electronics

Article

Predicting the Impact of Distributed Denial of Service (DDoS) Attacks in Long-Term Evolution for Machine (LTE-M) Networks Using a Continuous-Time Markov Chain (CTMC) Model

Mohammed Hammood Mutar [1], Ahmad Hani El Fawal [2,3,*], Abbass Nasser [2,4] and Ali Mansour [2]

[1] Center for Research in Applied Mathematics and Statistics (CRAMS), Beirut 1107, Lebanon
[2] Lab-STICC, UMR 6285—CNRS, ENSTA Bretagne, 29806 Brest, France; abbass.nasser@ieee.org (A.N.); mansour@ieee.org (A.M.)
[3] Computer Science Department, Modern University for Business and Science, Damour 5660, Lebanon
[4] Business Computing Department, UBS, Holy-Spirit University of Kalsik (USEK), Jounieh 1200, Lebanon
[*] Correspondence: elfawal@ieee.org

Abstract: The way we connect with the physical world has completely changed because of the advancement of the Internet of Things (IoT). However, there are several difficulties associated with this change. A significant advancement has been the emergence of intelligent machines that are able to gather data for analysis and decision-making. In terms of IoT security, we are seeing a sharp increase in hacker activities worldwide. Botnets are more common now in many countries, and such attacks are very difficult to counter. In this context, Distributed Denial of Service (DDoS) attacks pose a significant threat to the availability and integrity of online services. In this paper, we developed a predictive model called Markov Detection and Prediction (MDP) using a Continuous-Time Markov Chain (CTMC) to identify and preemptively mitigate DDoS attacks. The MDP model helps in studying, analyzing, and predicting DDoS attacks in Long-Term Evolution for Machine (LTE-M) networks and IoT environments. The results show that using our MDP model, the system is able to differentiate between Authentic, Suspicious, and Malicious traffic. Additionally, we are able to predict the system behavior when facing different DDoS attacks.

Keywords: IoT; LTE-M; DDoS; M2M; CTMC; Markov chain; Botnets

check for updates

Citation: Mutar, M.H.; El Fawal, A.H.; Nasser, A.; Mansour, A. Predicting the Impact of Distributed Denial of Service (DDoS) Attacks in Long-Term Evolution for Machine (LTE-M) Networks Using a Continuous-Time Markov Chain (CTMC) Model. *Electronics* **2024**, *13*, 4145. https://doi.org/10.3390/electronics13214145

Academic Editors: Irfan Awan, Amna Qureshi and Muhammad Shahwaiz Afaqui

Received: 11 October 2024
Revised: 20 October 2024
Accepted: 21 October 2024
Published: 22 October 2024

1. Introduction

The Internet and its applications are constantly developing and are an essential element of every person's daily life. Due to this overwhelming need, research has expanded beyond just connecting computers to the Internet. Indeed, the Internet of Things (IoT) allows Machine-to-Machine (M2M) interactions to coexist with Human-to-Human (H2H) interactions over the same communication network. The IoT is a disruptive technology that has the potential to alter both the physical and digital aspects of our lives. This technology describes a specific kind of network that links M2M objects and gadgets to the Internet in order to facilitate information sharing and smart recognition [1]. The total number of IoT connections has grown from 6 billion in 2015 and is expected to reach 27 billion in 2025 [2]. GSMA Intelligence forecasts IoT connections to reach more than 38 billion by 2030, with the enterprise segment accounting for more than 60% of the total [3]. After a slowdown in enterprise progress caused by the pandemic and chip shortages, growth is returning to previous levels. In 2030, smart buildings and smart homes will be the largest verticals for IoT connections, while smart manufacturing is forecast to grow at a Compound Annual Growth Rate (CAGR) of 20% between 2023 and 2030 [3].

Long-Term Evolution for Machines (LTE-M) is a type of cellular network specifically designed for IoT and M2M devices with a limited bandwidth of 1.4 MHz. M2M devices transmit compact data packets at varying intervals.

However, these devices differ from traditional Human-to-Human (H2H) communications in terms of their distinctiveness and functionality. M2M devices transmit their data payloads in synchronized bursts, creating a phenomenon like coordinated storms [4].

The synchronization behavior described above has led to various issues, particularly in light of the increasing prevalence of M2M devices. These issues encompass network saturation, access baring, resource depletion, and the inefficient utilization of the bandwidth. Consequently, these challenges have prompted extensive research efforts within the academic community to develop potential solutions. In addition to natural and human-induced catastrophes such as tsunamis, acts of terrorism, and wars, there is a significant challenge posed by the simultaneous transmission of alerts from various devices. This situation has a detrimental impact on both H2H and M2M communication traffic.

Distributed Denial of Service (DDoS) attacks have been one of the security gaps that most threaten services, applications, and information access. According to Forbes [5], there are about 1.09 billion websites on the Internet in 2024 [6].

In an attempt to stay undetected while carrying out attacks, the attacker precisely mimics the actions of users. The Malicious user divides their attack methods according to rate, admission pattern, etc., in order to initiate a HTTP-GET flood DDoS attack. The detection of HTTP-GET flood DDoS attacks has gained more attention because of a number of important issues and difficulties that have emerged from recent study. Working near conflicting HTTP-GET flood DDoS attacks presents a number of difficulties that are either unresolved or only partially handled [7]. DDoS assaults are organized, dispersed, and remotely managed networks that employ deployed computers, sometimes known as bots, to deliver a massive volume of synchronous, continuous requests to the target server. The frequency, intensity, and sophistication of DDoS attacks are all rising.

In order to conduct different DDoS attacks, malicious users are continuously changing their experience, modifying their tactics, and utilizing cutting edge technologies. Even though there are a number of ways to identify, stop, or lessen DDoS attacks, malicious people may always come up with new ways to get around existing defenses [8]. DDoS attacks continue to rank among the network's greatest dangers. DDoS attacks against Internet servers' application layers have increased recently, costing their targets huge amounts of money [9]. Attacks at the TCP/IP layer limit the number of requests per second and overwhelm the online server. These include DDoS attacks, zero-day attacks, and slowloris attacks that exploit vulnerabilities in Windows or Apache [10].

Only a limited number of DDoS incidents at the application layer are captured by the solutions provided to comprehend DDoS attacks at the TCP/IP layer. The formula for the resolutions that identify all kinds of application-layer assaults is extremely complex. The lack of landscapes to detect DDoS attacks is one set of challenges in detecting a DDoS out-break at the TCP/IP layer [11]. All web servers are vulnerable to HTTP-GET DDoS assaults since bots can mimic people and make it hard to distinguish harmful queries from legitimate ones. DDoS attacks are increasingly targeting businesses worldwide, regardless of their size or industry.

As more systems are admitted, vulnerabilities remain unpatched, and the impact on business grows, the complexity and intensity of these attacks are growing rapidly [12]. The cyber realm is significantly impacted by DDoS attacks. Due to IP overflow, bandwidth spoofing, high memory usage, and root sane or mouse damage, cyberattacks are anticipated to interfere with organizations' normal operations [13]. With its traffic, a slow-moving DDoS assault can simulate actual traffic. Avoiding detection by existing systems is easy. Rank correlation algorithms can identify important distinctions between legitimate and attack traffic based on their rank values [14].

Information servers, Internet servers, and cloud computing servers are all severely impacted by DoS attacks [15]. Among the most common threats are Botnets, DDoSs, hacking, malware, pharming, phishing, ransomware, spam, spoofing, and spyware [16].

IBM CEO Ginni Rometty claims that a cyberattack poses the greatest threat to any or all companies globally. As a result, cybercriminals are on the rise [14]. Malicious people compromise client servers using a variety of techniques. It is difficult to detect DDoS attacks since they are quite diverse and happen in between other cyberattacks.

Additionally, a diverse range of online applications have been integrated with various web services, encompassing domains such as e-commerce, online banking, online shopping, online education, e-healthcare, and Industrial Control Systems (ICSs) for critical infrastructure, among others [17]. Botnets are a set of devices infected by Malicious codes with the aim of overwhelming a certain website or service. Botnets refer to overlay networks that consist of compromised mobile devices owned by users. Botnets of this nature are managed by individuals known as Bot masters, who are cybercriminals responsible for the creation and dissemination of these Botnets. Email attachments are a prevalent method of infecting devices. These attachments are commonly associated with Trojan viruses. Once the machine is infected by the malware, it establishes a connection with a designated central server referred to as Command Control (CC), or alternatively, with a peer-to-peer network that constitutes the botnet [17]. Given the limited processing and memory resources for IoT devices, it becomes impossible for users to install anti-virus software on it. In addition, the large number of IoT devices makes it a desirable target for attackers to enslave IoT devices in their botnet Malicious networks [18].

Markov chains have lately been used to predict events. In fact, they have been successfully applied in a number of disciplines, including engineering, physics, meteorology, and medicine, to either prevent or mitigate the effects of disasters [19].

Markov chains are helpful for simulating complex scenarios and predicting the likelihood of future events. Markov chains have been used to predict a number of possible disasters, such as earthquakes, tsunamis, and even the spread of disease [20]. On this basis, we are motivated to use Markov chain as a statistical tool to model a DDoS attack and predict the behavior of the system before and during the attack by representing the impact of a DDoS attack with different states. Then, we represent the attack states with a linear system. By solving the linear system, we can show the probability of the system being in a certain state throughout the cycle of the attack.

