УДК 004.056.5:004.8:621.391
DOI: 10.31673/2409-7292.2025.031728

Tymokhin Yu.A.

REAL-TIME DETECTION OF INTERCONNECT BYPASS FRAUD IN TELECOMMUNICATION NETWORKS: CAMEL FRAMEWORK LOW-CODE APPROACH AND AI/ML ADAPTATION

Interconnect Bypass Fraud poses a significant threat to telecommunication operators, leading to substantial revenue losses and degraded service quality. This fraud involves routing calls through unauthorized, low-cost channels, bypassing legitimate interconnect agreements. Traditional detection methods often rely on offline or near real-time analysis, which may not suffice for timely mitigation.

This article proposes a real-time detection solution leveraging the CAMEL framework, enhanced by a low-code development approach and AI/ML integration. The solution aims to provide flexibility, rapid adaptation, and high accuracy in fraud detection while minimizing the need for deep programming expertise. By combining signaling protocol analysis (CAP/IMS_CAP/INAP) with AI-driven anomaly detection, the proposed system addresses both current and emerging fraud techniques. The article also explores the adaptation of AI/ML within the low-code software lifecycle to further optimize fraud detection workflows.

Keywords: Online interconnect bypass fraud detection, signaling, call-control, low-code, artificial intelligence, machine learning, information security.

Introduction

The telecommunications industry faces escalating challenges from fraud, particularly Interconnect Bypass Fraud, which exploits low-cost or unauthorized routes to bypass official interconnect agreements. This type of fraud not only results in significant financial losses for operators but also compromises service quality for end-users. As the demand for affordable international calling grows, so does the sophistication of fraudulent techniques, necessitating advanced, real-time detection mechanisms.

Current fraud detection systems often rely on offline post-processing or near real-time analysis of Call Detail Records (CDRs), which may delay response times and reduce effectiveness. A real-time approach, however, enables immediate identification and mitigation of fraudulent activities, especially critical for high-cost scenarios like international roaming. The CAMEL (Customized Applications for Mobile network Enhanced Logic) framework, with its CAP protocol, offers a robust foundation for real-time call control and fraud detection across multiple network generations (2G to 5G).

This article addresses the gap in real-time Bypass Fraud detection by proposing a solution built on the CAMEL framework, integrated with a low-code development platform (LCDP) for rapid adaptation of fraud detection logic. The low-code approach empowers telecommunications teams to modify and deploy fraud detection rules without extensive programming knowledge, significantly shortening the development lifecycle. Furthermore, the integration of AI and machine learning enhances the system's ability to detect anomalies and predict emerging fraud patterns, ensuring long-term scalability and accuracy.

The study also examines the architectural and procedural adaptations required to implement this solution, including the use of signaling protocols (CAP/IMS_CAP/INAP) and the role of AI/ML in augmenting low-code platforms. By combining these technologies, the proposed system aims to provide a flexible, efficient, and future-proof solution for combating Interconnect Bypass Fraud.

Purpose and tasks of research

The primary purpose of this research is to offer a real-time Interconnect Bypass Fraud detection solution using the CAMEL framework, low-code development, and AI/ML adaptation. The study aims to address the limitations of existing fraud detection methods by offering a solution that is both agile and scalable.

To achieve this goal, the following tasks are outlined:

1. Analyze the architecture and protocols of the real-time call control across 2G to 5G networks, focusing on the CAMEL framework and CAP/IMS_CAP/INAP signaling.

2. Propose a low-code development approach to enable rapid adaptation of fraud detection logic, reducing dependency on specialized programming skills.

3. Consider the integration of AI/ML to enhance fraud detection accuracy, focusing on anomaly detection, behavioral profiling, and predictive analytics.

4. Explore an AI-augmented low-code lifecycle to optimize the development, testing, and deployment of fraud detection rules.

By addressing these tasks, the research contributes to the advancement of real-time fraud detection in telecommunications, offering practical insights for operators and vendors seeking to mitigate revenue losses and improve service integrity.

Literature analysis and problem statement

Surveys [1], [2] and [3] provide a comprehensive review of scientific publications related to SIM-box and Bypass Fraud detection techniques, summarizing and classifying them into CDR-based, control-plane (signaling)-based, and user-plane (audio)-based solutions, as well as their combinations. The studies highlight the use of modern technologies such as machine learning (ML) and artificial intelligence (AI) as current methods for enhancing bypass fraud detection.

No studies were found that focused on real-time Bypass Fraud detection using CAP or IMS ISC/SIP protocols. Most works that claimed real-time approaches were in fact based on near real-time analysis of different CDR data, rather than truly real-time signaling monitoring.

Several detailed patents (for example [4÷8]) were found that propose Bypass Fraud detection methods based on signaling protocols usage and data analysis, including solutions that utilize CAMEL-based approaches.

There were identified numerous commercial Fraud Management solutions where vendors describe Bypass Fraud detection using CAP or IMS ISC/SIP protocols at a high level, but these lacked technical implementation details.

An analysis of national Ukrainian publications identified several articles, a study guide, and a few diploma theses that address topics related to bypass fraud in telecommunication networks, including SIM-box type fraud.

An analysis of recent international research and publications indicates that the scientific community has shown limited interest in developing online methods for Bypass Fraud detection and mitigation, focusing instead on near real-time post-processing techniques. On the other hand, mobile network operators and fraud management solution vendors express a clear interest in real-time Bypass Fraud detection using signaling protocols.

The main section

Mobile Network Generations and Real-Time Call Control

Nowadays there are four generations of 3GPP Mobile Networks in real operation: 2G (GSM) [8], 3G (UMTS), 4G (LTE) [9] and 5G (NR) [10]. Migration from one generation to another in real networks is a very slow process typically taking several years due to infrastructure costs, device compatibilities and regulatory factors. Thus, 3GPP has standardized a variety of mobile networks interworking mechanisms which support different integration options to ensure service continuity across generations [11], [12].

To propose a solution for real-time Bypass Fraud detection first we need to analyze available real-time interfaces for call control depending on 3GPP Network Generation.

In 2G [9] and 3G [9] mobile networks Call Control application architecture is based on CAMEL (Customized Applications for Mobile network Enhanced Logic) framework [13] with CAP protocol [14] and IN (Intelligent Network) framework with INAP protocol [15] for fixed networks.

In 4G (VoLTE) [9] and 5G (VoNR) [10] call control application is based on IMS [16] and can be done either on IMS AS via SIP protocol (17) or on legacy CAMEL Service (also used in 2G/3G networks) via IMS IM-SSF [18] and IMS CAP protocol [19]. IMS IM-SSF is a gateway between SIP and CAP protocols with support of required call control application functions. Below is the

summarizing table for call control application variants for each mobile network generation reflecting how services are triggered and executed using standardized protocols and architectures.

