UDS 621.39

COUNTERING FLASH CALLS IN 4G AND 5G WITH INNOVATIVE DETECTION AND BLOCKING TECHNIQUES

Ivan Vetoshko
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: ivan.vetoshko@ukr.net

ПРОТИДІЯ ФЛЕШ-ДЗВІНКАМ У МЕРЕЖАХ 4G ТА 5G ЗА ДОПОМОГОЮ ІННОВАЦІЙНИХ МЕТОДІВ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ

Досліджено методи виявлення та блокування Flash-дзвінків у мобільних мережах 4G та 5G. Проаналізовано параметри сигналів, поведінкові аномалії трафіку та алгоритми машинного навчання. Встановлено, що поєднання ШІ-аналітики, аналізу часу встановлення виклику та моніторингу заголовків SIP/SDP підвищує ефективність виявлення. Запропоновані рішення зменшують вплив нелегітимного трафіку за рахунок оптимізації захисту мереж сигналізації.

In today's 4G and 5G mobile networks, the problem of illegitimate use of signal space to optimise the cost of business processes is becoming increasingly relevant. One of these phenomena is Flash Calls, which are short-lived incoming calls used as an alternative to SMS for user authentication. While at first glance this technology seems to be an effective solution for companies looking to reduce the cost of SMS-OTP (One-Time Password), its widespread use poses serious challenges for telecoms operators, including loss of revenue, congestion of signalling channels and the possibility of abuse by malicious actors [1]. Unlike traditional signalling attacks, such as SMS spoofing or Caller ID manipulation, Flash Calls use legitimate call establishment mechanisms in VoLTE (Voice over LTE) and VoNR (Voice over New Radio) networks. They make identification and blocking difficult due to the lack of text content and the need for urgent real-time processing. The main technical challenge is to identify such calls among legitimate calls, which requires the implementation of traffic analysis algorithms, subscriber behavioural models and the use of artificial intelligence for automated classification. Given the rapid deployment of 5G SA (Standalone) networks, there is a need to develop new approaches to detecting and blocking Flash Calls. Traditional methods, such as blacklisting or analysing signalling parameters (Call Setup Time, SIP Headers), show limited effectiveness. Therefore, more flexible solutions based on machine learning, analysis of behavioural characteristics and correlation of traffic with massive usage patterns are in demand [1].

Flash Calls are based on establishing a short-term voice connection over the mobile network without answering the call. This allows the caller to identify the user by Caller ID (CLI) or the last digits of the phone number displayed in the incoming call [1]. On LTE (4G) and 5G networks, SA Flash Calls pass through the standard signalling stack, including:

- VoLTE (Voice over LTE) - Calls are initiated via the IMS (IP Multimedia Subsystem) using SIP (Session Initiation Protocol).
- VoNR (Voice over New Radio) - a similar principle, but with advanced QoS and call processing capabilities in 5G SA.
- Basic SIP requests (INVITE, 180 Ringing, BYE) are used, which do not actually terminate the session, but generate a record in the CDR (Call Detail Record).

The main feature of Flash Calls is the extremely short interval between connection establishment and completion (usually <1 second), which distinguishes them from standard voice calls. Implementing effective methods of countering Flash Calls requires a detailed analysis of signal traffic, including monitoring call parameters and analysing behavioural anomalies within the overall traffic of a mobile operator. Given that traditional blocking mechanisms, such as Caller ID filtering or static time limits, are ineffective, operators are implementing adaptive approaches to traffic classification. One of these methods is behavioural call analysis, which involves aggregating data on user call patterns and the correlation between subscriber activity and specific parameters of a signalling session [2]. If deviations from typical scenarios are detected, the call is automatically marked as suspicious, with subsequent application of blocking or slowdown policies.

In today's 4G and 5G mobile networks, it is critical to ensure resilience to threats caused by the illegitimate use of signalling traffic, including Flash Calls. The fig.1 illustrates a typical architecture for processing signalling traffic in a mobile network, including the points of interaction between network elements, signalling gateways, and external interconnects [2]. Diagram 1 shows a two-site STP/DRA (Signal Transfer Point/Diameter Routing Agent) infrastructure used to route signal traffic between internal network elements and external 3G/4G interconnects. Interaction between the elements takes place via several protocols, including SS7 M3UA (blue), Diameter (black), EWOK (dashed), as well as TCP/IP connections for management and analytics. Management and monitoring is carried out through analytics consoles integrated with the OSS (Operations Support System), which provides control over network performance parameters [3].

