Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.020598
Article

Tech Science Press

Rule-Based Anomaly Detection Model with Stateful Correlation Enhancing Mobile Network Security

Rafia Afzal and Raja Kumar Murugesan*

School of Computer Science and Engineering, Taylor's University, Subang Jaya, Selangor, 47500, Malaysia
*Corresponding Author: Raja Kumar Murugesan. Email: rajakumar.murugesan@taylors.edu.my
Received: 30 May 2021; Accepted: 26 July 2021

Abstract: The global Signalling System No. 7 (SS7) network protocol standard has been developed and regulated based only on trusted partner networks. The SS7 network protocol by design neither secures the communication channel nor verifies the entire network peers. The SS7 network protocol used in telecommunications has deficiencies that include verification of actual subscribers, precise location, subscriber's belonging to a network, absence of illegitimate message filtering mechanism, and configuration deficiencies in home routing networks. Attackers can take advantage of these deficiencies and exploit them to impose threats such as subscriber or network data disclosure, intercept mobile traffic, perform account frauds, track subscriber location, and deny services. Existing methods are unable to identify suspicious hosts as they use a minimal number of network parameters. So, there is a vital need to overcome these deficiencies to detect the abnormal behaviour of users and hence mitigate security attacks in a mobile network. This research proposes a model for anomaly detection in mobile networks based on Rule-based filtering with stateful correlation. The performance of the proposed method is evaluated using synthetic datasets. Results show that the proposed anomaly detection model performs 0.37% better in terms of security attack detection rate, 24.25% better in terms of false alarm rate, and 31.45% better in terms of true positive rate when compared with the existing pattern recognition Artificial Neural Network (ANN) algorithm.

Keywords: SS7; telecommunication; mobile network security; anomaly detection

1 Introduction

Signalling System 7 (SS7) is a set of signalling protocols for setting up and terminating calls or exchanging data between network devices in a telecommunication network. SS7 is used to monitor mobility, control billing information, produce user safety information, help call delivery, control access and service authorization [1]. SS7 was developed in 1975, and at that time, only the fixed-line operators, which were state-owned, had access to the network. Therefore, security was not a priority and relied on the mutual trust between operators [2,3].

Currently, the SS7 network is not limited only to fixed-line operators but also used in mobile networks. Deregulation of the telecommunication network across the world resulted in the liberalization and privatization of the telecommunication network. It allowed commercial organizations to start telecommunication networks, hence flooding the market. Moreover, it also created an opportunity for intruders to effortlessly gain access to the network taking advantage of its vulnerabilities, i.e., lack of actual subscriber location check, subscriber verification, and lack of illegitimate messages filtering mechanism that cause threats such as SS7 exposure, breach of subscriber information and confidentiality theft [4].

Intruders can perform attacks, namely, location tracking, interception of calls and SMS, and Denial of Service [5]. 4G and 5G networks employ diameter and 5G NR (5G New Radio) respectively as the signalling system. However, the same security threats present in SS7 also exist in 4G and 5G networks as operators need to support backward compatibility, enabling interaction with earlier generations [6].

The existing intrusion detection methods mainly use K-means clustering, decision trees, random forest, ANN, and generic rule-based filtering algorithm. The feature sets used by these methods are; distance travelled since the previous location, location update frequency, elapsed time since the previous location update message request, network the message originates from, and message request size [7–9]. Although, rule-based filtering algorithms outperform other machine learning algorithms mentioned above in terms of better accuracy and detection rate with decreased false alarm rates.

However, these methods fail to consider vulnerabilities such as lack of actual subscriber location check and verify subscriber's belonging to a network and lack of illegitimate messages filtering mechanism. If we do not consider these aforesaid SS7 network vulnerabilities, we will not check the legitimacy of message requests, leading to threats and attacks such as interception of calls and SMS, location tracking, fraud, and service denial. Based on the above methods, we can consider a rule-based filtering algorithm and improvise it to enhance SS7 network security.

Another major issue that hinders secure signalling transport is that trusted network elements carry out attacks on the signalling infrastructure. This happens because of the business model that allows selling connectivity access to third parties. So, the network is not restricted to only trusted parties. Anyone knowing the internal working of the SS7 network can get access and thus perform attacks.

Moreover, according to 3rd Generation Partnership Project (3GPP) Technical Specification documentation, the existing network protocol uses a stateless firewall that is not good enough to solve anomaly detection and mitigate security attacks. The current system does not check the subscriber's actual location and verifies the subscriber's belonging to a network [10,11].

In existing researches, authors have suggested using stateful security checks between parameters of protocol layers of the SS7 network, a correlation between time of message requests and distance between last known location to the current location that can be used to check subscriber's actual location and verify subscriber's belonging to a network while the subscriber is roaming [12].

Signalling Connection Control Part (SCCP), Transaction Capabilities Application Part (TCAP), and GSM MAP (Global System for Mobile Communications-Mobile Application Part) layers are responsible for connectivity between networks and subscribers. However, as illustrated in Tab. 3 in Section 4.1, the parameters of these layers are not analyzed for anomalies. They are abrupt change in location, malformed parameters, and inconsistencies in parameters between layers to hide or spoof a sender location. For example, if an intruder sends a MAP updateLocation (UL) message request, the existing filtering mechanism alone will not be enough. It only considers received parameters for verifying actual subscribers and ignores intra-layer parameters checks for inconsistencies and malformed. Further checks will be required to verify whether the subscriber is present at the location from where the message originated. This shows that current traffic filtering and blocking mechanisms cannot compensate for

architectural flaws in the SS7 network. Hence, a new strategy must mitigate the flaws mentioned above in the current filtering mechanism [13].

The above findings motivated this research to propose a model based on Rule-based filtering with stateful correlation to detect anomalies such as an abrupt change in location and hide or spoof a sender by using malformed parameters hence mitigate security attacks in a mobile network. The previous location of the subscriber is required to find a time distance correlation, essentially preserving the state of the subscriber's location to detect abrupt changes in location. This is analogous to stateful security checks and firewalls in TCP/IP networks.