Table 1

Mobile networks generations and online call control application options

Generation	Access Type	Call Control Framework	Service Execution and Application Protocol
2G (GSM)	Circuit-Switched	CAMEL	gsmSSF□CAP□gsmSCF
3G (UMTS)	Circuit-Switched	CAMEL	gsmSSF□CAP□gsmSCF
	Packet-Switched[1]	IMS (Mandatory for VoPS)	S-CSCF□ISC/SIP□IMS AS
		IMS with CAMEL backward compatability	S-CSCF□ISC/SIP□IM-SSF□IMS CAP□gsmSCF
4G (LTE)	Packet-Switched	IMS (Mandatory for VoLTE)	S-CSCF□ISC/SIP□IMS AS
		IMS with CAMEL backward compatability	S-CSCF□ISC/SIP□IM-SSF□IMS CAP□gsmSCF
5G (NR)	Packet-Switched	IMS (Mandatory for VoNR)	S-CSCF□ISC/SIP□IMS AS
		IMS with CAMEL backward compatability	S-CSCF□ISC/SIP□IM-SSF□IMS CAP□gsmSCF

Note[1]: 3GPP Release 5 introduced the theoretical possibility of delivering voice services over the packet-switched (PS) domain through the use of the IMS architecture. However, implementing this solution required the availability of an IMS core network, IMS-capable mobile devices with VoIP support, and specific configurations within the 3G packet-switched core. Given that 3G networks also supported voice services via the circuit-switched (CS) domain natively, most mobile network operators did not adopt voice over PS in practice. Therefore, this article does not cover such solutions.

As we can see, the CAP protocol can be considered a common protocol across different mobile network generations. Therefore, it is proposed to integrate real-time Bypass Fraud detection application with Mobile Network using CAP/IMS_CAP protocols and optionally with fixed networks using INAP protocol.

Roaming and Interconnect architecture with CAMEL-based call control

In today's telecom voice services landscape, operators no longer manage just a mobile access network. Instead, they orchestrate an intricate web of technologies that span multi-generation mobile cores (2G, 3G, 4G, 5G), IMS voice platforms, and numerous interconnect and roaming arrangements – both with 3GPP-compliant and non-3GPP partners.

What was once a circuit-switched SS7 interconnect and roaming setup has evolved into a multi-protocol, hybrid architecture encompassing SIP, RTP, Diameter, HTTP/2, H.248, and more. This chapter examines some technical and architectural complexity of delivering voice services in such an environment – from 3GPP roaming scenario to interconnect with external partners, including none 3GPP mobile networks, VoIP carriers, enterprise PBXs, IPX providers and other voice interconnect platforms.

For this article we take, as an example, one of scenarios involved in Bypass Fraud. This is when outbound roamer (subscriber A) makes mobile originated call from VLPMN to the HPLMN subscriber B and Optimal Call Routing [20] is not used for such the call, means such the MOC is home routed. Normally, this call should reach the HPLMN via voice trunks established according to the Interconnect and Roaming inter-operator Agreements. But in case of Bypass Fraud, such a call can come to the HPLMN via different illegal routes. HPLMN Operator should have the possibility to detect this Bypass Fraud scenario and apply appropriate actions depending on its own business needs.

Figure 1 illustrates the architecture example for a use case in which Subscriber A, who belongs to the HPLMN and has an O-CSI (or O-IM-CSI in case of IMS access) CAMEL subscription, is roaming in a 3GPP-compliant VPLMN and may be connected via 2G, 3G, 4G, or 5G access networks. Subscriber A initiates a mobile-originated call to Subscriber B, who is also served by the HPLMN

© Tymokhin Yu.A. (2025) Real-Time Detection of Interconnect Bypass Fraud in Telecommunication Networks: CAMEL framework Low-Code Approach and AI/ML Adaptation. Сучасний захист інформації, 3(63), 150–164. https://doi.org/10.31673/2409-7292.2025.031728

and may be either a mobile or fixed-line user. This scenario was chosen as an example to explain the theoretical basis for Bypass Fraud detection through call control via the CAP/IMS_CAP//INAP protocols. The proposed solution for Bypass Fraud detection is not limited to this particular call scenario.

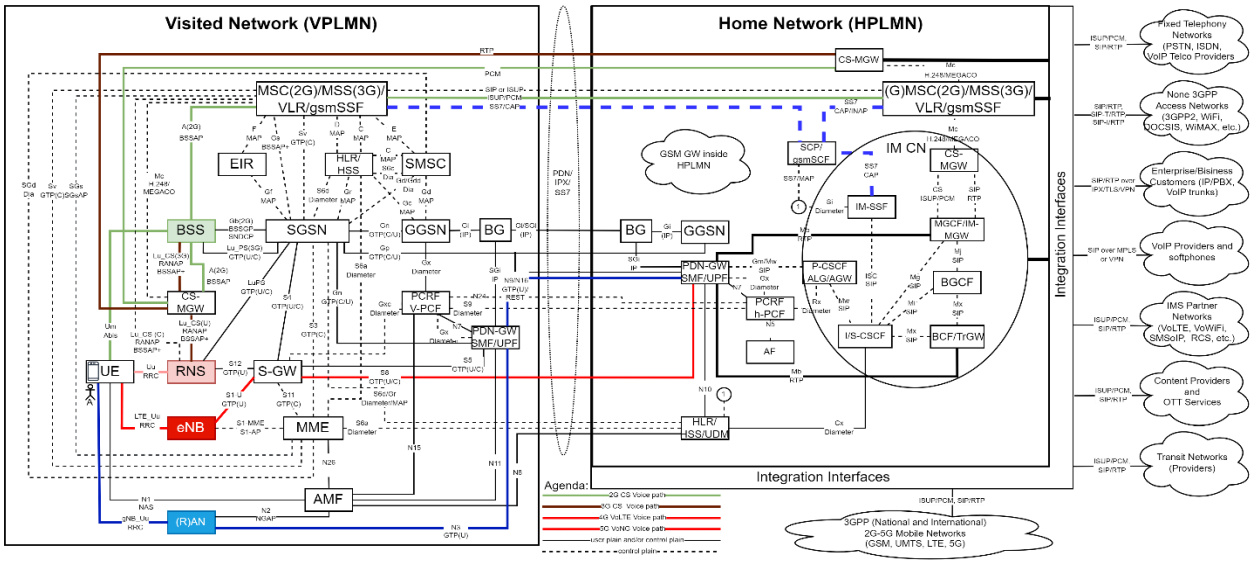

Fig. 1. Example of 3GPP Roaming Mobile Networks Architecture

In this scenario, bypass fraud detection is proposed to be carried out in two main steps. First, information about the initial call attempt is collected by processing the CAP InitialDP message triggered by the VPLMN based on the O-CSI of the roaming subscriber and sent to the HPLMN SCP (gsmSCF). In the second step, subsequent CAP and/or INAP InitialDP message(s) is/are captured when the actual voice call arrives at the HPLMN via an ISUP/PCM or SIP/RTP trunk. By performing real-time correlation between the signaling received in these two steps, the proposed solution can determine whether the call has been subject to Bypass Fraud. Let's review the call scenarios for this use-case based on the type of VPLMN access network where Subscriber A is roaming.

Access via 2G radio network. Option 1: Call Anchored in 2G Core Network. If the VPLMN supports voice calls only via its 2G Core Network A/Gb mode [21], the UE connects to the network using the Um interface with the 2G BSS. The 2G BSS forwards the connection via the A interface to the VPLMN MSC. The MSC retrieves the O-CSI (Originating CAMEL Subscription Information) from the VLR and engages the gsmSSF, which initiates call control using the CAMEL Application Part (CAP) protocol with the HPLMN's SCP (gsmSCF). This results in the triggering of the first CAP InitialDP interrogation with HPLMN SCP. Once the HPLMN SCP authorizes the call, the VPLMN MSC selects a voice trunk to the HPLMN. In this case, the call is routed via circuit-switched interconnect using ISUP signaling over PCM trunks to the HPLMN MSC (shown as the bold green line for the voice path from VPLMN MSC).

