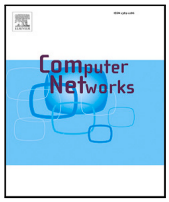
Computer Networks 188 (2021) 107871

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet



Composite and efficient DDoS attack detection framework for B5G networks

G.C. Amaizu, C.I. Nwakanma, S. Bhardwaj, J.M. Lee, D.S. Kim *

Department of IT Convergence Engineering, ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi, South Korea

ARTICLE INFO

Keywords:
Network security
5G
DDoS
Artificial intelligence

ABSTRACT

Distributed denial-of-service (DDoS) remains an ever-growing problem that has affected and continues to affect a host of web applications, corporate bodies, and governments. With the advent of fifth-generation (5G) network and beyond 5G (B5G) networks, the number and frequency of occurrence of DDoS attacks are predicted to soar as time goes by, hence there is a need for a sophisticated DDoS detection framework to enable the swift transition to 5G and B5G networks without worrying about the security issues and threats. A range of schemes has been deployed to tackle this issue, but along the line, few limitations have been noticed by the research community about these schemes. Owing to these limitations/drawbacks, this paper proposes a composite and efficient DDoS attack detection framework for 5G and B5G. The proposed detection framework consists of a composite multilayer perceptron which was coupled with an efficient feature extraction algorithm and was built not just to detect a DDoS attack, but also, return the type of DDoS attack it encountered. At the end of the simulations and after testing the proposed framework with an industry-recognized dataset, results showed that the framework is capable of detecting DDoS attacks with a high accuracy score of 99.66% and a loss of 0.011. Furthermore, the results of the proposed detection framework were compared with their contemporaries.

1. Introduction

Given that the Internet ecosystem is increasing rapidly, there has been an upward spike in the number of connected devices. Cisco once predicted that by 2030 there will be over 500 billion devices connected to the internet, though a much higher figure is expected with the current rate of connection. It is also estimated that all objects will have an internet node within them by 2025. The emergence and (gradual) adoption of fifth-generation (5G) networks have enabled the interconnection of more devices and people together. 5G networks have also been shown to have higher coverage and mobility, low latency and high transmission capacity [1,2] and has been deployed seamlessly into various Internet of things (IoT) applications such as smart homes, smart factories, transportation, and e-health [3–5]. With countries now launching 5G networks, the research focus has moved further to studies beyond fifth-generation (B5G) communication [6–8].

Numerous requirements have been considered in the deployment of 5G networks, one of which is security [9]. The security of 5G and B5G networks is a key requirement that needs to be addressed and as such has attracted lots of research works [4]. Previous generation networks had the main goal of ensuring proper functionality for securing the radio interface, by the encryption of the communication data rate. In the third generation, for instance, two-way authentication was used to eliminate any connections established with fake base stations(BSs). The fourth generation, however, employed advanced cryptographic protocols for user authentication. It also offered protection against physical attacks like the tampering of BSs, which is installed in user or public environments. Issues of 5G security and privacy however overpower these methods, as a result of the emergence of new services and changes in the architecture [9]. Subsequently, Table 1 contains a detailed list of all acronyms used in this paper.

There are three main components of security of 5G and B5G networks.

1. Firstly, all the security threats and system requirements of previous generations, still apply in 5G and B5G.
2. Secondly, there are a new set of security challenges which are as a result of an increase in the number of users, new network services, heterogeneity of connected device, high user privacy concerns, e.t.c.
3. Thirdly, network softwarization and the use of novel technologies like software-defined networking, network function virtualization, multi-access edge computing, and network slicing will lead to the evolution of new kinds of security and privacy challenges.

* Corresponding author.
E-mail address: dskim@kumoh.ac.kr (D.S. Kim).
URL: http://www.nsl.kumoh.ac.kr (D.S. Kim).

https://doi.org/10.1016/j.comnet.2021.107871
Received 2 December 2020; Received in revised form 12 January 2021; Accepted 25 January 2021
Available online 28 January 2021
1389-1286/

Table 1
Abbreviations and their corresponding meaning.

Acronym	Meaning
5G	Fifth-Generation
B5G	Beyond Fifth-Generation
IoT	Internet of Things
IIoT	Industrial Internet of Things
BS	Base Stations
DDoS	Distributed Denial of Service
UE	User Equipment
AI	Artificial Intelligence
PCC	Pearson Correlation Coefficient
DNN	Deep Neural Network
HTTP	Hypertext Transfer Protocol
SDN	Software-Defined Network
DF	Detection Framework
IP	Internet protocol
SN	Sensor Node
CH	Cluster Head
CNN	Convolution Neural Network
RNN	Recurrent Neural Network
KNN	K-Nearest neighbor
SVM	Support Vector Machine
API	Application Programming Interface
SYN	Synchronization Flood Attack
UDP	User Datagram Protocol
NetBIOS	Network Basic Input/Output System
MSSQL	Microsoft Structure Query Language
LDAP	Lightweight Directory Access Protocol
SSDP	Simple Service Discovery Protocol
NTP	Network Time Protocol
DNS	Domain Name System
TFTP	Trivial File Transfer Protocol
CICDDoS 2019	Canadian Institute for Cybersecurity DDoS 2019
ReLU	Rectified Linear Unit
SCC	Sparse Categorical Cross-entropy

One emerging technology to experience major security attack is the IoT due to the expected growth in the number of connected devices as well as connected devices per person. User Equipment (UE) such as smartphones and tablets are enabling the rise in the demand for services in 5G and B5G thus making them vulnerable to cyber-attacks such as Denial of Service and/or Distributed Denial of Service (DDoS) as the case may be [10]. While previous cyber-attacks seem to be less complicated and relatively sophisticated, future attacks such as code hacking, morphing, and bots may be very destructive both to other users and the entire 5G or B5G network if not detected and mitigated [10].

DDoS exhausts the network resource with requests from the attacker. Its target is usually to hinder network resource from serving and answering requests from legitimate users. The DDoS attack, however, reduces and hinders the availability of network service, by utilizing numerous compromised systems in a coordinated manner [11,12]. In 2016, the department of homeland security USA released a fact sheet drawing the public's attention to the perils of DDoS [13].

DDoS is a form of attack where the criminal sends an overwhelming number of traffic to a single website or machine so as to cause it to be unavailable for its intended users or purpose [14]. This can be in form of a volumetric attack where the attacker aims at taking up large volumes of bandwidth, protocol attack aimed at consuming server resources, and/or application layer attacks where the target is flooded in known web application vulnerabilities. Mitigating or controlling DDoS attacks involves classifying or differentiating traffic driven by an attack and regular traffic driven by intended users [15]. Fig. 1 shows Kaspersky's report of DDoS attacks in Q1 2020 where it can be observed that due to the COVID-19 lock-down, life not only shifted to the web, a lot of DDoS attacks also took place when compared to 2019. Key among the victims of DDoS attacks in 2020 is the website of the US Department of Health and Human Services (HHS), Lieferando (Germany), Thuisbezorgd (Netherlands), and Germany distance learning platform Mebis [16].

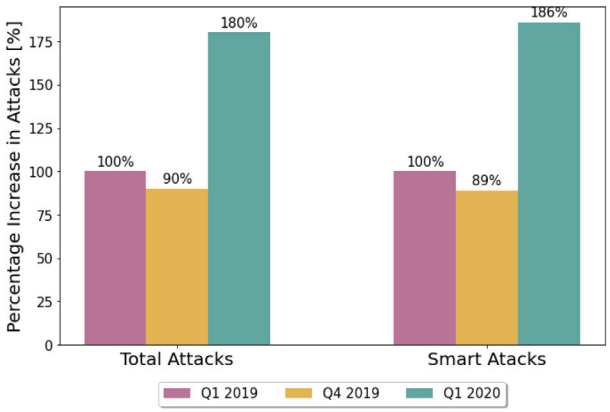


Fig. 1. Comparison of the total number of DDoS attacks in Q1 2020 and Q1 and Q4 2019; 2019 is taken as the 100% Ref. [16].

