Intrusion Detection System for 5G Device-to-Device Communication Technology in Internet of Things

Ola Malkawi[1], Wesam Almobaideen[2], Nadeem Obaid[3], Bassam Hammo[3]
[1]Amman Arab University, Jordan
[2]University of Jordan , Rochester Institute of Technology, Jordan
[3]University of Jordan, Jordan
E-mail: o.malkawi@aau.edu.jo, wxacad@rit.edu, obein@ju.edu.jo, b.hammo@ju.edu.jo

Keywords: device to device communication, intrusion detection system, machine learning, classification, 5G cellular communications

Received: Feb 1, 2023

The emergence of Internet of Things (IoT) has raised the need for high quality communications, and high performance networks. 5G cellular communication technology exhibits the readiness to provide such high quality communication channels by using various advanced technologies. Device to device communications is one of multiple technologies that have been suggested in 5G. By the employment of this technology, mobile devices can communicate with each other without the involvement of a base station (BS). This can eliminate congestion, expand coverage area and increase throughput. Communicating devices set up a multi-hop path using nearby devices which act as relaying elements, or routers. However, the Self-organizing nature and the lack of centralized control of D2D make it easier to launch multiple types of attacks. In this paper, an intrusion detection system IDS is proposed using machine learning techniques. Eight types of attacks are considered to train the system for intrusion detection, then, multiple classification algorithms have been compared. Finally, a multi-objective model has been designed based on the results of comparison to secure the communication process under D2D technology. The used dataset is generated using Network Simulator NS-2.

Povzetek: V članku je predstavljen sistem za odkrivanje vdorov (IDS) v komunikacijo naprava-naprava (D2D) v tehnologiji 5G, ki uporablja strojno učenje za prepoznavanje več vrst napadov.

1 Introduction

The massive growth in wireless communications poses many challenges to meet users' requirements. These requirements include the transmission of large data volumes, reliable communications and small response time. The need for these requirements increase dramatically, especially with the existence of Internet of Things (IoT) [27]. The result of the large number of communicating mobile devices is a fully overloaded, low performance or even a dis-functioning cellular networks [21]. The next generation of cellular networks, i.e. 5G, is a promising solution for the growing demand on high performance networks [9] as it utilizes a number of technologies including: multiple inputs multiple outputs (MIMO), mm-Waves, small cells, beam forming, full-duplex and device to device (D2D) communications [15] and [4], these technologies have come to fulfill the 5G promises.

Device to device communications can provide an efficient use of millimeter waves and better utilization of the available bandwidth. With D2D, the communication between two devices can be accomplished without the need for the involvement of a BS which may involve long distance communications. Any two devices can communicate depending on multiple small hops instead of two long hops, from the sender to (BS) and from (BS) to the receiver. Therefore, a User Equipment (UE) can either help other UEs to communicate without the need to contact a BS, as Figure 1 shows in the communication between devices (B) and (C), or a UE may assist another UE to communicate with BS, as depicted in Figure 1 between device (A) and (BS), even in the case where a UE is located out of the transmission range of the BS [34].

We can notice that there is a lack of researches investigating security in D2D cellular networks. That is, up to our knowledge, there is no research work that has considered security attacks resulted from the self-organizing nature of D2D devices where no centralized point is responsible for controlling communication process.Nevertheless, there are a number of researches considered other security problems such as [14] where a new key management approach is proposed to secure the communication process between devices in D2D technology. However, because there are many similarities between D2D technology and wireless ad hoc paradigm, security studies on ad hoc can be applied to D2D communications.

Intrusion detection in wireless environment networks be-

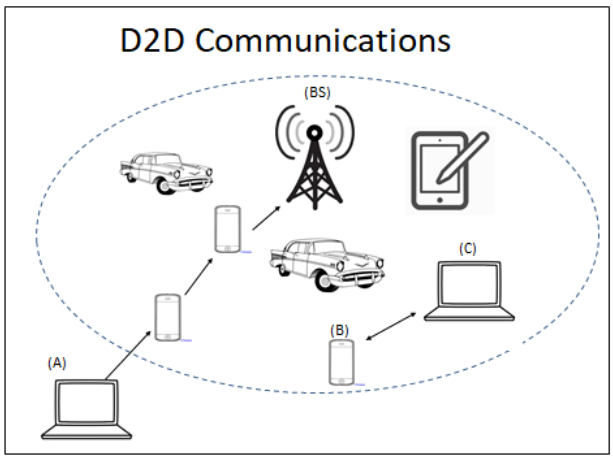

Figure 1: Communication in D2D technology

comes a very challenging task, especially with the emergence of the modern technologies where normal users can initiate the cellular communication process using their ordinary user equipment. That is, any user can advertise any piece of information to other users within the communication process regardless of the degree of authenticity or honesty of that user. This can imply a large amount of illegal actions which can arise and corrupt the functionality of such systems. Traditional systems which depend on pre-established rules to classify users' actions to normal versus malicious actions could be unable to perform efficiently as new attacks arise constantly. The more suitable choice is the use of data mining and machine learning techniques [11], where data can be collected and used to train a system how to discriminate normal behavior of a network from that with malicious actions.

In this paper, we suggest that a moderate database is established in each base station where the traffic is collected and analyzed based on a specially designed model to classify the network behavior to either normal or malicious. Consequently, taking the convenient procedure to secure the network. We have used NS-2 to simulate the D2D environment in order to create the dataset which contains normal network behavior as well as the behavior of eight attacks. Five classification algorithms have been compared to select the best classifier, including random forest, artificial neural networks, support vector machines, decision trees and Naïve Bayes. The suggested features are ordered based on the importance of each feature and have been tested to select the optimal subset of features for the final model. After the optimal classification algorithm, random forest, has been selected, it has been applied to design a general model to classify new types of attacks which have not been seen in the test dataset. Based on classification results, the proposed model is presented, discussed and has proved to provide a highly secured system.

The contribution of this work is summarized as follows:

1. A new dataset is generated using Network Simulator2, the dataset consists of 4200 instances, each instance represents either a normal network traffic or an attacked network traffic for a number of nodes within two minutes.
2. Multiple classification algorithms are tested to select the most appropriate classifier for the proposed IDS.
3. A complete intrusion detection model is proposed based on the selected classifiers.
4. The proposed model is tested and proved to be efficient in detecting both seen as well as unseen attacks.

This paper is organized as follows. A background for D2D technology, possible attacks, data mining field and classification algorithms is provided in Section 2. In Section 3 we discuss our methodology, experiment environment. Results are presented and discussed in Section 4. Section 5 presents the proposed intrusion detection model. Finally, conclusion is drawn in Section 6.

2 Background

In this section, a brief background is provided on D2D communication technology,its relation to ad hoc networks, security of D2D devices and types of possible attacks on D2D communication process.

2.1 D2D communications

The D2D is proposed for the first time in (3GPP Rel12) [35], the term D2D is suggested with the title (ProServ), which stands for Proximity based Services, and it was limited for the adjacent devices with only one hop. Afterward, the concept of D2D has evolved with 4G (LTE) for emergency services [19]. D2D can offer many advantages in cellular systems, this advantages include:

1. The ability to access communication services in the case of emergency or disaster situations [21], where nodes can relay info without connecting the disfunctioning cellular network.
2. Better utilization of the spectrum, by using millimeter waves and unlicensed spectrum [35], [31], [21] and [34].
3. Network coverage expansion, where the communication range can be expanded without adding additional BSs [35] and [21].
4. Optimizing Power consumption [15], [35], [31], [21] and [34].
5. Economic benefits, [15] by reducing the cost per bit and increasing revenue for operators [30] and [13].

6. Flexibility for traffic offloading [15].
7. Better exploitation of devices proximity [21].
8. Eliminating interference [35] and [25] due to the high path loss, which is defined as the attenuation of electromagnetic waves during propagation through space, path loss is considered as an advantage in D2D communications because concurrent communications can be carried out without interfering [4].
9. Eliminating congestion [35] because the traffic is distributed rather than accumulated around BS.
10. Diminishing data loss and the need for re-transmission which saves bandwidth [35].

