two game-theoretic approaches were put to the test to determine which one would perform better. The reasons for choosing these game theories are that the output of the models could be easily interpreted and implemented in the IDS. The proposed mathematical model and the algorithms for both strategies were developed in Chapter 3. Therefore, it is very important to measure the performance of both game strategies in the early detection of IoT-based threats. The researcher started with the pure game theory strategy and the mixed game theory strategy, as illustrated below. The next section provides an overview of the analysis conducted on the defense response time mechanism, employing a strategy based on pure game theory.

4.3.2 Early detection of IoT system threats using pure game theory

This section outlines the response time defence mechanism that is based only on pure game theory. With pure game theory, our main goal is to maximize the defender's response in order to turn on the IDS device as soon as possible in the SHAS so that IoT based threats are discovered as quickly as is possible. The measurement of response time is utilized to evaluate the rate at which a system responds to changes in its input. The game entails a collaborative interaction involving two players, namely an attacker and a defender. The 2x2 game matrix was formulated and evaluated using various parameter values to optimize response time in IDS. The initial participant assumes the role of the defender, with an in-depth knowledge of the IDS that monitors the connection that exists between the router and the designated SHA network. An algorithm for a suitable strategy to aid in the early detection response to IoT-based threats in SHAS using pure game theory was evaluated and simulated. Different variables affecting the performance of the detection response time are represented in the simulation.

	Player 2		
Player 1		Attacker	Defender
	Attacker	[5, 2]	[3, 6]
	Defender	[8, 3]	[0, 5]

Table 4.1 Differential variable.

The aforementioned results depicted in Figure 4.1, 4.2 and 4.4 displays the graphs of the derived algorithms in Chapter 3 to expedite the response time to the detection of IoT based threats in SHAS.

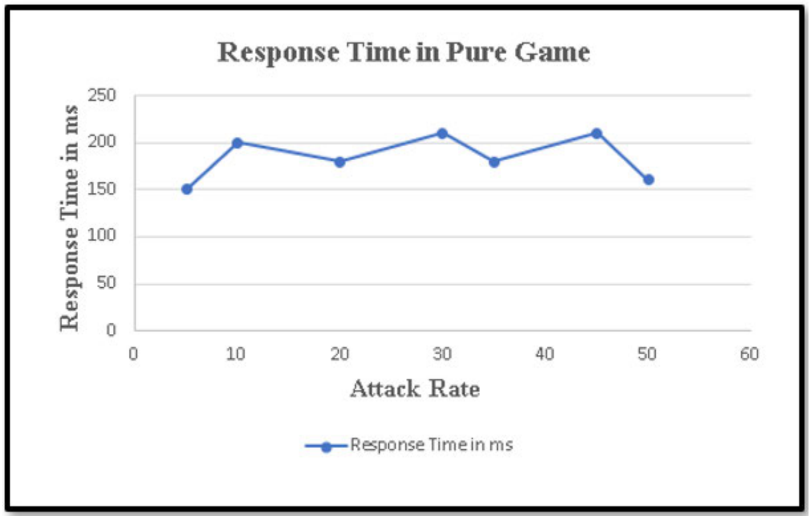

Figure 4.1: The response time graph for (Ha1,Hd1)=(0.3,0.7)

Figure 4.1 above is the graph of the response time for the payoffs of the pure game theory strategy. The graph represents the time it takes for the IDS to process an attack in the SHAS and respond with the defenders' strategy to make sure that the attacker doesn't gain unauthorized access. First, we measured the response time which is the time the system takes to respond to an attack over the attack rate which is the number of attacks that attacks the system at a certain period of time. The methodology is measured against calculated payoffs which are then simulated using MATLAB. To measure how quickly a new attack is detected we calculated the payoffs of each game strategy and the payoffs are (H_{a1}, H_{d1})=(0.3,0.7). The above figure shows the change in response time whenever the number of attacks is exposed by the IDS. The graph displays the response time of 150ms when an IDS detects an attack in the SHAS. As the number of attacker nodes increases, the rational attacker is more likely to withdraw more frequently (i.e., with a greater probability). Hence, the response time will vary in accordance with the likelihood of the attacker nodes, resulting in either an increase or decrease. As the number of nodes increases, the difference between the optimal time and the attack rate obtained will significantly increase. Response time is one of the important metrics in evaluating the defense system as it protects the system to getting exposed to a number of attacks in the system.

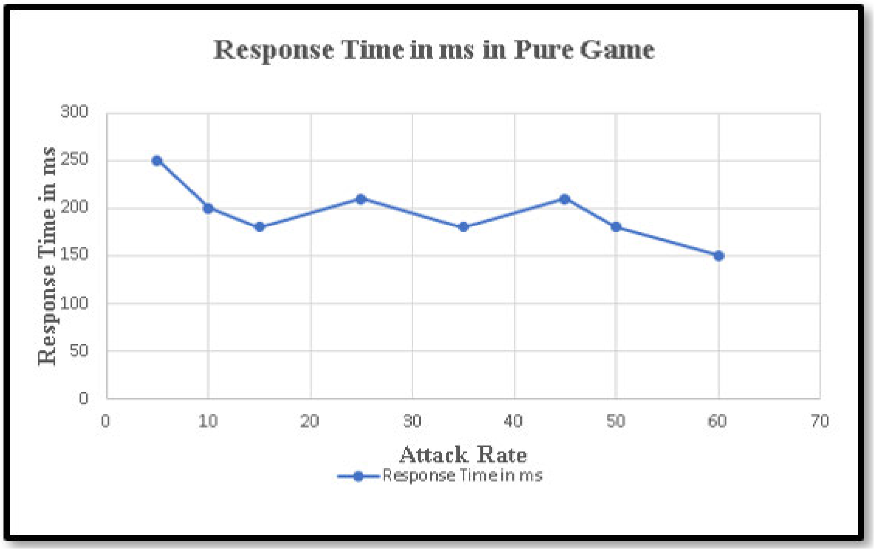

Figure 4.2: The response time graph for (Ha2,Hd2)=(0.5,0.8)

The simulated results of the payoffs for the attacker and the defender, as calculated in Chapter 3, are illustrated in Figure 4.2. The values (Ha2, Hd2) = (0.5, 0.8) represent these payoffs. An enhancement in responsiveness has been illustrated above, and the simulated outcomes indicate a significant improvement. If there are attackers in the SHAS, the IDS detects the threat at a response time of 250 ms. A positive correlation exists between the number of attackers involved in the SHAS and the efficiency of response time. The graph additionally demonstrates that when the attack rate is at 60, the IDS system exhibits a response time of 150 ms in mitigating attacks in the SHAS environment, indicating a significant enhancement.

The implementation of a pure game theory strategy algorithm into the IDS can effectively address the issue of resource allocation and enhance response time. The response time of the defenders' strategy and the response time in IDS will both be improved by speeding up the game by increasing the number of defenders. The next section illustrates the evaluation of response time using mixed game theory strategy.

4.3.3 Early detection of IoT system threats using mixed game theory

In this section, the evaluation of the mixed game theory technique is simulated and tested by employing the MATLAB simulation software. The essential part of this early detection system entails the application of mixed game strategies (δa, σd) to optimize the response time for detecting threats in the IoT within the SHAS. Furthermore, it is worth noting that both the players carrying out the attacks and those defending against them have the capacity to occasionally change their approaches with the aim of achieving the most effective results. A mixed game theory approach will be used to detect IoT-based threats early in SHA in order to evaluate its effectiveness to a pure game approach. The figures below show the outcomes of the simulation of the early detection of IoT-based threats in SHAS utilizing mixed game strategies.

