symmetry

MDPI

Article

Real-Time Intrusion Detection and Prevention System for 5G and beyond Software-Defined Networks

Razvan Bocu [1] and Maksim Iavich [2,*]

[1] Department of Mathematics and Computer Science, Transilvania University of Brasov, 500036 Brașov, Romania
[2] School of Technologies, Caucasus University, 0102 Tbilisi, Georgia
* Correspondence: miavich@cu.edu.ge; Tel.: +995-595511355

Abstract: The philosophy of the IoT world is becoming important for a projected, always-connected world. The 5G networks will significantly improve the value of 4G networks in the day-to-day world, making them fundamental to the next-generation IoT device networks. This article presents the current advances in the improvement of the standards, which simulate 5G networks. This article evaluates the experience that the authors gained when implementing Vodafone Romania 5G network services, illustrates the experience gained in context by analyzing relevant peer-to-peer work and used technologies, and outlines the relevant research areas and challenges that are likely to affect the design and implementation of large 5G data networks. This paper presents a machine learning-based real-time intrusion detection system with the corresponding intrusion prevention system. The convolutional neural network (CNN) is used to train the model. The system was evaluated in the context of the 5G data network. The smart intrusion detection system (IDS) takes the creation of software-defined networks into account. It uses models based on artificial intelligence. The system is capable to reveal not previously detected intrusions using software components based on machine learning, using the convolutional neural network. The intrusion prevention system (IPS) blocks the malicious traffic. This system was evaluated, and the results confirmed that it provides higher efficiencies compared to less overhead-like approaches, allowing for real-time deployment in 5G networks. The offered system can be used for symmetric and asymmetric communication scenarios.

Keywords: intrusion detection system; 5G security; networks; heterogeneous networks; real-time protection

Citation: Bocu, R.; Iavich, M. Real-Time Intrusion Detection and Prevention System for 5G and beyond Software-Defined Networks. *Symmetry* **2023**, *15*, 110. https://doi.org/10.3390/sym15010110

Academic Editors: Jeng-Shyang Pan and Debiao He

Received: 7 December 2022
Revised: 21 December 2022
Accepted: 27 December 2022
Published: 31 December 2022

1. Introduction

Nowadays, the global internet consists of billions of devices, the number of which is constantly growing. This trend is due to the increasing use of consumer electronics, where more and more sensors are installed every day. These devices have limited computing resources, and in most cases, information management is transferred to external devices. The latest devices, in turn, connect with each other and create communication channels to transmit time and status data. Existing 4G mobile networks cannot provide the necessary capabilities for the continued development of the networks of the Internet of Things. Therefore, we can immediately conclude that 5G networks should become the basis of the next generation of large-bandwidth data transmission networks.

Fifth-generation cellular networks forced the implementation of 5G and beyond networks, which offer capacity expansion strategies to handle great connectivity issues and can offer very high throughput and low-latency. 5G and beyond technology uses IoT, AI/ML, and blockchain, and its goal is to establish secure and reliable UAV networks. Therefore, the big work must be conducted to ensure security of 5G and beyond networks [1]. It can be very relevant to the integration of protected mechanisms, which use machine learning (ML) and artificial intelligence (AI) techniques. Scientists apply ML algorithms in the development of IDS systems in order to identify and classify malicious traffic [2]. It is

also important to identify the possible threats of 5G and beyond networks in real-time. The main problem with the research is that the security system must work very quickly, the processing delay should be very small, and in other cases, it is not efficient to use the system for real-time threats, identification, and classification.

The intrusion detection system, which is presented in this paper, addresses the stringent design, implementation, and deployment aspects of high-bandwidth 5G network cores. Thus, traditionally, the data traffic is filtered mostly using semiautomatic approaches. These usually generate low levels of data pattern detection accuracy, and they are not able to adapt and detect unknown data patterns. It is important to mention that the integrated intrusion detection system, which is presented in this paper, is one of the very few relevant systems that are proven to detect known and unknown threat patterns in a large 5G network core with high accuracy and without interfering with the low-latency levels of the implied data network, as they are perceived by the end users.

It is relevant to note that 5G networks create broad-bandwidth channels. However, the increased efficiency that these new networks create is largely due to the number of intelligent devices supported and the related applications. Broad-bandwidth data links: intelligent application deployments require data links capable of a minimum of 25 Mbps and are designed to sustain meaningful augmented reality (AR) and virtual reality (VR) and data containers [3]. Large scale and structurally flexible networks: This is defined by the network function virtualization (NFV) mechanism to create the networks needed. 5G IoT low-latency data networks are designed to sustain intelligent applications that need to transmit and receive data in real-time and use communication channels with delays of no more than five milliseconds [4]. Safety and fault tolerance: due to the presence of significantly fewer base stations in the 5G network, handoffs must be done when maintaining optimal coverage of the network. Data privacy and protection: applications that work with sensitive data, such as patient personal information, need mechanisms to prevent any unauthorized access attempts. Battery life: mobility is central to 5G data networks; hence, energy efficiency must be taken into account. Connectivity: 5G data networks must offer simultaneous, stable access to a huge number of devices, which means making the right design and implementation decisions. Mobility: This requirement supplements the need to create the right environment for the development of many devices that require reliable mobile data links. It must be noted that although smart devices that need to work on 5G networks must handle huge amounts of data, they do not, in most cases, have sufficient hardware resources to process the given data. Therefore, in most cases, information processing is transferred to systems in the cloud that extract useful information from unprocessed data by considering data analysis techniques [5,6].

The scientists discussed the security problems of 5G networks [7,8]. The following problems are identified: 1. As the 5G data network's architecture mainly uses software configurations, it has a much bigger exposure to attacks on the software. The attacks can be designed using existing security flaws or bugs. These attacks can influence the operation of 5G data networks. 2. The architecture of 5G data networks includes novel models and functions, because of this, they can be the target of hackers' attacks. The functions of key management for the networks and the base station can become the target of attacks. 3. The majority of 5G operators of mobile networks depend on suppliers; this fact can lead to additional attacks on 5G data networks. The impact of such attacks will also be greatly increased. 4. 5G data networks will include a huge amount of different smart devices. Therefore, attacks such as DOS and DDOS will become much more relevant and often. 5. The key feature of 5G network slicing can also be considered a security problem. The attackers can force the service to use the slice that was not intended for it.