These advantages implies a higher network performance in terms of throughput [35] and [31], latency [15], system capacity [12] and quality of service (QoS) [30], which can provide a significant advancement to a wide variety of uses. To encourage cellular network users to be participants in D2D technology, relaying D2D devices may be compensated with either a financial incentive or by provisioning services such as security during communication operation [30].

2.2 D2D communications and ad hoc networks

By studying the distinctions between D2D and ad hoc networks, we can conclude that D2D can easily operate in ad hoc mode. The most significant difference between D2D and ad hoc networks is that D2D can ask for some assistance from BS in some situations such as control, synchronization, path discovery [16], and resource allocation [18], while in ad hoc there are no such centralized assistance. Thus, D2D communication operation can be either controlled by a BS, or uncontrolled where each device perform a peer discovery.

In literature, the suitability of applying ad hoc routing on D2D is studied in [21] by implementing both AODV and DSDV in D2D communications. The results in [21] have shown that using ad hoc routing protocols with D2D is a promising approach for cellular communications. Additionally, AODV is proved as a convenient candidate for D2D. AODV has also shown better energy consumption for large scale D2D networks [26], and it has been suggested for D2D communications in [1] and [16]. In this paper, we have adopted AODV routing protocol to simulate D2D environment to create our own dataset for the proposed model training and testing.

2.3 Security in D2D communications

There is a lack in existing researches on the security of D2D communications technology. Up to our knowledge, there is no research that has considered possible attacks when applying D2D technology in cellular communications. Nevertheless, we cannot overlook security studies on ad hoc networks attacks which are highly linked to possible attacks on D2D. In this section we look over a number of existing researches related to IDSs in ad hoc networks. In [3], there is a summarized state of the art of IDSs in ad hoc networks. Multiple types of IDS are designed such as fuzzy logic based systems, and cross layer acknowledgement based systems. One major IDS type is the classification based IDS that depends on machine learning techniques. We consider this type as it is the most related type to our approach.

In [3] multiple classifiers are mentioned such as SVM, NN and NB, which have been proved to be the most efficient classifiers. In [7] different IDSs for ad hoc networks are investigated and classified into multiple types. The machine learning based IDS is discussed, the most common model for this type is Bayesian network, fuzzy logic, NN and GA. In this research, we are going to apply theses classifiers and compare them to select the most appropriate one for our model.

In [32], an IDS has been proposed for wireless mesh networks (WMN), which is a type of ad hoc networks. A dataset has been generated using NS3. Five attacks are targeted by the proposed IDS. Genetic algorithms have been used for feature selection, the main idea in [32] is that different set of features might be beneficial for each attack. Moreover, the proposed IDS is limited to the specified attacks. it does not discuss if it could be deal with further or unseen attacks. In [20] the notion of cooperative IDSs is discussed. An optimization problem for how long an IDS needs to remain active in mobile ad hoc network to achieve the higher protection as well as saving battery life is presented. In [29], an IDS is proposed based on clustering, where a cluster head is responsible for monitoring to detect attacks rather than individual nodes continuous monitoring which can lead to high depletion of node's battery life. In [23], a number of attacks have been considered based on the notion of the adaptive response mechanism depending on the fact that fixed response mechanisms have a lot of deficiencies related to the ability of detection and power consumption.

The use of machine learning in intrusion detection systems is also adopted in [5] where multiple classifiers are compared to construct an IDS for small smart home network, with eight connected devices, the proposed IDS has shown a promising results for a small network, it needs to be expanded to be applied for a wider network to prove the feasibility of using machine learning for such networks.

Despite the fact that the communication style of ad hoc networks is similar to D2D in many aspects, all IDSs of ad hoc depend on that fact that there is no centralized point to monitor traffic except cluster heads in cluster based ad hoc networks. Even in this type, clusters are often ordi-

nary nodes with limited capabilities. Most researches depend on host based detection which relies on the wireless node capabilities and traffic. However, in D2D, the main difference is the presence of base station, which can act as a centralized point and be utilized to monitor the overall traffic and to analyze this traffic and identify attacks if they occur. Table 1 summarizes the state of the art for security in literature, and highlights the main limitations in the state of the art. In this paper, we have considered these limitations. We have started from the security aspect by considering the most possible attacks and network variations as our first priority, then we consider the performance of machine learning algorithms and power consumption. We have also investigated the ability of the proposed IDS to detect new attacks. Moreover, we have consider moderate to large network sizes.

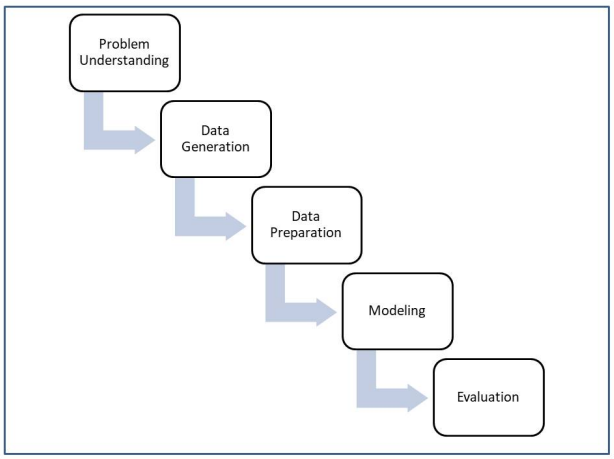

Figure 2: Main Steps of Proposed Methodology

3 Methodology

In this section, we discuss the methodology of this research and show the steps that we have gone through to develop our IDS. Figure 2 shows the block diagram of our methodology. As figure 2 shows , our methodology consists of five stages: problem understanding, data generation, data preparation, modeling, and evaluation. In the following subsections we provide a description of these stages.

3.1 Problem understanding

Internet of things is getting more and more acceptance and popularity by different categories of users. The free nature of (IoT) opens the door to a wide variety of attacks and makes them very easy to be launched [28]. In cellular communication, and particularly with D2D, it is very essential to detect these attacks in order to preserve communication process functioning efficiently by a robust and efficient IDS. To achieve this objective, this work proposes and design a data mining model to detect attacks as their occurrence in the network, and based on detection outcomes, the system behaves relying on a predefined plan to counter the malicious node.

3.2 Dataset generation

As D2D is an underdevelopment technology and up to our knowledge, we cannot find a real dataset for actual traffic. Therefore, we have generated this dataset using Network Simulator 2. In our conducted simulation experiments, we have selected AODV routing protocol [2], as it has been proved to be the most efficient routing protocol for D2D technology as it has been stated in [21].

We have conducted 4200 simulation scenario experiments, each within two minutes. 50-100 nodes are deployed within 1000mX1000m terrain area. Mobility speed has been varied from 0 m/s which denotes the static, immovable, nodes to 12m/s speed which denotes a node moving with 43 k/h which is equivalent the speed of driving a car in residential quarter. Table 2 illustrates the details of simulation environment.

Each instance of the generated dataset represents two minutes traffic of either 50 nodes or 100 nodes moving with either (0-3)m/s, (3-6)m/s,(6-9)m/s or (9-12)m/s. Part of this dataset represents normal network behaviour, the remaining instances represent the traffic with the aforementioned attacks launched. After the simulation has been conducted for the 4200 instances, performance has been measured in terms of predefined metrics which are considered as dataset features. In the next section we briefly discuss the proposed features that have been considered as inputs to the classification algorithm.

3.3 Feature extraction

After the simulation have been conducted, we have proposed a number of traffic properties to be considered as input features for classification algorithms.Table 3 shows our proposed features with a brief description for each feature. These features can be measures from trace files that have been resulted from the simulation. Trace files act as detailed log files for all communications in a given scenario. Trace files are analyzed to calculate the aforementioned features.