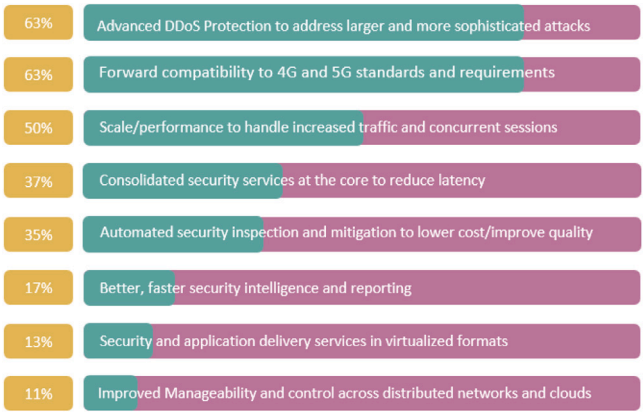


Fig. 2. DDoS as a Major Security Concern for 5G and B5G.

DDoS attacks are predicted to be of major concern in 2020 as it was predicted to have about 17 million DDoS attacks in 2020 [17]. For instance, IoT machines are vulnerable to the Mirai attack — a botnet capable of resulting in DDoS [18]. Another popular DDoS attack which is a variant of Mirai is Persirai know for infecting Internet Protocol (IP) cameras [19]. With the deployment of 5G and B5G, the authors of [20] believes that one of the common abuses of IoT proliferation is the DDoS attacks due to compromised IoT equipment. DDoS was listed among the expected challenges to confront 5G in addition to the challenges of flash network traffic, security of radio interface, user plane integrity, signaling storms, DoS attacks on end-user devices, and DDoS attacks on the infrastructure. Unfortunately, detection and mitigation of DDoS attacks have been deemed to be difficult, due to their distributed nature. It becomes more complicated to trace when attackers use fake IP addresses to hide their identities, as is often the case. Additionally, one critical issue to consider is the likely mobility of the devices used as a botnet. When UE moves around different locations, the network topology is bound to change and also quite unpredictably, making it much more difficult to trace the origin of the attack and mitigate it. Traditional detection and mitigation systems will be unable to protect 5G mobile networks because they are mostly not configures to recognize the irregular changes in the topology of the network. Attackers are known to move very often among various location, thereby capable of launching attacks difficult to pinpoint or trace [12]. This calls for the development of intelligent methods for the detection of DDoS attacks. Fig. 2 summarizes the growing security concern for future networks. It can be observed that the need for DDoS protection accounted for the greatest concern.

One of the most promising ways of improving the robustness and performance of 5G/B5G systems, coupled with the massive amount of data generated by such networks, is artificial intelligence (AI) [21,22]. Recently, there has been a surge in research works which either try to offer solutions to problems in 5G and B5G or combine these networks with other technologies using AI [23–25]. In the same vein, the researchers seek here to provide a solution to the easy detection of DDoS attacks in 5G and B5G networks.

In this paper, a composite and efficient DDoS attack detection framework for B5G networks is proposed. It is the kind that employs AI. As will be seen in the coming sections, four different scenarios were tried, and the best performing scenario was used as our proposed scheme. The model had two neural networks (hence the name composite) merged to produce a novel classifier capable of predicting various types of DDoS and benign traffic as well.

Against the limitations of existing solutions, the major contributions of this paper include:

1. Proposed a composite and efficient DDoS detection framework. The framework consists of a model obtained by concatenating two differently structured deep neural network models. This was aimed at improving the predictive accuracy of the model.
2. Proposed scheme was designed with an industry recognized, cutting edge, and recent dataset that was collated as recent as 2019.
3. Implemented Pearson Correlation Coefficient (PCC) for efficient feature selection. This minimizes the curse of dimensionality and classifier confusion. Invariably, this ensures improved predictive accuracy.
4. The proposed multi-class deep neural network (DNN) classifier takes DDoS detection beyond mere anomaly detection to a deeper paradigm where the type of attack(s) encountered are identified with minimal false alarm rate.
5. A comparison between the proposed scheme and existing solutions was implemented. Also commonly obtainable AI frameworks were assessed in scenario 2, 3, and 4.

Having given an introduction in this section (Section 1), the rest of this paper is structured as follows: Section 2 discusses some previous research on DDoS, then in Section 3 the system model, dataset and all other algorithms used were presented. Evaluation and results discussion was carried out in Section 4 before concluding the paper in Section 5.

2. Related works

There are quite a lot of detection methods and frameworks for DDoS detection, though this paper focuses more on the AI approach, "traditional approaches" shall also be considered in this section.

In [26], the concept of SLOW HTTP DDoS was introduced where authors proposed a defense mechanism called Slow HTTP DDoS Defense Application (SHDA) which is assisted by a software-defined network (SDN). The SHDA was installed in the SDN as an application and the authors had defined three types of clients namely legitimate clients, slow clients (clients having slow networks), and attackers. If the system receives an incomplete HTTP request the SHDA performs a DDoS attack check and receives the remaining HTTP requests on behalf of the server. If such requests keep reoccurring, they are then isolated from the system.

Cochain-sc was introduced by [27] consisting of decentralized controllers based on the Ethereum smart contract. For multiple SDN, the authors proposed a way of them communicating together using a smart contract. Firstly, a collaboration contract is created by one of the domains who then add other authorized participants into the collaboration and when there is an attack on any of the domain, the DDoS scheme in such domain detects and mitigates the attack while also storing the attackers IP address in the smart contract which is then mined by the authorized participants in the next mining block. Thus all authorized participants are granted access to a list of attackers' IP addresses which they have to block, hence preventing any malicious attacks in the future.

Entropy rate measurement (ERM) was used in [28] to detect DDoS attacks in a system. These researchers focused solely on the low rate (LR) DDoS and spoofing attack detection and discussed the reasons for mixed detection results for when the entropy value of legitimate traffic is greater than attack traffic (LGA) and when it is smaller (LSA). From these results, a new measurement was proposed with a better accuracy in the result.

Authors in [29] focused on cloud DDoS attacks and how to speed up the detection rate of such attacks. They were able to conclude that resource scaling during an attack is paramount to fast detection of an attack and hence proposed a scale inside-out approach that minimizes the resource utilization factor in order to obtain a quick absorption of the attack.

A scheme for detection of DDoS attacks in wireless sensor networks (WSNs) was introduced in [30]. The structure of this scheme consists of a BS and three sensor nodes (SN) which are relay nodes (RN), normal nodes, and cluster head (CH). For transmission to occur between SN and CH through the RN, a three-way handshake connection protocol is invoked after which the CH assigns a random number T_1 to the SN and keeps a copy of that number as T_c where $T_c \equiv T_1$. T_1 is valid for 10 s and can only be used once. Every time CH receives a message from SN, it checks to see if T_1 and T_c are the same, if not same, CH broadcasts the ID of that SN to its member nodes as a compromised SN before performing a second test to verify if indeed the SN has been compromised.