It must be mentioned that the vulnerabilities of injecting malicious code into the system of 5G networks were also identified [9–11]. The contribution that is presented in this paper relates to the following perspectives.

- This article presents the current advances in the improvement of standards that simulate 5G networks through virtualized infrastructures. This determines a significant

improvement in the telecommunications operators' administrative and infrastructure maintenance costs.
- This paper presents the experience that the authors gained when deploying the described system on the core infrastructure of a major telecommunications operator.
- This paper outlines the relevant research areas and challenges that are likely to affect the efficient design and implementation of large 5G data networks, which use secure and economically efficient virtualized infrastructures.
- The performance evaluation of the system, which considered a comprehensive sample of real networking data, demonstrates that the system is capable of detecting unknown and existing malicious data traffic patterns in a timely manner with a high level of accuracy.
- To the best of our knowledge, this is one of the very few machine-learning-based intrusion detection systems that is compatible with the proper and timely detection of malicious data traffic patterns in large broadband 5G data networks.

The rest of this paper is organized according to the following structure.: First, the essential materials and methods are described. Following, the architecture of the intrusion detection system is described, and the fundamental algorithmic and implementational features are presented. Following this, the real-world performance of the implemented system is thoroughly assessed through a comprehensive case study. The last section presents the planned development directions. It also concludes the paper.

2. Materials and Methods

2.1. Basic Technologies

The subject of ongoing research is to determine the best architectural model for designing 5G data transmission networks. However, any architectural design must take into account two points of view [12,13]. Data perspective deals with real-time data analysis that uses software-based frontend data paths, while the management perspective deals with the suitable administration of the network components and the associated services that they define. It must be mentioned that the structure of a 5G data transmission network must take into account considerable technical requirements, such as scalability and the ability to virtualize network functions, when implementing network resources and providing necessary capabilities to virtualize network functions [14]. Therefore, comprehensive functional requirements must be accessible to support effective network management. This should include the effective setting of guidelines under which mobile devices will behave optimally, defining a policy to control access to network resources, and the ability to virtualize given physical network resources.

2.2. Virtualized Wireless Network Function

VWNF, the virtualized wireless network function, is the main function in the design and implementation of 5G data networks. It is effectively used to design 5G network's core (5GC). The process is able to logically define a self-sufficient 5G data network using NFV, network function virtualization. The basic technology of 5G is visualized on Figure 1. It is worth noting that the mentioned process is important from both a theoretical and a research point of view. In addition, it allows the deployment of dedicated 5G networks in certain infrastructures, such as telecommunications or cloud providers, which provide network services. We effectively worked with this system to realize particular network services in the 5G data network of the relative telecommunications service provider. Thus, during implementation, we noticed that the virtualized network environment has the necessary logical plasticity and scalability, which allowed us to effectively develop an intrusion detection system in real-time [15,16]. Network virtualization model is visualized in Figure 2. In fact, we have determined that virtualization engine provides the ability to properly handle data streams passing through the 5G network to detect potential or known threat patterns. Figure 1 describes the application of the virtualized networking mechanism. By means of design, realization, and deployment of a real-time intrusion detection system

(IDS), we demonstrated that this system is appropriate for the correct formation of the needed dedicated virtual data network, which by itself confirms the conclusions outlined in paper [17].

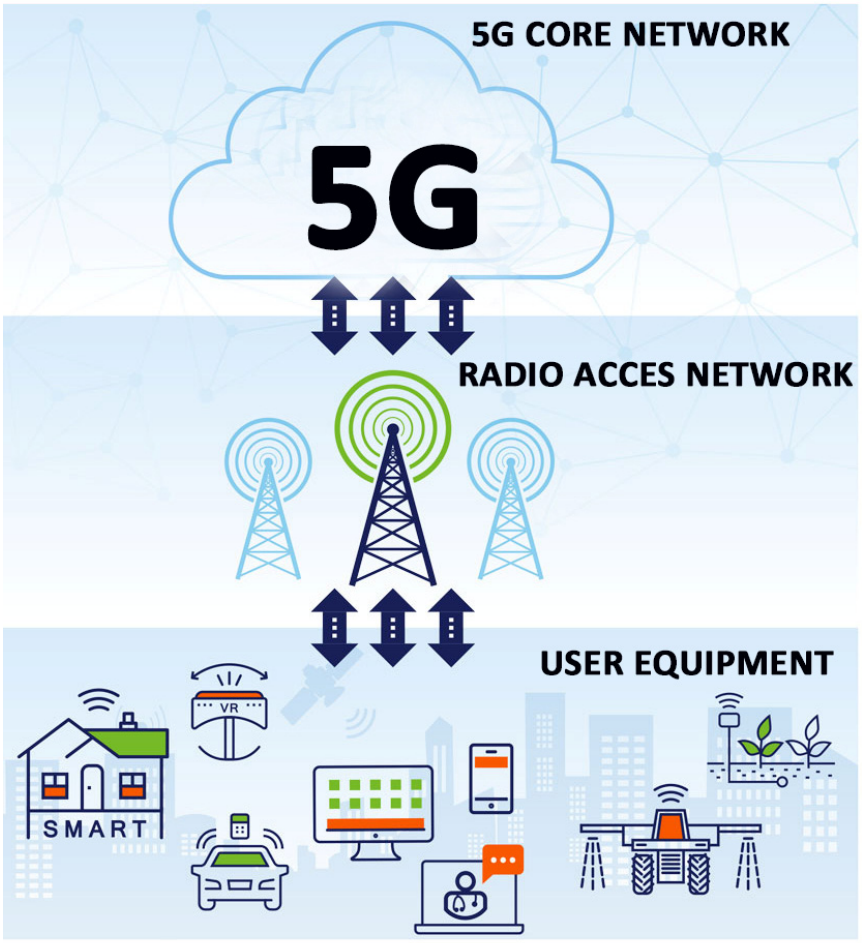

Figure 1. Basic technologies.