Figure 3 depicts a part of the final dataset.In Figure 3 we can see the aforementioned features of Table 3 as well as two class labels. we have considered two class labels since we will produce two models as we will discuss later.

3.4 Data preparation

As the dataset has been generated from a simulation tool, we was able to control data format by building output features as needed. The only pre-processing that have been needed was dealing with missing values by deleting instances which contain null or infinite values. By this step we have our final dataset version ready to be an input to

Table 1: Security in literature

Paper	Target NT Type	Goals	Limitations
(Alnaghes et. al)	Ad Hoc	Comparison between existing classifiers	Do not consider security aspects. (Just ML enhancement)
(Vijayanand et. al)	Wirels Mesh Networks	Feature Selection	Limited to 5 attacks . Do not considers unseen attacks
(Marchang et. al)	Ad Hoc	Studying how long an IDS need to be active	Limited to enhance battery life aspects and activation time of IDS.
(Subba et. al)	Clustered WSNs	Battery life IDS based on cluster heads	Cluster heads are normal nodes which means that monitoring can lead to battery depletion.
(Nadeem et. al)	Ad Hoc	Adaptive IDS to save battery	Battery life is the main consideration rather than security itself
(Anthi et. al)	Ad Hoc	Comparison of classifiers performance within a smart home environment	Limited to small networks (8 devises only)

Table 2: Simulation Environment

Simulation Parameter	Value
Simulator	NS2
Routing ProtocOl	AODV
Transport Layer Protocol	TCP
Simulation Duration	120 seconds
Number of UEs	50,100 nodes
Mobility Speed	(0-3, 3-6, 6-9, 9-12)
Terrain area	1500X1500 m2

classification algorithms. The class distribution of the final dataset is shown in figure 4 . The next step is to perform feature selection, the main target of applying feature selection here is to use as less features as possible to reduce computational cost. We have adopted a simple feature selection approach using R language which is a programming language used for statistical computations [8]. We have utilized R language to order the proposed 14 features according to feature importance in random forest classifier and using R importance function. Figure **??** shows features ranking using R importance function in random forest classifier, which will be discussed in details later.

3.5 Modeling

As the dataset has become ready for classification process, we have to select the most appropriate classification algorithm, we decided to compare multiple classifiers in order to select the best one based on classification outcomes. The compared classifiers have been chosen based on the previously designed IDSs. As denoted before, multiple classifiers are implemented in the literature such as support vector machines, K-nearest neighbors, artificial neural networks, decision trees and Naive Bayes and they have been proven to be efficient in developing IDSs [3]. Therefore, we have selected theses classifiers to be compared, then we propose to add random forest as it is considered as a promising classifier, specially in intrusion detection systems [24] and [22]. The target of this step is to find the best prediction model to get a high performance IDS. WEKA Environment for Knowledge Analysis version 3.8.3 has been used to apply the aforementioned classification algorithms and compare the results objectively.

In this research, our objective is to build two IDSs models, the first model is the binary classification model which classifies network traffic to either normal or abnormal where abnormal denotes the occurrence of an attack. On the other hand, the second model target is to specify attack name and type. In this paper, we will make our experiments based on each of these two models separately. Finally, we will integrate these two models into one multi-objective IDS.

WEKA is considered as a comprehensive collection of machine learning algorithms as well as data pre-processing tools. It is one of most common data mining tools [10]. The main advantages of using WEKA is that it contains a wide variety of algorithms , it provides the most necessary performance measurements, and it has a simple graphical user interface, which makes it easy to be utilized in data mining researches.

3.6 Evaluation

To evaluate the performance of of the selected classifiers to be compared, we have considered the most common evaluation parameters of classification algorithms. These performance metrics include: classification accuracy, sensitivity, specificity, G-means and AUC. The first four measure-

Table 3: Description of dataset features.

Abbreviation	Term	Description	Range
E2E	End to end delay	time elapsed between sending and receiving a packet	Between 0 to infinity
DUP	Duplicated packets	the number of packets that have been sent more than once	between 0 to infinity
OH	Overhead	the number of control packets sent	0 to infinity
SENT	Sent packets	the number of packets have been initiated by all sources	0 to infinity
RCVD	Received packets	the number of packets have been received by intended destinations	0 to infinity
LOST	Lost packets	the number of packets sent from their source and have not been delivered to final destination	0 to infinity
FWD	Forwards	the number of forwards for all transmitted packets by all intermediate nodes	0 to infinity
THRPUT	Throughput	the number of delivered packets per second	0 to infinity
RET	Re-transmissions	the number of packets that have been re-transmitted based on an error	0 to infinity
PDR	Delivery Ratio	received packets/sent packets	0 to 1
PATH	Path Length	average number of hops from source to destination for all transmitted packets	0 to the total number of nodes
TIME	Time	the time when the last packet has been sent or received	0 to 120
SPEED	Mobility Speed	The Maximum mobility speed of the mobile nodes	0 to 12
DENS	Density	Number of nodes per 1000m X 1000m	50,100

ments are based on the confusion matrix.

4 Experiments and results

In this section, we discuss the experiments that we have conducted based on the methodology described in Figure 2 and using the generated dataset. We consider the following experiment scenarios.

– **Scenario 1**: The standard classifiers k-NN, DT, NB and NN, RF, SVM are applied for the entire dataset without feature reduction, that is, the 14 features are considered as inputs to all classification algorithms. Accordingly, multiple performance metrics are measured. Figure 5 depicts accuracy, recall, Gmean, F-measure and AUC for the aforementioned classifiers. From Figure 5, we can notice that random forest do well in terms of all performance metrics and it achieves the higher level of performance. WEKA Environment for Knowledge Analysis version (3.8.3) has been used for all comparison experiments. For Naive Bayes, random forest, support vector machine and J48 decision trees, we have used their Java implementations in WEKA. For k-NN, K is set to 1 as this value produced the best output. For artificial neural networks, the number of hidden layers is set to 2, we have selected 2 as it is considered to be sufficient with simple data sets.

– **Scenario 2**: After the initial evaluation of the best classification algorithms to be used in our IDS, we have concluded that random forest is the most appropriate classifier, so, we have used R language random forest importance function to rank the dataset features. The outcomes of the ranking process are presented in Figure **??**. We have considered this ranking to apply

E2E	sent packets	receved packets	PDR	lost	throughput	Avg Path	Overhead	time	DUP	retransmissions	forwards	DENS	max spee	class	binary class
0.07	28446	28402	99.85%	44	236.685	1.00461	9521	120	54	290	24831	50	3	jellyfish	attack
0.07	28446	28402	99.85%	44	236.685	1.00461	9521	120	54	290	24831	50	3	jellyfish	attack
0.07	28446	28402	99.85%	44	236.685	1.00461	9521	120	54	290	24831	50	3	normal	normal
0.07	28446	28402	99.85%	44	236.685	1.00461	9521	120	54	290	24831	50	3	normal	normal
0.08	25366	25319	99.81%	47	210.997	1.00952	22656	120	220	1475	138924	50	9	wormhole	attack
0.06	27245	27191	99.80%	54	226.592	1.00121	15742	120	524	483	35595	100	3	cache poison	attack
0.07	24060	24011	99.80%	49	200.092	1.00033	17034	120	2	832	53216	100	6	cache poison	attack
0.07	25662	25608	99.79%	54	213.404	1.00676	21237	120	138	916	117502	50	9	hellofloding	attack
0.12	21838	21790	99.78%	48	181.585	1.32524	8475	120	188	125	14256	50	3	hellofloding	attack
0.12	21838	21790	99.78%	48	181.585	1.32524	8475	120	188	125	14256	50	3	hellofloding	attack
0.12	21838	21790	99.78%	48	181.585	1.32524	8475	120	188	125	14256	50	3	hellofloding	attack
0.08	28199	28134	99.77%	65	234.454	1.00778	7968	120	4	338	10080	50	3	cache poison	attack
0.11	22039	21987	99.76%	52	183.228	1.31164	8181	120	156	186	13081	50	3	blackhole	attack
0.1	33720	33640	99.76%	80	280.341	1.19741	20081	120	186	1512	80464	100	3	jellyfish	attack
0.12	26096	26031	99.75%	65	216.927	1.08724	8955	120	336	646	20869	50	3	wormhole	attack
0.12	26096	26031	99.75%	65	216.927	1.08724	8955	120	336	646	20869	50	3	wormhole	attack
0.12	26096	26031	99.75%	65	216.927	1.08724	8955	120	336	646	20869	50	3	wormhole	attack
0.08	27262	27191	99.74%	71	226.598	1.01872	9244	120	60	296	20523	50	3	normal	normal