Authors in [31] presented a multi-level DDoS mitigation framework for IIoT by proposing a three-level architecture that corresponds to the three layers of IIoT which are edge computing level, fog computing level, and cloud computing level. Attackers are known to move very often among various locations, the consequence being their capability to launch attacks difficult to pinpoint or trace. In all, these methods failed to consider the fact that attackers often move around, changing their network topology and making the attacks unpredictable and difficult to pinpoint or trace back, hence there is a need for a more unique and flexible method for DDoS detection in 5G and B5G networks [12]. Furthermore, since DDoS attacks are difficult to detect in real-time, merely relying on the past approach of just identification is not sufficient to help the mitigation process. Thus, [32] proposed a scheme called REATO for actively and dynamically detecting, countering and recovering from denial of service attacks within a running IoT middleware called Networked Smart Object (NOS) [33]. REATO was used to protect IoT platform and its resources showing good performance in terms of latency, computing effort and attack recovery time.

AI application in 5G/B5G has been extensively researched by academic and industry professionals. There has also been some research interest in the application of AI to DDoS detection. For instance, the authors in [34] survey the AI algorithms which have been used in classifying DDoS attack traffic and detecting DDoS attacks. Examples of such algorithms include Naive Bayes, support vector machine, and Random forest tree. In [35], a deep network-based progressive transfer learning method is proposed to enable router throttling to cope with DDoS attacks. Authors in [36] developed a classification framework and algorithm to identify various possible DDos attacks on IoT. In their work, they compared the performance of various machine learning algorithms such as Random forest (RF), CNN, and multilayered Perceptron (MLP). The conclusion was that CNN and indeed deep neural networks are best suited for DDoS classification.

Similarly, authors in [37] used a machine learning approach to detect and mitigate the DoS attack with an accuracy of 96%. A hybrid framework was proposed in [38] by using a combination of anomaly and misuse type of detection. Matching pursuit algorithm and wavelet techniques were also used in creating the model and the results were tested with two different datasets. K means algorithm was considered

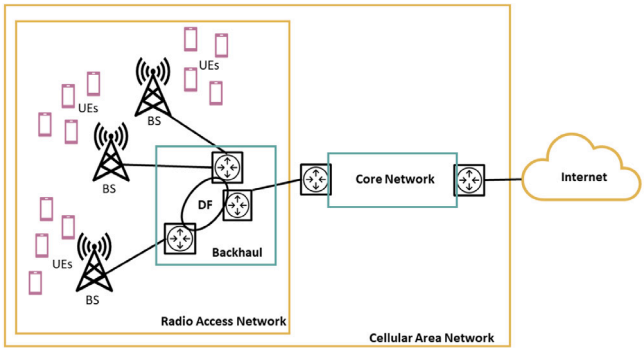


Fig. 3. System model depicting communication secure link between Detection Framework and Base Stations.

in [39] as they aimed to achieve a high detection rate. They had used two algorithms for feature selection, the first was a Hadoop-based algorithm then the second was an algorithm proposed by the authors to mitigate the problem of outliers and local optima. Authors [40,41] both proposed DDoS attack detection frameworks in SDN, [41] proposed two methods for mitigating DDoS attacks in SDN one of which uses the degree of attack to identify the attack and the other used an improved K-Nearest Neighbor algorithm to discover that attack. DeepSense was proposed in [17] and it consisted of CNN, RNN, and fully connected layers. The authors claimed to have a reduced error rate by over 5% and have better performance.

The datasets used by most of these works are somewhat old and some of the datasets are for network intrusion generally, thereby lacking details or features related to modern-day DDoS attacks. These datasets are mostly artificial and were generated using simulations and their results can only be as accurate as their simulations. Besides, most (if not all) of them were developed years before 5G, also, all of the frameworks above were only able to detect if a DDoS attack occurred or not without giving details on the type of DDoS attack as such information will enable the network administrators better set up the system in the future.

While it is certain that quite a lot of work has already been done in DDoS detection; the submission here is that the research is not mature enough in the AI context. In summary, this paper, unlike most others adopts the idea of merging two distinct neural networks together in solving the aforementioned problem of DDoS attacks. Moreover, there seem to be limited number of study grouping DDoS attacks into their respective classes as such information might be useful to a network administrator. Also, AI approaches to DDoS attack detection and classification should be based on high accuracy, precision, recall and F1-score. It is the major submission of this paper that the critical need for security in 5G and B5G era should adopt this more accurate approach to attack detection and classification.

3. Proposed methodology

5G networks which began a gradual roll out in 2019 is expected to cause a revolution and increase in connected devices. The 5G components in the cellular access network consists of two main subsystems: the radio access network and the core mobile network as shown in Fig. 3. The radio access network comprises of base station (BS), UE and backhaul network. The radio access network and core mobile network make up the cellular area network which constitute the possible target link of DDoS attack. In this paper, we agreed with numerous researches that have proposed that the security of a network be focused on BS hence, the DF is placed in the backhaul network which aggregates traffic to and from the BS. The 5G networks will have dense, distributed networks of BS in the small cell infrastructure. Details of 5G network components can be found in [42].

The BS acts as a radio receiver/transmitter and serves as a hub in wireless networks (in our case 5G and B5G networks). When a user equipment (UE) sends a request to the network through the BS, the BS communicates such a request with the DF mounted in the backhaul network to ascertain the security threat (if any). The DF then analyzes such requests and classifies them as either benign or any of the other classes of DDoS. The 5G core network is at the heart of the 5G specifications by the 3GPP and enables the increased throughput demand that 5G must support.

AI has been known for being able to challenge situations that are not fixed and are complex, hence it has risen to be an integral tool when talking about cyber-security, network security, and/or computer security [43]. However, there exist some concrete problems in AI safety as pointed out in [44]. And an example of such problems could be an attack that forces a model to classify its input sample wrongly.

To mitigate these and other related factors in this paper, an industry-recognized, recent dataset from a trusted source was used in training and testing the proposed model, also an effective gradient-based approach as proposed in [45] was implemented.

3.1. Composite multilayer perceptron

In this section, the architecture of the proposed composite multilayer DNN is presented. Using two models together has been shown to hold an advantage over a single model [40]. As can be seen in Fig. 4 the proposed scheme consists of two different DNN and classifies network traffic into ten separate attack classes and one class for benign traffics. DNN1 and DNN2 are two independent neural network models that are modeled differently. DNN1 is modeled sequentially using the Keras sequential Application Programming Interface (API), it consists of an input layer, seven hidden layers, two dropout layers arranged sequentially, and an output layer. The first and second dropout layers were placed just after the first and fourth hidden layers respectively. Likewise, DNN2 has an input layer, seven hidden layers, two dropout layers, and an output layer. Unlike DNN1, the layers of DNN2 were not sequentially arrange rather the Keras functional API was used. The output of the first hidden layer in DNN2 was used as an input to both the second and third hidden layers whose outputs acted as input to the fourth and fifth hidden layers respectively. The resulting outputs from both layers were fed as input to the first dropout layer then passed through the sixth hidden layer, the second dropout layer, and the seventh hidden layer in more of a sequential manner.