The rest of the paper is organized as follows: In Section 2, we present a literature review that focuses on the impact of DDoS attacks on different networks. In Section 3, we give an overview about the impact of DDoS attacks on LTE-M networks. Section 4 introduces our Markov Detection and Prediction (MDP) model. In Section 5, we solve the linear system and we discuss and analyze our mathematical results. Finally, the conclusion and future works are provided in the Section 6.

2. Literature Review

Before delving into the core of the paper, let us review the proposed strategies and approaches regarding DDoS attacks in terms of prediction, detection, or mitigation.

To anticipate DDoS attacks, Liu et al. [21] utilized two machine learning models: Support Vector Machine (SVM) and Random Forest (RF). Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE), two techniques for reducing the number of dimensions, are tested during the preparation of the data. The performance of models is assessed using the mean cross-validation accuracy. In the same study, they discovered that the performance of SVM is more accurate and stable than that of Logistic Regression (LR). In [22], Abaid et al. proposed an approach that focused on the anticipation of future attacks, with the objective of offering timely alerts to network administrators. This proactive strategy has enabled administrators to promptly implement containment measures or isolate affected hosts. The approach used by these researchers is founded upon the utilization of a Markov chain model to represent the sequence of Botnet infections. The primary aim of this model is to discern patterns of behavior that are indicative of potential attacks.

The findings of the study indicated that this particular method exhibited considerable potential in generating timely alerts for detecting attacks. The accuracy rate for predicting attacks was found to be over 98%, while the maximum rate of false alarms was observed to be under 2%. Rahal et al. in [23] presented an innovative architectural framework that combines DDoS attack prediction with botnet identification. The architectural design was based on the principle that the sooner a system detects signs of an oncoming DDoS attack and identifies the related bots, the more efficiently it can respond to neutralize the attack. The prediction process entails recognizing early signs of a network assault before it escalates to more advanced phases. The performance evaluations employed the CTU-13 [24] and CAIDA (Center for Applied Internet Data Analysis) [25]. The evaluations effectively detected the existence of bots in the dataset, attaining an accuracy rate of 99.9%. Ismail et al. [26] developed a framework for classifying and predicting DDoS attacks using machine learning techniques. The framework involves selecting a dataset, choosing appropriate tools, pre-processing data, extracting features, encoding data, and dividing data into training and testing sets. The model undergoes optimization, including kernel scaling and hyper-parameter tuning, resulting in an average accuracy of 90%. Comparatively, the model's precision of defect identification improved to 85% and 79%, respectively. In [27], Alasmary et al. introduced ShieldRNN, a novel methodology for training and prediction in Recurrent Neural Networks/Long Short-Term Memory models, to protect IoT devices from attacks. Their solution consists of an IoT node detector and a server detector. The researchers evaluated ShieldRNN on the CIC-IDS2017 dataset [28] and established benchmark outcomes for identifying DDoS attacks on the CIC-IoT2022 dataset [29]. Ettiane et al. in [30] proposed a cost-effective method for the real-time detection of M2M traffic using the Markov chain's recurrence property. They presented a DDoS attack targeting Machine Type Communication (MTC) devices, aiming to congest fourth-generation (4G)/5G networks. The 3rd-Generation Partnership Project (3GPP) traffic Markov-based modeling demonstrated the impact of these attacks on mobile network elements, highlighting their detrimental effects on signaling load. The proposed detection framework can detect active intrusions in around 380 s with a 91% detection accuracy. In [31], Javaheri et al. provided a comprehensive analysis of DDoS attacks and their impact on cyber security. They presented a hierarchical framework and analyzed studies in academic journals. They discussed strategies to improve intrusion detection systems and emphasize different types of intrusion detection systems. The authors explained the core principles of cyber security, including DDoS attacks, data anomalies, and intrusion detection. They also highlighted the introduction of fuzzy logic solutions to address DDoS attacks. The survey's findings offered benefits for businesses and governments seeking business sustainability. Hameed et al. in [32] proposed a security system consisting of two parts. In the first part, the authors explained how to compromise the network by infecting some IoT devices, and through them, the infection can be spread to the entire network. Second, the authors provided a set of methods that includes filtration, abnormal traffic created by IoT device identification, screening, and publishing the abnormal traffic patterns to the other home routers on the network. The proposed system blocks the connection received from Malicious nodes for a certain period of time without causing any delay for normal traffic.

Al-Naeem et al. in [33] evaluated the effectiveness of DDoS detection through multiple experimental scenarios. They analyzed traffic flow in transmission sessions, including regular and retransmission scenarios. The study's main contribution was its ability to predict DDoS attacks by analyzing transmission behavior variability. Sensor nodes can transmit signals simultaneously, and the study used a tablet computer as the primary communication hub. The optimal transmission interval is 23 milliseconds. The study highlighted the correlation between transmission session saturation and DDoS attack success.

Based on the previous literature review, and by analyzing a diverse range of sources, this section has highlighted the evolution of concepts, methodologies, and key findings for the use of predictive tools to analyze the behavior of a network, especially in the IoT domain.

However, two questions arise: What are the impacts of a DDoS attack over M2M traffic? Are LTE-M networks resilient toward this type of attack? To answer these questions, we study, hereinafter, the impact of DDoS attacks on LTE-M networks.

3. DDoS Attacks' Impact on LTE-M

LTE-M is a standardized technology launched in the 13th release by the 3GPP organization to enhance the performance of Low-Power Wide-Area Networks (LPWANs). The objective of M2M communication is to achieve cost-effectiveness, energy efficiency, simplicity, and broad geographical reach [34]. LTE-M networks are limited in terms of bandwidth networks to 1.4 Mbps. In September 2016, a spree of massive DDoS attacks temporarily crippled the Krebs organization to enhance the performance of LPWAN. The initial attack exceeded 600 Gbps in volume, and it was among the largest ones [35]. Additionally, on 26 April 2017, Persirai Botnet [36] was discovered on 64% of the IP cameras Trend Micro was monitoring, which is more than twice as many as Mirai [37]. Now, with an LTE-M limited bandwidth along with a huge attack speed, can LTE-M networks scale to afford the huge amount of data generated by DDoS attacks? To answer this question, we study and evaluate the LTE-M data-rate.

In order to explore the bandwidths and constraints of Long-Term Evolution–Advanced (LTE-A is a 4G standard) and LTE-M, we analyze the time-frequency resources and their relationship with data rates for M2M communication. In LTE, time-frequency resources are subdivided, as shown in Figure 1.

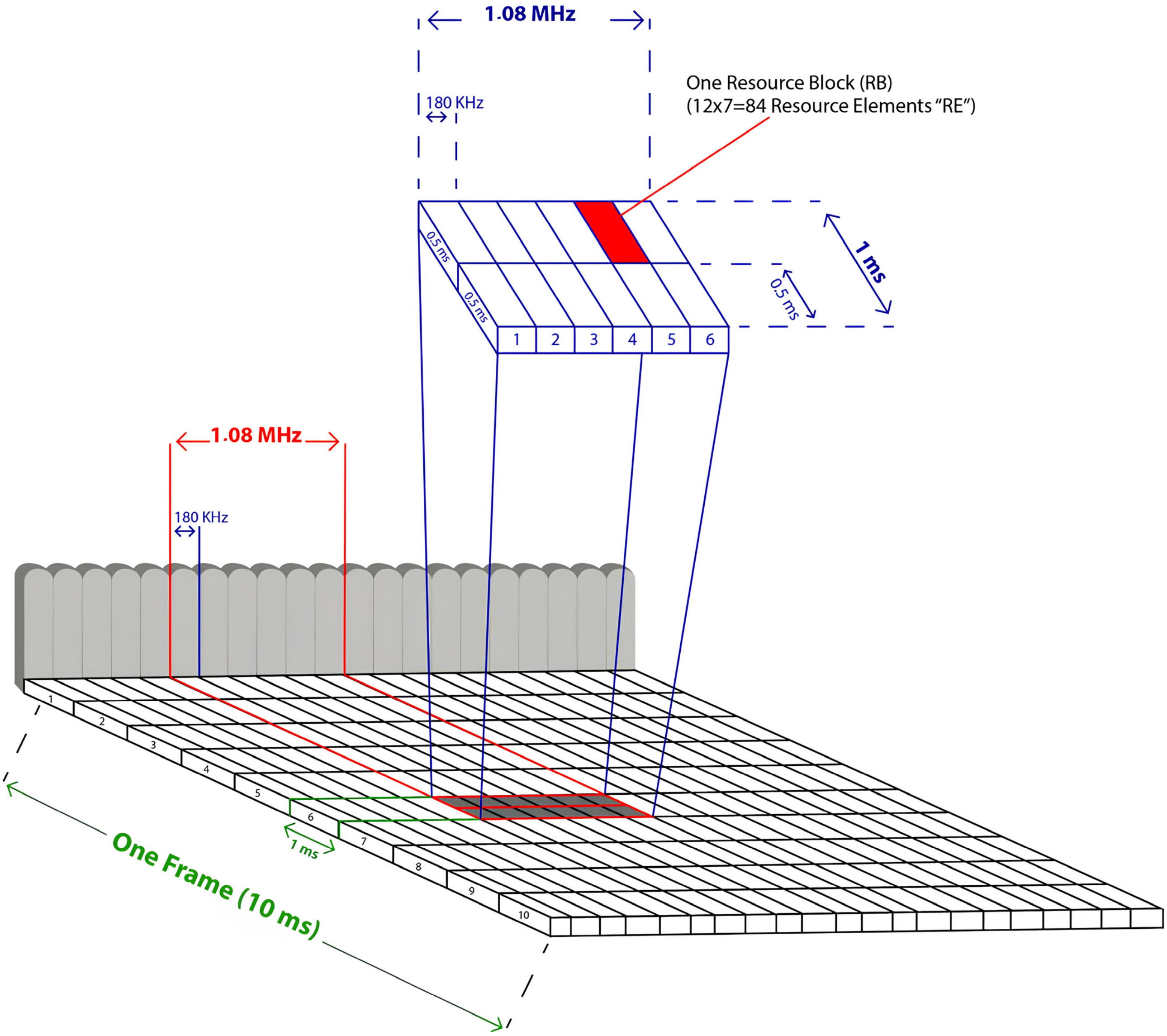

Figure 1. Limited bandwidth of LTE-M carrier in LTE-A carrier with a Resource Element (RE) and Resource Block (RB).