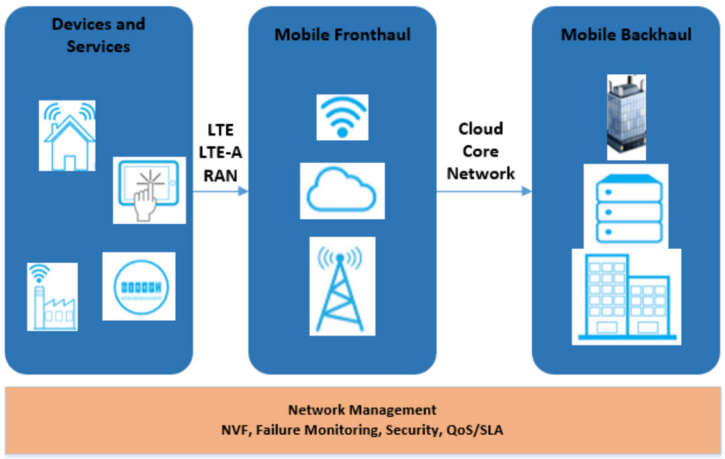

Figure 2. Partitioning a virtualized network.

In Figure 2, let us particularly note the mobile fronthaul and the mobile backhaul components. In its simplest form, the backhaul connects the mobile network to the wired network by backhauling traffic from geographically dispersed cell sites to mobile switching telephone offices (MTSOs). These links, which interconnect macro cell sites (e.g., sites

housing those large towers that you can easily see at great distances) to MTSOs, are quickly migrating from slower TDM-based T1/E1 connections towards packet-based Ethernet-over-fiber links, typically via 1Gbps+ physical interfaces to the macro cell site. Within a typical macro cell site resides a baseband unit (BBU) connected to a radio unit (RU). The former processer uses and controls data, while the latter generates radio signals transmitted over the airwaves via tower-mounted antennas.

Furthermore, the fronthaul is associated with a new and different type of radio access network (RAN) architecture consisting of centralized baseband controllers and standalone radio heads installed at remote cell sites located kilometers to tens of kilometers away. These BBU and RU functional blocks, as well as the equipment that performs these functions, are located further away from each other than in the mobile backhaul model.

In the fronthaul model, the RU equipment is now referred to as a remote radio head (RRH) but is still located at the cell site. The BBU is now located in a centralized, protected location where it serves multiple RRHs. The optical links that interconnect the newly centralized BBU and the multiple RRHs are referred to as *fronthaul*. In Figure 3, the logical features of this architecture are presented.

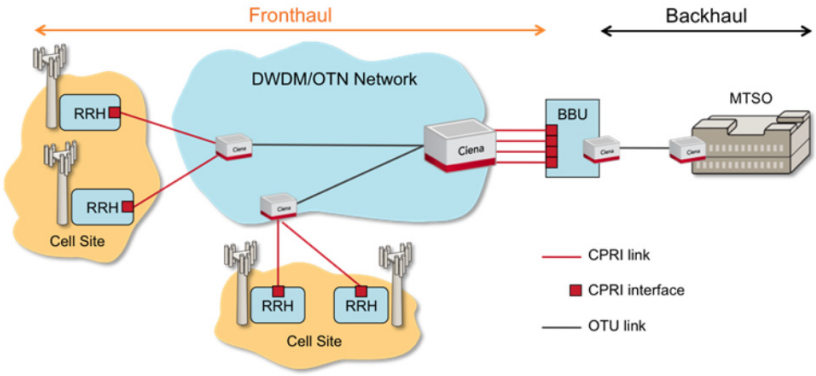

Figure 3. Logical architecture of the fronthaul and backhaul.

We also found that the 5G networks' logical characteristics optimize the distribution and use of radio resources, as we identified logical subnets that separately analyze data traffic through separate intrusion detection instances in real-time.

So, obtained results broadened and improved the work presented in [18]. Our test work shows that correctly defined 5G virtual networks can support applications that operate with huge amounts of data such as real-time IDSs.

3. Related Works

The succeeding paragraphs discuss some of the scientific works that are related to the heterogeneous networks that we have explored in our ongoing research process [19,20]. Thus, in articles [21,22], the problems of machine-to-machine communication (M2M) are analyzed. ETSI, the European Telecommunications Standards Institute, defines the protocols to be considered when using IoT devices that lack computing power [23,24]. Papers [25,26] provide guidelines for deploying machine-to-machine applications. The daily lives of people can potentially be influenced by machine-type communications, which allows us to consider heterogeneous networks as a reliable, technical option for the 5G IoT network implementation [27]. Machine-type communication is associated with an ever-increasing volume of transmitted data, and these problems are discussed in [28]. In addition, paper [29] described the corresponding quality of service (QoS) policies. The paper [30] suggests that a considerable number of 5G IoT devices can be deployed, which will provide certain services through their interactions and also ensure a proper balancing of data traffic. The contribution that is reported in [31] describes a system that actively handles data traffic generated by registered NB-IoT devices using the same ML-based intrusion detection engine. It is important to develop and deploy large 5G network topologies,

such as narrowband IoT (NB-IoT) and millimeter wave (mm wave) [32,33]. Scientists are working on the design of intrusion detection and prevention systems for 5G and beyond networks [34,35]. The authors of [36] offer to design the federated IDS architecture by means of federated learning for 5G networks. The authors of [37] offer a novel IDS for 5G networks to efficiently identify the attacks. The main problem with the offered works is that their designed IDS cannot work efficiently in real-time.

The heterogeneous networks (HNet) concept implies an additional paradigm that supports the design and realization of 5G logical networks in which services are hosted. We used this system to design a runtime that allows the IDS to correctly handle all data flaws in a 5G data network. It must be mentioned that this additional mechanism provides an opportunity to configure the virtualized network settings properly. Some data types are given priority during processing over others by defining appropriate QoS policies. This approach is unique and differs from the approaches offered in the related works.

The main advantage of our system is that it works in real-time, which is very important for the security of 5G and beyond networks. The integrated intrusion detection system, which is presented in this paper, relates favorably to similar existing contributions. Thus, the authors of papers [38,39] describe intrusion detection systems that ensure a fast processing of the data traffic that flows through the 5G network core; however, the detection accuracy is not satisfactory. Moreover, papers [40,41] present intrusion detection systems that generate a satisfactory level of detection accuracy, but they are not able to scale well for large real-world 5G data infrastructures. Furthermore, papers [42–44] propose relatively comprehensive surveys concerning significant intrusion detection approaches. Nevertheless, none of the presented models fulfill all technical performance criteria, at least when considering large, real-world deployments. It is relevant to note that the paper [45] proposes a data processing model that is based on ensemble learning, while the paper [46,47] discusses the security of optical data transmission mediums relative to 5G infrastructures. Essentially, the fundamental requirement that was envisaged is related to the mandatory automatic real-time processing of large amounts of data traffic that flow through the telecommunications operator's 5G network core. It is relevant to note that the proposed algorithmic and architectural structures fully comply with these constraints.

