A Data Mining Framework for Securing 3G Core Network from GTP Fuzzing attacks

Faraz Ahmed, M Zubair Rafique and Muhammad Abulaish

Center of Excellence in Information Assurance (CoEIA)
King Saud University (KSU)
Riyadh, Saudi Arabia
{fahmed.c, zrafique.c, mabulaish}@ksu.edu.sa

Abstract. Since the emergence of 3G cellular IP networks, internet usage via 3G data services has become ubiquitous. Therefore such network is an important target for imposters who can disrupt the internet services by attacking the network core, thereby causing significant revenue losses to mobile operators. GPRS Tunneling Protocol GTP is the primary protocol used between the 3G core network nodes. In this paper, we present the design of a multi-layer framework to detect fuzzing attacks targeted to GTP control (GTP-C) packets. The framework analyzes each type of GTP-C packet separately for feature extraction, by implementing a Markov state space model at the G_n interface of the 3G core network. The Multi-layered architecture utilizes standard data mining algorithms for classification. Our analysis is based on real world network traffic collected at the G_n interface. The analysis results show that for only 5% fuzzing introduced in a packet with average size of 85 bytes, the framework detects fuzzing in GTP-C packets with 99.9% detection accuracy and 0.01% false alarm rate.

Keywords: Intrusion Detection, Fuzzing attacks, GTP Security

1 Introduction

Connecting millions of people around the globe and providing exciting services to end users, the demand of internet is ever rising [1]. Every effort has been made to improve the user experience and to increase the Internet's circle. Cellular networks provides only voice services but, with the advent of 3G technologies mobile operators are providing data services with low broadband speed. The main reason for the popularity of 3G network is its ability to provide greater bandwidth with wide area coverage. Several data transmission techniques have been proposed for better performance, e.g., WCDMA, TD/CDMA and CDMA2000 are different Code Division Multiple Access techniques used for data transmission. The first two techniques are based on General Packet Radio Service (GPRS) and hence have the same core network architecture [2]. Our framework targets the security of GPRS core network interface, i.e., G_n interface.

As compared to the widespread use of internet via cellular network there is a huge threat to the security of the network. Attacks can come from inside the cellular network [3]. These attacks can cause network degradation and eventually lead to `Denial of Service` (DoS) to end users. However, 3G networks have some of their own security issues as addressed in [4] and [5]. Due to open nature of IP in 3G networks, attackers can exploit vulnerabilities in their core network nodes and protocols. Attacks on the core nodes of the 3G networks can be launched by compromising different nodes of the architecture such as the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN) [6]. As explained in [7], an attacker can establish herself as a legitimate 3G network element by IP spoofing. Such attacks pose serious threat to mobile user privacy by stealing user data such as $IMSI$ number, billing information, contact details, etc. An attacker can exploit protocol vulnerabilities by fuzzing sensitive fields of packet headers [8]. GPRS Tunneling Protocol GTP is the main communication protocol used in the core network. All user requests for internet services are made through GTP.

In this paper, we have analyzed the GTP protocol vulnerabilities and proposed an effective and efficient multi-layered framework for their mitigation. Our analysis is based on real world GTP (v1) traffic collected at the G_n interface. The main contribution of our work is a framework that can detect GTP-C fuzzing attacks in real time. It consists of three main modules: i) Packet Byte Analyzer (PBA), ii) Benign Packet Definition (BPD), and iii) Decision Module. The fuzzing is detected by modeling the differences in byte sequences of normal and fuzzed packets. We use Markov state-space model for extracting features. The less discriminative features are then pruned by using an information theoretic measure known as `Information Gain`. Each incoming packet is fed to BPA which performs the feature extraction and forwards them to the BPD module. The BPD module uses the extracted feature set as input and represents each packet as a feature vector. The decision module implements standard data mining algorithms to classify the incoming packets as normal or malformed. The rest of the paper is organized as follows. Section 2 gives a brief summary of the related works. In Section 4, we report different statistics of our real world benign dataset. Section 5 presents the architectural detail of the proposed framework. Section 6 presents the experimental setup and results. Finally in section 7, we conclude the paper with future directions of work.

2 Related Work

The attacks in the cellular networks are not unprecedented. Some known attacks are directed towards Mobile Stations (MSs) [9] and [10] whereas, some attacks try to disrupt the services in general as mentioned in [11] and [3]. [12] presents a taxonomy of such 3G attacks. The attacks have been classified as *Cross-Infrastructure*, which are directed from the internet to the cellular networks, and *Single Infrastructure* attacks which arise from within a cellular network. In [13], Patrick et al. holds the opposite design philosophies of internet and 3G networks responsible for making 3G networks vulnerable to Denial of Service (DoS) attacks, and also demonstrates two more attacks supporting this theory. The author highlights the fact that bandwidth is not the ultimate cause of such attacks rather, it is the inflexibility of architecture of 3G networks that makes these attacks practical.