In LTE, the most significant temporal unit is the radio frame with a duration of 10 milliseconds (ms). This radio frame is further divided into ten equal sub-frames. Each sub-frame consists of two slots, and each slot has a duration of 0.5 ms. Each time slot consists of seven Orthogonal Frequency Division Multiple Access (OFDMA) symbols [4].

- A Resource Element (RE) refers to a narrow channel with a spacing of 15 KHz in frequency domain and 0.5/7 ms in the time domain.
- A Resource Block (RB) consists of 15 KHz × 12 sub-carriers = 180 KHz in frequency domain and 0.5 ms in the time domain.
- A Physical Resource Block (PRB) is the smallest allocation block that could be assigned to a single User Equipment (UE) for scheduling purposes. It consists of 15 KHz × 12 sub-carriers = 180 KHz in frequency domain and 0.5 ms × 2 = 1 ms in the time domain.

A basic mathematical computation is employed:

$$(6\text{ RB} \times 2 \times 12\text{ Sub-carriers} \times 7\text{ OFDMA symbol} \times 2\text{ bits per RE})/1000 \approx 2\text{ Mbps}.$$

Since there are separate channels designated for upload and download in the LTE-M network due to its half-duplex nature, the bandwidth is determined to be 1 Mbps for the upload stream and 1 Mbps for the download stream.

Finally, to recall, LTE-M uses limited bandwidth (1.4 MHz) with a low data rate of 1 Mbps, and it is expected that DDoS attacks will flood the network with huge data (for example, the Krebs attack speed is about 600 Gbps). So, it is expected that LTE-M networks will be overloaded in a split second when facing a DDoS attack.

If we know that DDoS attacks can target any type of network or device that is connected to the Internet, including LTE-M networks, many research questions might arise regarding the impact of DDOS attacks on LTE-M networks:

- How may we detect and predict the occurrence of DDoS attacks?
- How can we analyze the behavior of the network during a DDoS attack?
- What are the impacts of a DDoS attack on M2M traffic?

4. Markov Detection and Prediction (MDP) Model

In the rapidly evolving landscape of technology, IoT has emerged as a pivotal factor, revolutionizing the way we gather, transmit, and process data. IoT devices have become ubiquitous, seamlessly integrating into our lives and environments, allowing us to remotely monitor and control various systems. One of the fundamental aspects of IoT is the transmission of data, which is achieved through a diverse network of technologies such as LTE-M, NB-IoT, EC-GSM, LoRa, and Sigfox.

Markov Chain is a probabilistic model that characterizes a series of potential occurrences, where the likelihood of each event is solely determined by the state achieved in the preceding event. One approach to represent a system is modeling the system, wherein the system is characterized by its states and transitions. These transitions are determined by the probabilities associated with transitioning between two states.

4.1. Authentic, Suspicious and Malicious Requests

With the huge data generated by IoT devices, effective classification is essential to extract meaningful insights and facilitate predictive analysis. To streamline this process, a classification framework is proposed, categorizing IoT generated-data into three distinct types of requests:

1. Authentic requests refer to accurate, reliable, and trustworthy information that has not been manipulated, fabricated, or altered in any way. This type of data reflects the true state of actions without bias or distortion for example a sensor that sends 8 messages per day.
2. Suspicious requests refer to the type of information that raises doubts about its accuracy, reliability, or legitimacy due to inconsistencies, anomalies, or unusual patterns.

It may indicate potential errors, manipulation, or deceptive practices for example a sensor that exceeds its normal data-rate by sending more than eight messages per day.

3. Malicious requests refer to intentionally crafted or manipulated information designed with harmful intent, with the aim of causing damage, compromising security, or deceiving individuals or systems (e.g., a hacker trying to delete some data or a sensor that sends massive data while exceeding a certain threshold).

The three types (Authentic, Suspicious, and Malicious) of requests are shown in Figure 2.

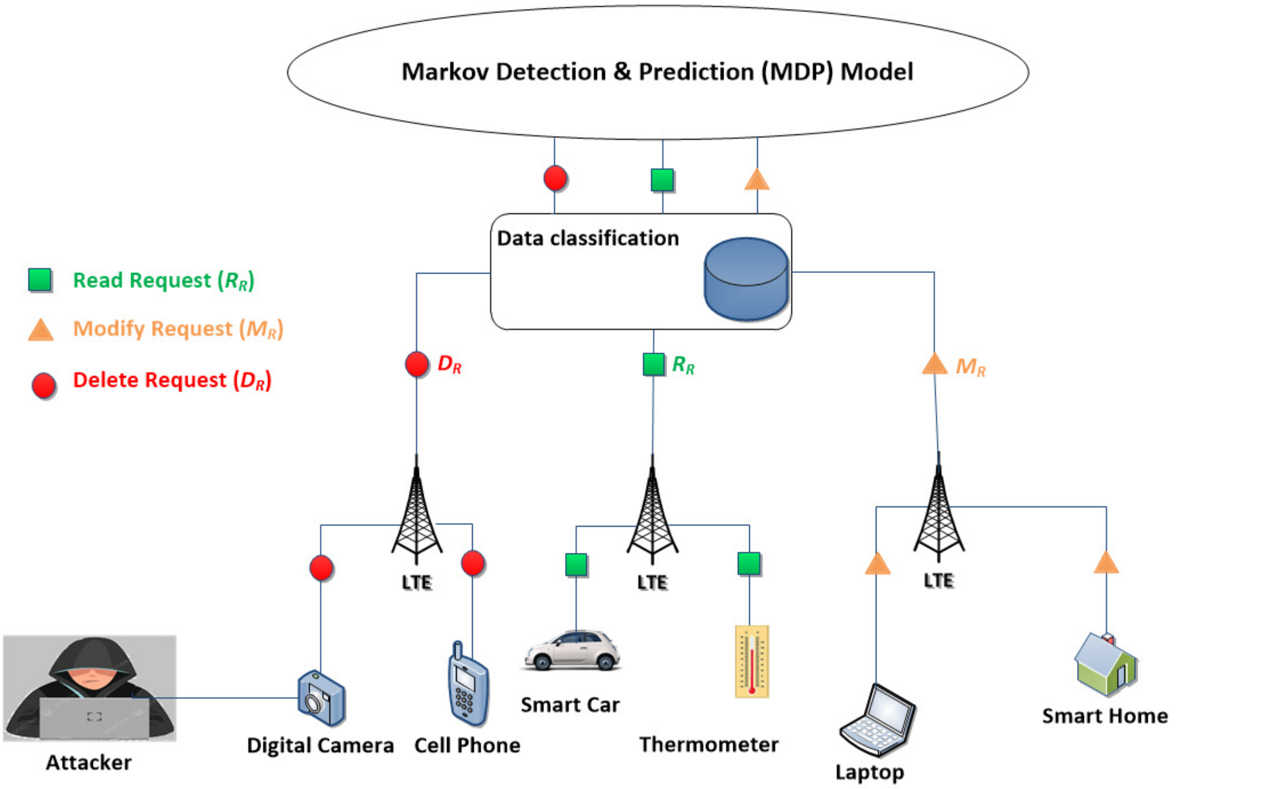

Figure 2. Authentic, Suspicious, and Malicious requests.

The MDP flowchart depicted in Figure 3 shows the system behavior when it receives Authentic, Suspicious, or Malicious requests.

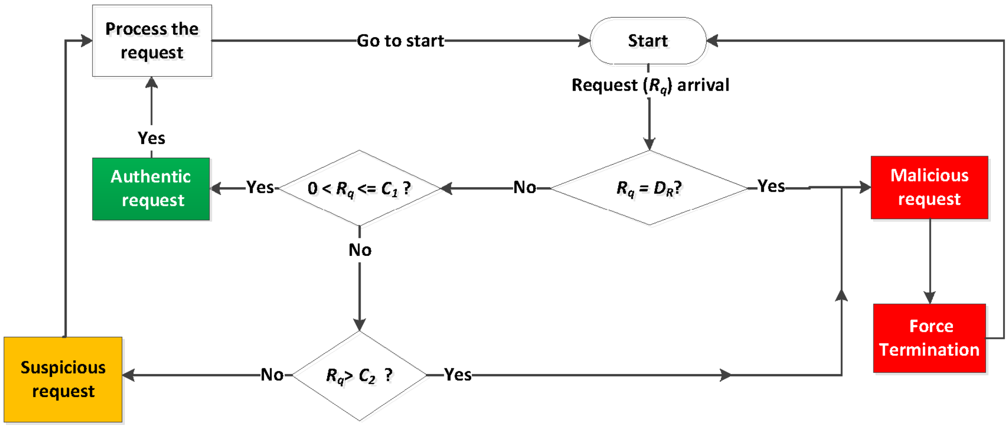

Figure 3. MDP flow chart upon the arrival of Authentic, Suspicious, or Malicious requests. Where "C_1" is the threshold of the Authentic phase, "C_2" is the threshold of the Suspicious phase, and "D_R" is the number of ongoing Malicious Delete Requests.