The performance of the proposed method is evaluated using synthetic datasets simulated using an open-source attack simulator [7]. Results show that the proposed model has improved the anomaly detection accuracy and reduces the high false alarm rate compared to the existing methods. The main contribution of this research is a model to detect anomalous subscribers and anomalous location of originating message requests in addition to verification of malformed parameters and intra-layer inconsistencies in parameters.

This paper is organized into the following sections. Section 2 highlights the review of security threats and vulnerabilities in SS7 networks. Section 3 discusses the related work in terms of 3 use of machine learning techniques to secure signalling network and their shortcoming, while Section 4 presents the proposed anomaly detection model. The results and discussion are in Section 5, and Section 6 concludes the paper with future directions.

2 Security Vulnerabilities, Threats, and Attacks in SS7 Networks

Researchers and media have reported SS7 network vulnerabilities [14–16]. Many attacks and network entry points have been disclosed both by the network industry and academic researchers. The following section describes the currently known attack types and how it works [17]. These SS7 vulnerabilities and threats landscape for an intruder to perform attacks can be divided into the following categories:

- SS7 Exposure and Breach of user information or confidentiality theft
- Eavesdropping
- Financial thievery
- Misuse of service
- Denial of Service
- Location Tracking

2.1 SS7 Exposure and Breach

Signalling System No. 7 security issues had been given extensive consideration in recent years. It is increasingly becoming clear that SS7 is strained with severe weakness and exposures that compromise cellular customer's privacy [17]. Jensen et al. [16] tried to utilize machine learning features to improve the SS7 network and the subscribers' identity. They have used simulators and produced artificial traffic in a controlled environment. Virtual verification was used to articulate near close to actual network traffic utilizing open-source SIGTRAN protocol stack software. However, the approaches described above remain ineffective, owing to numerous inadequacies.

Furthermore, Denial of Service (DOS) and SMS have been launched to intercept attacks and detect vulnerabilities using different classifiers. Its practicality needs to be seen in how it works. Sharma et al. [18] have explored different types of attacks over the SS7 network, i.e., breaches like tracking location, intercepting SMS and calls, eavesdropping, and finding entry point attacks, but no detection mechanism was implemented. Similarly, Holtmann et al. [19] have articulated different attacks on interworking

function (IWF) between diameter and SS7 networks for LTE. There is considerable existing research that has proposed various approaches to protect the SS7 network from such vulnerabilities and proposed some protection techniques, but no detection mechanism was implemented to provide proof-of-concept.

2.2 Eavesdropping

An attacker can eavesdrop on a subscriber's data, wiretap, and send/modify text messages to a victim by acting as a "man-in-the-middle (MiTM)" attack, the victim completely unaware of the attack [20]. The intruder bridges himself between the two calling parties and directs all the calls to its monitoring system. For this purpose, MAP messages and a call-forwarding function are used. The target user is not aware of this attack. The attacker sends the victim calls to the monitoring system at the SS7 MAP Message level. Consequently, the attacker establishes another call to the user to whom the call is being made. One cause described in [20] is the lack of encryption across the network for these attacks.

2.3 Financial Thievery

The victim's Mobile Switching Centre (MSC) is impersonated in the financial thievery attack. The aim is to get text messages or to receive information about the victim's bank account and other attacks. Unstructured Supplementary Service Data (USSD) is used to achieve the bank's secret information under such mentioned attack category. The victim's account can be misappropriated for monetary transactions [20]. Hall et al. [21] explained the reasons and pointed out flaws in the current network that cause the stated attacks.

Moreover, Van Do et al. [22] and Yeboah et al. [23] presented grey SMS traffic detection, which cannot be used in a real-time environment due to the high rate of false positives. Similarly, Sahin et al. [24] systematically explored telephony frauds types and their benefits in fraudsters' eyes and elaborate on root causes, vulnerabilities, and exploitation techniques. It also mentioned a few billings process and spamming frauds and their effects.

2.4 Misuse of Service

In the misuse of services attack, the subscriber's billing is exploited, leading to significant financial repercussions for the network operator. An increase in these attacks causes inaccessibility of services and decreases gross income [20]. At the same time, Azad et al. [25] assessed the method's enactment. They performed a simulation of spammers and non-spammers social behaviour by articulating artificial data. Their proposed Collaborative Spit Detection System (COSDS) approach yields better detecting accuracy than traditional standalone detection systems. However, as the research was conducted in a controlled setup, it cannot fully secure it.

2.5 Denial of Service (DOS)

The main motive of DOS is to decline the services for a specific subscriber. When a user is updated with a new location and gets registered with the latest MSC (Mobile Switching Centre)/VLR (Visitor Location Register), it first makes a MAP update request to (Home Location Register). After verifying the received message, HLR issues MAP InsertSubscriberData (ISD) command to new MSC/VLR and MAP DeleteSubscriberData (DSD) and MAP CancelLocation (CL) commands to old MSC/VLR [26]. By doing this, the attacker can change the victim's (subscriber) allowed services such as disallow the subscriber to make a phone call, sending SMS, or even altogether remove him from the subscriber's connected VLR.

2.6 Location Tracking

Location tracking can help find people in an emergency, but hackers can also track anyone anytime, and then they can perform any criminal activity they want. An attacker can use either MAP AnyTimeInterrogation (ATI) or MAP ProvideSubscriberInfo (PSI) message requests to track any

subscriber. To identify these, we must collect information on user behaviour and check for anomalies from user behaviour, subscribers, and network components. In Tab. 1, the causes behind these vulnerabilities, threats and attack triggers, and research gaps in the existing research are summarized.