Access via 2G radio network. Option 2: Call Anchored in 3G Core Network (via 2G radio access). In this case, the 2G BSS is connected to the 3G Core Network Lu mode [21]. The UE connects via the Um interface to the BSS, which in turn connects via the Lu-CS interface to the MSS (Mobile Switching Server) and CS-MGW (Circuit-Switched Media Gateway). The MSS obtains the O-CSI from the VLR and triggers the call control via CAP protocol, just like in Option 1, by involving the gsmSSF and HPLMN SCP (gsmSCF). This is first CAP InitialDP interrogation with HPLMN SCP. After receiving authorization, the VPLMN MSS instructs the CS-MGW via the Mc interface to select a VoIP-based trunk (e.g., SIP/RTP) toward the HPLMN. The call is then routed to the

HPLMN's GMSC function (possibly part of its MSS) using SIP signaling and RTP for media (represented by the brown bold line for the voice path from CS-MGW).

Access via 3G radio network. Call Anchored in 3G Core Network via Lu_CS. The UE connects to the 3G RNS via the Uu interface. The RNS is connected to the MSS and CS-MGW over the Lu_CS interface. The MSS retrieves the O-CSI from the VLR and initiates call control via the CAP protocol by involving the gsmSSF and the HPLMN's SCP (gsmSCF). This results in the first CAP InitialDP interrogation with the HPLMN gsmSCF. Upon receiving call authorization, the VPLMN MSS instructs the CS-MGW via the Mc interface to select the appropriate trunk – either ISUP/PCM or SIP/RTP based on the Interconnect and Roaming Agreement between the VPLMN and HPLMN. These two trunking options are represented as the green (ISUP/PCM) and brown (SIP/RTP) bold lines for the voice path from the VPLMN CS-MGW to the HPLMN CS-MGW.

Access via 3G radio network. Call Anchored in 3G Core Network via Lu_PS. Although Voice over Packet-Switched (VoPS) via IMS was technically defined for by 3GPP for 3G networks, it was never widely implemented in practice. This is because 3G networks already provided efficient and reliable Circuit-Switched (CS) voice services, making the additional complexity and cost of deploying IMS-based VoPS in 3G UMTS unjustified for most operators. Therefore, this option is not considered in this article.

Access via 4G radio network. Call Anchored in 2G or 3G access network using CS Fallback (CSFB). In VPLMN networks where VoLTE roaming is not available, voice calls initiated from a 4G radio network are handled using Circuit-Switched Fallback (CSFB) mechanisms [22]. In this approach, the UE is redirected from the LTE network to a legacy 2G or 3G CS domain (GSM or UMTS), where the voice call is established using standard CS call setup procedures. This fallback mechanism allows operators to offer voice services over LTE coverage without requiring full VoLTE deployment.

During initial attachment to the LTE network (via LTE-Uu and S1-MME interfaces), the UE also registers for CS services (including voice) through the SGs interface between the MME and MSC/MSS. When the UE initiates a call, the MME uses the SGs interface to coordinate with the MSC/MSS and triggers the CSFB procedure [22]. The eNB then redirects the UE to a suitable 2G or 3G radio cell. Once the UE connects to the legacy CS access network, the call proceeds according to the applicable 2G or 3G voice call flow. Finally, the call is routed to the HPLMN using ISUP/PCM or SIP/RTP voice trunks, depending on the interconnect and roaming agreement. During the CS call, the VPLMN's gsmSSF triggers call control toward the HPLMN SCP (gsmSCF) using the CAP protocol. Thus, this CSFB scenario ultimately follows one of the standard 2G/3G CS voice call handling flows described above.

Access via 4G/5G radio network. VoLTE/VoNR call Anchored in 4G/5G. For VoLTE and VoNR call scenarios in 4G/5G networks with IMS support, Bypass Fraud is generally not applicable, because both signaling and voice media (SIP and RTP) are securely routed end-to-end to the HPLMN’s IMS core. Unlike legacy CS voice or interconnect scenarios that rely on ISUP/PCM or SIP/RTP trunks between operators (where voice paths can be diverted or manipulated) VoLTE/VoNR roaming utilizes secure IP-based interfaces and dedicated IMS routing, leaving little to no opportunity for fraudsters to intercept or reroute traffic. As a result, traditional bypass techniques, such as call path manipulation or fraudulent trunk rerouting, are largely ineffective in fully IMS-based VoLTE and VoNR roaming and interconnect environments. An exception is SIM-box-based bypass fraud, which remains relevant even in 4G and 5G networks. Thus, for informational purposes, Figure 1 shows the bold red and blue user-plane voice paths for VoLTE and VoNR home routed roaming calls, which are anchored in and handled by the HPLMN IMS. SIM-box based bypass fraud detection is technically possible if involve the HPLMN SCP (gsmSCF) via the IMS_CAP interface [19] through the IMS IM-SSF [18] or IMS-AS (Application Server) via ISC/SIP Interface [17] for additional call control. Table 2 summarizes mobile originated voice call technologies, Bypass Fraud risk and proposal to control call initiation via CAMEL Framework (CAP protocol).

Table 2

Mobile Originated Bypass Fraud detection in Mobile Networks using CAMEL call control

Radio access	Core Network (Anchor)	Voice Technology	Interconnect Trunks	Call Control	Bypass Fraud Risk
2G	2G CS	CS Voice (GSM)	ISUP/PCM	CAMEL	High
2G	3G Lu-CS	CS Voice (UMTS)	ISUP/PCM or SIP/RTP	CAMEL	High
3G	3G Lu-PS	PS Voice (UMTS)	SIP/RTP with IMS (not used in real networks)	n/a	n/a
4G	2G CS via CSFB	CS Voice (GSM)	ISUP/PCM	CAMEL	High
	3G Lu-CS via CSFB	CS Voice (UMTS)	ISUP/PCM or SIP/RTP	CAMEL	High
4G	4G EPC	VoLTE	SIP/RTP (IMS)	CAMEL	Low
4G	5G Core via EPS Fallback	VoLTE	SIP/RTP (IMS)	CAMEL	Low
5G (NSA)	4G EPC + IMS	VoLTE	SIP/RTP (IMS)	CAMEL	Low
5G (SA)	5G Core + IMS	VoNR/VoNG	SIP/RTP (IMS or transit)	CAMEL	Low

In the next step, the voice call will reach the HPLMN via interconnect voice trunk, such as ISUP/PCM or SIP/RTP. In Figure 1, examples of these interconnect voice trunks are represented as "clouds," with the appropriate integration interfaces to the HPLMN. These interconnect trunks are connected to the HPLMN through Media Gateways (MGWs), depicted by bold black lines linking the integration interfaces with the HPLMN CS-MGW, MSC/MSS, and IMS CN. The exact integration point depends on the specific network configuration.

It is proposed to configure a trunk-based CAP or INAP protocol trigger on each voice trunk, with an appropriate Default Call Handling setting (to either block or continue the call) in cases where the HPLMN SCP is unavailable. Optionally, Subscriber B can be provisioned with a CAP T-CSI subscription to trigger the HPLMN SCP during a mobile-terminated call attempt.