Figure 3: A shot of the generated data set

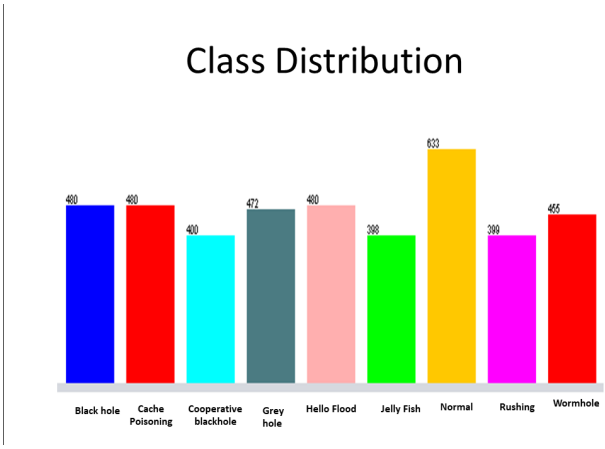

Figure 4: Class distribution of the generated data set

feature selection. We have simply removed the x least importance features and observe the performance of the target classifiers. x has been varied to find the optimal number of features to be removed in order to get the best performance. We have started with removing 4 features and keeping 10, then we have removed 8 and 12 features to keep 6 and 2 features, respectively.

In scenario 2, the same classifiers applied in scenario 1 are also applied using the same instances and parameter settings with varying the removed features. The target of the second scenario is to quantify the improvement in the performance of each classifier when the number of features is reduced. Thereafter, the main target is to use as less features as possible while getting the higher performance to optimize the proposed IDS in terms of computational cost. Figure 6 shows the steps of scenario 2.

4.1 Experimental setup

In this section we discuss the experiments which have been conducted to design the final model. The aforementioned classification algorithms, namely k-NN, DT, NB, NN , SVM and RF, are trained and tested based on 10-fold cross validation technique. In 10-fold cross validation, the dataset is divided into 10 equal parts, thereafter, training is carried out on nine parts and tested on the remaining one part. Training and testing are repeated ten times such that in each time the test part is changed. Finally, average of all test results is reported.

When 10-Fold cross validation is used, we can guarantee that the entire dataset is eventually used for both training and testing. Moreover, we ensure that stratified sampling is achieved by creating the 10 folds such that in each fold, class distribution is close as possible to the dataset distribution. Here, stratified sampling is very important to get better results in terms of bias and variance [17].

4.2 Experiment I: binary classification with all features dataset

In this experiment, our selected classification algorithms are applied to the generated dataset without removing any feature. Our target here is to evaluate the performance of all classifiers to determine if there is an attack or not using all features proposed. Results are depicted in the column chart of Figure 5. By examining the results, we notice that we can achieve a very high classification accuracy under most classifiers. We notice also that the lowest performance classifier is NB classification algorithm, this is due to the fact

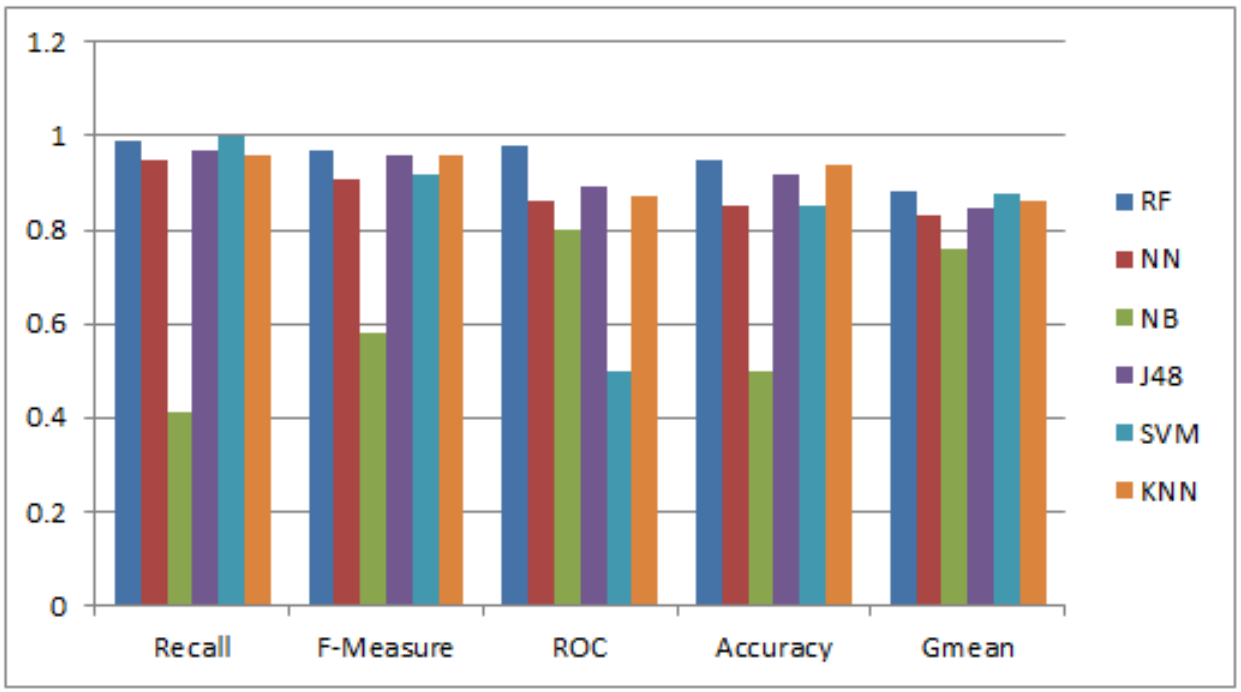

Figure 5: Binary classification performance of classification algorithms for the entire dataset

that the proposed features cannot be independent, they almost depend on each other.Delivery ratio for example is derived from the other two features, namely, sent and received packets. As another example, lost is the result of abstracting sent packets and received packets. In NB, the classification is built on the assumption that features are independent from each other [6]. As we can see, our generated dataset violates this assumption, therefore NB classifiers have the worst performance. In the next experiment we are going to compare all classifiers in terms of a number of performance metrics, however, we are going to a apply feature selection based on the performance-wise ranking shown in Figure **??** in order to optimize performance as well as the computation cost.

4.3 Experiment II: binary classification with feature selection

This experiment targets the process of determining if there is an attack or not. In this experiment, to optimize the performance and communication cost of the final classification model for our IDS, first, we have applied the R performance function order of the suggested 14 attributes. The result of ordering process for binary classification is shown in the left-hand table of Figure **??**. Then we have tried to remove the least importance features, unnecessary features increase computational cost and time and may hamper classification process which limits performance.
To identify the optimal number of features to be removed, we have tried different removal ratios to get the best model. We experienced the performance of selected classifiers by training them on datasets with different features, starting with full features dataset which produced results shown in Figure 5. Then, we have tried to remove the lowest 4,8 and 12 features and keeping the higher 10, 6, and 2 higher importance features, respectively. We have measured accuracy, root-mean-square-error, area under curve curve, recall, f-measure and g-mean. Figure 7 up to Figure 12 show the evaluation results of this experiment.