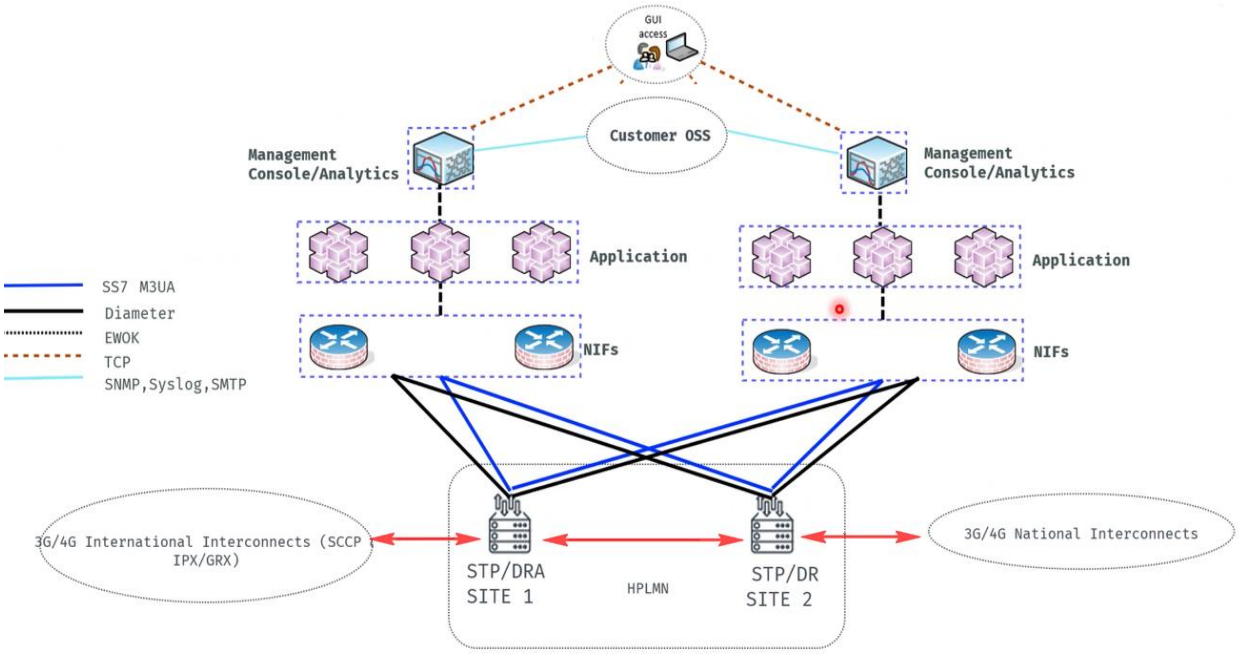

Fig. 1. Signal traffic management and fraud detection architecture.

A key feature of this architecture is the ability to centrally analyse and process signalling traffic, which allows for the identification of abnormal call patterns specific to Flash Calls. With the help of behavioural analysis algorithms integrated into the monitoring system, the operator can identify traffic that deviates from the normative parameters and automatically apply mechanisms to block or restrict unwanted calls. The dual-site distributed architecture provides increased fault tolerance and load balancing between STP/DRA nodes. This helps to minimise the impact of potential threats and abuse in signalling networks, and guarantees the stability of voice services in 4G and 5G mobile networks [3].

In 5G Standalone (SA), all VoNR calls are routed through the IMS Core without using EPC, which makes Flash Calls difficult to detect as they can masquerade as standard SIP sessions. Operators face the problem of short-lived calls that terminate before receiving 200 OKs, which are ineffective to identify through Caller ID or SIP-User Agent. SIP/SDP headers in Flash Calls may contain atypical or missing parameters, which is an indicator for analysis [2]. Particular attention should be paid to P-CSCF and S-CSCF behavioural anomalies, as an excessive number of cancelled or instantly terminated calls from a particular number range may indicate abuse. SIP header monitoring (User-Agent, P-Asserted-Identity), SDP parameter analysis, PCF QoS testing, and CDR behavioural analytics can be effective detection methods. Comprehensive analysis of signal traffic, together with the use of machine learning algorithms, will help operators to quickly identify and block Flash Calls in 5G SA [3].

Promising methods for detecting and blocking Flash Calls:

- Call Setup Time (CST) and Early Media analysis - Many Flash Calls do not reach the 200 OK stage of a SIP session, terminating before the voice channel is established. Analysing the time from INVITE to BYE or CANCEL can be a criterion for identifying suspicious calls [1].
- AI models for analysing call behaviour - Using Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM), operators can build models to detect anomalous activity. For example, Flash Calls often come in groups from different numbers in short periods of time, which can be detected through clustering.
- Using Session Border Controller (SBC) for adaptive blocking - SBCs can act as a first layer of protection by identifying suspicious SIP sessions based on several criteria, such as call establishment frequency, Caller ID matching registered numbers, and types of SIP User-Agents used [3].

Methods for detecting and blocking Flash Calls in 4G and 5G mobile networks are investigated. Signal parameters, traffic behavioural anomalies, and machine learning algorithms are analysed. It is established that the combination of AI analytics, Call Setup Time analysis, and SIP/SDP header monitoring increases the detection efficiency [2]. The proposed solutions reduce the impact of illegitimate traffic by optimising the protection of signalling networks. It was found that traditional blocking methods based on static Caller ID and SIP header filtering rules have limited effectiveness due to dynamic changes in Flash Calls patterns. Using behavioural analytics and clustering of anomalous sessions, you can detect traffic with atypical characteristics in real time. Integration of adaptive policies in Session Border Controllers (SBC) and Policy Control Function (PCF) provides flexible management of calls that match the Flash Calls profile. Further research should focus on improving distributed signal traffic analysis methods and integrating deep learning models to predict new fraudulent schemes.

References

1. Flash Calls [Electronic resource] // Mobileum. – Published: April 5, 2024. – Available: https://www.mobileum.com/products/risk-management/business-assurance/flash-calls/
2. Vetoshko I.P., Kravchuk S.O. Possibilities of improving the voice services quality in 5G networks // Information and Telecommunication Sciences. – 2023. – Vol.14, No 2. – P. 9-16. – DOI: https://doi.org/10.20535/2411-2976.22023.9-16
3. What are flash calls and how do they work? [Electronic resource] // Infobip. – Published: June 2024. – Available: https://www.infobip.com/blog/what-is-a-flash-call