Supplementary details of Unsupervised Cross-Protocol Anomaly Analysis in Mobile Core Networks via Multi-Embedding Models Consensus

anonymous authors

I. Methodology

B. Synthetic Anomaly Construction

We create protocol-plausible inconsistencies through single field-group swaps applied to pairs of fused records. A field group is a coherent set of paths that refer to the same concept across messages. For each mutation, we leverage two given source records and exchange all paths in the chosen group so that each swap preserves per-protocol validity yet induces a contradiction in the joint view. For both mutated outputs we attach minimal metadata, indicating the mutation family and field group. Each synthetic record includes exactly one swap group. Pairs where paths are absent or values are identical are skipped, and all other fields remain untouched. We implement the thirteen field groups listed below.

1) SS7: Calling-Party Global Title (CGGT): In Signalling System No. 7 (SS7) with the Mobile Application Part (MAP), the Calling-Party Global Title (CGGT) identifies the apparent originating node or interconnect (e.g., the serving Mobile Switching Centre/Visitor Location Register, MSC/VLR) and is carried in the Signalling Connection Control Part (SCCP) addressing fields [1]. MAP procedures that convey subscriber mobility context (e.g., `UpdateLocation`, `SendRoutingInfo`) are specified in 3GPP TS 29.002 [2]. Our mutation swaps the full CGGT group between two fused records (GT's value together with derived operator or location attributes such as country and PLMN identifiers MCC/MNC), which keeps the SS7 fragment syntactically valid and routable [3]. In the fused, minute-level view for the same subscriber, the apparent SS7 origin can then contradict contemporary indicators in other protocols, such as the `Origin-Host` attribute in the Diameter base protocol (RFC 6733) or the visited-network and location indicators carried in Diameter S6a and GTP control plane (3GPP TS 29.272 and TS 29.274) [4]. This produces the cross-protocol inconsistency we intend to surface while leaving each protocol's message individually valid [5].

2) SS7: Called-Party Global Title (CDGT): In SS7 with the Signalling Connection Control Part (SCCP), the Called-Party Global Title (CDGT) is the destination addressing element used for global title translation and routing to the target application entity (e.g., a Home Location Register, HLR) [1]. In Mobile Application Part (MAP) procedures, the called-party address commonly carries numbering formats such as E.214 that are derived from subscriber identifiers and used to reach databases like the HLR or serving switches [3]. Our mutation swaps the entire CDGT group between two fused records while leaving message structure and MAP operation semantics intact, so the SS7 segment remains syntactically valid and routable on its own [2]. In the fused, minute-level view for the same subscriber, the altered destination can conflict with contemporary context in other protocols (e.g., the Diameter `Origin-Host`/visited-PLMN or GTP control-plane state), creating an apparent misrouting of signalling traffic [6]. Such cross-protocol inconsistencies are consistent with known risks in interconnect signalling, where manipulated global titles can enable redirection, interception, or charging anomalies if downstream routing follows the modified address.

3) SS7: Point Codes (OPC/DPC): In SS7, the Originating Point Code (OPC) and Destination Point Code (DPC) identify the source and destination signalling points and are carried in the Message Transfer Part level 3 (MTP3) routing label [7]. In mobile core signalling, Mobile Application Part (MAP) transactions traverse network functions such as the Mobile Switching Centre/Visitor Location Register (MSC/VLR) and the Home Location Register (HLR), so the OPC/DPC pair implies which network nodes a transaction appears to use along its path [8]. Our mutation swaps the OPC and DPC (including operation-level fields when present) between two fused records while leaving other fields intact, which keeps the SS7 message syntactically valid and routable [7]. In the fused, minute-level view for the same subscriber, the altered OPC/DPC can contradict contemporary context carried in Diameter or GTP, exemplifying as an apparent change in the signalling path through different MSC/VLR domains [6]. Such cross-protocol inconsistencies align with documented interconnect risks where manipulated routing information can lead to misdirection or exposure of signalling traffic.