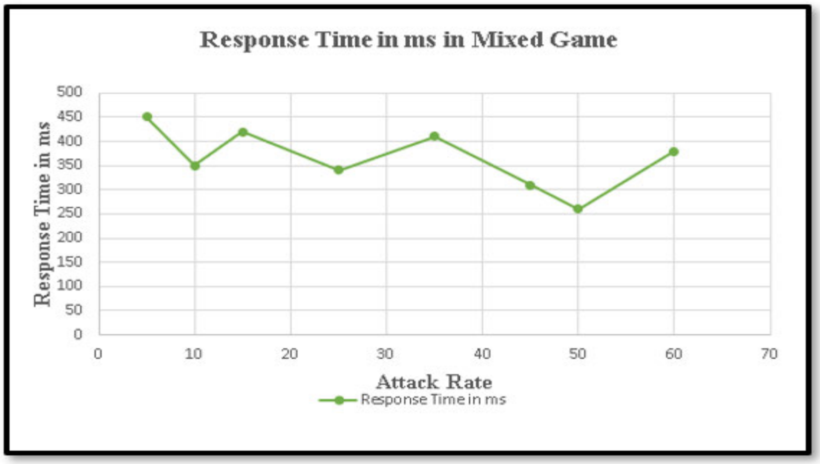

Figure 4.3: The response time in mixed strategy (δa1, σd1) = (0.3,0.7)

Figure 4.3 above depicts the response time graph of the mixed game theory with the proper payoffs (a1, d1) =(0.3,0.7) in the IDS. The aforementioned findings indicate that the system presents a response time of 450 milliseconds upon detecting an attack in the SHAS. Subsequently, the system demonstrates enhanced performance when the number of attackers within the system increases, hence enabling the system to promptly counteract and mitigate the increasing number of unwanted threats within the SHAS. Depending on the pace of attackers in the SHAS, the overall response time of the aforesaid mixed strategy is kept in the range of 250ms to 450ms.

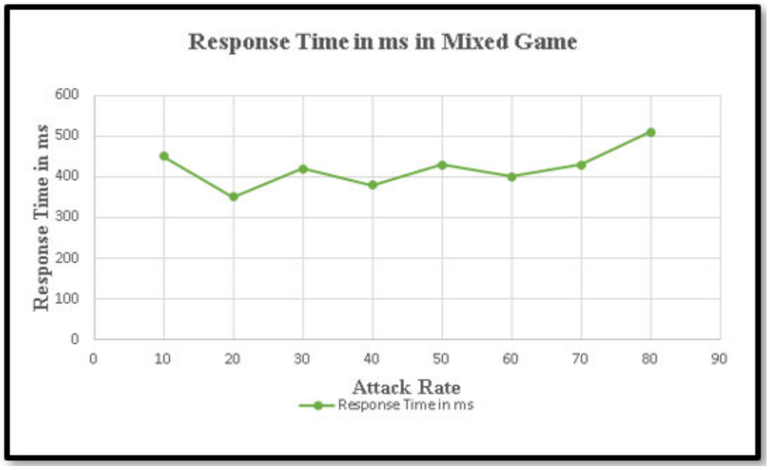

Figure 4.4: The response time in mixed strategy (δa2, σd2) =(0.5,0.5)

Figure 4.4 above displays the response time graph of the mixed game theory in the IDS, incorporating the suitable payoffs (δa_2, σd_2) = (0.5, 0.5). The SHAS has a response time of 450 milliseconds upon the detection of an attack, accompanied with an attack rate of 10. The aforementioned mixed strategy demonstrates that the observed response time of this particular approach falls within the range of 350 to 500 milliseconds, while maintaining an attack rate below 90. The system's response rate can be enhanced by increasing the number of defenders, hence accelerating its overall speed and improving the system's response time.

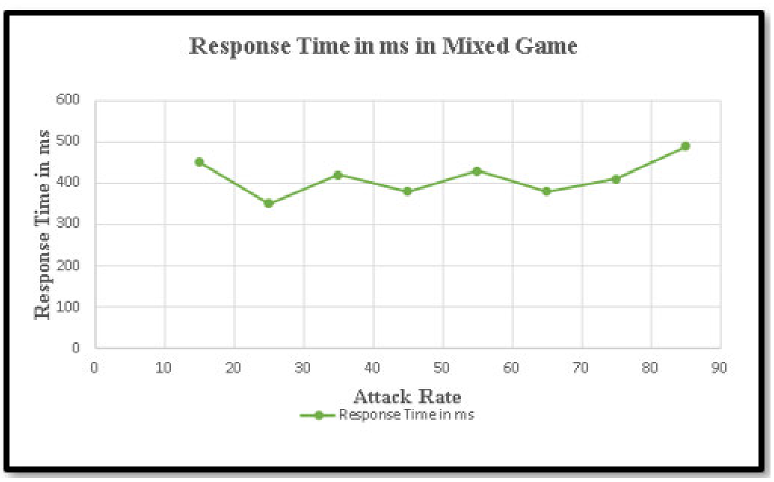

Figure 4.5: The response time for mixed strategy (δa3, σd3) = (0.7,0.3)

Figure 4.5 shows an illustration of the response time in anticipating the attacker. The possible enhancement of the efficiency of the IDS can be achieved by the application of mixed game theory with proper payoffs, specifically (δa_3, σd_3) = (0.7, 0.3). According to the results above, the mixed strategy illustrated in chapter 3 can react to an attack in a range of 350 to 500 milliseconds, with 450 milliseconds being the starting point. A minor enhancement can be implemented to improve the response time.

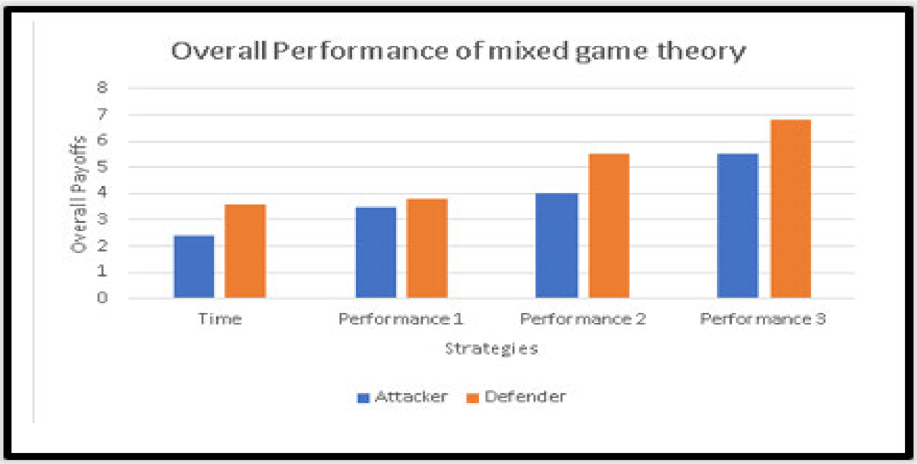

Figure 4.6: The overall performance of the mixed game theory strategies

Figure 4.6 depicts a comparison of the overall payoffs derived from mixed game theory for players employing three different mixed approaches. The payoffs for defenders appear to be slightly higher than those for attackers, indicating that the game model is more advantageous and steadier for the defenders. Furthermore, it is evident that the difference in overall payoffs between the attackers and defenders is rather small. This observation indicates that mixed game theory is advantageous not just for individual players but also for maintaining a balanced relationship between attackers and defenders.