4.2. MDP Model

The MDP model is designed to proactively identify and mitigate DDoS attacks within LTE-M networks in an IoT environment. In an era where IoT connectivity plays an essential role, the MDP model emerges as a vital safeguard, leveraging advanced predictive analytics to detect and preemptively thwart Malicious activities. This model promises to enhance the security and reliability of LTE-M networks, ensuring uninterrupted IoT operations and safeguarding critical data and services against the ever-evolving security threat landscape. In this section, we introduce the MDP model, exploring its architecture, functionality, and real-world applications.

The proposed MDP system delves into the intriguing realm of data transmission through IoT devices and communication towers, while proposing a comprehensive classification framework that aids in detecting the DDoS attacks and predicting the system's behavior. The MDP system involves three steps:

- Defining states using Markov chains.
- Generating equilibrium equations.
- Solving the linear system.

4.2.1. Defining States Using Markov Chains

A state refers to the likelihood of a system being in a particular state, which can be estimated using data-based models, sensor technology, or machine learning techniques [38].

The MDP involves three steps; therefore, in the first step, we use the Markov chain to define the sequence of possible events for different requests (Authentic, Suspicious, and Malicious requests) by turning any possible incident into different states and probabilities that identify this incident.

The MDP model is designed to support M2M traffic. The MDP model is characterized by the following properties:

- State Space: The set of all possible states that the system could resides in. Actually, the system might be in one of the following four phases:
  - Initial phase ($i = j = 0$).
  - Authentic phase ($0 < i + j \leq C_1$).
  - Suspicious phase ($C_1 < i + j \leq C_2$).
  - Malicious phase ($C_2 < i + j$) or ($D_R \geq 1$).
- Transition Probabilities: For each pair of states, there is a probability of transitioning from one state to another in one time step.
- Balance equations, also known as the equilibrium equations or steady-state equations. These equations are based on the principle that the inflow of probabilities into a state is equal to the outflow of probabilities from that state in the steady-state. In other words, the probabilities do not accumulate or deplete over time in equilibrium states.

In an MDP model, any request is classified by its nature and categorized in one of the three types:

- Read Request (R_R) denoted by the variable (i).
- Modify Request (M_R) denoted by the variable (j).
- Delete Request (D_R) denoted by ($D_R \geq 1$).

The two traffic streams R_R and M_R are characterized by two average arrival rates (λ_i, λ_j), respectively, which are assumed to conform to a Poisson distribution. Meanwhile, the two service rates (μ_i, μ_j) are assumed to follow an exponential distribution.

The transition between states in the system is possible upon the occurrence of an event (increase or decrease of i or j). The Initial phase represents the start of our system ($i = j = 0$), while the Authentic phase represents the normal cycle of our system ($0 < i + j \leq C_1$), where C_1 is the threshold of Authentic phase. As for the Suspicious phase, it represents doubtful requests where ($C_1 < i + j \leq C_2$), where C_2 is the threshold of Suspicious phase. Finally, in the Malicious phase, there is a clear evidence of harmful intents or actions (e.g., delete requests ($D_R \geq 1$) or a huge and unusual traffic that exceeds the threshold C_2 ($C_2 < i + j$), as shown in Figure 4.

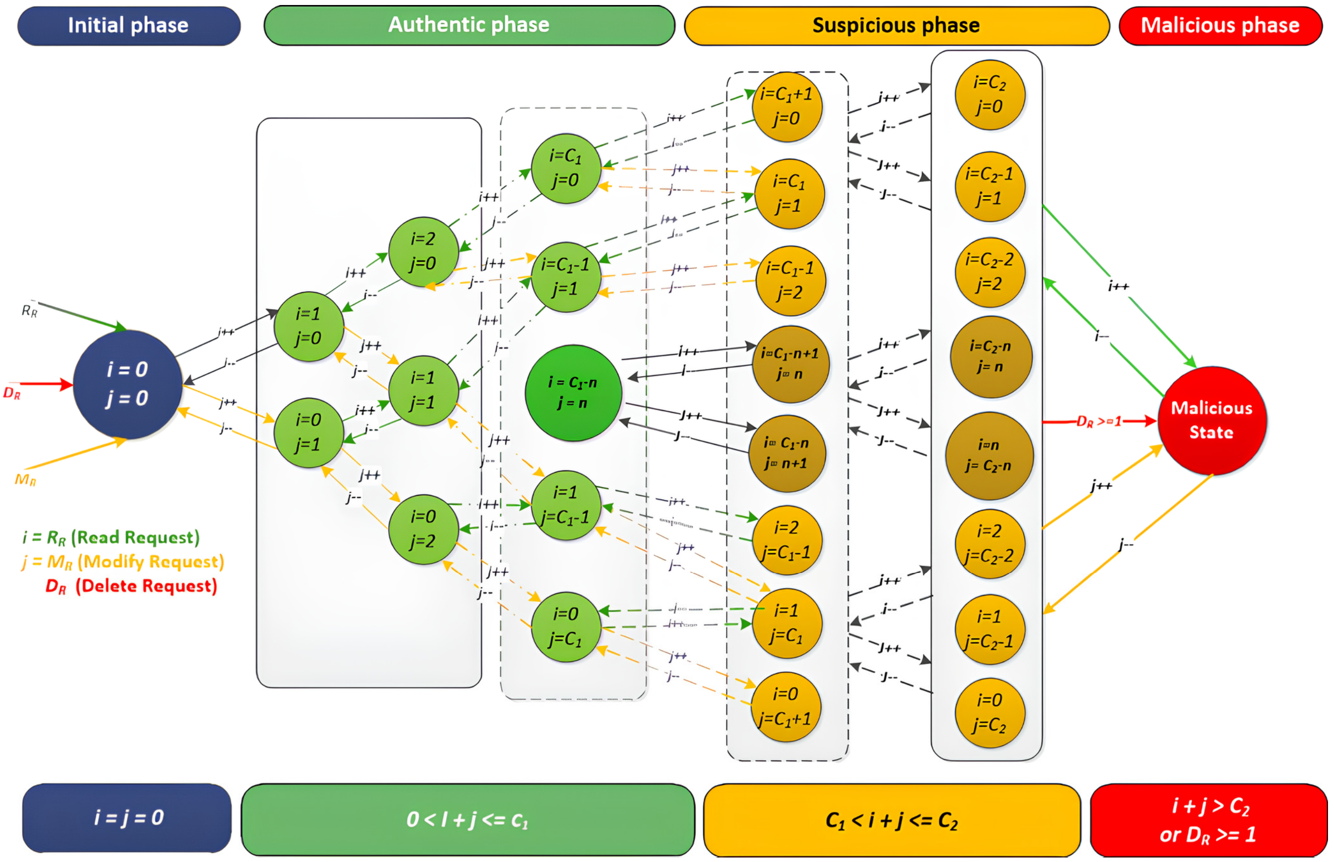

Figure 4. Representation of the MDP model as a set of generic states, where "i" represents the number of ongoing services for Read Request (R_R), "j" is the number of ongoing services for Modify Requests (M_R), "C_1" is the threshold of the Authentic phase, "C_2" is the threshold of suspicious phase, and "D_R" is the number of ongoing Malicious Delete Requests.

Assuming that $C_1 = 2$ and $C_2 = 3$, Figure 5 illustrates the MDP model with four phases: Initial, Authentic, Suspicious, and Malicious.

4.2.2. Generating the Equilibrium Equations

Since we have many notations in the following equations, we summarize them in Table 1.

Table 1. Symbols, values, and descriptions.

Symbol	Description
C_1	The threshold of the Authentic phase
C_2	The threshold of the Suspicious phase
i	number of ongoing services for the Read Request (R_R)
j	number of ongoing services for the Modify Request (M_R)
λ_i	average arrival rate for R_R (i++)
λ_j	average arrival rate for M_R (j++)
μ_i	completed service rate for R_R ($i--$)
μ_j	completed service rate for M_R ($j--$)
S(i,j)	The state with certain i and j requests
$\pi_{(i,j)}$	Steady-state probability
Π	Steady-state probability vector
D_R	number of ongoing Malicious for Delete Request (D_R)