One of the foremost attempt to highlight the vulnerabilities of GPRS core network is presented in [4]. In this work, the author has provided an overview of attacks and flaws associated with GPRS architecture. The report also provides recommendations to avoid such type of attacks. A more detailed categorization of attacks against GPRS is followed in [8]. In this paper, the authors have listed Overbilling attacks, misconfigured WAP's exploits and a detailed list of GTP risks. The paper proposes an alternative design for network architecture that can be adopted by network operators. The authors also present `Check point Firewall` product that can provide additional security.

Another important contribution in securing GPRS from attacks on the GPRS core is presented in [6]. Dmitriadis et al. presents a threat model with regard to GPRS core network, depicting nine possible attack groups, and also gives a feasibility study of honeynets in 3G networks. The authors propose `3GHNET`, a honeynet, for the improvement of GPRS core network security. The authors have compared the advantage of 3GHNET implemented GPRS network over an unprotected network and used concepts from the game theory for comparison.

[2] presents a defense mechanism for GTP security threats. The authors propose an event-based description language for the detection of attacks directed towards the GTP protocol. They have classified GTP security concerns as protocol abnormal attacks, infrastructure attacks and resource consumption attacks. They have categorized the GTP protocol into GTP-C, GTP-U and GTP', which are GTP control plane, GTP user plane and GTP prime respectively and analyzed them separately to perform the decision on the basis of events generated. The authors have tested their architecture on OpenGGSN emulator which is an open source implementation of the core network nodes - SGSN and GGSN [14]. Our work is different from [2] as it aims at securing only the GTP-C category of the GTP protocol from fuzzing attacks. GTP-C packets are most important for the communication between the GSNs. The architecture of our scheme enables us to further categorize the GTP-C packets and analyze them separately.

3 GPRS Architecture

GPRS is an extension GSM, in fact it has been overlaid on the already existing GSM infrastructure [15]. To handle packet data, a Packet Control Unit(PCU) is introduced at Base Transceiver Station(BTS). Besides that two GPRS support nodes(GSNs) have been added to the structure. SGSN is connected with many BTSs analogous to BSC, and serves to transfer data requests over the network. Whereas GGSN facilitates to connect the network to external data network. Any user that intends to send/receive data from external network has to register a context with these two nodes(SGSN and GGSN). The different interfaces of GPRS are shown in Figure 5.

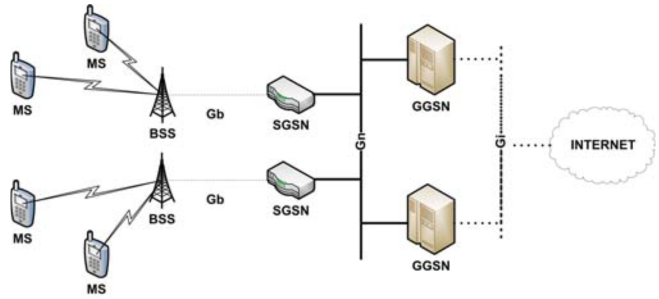
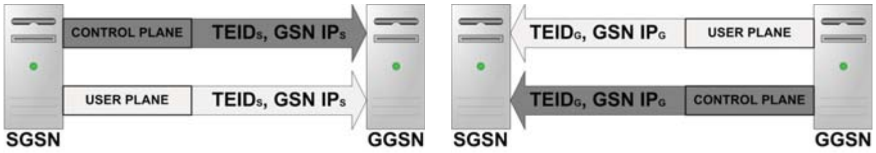


Fig. 1. Architecture of GPRS

The next section is dedicated to the description of this interface, and depicts how communication actually takes place on this interface. For the sake of brevity, we have only considered GTPv1 specifications for the matter at hand.

3.1 G_n interface

Whenever a user needs to send/receive packet data from external network, it requests the network to activate a PDP context. On receiving such a request, the SGSN sends a Create PDP context Request message containing IMSI number of the user,(Access Point NAme) APN and Tunnel Endpoint Identifiers (TEID) for GTP-C and GTP-U plane, to GGSN. Once the GGSN receives this information, it stores it for future correspondence and sends back Create PDP Context Response containing information elements(IEs to indicate wether the context was established successfully), End User Address field (which contains the IP address assigned by the GGSN to the user) and TEID for both GTP-C and GTP-U plane.