The performance assessment process, which is described, and the reviewed similar contributions suggest that the integrated intrusion detection system, which is presented in this paper, is one of the very few relevant systems that are proven to detect known and unknown threat patterns in a large 5G network core, with high accuracy and without interfering with the low-latency levels of the implied data network, as they are perceived by the end users.

4. The Intrusion Detection and Intrusion Prevention Systems

In this section, we describe the main design core of our system. In the system, we use entropy calculation in order to preprocess the data and apply the CNN model to it afterwards. All other modules give the system the opportunity to detect and classify the newly arrived data/malicious data and to take the decisions in milliseconds, which reflects the computational efficiency and the novelty of the offered approach. The IDS system's architecture consists of the following three layers: the data management and control layer, the machine learning-based data analysis layer, and the data traffic forwarding layer. The machine learning-based data analysis is trained using the dataset, which is a combination of different datasets. It includes DOS/DDOS datasets, KDD research datasets, and a dataset that was provided by a large telecommunications service provider. All the information is divided into 85% for training and 15% for testing and validation. Such splitting gave us the best accuracy. The received accuracy score is 0.9414. The presented model considers the convolutional neural network (CNN) model.

The design of our security system consists of four main functional stages:

The data forwarding layer is concerned with monitoring and collecting data traffic, which represents the first stage of the system. The data forwarding layer is capable of

collecting and transferring streams of suspicious information to the control plane, and the intrusion prevention system (IPS) blocks the suspicious traffic of data by following the commands of the controller. This determines the second logical and functional stage of the system.

The data management and control layer recognize the malicious data patterns and identifies the anomalies by means of the analyses of intercepted data. After taking the appropriate security measures based on the detected patterns at the data analysis layer, it sends the information to the data transfer layer, which is the third stage of the system. This process is visualized on Figure 4.

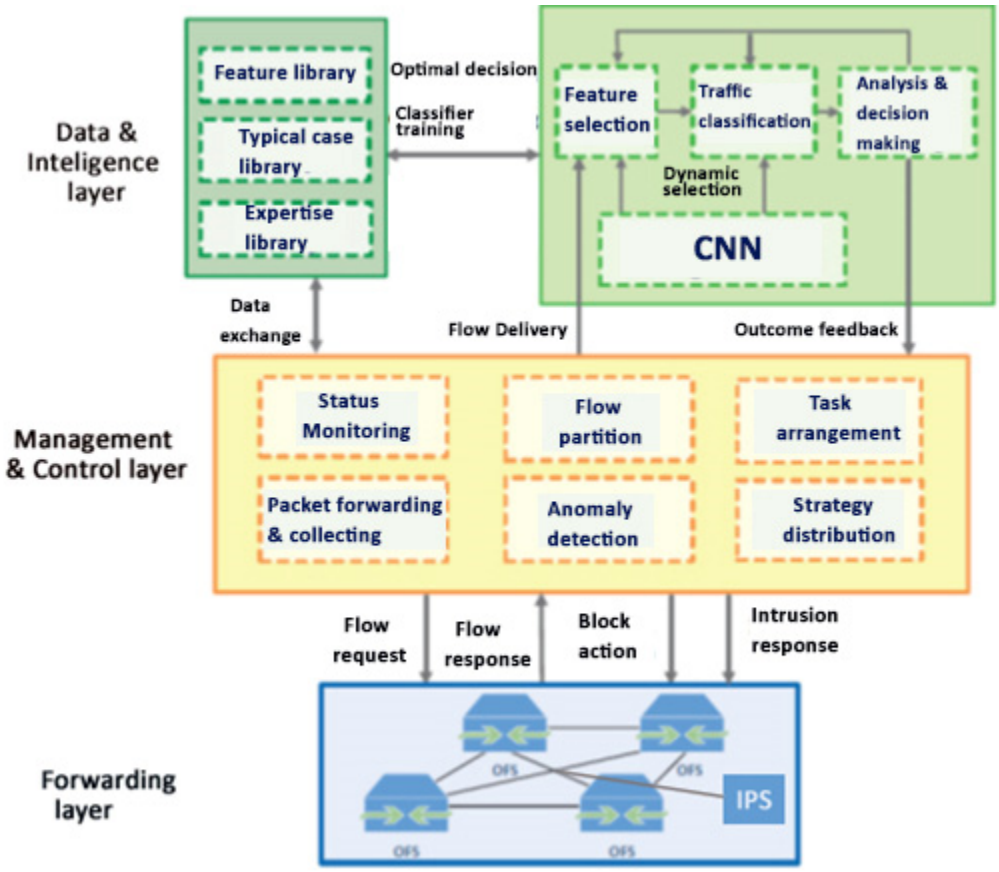

Figure 4. The architecture of IDS and IPS.

The data forwarding layer, which determines the fourth functional stage, collects suspicious data patterns in real time and sends information to the data management and control layer. The IPS instantly blocks intrusions and sends the suspicious files to other system leers for checking. The package collection and data stream splitting layer ensures the entire 5G network's global view. The state control unit monitors the status of the data transmission network and analyzes the received data packets. The data management plane operates and analyzes data traffic. In addition, it creates appropriate bunches of data packets and produces the data fingerprint that tracks the succeeding logical network parameters: source port and the network protocol in question. The data fingerprint identifies the markings of different data flow records representing specific network connections. The gathering and inspection of the packets is done continuously. The time interval of data gathering and inspection is optimized to avoid undesirable latency in the data assessment process in real-time.