4.3.4 Discussion of the early detection technique

The results pertaining to the response time for triggering the IDS in order to detect IoT-based threats in the SHAS utilizing game theoretic methodologies are presented in Figures 4.1 to 4.6 above. Both pure and mixed game theory were examined and the findings from the simulations were afterwards analysed. Pure game theory was chosen because of the game's flexibility in transforming interactions between two devices—the IDS device and the intruder—where conflict will be resolved utilizing the game's equilibrium conditions. We further advanced the application of mixed game theory in order to enhance the timely detection of IoT based threats within IDS. The utilization of pure game theory for early detection has demonstrated a modest enhancement in comparison to the implementation of a mixed game strategy. The primary reason for selecting pure game theory is based on the determination of a definite, premeditated course of action that a player will undertake within a game. In simple terms, a pure game strategy can be defined as the approach that yields the highest possible profit or optimal outcome for the participants involved. Hence, it is widely considered to be the optimal approach for all participants in the game. Therefore, in future research it can be recommended that using pure game strategy will improve the detection response time in the SHAS. By utilising the principles of game theory, employing a suitable IDS, and implementing efficient algorithms, the efficacy of the proposed model exceeds that of the evaluated solutions. The section that follows presents analysis and comparisons of the two detection techniques, DEDA and machine learning, which are then contrasted with game theory strategies.

4.3.5 Comparisons of the early detection techniques

The review and evaluation of the effectiveness of the detection rate involves a comparison between the prediction graph for the developed detection rate and the reviewed findings by Kiranda *et al*. [70] and Giang *et al*. [71] in the literature.

4.3.5.1 Early detection of IoT system threats using DEDA

Figure 4.7 below depicts the reviewed results of Karande *et al.* [70], where early detection of topology attacks in the IoT systems was employed. The graph displays the results of predicted error rate versus the predicted time ahead. The proposed algorithm, distributed early detection algorithm (DEDA) for topology attack detection in the IoT network works by placing monitoring nodes in addition to normal nodes for attack detection. The placement of additional nodes results in the uninterrupted operation of ordinary nodes by avoiding computing and memory overload of executing detection algorithms on them. These additional monitoring nodes monitors all traffic from nearby IoT nodes and build a descriptor table of it. This descriptor table includes a count of various control packets transmitted from the individual node.

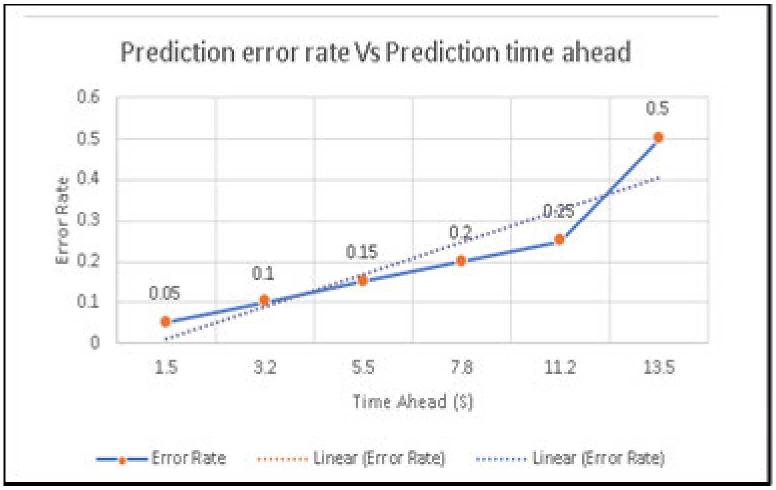

Figure 4.7: The detection response time using DEDA algorithm

4.3.5.2 Early detection of IoT system threats using machine learning

In their study, Giang *et al.* [71] introduced a collaborative machine learning approach that aims to improve the early detection of IoT Botnet, even when working with incomplete time series data. The framework for detecting IoT botnets has been developed using a collaborative machine learning model and a V-Sandbox execution environment. The results of the early detection of botnets using the machine learning method are illustrated in Figure 4.8. The effectiveness of the suggested model has been substantiated through comprehensive empirical findings utilizing a wide range of datasets.

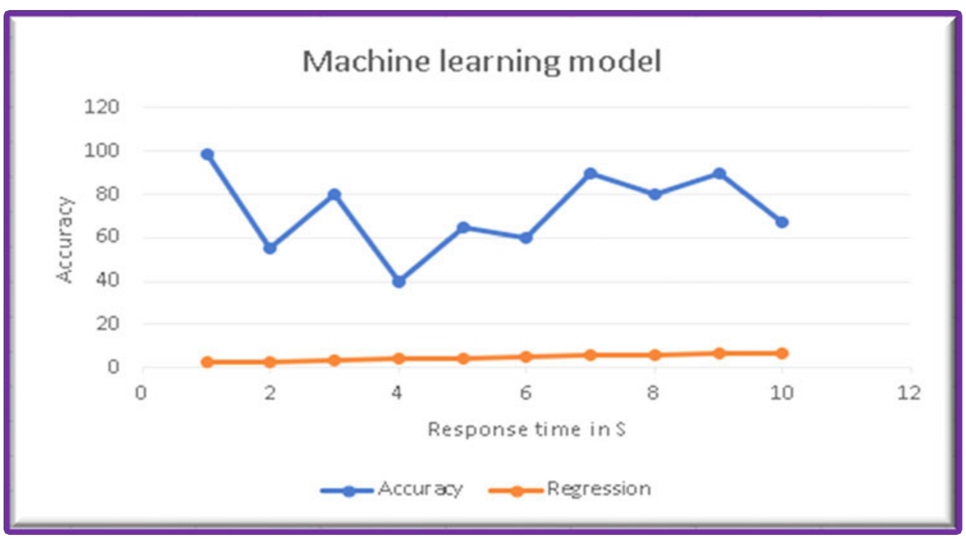

Figure 4.8: The detection response time using machine learning model

This assessment is predicated on the response time of early detection of these IoT devices. Figure 4.9 below displays the efficiency of various strategies or algorithm proposed in research in the realm of identifying the method for early detection of threats related to the IoT within different environments. By utilising the principles of game theory, employing a suitable IDS, and implementing efficient algorithms, the efficacy of the proposed model exceeds that of the evaluated solutions. And as mentioned in literature by Kurand *et al.* [70] that by adding more nodes into the system, it improves the performance of the detection and early response is highly achieved. The proposed method was indeed incorporated into our game theoretical strategies and in Chapter 3 the number of the defensive nodes in each game strategy was greater than the number of the attacker nodes.

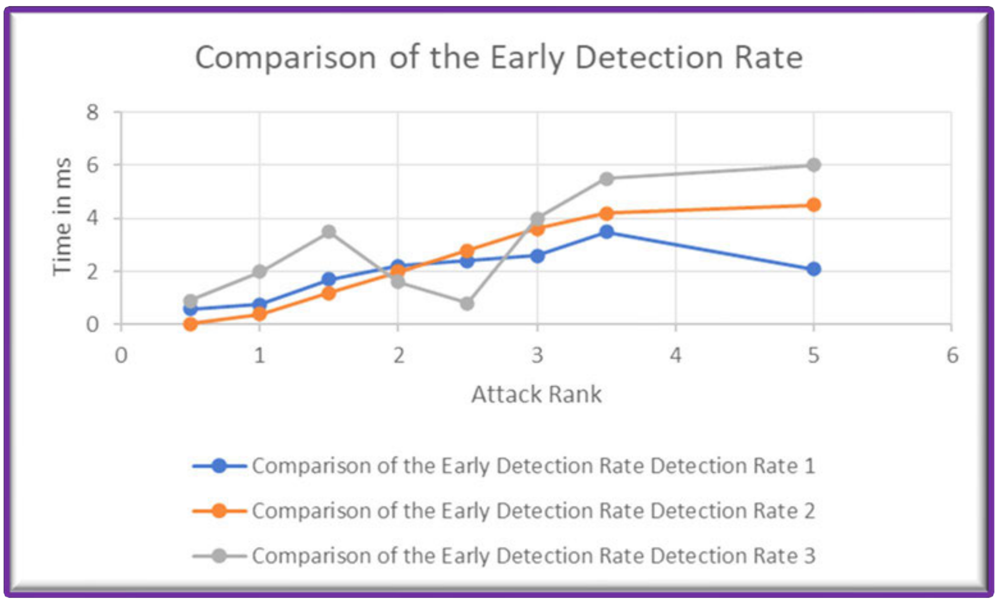

Figure 4.9: The comparison graph for Early Detection Rate

Based on the available evidence and analysis, the following conclusions can be drawn:

1. The game model has greater stability compared to other studied models and demonstrates improved response performance.

2. The implementation of a pure game theory method has been shown to significantly enhance the detection response time. It may be concluded that when the pure game theory strategy achieves the best payoffs by sticking to one strategy and can achieve optimal results.