In Figure 7, we can see that feature reduction did not affect classification accuracy significantly for all used classifiers except with NB which is the only classifier that has been improved in terms of accuracy with 40% approximately which was achieved by applying classification with the only two higher importance features, duplication and lost packets.

The same performance has been noticed in Figure 8, Figure 9, Figure 10, Figure 11 and Figure 12, for recall, f-measure, area under curve, G-mean and root mean square error, respectively. Results of theses figures indicate that it is still easy for random forest, decision trees and K-nearest neighbor classifiers to identify attacks which represent majority in the dataset.on the other hand naive Basie and support vector machine have the worst classification performance [33].

We have noticed that random forest classifier has achieved the best performance in f-measure (97%), accuracy (95%) and AUC (98%), while it was the second best

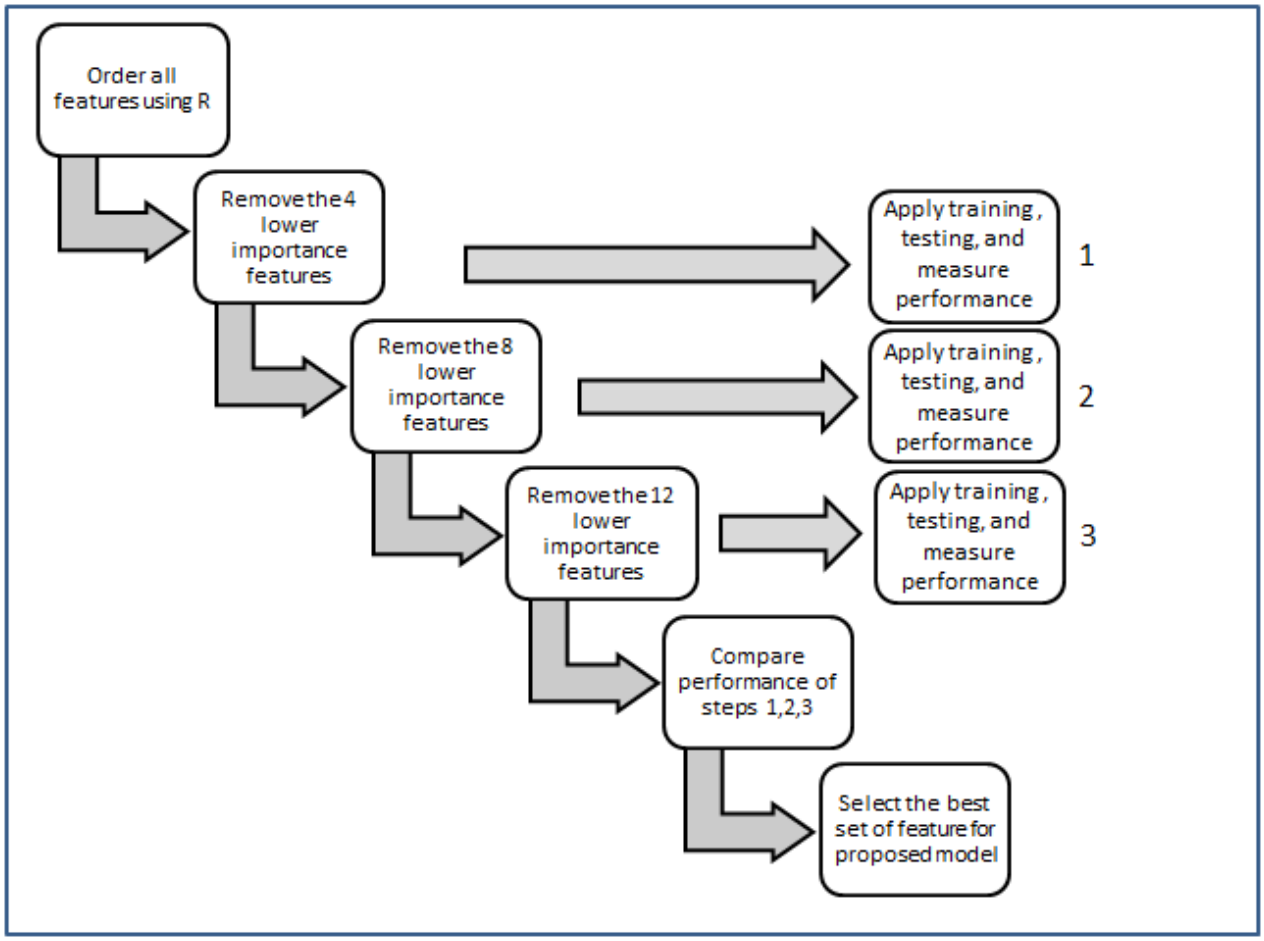

Figure 6: steps of feature selection

classifier in terms of Gmean (89%) and mean-square error(10%) metrics. We conclude that removing the least importance features did not significantly affect classification performance while it is guaranteed to limit computation cost. The aforementioned performance ratio of random forest indicates that it can identify an attack with a ratio of 95%.

As a conclusion of this experiment, random forest model is the best model for intrusion detection. This conclusion was made based on the values of accuracy, which is referred to as detection rate and considered as the most important metric in intrusion detection systems. This conclusion will be adopted in our final model.

4.4 Experiment III: attack based classification with feature selection

In this experiment our target is to exactly specify the type of attack launched, so, we have repeated steps of experiment II in order to optimize performance and communication cost of the final classification model for our IDS. we have started with applying the R performance function to order the 14 attributes. The output of the ordering process for attack classification is shown in the right-hand table of Figure **??**. Next, we have tried to remove the least importance features. As in experiment II, we have tried to remove different number of features and measuring the performance, starting with full features dataset which results are presented in Figure 13. Then, we have tried to remove the lowest 4,8 and 12 features and keeping the higher 10,6,and 2 higher importance features, respectively. classification is applied for the remaining features to identify the type of the attack. We have measured accuracy, root-mean-square-error, area under curve curve, recall,f-measure and g-mean. Figure 14 up to Figure 19 show the evaluation results of this experiment.

In Figure 14, we can see that feature reduction did not affect considerably classification accuracy for the three higher classifiers which are (RF,KNN, and J48). These three classifiers have shown the best accuracy, between (75% and 85%). The remaining classification algorithms have shown a significantly lower accuracy for attack specification (lower than 55%).

Similar performance has been noticed in Figure 15, Figure 16 , Figure 17 and Figure 18 for recall, f-measure, area