With DNN1 and DNN2 defined, the output from both DNN is concatenated to form a third model. The model resulting from combining DNN1 and DNN2 is then trained to predict various types of DDoS attacks when they occur in the network. Classes ranging from 0 up to 10 can be classified by the model, with each class representing one of the various DDoS attacks and one for benign traffic. Fig. 5 shows the various classes and the total number of samples per class. The ability to predict various classes was made possible by using $softmax$ activation function which unlike $sigmoid$, assigns a decimal probability to the various classes and these probabilities always sum up to 1.0. Full softmax was used as opposed to candidate sampling softmax as it calculates a probability for every possible class and is represented mathematically as:

$$p(y=j|x) = \frac{e^{(w_j^T x + b_j)}}{\sum_{k \epsilon K} e^{(w_k^T x + b_k)}}. \quad (1)$$

DNN1 and DNN2 could also be of the same configuration/structure. As a matter of fact, a model containing the same structure of DNN1 and DNN2 was implemented in this paper. Also, a model with just one of the two DNN was tried in order to further authenticate the accuracy and validity of the proposed model. These various configurations as will be seen in Section 4 were named scenarios

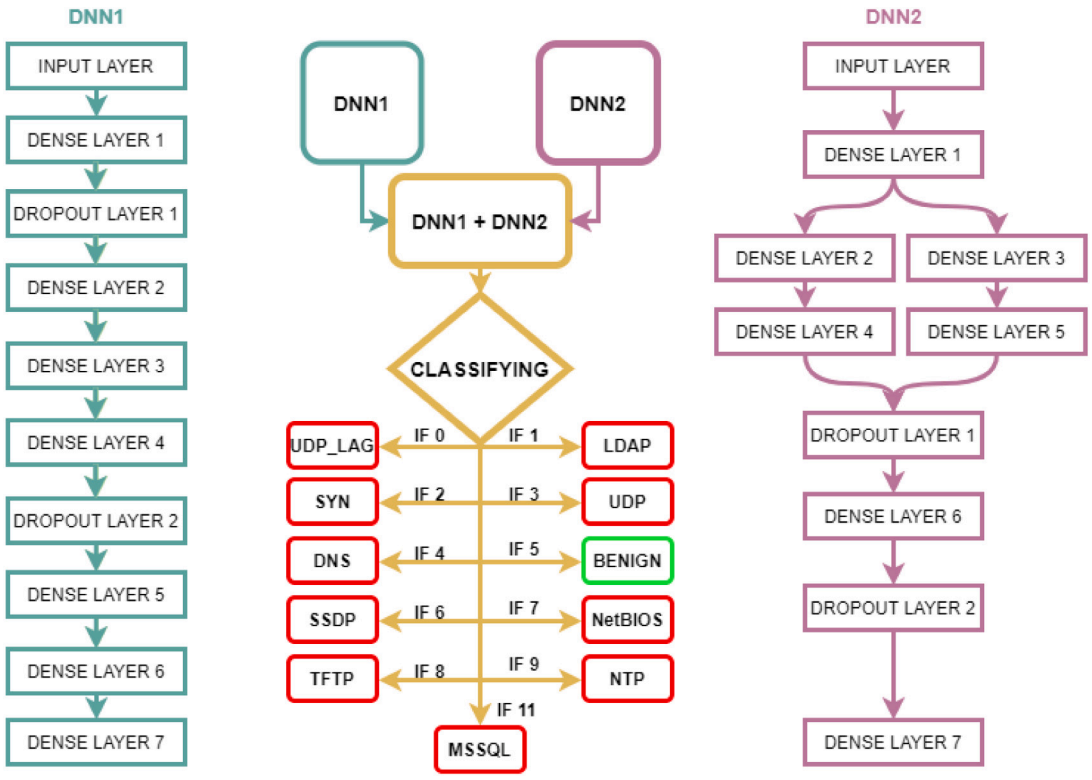


Fig. 4. Composite framework consisting of two DNN (DNN1 & DNN2) with a classifier having 11 output nodes each specifying a DDoS attack type and a benign traffic.

3.2. Dataset description and splitting

Over the years there have been several datasets proposed for the detection of DDoS, however, none was able to capture modern DDoS attacks like NetBIOS, UDP-Lag, and some others. CICDDoS2019 [46] addressed these issues and provides a dataset that was generated using real traffic. CICDDoS2019 which is a state-of-the-art dataset was used in training and testing the proposed model for optimal performance. This dataset consists of benign and other common DDoS attacks and it is to the best of the author's knowledge the most recent and sophisticated dataset for DDoS. The dataset consists of the various types of DDoS attacks grouped into reflection-based attacks and exploitation-based attacks. Under the exploitation-based attacks, we have SYN, UDP, and UDP-Lag DDoS, while the likes of NetBIOS, MSSQL, TFTP, etc., are under the reflection-based attacks. CICDDoS2019 has over 80 features. It is also worth noting that the traffic was captured for two days and the features were extracted using CICFlowMeter-V3.

The dataset used in this paper had over 180,000 samples consisting of both benign and the various other DDoS attacks classes. As can be seen in Fig. 5, each class has a total number of attacks ranging from 14,000 to 18,000. Here, care has been taken in order not to under-represent a class or over represent another class, leading to what is termed as an unrepresentative dataset. The number of samples per class is centered around 18,000 with only benign class having about 4,000 fewer samples. Numbers were assigned to each class as shown in Fig. 4 with the benign class having the number 5 assigned to it. With the help of train_test_split from scikit learn the dataset was partitioned into two parts (training and testing) as 70% of the dataset was used for training while the remaining 30% was kept for testing the model.

3.3. Efficient feature selection

Feature selection has come to be an important step in building a machine learning model for a few reasons. Firstly it solves the problem of dimensionality curse which is caused by having many features than samples and in most cases leads to overfitting of the model making it unable to generalize to new samples. Secondly, it is a good thing if the model is simple and explainable and this cannot be achieved by having lots of features that are not understandable. Lastly machine learning model behaves like a computer program, garbage in garbage out. Feeding the model with garbage as input will inevitably return garbage as output. It is a good practice to avoid feeding a model with too many features as it makes the model large in turn increasing complexity and training/testing time. This work implements PCC using the dependent variables and independent variables as inputs, where independent variables include all the features excluding the target column (the column containing the attack category) and the dependent variable contains only the target column. PCC mathematically is represented as below

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}}, \tag{2}$$

where n is the sample/dataset size, x_i, y_i are the individual sample points indexed as i. At the end of the PCC iteration, i.e, when $i == n$, the top features are selected and used for the model. Table 2 gives a list of the top 10 selected features.

Table 2
List of the top 10 selected features from the CICDDoS2019 dataset.

No.	Feature Name
1	Forward packet length max
2	Flow packets/seconds
3	Average packet size
4	Subflow forward bytes
5	Average forward segment size
6	Standard deviation of flow inter arrival time
7	Min packet length
8	Total forward packets
9	Packet length variance
10	Protocol

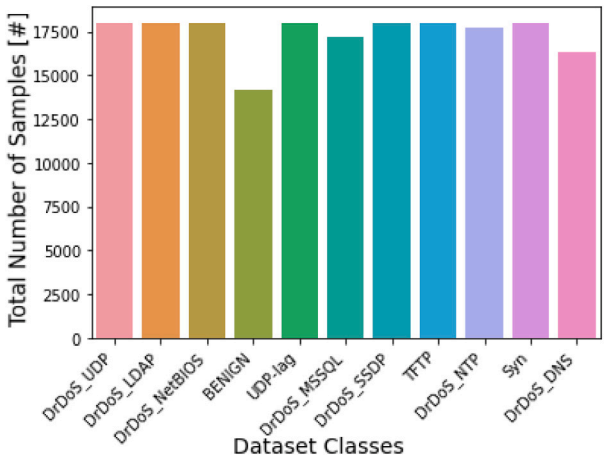


Fig. 5. Dataset class distribution showing the number of samples for all 10 attack classes and one benign class.