The pseudo-code of the basic part of the system can be seen bellow:

Class Data_Int_Layers:			
Private:			
	X = None		# Variable for training stage
	Y = None		# Variable for training stage
	Model = CNN		# Variable for CNN model
	Def __init__(file_name, model_type):		# Constructor for preprocess data.
		Compute_data_homogeneity_score	
		Noise clean_up	
Preprocessing data . . .			
	Def create_model(model_type):		
		Create CNN model . . .	
		Return model	
	Def train_model(data_frame, model_type):		
		Training model with data . . .	
		Return model	
	Def test_model(model, model_type):		
		Testing and measure accuracy . . .	
		Return accuracy_score	
Public:			
	Def predict(x_data):		
		Predicting with our model . . .	
		Return predictions	
	Def print_accuracy(model_type):		
		return IDS.test_model()	

```
Importing the necessary libraries
Waiting_procces(traffic) # process to catch the traffic
Def management_cntrol_data():
    While True:
        If traffic:
            forwarding_layer(traffic)
def Forwarding layers(df):
    Object1 = Data_Int_Layers(df)
    Object1. Predict(data)
If data in malicious:
    IPS(data)
Else:
    Data_management(data)
def IPS(df):
    Block df
    Block df.ip
def Data_management(df):
    Print (“data is benign”)
    Forwarding data to the users
```

Packages are collected and checked permanently. Data acquisition and time intervals have been optimized to avoid possible unwanted retention in real-time data assessment.

The detection of anomalies is based on the basic data stream statistics that recognize potential anomalies. The specific IDS module employs entropy analysis by means of Shannon's theory to detect variation in the distribution of analyzed data packet selections.

Calculation of the entropy of a random variable r:

$$\mathrm{H(r)} = \sum_{i=0}^{n} \mathrm{p}(r_i) \log p(r_i) \quad (1)$$

Here, $\mathrm{p}(r_i)$ denotes the probability that r will take the value r_i given all the values are already found. The equation takes into account four main parameters: source IP, source port, target IP address, and target port. The real-time traffic analysis component collects these values. Therefore, given a specific period of time, the constantly updated value provided by the entropy function H(r) assists in the discovery of probable patterns of malicious data packets. This continuously updated score is applied to all four considered networking parameters. Thus, this generates an aggregated entropy score, which allows for the traffic patterns to be classified with a high level of accuracy. Entropy is represented by E, and D indicates the standard deflection A possible suspect pattern suggests that H(r) is outside the range [(E − D), (E + D)]. Therefore, suspicious data is for additional analysis to the continuous layer of data analysis. The feature selector element creates and updates feature sets specific to detected patterns of malicious data. The section can work with huge data amounts in real-time when deleting irrelevant data features from the predictive data analysis layer. Therefore, the data can be categorized as appropriate, so that the patterns of malicious data packets are therefore detached from the patterns of harmless traffic. Table 1 shows the performance score that sets the five columns of the table. The performance score is calculated based on the input dataset, which is specified in the first column. The mentioned dataset contains 32 000 000 network connections that were checked by the intrusion detection system. Moreover, each connection object consists of thirty-nine functions which are checked by the machine learning (CNN) module of the IDS. The performance value indicators demonstrate that the mentioned system is well matched to the size of the checked dataset. In addition, the system is capable of identifying patterns of malicious traffic, minimizing the number of false positives. The behavior of the system in practice is principally important when using 5G data networks for commercial purposes.

Table 1. Values of indicators for assessing efficiency.

Data Size	Pr	Rb	Tr	A	FR
10%	97.05%	97.01%	94.51%	94.14%	0.81%
20%	97.25%	96.95%	94.42%	94.10%	1.05%
40%	97.08%	96.74%	94.41%	94.05%	0.95%
60%	96.05%	96.70%	93.55%	93.80%	0.92%
80%	96.01%	95.81%	93.20%	93.40%	0.97%
100%	95.60%	95.54%	93.10%	92.90%	1.08%

It is relevant to mention that the described system proposes a unique machine learning-based 5G data traffic processing core (5GC). Furthermore, as the following section suggests, the maximum level of accuracy obtained is approximately 94%. The algorithmic model of the data traffic detection core should be further improved, so that the accuracy level should be in the range of 98–99%. This is justified by the necessity to reduce the unnecessary overload that is placed on the machine learning-based data traffic management components by incorrectly classifying benign data traffic patterns as malicious data traffic patterns.

5. Results and Discussions

Our system was tested on the infrastructure of one of the largest telecommunications service providers. As a result, we collected data from the providers' 5G network intrusion detection process in real time. The reviewed dataset has thirty-two network connections that were checked. Every connection object consists of thirty-nine functions, divided into three categories. Therefore, the system takes into account network connectivity-based features, data traffic-based functions, and content-based features. In addition, each unit of data transfer is flagged as a unit of suspicious or normal traffic. Suspicious traffic is collected into four groups: remote to local, test, denial of service, and user-root. The following metrics are considered when evaluating performance: accuracy (A), tradeoff (Tr), reliability (Rb), precision (Pr), and false alarm rate (FR). Accuracy is calculated as the percentage of correct predictions of malicious data traffic according to the total number of predictions made by the IDS. Reliability is measured by the ratio of strong intrusion attempts to the total number of intrusions. The tradeoff is a hybrid of accuracy and reliability that provides greater accuracy in classifying data using the following equation:

$$\mathrm{Tr} = 2/((1/\mathrm{Pr}) + (1/\mathrm{Rb})) \quad (2)$$

Accuracy is calculated by adding the number of correctly identified benign and malicious packages to the ratio of the sum of accurately detected legitimate and malicious packages and the number of incorrectly identified benign and malicious packages. The number of false positives can be calculated as the ratio of incorrectly classified legitimate packets to the total number of correctly classified benign packets and incorrectly classified benign traffic. Table 1 shows the performance score that defines the five columns of the table. In addition, performance metrics are calculated based on several parts of the input dataset, specified in the first column of the table. As we mentioned above, the dataset contains 32 000 000 network connections that were checked by the offered IDS. Furthermore, each connection object has thirty-nine functions, which are assessed by the intrusion detection system's machine learning core, which uses CNN.