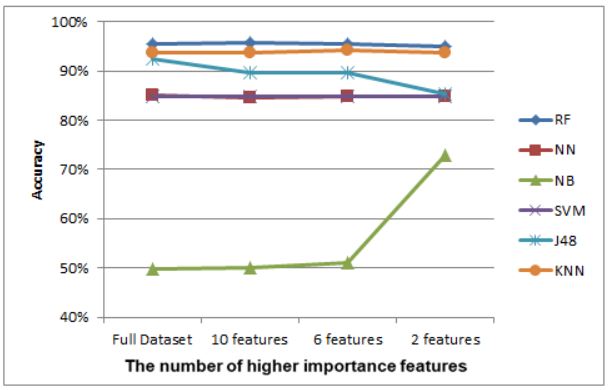

Figure 7: Accuracy of classification algorithms for the different datasets

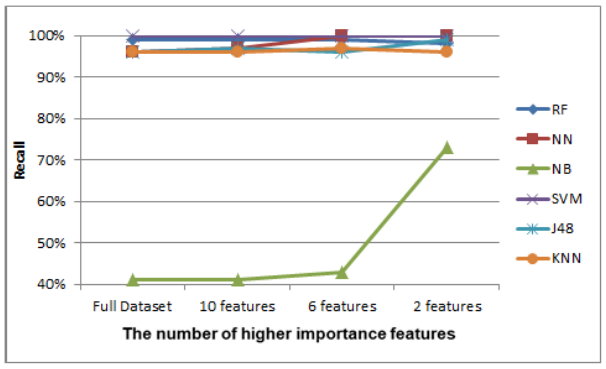

Figure 8: Recall of classification algorithms for the different datasets

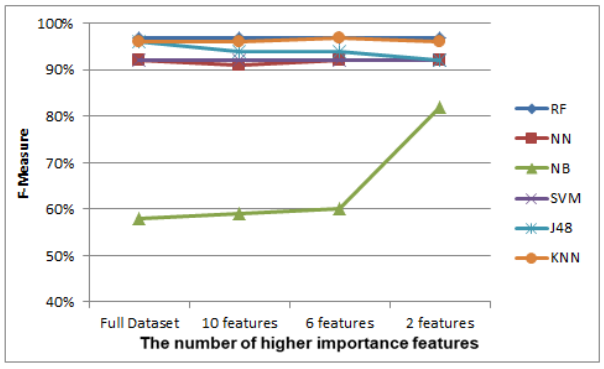

Figure 9: F-measure of classification algorithms for the different datasets

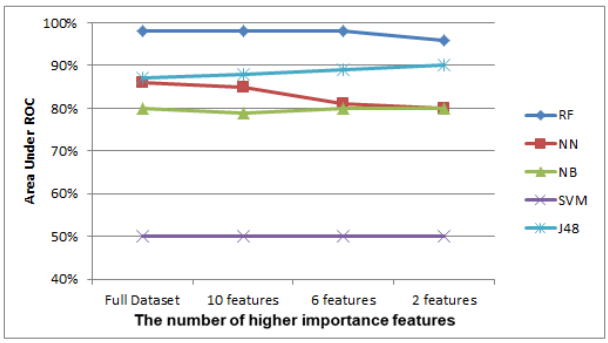

Figure 10: Area under curve of classification algorithms for the different datasets

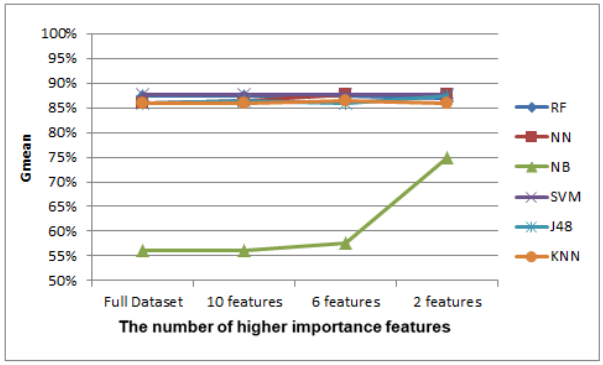

Figure 11: Gmean for classification algorithms for the different datasets

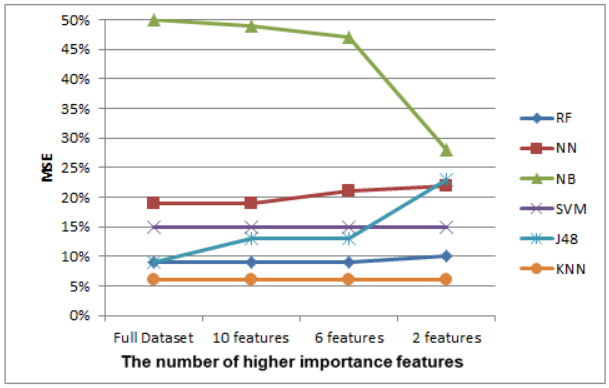

Figure 12: Root mean square error of classification algorithms for the different datasets

under curve and Gmean, respectively, where the dominated observations of these metrics for the experienced classifiers are that RF,KNN and J48 have the highest performance in terms of these metrics. Random forest is the best of them with 80%, 82%, 98% and 90% for each of recall, f-measure, area under curve and Gmean, respectively.

The next observation is that classification with all features included has the best performance. Finally, the last observation is related to NN, which shows an improvement of performance with feature reduction until we remove 8 features and keep 6. With less than 6 features, we notice a sig-

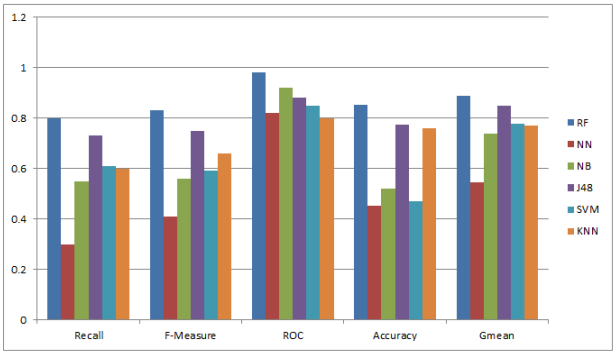

Figure 13: Attack classification performance of classification algorithms for the entire dataset

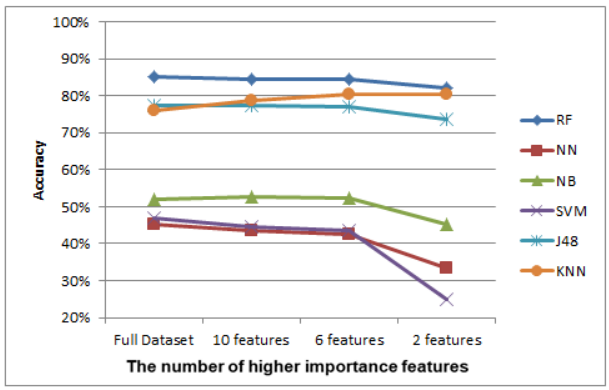

Figure 14: Accuracy of classification algorithms for the different datasets

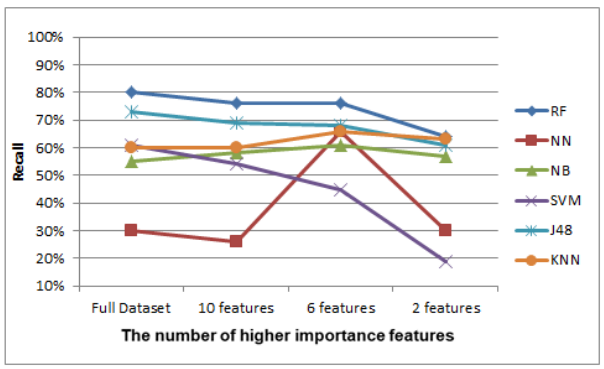

Figure 15: Recall of classification algorithms for the different datasets

nificant drop of performance metrics for NN particularly.

Figure 19 shows the root mean square error metric for experimented classification algorithms, results seem to be different for this metric because we notice that there are no significant improvement as features are eliminated, moreover, random forest classifier has achieved the lower

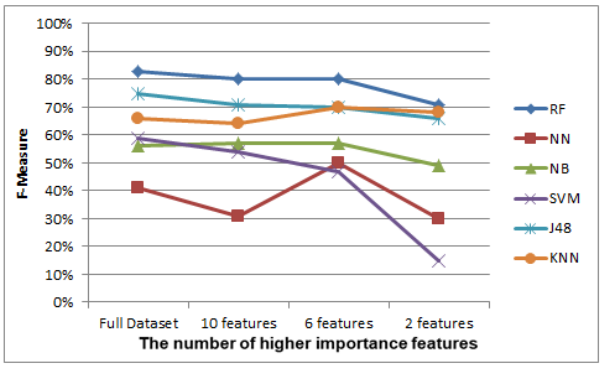

Figure 16: F-measure of classification algorithms for the different datasets

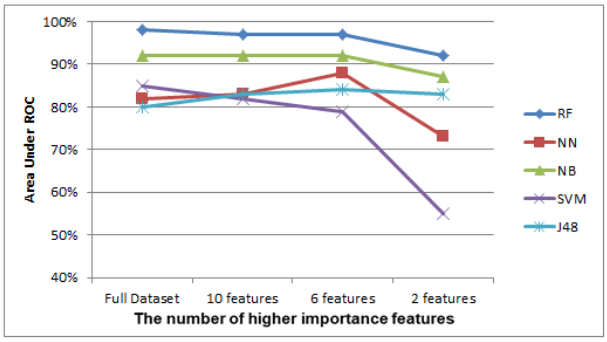

Figure 17: Area under curve of classification algorithms for the different datasets

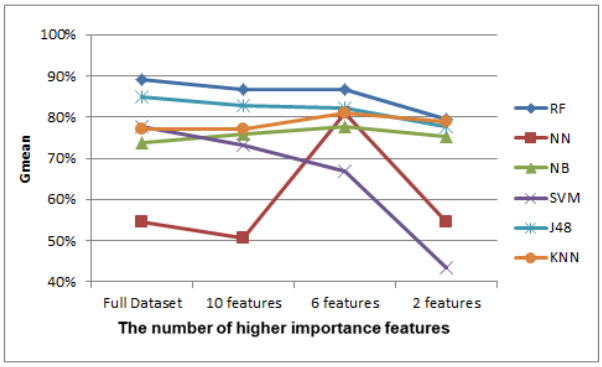

Figure 18: G-mean for classification algorithms for the different datasets

root mean square error with 16% using all features.