Table 1: Causes behind vulnerabilities, threats, and attacks with existing solutions and research gaps

Causes behind vulnerabilities	Threats	Attacks	Existing solutions	Research gaps & possible solution
Lack of subscriber actual location check	PRIVACY	Subscriber/ network information disclosure, location privacy	Simulated prototype to detect attacks through different machine learning techniques such as K-means, random forest, decision trees, SVM, ANN, and rule-based filtering [7–9].	Unable to verify actual subscribers belonging to a network and check actual location using received parameters alone. Need of actual subscriber check along with location verification to solve this issue. Using this, further scrutiny is necessary to identify suspicious hosts by applying a mechanism to filter illegitimate messages.
Inability to authenticate a subscriber	SECRECY	Communication disclosure		
SMS home routing configuration flaws	INTEGRITY	System integrity, subscriber traffic interception		
Lack of message filtering	FRAUDS	Direct under-billing effects operator. directly over-billing affects subscribers. Cheating through indirect ways encompasses telephonic scams or spam.		

3 Machine Learning and Secure Signalling Network

Qasim et al. [8] and Ullah et al. [9] in their research have suggested using machine learning classifiers such as decision trees, random forest, support vector machine, ANN, pattern recognition, and rule-based filtering on a minimal number of feature sets such as distance travelled since previous location update, frequency of location updates, and time since previous location update, message network origin, and byte length of location update only. Jensen et al. [16] tried to utilize machine learning features to improve the SS7 network and subscribers' identity security. Researchers have proposed an "RC4 stream cypher for SMS data confidentiality" as a solution to identify network vulnerabilities in SMS services. Their research has also explained how SMS routing procedures can be exploited for attacks such as interception [27].

Researchers had also identified vulnerabilities in breach of user profile information, user location tracking, eavesdropping, and misuse of user profile information for financial fraud. They have proposed decision trees, SVM, and random forest algorithms for anomaly detection. Loay et al. [28], in their research, had discussed calls/SMS interception and location tracking attacks. They have proposed a penetration testing tool for

detecting attacks in SS7 networks. Liu et al. [29] explained how any subscriber's identity and location could be compromised due to a lack of secure network channels and propose a defence model.

Similarly, Holtmann et al. [30] have articulated different attacks on interworking function (IWF) between diameter and SS7 networks for LTE. Sharma et al. [18] and Holtmann et al. [30] have exposed the susceptibilities of the SS7 network and proposed some protection techniques such as the use of closed subscriber group in case of dealing with roaming scenarios or validate the authenticity of the incoming message requests, as protection measures to be implemented by GSMA (Global System for Mobile Communications) but no proof of concept is given.

However, the approaches described above remain ineffective, owing to numerous inadequacies such as lack of detection mechanisms without maintaining user states and optimal accuracy and false-positive rates. Moreover, these methods fail to address subscriber's actual location checks and subscriber's belongings checks, leading to vulnerabilities such as interception of calls and SMS and location tracking. The recent research to detect and mitigate security attacks on the SS7 network is summarized in Tab. 2.

Table 2: Summary of recent research to mitigate security attacks in SS7 networks

Ref	Working	Algorithm/Tools used	Pro	Cons	Research gaps & possible solution
Ullah [5]	Overview of possible attacks on SS7	Suggests how critical security controls	–	Suggested critical security controls	Unable to verify actual subscriber's belonging and check actual location using received parameters alone. Need of actual subscriber check along with location verification to solve this issue. Further scrutiny is necessary to identify suspicious hosts by applying a mechanism to filter illegitimate messages.
Jensen et al. [7,16]	A brief overview of SS7 attacks, and SS7 core network entry points	Use of ML algorithms, i.e., K-means and twitter anomaly detection algorithm	Simulated prototype to detect attacks using K-means algorithm	Limited parameters	
Qasim et al. [8]	Overview of possible attacks on SS7	Use of ML algorithms, i.e., decision trees, SVM, random forest	Simulated prototype to detect attacks using ML techniques	Limited parameters	
Ullah et al. [9]	Overview of possible attacks on SS7	Use of generic ML algorithms, i.e., ANN, pattern recognition and rule base filtering for already presented parameters by [7,16]	Simulated prototype to detect attacks using rule-based filtering	Limited parameters	
Rao et al. [31]	Gave an overview of SS7 location tracking attacks with methods	Recommends a generic approach and suggests better practices	Brief report on entry points of SS7	Suggested generic solution	

4 Proposed Anomaly Detection Model

The proposed anomaly detection model shown in Fig. 1 comprises four phases and is explained below.

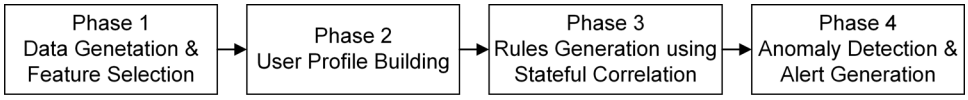

Figure 1: Proposed anomaly detection model

4.1 Phase 1-Data Generation and Feature Selection

An open-source SS7 attack simulator defined by Jensen et al. [16] was used to simulate an SS7 network that produces regular and abnormal traffic, detecting anomalies and generating alerts. Three network operators are created using the SS7 attack simulator complex mode. The first network operator (A) has a subscriber as a victim, the second network operator (B) is considered as a roaming network, and the third network operator (C) has an adversary as a subscriber. These operators interact with each other using thirteen standard messages, which do not involve an attack procedure reflecting the usual network traffic. Along with the regular messages, location tracking and call/SMS intercept attacks are carried out using MAP UpdateLocation (UL) and MAP ProvideSubscriberInfo (PSI) messages requests which target operator A's subscriber. The attacks are simulated by an attacker who is a subscriber from network operator C.

A set of features as illustrated in Tab. 3 are selected to create a subscriber profile in network operator A. This profile is used to detect an abrupt change in the location of the subscriber and malformed parameters anomalies.