(a) Create PDP Context Request (b) Create PDP Context Response

Fig. 2. Context Establishment between SGSN and GGSN

Figure 2 demonstrates how a context is established between the two nodes, and how do SGSN and GGSN recognize tunnels at their ends, both in User and Control plane. When SGSN sends a Create PDP context Request to the

Table 1. Benign dataset summary

Type	**No.**	**Avg. Size(Bytes)**	**Description**
Create PDP Request	1183681	197	Request for initiation of user session
Create PDP Response	3866	135	Response to the initiation request
Update PDP Request	555	85	Request to update the QoS, TFT etc parameters
Update PDP Response	684	95	Response to the update parameter request
Delete PDP Request	4317	60	Request for termination of user session
Delete PDP Response	3237	56	Response to the termination request

GGSN as shown in Figure 2(a), it advertises a $TEID_S$ and an IP_S address for User plane and a $TEID_S$ and an IP_S(subscript S is used for SGSN) for Control plane to the GGSN, to be used in future by the GGSN when addressing the specified tunnel at SGSN. SGSN uses the same parameters(the $TEID_S/IP_S$ that it advertised) to discern between different tunnels operating at SGSN. Similarly, when GGSN responds with a `Create PDP context Response` message as shown in Figure 2(b), it advertises a $TEID_G$ and IP_G for User plane as well as for the Control plane to the SGSN, which are to be used in future by the SGSN when addressing a specific tunnel at GGSN. The GGSN uses these parameters to discern between different tunnels operating at GGSN. Also, the port numbers are fixed for both Control and User plane data. Similar to the `Create PDP Context Request/Response` messages, `Delete PDP Request/Response` messages also exist, which are used to delete an active tunnel. Since the payload of user is tunneled through the G_n interface, it becomes a natural choice for analysis when it comes to anomaly/intrusion detection in the core network. A compromised SGSN or GGSN can host attacks to other critical systems, such as the Mobile Switching Center (MSC), home location register (HLR), visitor location register (VLR) and other SGSN/GGSN nodes of the network. Such attacks directly affect crucial information such as subscriber identity database residing in the HLR, charging/ billing gateways (CG/BG), handoff operations which involves VLR etc.

4 Dataset

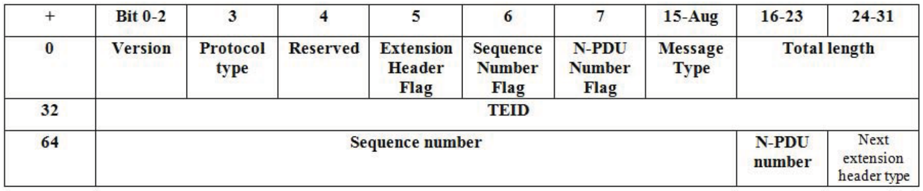
In this section we describe the benign and malformed GTP dataset that we have used in this study. We also give a brief description of our fuzzing algorithm used to generate malformed GTP packets.

4.1 Benign Traffic

Our benign dataset consists of real world GTP-v1 traffic collected at the G_n interface. The traffic was logged at GPRS core network `node`, during the peak usage hours of the day. All type of GTP packets were captured however, our analysis is based on only GTP-C packets, which are responsible for the creation and deletion of user sessions between the GSNs. Table 1 provides different statistics of the data set. The total number of PDP contexts shows the number of GTP tunnels created, updated or deleted between the SGSN and the GGSN. It is obvious that there are unequal number of requests and responses, which is due to window censoring phenomenon [16]. This means that user sessions initiated during the data logging period are not torn down before the end of the logging process.

4.2 Fuzzed Dataset

We performed fuzzing of each type of GTP-C packet separately. The format of the GTP packets is shown in Figure 3. For fuzzing, we have employed standard bit-fuzzing technique used for other IP-based protocols, i.e., for 1% fuzzing a bit is randomly selected from a packet and is inverted. Similarly for n% fuzzing, we select n% bits randomly from a packet and invert them. In this way, we have generated 24 different fuzzed datasets for each GTP-C packet category corresponding to 2%, 5%, 10% and 20% fuzzing of each n-gram where, n varies from 1 to 6.