The following section presents an analysis and discussion of early mitigation technique using pure and mixed game theory strategies in the context of the drop packet firewall approach.

4.4 Early mitigation of IoT-based threats using game theory

4.4.1 Introduction

The decision was made to implement the drop packet firewall strategy as the preferred method of mitigation. Nevertheless, this strategy is not without its drawbacks. One of the drawbacks associated with this strategy is the potential decrease in the sender's throughput. Hence, this section includes an analysis of both pure and mixed game theoretical approaches, with the drop packet firewall, to ascertain the optimal strategy for early mitigation of IoT based threats in SHAS. The mathematical model and algorithms for both strategies were developed and documented in Chapter 3 of the research paper. Therefore, it is crucial to assess the efficacy of both gaming tactics in the initial mitigation of IoT-based threats in the SHAS. The researcher initiated the implementation of mitigation methods employing a pure game theory technique, then transitioning to a mixed game theory approach.

4.4.2 Early mitigation scheme using pure game theory

Pure game theory is applied to the early mitigation of IoT-based threats in SHAS approaches. The MATLAB simulation software was utilized to facilitate the evaluation of the simulation outcomes related to the suggested approach for early mitigation of IoT-based threats. This approach involved enhancing the data rate of the mitigation technique in order to protect SHU. The firewall employs an effective filtering technique that incorporates settings developed from a robust pure game theoretical approach. This enables the configuration of drop packets at an optimal level to accomplish prompt mitigation. The firewall, acting as the defender in the game, will employ a strategy aimed at minimizing the delay in dropping packets and ensuring that legitimate packets from the SHAS are not mistakenly dropped. The game matrix is a 2x2 matrix that represents the strategies available to both the attacker and the firewall. The methods are limited by two parameters, namely the sending rate and the maximum number of connections. The mitigation strategy was implemented within the MATLAB software, including the control of the sending rate, the duration of wait time for dropped packets, and the control of the amount of connections by SHU.

Table 4.1 presents the packet and mitigation procedure, wherein the control of packets is achieved through the manipulation of the sending rate. Due to the system's high workload in blocking packets, there is a likelihood that it may experience exhaustion and exhibit disruptive behaviour. The mitigation scripts function by implementing measures that restrict attacker nodes from transmitting packets to the targeted server for a duration of one minute, while simultaneously permitting the passage of permitted packets within the network.

Parameter	Value	Remark
Sending rate	5s	Specifically adapted to the simulation environment
Maximum Connection	10	The most effective approach to solve the game
Waiting time	0.5 minute	Specifically adapted to the simulation environment

Table 4.2: The firewall settings

To perform the simulation, the total number of SHU to be allowed on the SHAS network is 5 for experimental purposes. This value will be used to determine the number of connections allowed for a single user. The game output to be used for the simulation is looked up in the fitness table 4.2 as shown below.

Sending rate	Number of connections	Game strategy
0,5minutes	2.5	x_1
1 minute	5	x_2

Table 4.3: The fitness settings

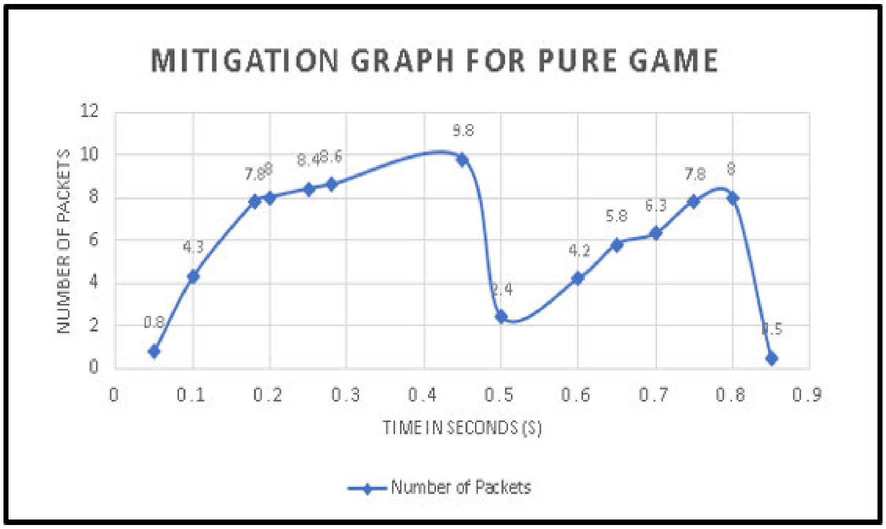

Figure 4.10: The sending rate curve for mitigation using pure game theory

Figure 4.10 illustrates an identifiable trend wherein malicious packets are effectively blocked prior to one minute, following an extended duration of maintaining an acceptable threshold of 10 maximum connections for the SHAS. The firewall which is the defender in the game actively monitors the SHAS for a duration of one minute, during which it permits only a limited number of packets emanating from the home users. Concurrently, the firewall actively monitors the number of packets being sent. The accessibility of the attacker remains as long as the mitigation strategies accurately detects the existence of unauthorized packets originating from the attacker.

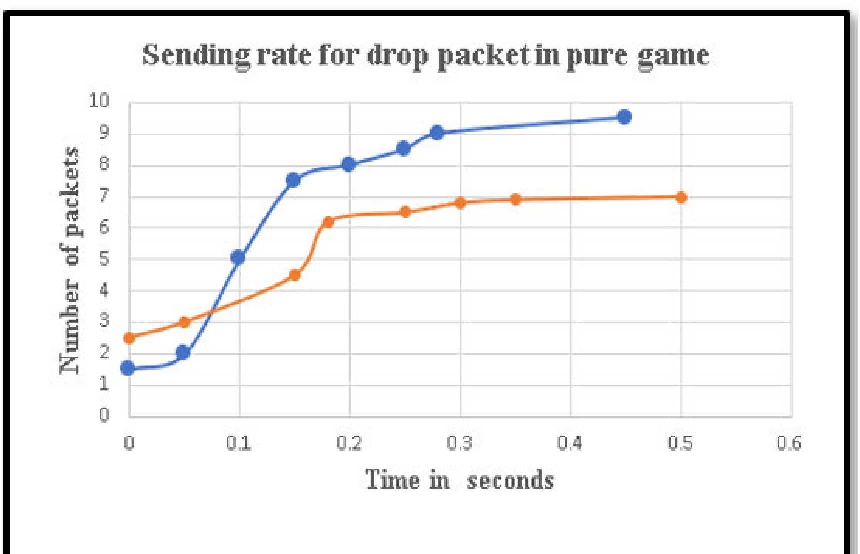

Figure 4.11: The diagram of packet drops and packet allowed

The time in seconds and the number of packets allowed in the firewall settings are depicted in Figure 4.11 above. Because of how the firewall is configured, it can be clearly seen that packet eliminate is kept at roughly 0.6 seconds while packet allowed is pined at 10. The firewall restricts the sending of packets that exceed the predetermined limit established by the administrator of SHAS. It is important to acknowledge that all authorized SHU are duly registered, as they adhere to the prescribed guidelines and prevent from sending packets that exceed the allowable amount.