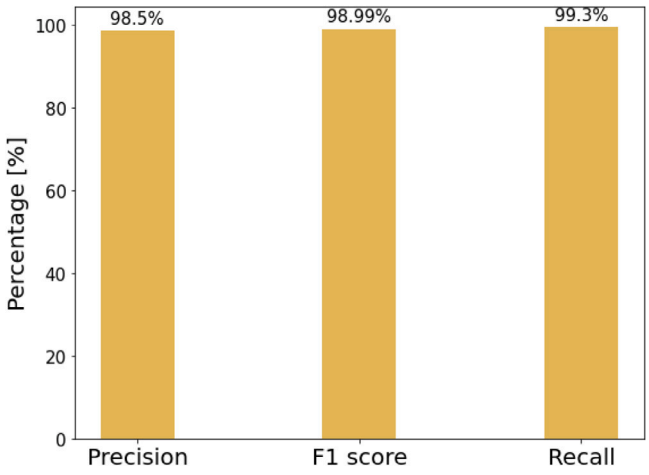


Fig. 6. Evaluation metrics consisting of precision, f1-score and recall rate all in percentages. This is the summary of the performance of the proposed deep neural network represented by scenario 1.

3.4. Hyperparameters

Hyperparameters are used in controlling and monitoring the learning process of a model. These parameters are set before training can begin as they oversee the whole training process of the model. They may not have an influence on the model's performance but they sure do influence the speed and quality of the learning process. Picking good hyperparameters could be the difference between an average model and a high performing model. Examples of hyperparameters are the number of hidden layers, number of neurons per layer, learning rate, number of epochs, and activation function. The process of selecting the perfect set of hyperparameters for a model is referred to as hyperparameter tuning, and this process was accomplished in this paper by making use of the Keras-tuner Library [47]. This library enables for picking the optimal set of hyperparameters for a model.

3.5. Feature scaling and dimension reduction

Feature scaling and dimension reduction are parts of what is termed as data preprocessing. This is a phase where the dataset is prepared to not just conform with the machine learning algorithm to be used, but also to make it easier for the algorithm to be more efficient/accurate in reading the data. Features in the dataset has different ranges and most times the range is just too wide, for example, a particular feature could have a value of 10 and 100 or even 10 and 10000. In such case it is necessary to carry out normalization or feature scaling where the range in a feature is made smaller, like say between 0 and 1 using the Min–Max Scaling function of scikit learn. Given a feature x which needs to be between the range of 0 and 1, Min–Max Scaler is defined as:

$$x' = a + \frac{x - min(x)(b - a)}{max(x) - min(x)}, \tag{3}$$

where b is 1 and a is 0.

4. Experiment and performance evaluation

4.1. Experimental setup

As explained in Section 3.2, the dataset used in this paper was developed by [46]. The data is generated by implementing two different networks. The first is an Attack-Network, then a Victim-Network [46, Fig. 2]. The different types of DDoS attacks obtained were made possible by separating the Attack-Network by means of a third-party company. The Victim-Network is a high-level security system comprising of the network components listed in Table 3.

Table 3
Victim-Network Configuration.

Quantity	Machine
1	Server
1	Firewall
2	Switches
4	PC (with different versions of widely used operating systems)

Table 4
Simulation Parameters of proposed scheme (scenario 1)

DNN1		DNN2	
No. of hidden layers	7	No. of hidden layers	7
Activation function	ReLU	Activation function	ReLU
Dropout Layers	2	Dropout Layers	2
Learning rate	0.001	Learning rate	0.001

Table 5
DDoS attack Classification report of the various scenarios.

Model	Precision (%)	F1-Score (%)	Recall (%)
Scenario 1	**99.52**	**99.99**	**99.30**
Scenario 2	93.40	90	96
Scenario 3	91.60	86.74	92
Scenario 4	71	80	91

As previously mentioned, there are four scenarios considered in determining the best model to use in implementing the proposed framework. A run down of the four different scenario is given below:

4.1.1. Scenario 1

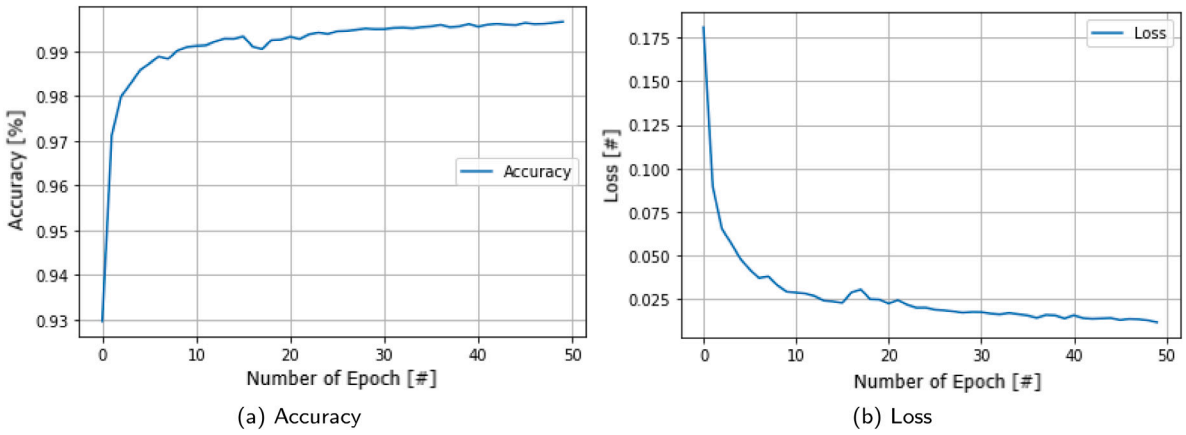
In this setup which can be seen in Table 4, DNN1 and DNN2 are differently configured, it is basically the structure in Fig. 4 with DNN1 being implemented using the Keras Sequential API and DNN2 implemented with the Keras Functional API.

4.1.2. Scenario 2

In this scenario, we still have both the DNN1 and DNN2, but in this case, the structure of DNN1 was used in DNN2. That is to say, DNN1 was used as the two DNN.

4.1.3. Scenario 3

Here, instead of having two DNN, we had opted for one DNN using the configuration of the original DNN2 (built with Keras Functional API).



(a) Accuracy (b) Loss

Fig. 7. Accuracy and Loss vs Number of epoch of proposed framework.

4.1.4. Scenario 4

So far, the activation function used in all layers of our DNN (DNN1 & DNN2) has been the Rectified Linear Unit (ReLU). In this scenario, we changed things a little bit by making use of the hyperbolic tangent activation function (Tanh) as opposed to the ReLU activation function. Eqs. (4) and (5) gives the mathematical notation of ReLU and Tanh activation functions respectively.

$$f(x) = x^{+} = max(0, x). \tag{4}$$

$$f(x) = tanh(x) = \frac{2}{1 + e^{-2x}} - 1. \tag{5}$$

where x is input to the neurons

4.2. Performance evaluation

First, the mathematical notations for metrics used in evaluating the proposed scheme for correctness are introduced.

$$Recall = \frac{TP}{TP + FN}, \tag{6}$$

$$Precision = \frac{TP}{TP + FP}, \tag{7}$$

$$F1 - score = \frac{2 * (Precision * Recall)}{(Precision + Recall)}, \tag{8}$$

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN}, \tag{9}$$

where TP is true positive, TN is true negative, FP is false positive and FN is false negative.

A classification report for the four scenarios can be seen in Table 5 while Fig. 6 contains a plot of the models precision f1-score and recall.