Table 3: Features selected to detect anomalies

Feature description	Type
1. SCCP layer elements	1. SCCP layer elements
a. Calling party address (CgPA)	a. Destination address
b. Called party address (CdPA)	b. Source address
c. Calling & called GT digits	c. Global title codes
d. e164.country_code	d. Country code–numbering plan
e. Subsystem number (SSN)	e. HLR/VLR/MSC number
2. TCAP layer elements	2. TCAP layer elements
a. Application context name (ACN)	a. Object identifier
b. Local & global opcodes	b. Operation codes
3. GSM MAP layer elements	3. GSM MAP layer elements
a. Local & global opcodes	a. Operation code
b. IMSI, e.mcc, e.mnc	b. User HLR database objects
c. MSC/VLR number, MSISDN	c. User current connected location
d. e164.country_code	d. Country code
e. Location area code	e. Location area, paging area
4. Timestamps of message requests	4. Time of message requests received

4.2 Phase 2-User Profile Building

We have proposed to build a user profile to capture the behaviour of subscribers. Because when an attack occurs, it will introduce abnormalities in the subscriber's behaviour contrary to its profile parameters. The anomalies introduced in profile due to attacks can be detected by analyzing user profiles using our proposed Rule-based filtering with stateful correlation. One would assume that a simple metric comparison with a changed threshold would detect an attack, but this simple method will not always be successful in attack detection due to the dynamic nature of subscriber actions as it may also assume the rightful user as an attacker. Our proposed model avoids this scenario by building a user profile that is compatible with stateful correlation algorithms. This serves as a key to detect anomalous behaviour.

We create a user profile using the algorithm shown in Fig. 2 with the help of the following attributes derived from the synthetic data file from phase one:

- Message request type (UL, PSI)
- Previous location-old VLR LAC
- Time since previous location update
- Message network origin-new VLR LAC
- ACN
- CgPA, CdPA fields (global title, SSN)
- paging Area
- e212.mcc and e212.mnc

In the algorithm illustrated in Fig. 2, the dataset from the simulator is given as input to the User profile-building algorithm. The algorithm builds a User Profile by retaining states using MAP UpdateLocation (UL) message requests of all network subscribers. The last VLR address, current VLR address, and time between the current and last location update message are the main features to build a user profile. The last known VLR address is retrieved by the VLR address stored in HLR, based on successful location updates, and the current VLR address will be retrieved from the new VLR database. The time difference is calculated by subtracting the last UL message request timestamp from the current UL message request timestamp. Both VLR address features are used to find the coordinates of the subscriber, and the time difference feature is used in the time velocity check rule of the stateful correlation module from Section 4.3.

Algorithm : User Profile Building

```
Result: User Profile
initialization
last-update, last-lac = None
message-counter = 0
Groupby all inbound messsage for each IMSI
for each inbound messsage do
    if message-type == 'invoke updateLocation' OR
    message-type == 'invoke provideSubscriberInfo'
    OR message-type == 'invoke sendRoutingInfo' then
        message-counter +=1
        new-lac = message[lac]
    end
    if if last-lac is None then
        last-lac = new-lac
    end
    distance-traveled = lac-distance(last-lac, new-lac)
    if last-update is None then
        last-update-date = message[timestamp]
        old-location = message[sccp.calling.digits]
    end
    dt1 = message[timestamp]
    dt2 = last-update-date
    last-update-sec = (dt1 - dt2).total-seconds()
    last-update-mins = (dt2 - dt1)
    last-update-date = message[timestamp]
    create user profile ([parameters list])
    last-lac = message[lac]
end
```

Figure 2: User profile building module

4.3 Phase 3–Rules Generation Using Stateful Correlation

If an operator can maintain subscriber states, it would be possible to identify anomalies in how a single subscriber moves geographically. For example, according to our simulation, the subscriber from operator A would travel consistently daily. An anomaly occurs when an attacker uses the MAP UpdateLocation (UL) message with a different location that is significantly far away from the subscriber's current location. This signals a journey between two far away locations in a brief period. The user profile is built to detect this anomalous behaviour. We achieve this by correlating the time and distance travelled by the subscriber from his last known VLR location to his current VLR location (updated by the attacker). Fig. 3 describes the algorithm to detect anomalous updated location requests. Stateful security checks and time distance correlation are performed with the help of the attributes derived from the user profile listed in Section 4.2 to generate rules. Below are the step-by-step details of rules generation.

Algorithm : Time Distance Correlation Algorithm

Input: User Profile data
Result: minimum Travel Time and Distance from Old Vlr to New Vlr
Function FindCoordinates()(*OldVlr, NewVlr*):
  Find lat, lon of OldVlr and NewVlr using OpenCellId API
  return lat, lon of OldVlr and NewVlr
End Function
Function FindDistance():
  FindCoordinates()
  $\varnothing$ = Latitude
  λ = Longitude
  $distance = 2R\,arcsin\left(\sqrt{sin^2\left(\frac{\varnothing_2-\varnothing_1}{2}\right) + cos(\varnothing_1)cos(\varnothing_2)sin^2\left(\frac{\lambda_2-\lambda_1}{2}\right)}\right)$
  return *distance*
End Function
Function FindTravelTime():
  Travel-Time using Google Distance Matrix API
  return Travel-Time
End Function
Function Main():
  distance = **FindDistance()**
  minimum-travel-time = **FindTravelTime()**
End Function

Figure 3: Time distance correlation algorithm

4.3.1 Detect Anomalous Updated Location Request

The algorithm given in Fig. 3 is used to get the exact coordinates of the subscriber's last known VLR location and current VLR location addresses from the user profile. The Great Circle Distance Haversine formula is used to find the distance between these two coordinates. After calculating distance, it is required to calculate the minimum travel time between the same for which Google Map distance matrix API has been used. This minimum travel time is used as a threshold of the time required for travelling between the current and last known VLR location. If the time difference between the two updateLocation (UL) message requests (using message timestamp) is less than this threshold time, an anomaly has been detected. This anomaly detection rule has been labelled as a velocity check rule described in Fig. 4.