4) SS7: Application Context: In SS7 with the Mobile Application Part (MAP), the Application Context Name (ACN) identifies the negotiated set of MAP operations and version for a Transaction Capabilities Application Part (TCAP) dialogue [2]. The ACN is carried in the TCAP dialogue portion and constraints that MAP operations are semantically valid. An invoked operation that does not match the negotiated ACN constitutes a protocol-level inconsistency even if lower-layer encoding remains well formed [9]. Our mutation swaps the ACN between two fused records while leaving other fields unchanged, which preserves SS7 decodability but alters the intended operation family and version associated with the MAP transaction [2]. In the fused, minute-level view for the same subscriber, the altered ACN can conflict with contemporary context in other protocols (e.g., procedure stage or visited-network information inferred from Diameter or GTP), inducing a cross-protocol inconsistency [6]. Such inconsistencies align with documented interconnect risks, where manipulated or inappropriate MAP application contexts can contribute to misrouting or information exposure when combined with other control-plane signals.

5) Diameter: User Identifier (User-Name): In the Diameter control plane, the *User-Name* Attribute-Value Pair (AVP) serves as the user identity container and is defined by the Diameter base protocol [4]. On the Subscription-Data-Application (S6a) interface used between the Mobility Management Entity (MME) and the Home Subscriber Server (HSS), 3GPP specifies that *User-Name* carries the International Mobile Subscriber Identity (IMSI) for the subscriber [5]. Our mutation swaps the entire *User-Name* AVP between two fused records, which preserves message structure and remains valid under the Diameter AVP rules. In the fused, minute-level view for the same subscriber, the altered Diameter identity can then disagree with the IMSI conveyed or implied by other protocols, such as the IMSI and location context present in GPRS Tunnelling Protocol control signalling (GTPv2-C) and MAP procedures [10]. This identity mismatch across protocols is a cross-protocol inconsistency of operational concern, as highlighted in signalling-security guidance for interconnect environments [6].

6) Diameter: Session-Id: In the Diameter control plane, the *Session-Id* Attribute-Value Pair (AVP) is the end-to-end identifier that uniquely labels a Diameter session and must remain constant across all related requests and answers [4]. On the Subscription-Data-Application (S6a) interface between the Mobility Management Entity (MME) and the Home Subscriber Server (HSS), procedures require the request and the corresponding answer to carry the same *Session-Id* so that transactions are correlated reliably [5]. Our mutation swaps the *Session-Id* between two fused records while leaving the Diameter message structure intact, which preserves AVP validity but alters the session linkage implied by the control plane. In the fused, minute-level view for the same subscriber, this change can make two different subscribers appear to share one Diameter session or can split one subscriber's activity across mismatched sessions, which conflicts with GPRS Tunnelling Protocol control-plane (GTPv2-C) bearer and tunnel state [10]. Such cross-protocol inconsistencies align with known interconnect risks, where manipulated identifiers in one protocol can mislead downstream processing or create opportunities for misrouting and abuse.

7) Diameter: Origin-Host: In the Diameter control plane, the *Origin-Host* Attribute-Value Pair (AVP) identifies the sending Diameter node and is used together with *Origin-Realm* for peer identification and routing. On the S6a interface between the Mobility Management Entity (MME) and the Home Subscriber Server (HSS), messages carry *Origin-Host* to denote the specific MME instance and its administrative domain, which anchors subsequent transactions for the same subscriber [5]. Our mutation swaps the *Origin-Host* value in the request across two fused records while leaving other AVPs intact, which preserves AVP syntax and Diameter message validity but alters the apparent source node and realm [4]. In the fused, minute-level view for the same subscriber, the altered Diameter origin can contradict contemporary SS7 routing indicators (e.g., Calling-Party Global Title or point codes) and GPRS Tunnelling Protocol (GTP) control-plane context such as visited-network or location information, thereby creating a cross-protocol inconsistency. This kind of origin impersonation is consistent with signalling-security concerns reported for interconnect environments, where manipulation of peer-identifying attributes can enable misleading transaction provenance and misrouting [6].