+	Bit 0-2	3	4	5	6	7	15-Aug	16-23	24-31
0	Version	Protocol type	Reserved	Extension Header Flag	Sequence Number Flag	N-PDU Number Flag	Message Type	Total length	
32	TEID								
64	Sequence number							N-PDU number	Next extension header type

Fig. 3. GTP packet format

Our fuzzed dataset consists of packets with fuzzed fields such as `message type` field. Fuzzing this type of field changes the message type, for example, from `Create PDP Context Request` message(message type=0x10) to some other message type, which may result in a message type that is not recognizable by the GGSN or in a message type that GGSN is not expected to receive. In addition, there are some information elements following the mandatory header in the message that are more apposite for fuzzing. This is because each type of packet uses the extension header information elements differently. More specifically, the information elements(IEs) are divided into TV (Type, Value) or TLV (Type,Length,Value) format. Figure 4 shows details of the formatting of such IEs. Our fuzzed dataset include packets with fuzzed TV-formatted IE's because when we fuzz such a field, the length of the fuzzed field may increase from that of the expected length known to the GGSN, making the IEs following it to be unreadable. The fuzzed packet dataset also contains fuzzed values of TLV-formatted IEs fields, end user address, access point name (APN), protocol configuration options (PCO) and GPRS serving node (GSN) address IEs. Table 2 describes the possible impact of fuzzing different fields of GTP packet.

Table 2. Fuzzed fields and possible results of fuzzing

Fuzzed Field	Explanation	Result
Message Type	Allows 255 different message types values	Invalid message type
IE	Contain packet specific information	DoS/Dependent on Device Vulnerability
IE length	Contains the length of IE	Buffer overflow/System Crashes
End User Address	Address of the Mobile Station	DoS/Dependent on Device Vulnerability

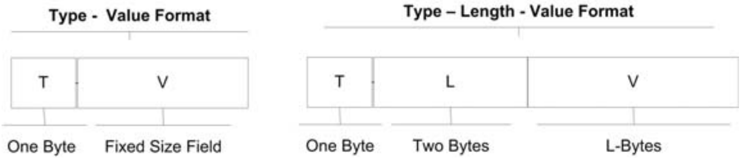


Fig. 4. Information element formats

5 GTP Malformed Packet Detection Framework

In this section, we present the architectural detail of the proposed intrusion detection framework, which consists of a bi-directional detection module at the G_n interface. Figure 5 shows the architecture of the proposed framework for detection of malformed GTP packets. GTP protocol is used by most of the 3G transmission techniques including WCDMA and TD/CDMA, which employ the GPRS core network architecture. So for simplicity we consider the GPRS network for explanation of the proposed framework. SGSN is connected with many Base Transceiver Stations (BTSs), and serves to transfer data requests over the network. Whereas GGSN facilitates to connect the network to external data network. The architecture secures the control plane of the GTP protocol by employing a parallel design. The parallel architecture has two main advantages. Firstly, it reduces the processing overhead by the simultaneous analysis of different GTP control packets and secondly, it allows a deeper level of inspection by analyzing each packet type according to its use of extension headers as explained in section 4.2. The detection framework perform byte-level analysis of the incoming GTP-C packets and classify them as normal or malformed. The proposed framework consists of three main modules - Packet Byte Analyzer, Benign Packet Definitions, and Decision module. A detailed description of these modules appears in the following sub-sections.

5.1 Packet Byte Analyzer

The PBA module acts separately for each type of GTP control packet. Its inputs are the validated GTP packets. The validation process is done through an input interface, which checks input packets for explicit errors like invalid message type. For each packet, it performs a byte-level analysis. The module uses a windowing methodology for the collection of important discriminating features. It implements a sliding window of n bytes. Given a byte sequence P_s, of a packet P, sliding a window of size $n = 1$, we get $P_s =< \Phi_1, \Phi_2, ..., \Phi_i, .. >$, where Φ_i

