International Journal of Technology 14(3) 549-560 (2023)
Received July 2020 / Revised November 2020 / Accepted July 2022

International Journal of Technology

http://ijtech.eng.ui.ac.id

Performance Evaluation of Anomaly Detection System on Portable LTE Telecommunication Networks Using OpenAirInterface and ELK

Yeremia Nikanor Nugroho[1], Ruki Harwahyu[1], Riri Fitri Sari[1*], Navid Nikaein[2], Ray-Guang Cheng[3]

[1]*Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok 16424, Indonesia*
[2]*EURECOM, Sophia Antipolis, Biot 06410 , France*
[3]*National Taiwan University of Science and Technology, Taipei City 106335, Taiwan*

Abstract. Anomaly detection (AD) is a solution for cellular operators to overcome the difficulty of quality control over the proliferation of cellular phone usage. The telecommunications network monitoring system with anomaly detection enables immediate discovery of problems before they become more complex. Monitoring activities produce logs, which are then analyzed according to the interest, often with the help of statistics and visualizations. Relying on humans for analysis is increasingly difficult due to the immense amount of logs in modern telecommunication networks. This work extends the monitoring to automated anomaly detection by using various ELK modules to form an intelligent monitoring system. A testbed based on OpenAirInterface (OAI) and USRP B210 radiohead is used, which includes the functionalities of HSS, MME, SGW, PGW, eNB, and UE. The proposed system has an average accuracy of 91.5%. This is supported by an average value of the proportion of normal conditions that are correctly predicted at 99.31%. On the other hand, the system can still maintain the functionality of the cellular telecommunications network with an excellent predicate on service quality.

Keywords: Anomaly detection; Elasticsearch-Logstash-Kibana stack; Long-Term Evolution; OpenAirInterface; Telecommunication network

1. Introduction

It is important for telecommunication operators to closely monitor network conditions because any ongoing problem can make a loss in revenue and productivity, or even damage its reputation. Customer service with a traditional approach, which reacts upon complaints, will only leave bad consequences for the company even before the company knows that there is a problem due to the negative customer sentiments on service quality. Among many purposes of network monitoring, anomaly detection is needed to identify critical incidents and resolve potential technical error problems in various crucial performance components before they can affect users. Such monitoring serves as an important component of a forensic-enabled system.

In general, detecting the non-ideal condition of a system is a technical challenge. The plan is initiated by different variables, for example, the characteristics of the system (e.g., uni- or multi-variate), availability of labeled samples, and classes of anomalies. Existing

*Corresponding author's email: riri@ui.ac.id, Tel.: 62217270078, Fax.: 62217270077
doi: 10.14716/ijtech.v14i3.4237

literatures have surveyed anomaly detection, where unsupervised learning (UL) models, such as Recurrent Neural Networks (RNN) and Auto Encoders (AE), show the preferred performance. Long-short-term memory (LSTM) is one example implementation of RNNs, which separates temporal data from historical observation and embeds it in hidden units. Thus, it can represent time dependence. AE with a single layer is almost comparable to Principal Component Analysis (PCA). While PCA is limited to a linear dimensionality reduction, AE empowers both linear and nonlinear transformations. That is, AE computes weights during the dimensionality reduction and tries to predict the information.

The availability of the labeled data and characteristics of the cellular system are also challenging for conducting anomaly detection. This, along with the need for better performance anomaly detection, motivate us to set up the experiment and conduct a performance evaluation. Despite of extensive research has been done in the effort of modeling and simulating the behavior of telecommunication network (Salem *et al*., 2022; Tan *et al*., 2022; Lukman *et al*., 2022), telecommunication operators need real platform to conduct more realistic experiment and measurement, and identify unexpected or anomalous result. To conduct anomaly detection research ideally on cellular telecommunications networks, a realistic research environment representing the actual condition is preferred. Open-source software in the field of cellular telecommunications networks and Software Defined Radio (SDR) fit this purpose. These technologies enable realizing cellular telecommunications networks in a portable manner with higher flexibility at a more affordable price (Mishra *et al*., 2017; Ramacher, 2011). OpenAirInterface (OAI) is an open-source software created to develop the next generation of LTE cellular network technology (Paudel, 2016). It enables the user to learn about the protocol and standards being implemented in the industry as well as fine-tune the configuration and evaluate the behavior (Sari and Harwahyu, 2019). By integrating OAI with SDR, various components such as frequency band, bandwidth, duplexing scheme, type of modulation, number of antennas, and power values can be configured.