Thus, for each call in this roaming use-case scenario example, the HPLMN SCP is expected to receive the following CAP/IMS_CAP/INAP InitialDP messages:

1. An initial mobile-originated call attempt from the VPLMN.
2. When the voice call arrives at the HPLMN via an interconnect voice trunk.
3. When the mobile network initiates a mobile-terminated call attempt to connect the voice trunk to Subscriber B’s terminal. This message is optional and relevant only if Subscriber B is mobile subscriber having T-CSI/T-IM-CSI CAMEL service subscription.

In Figure 1, one variant of call termination is depicted as a "cloud" within the HPLMN network, labeled "GSM GW", which is not integrated through any standard interconnect interfaces. This scenario represents a form of bypass fraud where the call is terminated using a SIM card and user equipment (UE) that connects directly to the HPLMN via its radio access network. Examples of such termination methods include the use of SIM boxes or third-party mobile applications that utilize local HPLMN SIM cards to deliver calls. These setups effectively bypass legitimate interconnect or roaming agreements, enabling unauthorized call termination at reduced cost and potentially causing revenue loss and service quality degradation for the HPLMN operator. Unfortunately, in some other scenarios this type of bypass fraud typically requires multiple calls to be detected, making it difficult to identify in real time from the very first fraudulent call from SIM card.

Figure 2 provides three simplified call flow scenario examples for Figure 1 roaming call architecture. Scenario 1 – normal voice trunk selection for roaming call termination. Scenarios 2 and 3 – are Bypass Fraud examples.

Scenario 1:

1. Subscriber A makes MOC from VPLMN to HPLMN Subscriber B;
2. VPLMN MSC (gsmSSF) triggers HPLMN SCP (gsmSCF) with CAP InitialDP message to control and charge the call;

3. SCP allows the call sending CAP Connect or Continue Message;
4. MSC selects the voice trunk group to connect call to the HPLMN GMSC. In this scenario this is green line, meaning that voice trunk group is selected according to the Roaming and Interconnect agreement between VPLMN and HPLMN networks;
5. HPLMN MSC has trunk-based CAP trigger, invokes gsmSSF function and sends CAP InitialDP message to the SCP;
6. SCP checks this IDP message parameters and allows the call;
7. MSC establish voice channel with another MSC where subscriber B is located;
8. If subscriber B has T-CSI CAP subscription, MSC invokes gsmSSF function and sends CAP InitialDP message to the SCP asking what to do with this call;
9. SCP allows the call;
10. Call is connected to the Subscriber B.

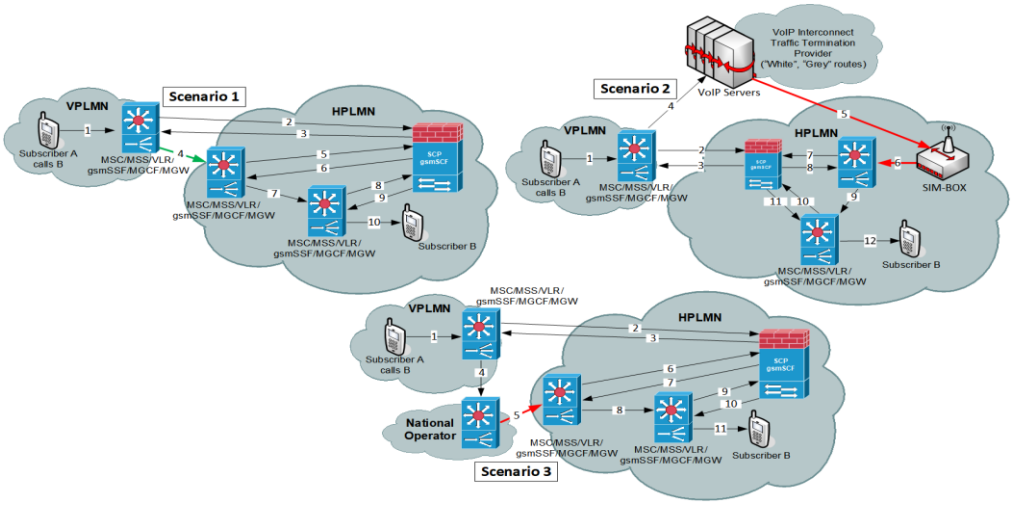

Fig. 2. Bypass Fraud Scenario Examples

Scenario 2 (Fraud Bypass via VoIP Interconnect Traffic Provider and SIM-Box (GSM-GW) in HPLMN):

Steps 1 to 3 are identical to the Scenario 1 steps. VPLMN MSC routes voice call not via legal trunk, but to the VoIP Interconnect Traffic Provider. VoIP Interconnect Traffic Provider via VoIP channel sends voice call to the SIM-Box (GSM-GW) with HPLMN SIM card having O-CSI CAP subscription connected to the HPLMN via radio access as normal HPLMN mobile phone. SIM-Box initiates new Mobile Originated Call using own A MSISDN number linked to the SIM card IMSI. GMSC invokes gsmSSF function and triggers SCP using CAP InitialDP message asking what to do with this MOC call. At this step SCP can correlate CAP InitialDP from step 2 and CAP InitialDP from step 7 and detect Bypass Fraud scenario. Let's assume that HPLMN operator decided not to block this call at this step. Voice call is connected to the MSC where subscriber B is located. If subscriber B has T-CSI CAP subscription, MSC invokes gsmSSF function and sends CAP InitialDP message to the SCP asking what to do with this call. At this step SCP can correlate three InitialDP messages from steps 2, 7 and 10 to make decision regarding Bypass Fraud scenario. Let's assume that call is not blocked on this step. SCP allows the call. Call is connected to the Subscriber B.

Scenario 3 (Fraud Bypass via National Operator (mobile of fixed)):

1. Steps 1 to 3 are identical to the Scenario 1 steps. VPLMN MSC routes voice call not via legal trunk, but to the National Telecommunication Provider which has own voice trunks with HPLMN. National Telecom Provider sends voice call to the HPLMN via his voice trunk. HPLMN MSC has trunk-based CAP or INAP trigger, invokes gsmSSF function and sends CAP/INAP InitialDP message to the SCP. At this step SCP can correlate CAP InitialDP from step 2 and CAP InitialDP from step 6 and detect Bypass Fraud scenario. Let's assume that HPLMN operator decided

not to block this call at this step. MSC establish voice channel with another MSC where subscriber B is located. If subscriber B has T-CSI CAP subscription, MSC invokes gsmSSF function and sends CAP InitialDP message to the SCP asking what to do with this call. At this step SCP can correlate three InitialDP messages from steps 2, 6 and 9 to make decision regarding Bypass Fraud scenario. Let' assume that call is not blocked on this step. SCP allows the call. Call is connected to the Subscriber B. Bypass Fraud detection logic in the HPLMN can be implemented either as an application on the existing SCP platform or as a dedicated, standalone SCP instance. If the logic is integrated into the existing SCP, no significant changes to the SCCP routing configuration in the HPLMN are required.

However, if a dedicated SCP is used for Bypass Fraud detection, O-CSI and T-CSI CAP InitialDP messages should first be routed to the Bypass Fraud detection SCP. After processing, these messages should be forwarded (re-routed) to the primary HPLMN SCP, which will handle standard call control functions such as online charging or PrePaid or VPN services.

Figure 3 illustrates a messages flow for scenario in which Bypass Fraud detection, online charging, Prepaid and VPN services are distributed across two separate SCP platforms.