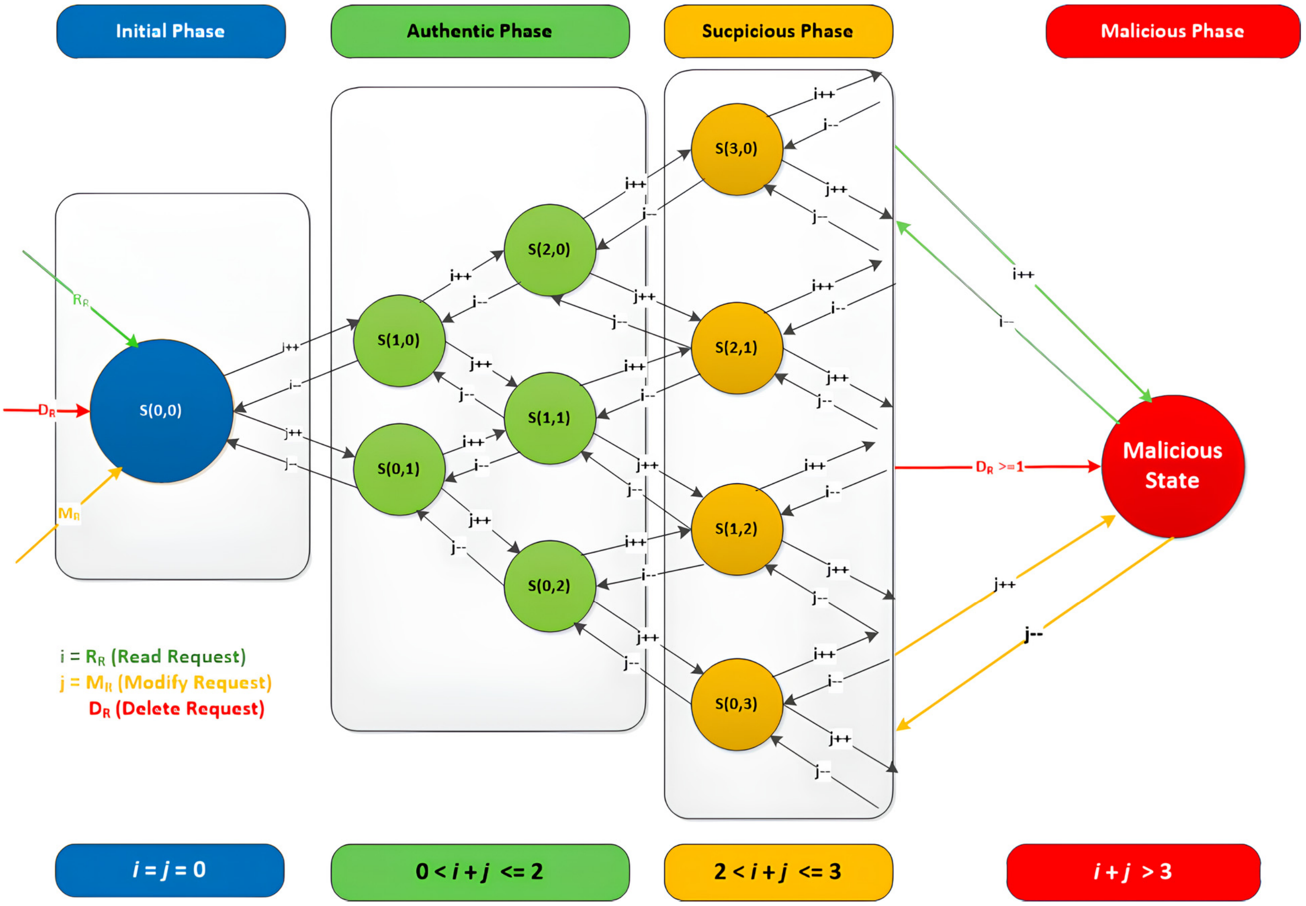

Figure 5. Representation of the MDP model as a set of states ($C_1 = 2$ and $C_2 = 3$), where "S(*i*,*j*)" is the state with certain *i* and *j* requests, "*i*" represents the number of ongoing services for Read Requests (R_R), "*j*" is the number of ongoing services for Modify Requests (M_R), "$C_1 = 2$" is the threshold of the Authentic phase, "$C_2 = 3$" is the threshold of the suspicious phase, and "D_R" is the number of ongoing Malicious Delete Requests.

We will generate the equilibrium equations by considering new arrival events with an arrival rate "λ" and a service rate "μ".

In this paper, we assume that the time intervals for observation are sufficiently brief so that only one transition ($i{+}{+}$, $i{-}{-}$, $j{+}{+}$, $j{-}{-}$) may occur during each period.

Based on this assumption, the system might fall into one of the following four phases:

(1) Initial phase, where $i = j = 0$ includes one state S(0,0), as shown in Figure 6.

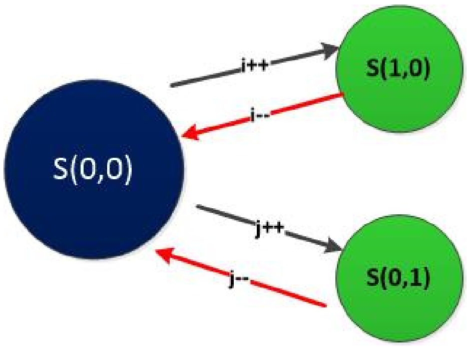

Figure 6. Transitioning from S(0,0) in the "Initial phase" to different states in the "Authentic phase"; "S(*i*,*j*)" represents different states, where "*i*" is the number of ongoing services for Read Requests (R_R) and "*j*" is the number of ongoing services for Modify Requests (M_R).

S(0,0) can be represented with the following equilibrium equation:

$$(\lambda_i + \lambda_j)\pi_{(0,0)} = \mu_i\pi_{(1,0)} + \mu_j\pi_{(0,1)} \tag{1}$$

(2) Authentic phase, where $0 < i + j \leq C_1$, as show in Figure 7:

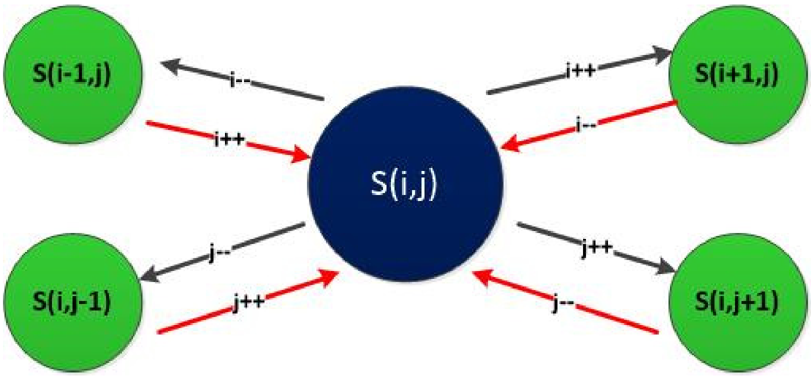

Figure 7. Transitioning from the "Authentic phase" to the "Initial phase" or the "Suspicious phase"; "S(*i*,*j*)" represents different states, where "*i*" is the number of ongoing services for Read Requests (R_R) and "*j*" is the number of ongoing services for Modify Requests (M_R).

This phase can be represented with the following equilibrium equation:

$$(\lambda_i + \lambda_j + \mu_i + \mu_j)\pi_{(i,j)} = \lambda_i\pi_{(i-1,j)} + \lambda_j\pi_{(i,j-1)} + \mu_i\pi_{(i+1,j)} + \mu_j\pi_{(i,j+1)} \tag{2}$$

(3) Suspicious phases, where $C_1 < i + j \leq C_2$, as show in Figure 7.

This phase can be represented with the equilibrium Equation (2).

(4) Malicious phase, where $C_2 < i + j$, as shown in Figure 8:

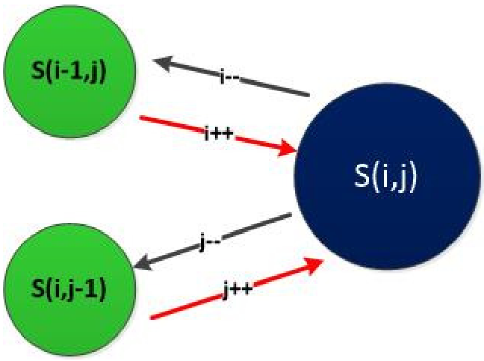

Figure 8. Transitioning from the "Malicious phase" to the "Suspicious phase"; "S(*i*,*j*)" represents different states, where "*i*" is the number of ongoing services for Read Requests (R_R) and "*j*" is the number of ongoing services for Modify Requests (M_R).

The Malicious phase can be represented with the following equilibrium equation:

$$(\mu_i + \mu_j)\pi_{(i,j)} = \lambda_i\pi_{(i-1,j)} + \lambda_j\pi_{(i,j-1)} \tag{3}$$

Assuming that $C_1 = 2$ and $C_2 = 3$, and based on the generic balance Equations (1)–(3), we can generate ten balance equations that rule ten states:

1. Balance Equation (1) for S(0,0) in the "Initial phase", where $i = j = 0$:

$$(\lambda_i + \lambda_j)\pi_{(0,0)} = \mu_i\pi_{(1,0)} + \mu_j\pi_{(0,1)} \tag{4}$$

2. Balance Equation (2) for S(1,0) in the "Authentic phase", where $0 < i + j \leq 2$:

$$\lambda_i \pi_{(0,0)} + (\lambda_i + \lambda_j)\pi_{(1,0)} = \mu_i \pi_{(2,0)} + \mu_j \pi_{(1,1)} + \mu_i \pi_{(1,0)} \quad (5)$$

3. Balance Equation (3) for S(0,1) in the "Authentic phase", where $0 < i + j \leq 2$:

$$\lambda_j \pi_{(0,0)} + (\lambda_i + \lambda_j)\pi_{(0,1)} = \mu_i \pi_{(1,1)} + \mu_j \pi_{(0,2)} + \mu_j \pi_{(0,1)} \quad (6)$$

4. Balance Equation(4) for S(2,0) in the "Authentic phase", where $0 < i + j \leq 2$:

$$\lambda_i \pi_{(1,0)} + (\lambda_i + \lambda_j)\pi_{(2,0)} = \mu_i \pi_{(2,0)} + \mu_i \pi_{(3,0)} + \mu_j \pi_{(2,1)} \quad (7)$$

5. Balance Equation(5) for S(0,2) in the "Authentic phase", where $0 < i + j \leq 2$:

$$\lambda_j \pi_{(0,1)} + (\lambda_i + \lambda_j)\pi_{(0,2)} = \mu_j \pi_{(0,2)} + \mu_i \pi_{(1,2)} + \mu_j \pi_{(0,3)} \quad (8)$$