4.4.3 Early mitigation scheme using mixed game theory

The application of mixed game theory strategy is utilized in the early mitigation of threats that arise from IoT in SHAS. The game matrix, also known as the payoff matrix, is created using a scale that ranges from 0% to 100% to represent the payoffs. The firewall can be positioned within a range of 10 to 50 connections, accommodating the potential rates at which attackers can send data. In the event that the firewall imposes restrictions below the attacker's maximum threshold, the firewall will experience negative consequences. Moreover, in the event that the firewall imposes a restriction that exceeds the capacity of the attacker, a greater number of packets will be discarded, hence increasing the likelihood of legitimate packets being mistakenly rejected as well. The experimental bed should have a minimum of 50 connections and a maximum of 90 connections. Consequently, the payoff matrix is designed to accommodate this range. The game matrix is restricted to a 5 x5 matrix indicating 5 strategies each for the attacker and firewall respectively. Table 4.3 presented below illustrates the output strategies employed in the game to replicate the early sending rate and packet drop of threats originating from the IoT in SHAS. The strategies are related to two parameters on the fitness table which are the number of connections allowable and the maximum sending rate (which is fixed in this case to 3/s general limit) allowable for each connection. The number of connections determines where the firewall is placed. The payoff matrix contains only payoffs for the firewall (the owner of the game).

Sending rate	Number of connections	Strategy
0.2	2.5	*D1*
0.4	5	*D2*
0.6	7.5	*D3*
0.8	8.5	*D4*

Table 4.4: The Mixed game strategies output

The below results in Figure 4.12 displays the mitigation results using mixed game theory. After the simulation, the mitigation mechanism blocks the threat packets entering the SHS at a rate of 3 minutes with the 10 probabilities that preserves system functionality and allows authorised users access.

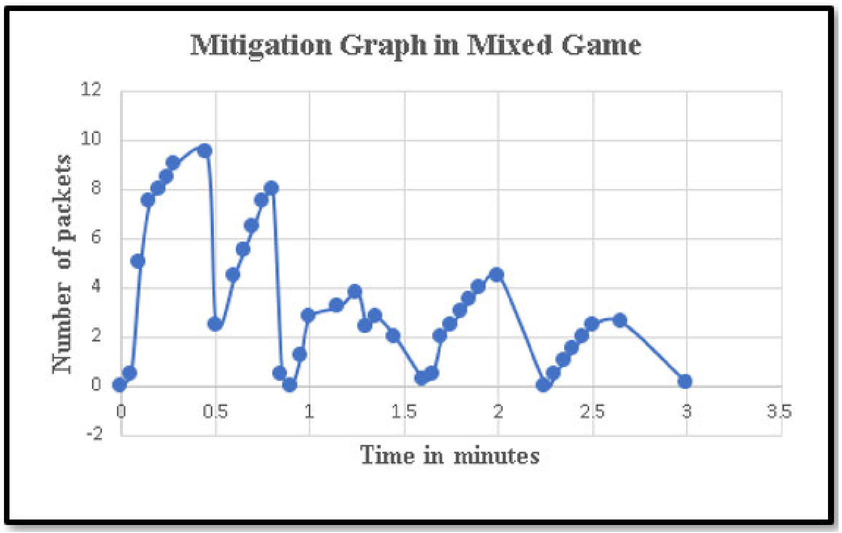

Figure 4.12: The sending rate curve for mitigation using mixed game theory

The above Figure 4.12 displays how the results are depicted in order to early mitigate the IoT based threats in SHAS. The graph on the horizontal represents the number of packets allowed to access the SHAS and the vertical represents the time it takes for sending rate to drop the packets and get rid of attackers in the SHAS. The firewall which is the defender will use the above settings depicted in table 4.3 in order to assist with the evaluation and the simulation of the sending rate and dropping malicious packets (attackers). The mitigation strategy involves the implementation of a designated period during which a node is identified as an attacking node. In order to facilitate experimentation, the simulation bed has the capability to accommodate a minimum waiting period of 3 minutes. This implies that a node designated as an attacking node will continue to transmit packets as long as it maintains a rate of sending that exceeds the permitted threshold specified by the firewall. The sending rate needs to be as early as possible in order to ensure that unwanted packets are blocked and the legitimate ones are not delayed access due to the blocking of malicious ones. A periodic evaluation is conducted at three-minutes intervals to determine whether the sending rate has decreased, with the purpose of unblocking the legitimate users. For a minimum time of 3 minutes we can observe that it takes 0.5 minutes sending rate to send the maximum number of packets and then drop and block the unwanted for a period of 1seconds.

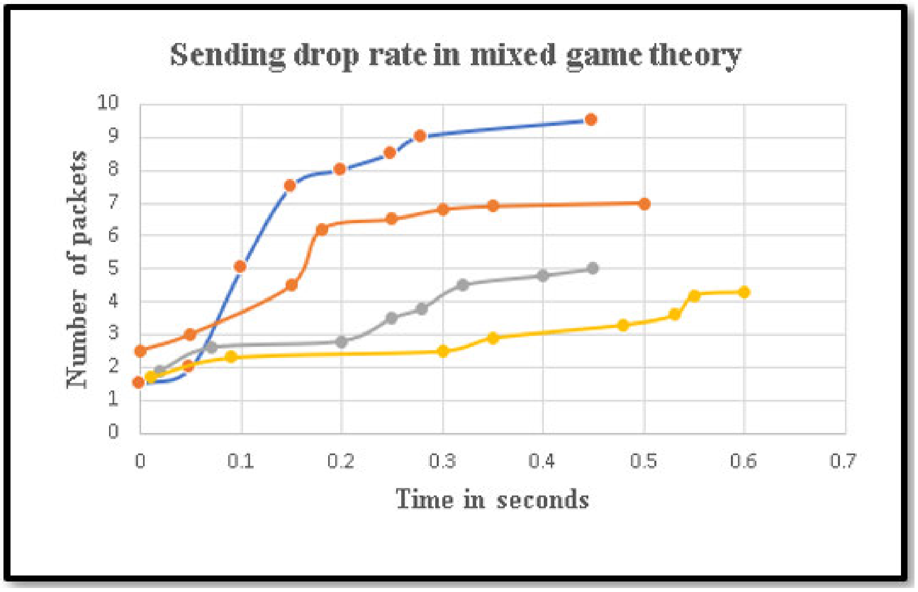

Figure 4.13: The diagram of the sending drop rate in mixed game theory

Figure 4.13 illustrates the impact of four strategies (D1-D4) on the drop rate of bits when employing an early sending rate. In the provided figure 4.13, D1 is depicted by the blue line, D2 is depicted by the grey line, D3 is depicted by the orange line, and D4 is depicted by the red line. Based on the above figure, it can be observed that the response time for the packets decreases if an intruder or attacker is discovered. It is crucial to monitor this response time as it enables the smart home user to witness the improvement in the system's ability to respond to intruders using the game theory approach. The initial three strategies exhibit a slight deviation from the prescribed limits of 7, 5, and 4.5, which can be attributed to the rapidity of the attack. This observation suggests that it is feasible for legitimate packets to be dropped, as legitimate users are capable of transmitting at these rates. Notably, Figure 4.13 demonstrates a distinct restriction on packet transmission for a firewall configuration with a game value of 10 connections. In the simulation environment, the early sending rate is determined to be 10 based on the game output, employing strategy D4 and a time interval of approximately 0.6 seconds.