8) Diameter: Visited-PLMN-Id: On the Subscription-Data-Application (S6a) interface, the *Visited-PLMN-Id* Attribute-Value Pair (AVP) conveys the identifier of the currently visited Public Land Mobile Network as an MCC/MNC pair. The encoding and interpretation of PLMN identifiers (MCC/MNC) are specified in the Non-Access Stratum (NAS) procedures for Evolved Packet System mobility management [11]. Our mutation swaps the MCC/MNC carried in *Visited-PLMN-Id* between two fused records, which preserves Diameter message syntax while changing the asserted visited network for the same subscriber and minute. In the fused view, this altered Diameter visited-PLMN can conflict with contemporaneous SS7 or GTP indicators (e.g., routing addresses, user-location information, or APN context), producing a false roaming or location-spoofing signal [12]. Roaming guidelines further emphasize that consistent PLMN identity across interfaces is required for correct inter-PLMN procedures, which motivates cross-protocol checks for such inconsistencies.

9) Diameter: APN Service-Selection: On the S6a interface, subscriber provisioning is conveyed in the *Subscription-Data* container, which includes an *APN-Configuration* list. Each entry carries a *Service-Selection* AVP that names the allowed Access Point Name (APN) for packet-data connectivity. The APN string format and naming rules are defined by 3GPP as a DNS-like label sequence that identifies the external packet data network (PDN) to be reached [3]. In the control plane for bearer establishment, the requested APN is carried in GPRS Tunnelling Protocol for Control plane (GTPv2-C) messages such as `Create Session Request`, and the network selects or verifies the APN accordingly [10]. Our mutation swaps the *Service-Selection* entries in the *APN-Configuration* list between two fused records while keeping Diameter syntax valid, which can cause the provisioned APN profile in Diameter to diverge from the APN signalled in concurrent GTP procedures for the same subscriber and minute [5]. Such divergence is operationally relevant because alignment of the provisioned APN set with the APN used on the bearer is assumed by roaming and interworking guidelines and by EPC architectural specifications [6].

10) GTP: TEIDs: In the GPRS Tunnelling Protocol (GTP), the Tunnel Endpoint Identifier (TEID) labels a specific tunnel and binds user traffic or control transactions to that tunnel context. On the control plane (GTPv2-C), Fully Qualified TEID (F-TEID) information elements carry the TEID together with the associated IP address to identify endpoints of EPS bearer procedures [10]. On the user plane (GTP-U), the TEID appears in every GTP-U header and demultiplexes user packets to the correct EPS bearer at the receiving gateway [13]. Our mutation swaps TEID values between two fused records (for control and, when present, user plane) while leaving message structure intact, which preserves protocol syntax but changes the tunnel binding implied by the control and user planes [14]. In the fused, minute-level view for the same subscriber, such swaps can make two different user equipments (UEs) appear to share one bearer or can split one UE's traffic across mismatched tunnels, contradicting the session and bearer relationships defined for the Evolved Packet System (EPS) and exposed concurrently in Diameter.

11) GTP: APN: In the GPRS Tunnelling Protocol control plane (GTPv2-C), the Access Point Name (APN) is carried as an information element in procedures such as `Create Session Request` to indicate the external packet data network to be reached. APN naming and resolution follow 3GPP DNS procedures that derive a fully qualified domain name and select appropriate gateways for the requested PDN [10]. Our mutation swaps the APN value in the relevant GTP control messages between two fused records while leaving message structure and syntax valid for GTPv2-C. In the fused, minute-level view for the same subscriber, the altered APN in GTP can conflict with the subscribed APN profile conveyed in Diameter S6a within the *Subscription-Data* container (APN-Configuration and Service-Selection), creating a cross-protocol inconsistency [5]. Such divergence is operationally relevant because policy and charging control assume alignment between the subscriber's provisioned APN set and the APN used on the bearer during establishment and enforcement.