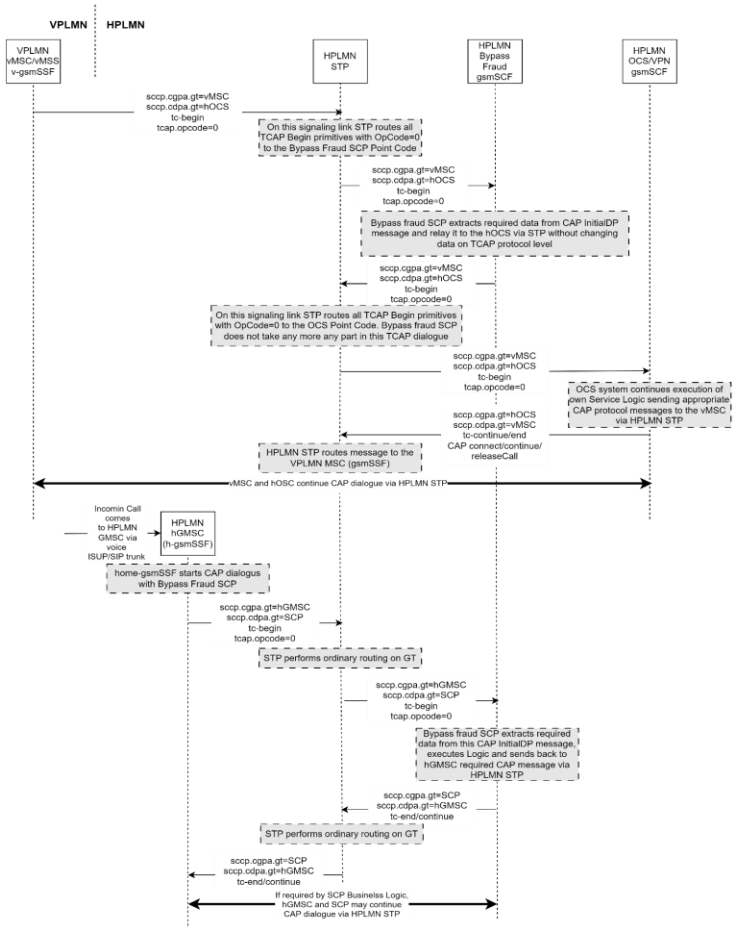

Fig. 3. Bypass Fraud detection flow example in case
Fraud Detection and OCS/VPN Services are distributed across two separate SCP platforms

To ensure that the InitialDP message is routed to the Bypass Fraud Detection SCP instead of the HPLMN's main OCS/PrePaid/VPN SCP, the HPLMN STP must support SCCP routing based on TCAP protocol content analysis. This includes an evaluation of the TCAP Primitive Type, Operation Code (OpCode) and optionally Application Context Name. Many modern STP vendors like Oracle, Dialogic, Ericson, etc. provide advanced TCAP-aware routing capabilities to support such configurations. The proposed solution can be extended to detect additional Bypass Fraud scenarios by routing CAP InitialDP messages not only for home subscribers but also for inbound roamers to

the HPLMN SCP. This can be achieved using STP TCAP-aware routing capabilities as described above and the SCCP High-Level Relay function, which allows inspection of CAP InitialDP messages without interrupting the TCAP dialogue between the HPLMN gsmSSF and VPLMN gsmSCF.

Section summary: in this chapter, we examined a single simple roaming Mobile-Originated Call (MOC) scenario, along with its associated roaming architecture and simplified examples of voice call termination within the HPLMN. In practice, there are many more complex Bypass Fraud scenarios. However, a significant portion of these can be detected and controlled by the HPLMN SCP (gsmSCF) using the CAP (IMS_CAP) and/or INAP protocols.

CAP/IMS_CAP/INAP InitialDP parameters for Bypass Fraud detection logic implementation

In the previous chapter, we reviewed the telecommunication network architecture and the key aspects required to support real-time Bypass Fraud detection using CAP/IMS_CAP/INAP protocols. The SCP business logic responsible for detecting Bypass Fraud on the HPLMN SCP (gsmSCF) relies both on data extracted from CAP/IMS_CAP/INAP messages and on internal SCP data and inputs from external BSS/IT systems. Table 1 lists the most valuable CAP/IMS_CAP/INAP protocol parameters relevant to the SCP's Bypass Fraud detection business logic, which are obtained from Telecommunication Networks via CAP/INAP/CAP_IMS protocols. The complete set of parameters can be found in the [14], [15] and [19] specifications.

Table 3

CAP, INAP, and CAP_IMS Protocol Parameters Relevant to Bypass Fraud Detection

ID	Information Element	CAP	CAP for IMS	INAP
1	serviceKey	yes	yes	yes
2	dialledDigits	no	no	yes
3	calledPartyURL	no	yes	no
4	calledPartyNumber	yes	yes	yes
5	callingPartyNumber	yes	yes	yes
6	callingPartyURL	no	yes	no
7	callingPartyBusinessGroupID	no	no	yes
8	callingPartysCategory	yes	yes	yes
9	iPSSPCapabilities	yes	yes	yes
10	locationNumber	yes	yes	yes
11	originalCalledPartyID	yes	yes	yes
12	originalCalledPartyURL	no	yes	no
13	mediaTypeInfoList	no	yes	no
14	serviceProfileIdentifier	no	no	yes
15	terminalType	no	no	yes
16	highLayerCompatibility	yes	yes	yes
17	additionalCallingPartyNumber	yes	yes	yes
18	bearerCapability	yes	yes	yes
19	eventTypeBCSM	yes	yes	yes
20	redirectingPartyID	yes	yes	yes
21	redirectingPartyURL	no	yes	no
22	redirectionInformation	yes	yes	yes
23	IMSI	yes	yes	no
24	subscriberState	yes	yes	no
25	locationInformation	yes	yes	no
26	ext-basicServiceCode	yes	yes	no
27	callReferenceNumber	yes	yes	no
28	sipCallId	no	yes	no
29	mscAddress	yes	yes	no
30	calledPartyBCDNumber	yes	yes	no
31	timeAndTimezone	yes	yes	no
32	gsm-ForwardingPending	yes	yes	no
33	gmscAddress	yes	yes	no
34	naCarrierInformation	yes	yes	no

The "serviceKey" information element is proposed to be used to uniquely identify each ISUP/SIP interconnect voice trunk. The values assigned to the serviceKey should not overlap with those used in O-CSI/O-IM-CSI or T-CSI/T-IM-CSI CAMEL subscriptions.

Bypass Fraud detection SCP platform and integration interfaces

The Bypass Fraud Detection SCP platform should be integrated with both the telecommunications network and the IT/OSS/BSS domains.

The BSS (Business Support Systems) domain encompasses platforms such as the Fraud Management System, Revenue Leakage Control System, Interconnect Billing System, Customer Relationship Management System, CDR and online Protocols Mediation System, and others. These systems should interface with the Bypass Fraud Detection SCP via an orchestration layer and through offline/online interfaces to avoid direct integration and simplify API changes when needed.