6. Balance Equation (6) for S(1,1) in the "Authentic phase", where $0 < i + j \leq 2$:

$$\mu_i \pi_{(1,1)} + \mu_j \pi_{(1,1)} + (\lambda_i + \lambda_j)\pi_{(1,1)} = \mu_j \pi_{(1,2)} + \mu_i \pi_{(2,1)} + \lambda_j \pi_{(1,0)} + \lambda_i \pi_{(0,1)} \quad (9)$$

7. Balance Equation (7) for S(1,2) in the "Suspicious phase", where $2 < i + j \leq 3$:

$$\lambda_j \pi_{(1,1)} + \lambda_i \pi_{(0,2)} + (\lambda_i + \lambda_j)\pi_{(1,2)} = (\mu_i + \mu_j)\pi_{(1,2)} + \mu_i \pi_{(2,2)} + \mu_j \pi_{(1,3)} \quad (10)$$

8. Balance Equation (8) for S(2,1) in the "Suspicious Phase", where $2 < i + j \leq 3$:

$$\lambda_j \pi_{(2,0)} + \lambda_i \pi_{(1,1)\,+} (\lambda_i + \lambda_j)\pi_{(2,1)} = (\mu_i + \mu_j)\pi_{(2,1)} + \mu_i \pi_{(3,1)} + \mu_j \pi_{(2,2)} \quad (11)$$

9. Balance Equation (9) for S(0,3) in the "Suspicious Phase", where $2 < i + j \leq 3$:

$$\lambda_j \pi_{(0,2)} + (\lambda_i + \lambda_j)\pi_{(0,3)} = \mu_j \pi_{(0,3)} + \mu_i \pi_{(1,3)} + \mu_j \pi_{(0,4)} \quad (12)$$

10. Balance Equation (10) for S(3,0) in the "Suspicious Phase", where $2 < i + j \leq 3$:

$$\lambda_i \pi_{(2,0)} + (\lambda_i + \lambda_j)\pi_{(3,0)} = \mu_i \pi_{(3,0)} + \mu_i \pi_{(4,0)} + \mu_j \pi_{(3,1)} \quad (13)$$

4.2.3. Solving the Linear System

Based on the above equations with the variables $\pi_{(i,j)}$, we can build our linear system.

To recall, the system moves from one state to another, when a service is accomplished or a new request arrives (by increasing or decreasing *i* or *j*) with a steady-state probability $\pi_{(i,j)}$ that should respect the following two constraints:

$$\sum_{i=0}^{c} \sum_{j=0}^{c-i} \pi_{(i,j)} = 1 \quad (14)$$

$$0 \leq \pi_{(i,j)} \leq 1 \quad (15)$$

The ten equilibrium equations can be written in a matrix form, $\mathrm{A}\Pi = 0$, where the square matrix A represents the coefficients of a linear system, and Π represents the steady-state probability vector:

$$\Pi = \left(\pi_{(0,0)}\ \pi_{(1,0)}\ \pi_{(0,1)}\ \pi_{(1,1)}\ \pi_{(0,2)}\ \pi_{(2,0)}\ \pi_{(1,2)}\ \pi_{(2,1)}\ \pi_{(3,0)}\ \pi_{(0,3)}\right)^T \quad (16)$$

$$A\Pi = (0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0)^T \quad (17)$$

where A is a (10 × 10) rank-deficient matrix. By replacing the first row of the matrix A by the coefficients of (14), we obtain the following modified system:

$$B\Pi = (1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0)^T \tag{18}$$

where B becomes a full-rank (10 × 10) matrix.

5. Simulations, Results, and Discussions

In this section, we develop a simulation model and find an acceptable solution by solving a linear system [39]. The model is capable of generating several types of traffic, including R_R and M_R, with a high degree of flexibility. The findings obtained from the simulation are thoroughly examined and analyzed.

5.1. Normal-Cycle Scenario

This scenario represents the normal cycle (no attack is detected) in which the system receives low requests such as in rural areas.

We consider the following parameters:

- An LTE system with 3 PRB ($C = 3$).
- An average arrival rate of R_R (λ_1 = 1).
- An average arrival rate of M_R (λ_2 = 1).
- A service rate of R_R (μ_1 = 3).
- A service rate of M_R (μ_2 = 3).

The results of the normal cycle scenario are shown in Table 2:

Table 2. The probability values for each state S(*i*,*j*) in the normal cycle, where "S(*i*,*j*)" represents different states, π(*i*,*j*) is the Steady-state probability, "*i*" is the number of ongoing services for Read Requests (R_R), and "*j*" is the number of ongoing services for Modify Requests (M_R).

State	Steady-State Probability	Probability Value	Phase
S(0,0)	π(0,0)	162/314 = 51.6%	Initial
S(0,1)	π(0,1)	54/314 =17.2%	Authentic
S(0,2)	π(0,2)	9/314 = 2.86%	Authentic
S(0,3)	π(0,3)	1/314 = 0.3%	Suspicious
S(1,0)	π(1,0)	54/314 = 17.2%	Authentic
S(1,1)	π(1,1)	18/314 = 5.73%	Authentic
S(1,2)	π(1,2)	3/314 = 0.95%	Suspicious
S(2,0)	π(2,0)	9/314 = 2.86%	Authentic
S(2,1)	π(2,1)	3/314 = 0.95%	Suspicious
S(3,0)	π(3,0)	1/314 = 0.3%	Suspicious

In Figure 9, the results and percentages of different phases for the normal cycle scenario:

- Initial phase probability = $\pi_{(0,0)}$ = 52%.
- Authentic phase probability = $\pi_{(0,1)} + \pi_{(1,0)} + \pi_{(0,2)} + \pi_{(1,1)} + \pi_{(2,0)}$ = 45%.
- Suspicious phase probability = $\pi_{(0,3)} + \pi_{(1,2)} + \pi_{(2,1)} + \pi_{(3,0)}$ = 3%.

5.2. Suspicious Scenario

This scenario represents a high average arrival rate that might be either normal (e.g., dense areas) or Suspicious (e.g., the launching of an attack).

In this scenario,

- We keep using the same resources for the LTE system ($C = 3$).
- We increase the average arrival rate of R_R to be (λ_1 = 2).
- We also increase the average arrival rate of M_R to be (λ_2 = 2).
- We decrease the service rate of R_R to be (μ_1 = 2).
- We also decrease the service rate of M_R to be (μ_2 = 2).

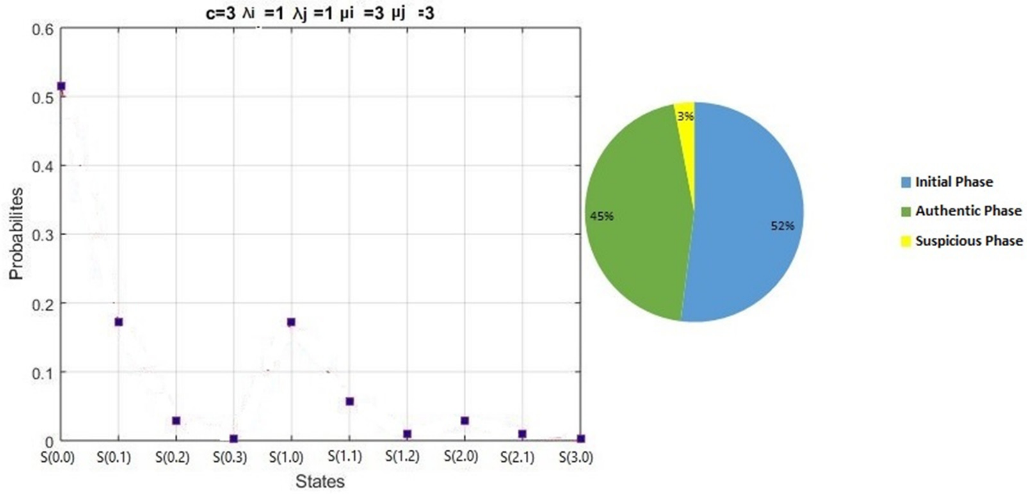

Figure 9. The probability values for each state S(i,j) in the normal cycle, where "S(i,j)" represents different states, $\pi(i,j)$ is the steady-state probability, "i" is the number of ongoing services for Read Requests (R_R), and "j" is the number of ongoing services for Modify Requests (M_R).

The results of the Suspicious scenario are shown in Table 3:

Table 3. The probability values for each state S(i,j) in the Suspicious scenario, where "S(i,j)" represents different states, $\pi(i,j)$ is the steady-state probability, "i" is the number of ongoing services for Read Requests (R_R), and "j" is the number of ongoing services for Modify Requests (M_R).

State	Steady-State Probability	Probability Value	Phase
S(0,0)	$\pi(0,0)$	6/38 = 15.78%	Initial
S(0,1)	$\pi(0,1)$	6/38 = 15.78%	Authentic
S(0,2)	$\pi(0,2)$	3/38 = 7.9%	Authentic
S(0,3)	$\pi(0,3)$	1/38 = 2.63%	Suspicious
S(1,0)	$\pi(1,0)$	6/38 = 15.78%	Authentic
S(1,1)	$\pi(1,1)$	6/38 = 15.78%	Authentic
S(1,2)	$\pi(1,2)$	3/38 = 7.9%	Suspicious
S(2,0)	$\pi(2,0)$	3/38 = 7.9%	Authentic
S(2,1)	$\pi(2,1)$	3/38 = 7.9%	Suspicious
S(3,0)	$\pi(3,0)$	1/38 = 2.63%	Suspicious

Figure 10 shows the results and percentages of different phases in the Suspicious scenario:

- Initial phase probability = $\pi_{(0,0)}$ = 16%.
- Authentic phase probability = $\pi_{(0,1)} + \pi_{(1,0)} + \pi_{(0,2)} + \pi_{(1,1)} + \pi_{(2,0)}$ = 63%.
- Suspicious phase probability = $\pi_{(0,3)} + \pi_{(1,2)}) + \pi_{(2,1)} + \pi_{(3,0)}$ = 21%.