A. Find_Coordinates ()

In this function, we have used the OpenCellId API and the world cities database by simplemaps. The APIs return the coordinates of the given addresses, and these coordinates are saved as the subscriber's old and new VLR address coordinates.

B. Find_Distance ()

Using this function, we find the distance between the old and new VLR addresses. This distance is then correlated and used to identify irregularities since the last updateLocation (UL) message requests. To find the distance, we have used the Great Circle Distance Haversine formula [32]. This function finds the distance

between the old and new VLR address coordinates. The mathematical representation of the formula is shown as follows.

$$a = \sin 2\left(\frac{\Delta\varphi}{2}\right) + \cos\varphi 2 * \sin 2\left(\frac{\Delta\lambda}{2}\right)$$

$$c = 2 * \text{a} * \tan 2\left(\sqrt{a}, \sqrt{1-a}\right)\Big)$$

$$d = R * c$$

where φ is latitude, λ is longitude, R is earth's radius (mean radius = 6,371 km);

C. Shortest–TravelTime()

After finding the distance between old VLR and new VLR addresses, we have to find the minimum travel time between two location coordinates, for which we have used Google Maps distance matrix API [33].

```
Algorithm : velocity check rule
  Result: Block packets if the received VLR
  address in the CgPA is not reasonable with
  last known location
  for each inbound messsage do
  |  if MAP opCode = UpdateLocation AND
  |  (minimum travel time >time difference
  |  between messages ) then
  |  |  BLOCK;
  |  else
  |  |  ALLOW;
  |  end
  end
```

Figure 4: Velocity check rule

4.3.2 Using Velocity Check Rule

The algorithm given in Fig. 4 will be called on each updateLocation (UL) request. It utilizes the algorithm illustrated in Fig. 3 to calculate the distance travelled and the minimum time required to travel this distance. If the timestamp difference between two updateLocation (UL) message requests is less than the minimum time threshold, a velocity check anomaly has been detected, showing that the subscriber location has been abruptly changed.

4.3.3 Detect Malformed and Inconsistency in Parameters Between Layers

A. Using Malformed Parameters Check Rule

The MAP OpCodes are the key identifiers for MAP category messages 1 or 2 threats. Recommendations and evidence to date show that using the MAP OpCode alone is sufficient to apply rules to such MAP messages. However, it is anticipated that the ACN may provide the environment to carry out different attacks by malformed it or even removing it from the message parameters [34]. Therefore, the ACN is considered a valuable factor for anomaly detection from a rule's definition perspective. Similar anomalies may be distinguishable by the absence of the OpCode value and numbering plan alterations for attacking subscribers [34]. From Fig. 5, we can see how these malformed parameters can be used to attack subscribers.

The following malformed parameters check rule algorithm in Fig. 6 will be called on each PSI message request.

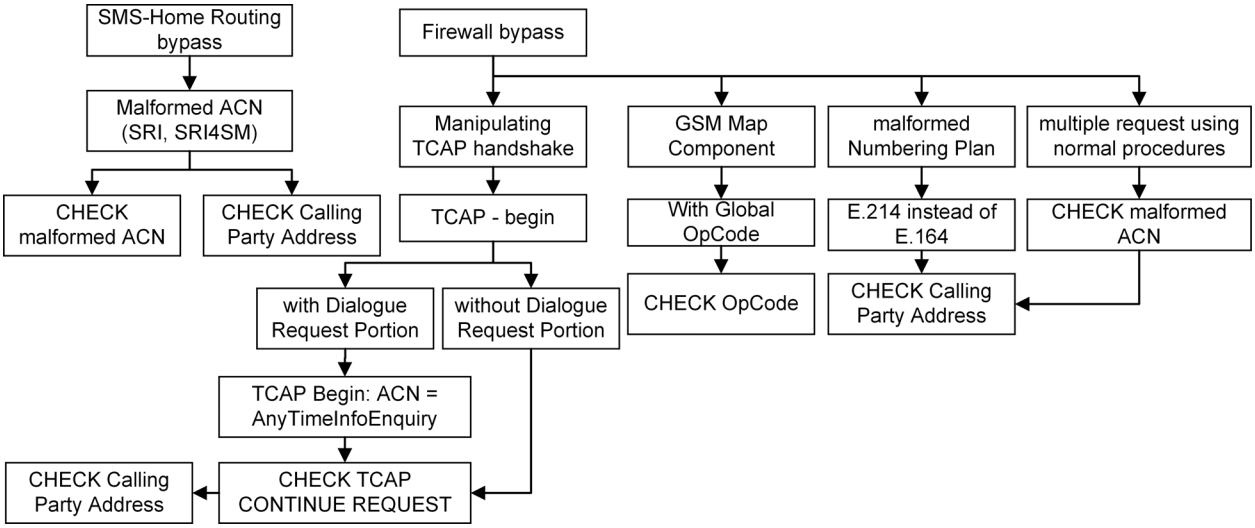

Figure 5: Different ways of attack personifications using malformed parameters

Algorithm : malformed parameters check rule

Result: Block all received messages with malformed application context name (ACN), numbering plan & OpCode

initialization
ACN = associated ACN list with respect to MAP message requests
NP = associated numbering plan list with respect to MAP message requests
OPCode = associated OPCode list with respect to MAP message requests
for *each inbound MAP messsage request* **do**
  if *MAP ACN not NOT IN ACN* **then**
    BLOCK;
  else
    ALLOW;
  end
  if *MAP numbering plan NOT IN NP* **then**
    BLOCK;
  else
    ALLOW;
  end
  if *MAP OpCode NOT IN Opcode* **then**
    BLOCK;
  else
    ALLOW;
  end
end

Figure 6: Malformed parameters check rule

B. Using Addressing Correlation & Inconsistent Message Format Check Rule

Attack messages may contain inconsistencies to hide or spoof a sender or the purpose of the packet. One way to discover a potential attack is to perform consistency checks between the layers or messages themselves. Another efficient check is to perform cross-layer checks on addressing information, for example, to validate if the CgPA in the SCCP layer and the information available, e.g., GT(s), in the MAP layer belong to the same operator.