4.2.1. Accuracy and loss

Accuracy score is one of the most important metrics when it comes to evaluating the performance of a classifier like the one introduced in this paper. Fig. 7(a) depicts the accuracy of the proposed model at each iteration (epoch). Since random weights are assigned at the first epoch it is expected to have a low accuracy which then increases over time (measured as epoch). The model started with an accuracy of approx 93% but was able to rise, climbing to 99% in the first 10 epochs, and by the 50th epoch, an accuracy of 99.66% was reached.

Along with side accuracy is loss. Normally, when dealing with neural networks, the aim is to minimize loss for every epoch or iteration by using a loss function. The loss function calculates and keeps track of the model loss at the end of each epoch, then adjusts the weights and biases to values that will invariably reduce loss in the next iteration/epoch. The problem at hand is a multi-classification problem and as such the sparse categorical cross-entropy (SCC) as our loss function and is given by:

$$\alpha = -\frac{1}{N} \sum_{s \epsilon S} \sum_{c \epsilon C} 1_{sec} \log p(sec). \tag{10}$$

where α is the SCC, S is samples and C is classes. Fig. 7(b) shows that the proposed scheme recorded a low loss of 0.011. Loss is said to be at the best possible value when it is closer to 0.0.

4.2.2. Confusion matrix

Confusion matrix has extensively been used in the evaluation of a classification algorithm, it gives a detailed analysis of the algorithm's performance in predicting previously unseen data. In Fig. 8 the confusion matrix of all four scenarios is presented. Fig. 8(a) shows the confusion matrix of scenario 1 which is the proposed scheme while Fig. 8(b), 8(c) and 8(d) shows the confusion matrix of scenario 2, scenario 3 and scenario 4 respectively. Each diagonal element in the four figures contains the percentage of correctly classified samples for each corresponding class. The distinct diagonal formed in Fig. 8(a) (Scenario 1) shows that there is a higher number of correctly classified samples as opposed to that of other scenarios that have a higher number of wrongly classified samples. Therefore, the configuration in scenario 1 has a better all-around performance than other configurations (scenarios).

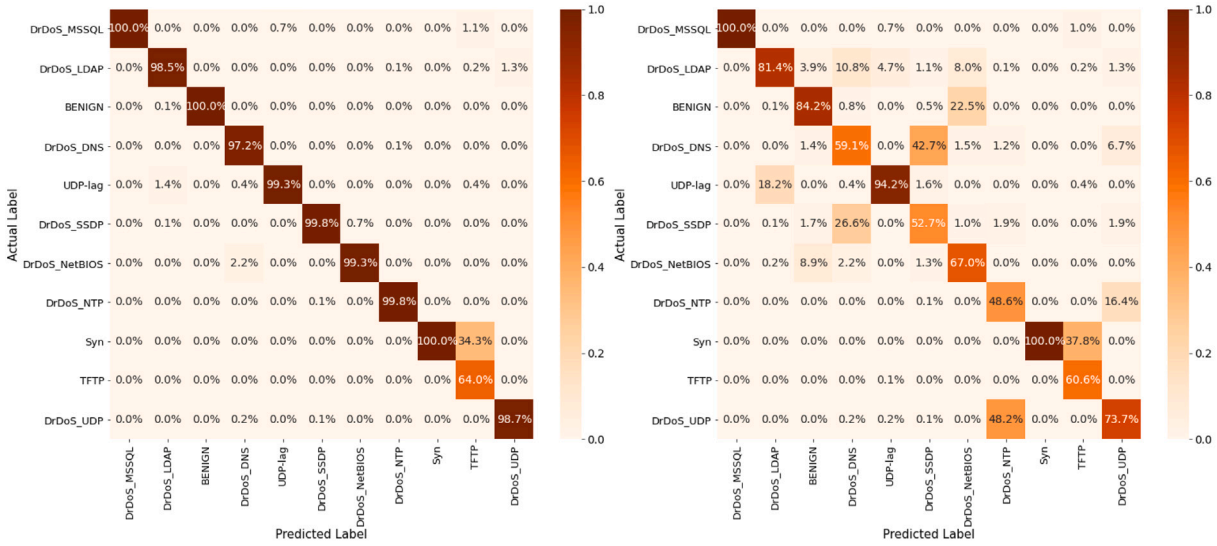
4.2.3. Comparative study

The performance of the proposed scheme was compared with other algorithms/methods and the results given in Table 6. Here, the proposed scheme outperformed K-Nearest Neighbor (KNN), Support Vector Machine (SVM), and deepsense [17] both in accuracy, precision, f1_score, and recall. When compared to CNN ensemble [40], the proposed scheme had better performance in both accuracy and f1_score, falling a little bit short in precision and recall. However, the proposed scheme included recent DDoS attack classes not accounted for in [40] and is capable of giving the exact DDoS attack class that it encounters.

From the results of the various scenarios obtained above, scenario 1, where two DNN were combined gave the best performance as compared to various other scenarios (scenario 2, 3 & 4). In using two distinct DNN consisting of dropout layers and employing an efficient feature selection mechanism, the detection accuracy of the model is increased while loss is brought to a minimal.

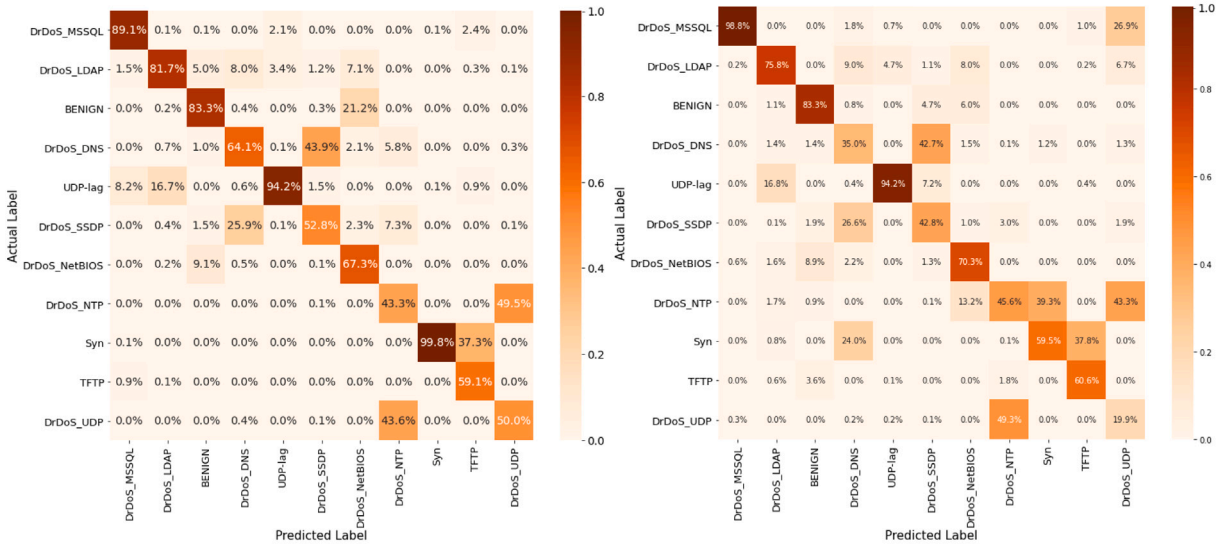
5. Conclusion

Secured communication has always been a problem and that problem has increased and will continue to increase, especially with the recent adoption of 5G and B5G networks. DDoS tops when it comes to security threats for these networks and that precipitated the need



(a) Scenario 1: Proposed scheme confusion matrix having different setup for DNN1 and DNN2

(b) Scenario 2: Same configuration of DNN1 and DNN2



(c) Scenario 3: Confusion matrix with one DNN

(d) Scenario 4: Proposed scheme using Tanh activation function

Fig. 8. Confusion matrix of various scenarios. It can be observed that Scenario 1 which depicts the proposed scheme performed better than scenarios 2, 3 and 4 respectively. This implies that using ReLU activation function with different configurations for the Deep Neural Networks gave best performance.