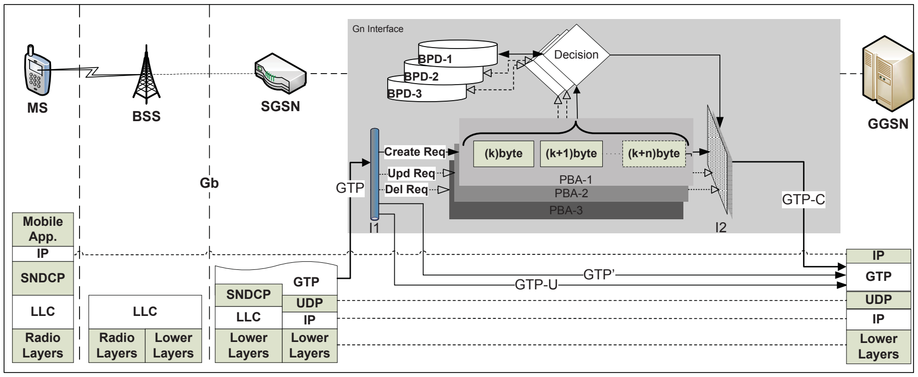


Fig. 5. Architecture of proposed framework for GTP fuzzing attacks

represents the i^{th} byte of P. Similarly for $n = 2$ the representation becomes $P_s =< \Phi_1|\Phi_2, \Phi_2|\Phi_3 ..., \Phi_{i-1}|\Phi_i, .. >$, where the symbol $|$ represents a string concatenation operator. This relation explains the tradeoff that exists between the amount of information and the size of the training data. Therefore, a thorough analysis for the selection of the window size is necessary for better performance. Accordingly, we model the byte sequences so that analysis can be performed with varying window size. For this, we use discrete time Markov chain. We consider the position of the window $(size = n)$ as a state which changes in accordance with the window slides. Therefore, for a representation P_s if $S = s_0, s_1, ..., s_k$ is the set of possible states, then the position to state mapping function can be described as: $(f : p_i \rightarrow s_j \in S)$ where, $p_i \in P =< p_0, p_1, ..., p_m >$. So for two consecutive window positions the mapping functions are $(f : p_i \rightarrow s_x)$ and $(f : p_{i+1} \rightarrow s_y)$. The transition between two states is represented as s_{xy} and that the transition probability as τ_{xy}. This gives a state transition probability matrix calculated as $F : S \times P \rightarrow \tau(S)$ where, F is a transition function. The PBA computes $\tau(S)$ for each packet and outputs the probability matrix which is used by the decision module.

5.2 Benign Packet Definitions

This module is used to model incoming data into an n-dimensional feature space where, n represents the number of features identified by PBA module. n varies for different types of control packets depending on the number and size of the packet type. During training phase the PBA calculates transition probabilities of the training dataset. Each transition probability is considered as a potential feature which can help in discriminating normal packets from malformed packets. So, during training phase six different feature vector sets are created one for each packet type.

5.3 Decision Module

The decision module implements three classifiers: Decision tree (J48), Naïve Bayes (NB) and inductive rule learner (Jrip). The module takes $\tau(S)$ as an input from the PBA and on the basis of training dataset residing in the respective BPD and generates the output for output filter. A brief description of the three classifiers used is presented in the following paragraphs.

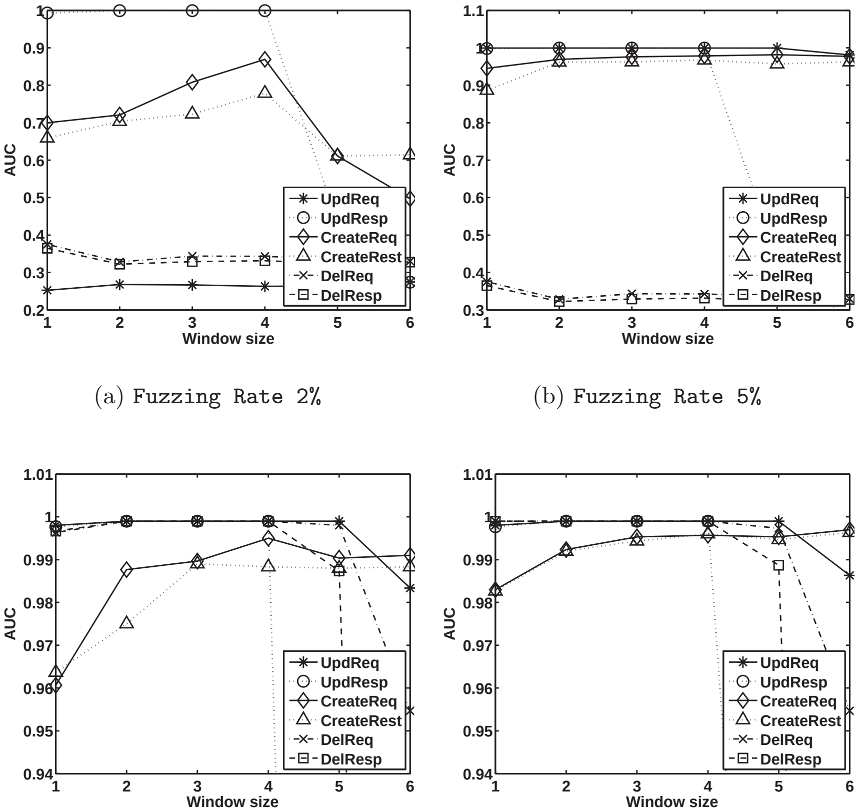
Decision Tree (J48) Decisions trees are usually used to map observations about an item to conclusions about the items target value using some predictive model [17]. They are very easy to understand and are efficient in terms of time especially on large datasets. They can be applied on both numerical and categorical data, and statistical validation of the results is also possible. We use $C4.5$ decision tree (J48) that is implemented in WEKA. We do not utilize binary splits on nominal attributes for building trees. The confidence factor for pruning is set to 0.25, where lower values lead to more pruning. The minimum number of instances per leaf is set to 2. The number of folds of training data is set to 3, where one fold is used for pruning and the rest are used for growing the tree.