The performance evaluation setup considers six fractions of the entire dataset, which were analyzed and are mentioned in the first column. Furthermore, the five considered metrics are evaluated through their defining percentages. The first four metrics indicate that the system can accurately detect malicious data traffic patterns that flow through the network operator's core. The values, which were computed relative to the false alarm rate (FR) metric, further justify the integrated system's capability to accurately process the data traffic patterns. Additionally, the consistent system's behavior in the case of all six fractions of the dataset demonstrates the scalability of the proposed solution. These features have also been fully demonstrated during the integrated system's deployment on the provider's infrastructure. In fact, the uniform behavior of the integrated system, which considers both its intrusion detection and intrusion prevention components, represents one of the key features. Thus, the system is simply deployed on the target infrastructure, and it is demonstrated to work reliably regardless of the particular configuration parameters, which pertain to the particular deployment infrastructure.

The performance appraisal scores confirm that the system is well-scalable relative to the size of the dataset being analyzed, and that the system can accurately detect malicious traffic patterns and minimize false positives. The behavior of the mentioned system in practice is principally important when using 5G data networks for commercial purposes that transfer and analyze a large number of data connections that need to be checked proactively. Moreover, it is also relevant to note that the dedicated 5G network cores, which process the related data traffic, pose unique challenges that are determined by several practical aspects. First, a sensibly larger number of concurrent data sessions should be processed, as compared to other types of mobile networks. Furthermore, this induces a greater variability in the logical structure of the respective data patterns, which should therefore be processed using efficient algorithmic detection cores. The results of the real-

world performance assessment process demonstrate that the system is capable of satisfying all these essential requirements, which individualizes it in the context of similar intrusion detection systems that are deployed in 5G data networks cores (5GC). This also implies that the processing time, in the case of all assessed data samples, is in the millisecond range, which fully ensures the real-time nature of the system. Furthermore, although we did not have access to the experimental data concerning the execution times of other similar software platforms, to the best of our knowledge, this represents one of the very few approaches that determines real-time data processing in the range of milliseconds. This further constitutes proof of the system's real-world relevance.

We have also tested our system with Google Colab and have produced the following results, which are showed on Table 2.

Table 2. Experiment results.

Data Size	Accuracy	Average Detection Time
10%	94.14%	200 milliseconds
20%	94.10%	180 milliseconds
40%	94.05%	240 milliseconds
60%	93.80%	350 milliseconds
80%	93.40%	294 milliseconds
100%	92.90%	320 milliseconds

Comparing the system to the related approaches such as [48,49], the processing delay of ours is approximately four times decreased, the false alarm rate has only decreased a by a small amount, but it must be emphasized that the accuracy score has decreased, please see Table 3.

Table 3. Comparison.

Approaches	Average Detection Time	A	FR
Our approach	200 milliseconds	94.14%	0.81%
Full set filter	2760 milliseconds	99.55%	1.02%
Info gain	840 milliseconds	99.64%	1.2%
Gain ratio	1310 milliseconds	99.64%	1.4%
Chi-squared	920 milliseconds	99.65%	1.6%
Relief	930 milliseconds	99%	0.98%

6. Conclusions and Future Work

The 5G networks have support for real-world applications. These applications provide enough potential to form the foundation of an ever-connected community. However, there are still problems with their design, launch, and implementation, which interest all aspects of 5G network research. One of the most important of these research problems pertains to the timely detection of unauthorized access attempts, especially in the case of commercial networks. Thus, this article presents the current results of research carried out on this very important topic. This article also describes a real-time intrusion detection and prevention system based on machine learning. The system was tested by monitoring real-time 5G data traffic on the network of one of the leading Romanian telecommunications service providers using real data. The system was checked in terms of the concept of symmetric and asymmetric communication scenarios. The research shows that it is possible to develop a software system that blocks illegal traffic in real-time on a 5G data network. The tests on the real-world 5G network show us that the system can detect and classify newly arrived data/malicious data and make decisions in milliseconds, which reflects the computational efficiency and novelty of the offered product. In addition, the article describes, in an analytical form, the contribution that is related to the topic under discussion, which analyzes the existing problems and presents possible ways to solve them. The idea of this system can also be used for future generations of networks. The big advantage

of this system is that it can work in real-time; however, the system also has limitations. It must be mentioned that the received accuracy score is 0.9414, which is rather low and must be increased. This is the big limitation of our system, and it must be improved. We suggest the use of data augmentation techniques to increase the accuracy score. We plan to improve the algorithm in order to increase the accuracy score. It could be interesting for other researchers to contribute to our research in order to increase the corresponding accuracy metric. In the future, we also suggest the addition of post-quantum encryption to the identification stage of 5G networks, which requires asymmetric encryption. We also suggest the addition of artificial intelligence to 5G and beyond networks in order to identify if the attack comes from a classical or quantum computer. Finally, we want to offer the novel model of 5G security, which will contain needed security mechanisms. The effective real-world relevance of the presented intrusion detection system is sufficiently justified by the requirement to automatically process 5G data traffic flows using self-developing data traffic analysis algorithmic cores and also by its demonstrated efficiency relative to a real-world deployment. Consequently, any further improvement of its detection accuracy and computational efficiency is implicitly useful.

Author Contributions: Conceptualization, R.B. and M.I.; methodology, R.B. and M.I.; software, M.I.; validation, R.B. and M.I.; formal analysis, R.B.; investigation, R.B. and M.I.; resources, R.B. and M.I.; data curation, R.B.; writing—R.B.; writing—review and editing, M.I.; supervision, R.B. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSF) [STEM—22 -1076].

Data Availability Statement: Not applicable.