Table 6
Performance evaluation and comparison of proposed scheme with state-of-the art. The proposed scheme outperformed in accuracy and F1-score and performed comparatively in precision and recall.

Model	Accuracy(%)	Precision(%)	F1-score(%)	Recall(%)	Dataset Description
KNN	88.53	87.96	87.99	88.31	Current and state-of-the-art dataset containing all DDoS attack classes.
SVM	75.72	73.60	70.66	70.98	Current and state-of-the-art dataset containing all DDoS attack classes. SVM
CNN & RNN [17]	98.41	98.34	98.40	98.47	Dataset does not contain updated DDoS attack classes.
CNN Ensemble [40]	99.45	**99.57**	99.61	**99.64**	Dataset does not contain updated DDoS attack classes.
Proposed scheme	**99.66**	99.52	**99.99**	99.30	Current and state-of-the-art dataset containing all DDoS attack classes.

for efficient DDoS prevention and detection. The researchers here have proposed a composite and efficient DDoS detection framework to tackle these threats and pave way for a smooth transition into 5G and B5G networks. The proposed framework is made up of a composite machine learning model, where two differently structured DNN were merged into one and a classifier was built to correctly classify ten different DDoS attacks as well as benign or normal transaction. We had used the PCC algorithm to select features that contribute the most in predicting the classes accurately, also four scenarios were set up with different configurations of DNN to identify the most performed model upon which the proposed framework would be based. An accuracy of 99.66% and a low loss of 0.011 was recorded and the proposed framework showed that it was capable of not just predicting when there was a DDoS attack, but also the type of DDoS attack it encountered. For future work, it is desirable to reduce computational effort, training, and testing by altering the proposed deep neural network while improving the accuracy as much as practicable. A high accuracy and low loss amongst other metrics achieved the goal of ensuring DDoS attack detection in a network. However, in the 5G and B5G era, research into latency aware and computational cost management is a promising candidate. To achieve this, exploring ways of developing a lightweight deep neural network for DDoS detection would be studied next.

CRediT authorship contribution statement

G.C. Amaizu: Conceptualization, Methodology, Data curation, Software, Investigation, Writing - review & editing, Visualization. **C.I. Nwakanma:** Data curation, Writing - original draft, Writing - review & editing, Visualization. **S. Bhardwaj:** Data curation, Writing - original draft, Supervision, Editing, Visualization. **J.M. Lee:** Supervision, Funding acquisition. **D.S. Kim:** Supervision, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work was supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2018R1A6A1A03024003). It was also supported by the MSIT (Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program (IITP-2020-2020-0-01612) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation).

References

[1] K. Shafique, B.A. Khawaja, F. Sabir, S. Qazi, M. Mustaqim, Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G–IoT scenarios, IEEE Access 8 (2020) 23022–23040.

[2] A. Ghosh, A. Maeder, M. Baker, D. Chandramouli, 5G evolution: A view on 5G cellular technology beyond 3GPP release 15, IEEE Access 7 (2019) 127639–127651.

[3] T.-D. Hoa, N. Krommenacker, P. Charpentier, D.-S. Kim, The internet of things for logistics: Perspectives, application review, and challenges, IETE Tech. Rev. (2020) 1–29.

[4] L. Chettri, R. Bera, A comprehensive survey on internet of things (IoT) toward 5G wireless systems, IEEE Internet Things J. 7 (1) (2020) 16–32.

[5] H. Tran-Dang, N. Krommenacker, P. Charpentier, D. Kim, Toward the internet of things for physical internet: Perspectives and challenges, IEEE Internet Things J. 7 (6) (2020) 4711–4736.

[6] B. Li, Z. Fei, Y. Zhang, UAV communications for 5G and beyond: Recent advances and future trends, IEEE Internet Things J. 6 (2) (2019) 2241–2263.

[7] S.J. Nawaz, S.K. Sharma, S. Wyne, M.N. Patwary, M. Asaduzzaman, Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future, IEEE Access 7 (2019) 46317–46350.

[8] L. Zhu, Z. Xiao, X. Xia, D. Oliver Wu, Millimeter-wave communications with non-orthogonal multiple access for B5G/6G, IEEE Access 7 (2019) 116123–116132.

[9] R. Khan, P. Kumar, D.N.K. Jayakody, M. Liyanage, A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions, IEEE Commun. Surv. Tutor. 22 (1) (2020) 196–248.

[10] G. Mantas, N. Komninos, J. Rodriuez, E. Logota, H. Marques, Security for 5G communications, in: J. Rodriguez (Ed.), Fundamentals of 5G Mobile Networks, John Wiley & Sons, Ltd., 2015, pp. 207–220.

[11] M.K. Forland, K. Kralevska, M. Garau, D. Gligoroski, Preventing DDoS with SDN in 5G, in: 2019 IEEE Globecom Workshops (GC Wkshps), 2019, pp. 1–7.

[12] A.S. Mamolar, Z. Pervez, Q. Wang, J. M. Alcaraz-Calero, Towards the detection of mobile DDoS attacks in 5G multi-tenant networks, in: 2019 European Conference on Networks and Communications (EuCNC), 2019, pp. 273–277.

[13] USA HMS, 2020, https://www.dhs.gov/publication/st-distributed-denial-service-defense-fact-sheet [Accessed 13 July 2020].

[14] M. Kim, Supervised learning-based DDoS attacks detection: Tuning hyperparameters, ETRI J. 41 (5) (2019) 560–573.

[15] K. Lee, J. Kim, K.H. Kwon, Y. Han, S. Kim, DDoS attack detection method using cluster analysis, Expert Syst. Appl. 34 (3) (2008) 16959–1665.

[16] O. Kupreev, E. Badovskaya, A. Gutnikov, DDoS attacks in 2020, Kasperky DDoS reports, 2020.

[17] X. Yuan, C. Li, X. Li, Deepdefense: Identifying DDoS attack via deep learning, in: 2017 IEEE International Conference on Smart Computing (SMARTCOMP), 2017, pp. 1–8.

[18] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, DDoS in the IoT: Mirai and other botnets, Computer 50 (2017) 80–84.

[19] P. Radanliev, Future developments in cyber risk assessment for internet of things, Comput. Ind. 102 (2018) 14–22.

[20] H. Ghorbani, M.S. Mohammadzadeh, M.H. Ahmadzadegan, DDoS attacks on the IoT network with the emergence of 5G, in: 2020 International Conference on Technology and Entrepreneurship - Virtual (ICTE-V), 2020, pp. 1–5.

[21] C. Zhang, Y. Ueng, C. Studer, A. Burg, Artificial intelligence for 5G and beyond 5G: Implementations, algorithms, and optimizations, IEEE J. Emerging Sel. Top. Circuits Syst. 10 (2) (2020) 149–163.

[22] M.E. Morocho-Cayamcela, H. Lee, W. Lim, Machine learning for 5G/B5G mobile and wireless communications: Potential, limitations, and future directions, IEEE Access 7 (2019) 137184–137206.

[23] A.P. Hermawan, R.R. Ginanjar, D. Kim, J. Lee, CNN-based automatic modulation classification for beyond 5G communications, IEEE Commun. Lett. 24 (5) (2020) 1038–1041.