Previous research has established cellular telecommunications networks implementing LTE technology through the use of OAI (Nugroho, Sari, and Harwahyu, 2020). The networks are portable because they can be formed using only a computer and an SDR and a standard Internet connection. In this study, we developed an evaluation system using unsupervised machine learning that can be applied to detecting anomalies in the data describing transport components within the cellular network. The development is to extract information from the networks through the use of FlexRAN (Nikaein *et al.*, 2014). FlexRAN is a monitoring system that can be integrated with OAI, informing real-time the state of each RAN. Each RAN contains enormous amounts of data generated each second, and there are thousands of key performance indicators (KPIs) and configuration parameters that should be tracked to analyze network behavior and diagnose problems. We then process these enormous amounts of data through the use of the ELK stack. The use of ELK aims to implement the data storage and processing until it can define anomalous conditions by studying all the data received.

The proposed model aims to accurately and automatically identify anomalous behavior in the LTE network, with which a similar concept can be derived for the 5G network. It can learn independently from historical data and adapt to network conditions. It enables efficient problem diagnosis, continuous health checks, and process automation. It could indicate to telecommunications network providers about possible failures that could lead to network degradation, large maintenance costs, and poor user experience. Subsequently, the performance of the detection techniques is evaluated. Hence, the contributions of this work are (i) presenting a method to implement anomaly detection, (ii) proofing that such a

concept can be implemented in a lab-scale testbed of an LTE network, and (iii) revealing the performance of the proposed method in term of its accuracy.

2. Methods

This study evaluates the application of anomaly detection in the field of telecommunications networks, especially on LTE networks, to anticipate the handling of the problems of sleeping cells and cell outages, which may affect network performances and user experience, by knowing it as soon as possible (Djordjevic, Milosevic, and Poledica, 2020). Anomalies are defined as the sudden drops and correlation changes of KPIs in the LTE network. Various algorithm has been introduced for network anomaly detection.

Feng *et al.* (2014) combines Support Vector Machine (SVM) with an ant colony network to produce a high-performance real-time intrusion detection system. Several phases are employed simultaneously to decrease the time. This combination also increases accuracy. However, the efficiency of the algorithms was not elaborated.

Mirsky *et al.* (2017) introduced the pcStream clustering algorithm to detect three types of anomalies in network streams, namely malware, data leakage, and device thefts. The algorithm uses a non-exhaustive grid search for finding suitable parameters to be used, and thus it takes a considerable amount of time for the training phase.

Guha *et al.* (2016) proposes a robust random cut forest (RRCF) technique as regression-based anomaly detection to perform anomalies detection over a dynamic data stream. The system constructs different KPIs into different dimensions and treated them independently. It conserves pairwise distance, which is important for computation and likewise for anomaly detection. Consequently, the algorithm result shows great promise to fight against the false alarm. However, the dataset size used in the existing literatures is limited.

In this paper, the RRCF algorithm is adopted. RRCF efficiently detects anomalies in the data stream while at the same time adapting to change the input data signal as well as handling collusive outliers due to contaminating the data set. The anomalous conditions are denoted in terms of probability, ranging from 0 to 1, with the number 1 indicating the tendency to be an anomaly.

Confusion Matrix and Evaluation Metrics are used to test the accuracy and the correctness of the detection results. In our iteration, to achieve higher accuracy and correctness, adjustments are made to the threshold limits for normal and anomaly conditions, setting the period for clustering, and the proportion between the training phase and the testing phase.

To evaluate the proposed algorithm, a lab-scale testbed of the LTE network is constructed. It is constructed with the help of OpenAirInterface (OAI) and Texas Instrument's Universal Software Radio Peripheral (USRP) B210, comprising functionalities of Home Subscriber Server (HSS), Mobility Management Entity (MME), Serving Gateway (SGW), Packet Data Network Gateway (PGW), enhanced Node-B (eNB), and Radio Access Network (RAN). Meanwhile, the User Equipment (UE), OAI UE simulator, and ready off-the-shelf UE with suitable LTE-band are used. Data collection is conducted on the transport layer of the LTE network. Analyzing the transport KPIs originating from the RAN reveals the network traffic conditions. Several scenarios are examined and compared.

The subsequent elaboration in this section presents two main topics, namely related to the cellular telecommunications network that was built and an evaluation method for analyzing data using anomaly detection.

2.1. *OpenAirInterface*

OpenAirInterface (OAI) is software created to develop the next generation of LTE cellular network technology. OAI is a prototype and open-source experimental platform that can implement and integrate EUTRAN (including eNB and UE using Software Defined Radio) and EPC (including SGW, PGW, MME, & HSS) (Paudel, 2016). OAI-related research topics are generally about spectral efficiency, algorithm, and protocol, with the hope that it can be used for various 5G network needs such as D2D, M2M, HCN, CloudRAN, Software Defined Mobile, Millimeter Waves, and Shared Spectrum (Paudel, 2016; Nikaein *et al.*, 2014). The work environment for OAI uses Linux-based hardware, from a single computer to a cluster with sophisticated device specifications or even a GPU workstation (Romdhanne, Nikaein, and Bonnet, 2011).