Other inconsistencies may involve a comparison of expected parameters based on usage. For example, a comparison of the TCAP Application Context used per packet type/operation code, i.e., using a MAP InsertSubscriberData packet with a vcsgLocationUpdate application context name classed abnormal. In

this case, the check ensures that the context needs to be consistent with the usage. The parameters inconsistency checking rules are described in Figs. 7 and 8, respectively.

```
Algorithm : Parameters Inconsistency
between Protocol Layers rule 1
  Result: Block all outbound roaming subscribers
  messages where MCC + MNC of IMSI AND CdPA or prefix
  ID of the HLR do not match
  for each inbound messsage do
  |  if MAP opCode = vPlmnOriginating AND
  |  (operatorByMAP != operatorByCdPA OR
  |  operatorByMAP != operatorByHLRid ) then
  |  |  BLOCK;
  |  else
  |  |  ALLOW;
  |  end
  end
```

Figure 7: Parameters inconsistency check rule 1

```
Algorithm : Parameters Inconsistency
between Protocol Layers rule 2
  Result: Block all outbound roaming subscribers
  messages where VLR Id AND CgPA do not match
  for each inbound messsage do
  |  if MAP opCode = vPlmnOriginating AND
  |  (operatorByVlrid != operatorByCgPA) then
  |  |  BLOCK;
  |  else
  |  |  ALLOW;
  |  end
  end
```

Figure 8: Parameters inconsistency check rule 2

In a nutshell, for UL message requests, time distance correlation is considered, and for PSI and SRI messages requests, parameters pattern matching is performed.

4.4 Phase 4-Anomaly Detection and Anomaly Blocking Alert

The time velocity check rule, malformed parameters check rule, and inconsistency in parameters between protocols layers check rules must be utilized to detect anomalies and generate blocking alerts. One way is to apply all these checks on all message types; however, that would not provide an efficient implementation. Hence, we propose to apply the velocity check rule only for updateLocation (UL) message requests. Applying malformed parameters check rule and inconsistency in parameters between protocol layers rules for Provider Subscriber Info message requests and Send Routing Info message requests. The anomaly detection algorithm is given in Fig. 9.

The proposed model can detect multiple attacks happening at the same time from different regions. The proposed model works in conjunction with the existing SS7 firewall at network borders and checks each inbound packet whether it is malicious. Parallelization, known as load balancing firewalls, is an architecture that allows packet inspection under high traffic loads and speeds. Parallel firewall designs are used to cater to multiple attacks happening simultaneously [34].

```
Algorithm 1: Anomaly Detection Algorithm
Result: Block all received Anomalous messages
for each inbound messsage do
    if message-type == 'invoke updateLocation' then
        RUN velocity check rule
    end
    if message-type == 'invoke provideSubscriberInfo'
    OR message-type == 'invoke sendRoutingInfo' then
        RUN malformed parameters check rule
        RUN Parameters Inconsistency check rules
    end
end
```

Figure 9: Anomaly detection algorithm

5 Results and Discussion

5.1 Results

The proposed model using the feature set proposed as illustrated in Tab. 3 was tested to detect the anomalies and mitigate attacks. The results show an increased true positive rate (TPR) and a low false alarm rate (FAR), respectively. This performance is compared with existing algorithms and methods, as shown in Tab. 4, demonstrating the proposed model better.

Table 4: Evaluation of the proposed model with the existing algorithms

Evaluation matrix / Algorithms	Detection rate %	False alarm rate %	True positive %
K-means clustering	100	49	75.25
SHESD algorithm	100	43	57
Rule-based filtering	98.8	33.2	66.8
Pattern recognition ANN	99.58	24	76
The proposed model	99.95	18.18	99.90

We have used a dataset of 7,056 samples generated using the SS7 attack simulator. Out of these samples, 11 samples were detected as anomalies for a particular MAP updateLocation (UL) message request, and 100 MAP ProviderSubscriberInfo (PSI) message requests were detected as anomalies out of a total of 2145 anomalies. Based on the dataset for a particular MAP updateLocation (UL) message request, 9 of these detected anomalies were actual attacks, i.e., true positives, leaving four false positives. Similarly, for MAP ProviderSubscriberInfo (PSI) message request, 96 of these detected anomalies were actual attacks, i.e., true positives, leaving only two false positives in case of MAP updateLocation (UL) message request and four false positives for MAP ProviderSubscriberInfo (PSI) message request. The accuracy of the detection of attacks was 99.95%.

Based on the results in Tab. 4, it can be concluded that rule-based filtering for all SS7 MAP messages can be implemented for actual SS7 network data. From the results illustrated in Tab. 4, machine learning can be applied successfully, and it can detect zero-day attacks. However, it can skip some legitimate attacks and generate more false alarms than rule-based filtering. As opposed to machine learning techniques, rule-based filtering can filter various types of messages with greater accuracy. It is supposed to produce fewer false alarms than machine learning techniques. The limitation of rule-based filtering is that it requires a separate rules template for all category types of SS7 messages for attack detection. Furthermore, more excellent knowledge of the internal functioning of the SS7 network is required for the design of these templates.

5.2 Evaluation Matrix

The Anomaly detection model is evaluated using the following metrics:

- True Positive (TP), the number of instances correctly predicted as attacks.
- False Positive (FP), number of instances wrongly predicted as attacks.
- True Negative (TN), the number of instances correctly predicted as non-attacks.
- False Negative (FN), the number of cases wrongly predicted as non-attacks.
- Accuracy = TP + TN/(TP + FP + FN + TN)
- False Alarm Rate = FP/(FP + TN)
- Detection Rate = DR = TP/(TP + FN) It is the ratio between the total numbers of attacks detected by the system to the total number of attacks present in the dataset

The results are validated by comparing with A-NADS [16] and Anomaly Detector [9].