Naïve Bayes (NB) Naïve Bayes is a simple probabilistic classifier assuming naïve independence among the features, i.e., the presence or absence of a feature does not affect any other feature [18]. The algorithm works efficiently when trained in a supervised learning environment. Due to its inherent simple structure it often gives very good performance in complex real world scenarios. The maximum likelihood technique is used for parameter estimation of Naïve Bayes models. We have neither used kernel estimator functions nor numeric attributes for supervised discrimination that converts numeric attributes to nominal ones.

Inductive Rule Learner (Jrip) We chose rule based learners due to their inherent simplicity that results in a better understanding of their learner model. Jrip, performs quite efficiently on large noisy datasets with hundreds of thousands of examples.The algorithm works by initially making a detection model composed of rules which are improved iteratively using different heuristic techniques. The constructed rule set is used to classify the test cases.

6 Experiments and Results

In this section we evaluate the performance of the proposed GTP-C fuzzing detection framework. We measure the performance on the basis of detection rate. We have carried out the standard Receiver Operating Characteristics (ROC) analysis to evaluate the detection accuracy of our system. We report area under the ROC curve (AUC) of three data mining algorithms: decision tree (J48), Naïve Bayes (NB) and inductive rule learner (RIPPER).



(a) `Fuzzing Rate 2%`

(b) `Fuzzing Rate 5%`

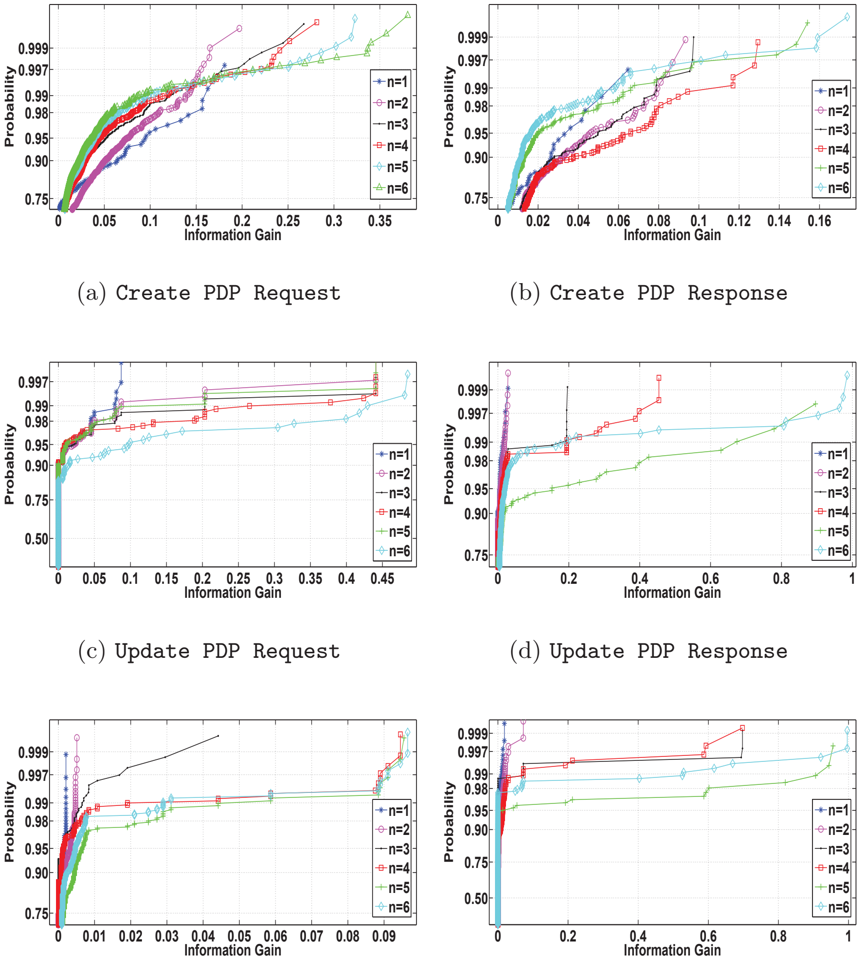
(c) `Fuzzing Rate 10%`

(d) `Fuzzing Rate 20%`

Fig. 6. Average AUC at $2, 5, 10$ and 20% fuzzing rate showing peaks at $n = 4$

Our experiments are based on two sets of analysis. In the first set we determine the optimum value of n for best average detection accuracy. We perform ROC analysis for window sizes of 1 to 6. For generalization we averaged the AUCs of the three classifiers and using their AUC averages we calculated detection accuracy for all categories of packets. In Figure 6, the overall average detection accuracy for different levels of fuzzing is shown. The figure shows that in most cases window size of 4 gives the best performance in terms of AUC. Increasing the size of n increases the number of features and hence the dimensionality of the data set, thereby exhibiting the `curse of dimensionality`. Whereas, features extracted at smaller values of n, due to simplicity, do not have sufficient discriminative abilities.

In the second set of experiments, to select the most *discriminative* features, we have used standard feature selection method. We employ information-



(a) `Create PDP Request`

(b) `Create PDP Response`

(c) `Update PDP Request`

(d) `Update PDP Response`

(e) `Delete PDP Request`

(f) `Delete PDP Response`