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

References

1. Khan, M.A.; Kumar, N.; Mohsan, S.A.H.; Khan, W.U.; Nasralla, M.M.; Alsharif, M.H.; Zywiolek, J.; Ullah, I. Swarm of UAVs for Network Management in 6G: A Technical Review. *IEEE Trans. Netw. Serv. Manag.* **2022**, *35*, 9. [CrossRef]
2. Ravi, V.; Chaganti, R.; Alazab, M. Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system. *Comput. Electr. Eng.* **2022**, *102*(C), 108156. Available online: https://www.sciencedirect.com/science/article/pii/S0045790622004037 (accessed on 1 September 2022). [CrossRef]
3. May, D.; Landwehr, A.; Browning, T.; Cotton, C.; Kiamilev, F. Next Generation Data Link for IRSP Systems. In Proceedings of the 2021 IEEE Research and Applications of Photonics in Defense Conference (RAPID), Miramar Beach, FL, USA, 2–4 August 2021; pp. 1–2. [CrossRef]
4. Santos, J.; Wauters, T.; Volckaert, B.; De Turck, F. Towards Low-Latency Service Delivery in a Continuum of Virtual Resources: State-of-the-Art and Research Directions. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 2557–2589. [CrossRef]
5. Akpakwu, G.A.; Silva, B.J.; Hancke, G.P.; Abu-Mahfouz, A.M. A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges. *IEEE Access* **2017**, *6*, 3619–3647. [CrossRef]
6. Parvez, I.; Rahmati, A.; Guvenc, I.; Sarvat, A.; Dai, H. A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3098–3130. [CrossRef]
7. Vasudevan, V.A.; Tselios, C.; Politis, I. On Security Against Pollution Attacks in Network Coding Enabled 5G Networks. *IEEE Access* **2020**, *8*, 38416–38437. [CrossRef]
8. Braeken, A.; Liyanage, M.; Kumar, P.; Murphy, J. Novel 5G Authentication Protocol to Improve the Resistance Against Active Attacks and Malicious Serving Networks. *IEEE Access* **2019**, *7*, 64040–64052. [CrossRef]
9. Jover, R.P.; Marojevic, V. Security and Protocol Exploit Analysis of the 5G Specifications. *IEEE Access* **2019**, *7*, 24956–24963. [CrossRef]
10. Ogbodo, E.U.; Abu-Mahfouz, A.M.; Kurien, A.M. A Survey on 5G and LPWAN-IoT for Improved Smart Cities and Remote Area Applications: From the Aspect of Architecture and Security. *Sensors* **2022**, *22*, 6313. [CrossRef] [PubMed]
11. Shaik, A.; Borgaonkar, R. New Vulnerabilities in 5G Networks. Technische Universität Berlin and Kaitiaki Labs. Available online: https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-NewVulnerabilities-In-5G-Networks-wp.pdf (accessed on 7 August 2019).
12. Khan, J.A.; Chowdhury, M.M. Security Analysis of 5G Network. In Proceedings of the 2021 IEEE International Conference on Electro Information Technology (EIT), Mt. Pleasant, MI, USA, 14–15 May 2021; pp. 001–006. [CrossRef]
13. Akyildiz, I.; Wang, P.; Lin, S. SoftAir: A software defined networking architecture for 5G wireless systems. *Comput. Netw.* **2015**, *85*, 1–18. [CrossRef]

14. Xia, X.; Xu, K.; Wang, Y.; Xu, Y. A 5G-Enabling Technology: Benefits, Feasibility, and Limitations of In-Band Full-Duplex mMIMO. *IEEE Veh. Technol. Mag.* **2018**, *13*, 81–90. [CrossRef]
15. Qureshi, K.N.; Ahmad, E.; Anwar, M.; Ghafoor, K.Z.; Jeon, G. Network Functions Virtualization for Mobile Core and Heterogeneous Cellular Networks. *Wirel. Pers. Commun.* **2022**, *122*, 2543–2559. [CrossRef]
16. Hajar, M.A.; Alkahtani, A.A.; Ibrahim, D.N.; Al-Sharafi, M.A.; Alkawsi, G.; Iahad, N.A.; Darun, M.R.; Tiong, S.K. The Effect of Value Innovation in the Superior Performance and Sustainable Growth of Telecommunications Sector: Mediation Effect of Customer Satisfaction and Loyalty. *Sustainability* **2022**, *14*, 6342. [CrossRef]
17. Iavich, M.; Bocu, R.; Gagnidze, A. Real Time Self-developing Cybersecurity Function for 5G. In *Advanced Information Networking and Applications. AINA 2022*; Barolli, L., Hussain, F., Enokido, T., Eds.; Lecture Notes in Networks and Systems; Springer: Cham, Switzerland, 2022; Volume 451. [CrossRef]
18. Xu, L.; Collier, R.; O'Hare, G.M.P. A Survey of Clustering Techniques in WSNs and Consideration of the Challenges of Applying Such to 5G IoT Scenarios. *IEEE Internet Things J.* **2017**, *4*, 1229–1249. [CrossRef]
19. Sekander, S.; Tabassum, H.; Hossain, E. Multi-Tier Drone Architecture for 5G/B5G Cellular Networks: Challenges, Trends, and Prospects. *IEEE Commun. Mag.* **2018**, *56*, 96–103. [CrossRef]
20. Hasan, M.; Hossain, E. Random Access for Machine-to-Machine Communication in LTE Advanced Networks: Issues and Approaches. *IEEE Commun. Mag.* **2013**, *51*, 86–93. [CrossRef]
21. Lei, K.; Zhong, S.; Zhu, F.; Xu, K.; Zhang, H. An NDN IoT Content Distribution Model with Network Coding Enhanced Forwarding Strategy for 5G. *IEEE Trans. Ind. Inform.* **2017**, *14*, 2725–2735. [CrossRef]
22. Morgado, A.; Huq, K.M.S.; Mumtaz, S.; Rodriguez, J. A Survey of 5G Technologies: Regulatory, Standardization and Industrial Perspectives. *Digit. Commun. Netw.* **2018**, *4*, 87–97. [CrossRef]
23. Potter, C.H.; Hancke, G.P.; Silva, B.J. Machine-to-Machine: Possible applications in industrial networks. In Proceedings of the 2013 IEEE International Conference on Industrial Technology (ICIT), Western Cape, South Africa, 25–28 February 2013; pp. 1321–1326. [CrossRef]
24. Gyrard, A.; Bonnet, C.; Boudaoud, K. Enrich machine-to-machine data with semantic web technologies for cross-domain applications. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 559–564. [CrossRef]
25. Palattella, M.R.; Dohler, M.; Grieco, A.; Rizzo, G.; Torsner, J.; Engel, T.; Ladid, L. Internet of Things in the 5G Era: Enablers, Architecture and Business Models. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 510–527. [CrossRef]
26. Linge, N.; Odum, R.; Hill, S.; Von-Hunerbein, S.; Linnebank, P.; Sutton, A.; Townend, D. The impact of atmospheric pressure on the performance of 60 GHz point to point links within 5G networks. In Proceedings of the Loughborough Antennas and Propagation Conference, Loughborough, UK, 12–13 November 2018.
27. Habiba, U.; Hossain, E. Auction Mechanisms for Virtualization in 5G Cellular Networks: Basics, Trends, and Open Challenges. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2264–2293. [CrossRef]
28. Khurpade, J.M.; Rao, D.; Sanghavi, P.D. A Survey on IOT and 5G Network. In Proceedings of the 2018 International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, India, 5 January 2018; pp. 1–3. [CrossRef]
29. Jiang, N.; Deng, Y.; Nallanathan, A.; Chambers, J.A. Reinforcement Learning for Real-Time Optimization in NB-IoT Networks. *IEEE J. Sel. Areas Commun.* **2019**, *37*, 1424–1440. [CrossRef]
30. Chen, J.; Li, S.; Tao, J.; Fu, S.; Sobelman, G.E. Wireless Beam Modulation: An Energy- and Spectrum-Efficient Communication Technology for Future Massive IoT Systems. *IEEE Wirel. Commun.* **2020**, *27*, 60–66. [CrossRef]
31. Qamar, F.; Hindia, M.N.; Dimyati, K.; Noordin, K.A.; Majed, M.B.; Abd Rahman, T.; Amiri, I.S. Investigation of Future 5G-IoT Millimeter-Wave Network Performance at 38 GHz for Urban Microcell Outdoor Environment. *Electronics* **2019**, *8*, 495. [CrossRef]
32. Madapatha, C.; Makki, B.; Muhammad, A.; Dahlman, E.; Alouini, M.S.; Svensson, T. On Topology Optimization and Routing in Integrated Access and Backhaul Networks: A Genetic Algorithm-Based Approach. *IEEE Open J. Commun. Soc.* **2021**, *2*, 2273–2291. [CrossRef]
33. Sun, X.; Tang, Z.; Du, M.; Deng, C.; Lin, W.; Chen, J.; Qi, Q.; Zheng, H. A Hierarchical Federated Learning-Based Intrusion Detection System for 5G Smart Grids. *Electronics* **2022**, *11*, 2627. [CrossRef]
34. Mendonça, R.V.; Teodoro, A.A.; Rosa, R.L.; Saadi, M.; Melgarejo, D.C.; Nardelli, P.H.; Rodríguez, D.Z. Intrusion Detection System Based on Fast Hierarchical Deep Convolutional Neural Network. *IEEE Access* **2021**, *9*, 61024–61034. [CrossRef]
35. Maimó, L.F.; Gómez, Á.L.P.; Clemente, F.J.G.; Pérez, M.G.; Pérez, G.M. A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks. *IEEE Access* **2018**, *6*, 7700–7712. [CrossRef]
36. Duan, P.; Jia, Y.; Liang, L.; Rodriguez, J.; Huq KM, S.; Li, G. Space-Reserved Cooperative Caching in 5G Heterogeneous Networks for Industrial IoT. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2715–2724. [CrossRef]
37. Condoluci, M.; Araniti, G.; Mahmoodi, T.; Dohler, M. Enabling the IoT Machine Age With 5G: Machine-Type Multicast Services for Innovative Real-Time Applications. *IEEE Access* **2016**, *4*, 5555–5569. [CrossRef]
38. Vilalta, R.; Mayoral, A.; Casellas, R.; Martinez, R.; Verikoukis, C.; Munoz, R. TelcoFog: A Unified Flexible Fog and Cloud Computing Architecture for 5G Networks. *IEEE Commun. Mag.* **2017**, *55*, 36–43. [CrossRef]
39. Hu, N.; Tian, Z.; Lu, H.; Du, X.; Guizani, M. A multiple-kernel clustering based intrusion detection scheme for 5G and IoT networks. *Int. J. Mach. Learn. Cybern.* **2021**, *12*, 3129–3144. [CrossRef]