12) GTP: User Location Information: In the GPRS Tunnelling Protocol control plane (GTPv2-C), the *User Location Information* (ULI) information element carries the serving network and cell context, including Mobile Country Code/Mobile Network Code (MCC/MNC) and area or cell identifiers such as Location Area Code (LAC), Tracking Area Code (TAC), Routing Area Code (RAC), and Cell Identity (CI) [10]. The formats and semantics of these identifiers (PLMN codes, LAC/TAC, and GERAN/UTRAN/E-UTRAN cell identities) are defined in the 3GPP numbering and identification specification [3]. Our mutation swaps the MCC, MNC, and the relevant area and cell identifiers within the ULI between two fused records while leaving GTP message structure and syntax valid. In the fused, minute-level view, the altered ULI can contradict the visited-network identity conveyed concurrently on the Diameter S6a interface (e.g., the *Visited-PLMN-Id* AVP), producing a location or roaming inconsistency [5]. The altered ULI can also disagree with recent mobility updates recorded in SS7/MAP procedures such as `UpdateLocation`, which further exposes cross-protocol contradictions for the same subscriber and time window [2].

13) GTP: PDN IP Address: In the GPRS Tunnelling Protocol control plane (GTPv2-C), the PDN Address Allocation (PAA) information element carries the IP address (IPv4 and/or IPv6) assigned to the user equipment and is included by the Packet Data Network Gateway (P-GW) in procedures such as `Create Session Response` [10]. The allocation and binding of this PDN address to the subscriber's EPS bearer context are specified in the Evolved Packet System mobility architecture, which requires consistent association of the address with the corresponding PDN connection and user identity [14]. Our mutation swaps the assigned PDN IPv4 address between two fused records while leaving GTPv2-C message structure valid, so the control-plane signalling remains syntactically correct although the address-to-subscriber binding is altered. In the fused, minute-level view, this change can make the same IP address appear on multiple subscribers or can decouple a subscriber's Diameter and GTP contexts, which is inconsistent with the EPS requirement that a PDN address be uniquely and correctly associated with a single active PDN connection [2].

References

[1] "Q.713:Signalling connection control part formats and codes." [Online]. Available: https://www.itu.int/rec/T-REC-Q.713

[2] "Specification # 29.002." [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1585

[3] "TS 123 003 - V16.3.0 - Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification (3GPP TS 23.003 version 16.3.0 Release 16)."

[4] V. Fajardo, J. Arkko, J. A. Loughney, and G. Zorn, "Diameter Base Protocol," Internet Engineering Task Force, Request for Comments RFC 6733, Oct. 2012, num Pages: 152. [Online]. Available: https://datatracker.ietf.org/doc/rfc6733

[5] "ETSI TS 129 272 V17.2.0 (2022-05) Universal Mobile Telecommunications." [Online]. Available: https://www.intertekinform.com/en-gb/standards/

[6] "Signalling Security in Telecom SS7/Diameter/5G | ENISA," Sep. 2025. [Online]. Available: https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g

[7] "Q.704:Signalling network functions and messages." [Online]. Available: https://www.itu.int/rec/T-REC-Q.704

[8] "Specification # 23.002." [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=728

[9] "Q.773:Transaction capabilities formats and encoding." [Online]. Available: https://www.itu.int/rec/T-REC-Q.773

[10] "ETSI TS 129 274." [Online]. Available: https://store.accuristech.com/standards/etsi-ts-129-274?product_id=2208669&srsltid=AfmBOopGku6zMszUYfVoYp4YwMP2Vak_x8L6ZPzYwOFCfam5yXXaeAt4

[11] "IR.88 EPS Roaming Guidelines Version 29.0," Dec. 2021. [Online]. Available: https://www.gsma.com/newsroom/gsma_resources/ir-88-eps-roaming-guidelines-version-27-1/

[12] "Communications Security, Reliability, and Interoperability Council VI | Federal Communications Commission." [Online]. Available: https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council

[13] "ETSI TS 129 281 V17.4.0 (2022-10) Universal Mobile Telecommunications." [Online]. Available: https://www.intertekinform.com/en-ca/standards/

[14] "TS 123 401 - V17.11.0 - LTE; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401 version 17.11.0 Release 17)."