2.2. *FlexRAN*

A monitoring system that can be integrated with OAI is shown in Figure 1. The FlexRAN component consists of the Service and Control Plane, and Application Plane. In the Service and Control Plane, there is a Real-time Controller (RTC) that is connected to one or more RAN runtime modules. The RAN runtime module is in an abstraction layer that is different from RTC but has a hierarchical binding under RTC. Each RAN runtime module will act separately from one another and has the respective communication facilities with RTC through the RAN agent contained in each RAN runtime module (Papa *et al.*, 2019). On the other hand, the Application Plane has a mapping that connects each RAN runtime module with the Software Development Kit (SDK). The Application Plane monitors, controls, and coordinates the state of each module that represents the RAN infrastructure (Yala *et al.*, 2019; Costanzo *et al.*, 2018). All RAN and API data generated are open for processing using other applications outside the OAI environment.

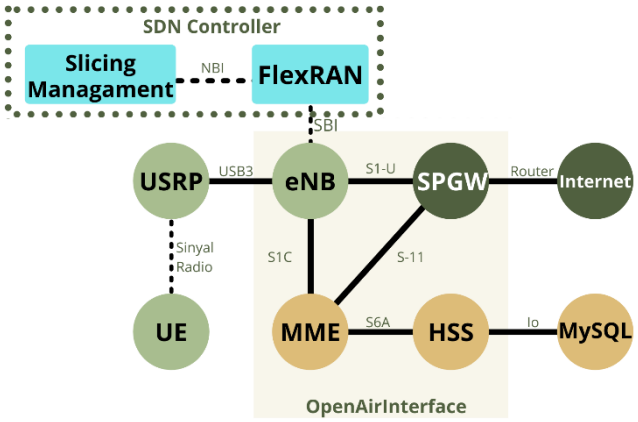

Figure 1 Integration of various OAI elements and FlexRAN

2.3. *ELK*

ELK is an abbreviation of three open-source projects commonly used as a single unit consisting of Elasticsearch, Logstash, and Kibana which can be assumed to be a wafer stack (Chang *et al.*, 2014). Elasticsearch is a search engine based on the Lucene library. It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents. Logstash is a free and open server-side data processing pipeline that ingests data from a multitude of sources, transforms it, and then sends it to be used or for storage. Kibana is an alternative data visualization dashboard suitable for Elasticsearch. When OAI carries out the overall function of elements in the cellular telecommunications network architecture, FlexRAN plays a role in the control elements and probes that pull data from the device. Subsequently, ELK in this case will act as an extension

to the monitoring system. ELK in this case will be mapped to connect as an endpoint to FlexRAN so that all infrastructure records will be forwarded to ELK (Al-Mahbashi, Potdar, and Chauhan, 2017). Furthermore, ELK's role is to carry out the transformation and processing of data into a new format specified by the user and perform visualization to the expected analysis.

2.4. Robust Random Cut Forest

The Robust Random Cut Forest (RRCF) algorithm is an algorithm that will be used to detect anomalies in research. RRCF is an unsupervised method for the detection of anomalies that are specialized in handling data flows (Guha *et al*., 2016). RRCF is specifically used by several applications such as Amazon Kinesis and ELK for the detection of anomalies with a real-time analytic engine.

2.5. Experimental Design

The physical design of the system used can be seen in Figure 2. The following are the hardware required to conduct this research, i.e. general-purpose computers, USRP B210, VERT (Vertical Antenna) 900 series, USB 3.0, ethernet cable, router, and cellphones. We use a computer with a 64-bit operating system and have 8GB of RAM. The computer has an Intel® Core ™ i7-8750H CPU @ 2.20GHz × 12 specification. USRP B210 includes RF frequencies from 70 MHz to 6 GHz. It has the ability of the two-channel receivers and two transmissions, GPIO, and includes an external power supply, as well as RFIC analog devices to produce RF that can emit bandwidth up to 56 MHz. VERT (Vertical Antenna) 900 series works at a power of 3dBi and can work with quad-band cellular / PCS and ISM Band omnidirectional vertical antenna. Super Speed (SS) USB 3.0 accommodates data transmission speeds of up to 20 Gbit / sec (equivalent to 2.5 GB / sec). On the other hand, the software we use includes Ubuntu 16.04.6 LTS (Xenial Xerus) with kernel 4.15.0-45-generic, OpenAirInterface (includes three modules, namely CN, RAN, and FlexRAN), ELK with version 7.8.0, GNU Radio version 7.4.0, UHD with version 3.14.1.1, and Iperf.

Figure 2 Physical Design of the System

The system was assembled using the hardware prepared. The VERT 900 antenna was attached to the Tx and Rx port. The computer was then connected to the USRP B210 using a USB 3.0 cable. These steps were enough to be able to establish a cellular telecommunications system, but the network had not provided a connection to the Internet. An additional path was needed to access data on the Internet. In this research, we used an ethernet cable connected to the router to access the Internet.