5.3 Discussion

Defending and shielding mobile networks is a foremost concern for mobile network operators. The use of internet protocol (IP) by the telecom industry and the deregulation and liberalization of mobile network architecture makes the network easily accessible to an attacker. Along with the use of off-the-shelf hardware, an attacker could efficiently perform imminent attacks. The persisting causes behind vulnerabilities and attacks are the lack of checking a subscriber's belonging to a network and their actual location, lack of message filtering mechanisms, and SMS Home Routing configuration flaws in the current infrastructure.

Since the SS7 network standards remain in use for decades, only new network generations can make structural or reverse incompatible changes. To eliminate insecure legacies, we could use 5G's window of opportunity to develop future mobile safety specifications. As the previous generation of network technology will still be in use (backward compatibility), there is a need to solve these issues in legacy networks. The persisting challenges where an attacker can perform location tracking attack via Global Opcode by using PSI message request with Global Opcode tag and could do Voice call interception (MiTM) with the help of ISD message request and double MAP messages requests to perform MiTM attack are unable to be prevented by the present signalling firewalls. The existing signalling firewalls could only inspect and forward message requests to the network for processing and do not bother about the incorrectness of request and response back, leading to location tracking attacks [34].

While 3G and 4G mobile networks' security properties have improved dramatically compared to 2G (GSM), there are still substantial limitations in users' privacy. Several potential changes to the 2G–4G protocols have been proposed to ensure more excellent protection for users; however, they all entail substantial alterations to currently deployed infrastructures, which are almost certainly not realistic to achieve in practice [35]. Signalling networks attack risks are becoming very common, forcing the industry to protect its infrastructure very severely. As the industry is trying to find preventing measures, adversaries, at the same time, are trying to scale their attack vectors over different technologies from 2G/3G to 5G. Due to undermined mobile security, signalling infrastructure is continuously being compromised somehow. Real-time intelligent defensive monitoring can understand, track, and respond to these intimidations. The introduction of emerging technology and modernization has led to the realization that the SS7 core network is no longer a stable network that has accelerated its weaknesses and defences. Even after this acknowledgement, SS7 vulnerabilities and exploits were not widely documented or well-known due to complicated cellular networks, complex protocols, and elusive network interfaces [36].

6 Conclusion

In SS7, the networks' backward compatibility, such as 4G to 3G, market deregulation, and exposure to the IP technology, makes the attack vectors possible. The attacks are mainly caused by "unsecured pre-authentication traffic" and "wireless channel openness." While the modifications to the protocol and current cryptographic techniques can solve unsafe pre-authentication, more substantial network architecture improvements are needed for the wireless channel. Network architecture flaws can only be mitigated by regular monitoring and analysis of real-time network traffic and message filtering mechanism. As mentioned earlier, those can be accomplished by rigorous attack detection and response systems to protect against the attacks described.

The existing methods are unable to identify suspicious hosts as they use a minimal number of parameters. In this research, Rule-based filtering with stateful correlation is proposed to detect attacks against the SS7 network. The proposed anomaly detection model performs better than the existing methods in terms of attack detection rate, false alarm rate, and true positive rate. The proposed anomaly detection model performs 0.37% better in terms of security attack Detection Rate, 24.25% better in terms of False Alarm rate, and 31.45% better in terms of True Positive rate when compared with the existing Pattern Recognition ANN algorithm that is the closest in terms of performance.

Acknowledgement: This research work was supported by Taylor's University, Malaysia, through Taylor's Ph.D. Scholarship Program.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. Jensen, "Improving SS7 security using machine learning techniques," M.S. thesis. Department of Computer Science and Media Technology, Norwegian University of Science and Technology, Gjøvik, Norway, 2016.

[2] B. Welch, "Exploiting the weaknesses of SS7," *Network Security*, vol. 2017, no. 1, pp. 17–19, 2017.

[3] S. Puzankov, "Stealthy SS7 attacks," *Journal of ICT Standardization*, vol. 5, no. 1, pp. 39–52, 2017.

[4] M. Shi, "Alternative solutions for the improvement of SS7 security," in *Proc. ITU Workshop on SS7 Security*, Geneva, Switzerland, pp. 1–23, 2016.

[5] K. Ullah, "Enhancing security architecture of signalling system no.7 with emphasis on machine learning techniques to detect vulnerabilities," M.S. thesis. Dept. Faculty of Information Security, Military College of Signals, National University of Sciences and Technology, Rawalpindi, Pakistan, 2018.

[6] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury and E. Bertino, "5Greasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol," in *Proc. ACM SIGSAC Conference on Computer and Communications*, London, United Kingdom, pp. 669–684, 2019.

[7] K. Jensen, H. T. Nguyen, T. V. Do and A. Arnes, "A big data analytics approach to combat telecommunication vulnerabilities," *Cluster Computing*, vol. 20, no. 3, pp. 2363–2374, 2017.

[8] T. Qasim, M. H. Durad, A. Khan, F. Nazir and T. Qasim, "Detection of signaling system 7 attack in network function virtualization using machine learning," in *Proc. 15th Int. Bhurban Conf. on Applied Sciences and Technology*, Bhurban, Pakistan, pp. 484–488, 2018.

[9] K. Ullah, I. Rashid, H. Afzal, W. Iqbal and Y. A. Bangash, "SS7 vulnerabilities-a survey and implementation of machine learning *vs*. rule based filtering for detection of SS7 network attacks," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2, pp. 1337–1371, 2020.

[10] D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl and C. Popper, "On security research towards future mobile network generations," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 3, pp. 2518–2542, 2018.