40. Mirzaee, P.H.; Shojafar, M.; Pooranian, Z.; Asefy, P.; Cruickshank, H.; Tafazolli, R. FIDS: A Federated Intrusion Detection System for 5G Smart Metering Network. In Proceedings of the 2021 17th International Conference on Mobility, Sensing and Networking (MSN), Exeter, UK, 13–15 December 2021; pp. 215–222.
41. Almiani, M.; AbuGhazleh, A.; Jararweh, Y.; Razaque, A. DDoS detection in 5G-enabled IoT networks using deep Kalman backpropagation neural network. *Int. J. Mach. Learn. Cybern.* **2021**, *12*, 3337–3349. [CrossRef]
42. Kou, L.; Ding, S.; Rao, Y.; Xu, W.; Zhang, J. A Lightweight Intrusion Detection Model for 5G-enabled Industrial Internet. *Mob. Netw. Appl.* **2022**, *133*, 1–10. [CrossRef]
43. Esenogho, E.; Djouani, K.; Kurien, A. Integrating Artificial Intelligence Internet of Things and 5G for Next-Generation Smartgrid: A Survey of Trends Challenges and Prospect. *IEEE Access* **2022**, *10*, 4794–4831. [CrossRef]
44. Afaq, A.; Haider, N.; Baig, M.Z.; Khan, K.S.; Imran, M.; Razzak, I. Machine learning for 5G security: Architecture, recent advances, and challenges. *Ad. Hoc. Netw.* **2021**, *123*, 102667. [CrossRef]
45. Rayan, T.; Sandeep, S.C. Machine learning IDS models for 5G and IoT. In *Secure Communication for 5G and IoT Networks*; Springer: Cham, Switzerland, 2022; pp. 73–84.
46. Lei, L.; Kou, L.; Zhan, X.; Zhang, J.; Ren, Y. An Anomaly Detection Algorithm Based on Ensemble Learning for 5G Environment. *Sensors* **2022**, *22*, 7436. [CrossRef] [PubMed]
47. Gong, X.; Zhang, Q.; Zhang, X.; Xuan, R.; Guo, L. Security Issues and Possible Solutions of Future-Oriented Optical Access Networks for 5G and Beyond. *IEEE Commun. Mag.* **2021**, *59*, 112–118. [CrossRef]
48. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecur* **2019**, *2*, 20. [CrossRef]
49. Song, H.M.; Kim, H.R.; Kim, H.K. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. In Proceedings of the 2016 International Conference on Information Networking (ICOIN), NW Washington, DC, USA, 13–15 January 2016; pp. 63–68. [CrossRef]