2.6. Work Scheme

By applying the basic principles of anomalous characteristics that are much smaller than normal conditions, several cases were formed to illustrate the anomaly state using TCP and UDP protocol packet data transmission. Researchers use the term contamination to describe the proportion of anomalous conditions that are intentionally created. The duration of the time series created for each case is two hours. As seen in Figure 3, from the two hours duration of the experiment, most of it is used initially for the training process and only the last 15 minutes are used for the analysis process.

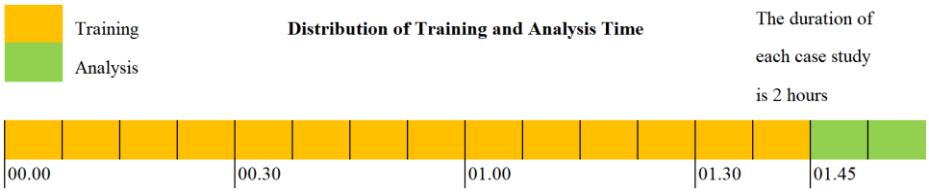

Figure 3 Distribution of Training and Analysis Time

Four cases are constructed, with each can be defined as TCP with 5% contamination, TCP with 2.5% contamination, UDP with 2.5% contamination, and UDP with 0% contamination. The contamination in question is a situation other than transmitting data packets with the specified protocol.

2.7. Confusion Matrix

A confusion matrix is a description of all types of results that might be obtained from research on the detection of anomaly by classifying any combination that might be formed using two binaries to produce four conditions. In the case of anomalous detection, the possible conditions are shown in Figure 4.

True Positives (TP) When the anomalous state detected is correctly defined as the state of anomaly by the system.	**False Negatives (FNs)** When an anomalous state is however detected as a normal state by the system.
False Positives (FPs) When a normal state however is detected as an anomalous state by the system.	**True Negatives (TNs)** When a normal state and detected correctly as a normal state by the system.

Figure 4 Confusion Matrix

2.8. Evaluation Metrics

Concerning the confusion matrix, the following are some further calculations as a derivative of these metrics. They can be used to evaluate the accuracy of the anomaly detection system (Lam and Abbas, 2020; Mdini, 2019; Trinh *et al*., 2019).

2.8.1. Specificity - True Negative Rate (TNR)

TNR measures the proportion of normal states that are correctly labeled between all points that should be predicted as normal.

$$TNR = \frac{TN}{TN+FP} \quad (1)$$

2.8.2. Precision - Positive Predictive Value (PPV)

PPV measures the proportion of anomalies that are correctly labeled between all points predicted as anomalous by the system.

$$PPV = \frac{TP}{TP+FP} \quad (2)$$

2.8.3. Recall / Sensitivity - True Positive Rate (TPR)

TPR measures the proportion of anomalies that are correctly labeled between all points that should be predicted as anomalous conditions.

$$TPR = \frac{TP}{TP+FN} \quad (3)$$

2.8.4. Fallout - False Positive Rate (FPR)

Measuring the proportion of detection errors as an anomalous state by the system between all points that should be predicted as normal.

$$FPR = \frac{FP}{FP+TN} \quad (4)$$

2.8.5. False Negative Rate (FNR)

FNR measures the proportion of anomalous conditions not detected by the system between all points that should be predicted as anomalous conditions.

$$FNR = \frac{FN}{FN+TP} \quad (5)$$

2.8.6. Accuracy (ACC)

ACC measures the proportion of all predictions that are correctly labeled by the system among all predictions that have been made.

$$ACC = \frac{TN+TP}{TN+TP+FN+FP} \quad (6)$$

2.8.7. Complementary

In the various calculation components used to evaluate anomalous detection systems, there are several complementary components as seen in the following equations which show the relationship between TNR and FPT and TPR and FNR.

$$TNR + FPR = 1 \quad (7)$$

$$TPR + FNR = 1 \quad (8)$$

3. Results and Discussion

To determine whether the developed model can meet the research objectives, an approach with data labeling was used. Data labeling is carried out for each instance into normal or anomalous categories based on the calculated threshold for KPIs. Labeling techniques are used to automate the process of identifying problems that may occur, it is illogical for researchers or even experts to analyze all data one by one and identify all RANs in the LTE network that have anomalous behavior. In this study, three main KPIs were filtered from all existing KPIs for use in the analysis of the labeling approach. The labeling results are then tested by mapping the conditions according to the evaluation matrix. Accuracy scores and a rough evaluation of the cases can be calculated as the data is labeled. Non-conforming conditions, such as false positives and false negatives, can be further analyzed and these data allow the operator to prepare corrective action when certain anomalies are detected.