In this experiment, we can conclude that random forest is the most suitable classifier to be considered in our proposed IDS. In the next experiment, we are going to integrate results and conclusions of these three experiments to provide the final model of the proposed IDS.

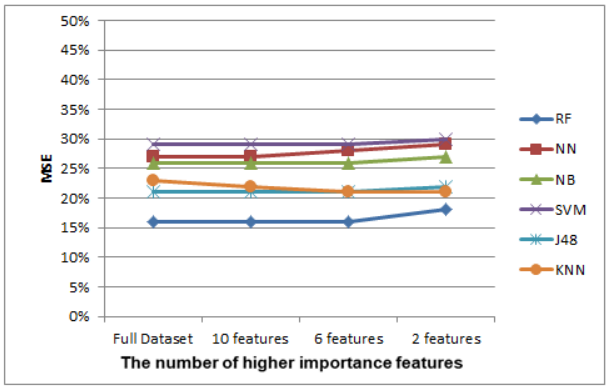

Figure 19: Root mean square error of classification algorithms for the different datasets

4.5 Experiment VI: detection unseen attacks

AS the number of users increases and new technologies are taking place with the emergence of Internet of Things, new attacks are continuously occur. In this section, we are going to test the ability of random forest classifier to detect new attacks which have not been included in the training dataset.

We have selected random forest based on the previous experiments which have shown that it is the most appropriate classification algorithm. We have divided our dataset into two parts, training and testing datasets. In testing dataset, we have included instances for only two attacks, A and B, as well as normal instances. On the other hand, the training dataset include all attacks except A and B.

The target is to measure the ability of the classifier to recognize new attacks such that it has not been trained on. We have tried this experiment 4 times with different values of A and B to cover all attacks. Table 3 shows the performance of random forest classifier during four conducted experiments in terms of accuracy, recall, F-measure and area under curve. From Figure 3, we can notice that random forest is able to detect 86% of unseen attacks, which is represented by the average recall metric. Detection ratio is also near 86% which represents the classifier's ability to distinguish normal network behaviour from attacks. F-measure and area under curve metrics achieved 84% and 79%, respectively, which are considered as acceptable detection for unseen and emerged attacks.

5 Intrusion detection model for D2D communications

In this section we integrate outcomes of the conducted experiments to provide a design for a complete intrusion detection system for D2D communications. Figure shows the IDS design for a cellular network. This model suggests to add a spatio-temporal database system, which is used in wireless communication networks, and only for a short time-span within a geographic region. By adding the spatio-temporal database to the cellular system, traffic of all nodes connecting to a base-station is temporally stored in the aforementioned database. From this database, we can extract the features of our proposed dataset. Classification algorithm, random forest, which has been selected based on this research can be applied periodically, e.g. every two minutes, in the initial step, random forest performs binary classification to determine if there is an attack. If no attack is detected, there is nothing to do, otherwise, if an attack is detected, a second classification is applied to determine its type. When the attack is specified, the appropriate response is determined by either disabling D2D communication and returning to the usual cellular communication paradigm, or by enabling one of the detection or mitigation techniques. Response of detecting an attack represents a separate and complementary part of our designed IDS.

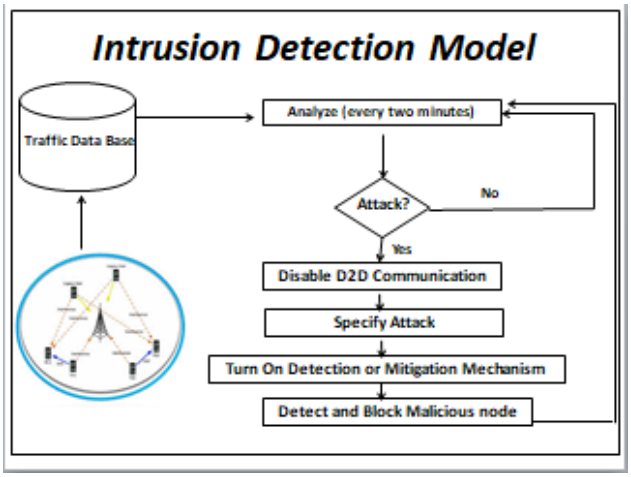

Figure 20: Intrusion Detection Model for a cellular network with D2D communications

6 Conclusion

According to the increasing number of internet users and the emergence of new technologies, the number of cybersecurity attacks increases. The existence of an intrusion detection system becomes a high necessity. Detection and mitigating techniques are often provided at the expense of some cost such as, delay, additional equipment, overhead, and so on. The employment of machine learning techniques help to detect intrusions based on the existing knowledge and data, and without adding any extra cost.

In this research, the target was to use classification algorithms in intrusion detection for D2D communications. First, we have generated our own dataset using NS-2 simulator, then, we have compared multiple classification algorithms to select the most appropriate classifier to be used in our IDS. We have also applied a simple feature selection based on feature importance estimated using R language.

Table 4: Performance results of unseen attacks

Exp No.	Unseen Attacks	Accuracy	Recall	F-Measure	AUC
1	Rushing + Wormhole	86.30%	0.863	0.866	0.898
2	Blackhole + Cachepoisoning	84.10%	0.841	0.864	0.631
3	Hellofloding+Jellyfish	99.60%	0.997	0.991	1
4	Cooperative BH + Greyhole	75.20%	0.752	0.646	0.66
	Average	86.30%	86.33%	84.18%	79.73%

Main limitations in the SOTA	Main improvements in this work
Do not consider security aspects. (Just ML enhancement)	Security is considered as the first priority and the most possible attacks are implemented
Do not considers unseen attacks	Unseen attacks are considered to test the ability of the system to detect new attacks
Limited to enhance battery life aspects and activation time of IDS.	Battery and power consumption are not the main consideration as they present a less severe issue in D2D communications.
Limited to small networks	The study includes large to medium networks and variety of mobility speeds and static networks

Figure 21: Contribution of this work as compared to SOTA

Figure 21 dpicts the main contribution of this paper as compared to previous research in the SOTA (State Of The Art)

Experiments indicated that random forest is the most appropriate classification algorithm to be used for our IDS. It has proved a 97% detection rate for binary classification, and 85% accuracy in attack type identification. Finally, we have provided a suggested design for an IDS of a cellular network.

References

[1] S. A. Abd, S. Manjunath, and S. Abdulhayan. "Direct Device-to-Device communication in 5G Networks". In: *Computation System and Information Technology for Sustainable Solutions (CSITSS), International Conference on*. doi: 10.1109/CSITSS.2016.7779425. IEEE. 2016, pp. 216–219.

[2] W. Almobaideen and D. AlKhateeb. "CSPDA: Contention and stability aware partially disjoint AOMDV routing protocol". In: *Cross validation2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)*. doi: 10.1109/AEECT.2015.7360548. IEEE. 2015, pp. 1–6.