The main functional tasks to be supported by the Bypass Fraud Detection SCP in interaction with the BSS domain include:

- Provisioning the Bypass Fraud Detection service with parameters used by the SCP business logic:
  - Subscriber profiles
  - Interconnect and roaming partner profiles
  - Various blacklists, whitelists, and other data inputs of different types (volume, destination, duration, event type, event time, location, ratios, call spreads, etc.) required by the SCP logic
- Generating output data, including:
  - Offline CDRs
  - Online push notifications about events related to the execution of the Bypass Fraud Detection service logic

It is important to note that not all Bypass Fraud scenarios can be detected in real time. Therefore, near-real-time data analysis may be required at BSS domain nodes to assist the SCP logic in identifying fraudulent calls. In such scenarios, the SCP acts as an online interface between the core network and the fraud management components within the BSS domain.

The OSS (Operations Support Systems) domain includes components such as software/hardware monitoring, operational statistics, traffic processing KPI dashboards, configuration management, and other related systems and services.

The IT domain comprises services such as the National Mobile Number Portability (MNP) database, DNS, ENUM, NTP, Backup/Restore and various other IT-related functionalities.

Additionally, the SCP should be integrated with the HLR/HSS of the HPLMN using MAP [23] protocol. This integration enables real-time retrieval/update of subscriber profile data and location information directly from the telecommunications network when required.

Overall recommendations for Fraud Management Systems are outlined in [24] and [25]. Near real-time fraud detection techniques are discussed in GSMA FF.18 and 19. A comprehensive overview of various types of fraud affecting telecommunication networks is provided in [26]. The role of CAMEL services in real-time fraud detection and management procedures is reviewed in [27].

Bypass Fraud detection SCP platform Business Logic development and adaptation using Low-Code SW development lifecycle

Fraud in telecommunication networks continues to evolve, driven by the constant development of both new fraud techniques and corresponding detection and prevention methods. Among the most persistent and impactful threats are Roaming and Interconnect Fraud, where malicious actors or even dishonest operators exploit signaling, routing, or billing mechanisms to gain unauthorized financial advantage. This ongoing challenge is not merely a matter of criminal activity – it often represents a competitive and ethically gray struggle between operators seeking to maximize revenue from roaming and interconnect services. As a result, detecting and preventing such fraud requires continuous innovation, collaboration, and the deployment of intelligent network-based SCP-based solutions.

To enable a rapid response to continuously evolving fraud scenarios, the SCP-based Bypass Fraud Detection solution must provide mechanisms for the swift implementation, testing, and activation of business logic changes. One effective way to achieve this agility is by adopting a low-code software development approach, which significantly reduces development time and allows fraud detection rules and logic to be adapted with minimal programming effort. To support this approach, the telecommunications service operator should utilize an appropriate Low-Code Development Platform (LCDP) with Visual or Flow-Based Programming capabilities, integrated via the interfaces outlined in the previous chapter.

This approach enables telecommunication operator's staff to create custom applications or modify existing system functionality without deep knowledge of programming languages. Users interact with a graphical interface to manage business logic and system integration interfaces. Unlike the No-Code Software Development approach, where users can only utilize predefined system functionalities, the Low-Code Software Development approach provides users with a set of tools to customize system features or develop additional software modules. As a result, the software development lifecycle for solutions built using traditional methods differs significantly from that of Low-Code based development.

Figure 4 provides a comparison between the traditional software development platform lifecycle and the proposed Low-Code Development Platform (LCDP) lifecycle.

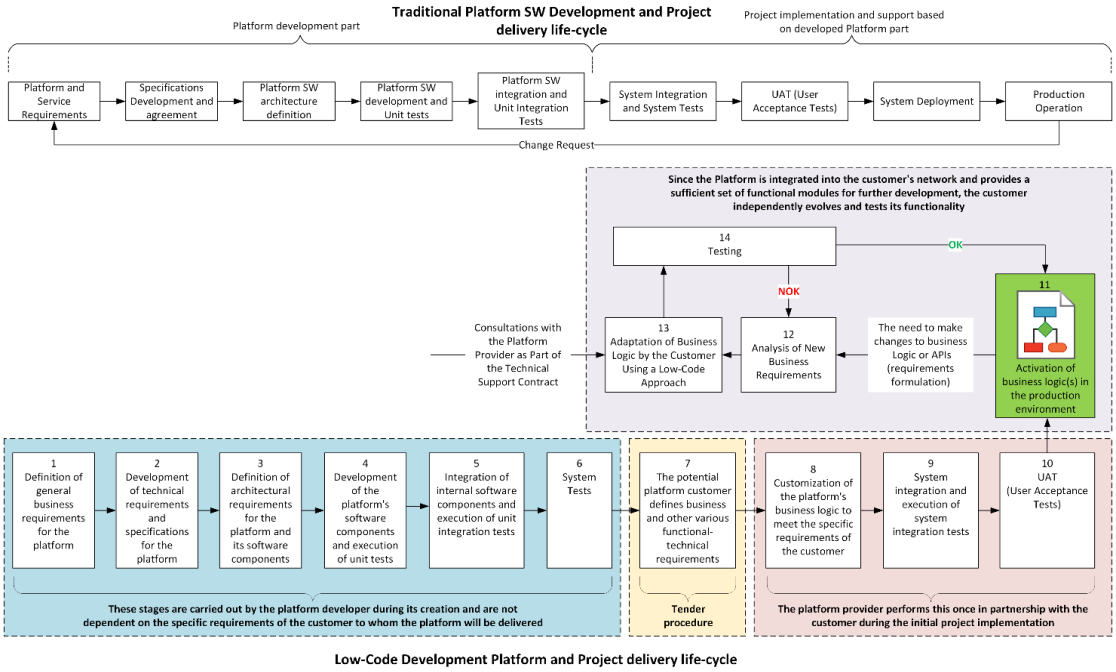

Fig. 4. Comparison between the traditional software development platform lifecycle and the proposed Low-Code Development Platform (LCDP) lifecycle

The main purpose of using a Low-Code Software Development Platform with Visual/Flow-Based programming capabilities for Bypass Fraud detection logic is to significantly shorten the change request implementation lifecycle, while eliminating the need to involve the core platform development team. Depending on the specific project, it is also possible to combine Low-Code with other software development approaches that support the so-called "runnable specification" methodology (such as DevOps development, Agile development, Model-Driven Development and others) where models, test definitions, or business logic diagrams serve not only as documentation but also as executable artifacts. This approach improves traceability, reduces implementation gaps, and accelerates the development lifecycle through SW lifecycle automation and early validation.

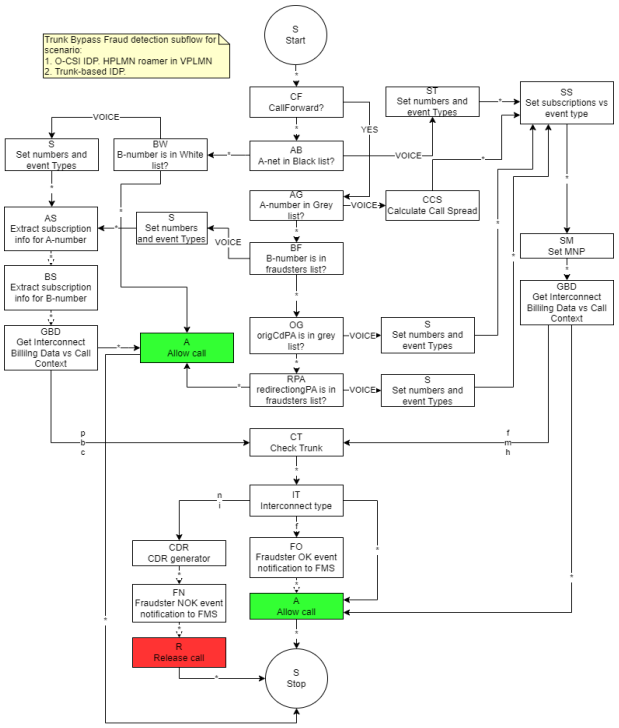

Fig. 4. Simplified example of Bypass Fraud detection
SCP business logic created using a Low-Code platform GUI

As shown in Figure 4, the user simply drags and drops the required handler implemented as functions via functional interfaces in Java onto the business logic canvas. The user then defines the execution flow by linking the handlers with arrows that represent specific events (“VOICE”, “p”, “b”, “c” as an example) – these events correspond to possible "exit codes" resulting from the execution of each individual handler.