3.1. Result from Data Processing

An outline of the data processing stages is depicted in Figure 4. Basically, after going through the format adjustment process, the original data in the JSON format generated by FlexRAN can be read by the ELK module. At one time the receipt of JSON data, there are two major parts of the data structure which are then used as an index in ELK, namely *enb_config* and *mac_stats*. The *enb_config* index is entirely static data containing configuration information that has been set up so that it is not possible to be processed further. Therefore, the research will focus on data from the *mac_stats* index.

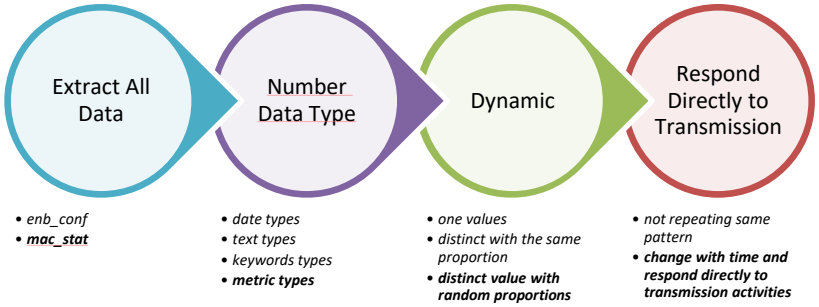

Figure 5 Data Processing

There are four classifications of data types in ELK, namely text types, keyword types, date types, and metrics types. There are 60 data metrics types. Data with other metric types will be ignored because they cannot be processed. Furthermore, there are 27 dynamic metrics data types, which are those that change with time and have very diverse component values. However, the final result from processing the data determines that three components have a direct link to the transmission of UDP and TCP data packets because they have a fast response and are in accordance with network traffic conditions.

The three data components are mac_stats.mac_stats.macStats.mcs2Dl, mac_stats.mac_stats.macStats.tbsDl, and mac_stats.mac_stats.macStats.prbDl. If we look from the perspective of eNB, these data have a common feature of residing in some parts or elements of the receiver. The component is sufficient to describe network traffic because it is the part that receives data packets directly from a cell phone that acts as a server that transmits data.

Furthermore, mcs-2dl is a term to refer to packet data block type 6 which is one of thirteen standard schemes for packet data traffic channel coding. Apart from mcs-2dl, there is tbsdl which is the name of the Transport Block Size (TBS) data variable in the downlink section for UE BL/CE as determined by LTE standardization. Each pdsch transmission to the UE contains a collection of information whose size is determined by the TBS. Finally, prbdl is the name of the data variable for the Physical Resources Block (PRB). PBR defines how much capacity as traffic grows and can increase the frequency of use as needed. In real networks, the spectral efficiency can exceed the 3GPP limit if the load is unbalanced between cells in a cellular telecommunication network.

3.2. Evaluation of Anomaly Detection Performance

The three data processing results are tested based on the scenario described in each case. The three data are analyzed by univariate time series for each of each component and data samples are grouped into 1 second. Every second of data collection represents the points to be analyzed. Confusion matrix results can be seen in Table 1. The data that has been obtained is evaluated using the evaluation metric and the results can be seen in Figure 6.

Table 1 Confusion Matrix Results in (a) Case I, (b) Case II, (c) Case III, and (d) Case IV

	TP	FP	FN	TN
mcs2dl	119	7	181	593
tbsdl	139	7	161	593
prbdl	139	7	161	593

(a)

	TP	FP	FN	TN
mcs2dl	54	0	66	780
tbsdl	61	0	59	780
prbdl	61	0	59	780

(b)

	TP	FP	FN	TN
mcs2dl	114	7	66	713
tbsdl	116	9	64	711
prbdl	138	6	42	714

(c)

	TP	FP	FN	TN
mcs2dl	0	0	0	900
tbsdl	0	12	0	888
prbdl	0	4	0	896

(d)