5.3. *Attack Scenario*

In this scenario, we assume an excessive data rate is received as a result of an attack. In this scenario:

- We fix the resources used in the LTE system with 3 PRB ($C = 3$).
- We increase the average arrival rate of R_R to be (λ_1 = 3).
- We keep using the same average arrival rate of M_R (λ_2 = 2).
- We decrease the service rate of R_R to be (μ_1 = 1).
- In addition, we decrease the service rate of M_R to be (μ_2 = 1).

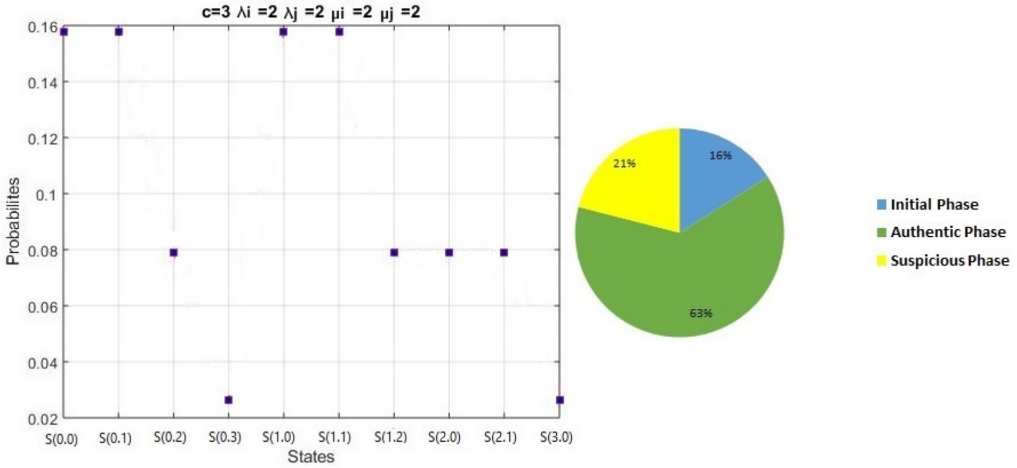

Figure 10. The probability values for each state S(*i*,*j*) in the Suspicious scenario, where "S(*i*,*j*)" represents different states, $\pi(i,j)$ is the steady-state probability, "*i*" is the number of ongoing services for Read Requests (R_R), and "*j*" is the number of ongoing services for Modify Requests (M_R).

The results of the attack scenario are shown in Table 4.

Table 4. The probability values for each state S(*i*,*j*) in the attack scenario, where "S(*i*,*j*)" represents different states, $\pi(i,j)$ is the steady-state probability, "*i*" is the number of ongoing services for Read Requests (R_R), and "*j*" is the number of ongoing services for Modify Requests (M_R).

State	Steady-State Probability	Probability Value	Phase
S(0,0)	$\pi(0,0)$	6/236 = 2.54%	Initial
S(0,1)	$\pi(0,1)$	12/236 = 5.08%	Authentic
S(0,2)	$\pi(0,2)$	12/236 = 5.08%	Authentic
S(0,3)	$\pi(0,3)$	8/236 = 3.4%	Suspicious
S(1,0)	$\pi(1,0)$	18/236 = 7.62%	Authentic
S(1,1)	$\pi(1,1)$	36/236 = 15.25%	Authentic
S(1,2)	$\pi(1,2)$	36/236 = 15.25%	Suspicious
S(2,0)	$\pi(2,0)$	27/236 = 11.44%	Authentic
S(2,1)	$\pi(2,1)$	54/236 = 22.88%	Suspicious
S(3,0)	$\pi(3,0)$	27/236 = 11.44%	Suspicious

Figure 11 shows the results and percentages of different phases the attack scenario.

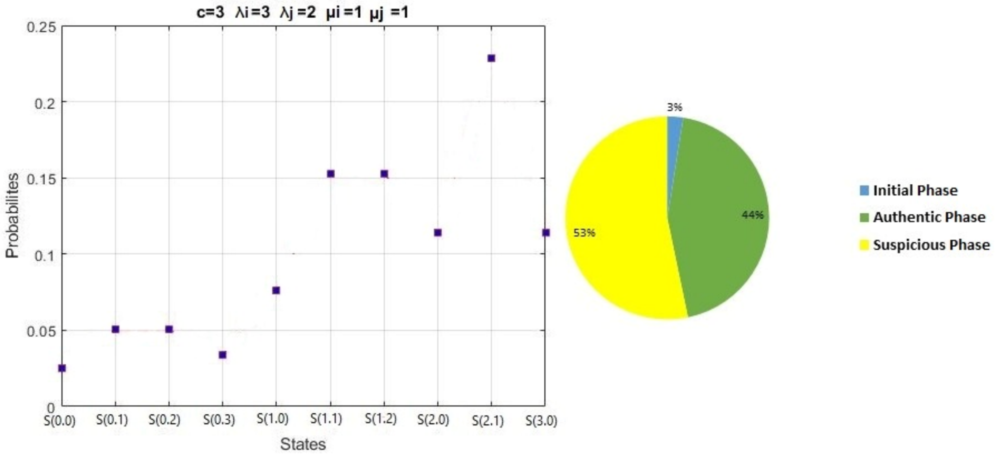

Figure 11. The probability values for each state S(*i*,*j*) in the attack scenario, where "S(*i*,*j*)" represents different states, $\pi(i,j)$ is the steady-state probability, "*i*" is the number of ongoing services for Read Requests (R_R), and "*j*" is the number of ongoing services for Modify Requests (M_R).

- Initial phase probability = $\pi_{(0,0)}$ = 3%.
- Authentic phase probability = $\pi_{(0,1)} + \pi_{(1,0)} + \pi_{(0,2)} + \pi_{(1,1)} + \pi_{(2,0)}$ = 44%.
- Suspicious phase probability = $\pi_{(0,3)} + \pi_{(1,2)} + \pi_{(2,1)} + \pi_{(3,0)}$ = 53%.

6. Conclusions

Our study starts with an approach analysis for the impact of DDoS attacks on LTE-M networks named the MDP model. A first congestion is expected on an LTE-M network due to the huge number of requests attempting to concurrently link to the network as a result of a DDoS attack, which eventually causes an overload issue. In this paper, a survey was provided for the main literature approaches to address this issue. In our work, we begin to research LTE-M network infrastructure and IoT devices' technological features in order to differentiate among Authentic, Suspicious, or Malicious requests. By modeling the system, we end up with promising results regarding the effect of DDoS attacks on M2M and the bottlenecks that occur due to these attacks on LTE-M networks. We realize that LTE-M networks can be affected by the increase in the number of Read, Modify, or Delete Requests. Under different scenarios, we analyze the data traffic and predict the system state to determine the behavior of the system and its probability of being under attack.

Our results show that in normal cycle, most of the time the system will stay in the initial phase with a probability of 52%. Meanwhile, the system will reside 63% in the Authentic phase during a Suspicious scenario. Moreover, during the attack scenario, a probability of 53% is calculated in the Suspicious phase.

In our future work, we INtend to study, analyze, and predict potential DDoS attacks or other attacks on H2H traffic and LTE-A networks. Additionally, we will develop our work to find a solution to mitigate the DDoS attack influence by filtering Malicious traffic, which helps in maintaining a good QoS for all traffic.

Author Contributions: Conceptualization, A.H.E.F., M.H.M. and A.M.; methodology, A.H.E.F., M.H.M. and A.M.; software, A.H.E.F. and M.H.M.; validation, A.H.E.F., M.H.M. and A.M.; formal analysis, A.H.E.F., M.H.M. and A.M.; investigation, A.H.E.F., M.H.M., A.N. and A.M.; resources, A.H.E.F. and M.H.M.; data curation, A.H.E.F., M.H.M., A.N. and A.M.; writing—original draft preparation, A.H.E.F. and M.H.M.; writing—review and editing, A.H.E.F., M.H.M., A.N. and A.M.; visualization, A.H.E.F., M.H.M., A.N. and A.M.; supervision, A.M.; project administration, A.M.; funding acquisition, A.H.E.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article in [39].

Conflicts of Interest: The authors declare no conflicts of interest.