This approach is based on the Event-Driven Architecture (EDA) concept, where services (or business logic flows) are constructed as Finite State Machines (FSMs) represented graphically with a finite number of states. One of the international standards used to describe such finite-state-based models is SCXML [28] – a markup language designed to represent FSM behaviour. SCXML evolved from the CCXML standard, which defines state-based interaction models for communication systems. These standards are grounded in mathematical models of state transitions [29] and UML state diagrams [30]. To visualize and design business logic flows, the low-code platform proposed to use an XML-based data format and a visual diagramming component.

Accordingly:

- The graphical user interface for designing Bypass Fraud detection business logic using the Low-Code Software Development (LCSD) approach is proposed to be built using the XML standard and the aforementioned visualization component.
- To execute the business logic in the Runtime Environment (RTE), the XML format is converted into SCXML [28].
- The JSON data interchange format, is proposed for describing business logic objects with their parameters and will serve as the primary internal data format for the platform.
- To enable users to create custom program modules without relying solely on built-in platform handlers should be supported two options:
  - possibility to develop its own handlers as java classes implementing the function interface required by the platform
  - a special type of handler should be provided. In this handler, user can write their own code using a scripting language that complies with the ECMAScript standard. This code is proposed to be

executed by the platform's core Java runtime engine using the Oracle GraalVM or Oracle Nashorn technology. Optionally this handler should support other programming languages like Python, Ruby, R, C/C++, Kotlin, Scala, Groovy, Clojure, etc.

The difference between the two options mainly relates to agility and the level of skill required. It is generally easier to start with a scripting-based solution. Scripts are compiled to bytecode and can be further translated to machine code at runtime by a Just-In-Time (JIT) compiler, so there is usually no significant performance loss. Later, the solution can be migrated to a more traditional software development lifecycle and implemented as a conventional Java artifact if needed.

AI-Augmented Low-Code Development for Fraud Detection

The integration of Artificial Intelligence (AI) and Machine Learning (ML) with low-code development platforms significantly enhances the agility, accuracy, and scalability of fraud detection systems in telecommunications. By automating key aspects of business logic design, anomaly detection, and system optimization, AI reduces dependency on manual programming while improving real-time fraud mitigation. Below are the core applications of AI in this context:

1) AI-Assisted Code Generation for Flow Blocks

Automated Block Creation: AI analyzes historical fraud patterns and automatically generates low-code blocks (e.g., CAP message validators, trunk routing checks) using natural language prompts (e.g., "Create a rule to flag calls from non-whitelisted trunks").

Smart Recommendations: AI suggests relevant logic blocks based on the developer's workflow (e.g., adding a "SIM-Box Detection" node after a "Call Routing Analysis" block).

2) Machine Learning for Real-Time Fraud Detection

Anomaly Detection: ML models (e.g., Isolation Forest, LSTM networks) process signaling data (CAP/INAP parameters) to identify deviations from normal call patterns (e.g., sudden spikes in international call durations).

Behavioral Profiling: Unsupervised learning clusters subscribers/interconnect partners into risk groups (e.g., "high-risk VoIP carriers") based on call metadata (serviceKey, calledPartyNumber).

3) AI-Driven Log Processing for Traffic Anomalies

Automated Log Analysis: NLP models parse system logs to detect hidden fraud patterns (e.g., repeated CAP errors from a specific MSC, suggesting trunk manipulation).

Root Cause Identification: AI correlates log anomalies with fraud incidents (e.g., linking a surge in InitialDP messages to a SIM-box attack).

4) Dynamic Business Logic Adjustment

Adaptive Rule Optimization: Reinforcement Learning (RL) fine-tunes fraud detection thresholds (e.g., adjusting callDuration limits) based on real-world efficacy.

Self-Healing Flows: AI identifies and corrects logic inefficiencies (e.g., replacing a slow "CDR Cross-Check" block with a pre-trained ML model).

5) AI-Powered Flow Navigation & Documentation

Semantic Search for Large Projects: AI indexes low-code workflows and enables natural language queries (e.g., "Find all blocks handling VoIP trunk validation").

Auto-Generated Documentation: AI summarizes complex flows into human-readable reports (e.g., "This path checks for SIM-box fraud using IMSI-IMPI binding").

Implementation Example:

Fraud Detection Flow: A developer drags an "ML Anomaly Detector" block onto the canvas. AI auto-configures the block to analyze calledPartyNumber and callReferenceNumber for patterns. Continuous Learning: The system flags a new bypass fraud tactic (e.g., "call forwarding to premium numbers"). AI recommends adding a "Premium Number Block" node to existing flows.

Such an AI/ML approach to low-code development has valuable benefits:

- AI reduces low-code development time by ~40% (e.g., auto-generating CAP/INAP handlers);
- ML models achieve better precision in fraud classification vs. rule-based systems;
- AI manages complexity in large projects (e.g., 1000+ logic blocks) via semantic search.

© Tymokhin Yu.A. (2025) Real-Time Detection of Interconnect Bypass Fraud in Telecommunication Networks: CAMEL framework Low-Code Approach and AI/ML Adaptation. Сучасний захист інформації, 3(63), 150–164. https://doi.org/10.31673/2409-7292.2025.031728

Future research direction possibilities:

- The use of generative AI, such as LLMs (e.g., GPT-4) to draft entire fraud detection workflows from scratch;

- Train local model/create local API solution within SCP platform to manage the use of external LLM without sharing raw data to avoid user data leak.

Conclusions

This article proposes a real-time solution for detecting Interconnect Bypass Fraud in telecommunication networks, leveraging the CAMEL framework, a low-code development approach, and AI/ML integration. The presented solution addresses the limitations of traditional detection methods by offering enhanced agility, scalability, and accuracy in combating evolving fraud techniques.

The CAMEL framework, specifically its CAP protocol, serves as a robust foundation for real-time call control and fraud detection across 2G, 3G, 4G, and 5G networks, including IMS-based call control through IMS_CAP. The proposed system integrates signaling protocol analysis (CAP/IMS_CAP/INAP) with AI-driven anomaly detection to address current and emerging fraud techniques.

A key aspect of this solution is the adoption of a low-code development platform (LCDP). This approach empowers telecommunication teams to rapidly adapt and deploy fraud detection rules with minimal programming expertise, significantly shortening the development lifecycle and reducing dependency on specialized programming skills.

Furthermore, the integration of AI and machine learning greatly enhances the system's ability to detect anomalies, profile behavior, and predict emerging fraud patterns, ensuring long-term scalability and accuracy. AI assists in code generation, provides smart recommendations for logic blocks, and enables dynamic adjustment of business logic. ML models are utilized for real-time anomaly detection and behavioral profiling based on signaling data.