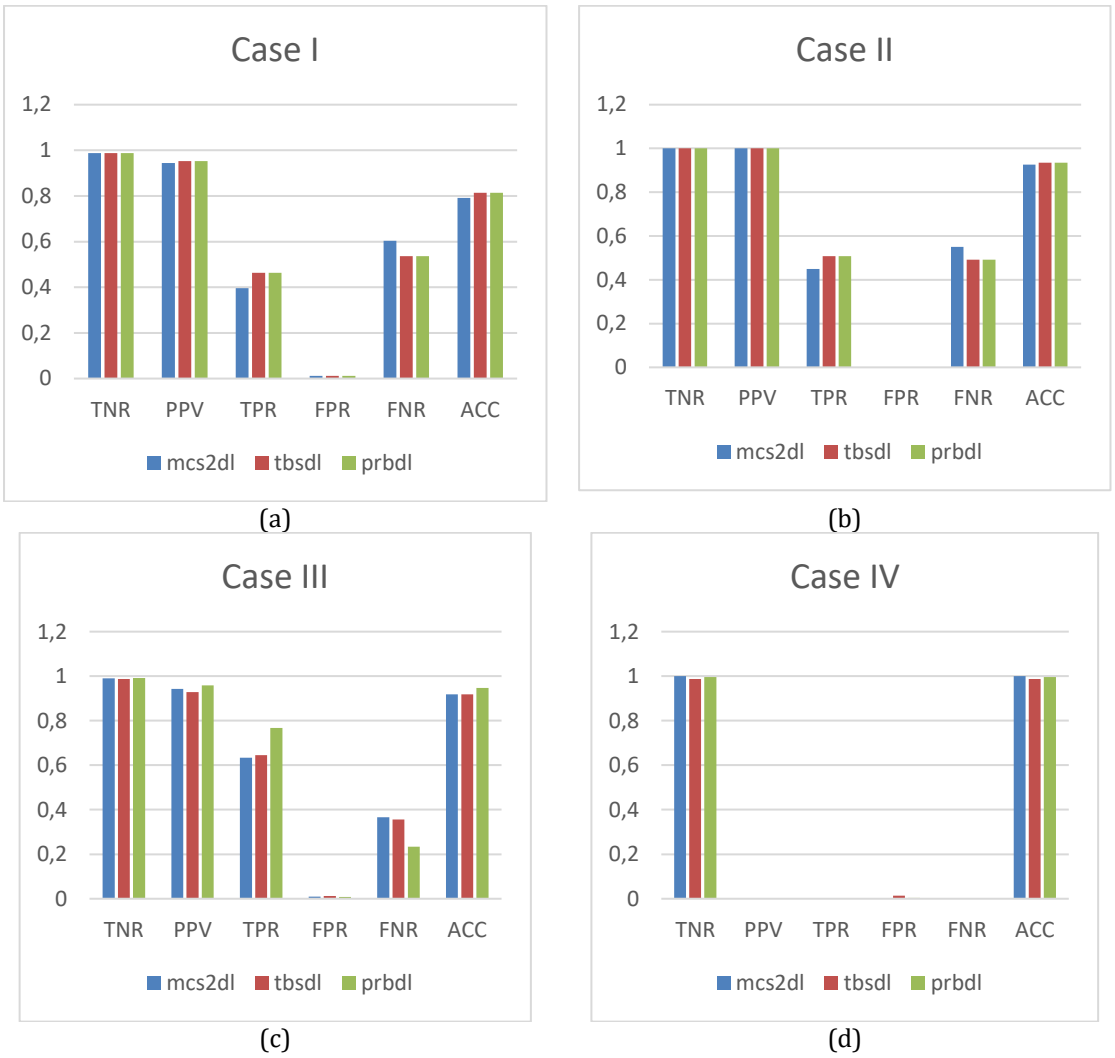

Figure 6 Evaluation Metrics Results for (a) Case I, (b) Case II, (c) Case III, and (d) Case IV

The presented tables and graphs show a quantitative analysis of the varivous cases and evaluation matrix components. It can be seen that anomaly detection using RRCF has high accuracy for each KPI whose anomalous condition is observed. The processing is fast because each instance has a clustering period every one second that contains hundreds of data for all KPIs. Hence, it is suitable to be used in real-time applications.

The average evaluation results of Case I yields TNR, PPV, TPR, FPR, FNR, and ACC of 0.9883, 0.9495, 0.4411, 0.0117, 0.5589, and 0.8059, respectively. Note that Case I represents the condition where the traffic is TCP with 5% contamination. A True Negative Rate of 0.9883 indicates that almost all normal traffics are correctly detected as normal traffic. This corresponds with the False Positive Rate of 0.0117, which demonstrates that only 1.17% of the normal traffics are detected as anomalies and triggers a false alarm. A Positive Predicted Value of 0.9495 indicates that in the time when the alarm is triggered, 94.95% of the alarm is correctly indicating anomaly, i.e., only 5.05% of the triggered alarm

is caused by false positive. A True Positive Rate of 0.4411 is considerably low, as this indicates that only 44.11% of the occurred anomaly are reported as anomalies. Meanwhile, the rest of 55.89% of the occurred anomalies, which is indicated in a False Negative Rate of 0.5589, was mistakenly reported as normal traffic and didn't trigger the alarm. These bring an accuracy of 80.59% for Case I.