[3] M. S. Alnaghes and F. Gebali. "A Survey on Some Currently Existing Intrusion Detection Systems for Mobile Ad Hoc Networks". In: *The Second International Conference on Electrical and Electronics Engineering, Clean Energy and Green Computing (EEECEGC2015)*. Vol. 12. 2015. URL: `https://api.semanticscholar.org/CorpusID:54682924`.

[4] R. I. Ansari et al. "5G D2D networks: Techniques, challenges, and future prospects". In: *IEEE Systems Journal* (2017). doi: 10.1109/JSYST.2017.2773633.

[5] E. Anthi et al. "A supervised intrusion detection system for smart home IoT devices". In: *IEEE Internet of Things Journal* 6.5 (2019). doi: 10.1109/JIOT.2019.2926365, pp. 9042–9053.

[6] M. Bramer. *Principles of data mining*. Vol. 180. doi: 10.2165/00002018-200730070-00010. Springer, 2007.

[7] I. Butun, S. D. Morgera, and R. Sankar. "A survey of intrusion detection systems in wire-

less sensor networks". In: *IEEE communications surveys & tutorials* 16.1 (2014). doi: 10.1109/SURV.2013.050113.00191, pp. 266–282.

[8] M. J. Crawley. *The R book*. doi: 10.1002/9781118448908. John Wiley & Sons, 2012.

[9] A. Habbal, S. I. Goudar, and S. Hassan. "A Context-aware Radio Access Technology selection mechanism in 5G mobile network for smart city applications". In: *Journal of Network and Computer Applications* 135 (2019). doi: 10.1016/j.jnca.2019.02.019, pp. 97–107.

[10] M. Hall et al. "The WEKA data mining software: an update". In: *ACM SIGKDD explorations newsletter* 11.1 (2009). doi: 10.1145/1656274.1656278, pp. 10–18.

[11] K. M. Harahsheh and C.-H. Chen. "A survey of using machine learning in IoT security and the challenges faced by researchers". In: *Informatica* 47.6 (2023). doi: 10.31449/inf.v47i6.4635.

[12] Z. Hashim and N. Gupta. "Futuristic device-to-device communication paradigm in vehicular ad-hoc network". In: *Information Technology (InCITe)-The Next Generation IT Summit on the Theme-Internet of Things: Connect your Worlds, International Conference on*. doi: 10.1109/INCITE.2016.7857618. IEEE. 2016, pp. 209–214.

[13] Y. Jung, E. Festijo, and M. Peradilla. "Joint operation of routing control and group key management for 5G ad hoc D2D networks". In: *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*. doi: 10.1109/PRISMS.2014.6970602. IEEE. 2014, pp. 1–8.

[14] M. A. Kandi et al. "A versatile Key Management protocol for secure Group and Device-to-Device Communication in the Internet of Things". In: *Journal of Network and Computer Applications* 150 (2020). doi: 10.1016/j.jnca.2019.102480, p. 102480.

[15] U. N. Kar and D. K. Sanyal. "An overview of device-to-device communication in cellular networks". In: *ICT Express* (2017). doi: 10.1016/j.icte.2017.08.002.

[16] B. Kaufman and B. Aazhang. "Cellular networks with an overlaid device to device network". In: *Signals, Systems and Computers, 2008 42nd Asilomar Conference on*. doi: 10.1109/ACSSC.2008.5074679. IEEE. 2008, pp. 1537–1541.

[17] R. Kohavi et al. "A study of cross-validation and bootstrap for accuracy estimation and model selection". In: *Cross validation*. Vol. 14. Montreal, Canada. 1995, pp. 1137–1145. URL: `https://www.ijcai.org/Proceedings/95-2/Papers/016.pdf`.

[18] X. Lin et al. "An overview of 3GPP device-to-device proximity services". In: *IEEE Communications Magazine* 52.4 (2014). doi: 10.1109/MCOM.2014.6807945, pp. 40–48.

[19] J. Liu et al. "Device-to-device communication in LTE-advanced networks: A survey". In: *IEEE Communications Surveys & Tutorials* 17.4 (2015). doi: 10.1109/COMST.2014.2375934, pp. 1923–1940.

[20] N. Marchang, R. Datta, and S. K. Das. "A novel approach for efficient usage of intrusion detection system in mobile Ad Hoc networks". In: *IEEE Trans. Vehicular Technology* 66.2 (2017). doi: 10.1109/TVT.2016.2557808, pp. 1684–1695.

[21] P. Masek, A. Muthanna, and J. Hosek. "Suitability of MANET routing protocols for the next-generation national security and public safety systems". In: *Conference on Smart Spaces*. doi: 10.1007/978-3-319-23126-$6_2$2. Springer. 2015, pp. 242–253.

[22] Y. Meidan et al. "Detection of unauthorized iot devices using machine learning techniques". In: *arXiv preprint arXiv:1709.04647* (2017). doi: 10.48550/arXiv.1709.04647.

[23] A. Nadeem and M. P. Howarth. "An intrusion detection & adaptive response mechanism for MANETs". In: *Ad Hoc Networks* 13 (2014). doi: 10.1016/j.adhoc.2013.08.017, pp. 368–380.

[24] F. A. Narudin et al. "Evaluation of machine learning classifiers for mobile malware detection". In: *Soft Computing* 20.1 (2016). doi: 10.1007/s00500-014-1511-6, pp. 343–357.

[25] J. Qiao et al. "Enabling device-to-device communications in millimeter-wave 5G cellular networks". In: *IEEE Communications Magazine* 53.1 (2015). doi: 10.1109/MCOM.2015.7010536, pp. 209–215.

[26] S. Riaz, H. K. Qureshi, and M. Saleem. "Performance evaluation of routing protocols in energy harvesting D2D network". In: *Computing, Electronic and Electrical Engineering (ICE Cube), 2016 International Conference on*. doi: 10.1109/ICECUBE.2016.7495233. IEEE. 2016, pp. 251–255.

[27] H. Saadeh et al. "Hybrid SDN-ICN Architecture Design for the Internet of Things". In: *2019 Sixth International Conference on Software Defined Systems (SDS)*. doi: 10.1109/SDS.2019.8768582. IEEE. 2019, pp. 96–101.

[28] J. Sengupta, S. Ruj, and S. D. Bit. "A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT". In: *Journal of Network and Computer Applications* 149 (2020). doi: 10.1016/j.jnca.2019.102481, p. 102481.

[29] B. Subba, S. Biswas, and S. Karmakar. “Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation”. In: *Engineering Science and Technology, an International Journal* 19.2 (2016). doi: 10.1016/j.jestch.2015.11.001, pp. 782–799.

[30] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu. “Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions”. In: *IEEE Communications Magazine* 52.5 (2014). doi: 10.1109/MCOM.2014.6815897, pp. 86–92.

[31] M. Usman et al. “A software-defined device-to-device communication architecture for public safety applications in 5G networks”. In: *IEEE Access* 3 (2015). doi: 10.1109/ACCESS.2015.2479855, pp. 1649–1654.

[32] R. Vijayanand, D. Devaraj, and B. Kannapiran. “Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection”. In: *Computers & Security* 77 (2018). doi: 10.1016/j.cose.2018.04.010, pp. 304–314.

[33] D. Wang and G. Xu. “Research on the detection of network intrusion prevention with SVM based optimization algorithm”. In: *Informatica* 44.2 (2020). doi: 10.31449/inf.v44i2.3195.

[34] L. Wei et al. “Energy efficiency and spectrum efficiency of multihop device-to-device communications underlaying cellular networks”. In: *IEEE Transactions on Vehicular Technology* 65.1 (2016). doi: 10.1109/TVT.2015.2389823, pp. 367–380.

[35] V. Yazıcı, U. C. Kozat, and M. O. Sunay. “A new control plane for 5G network architecture with a case study on unified handoff, mobility, and routing management”. In: *IEEE communications magazine* 52.11 (2014). doi: 10.1109/MCOM.2014.6957146, pp. 76–85.