While the focus of this article is on a specific mobile-originated call scenario, the proposed solution is flexible and can be extended to detect various other complex bypass fraud scenarios by leveraging the capabilities of the HPLMN SCP (gsmSCF) with CAP (IMS_CAP) and/or INAP protocols. The ability to route InitialDP messages for both home subscribers and inbound roamers to the Bypass Fraud Detection SCP further enhances detection capabilities.

Overall, the research presented offers practical insights for telecommunication operators and vendors aiming to mitigate revenue losses and improve service integrity through an agile, efficient, and future-proof real-time fraud detection system. Future research directions include exploring the use of generative AI, such as Large Language Models (LLMs), to draft entire fraud detection workflows and developing local API solutions within the SCP platform to manage external LLMs while safeguarding user data.

References

1. Kouam, A. J., Viana, A. C., & Tchana, A. (2021). SIMBox bypass frauds in cellular networks: Strategies, evolution, detection, and future directions. IEEE Communications Surveys & Tutorials, 23(4), 2295–2323. https://doi.org/10.1109/COMST.2021.3100916

2. Kouam, A. J., Viana, A. C., & Tchana, A. (2024). Battle of Wits: To What Extent Can Fraudsters Disguise Their Tracks in International Bypass Fraud? ACM ASIACCS. https://dl.acm.org/doi/10.1145/3639912.3644265

3. Salaudeen, L. G., et al. (2022). A Plethoric Literature Survey on SIMBox Fraud Detection in Telecommunication Industry. Direct Research Journal of Engineering and Information Technology, 8(1), 1–11. https://www.directresearchpublisher.org/direct-research-journal-of-engineering-and-information-technology/volume-8-issue-1/a-plethoric-literature-survey-on-simbox-fraud-detection-in-telecommunication-industry/

4. Advanced predictive intelligence for termination bypass detection and prevention. (2012). WO 2012/003514 A1. World Intellectual Property Organization. https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2012003514

5. Illegal carrier detection platform and method. (2011). WO 2011/080638 A1. World Intellectual Property Organization. https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2011080638

6. Predictive intelligence. (2009). US 8,238,905 B2. U.S. Patent and Trademark Office. https: // patents. google.com/patent/US8238905B2/en

7. A method and system for detecting mobile numbers used by international gateway bypass (SIM Box) operators. (2012). WO 2012/080781 A1. World Intellectual Property Organization. https://patentscope.wipo.int/search /en/ detail.jsf?docId=WO2012080781

8. A system and method for detecting call bypass fraud in mobile communication networks. (2018). WO 2018/203842 A2. World Intellectual Property Organization. https://patentscope.wipo.int/search / en / detail. jsf?docId=WO2018203842.

9. Sahaidak, V. (2024). OVERVIEW OF FRAUD DETECTION SYSTEMS AND PERFORMANCE KPI DEVELOPMENT. Кібербезпека: освіта, наука, техніка. https://szu-journal.duit.edu.ua/

10. Sahaidak, V. A., Lysenko, M. M., & Senkov, O. V. (2022). Telecom fraud and its impact on mobile carrier business. Connectivity, 1(1), 47–56. https://connectivity.knuba.edu.ua/index.php/journal/article/view/17

11. Карпишин, Н. Я., & Кравчук, С. О. (2023). ДОСЛІДЖЕННЯ МЕТОДІВ МОНІТОРИНГУ ТРАФІКУ ДЛЯ ПРОТИДІЇ ФРОДУ В IP-ТЕЛЕФОНІЇ. Міжнародна науково-технічна конференція.

12. ETSI. (n.d.). GSM 03.02: Digital cellular telecommunications system (Phase 2+); Network architecture. Retrieved from https://www.etsi.org/deliver/etsi_gts/03/0302/05.00.00_60/gsm_0302v050000p.pdf

13. 3GPP. (n.d.). TS 23.002: Universal Mobile Telecommunications System (UMTS); LTE; Network architecture. Retrieved from https://www.3gpp.org/ftp/Specs/archive/23_series/23.002/

14. 3GPP. (n.d.). TS 23.501: System architecture for the 5G System (5GS). Retrieved from https://www.3gpp.org/ ftp/Specs/archive/23_series/23.501/

15. GSMA. (n.d.). IR.88: EPS Roaming Guidelines. Retrieved from https://www.gsma.com/newsroom/ resources /ir-88-eps-roaming-guidelines/

16. GSMA. (n.d.). NG.113: 5GS Roaming Guidelines. Retrieved from https://www.gsma.com/newsroom/ resources/ng-113-5gs-roaming-guidelines/

17. 3GPP. (n.d.). TS 23.078: Customised Applications for Mobile network Enhanced Logic (CAMEL). Retrieved from https://www.3gpp.org/ftp/Specs/archive/23_series/23.078/

18. 3GPP. (n.d.). TS 29.078: CAMEL Application Part (CAP) specification. Retrieved from https://www.3gpp. org/ftp/Specs/archive/29_series/29.078/

19. ITU-T. (n.d.). Recommendation Q.1200-Q.1699: Intelligent Network (IN) recommendations. Retrieved from https://www.itu.int/rec/T-REC-Q.1200-200503-I/en

20. 3GPP. (n.d.). TS 23.228: IP Multimedia Subsystem (IMS). Retrieved from https://www.3gpp.org/ ftp/Specs/archive/23_series/23.228/

21. 3GPP. (n.d.). TS 24.229: IP multimedia call control protocol based on SIP and SDP. Retrieved from https://www.3gpp.org/ftp/Specs/archive/24_series/24.229/

22. 3GPP. (n.d.). TS 23.278: Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 4 – Stage 2. Retrieved from https://www.3gpp.org/ftp/Specs/archive/23_series/23.278/

23. 3GPP. (n.d.). TS 29.278: CAMEL Application Part (CAP) specification for IMS. Retrieved from https://www.3gpp.org/ftp/Specs/archive/29_series/29.278/

24. 3GPP. (n.d.). TS 23.272: Circuit Switched (CS) fallback in Evolved Packet System (EPS). Retrieved from https://www.3gpp.org/ftp/Specs/archive/23_series/23.272/

25. GSMA. (n.d.). FF.02: Fraud Management Systems - Guidelines for Mobile Network Operators. Retrieved from https://www.gsma.com/newsroom/resources/ff-02-fraud-management-systems-guidelines-for-mobile-network-operators/

26. GSMA. (n.d.). FF.21: Fraud Manual. Retrieved from https://www.gsma.com/newsroom/resources/fraud-manual/

27. GSMA. (n.d.). FS.24: CAMEL Roaming Fraud Management Handbook. Retrieved from https://www.gsma. com/newsroom/resources/fs-24-camel-roaming-fraud-management-handbook/

28. W3C. (n.d.). State Chart XML (SCXML): State Machine Notation for Control Abstraction (W3C Recommendation). Retrieved from https://www.w3.org/TR/scxml/

29. Ecma International. (n.d.). ECMA-404: The JSON data interchange syntax. Retrieved from https://www.ecma-international.org/publications-and-standards/standards/ecma-404/

30. Oracle. (n.d.). GraalVM: An advanced JDK with ahead-of-time Native Image compilation. Retrieved from https://www.graalvm.org/

Надійшла 01.08.2025