List of Abbreviations

3GPP	3rd Generation Partnership Project
4G	Fourth Generation
CAIDA	Center for Applied Internet Data Analysis
CC	Command Control
CIC	Canadian Institute for Cybersecurity
DDoS	Distributed Denial of Service
H2H	Human-to-Human
ICS	Industrial Control Systems
IoT	Internet of Things
LPWAN	Low Power Wide Area Networks
LR	Logistic Regression
LTE-A	Long-Term Evolution-Advanced
LTE-M	Long-Term Evolution for Machines
M2M	Machine-to-Machine
MDP	Markov Detection and Prediction

MTC	Machine Type Communications
OFDMA	Orthogonal Frequency Division Multiple Access
PCA	Principal Component Analysis
PRB	Physical Resource Block
RB	Resource Block
RE	Resource Element
RF	Random Forest
RFE	Recursive Feature Elimination
SVM	Support Vector Machine
UE	User Equipment

References

1. Pourrahmani, H.; Yavarinasab, A. The applications of internet of things in the automotive industry: A review of the batteries, fuel cells, and Engines. *Internet Things* **2022**, *19*, 100579. [CrossRef]
2. IoT Business News. Global Internet of Things Market to Grow to 27 Billion Devices, Generating USD 3 Trillion Revenue in 2025. 2016. Available online: https://iotbusinessnews.com/2016/08/03/97077-global-internet-things-market-grow-27-billion-devices-generating-usd-3-trillion-revenue-2025/ (accessed on 19 October 2024).
3. Iji, M.; Gurung, R. IoT Connections Forecast to 2030. 2023. Available online: https://data.gsmaintelligence.com/research/research/research-2023/iot-connections-forecast-to-2030 (accessed on 19 October 2024).
4. El Fawal, A.H.; Mansour, A. LTE-M Adaptive eNodeB for Emergency Scenarios. In Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 18–20 October 2017.
5. Haan, K. Top Website Statistics for 2024. 2024. Available online: https://www.forbes.com/advisor/business/software/website-statistics/ (accessed on 19 October 2024).
6. Ahmed, S.; Khan, Z.A.; Mohsin, S.M.; Latif, S.; Aslam, S.; Mujlid, H.; Adil, M.; Najam, Z. Effective and Efficient DDoS Attack Detection Using Deep Learning Algorithm, Multi-Layer Perceptron. *J. Future Internet* **2023**, *15*, 76. [CrossRef]
7. Singh, K.; Singh, P.; Kumar, K. Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges. *Comput. Secur.* **2017**, *65*, 344–372. [CrossRef]
8. Behal, S.; Kumar, K. Characterization and Comparison of DDoS Attack Tools and Traffic Generators: A Review. *Int. J. Netw. Secur.* **2017**, *19*, 383–393.
9. Jiang, M.; Wang, C.; Lu, X.; Miu, M.; Chen, T. Characterizing the Impacts of Application Layer DDoS Attacks. In Proceedings of the 2017 IEEE International Conference on Web Services (ICWS), Honolulu, HI, USA, 25–30 June 2017; pp. 500–507.
10. Yusof, M.A.M.; Ali, F.H.M.; Darus, M.Y. Detection and Defense Algorithms of Different Types of DDoS Attacks. *Int. J. Eng. Technol.* **2017**, *9*, 410. [CrossRef]
11. Yadav, S.; Subramanian, S. Detection of Application Layer DDoSattack by feature learning using Stacked AutoEncoder. In Proceedings of the 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), New Delhi, India, 11–13 March 2016; pp. 361–366.
12. Stefanidis, K.; Serpanos, D.N. Countermeasures Against Distributed Denial of Service Attacks. In Proceedings of the 2005 IEEE Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Sofia, Bulgaria, 5–7 September 2005; pp. 439–442.
13. Bandara, K.R.W.V.; Abeysinghe, T.; Hijaz, A.; Darshana, D.G.T.; Aneez, H.; Kaluarachchi, S.J.; Sulochana, K.D.; DhishanDhammearatchi, M. Preventing DDoSAttack Using Data Mining Algorithms. *Int. J. Sci. Res. Publ.* **2016**, *6*, 390.
14. Ain, A.; Bhuyan, M.H.; Bhattacharyya, D.K.; Kalita, J.K. Rank Correlation for Low-Rate DDoS Attack Detection: An Empirical Evaluation. *Int. J. Netw. Secur.* **2016**, *18*, 474–480.
15. Devare, A.; Shelake, M.; Varsha, V.; Kamble, P.; Tamboli, B. A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis. *Int. Res. J. Eng. Technol.* **2016**, *3*, 1917–1923.
16. Haq, M.A.; Khan, M.A.R. DNNBoT: Deep neural network-based botnet detection and classification. *Comput. Mater. Contin.* **2022**, *71*, 1729–1750.
17. Zinno, S.; Di Stasi, G.; Avallone, S.; Ventre, G. A Load Balancing Algorithm against DDoS attacks in beyond 3G wireless networks. In Proceedings of the 2014 Euro Med Telco Conference (EMTC), Naples, Italy, 12–15 November 2014; pp. 1–6. [CrossRef]
18. Lee, S.H.; Shiue, Y.L.; Cheng, C.H.; Li, Y.H.; Huang, Y.F. Detection and Prevention of DDoS Attacks on the IoT. *Appl. Sci.* **2022**, *12*, 12407. [CrossRef]
19. Hongman, L. Research on Construction Cost Estimation of Highway Engineering Based on Markov Chain. *J. Liaoning Univ. Technol.* **2023**, *43*, 201–205.
20. Shao, H. Theory of Markov chain and its application in several representative examples. *Theor. Nat. Sci.* **2024**, *38*, 184–189. [CrossRef]
21. Liu, Z.; Qian, L.; Tang, S. The prediction of DDoS attack by machine learning, Proc. SPIE 12167. In Proceedings of the Third International Conference on Electronics and Communication; Network and Computer Technology (ECNCT2021), Harbin, China, 7 March 2022. [CrossRef]

22. Abaid, Z.; Sarkar, D.; Kaafar, M.; Jha, S. The Early Bird gets the botnet: A Markov chain based Early Warning System for botnet attacks. In Proceedings of the 2016 IEEE 41st Conference on Local Computer Networks (LCN), Dubai, United Arab Emirates, 7–10 November 2016; pp. 61–68. [CrossRef]
23. Rahal, B.M.; Santos, A.; Nogueira, M. A Distributed Architecture for DDoS Prediction and Bot Detection. *IEEE Access* **2020**, *8*, 159756–159772. [CrossRef]
24. Stratosphere Lab. The CTU-13 Dataset. A Labeled Dataset with Botnet. Normal and Background Traffic. 2011. Available online: https://www.stratosphereips.org/datasets-ctu13 (accessed on 19 October 2024).
25. CAIDA. Center for Applied Internet Data Analysis (CAIDA) Conducts Network Research and Builds Research Infrastructure to Support Large-Scale Data Collection, Curation, and Data Distribution to the Scientific Research Community. 2020. Available online: https://www.caida.org/about/ (accessed on 19 October 2024).
26. Ismail; Mohmand, M.I.; Hussain, H.; Ali Khan, A.; Ullah, U.; Zakarya, M. A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks. *IEEE Access* **2022**, *10*, 21443–21454. [CrossRef]
27. Alasmary, F.; Alraddadi, S.; Al-Ahmadi, S.; Al-Muhtadi, J. ShieldRNN: A Distributed Flow-Based DDoS Detection Solution for IoT Using Sequence Majority Voting. *IEEE Access* **2022**, *10*, 88263–88275. [CrossRef]
28. Canadian Institute for Cybersecurity. Intrusion Detection Evaluation Dataset (CIC-IDS2017). 2017. Available online: https://www.unb.ca/cic/datasets/ids-2017.html (accessed on 19 October 2024).
29. Canadian University of New Brunswick. CIC IoT Dataset 2022. Available online: https://www.unb.ca/cic/datasets/iotdataset-2022.html (accessed on 19 October 2024).
30. Ettiane, R.; Chaoub, A.; Elkouch, R. Robust detection of signaling DDoS threats for more secure machine type communications in next generation mobile networks. In Proceedings of the 2018 19th IEEE Mediterranean Electrotechnical Conference (MELECON), Marrakech, Morocco, 2–7 May 2018; pp. 62–67. [CrossRef]
31. Javaheri, D.; Gorgin, S.; Lee, J.; Masdari, M. Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, Overview, and future perspectives. *Inf. Sci.* **2023**, *626*, 315–338. [CrossRef]
32. Hameed, S.; Khan, F.I.; Hameed, B. Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. *J. Comput. Netw. Commun.* **2019**, *2019*, 9629381. [CrossRef]
33. Al-Naeem, M.A. Prediction of Re-Occurrences of Spoofed ACK Packets Sent to Deflate a Target Wireless Sensor Network Node by DDOS. *IEEE Access* **2021**, *9*, 87070–87078. [CrossRef]
34. Gartner. Machine-to-Machine (M2M) Communications. 2020. Available online: https://www.gartner.com/en/information-technology/glossary/machine-to-machine-m2m-communications (accessed on 19 October 2024).
35. Unit 42. New Mirai Variant Targeting Network Security Devices. 2021. Available online: https://unit42.paloaltonetworks.com/mirai-variant-iot-vulnerabilities (accessed on 19 October 2024).
36. Trend. Persirai: New IoT Botnet Targets IP Cameras. 2017. Available online: https://www.trendmicro.com/fr_fr/research/17/e/persirai-new-internet-things-iot-botnet-targets-ip-cameras.html (accessed on 19 October 2024).
37. University of Hawaii. The Persirai Botnet. 2017. Available online: https://westoahu.hawaii.edu/cyber/regional/gce-us-news/the-persirai-botnet (accessed on 19 October 2024).
38. Mourik, S.V.; Tol, R.V.D.; Linker, R.; Reyes-Lastiri, D.; Kootstra, G.; Koerkamp, P.G.; Henten, E.J.V. Introductory overview: Systems and control methods for operational management support in agricultural production systems. *Environ. Model. Softw.* **2021**, *139*, 105031. [CrossRef]
39. Github. Github Repository. Available online: https://github.com/H-Fawal/Modeling-Emergency-Traffic-using-a-Continuous-Time-Markov-Chain.git (accessed on 19 October 2024).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.