The average evaluation results of Case II yield TNR, PPV, TPR, FPR, FNR, and ACC of 1, 1, 0.4889, 0, 0.5111, and 0.9319, respectively. Note that Case II represents the condition where the traffic is TCP with 2.5% contamination. A True Negative Rate of 1 indicates that almost all normal traffics are correctly detected as normal traffic. This corresponds with the False Positive Rate of 0, which demonstrates that no normal traffics are falsely detected as anomalies and triggers a false alarm. A Positive Predicted Value of 1 indicates that at the time when the alarm is triggered, all of the alarm is correctly indicating anomaly. A True Positive Rate of 0.4889 is considerably low, as this indicates that only 48.89% of the occurred anomaly are reported as anomalies. Meanwhile, the rest of 51.11% of the occurred anomalies, which is indicated in a False Negative Rate of 0.5111, is mistakenly reported as normal traffic and will not trigger the alarm. These bring overall accuracy of 93.19% for Case II.

The average evaluation results of Case III yield TNR, PPV, TPR, FPR, FNR, and ACC of 0.9898, 0.9428, 0.6815, 0.0102, 0.3185, and 0.9281, respectively. Note that Case III represents the condition where the traffic is UDP with 2.5% contamination. A True Negative Rate of 0.9898 indicates that almost all normal traffics are correctly detected as normal traffic. This corresponds with the False Positive Rate of 0.0102, which demonstrates that only 1.02% of the normal traffics are detected as anomalies and triggers a false alarm. A Positive Predicted Value of 0.9428 indicates that in the time when the alarm is triggered, 94.28% of the alarm is correctly indicating anomaly, i.e., only 5.72% of the triggered alarm is caused by false positive. A True Positive Rate of 0.6815 is considerably low, as this indicates that only 68.15% of the occurred anomaly are reported as anomalies. Meanwhile, the rest of 31.85% of the occurred anomalies, which is indicated in a False Negative Rate of 0.3185, is mistakenly reported as normal traffic and will not trigger the alarm. These bring an accuracy of 92.81% for Case III.

The average evaluation results of Case IV yield TNR, FPR, and ACC of 0.9941, 0.0059, and 0.9941, respectively. PPV, FPR, and FNR cannot be defined because they are zero when the contamination conditions are 0% in Case IV. A True Negative Rate of 0.9941 indicates that almost all normal traffics are correctly detected as normal traffic. This corresponds with the False Positive Rate of 0.0059, which demonstrates that only 0.59% of the normal traffics are detected as anomalies and triggers a false alarm. These bring an accuracy of 99.41% for Case IV.

Based on the evaluation matrix, it appears that there is a tendency for the system to have a better ability to detect the normal state than the other three conditions. On the other hand, the smaller the duration of the anomalous state, the evaluation results show there is a trend that is getting better in each component of the evaluation metric. In addition, from the three data analyzed, it can be seen that PRB is the data element that best matches the circumstances of the case defined. The average accuracy value of the anomaly detection system for all cases is 91.5% so it can be assumed that the anomaly detection system has worked accurately. The accuracy results are supported by the average proportion value of the normal state that is predicted correctly by 99.31%. This shows the process of predicting the normal state to all normal conditions shows a very accurate capacity. Finally, for the four observed cases, the overall accuracy of the system is 93.19%.

4. Conclusions

From our research, it can be concluded that the fourth generation (4G) LTE cellular telecommunication network system can be implemented using the OpenAirInterface platform. Additional applications are needed, namely FlexRAN to extract data in real-time from the eNB runtime module. ELK can be integrated with FlexRAN to form a system of cellular telecommunications network monitoring, and the system formed is able to fulfill the functions of the monitoring system in the form of data collection and problem detection. Furthermore, the anomaly detection system that was formed can accurately detect anomalous conditions on the cellular telecommunications network with an average accuracy value of 91.5%, supported by an average proportion of normal conditions predicted correctly by 99.31%. This research uses machine learning techniques to perform automatic anomaly detection on cellular telecommunication networks. Process automation on anomaly detection has a tremendous impact on processing large amounts of data, in addition to saving analysis time it also saves costs that might be required for manual identification processes by experts. In its application, an unsupervised approach is especially important in the case of analyzing all features simultaneously in real-time data streams. By using data KPIs associated with the transport layer, unusual network traffic behavior can be detected.

Acknowledgments

We thank the Ministry of Education and Culture of the Republic of Indonesia for financial support for this research under the PDUPT Research Grant number NKB-255/UN2.RST/HKP.05.00/2020.