[24] W. Chien, H. Cho, C. Lai, F. Tseng, H. Chao, M.M. Hassan, A. Alelaiwi, Intelligent architecture for mobile hetnet in B5G, IEEE Netw. 33 (3) (2019) 34–41.

[25] K.I. Ahmed, H. Tabassum, E. Hossain, Deep learning for radio resource allocation in multi-cell networks, IEEE Netw. 33 (6) (2019) 188–195.

[26] K. Hong, Y. Kim, H. Choi, J. Park, SDN-assisted slow HTTP DDoS attack defense method, IEEE Commun. Lett. 22 (4) (2018) 688–691.

[27] Z. Abou El Houda, A.S. Hafid, L. Khoukhi, Cochain-SC: An intra- and inter-domain Ddos mitigation scheme based on blockchain using SDN and smart contract, IEEE Access 7 (2019) 98893–98907.

[28] L. Zhou, K. Sood, Y. Xiang, ERM: An accurate approach to detect DDoS attacks using entropy rate measurement, IEEE Commun. Lett. 23 (10) (2019) 1700–1703.

[29] G. Somani, M.S. Gaur, D. Sanghi, M. Conti, M. Rajarajan, Scale inside-out: Rapid mitigation of cloud DDoS attacks, IEEE Trans. Dependable Secure Comput. 15 (6) (2018) 959–973.

[30] A.P. Abidoye, I.C. Obagbuwa, DDoS attacks in WSNs: Detection and countermeasures, IET Wirel. Sensor Syst. 8 (2) (2018) 52–59.

[31] Q. Yan, W. Huang, X. Luo, Q. Gong, F.R. Yu, A multi-level DDoS mitigation framework for the industrial internet of things, IEEE Commun. Mag. 56 (2) (2018) 30–36.

[32] S. Sicari, A. Rizzardi, D. Miorandi, A. Coen-Porisini, REATO: REActing TO denial of service attacks in the internet of things, Comput. Netw. 137 (2018) 37–48.

[33] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, A. Coen-Porisini, A secure and quality-aware prototypical architecture for the internet of things, Inf. Syst. 58 (2016) 43–55.

[34] B. Zhang, T. Zhang, Z. Yu, DDoS detection and prevention based on artificial intelligence techniques, in: 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2017, pp. 1276–1280.

[35] S. Xia, L. Zhang, W. Bai, X. Zhou, Z. Pan, DDoS traffic control using transfer learning DQN with structure information, IEEE Access 7 (2019) 81481–81493.

[36] B. Susilo, R.F. Sari, Intrusion detection in IoT networks using deep learning algorithm, Information 11 (279) (2020) 1–11.

[37] F.S.L. Filho, F.A.F. Silveira, A.M. Brito, G. Vargas-Solar, L.F. Silveira, Smart detection: An online approach for DoS/DDoS attack detection using machine learning, Hindawi Secur. Commun. Netw. 2019 (1574749) (2019) 1–15.

[38] D. Erhan, E. Anarim, Hybrid DDoS detection framework using matching pursuit algorithm, IEEE Access 8 (2020) 118912–118923.

[39] Y. Gu, K. Li, Z. Guo, Y. Wang, Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm, IEEE Access 7 (2019) 64351–64365.
[40] S. Haider, A. Akhunzada, I. Mustafa, T.B. Patel, A. Fernandez, K.R. Choo, J. Iqbal, A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks, IEEE Access 8 (2020) 53972–53983.
[41] S. Dong, M. Sarem, DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks, IEEE Access 8 (2020) 5039–5048.
[42] J. Kim, D. Kim, S. Choi, 3GPP SA2 architecture and functions for 5G mobile communication system, ICT Express 3 (1) (2017) 1–8.
[43] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu, V.C.M. Leung, A survey on security threats and defensive techniques of machine learning: A data driven view, IEEE Access 6 (2018) 12103–12117.
[44] D. Amodei, C. Olah, J. Steinhardt, P. Christiano, J. Schulman, D. Mané, Concrete problems in AI safety, 2016.
[45] B. Biggio, I. Corona, D. Maiorca, B. Nelson, N. Srndic, P. Laskov, G. Giacinto, F. Roli, Evasion attacks against machine learning at test time, 2017.
[46] I. Sharafaldin, A.H. Lashkari, S. Hakak, A.A. Ghorbani, Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy, in: 2019 International Carnahan Conference on Security Technology (ICCST), 2019, pp. 1–8.
[47] Keras-tuner, 2020, https://keras-team.github.io/keras-tuner/ [Accessed 13 July 2020].

Gabriel Chukwunonso Amaizu received his bachelor's degree in computer application from the prestigious Bangalore University, India in 2017. He is currently pursuing his master's degree in the Department of IT Convergence Engineering, Kumoh National Institute of Technology, South Korea. His research interests include network security, machine learning, systems design and industrial IoT.

Cosmas Ifeanyi Nwakanma is currently a Ph.D. Student and full time researcher at Networked System Laboratory, IT-Convergence Engineering in Kumoh National Institute of Technology Gumi, South Korea. He received his National Diploma (Distinction) in Electrical/Electronics Engineering from Federal Polytechnic Nekede Imo State Nigeria in 1999. He later received his Bachelor of Engineering in Communication Engineering (2004), Master's in Information Technology (2012) and Master of Business Administration (MBA) in Project Management Technology (2016) all from the Federal University of Technology Owerri Imo State Nigeria where he has put in ten (10) years of lecturing and research experience. He was an intern with Asea Brown Boveri (ABB) Nigeria in 2003. As a member of IEEE, he has served as a volunteer reviewer to IEEE Access. His research interests are Reliability and Prediction in Real-Time Industrial Networked Systems using machine learning.

Sanjay Bhardwaj received his Ph.D. degree from the Department of IT convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea in 2020. From 2012 to 2018 he worked as Assistant Professor in the department of Electronics and Communication at Shoolini University, India. He is currently postdoctoral researcher at ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi, South Korea. His research areas of interest are bioinspired CRNs, IoT, IIoT and URLLC in the industrial wireless network.

Jae-Min Lee received the Ph.D. degree in electrical and computer engineering from the Seoul National University, Seoul, Korea, in 2005. From 2005 to 2014, he was a Senior Engineer with Samsung Electronics, Suwon, Korea. From 2015 to 2016, he was a Principle Engineer in Samsung Electronics, Suwon, Korea. Since 2017, he has been an assistant professor with School of Electronic Engineering and Department of IT-Convergence Engineering, Kumoh National Institute of Technology, Gyeongbuk, Korea. He is a member of IEEE. His current main research interests are industrial wireless control network, performance analysis of wireless networks, and TRIZ.

Dong-Seong Kim received his Ph.D. degree in Electrical and Computer Engineering from the Seoul National University, Seoul, Korea, in 2003. From 1994 to 2003, he worked as a full-time researcher in ERC-ACI at Seoul National University, Seoul, Korea. From March 2003 to February 2005, he worked as a postdoctoral researcher at the Wireless Network Laboratory in the School of Electrical and Computer Engineering at Cornell University, NY. From 2007 to 2009, he was a visiting professor with Department of Computer Science, University of California, Davis, CA. He is currently a director of kit Convergence Research Institute and ICT Convergence Research Center (ITRC and NRF advanced research center program) supported by Korean government at Kumoh National Institute of Technology. He is a senior member of IEEE and ACM. His current main research interests are real time IoT and smart platform, industrial wireless control network, networked embedded system and Fieldbus.