4.4.4 Discussions of the performance results for early mitigation schemes

The second objective entailed the early mitigation of IoT based threats in SHAS through the implementation of both pure and mixed game theoretical approach. The mitigation strategy includes a predetermined time delay prior to identifying an attacker as an opposing attack. The simulation platform has a minimum delay time capability of 0.4 minutes, which is suitable for conducting experimental investigations. This implies that the players selected as an attacker will continuously receive packets as long as they maintain a sending rate that doesn't exceed the allowable rate of the firewall. As a result, both the pure and mixed game theoretical approaches were put to test in order to determine which one will perform better to early send the drop packets to eliminate the unwanted packets in SHAS.

As a result of the shortage of literature pertaining to IoT-based threat mitigation strategies in the realm of SHAs, it has been established that the implementation of a drop packet firewall serves as the superior approach for enhancing the initial packet sending rate with the objective of preventing unauthorised access to the SHAS. According to the results of the proposed research, an SHAS can benefit from the application of mixed game theory to counteract the IoT based security threats. A mixed game strategy, which is typically based on a random selection with some probability, will select various possibilities at various points. The variety of choices each player in a mixed game theory chooses leads to the proposed early mitigation strategy performing better since it necessitates a solution that can solve both the dropping and improving the sending rate. The success of this endeavour can be attributed to the use of a game-theoretical strategy, which has already been shown to successfully deal with the challenges of timely mitigation in more general system security contexts. Further research is needed to boost the efficiency with which these IoT based threats are detected and mitigated in the context of SHA.

4.5 Chapter summary

This chapter discussed different methods for evaluating the efficiency of early detection and mitigation of IoT-based threats in SHAS. The study started by analysing the early time response to the detection of IoT based threats in SHAS through the application of a combination of mixed and pure game theoretical methodologies. Pure game theory was found to be the most effective strategy for early detection of threats in IoT-based systems. Pure game theory is considered the optimal approach due to its ability to effectively address early detection in SHAS. By employing a fixed strategy that prioritizes the given strategy, the implementation of early detection can be facilitated. The selected game strategy exhibits a level of comparability with other existing strategies. The second objective was assessed by comparing pure and mixed game theory approaches to aid in the early mitigation of IoT threats in SHAS. A comparison was made between the simulated outcomes of both mixed and pure game theory approaches, suggesting that the use of mixed game theory is well-suited for the early mitigation of IoT threats in SHAS. In conclusion, it has been demonstrated that early detection and mitigation of IoT-based threats using a game theoretic method yield better results in terms of early response time and sending rate.

Chapter 5: Conclusion and recommendations

5.1 Summary of findings

As outlined in section 1.2, the main purpose of this research was to develop an early detection and mitigation of IoT-based threats in a SHAS using game theory. Both pure and mixed game theory strategies were employed in the system to assist with the early detection and mitigation of those IoT-based threats. Many studies were reviewed regarding the use of game theory strategies to better enhance the performance of the IDS and the block port, as evidenced in Chapter 2. The proposed method combined the advantages drawn from the different game theory-based methods.

Chapter 3 focused on the system modelling of the research to look at the background information needed to solve the problem. This provides background information on game theory and its different strategies, including their mathematical equations and algorithms. The methodology outlined in Chapter 3 also shows the proposed approach to solving the security issues of smart home automation by applying game theory strategies to the deployed IDS and firewall in the system. There were two parts to this approach. The first part was to develop a suitable pure and mixed game theory strategy for the early detection of IoT-based threats. The second part consisted of the development of a suitable pure game strategy for early mitigation of IoT-based threats.

The first part focused on the modelling of early detection of IoT-based threats. The main goal of the detection module is to detect using the IDS early on to assist with pure game techniques. The IDS was deployed to process attack information in the context of the system to accurately identify the target of an attack. Intrusion detection systems use algorithms to carry out the various steps of intrusion detection. They made use of the anomaly-based IDS.

The second part focused on modelling the early mitigation of IoT-based threats. The main goal of the mitigation module was to take the necessary steps to prevent the discovered threats from causing harm. The algorithm for the mitigation technique was created using game theory. The pure game theory strategy, based on an algorithm, aided in the removal of unwanted packets from the smart home system. The mitigation module assisted in limiting access to smart home automation and ensuring that threats are dealt with in real time before any damage is inflicted.

In Chapter 4, the results of the simulations of early detection and prevention using pure game theory were looked at, compared, and talked about. The results of the early detection using pure game theory indicated the response time required to detect an intruder. When threats are detected in real-time and the detection rate is increased in a smart home system, it ensures the safety of the homeowners.

The results of the early mitigation model using pure game theory showed that the firewall drops packets whenever an IoT threat is detected to prevent further harm or damage to the smart home system. The mixed game strategy was also tested, and the results were compared, discussed, and concluded. According to the results of the proposed research, smart home automation systems could benefit from the application of mixed game theory to identify and counteract IoT-based security risks. A 0.5 ms detection rate and a 20 s sending rate to mitigate unwanted threats can be achieved, allowing for the elimination of IoT hazards before they cause any damage.

5.2 Conclusion of the study

In this research, the researcher used game theory for the early detection and mitigation of IoT-based threats in a SHAS. The main objectives were to solve the response time to early detect by activating the IDS as early as possible and to early mitigate by activating the firewall to block those threats as quickly as possible. The following objectives were developed to achieve the proposed solution.

A suitable pure game theoretical strategy can improve the early detection of IoT system-based threats in smart home automation. The IDS can recognise attackers for 0.4 ms probability or omit attackers for a 0.16 probability. Based on the results discussed in Chapter 4, it was demonstrated that indeed using pure game theory can improve the detection rate of the IoT based threats in a SHAS.

A suitable pure game theoretical strategy can improve the early mitigation of the IoT system-based threats in smart home automation. The results indicate that the rate of blocking packet transmission whenever an intruder is detected at the sending rate of 2 is 35 ms probability with the false alarm of 1225 ms.

A suitable mixed game theoretical strategy can improve the joint early detection and mitigation of IoT system-based threats. The IDS can detect an intruder at 0.3 ms with the false alarm of 0.09 probability. The mitigation mechanism blocks threat packets entering the SHS at a rate of 10 ms with 100 probabilities that preserve system functionality and allows authorised users access.

Overall, the primary objective to early detect and mitigate IoT based threats in SHAS using game theoretic has been proven to be an efficient and effective method. Timely detection of IoT based threats in SHA is critical given the impacts the intruder can cause to home users. Therefore, using the above solutions has proven that the response time requirements in the system can be further improved. Game theory demonstrated the ability to improve the system by detecting and mitigating the IoT-based threats in the SHAS as early as possible.

5.3 Recommendation

The study recommends the following issues for further research:

1. The importance of providing SHA users with proper guidance regarding the security of the IoT system so that they can also find ways to mitigate the situation on their side by making sure they set up strong passwords to prevent intrusion.
2. Future research needs to concentrate on enhancing the functionality of the early detection and mitigation of the IoT based threats in smart home automation. The goal of future research is to design a fully automated system that is capable of learning and training itself.
3. A full-scale implementation of the game theory output should be incorporated into the firewall mechanism on the router.
4. A concerted and deliberate effort should be made by security experts in educating the public on the danger of using computers that are prone to IoT threats in smart home automation. When a system does not have at least some minimum level of security, the tendency that it will form part of the Internet, and the likelihood of IoT based threats is very high, especially if that system is always connected to the Internet.

6 References

[1] O. Vermesan, and P. Friess, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystem." Aalborg, Denmark: River Publishes, 2013.