[11] S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury and E. Bertino, "Insecure connection bootstrapping in cellular networks: The root of all evil," in *Proc. 12th ACM Conf. on Security and Privacy in Wireless and Mobile Networks*, Miami, Florida, USA, pp. 1–11, 2019.

[12] U. Noor, Z. Anwar, A. W. Malik, S. Khan and S. Saleem, "A machine learning framework for investigating data breaches based on semantic analysis of adversary's attack patterns in threat intelligence repositories," *Future Generation Computer Systems*, vol. 95, no. 1, pp. 467–487, 2019.

[13] E. Magklaris, "Attacks on SS7," M.S. thesis. Department of Digital Systems, University of Piraeus, Piraeus, Greece, 2019.

[14] S. Holtmanns, "Interconnection security standards-we are all connected," *Journal of ICT Standardization*, vol. 4, no. 1, pp. 1–18, 2016.

[15] F. Liu, J. Peng and M. Zuo, "Toward a secure access to 5G network," in *Proc. 17th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications*, New York, USA, pp. 1121–1128, 2018.

[16] K. Jensen, T. Van Do, H. T. Nguyen and A. Arnes, "Better protection of SS7 networks with machine learning," in *Proc. 6th Int. Conf. on IT Convergence and Security*, Prague, Czech Republic, pp. 1–7, 2016.

[17] M. B. Savadatti and D. Sharma, "SS7 network and its vulnerabilities: An elementary review," *Imperial Journal of Interdisciplinary Research*, vol. 3, no. 3, pp. 911–916, 2017.

[18] G. Sharma, "SS7 signaling protocol-attacks against privacy," *International Journal of Engineering Research in Computer Science and Engineering*, vol. 3, no. 7, pp. 1–5, 2016.

[19] S. Holtmanns, S. P. Rao and I. Oliver, "User location tracking attacks for LTE networks using the interworking functionality," in *Proc. 2016 IFIP Networking Conf. and Workshops*, Vienna, Austria, pp. 315–322, 2016.

[20] J. Cao, M. Ma, H. Li and Y. Zhang, "A survey on security aspects for LTE and LTE-A networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 283–302, 2014.

[21] B. Hall, "Positive research," *Journal of Information Security*, vol. 2018, no. 1, pp. 104–121, 2018.

[22] T. Van Do, P. Engelstad, B. Feng and V. T. Do, "A near real time SMS grey traffic detection," in *Proc. 6th Int. Conf. on Software and Computer Applications*, Bangkok, Thailand, pp. 244–249, 2017.

[23] P. N. Yeboah, "Proposal and implementation of an IDS for potential SMS spam signaling messages on SS7," M. S. thesis. Department of Telematics, Norwegian University of Science and Technology, Norway, 2016.

[24] M. Sahin, "Understanding telephony fraud as an essential step to better fight it," Ph.D. dissertation. Department of Telecommunication et Electronique, ParisTech Institute, Paris, 2017.

[25] M. A. Azad and R. Morla, "Rapid detection of spammers through collaborative information sharing across multiple service providers," *Future Generation Computer Systems*, vol. 95, no. 1, pp. 841–854, 2019.

[26] K. Sultan, H. Ali and Z. Zhang, "Call detail records driven anomaly detection and traffic prediction in mobile cellular networks," *IEEE Access*, vol. 6, no. 1, pp. 41728–41737, 2018.

[27] T. M. Aung, K. H. Myint and N. N. Hla, "A data confidentiality approach to SMS on android," *Intelligent Computing & Optimization Springer*, vol. 866, no. 1, pp. 505–514, 2018.

[28] L. Abdelrazek and M. A. Azer, "SigPloit: A new signaling exploitation framework," in *Proc. 2018 Tenth Int. Conf. on Ubiquitous and Future Networks*, Prague, Czech Republic, pp. 481–486, 2018.

[29] C. Liu, X. Ji, J. Wu and X. Qin, "A proactive defense mechanism for mobile communication user data," *Science China Information Sciences*, vol. 61, no. 10, pp. 6–8, 2018.

[30] S. Holtmanns, I. Oliver and Y. Miche, "Mobile subscriber profile data privacy breach via 4G diameter interconnection," *Journal of ICT Standardization*, vol. 6, no. 3, pp. 245–262, 2018.

[31] S. P. Rao, I. Oliver, S. Holtmanns and T. Aura, "We know where you are," in *Proc. 2016 8th Int. Conf. on Cyber Conflict*, Tallinn, Estonia, pp. 277–293, 2016.

[32] E. Winarno, W. Hadikurniawati and R. N. Rosso, "Location based service for presence system using haversine method," in *Proc. Int. Conf. on Innovative and Creative Information Technology*, Salatiga, Indonesia, pp. 1–4, 2017.

[33] S. C. Satapathy, V. Bhateja and S. Das, "Smart intelligent computing and applications," in *Second Int. Conf. on SCI, 2018, Proc.: Smart Innovation, Systems and Technologies Book Series*, Singapore, vol. 104, pp. 1–731, 2018.

[34] T. E. Hadjadj, R. Tebourbi, A. Bouhoula and R. Ksantini, "Optimization of parallel firewalls filtering rules," in *Proc. 2019 Int. Conf. on Software, Telecommunications and Computer Networks*, Split, Croatia, pp. 1–6, 2019.

[35] K. Puzankov, "Hidden agendas: bypassing GSMA recommendations on SS7 networks ongoing security," in *Proc. Hack in the Box Security Conf.*, Amsterdam, Netherlands, pp. 1–59, 2019.

[36] V. T. Do, P. Engelstad and B. Feng, "Strengthening mobile network security using machine learning," in *Int. Conf. on Mobile Web and Information Systems, Proc.*, *Lecture Notes in Computer Science Book Series*, Vienna, Austria, vol. 9847, pp. 173–183, 2016.