Fig. 7. Normal probability plot of different types of GTP-C packets

theoretic measure for feature ranking. Information gain is one such measure to calculate the discriminative ability of a feature.

$$IG(Y;X) = H(Y) - H(Y|X)$$

Where ($IG \in [0,1]$) and $H(X)$ and $H(Y)$ are the entropies of a given attribute X and a class attribute Y. We perform feature quantification to support the notion of introducing feature selection. Figure 7 shows the normal probability plot of the information gain of the extracted features. It can be observed that for smaller values of n the IG values of almost all of the features are very low. However for larger values of n some features exhibit significantly large IG values. But as we increase the value of n the curse of dimensionality increases. Therefore our analysis show that $n = 4$ is most suitable in terms of detection.

After determining the suitable value of n, i.e., 4 we improve the results by selecting features of high IG values, which results in reduced number of features. The analysis include all types of control packets for the value of window size 4. Table 3 gives detection accuracies (DA) and false alarm rate (FA) for different levels of fuzzing rate (FR). In this figure, we can see that 2% fuzzing is most difficult to detect for some type of packets. The difficulties arrive when the packet size is small. For example in Delete PDP Request/Response packets the average sizes are 60 and 56 bytes respectively. So even for 5% fuzzing the number of bits fuzzed will be 3, which makes it difficult to detect. Packets with fuzzing rate as low as 2% have a very low threat level and can be considered as minor bit errors. However, when the packet size increases as in the case of Create PDP Request/Response the number of bits fuzzed are relatively larger and have a higher threat level. It can be seen from the results that the detection accuracy for packets with higher threat level is as high as 99.9% whereas, the false alarm rate is as low as 0.1%.

7 Conclusion and Future Work

In this paper, we have presented an efficient data mining framework for detection of fuzzing attacks directed towards $3G$ core networks using the control packets of the GTP protocol. The results show that the Markov chain model for feature selection combined with standard classification algorithms is a good technique for detection of fuzzing attacks. The analysis done for $n = 4$ shows that it is most suitable for efficient detection of fuzzing attacks with fuzzing rate of 5% or more whereas, performance results are also satisfactory in most of the cases where fuzzing rate is less than 5%. Currently, we are working on exploring some other data mining techniques to identify features resulting in improved detection accuracy for lower fuzzing rates (1% and 2%). The future work also includes a thorough analysis of the processing overheads of the proposed framework to make it deployable in a real environment.