[2] Gartner I, "Gartner Identifies Top 10 strategic IoT Technologies and Trends", https://www.gartner.com/en/newsroo/press-releases, 2018.

[3] J. Zhou, Z. Cap, X. Dong, and A.V. Vasilakos, "Security and privacy for cloud-based IoT: challenges." IEEE Commun Mag, pp. 55(1):26–33, 2017.

[4] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, ``The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1606_1616, Apr. 2018.

[5] M. B. Yassein, I. Hmeidi, F. Shatnawi, W. Mardini, and Y. Khamayseh,``Smart home is not smart enough to protect you_protocols, challenges and open issues," *Proc. Comput. Sci.*, vol. 160, pp. 134_141, Jan. 2019.

[6] T. Bailey, J. Greis, M. Watters, and J. Welle, "Cybersecurity legislation: Preparing for increased reporting and transparency. McKinsey and Company", 17 June 2022. Available online:

https://www.mckinsey.com/capabilities/risk-and-resilience/ourinsights/cybersecurity/cybersecurity-legislation-preparing-for-increased-reporting-and-transparency

[7] P. Chithaluru, A.T. Fadi, M. Kumar and T. Stephan, "Computational Intelligence Inspired Adaptive Opportunistic Clustering Approach for Industrial IoT Networks." *IEEE Internet of Things Journal*, 2023.

[8] A.T. Fadi and D. B. David, "Seamless authentication: For IoT-big data technologies in smart industrial application systems," *IEEE Transactions on Industrial Informatics*, 2020.

[9] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," *Information Sciences*, vol. 479, pp. 567-592, 2019.

[10] Q. Liu, B. Gong, and Z. Ning, "Research on clpkc-idpkc cross-domain identity authentication for IoT environment," *Computer Communications*, 2020.

[11] S. Mousavi, A. Mosavi , and A.R. Varkonyi-Koczy,"A Load Balancing Algorithm for Resource Allocation in Cloud Computing," Recent Advances in Technology Research and Education. INTER-ACADEMIA 2017. *Advances in Intelligent Systems and Computing*, 2017, vol 660. pp. 289-296.

[12] A. Gueye, and V. Marbukh, “A game-theoretic framework for network security vulnerability assessment and mitigation.” In Proceedings of the International Conference on Decision and Game Theory for Security, Budapest, Hungary, Springer International Publishing AG: Cham, Switzerland, pp. 186–200, 5–6 November 2012.

[13] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu,” A survey of game theory as applied to network security.” In Proceedings of the 43rd International Conference on System Sciences (HICSS), USA, pp. 1-10, 5-8 January 2010.

[14] G. Asharov, R. Canetti, and C. Hazay, “Towards a game theoretic view of secure computation.” In Proceedings of Advances in Cryptology (EUROCRYPT), pp 426–445, 2011.

[15] L. Huang, J. Chen, and Q. Zhu, “ A large-scale markov game approach to dynamic protection of interdependent infrastructure networks.” In International Conference on Decision and Game Theory for Security, Springer, pp. 357–376, 2017.

[16] T. Denning, T. Kohno, and H.M. Levy, “Computer Security and the Modern Home”, Comm. of the ACM, Vol. 56, No. 1, pp. 94-103, 2013.

[17] 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.

[18] M. Aamir, and M. Arif, “Study and performance evaluation on recent DDoS trends of attack & defense,” Int. J. Inf. Technol. Comput. Sci. Inf. Technol. Comput. Sci. 05 (08), pp 54–65, 2013.

[19] R. Williams, E. McMahon, S. Samtani, M. Patton, and H. Chen, “Identifying vulnerabilities of consumer Internet of things (IoT) devices: A scalable approach,” IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 179-181, 2017.

[20] A. Arena, P. Perazzo, C. Vallati, G. Dini, and G. Anastasi, “Evaluating and improving the scalability of RPL security in the internet of things,” *Computer Communications*, vol. 151, pp. 119-132, 2020.

[21] S.T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against Distributed Denial of Service (DDoS) flooding attacks," IEEE Commun. Surv. Tutor. 15 (4), 2046–2069, (2013).

[22] X. Bellekens, A. Seeam, K. Nieradzinska, C. Tachtatzis, A. Cleary, R. Atkinson, and I. Antonovich, "Cyber-Physical-Security Model for Safety-Critical IoT Infrastructures." Wireless World Research Forum Meeting 35 (WWRF35), Copenhagen, Denmark, 2015.

[23] A. A. Gendreau and M. Moorman, "A survey: Intrusion detection system for the Internet of Things," *Int. J. Comput. Sci. Eng.*, vol. 5, no. 2, pp. 2278–9960, 2016.

[24] F. Yazdankhah, and A. L. Honarvar," An intelligent Security Approach using Game theory to Detect Dos Attacks in IoT", *International Journal of Advanced computer science and application,* volume 8, No. 9, January 2017.

[25] H. Wu and W. Wang, "A Game Theory Based Collaborative Security Detection Method for Internet of Things Systems," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 6, pp. 1432-1445, June 2018.

[26] P. Pirozmand, M. A. Ghafary, S. Siadat, and J. Ren, "Intrusion Detection into Cloud-Fog-Based IoT Networks using game theory", Hinduwa Wireless Communications and Mobile Computing, volume 2020, Article ID 8819545, 16 November 2020.

[27] S. Nobahary, H. G. Garakani, A. Khademzadeh, and A.M. Rahmani, "Selfish node detection based on hierarchical game theory in IoT", *EARASIP Journal on wireless communications and networking*, volume 255, 2019.

[28] K. Wang, M. Du, D. Yang, C. Zhu, J. Shen, and Y. Zhang, "Game theory-based

active defense for intrusion detection in cyber-physical embedded systems", ACM Trans. Embed. Comput. Syst. 16, 1, Article 18, 21 pages, October 2016.

[29] G. Nychis, V. Sekar, D.G. Andersen, and H. Zhang, "An empirical evaluation of entropy-based traffic anomaly detection", In Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement Conference, pp 151, 2008.

[30] S.T. Ali, V. Sivaraman, and A. Jha, “A survey of securing networks using software defined networking”, IEEE Trans. Reliab. 64(3), 1086-1097, 2015.

[31] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, and V. Maglaris, “Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments”, Computer Network 62, 122-136, 2014.

[32] C. Dillon, and M. Berkelaar, “OpenFlow(D) DoS Mitigation”, Technical Report, February 2014.

[33] T. Chin, X. Mountrouidou, X. Li, and K. Xiong, “Selective packet inspection to detect Dos flooding using software defined networking (SDN)”, IEEE 35th International Conference on distributed Computing Systems Workshops (ICDCSW), pp. 95-99, 2015.

[34] C. J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang,” NICE: Network Intrusion Detection and countermeasure”, IEEE Trans. Dependable Secure Computer 198-211, 2013.

[35] S. Lim, J. Ha, H. Kim, Y. Kim, and S. Yang, “A SDN-oriented DDos blocking scheme for botnet-based attacks”, Sixth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 63-68, 2014.

[36] T. Xing, D. Huang, L. Xu, C.J. Chung, and P. Khatkar,” Snort-Flow: a OpenFlow-based intrusion prevention system in cloud environment”, In Proceedings 2nd GENI Research and Educational Experiment Workshop, pp.89-92, 2013.

[37] A. F. M. Piedrahita, S. Rueda, D. M. F. Mattos, and O.C.M.B Duarte,” Flow Fence: a denial-of-service defense system for software defined networking”, Global Information Infrastructure and Networking Symposium (GIIS), Guadalajara, pp.1-6, 2015.