References

Al-Mahbashi, I.Y., Potdar, M.B., Chauhan, P., 2017. Network Security Enhancement Through Effective Log Analysis Using ELK. *In*: Proceedings of the International Conference on Computing Methodologies and Communication (ICCMC), pp. 566–570

Chang, N., Lan, A., Liao, M., Chen, E., 2014. ELK Delaminate Improvement Methodology On Cu Pillar Interconnect BOP Structure. *In*: Proceedings of the Electronic Components and Technology Conference, pp. 81–84

Costanzo, S., Fajjari, I., Aitsaadi, N., Langar, R., 2018. A Network Slicing Prototype For A Flexible Cloud Radio Access Network. *In*: Proceedings of the Annual Consumer Communications & Networking Conference, pp. 1–4

Djordjevic, V., Milosevic, P., Poledica, A., 2020. Machine Learning Based Anomaly Detection As An Emerging Trend In Telecommunications. *Journal of Sustainable Business and Management Solutions in Emerging Economies*, Volume 27(2), pp. 71–82

Feng, W., Zhang, Q., Hu, G., Huang, J.X., 2014. Mining Network Data for Intrusion Detection Through Combining SVMs With Ant Colony Networks. *Future Generation Computer Systems*, Volume 37, pp. 127–140

Guha, S., Mishra, N., Roy, G., Schrijvers, O., 2016. Robust Random Cut Forest Based Anomaly Detection Onon Streams. *In*: Proceedings of the International Conference on Machine Learning, pp. 2712–2721

Lam, J., Abbas, R., 2020. Machine Learning Based Anomaly Detection For 5G Networks. *arXiv e-prints*, Volume 12, p. 03474

Lukman, S., Nazaruddin, Y.Y., Ai, B., Joelianto, E., 2022. Path Loss Modelling for High Speed Rail in 5G Communication System. *International Journal of Technology*, Volume 13(4), pp. 848–859

Mdini, M., 2019. *Anomaly Detection Andand Root Cause Diagnosis in Cellular Networks*. Doctoral Dissertation, Ecole nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire

Mirsky, Y., Shabtai, A., Shapira, B., Elovici, Y., Rokach, L., 2017. Anomaly Detection Forfor Smartphone Data Streams. *Pervasive and Mobile Computing*, Volume 35, pp. 83–107

Mishra, M., Potnis, A., Dwivedy, P., Meena, S.K., 2017. Software Defined Radio Based Receivers Using RTL — SDR: A Review. *In*: Proceedings of the International Conference on Recent Innovations in Signal processing and Embedded Systems, pp. 62–65

Nikaein, N., Marina, M.K., Manickam, S., Dawson, A., Knopp, R., Bonnet, C., 2014. OpenAirInterface: a Flexible Platform for 5G Research. *ACM SIGCOMM Computer Communication Review*, Volume 44(5), pp. 33–38

Nugroho, Y.N., Sari, R.F., Harwahyu, R., 2020. Performance Comparison of GPRS and LTE Telecommunication Network Using Openairinterface and OpenBTS with USRP. *In:* Proceedings of the International Conference on Industrial Electrical and Electronics, pp. 197–204

Papa, A., Durner, R., Edinger, F., Kellerer, W., 2019. SDRBench: a Software-Defined Radio Access Network Controller Benchmark. *In:* Proceedings of the Conference on Network Softwarization, pp. 36–41

Paudel, S., 2016. *Investigation, Analysis and Implementation of Open-Source Mobile Communication Software*. Master's Thesis, Norwegian University of Science and Technology NTNU

Ramacher, U., 2011. Architecture and Implementation of A Software-Defined Radio Baseband Processor. *In*: Proceedings of the International Symposium of Circuits and Systems, pp. 2193–2196

Romdhanne, B., Nikaein, N.K., Bonnet, C., 2011. Openairinterface Large-Scale Wireless Emulation Platform and Methodology. *In:* Proceedings of the International Workshop on Performance Monitoring, Measurement and Evaluation of Heterogeneous Wireless and Wired Networks, pp. 1–4

Salem, M.A., Lim, H.S., Chua, M.Y., Chien, S.F., Zarakovitis, C.C., Ng, C.Y., Rahman, N.Z.A., 2022. Investigation oOf EMF Exposure Level for Uplink aAnd Downlink oOf 5G Network Using Ray Tracing Approach. *International Journal of Technology*, Volume 13(6), pp. 1298–1307

Sari, R.F., Harwahyu, R., 2019. Teaching Internet Protocol Engineering Withwith Open Source Simulators: aA Long Road From WAN to 5G. *In*: Proceedings of the International Conference on Engineering Education, pp. 122–127

Tan, K.H., Lim, H.S., Diong, K.S., 2022. Modelling aAnd Predicting Quality-oOf-Experience Ofof Online Gaming Users in 5G Networks. *International Journal of Technology*, Volume 13(5), pp. 1035–1044

Trinh, D., Zeydan, E., Giupponi, L., Dini, P., 2019. Detecting Mobile Traffic Anomalies Through Physical Control Channel Fingerprinting: aA Deep Semi-Supervised Approach. *IEEE Access*, Volume 7, pp. 152187–152201

Yala, L., Iordache, M., Bousselmi, A., Imadali, S., 2019. 5G Mobile Network Orchestration Andand Management Using Open-Source. *In*: Proceedings of the 5G World Forum, pp. 421–426