References

1. Odlyzko, A.: Internet traffic growth: Sources and implications. In: Proc. SPIE. Volume 5247., Citeseer (2003) 1–15
2. Peng, X., Yingyou, W., Dazhe, Z., Hong, Z.: GTP Security in 3G Core Network. In: 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, IEEE (2010) 15–19
3. Traynor, P., Lin, M., Ongtang, M., Rao, V., Jaeger, T., McDaniel, P., La Porta, T.: On cellular botnets: Measuring the impact of malicious devices on a cellular network core. In: Proceedings of the 16th ACM conference on Computer and communications security, ACM (2009) 223–234

Table 3. Performance evaluation results for different packet types

FR→	2%		5%		10%		20%	
Classifier↓	DA	FA	DA	FA	DA	FA	DA	FA
NB	.392	.570	1.00	0.00	1.00	0.00	1.00	0.00
Jrip	.474	.514	1.00	0.00	1.00	0.00	1.00	0.00
J48	.470	.516	1.00	0.00	1.00	0.00	1.00	0.00

(a) Update PDP context request

FR→	2%		5%		10%		20%	
Classifier↓	DA	FA	DA	FA	DA	FA	DA	FA
NB	1.00	0.00	.999	.001	.999	.001	.999	.001
Jrip	.999	.001	.999	.001	1.00	0.00	.999	.001
J48	1.00	0.00	.999	.001	.999	.001	.999	.001

(b) Update PDP context response

FR→	2%		5%		10%		20%	
Classifier↓	DA	FA	DA	FA	DA	FA	DA	FA
NB	.490	.506	.490	.510	.999	.001	1.00	0.00
Jrip	.498	.501	.498	.502	1.00	.001	1.00	0.00
J48	.500	.500	.500	.500	.999	.001	.999	.001

(c) Delete PDP context request

FR→	2%		5%		10%		20%	
Classifier↓	DA	FA	DA	FA	DA	FA	DA	FA
NB	.481	.506	.490	.510	1.00	0.00	.999	.001
Jrip	.498	.502	.498	.502	.999	.001	1.00	0.00
J48	.498	.502	.498	.502	.999	.001	.999	.001

(d) Delete PDP context response

FR→	2%		5%		10%		20%	
Classifier↓	DA	FA	DA	FA	DA	FA	DA	FA
NB	1.00	0.00	1.00	0.00	.999	.001	1.00	0.00
Jrip	.999	.001	.999	.001	1.00	0.00	1.00	0.00
J48	.999	.001	.999	.001	.999	.001	1.00	0.00

(e) Create PDP context request

FR→	2%		5%		10%		20%	
Classifier↓	DA	FA	DA	FA	DA	FA	DA	FA
NB	.764	.226	.957	.130	.998	.170	.999	.001
Jrip	.760	.229	.956	.051	.996	.110	.995	.007
J48	.640	.362	.906	.113	.990	.015	.995	.004

(f) Create PDP context response

4. Whitehouse, O.: GPRS wireless security: not ready for prime time. In: GSM Association Security Group Meeting, Berlin. (2002)
5. 3GPP: Security Threats and Requirements. TS 21.133 (V 4.1.00)
6. Dimitriadis, C.: Improving mobile core network security with honeynets. IEEE Security & Privacy (2007) 40–47
7. Xenakis, C., Merakos, L.: Vulnerabilities and possible attacks against the GPRS backbone network. Critical Information Infrastructures Security 262–272
8. Whitehouse, O., Murphy, G.: Attacks and counter measures in 2.5 G and 3G cellular IP networks. Atstake Inc., Mar (2004)
9. Mulliner, C., Vigna, G.: Vulnerability analysis of MMS user agents. In: Computer Security Applications Conference, 2006. ACSAC'06. 22nd Annual. (2006) 77–88
10. Racic, R., Ma, D., Chen, H.: Exploiting mms vulnerabilities to stealthily exhaust mobile phones battery. IEEE SecureComm (2006)
11. Enck, W., Traynor, P., McDaniel, P., La Porta, T.: Exploiting open functionality in SMS-capable cellular networks. In: Proceedings of the 12th ACM conference on Computer and communications security, ACM (2005) 404
12. Kotapati, K., Liu, P., Sun, Y., LaPorta, T.: A taxonomy of cyber attacks on 3G networks. Intelligence and Security Informatics 631–633
13. Traynor, P., McDaniel, P., La Porta, T., et al.: On attack causality in internet-connected cellular networks. In: USENIX Security Symposium (SECURITY). (2007)
14. `http://www.openggsn.org/`
15. Sanders, G.: GPRS networks. John Wiley & Sons Inc (2003)
16. T. Madsen, P. Schwefel, M.H.J.B., Prasad., R.: On Traffic Modelling in GPRS Networks. (2005) 1785–1789
17. Quinlan, J.: C4. 5: programs for machine learning. Morgan Kaufmann (1993)
18. Maron, M., Kuhns, J.: On relevance, probabilistic indexing and information retrieval. Journal of the ACM (JACM) **7**(3) (1960) 216–244