[38] M. Nobakht, V. Sivaraman, and R. Boreli,” A Host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow”, publication 311771106, August 2016.

[39] S. S. Bhunai, and M. Gurusamy,” Dynamic Attack Detection and Mitigation in IoT using SDN”, 27th International Telecommunication Networks and Applications Conference (ITNAC), 2017.

[40] N. Ravi, and S. M. Shalinie," Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture", IEEE Internet of Things Journal, volume 7, No. 4, April 2020.

[41] Y. Yilmaz, and S. Uludag," Timely detection and mitigation of IoT-based cyberattacks in the smart grid", Jornal of the frankline Institute, March 2019.

[42] J. Abegunde, H. Xiao, and J. Spring, "A smart game for data transmission and energy consumption on the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 528–543, Jan. 2020.

[43] J. Antoniou, "Game Theory, the Internet of Things and 5G Networks". Cham, Switzerland:Springer, 2019.

[44] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, "Resource trading in blockchain-based Industrial Internet of Things," *IEEE Trans. Ind. Informat.,* vol. 15, no. 6, pp. 3602–3609, Jun. 2019.

[45] H. Zhang, Y. Xiao, S. Bu, D. Niyato, F. R. Yu, and Z. Han, "Computing resource allocation in three-tier IoT fog networks: A joint optimization approach combining stackelberg game and matching," *IEEE Internet Things J.,* vol. 4, no. 5, pp. 1204–1215, Oct. 2017.

[46] H. S. Mansouri and V. W. S. Wong, "Hierarchical fog-cloud computing for IoT systems: A computation offloading game," *IEEE Internet Things J.,* vol. 5, no. 4, pp. 3246–3257, Aug. 2018.

[47] R. Fantacci and B. Picano, "A matching game with discard policy for virtual machines placement in hybrid cloud-edge architecture for industrial IoT systems," *IEEE Trans. Ind. Informat*., vol. 16, no. 11, pp. 7046–7055, Nov. 2020.

[48] H. Gao, Y. Xiao, H. Yan, Y. Tian, D. Wang, and W. Wang, "A learning-based credible participant recruitment strategy for mobile crowd sensing," *IEEE Internet Things J.,* vol. 7, no. 6, pp. 5302–5314, Jun. 2020.

[49] L. P. Gao, T. Jin, and C. Lu, "A long-term quality perception incentive strategy for crowdsourcing environments with budget constraints," *Int. J. Cooperative Inf. Syst.,* vol. 29, no. 1, pp. 901–914, 2020.

[50] H. Sedjelmaci, S. M. Senouci, and T. Taleb, "An accurate security game for low-resource IoT devices," *IEEE Trans. Veh. Technol.,* vol. 66, no. 10, pp. 9381–9393, Oct. 2017.

[51] F. Guo, "Game Theory". Wuhan, China: Wuhan Univ. Press, 2019.

[52] B. Li and Y. Wang, "Game Theory and Information Economics". Beijing, China: Sci. Press, 2016.

[53] L. Militano, M. Nitti, L. Atzori, and A. Iera, "Using a distributed Shapley-value based approach to ensure navigability in a social network of smart objects," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., 2015, pp. 692–697.

[54] T. F. Rahman, V. Pilloni, and L. Atzori, "Application task allocation in cognitive iot: A reward-driven game theoretical approach," *IEEE Trans. Wireless Commun.,* vol. 18, no. 12, pp. 5571–5583, Dec. 2019.

[55] M. S. Abdalzaher and O. Muta, "A game-theoretic approach for enhancing security and data trustworthiness in iot applications," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 11250–11261, Nov. 2020.

[56] B. Li and Y. Wang, "Game Theory, and Information Economics." Beijing, China: Sci. Press, 2016.

[57] Y. Zhou,M. Kantarcioglu, and B. Xi, "A survey of game theoretic approach for adversarial machine learning," *WIREs Data Mining and Knowledge Discovery*, vol. 9, no. 3, p. e1259, 2019.

[58] D. He, S. Chan and M. Guizan, "Cyber security analysis and protection of wireless sensor networks for smart grid monitoring,: in *IEEE Wireless communications*, vol.24, no. 6, pp. 98-103, Dec. 2017.

[59] Y. A. Qadri, A. Musaddiq, D. W. Kim, and S. W. Kim, "An overview of selection forwarding and wormhole attacks in healthcare IoT." In: Asia Pacific Conference on Information Communication Technology (APCICT-2018), Daegu, Korea, 2018.

[60] M. R. K. Naik, P. Samundiswary,"Wireless body area network security issues-survey," International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), India, pp. 190-194, 2016.

[61] P. Gasti, and G. Tsudik,"Content-Centric and Named-Data Network Security: The Good, The Bad and The Rest," IEEE International Symposium on Local and Metropolitan Area Networks, Wasington DC, USA, 2018.

[62] D. Kasthurirathna, H. Nguyen, M. Piraveenan, and S. Uddin, U. Senanayake,"Optimisation of strategy placements for public good in complex networks." Proceedings of the International Conference on Social Computing. ACM, p1, 2014.

[63] J. Pawlick, E. Colbert, and Q. Zhu, "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy," *ACM Computing Surveys (CSUR)*, vol. 52, no. 4, pp. 1–28, 2019.

[64] D. Kasthurirathna, M. Piraveenan, and S. Uddin, "Evolutionary stable strategies in networked games: the influence of topology." *Journal of Artificial Intelligence and Soft Computing Research* 5, 83–95, 2015.

[65] K. Binmore, "Playing for real: a text on game theory." Oxford university press, 2007.

[66] J. Chen, C.. Touati, and Q. Zhu,"A dynamic game analysis and design of infrastructure network protection and recovery." ACM SIGMETRICS Performance Evaluation Review 45, 2 , 128, 2017.

[67] M. S. Abdalzaher and O. Muta, "A game-theoretic approach for enhancing security and data trustworthiness in iot applications," IEEE Internet Things J., vol. 7, no. 11, pp. 11250–11261, Nov. 2020.

[68] S. Yan, M. Peng, and X. Cao, "A game theory approach for joint access selection and resource allocation in UAV assisted iot communication networks ," IEEE Internet Things J., vol. 6, no. 2, pp. 1663–1674, Apr. 2019.

[69] T. F. Rahman, V. Pilloni, and L. Atzori, "Application task allocation in cognitive iot: A reward-driven game theoretical approach," IEEE Trans. Wireless Commun., vol. 18, no. 12, pp. 5571–5583, Dec. 2019.

[70] J. Karande, and S. Joshi, "DEDA: An algorithm for early detection of topology attacks in the internet of things," *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 11, No. 2, pp. 1761~1770, April 2021.

[71] L.N Giang , D. Braulio ,N. Quoc-Dung ,V. L Hai-Viet , and N. N Tu , "A collaborative approach to early detection of IoT Botnet," *Computers & Electrical Engineering,* Volume 97, 2022.

[72] H. V Le, and Q. D Ngo, "V-Sandbox for dynamic analysis IoT botnet." *IEEE Access* 2020;8:145768–86.

[73] C. Chi, Y. Wang, X. Tong, M. Siddula and Z. Cai, "Game Theory in Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 9, no. 14, pp. 12125-12146, 15 July15, 2022.

[74] C. Ponsard, V. Ramon and M. Touzani, "Improving Cyber Security Risk Assessment by Combined Use of i* and Infrastructure Models." In the 14th International iStar Workshop ,pp. 63-69, 2021.

[75] E. Brynjolfsson, D. Rock, C. Syverson, "Artificial intelligence and the modern productivity paradox: A clash of expectations and statistics." National Bureau of Economic Research, Cambridge, MA, 2017.