UE-Guard: Formal Specification-Based Cellular Attack Detection of False Base Stations and Attacks on UE *

Vincent Abella[1], Philip Virgil Astillo[2], I Wayan Adi Juliawan Pawana[1,3], and Ilsun You[1]

[1] Kookmin University, Seoul, South Korea
{vincent, adijuliawan, isyou}@kookmin.ac.kr
[2] University of San Carlos, Cebu, Philippines
pvbastillo@usc.edu.ph
[3] Udayana University, Badung, Indonesia
adijuliawanpawana@unud.ac.id

Abstract

Cellular networks face significant security threats from false base station attacks and signal overshadowing that exploit asymmetric authentication between user equipment (UE) and network infrastructure. Current detection approaches using machine learning suffer from computational overhead, limited interpretability, and excessive resource consumption on mobile devices. This paper presents UE-Guard, a specification-based intrusion detection framework for 4G/5G User Equipment that leverages UPPAAL formal verification to detect cellular network attacks through integrated protocol monitoring. UE-Guard implements a coordinated system of twelve behavior rules (BR1-BR12) derived from 3GPP RRC and NAS protocol specifications, designed to operate collectively across protocol layer boundaries and state machine transitions. The rule framework detects attacks through coordinated violations rather than isolated checks, where BR1-BR3 establish RRC layer trust, BR4-BR8 validate NAS registration and security with state-dependent context, and BR9-BR12 enforce post-registration integrity through rule interdependencies. We formally verify all behavior rules using UPPAAL model checking, successfully verifying 20 temporal logic properties across three dimensions—completeness, correctness, and temporal compliance—providing formal-model assurances for the verified properties. Evaluation across 17,096 packets from 51 datasets shows a 97.57% message-level detection rate over 16,582 attack messages with zero false positives across 514 normal packets. The framework, measured on a Python prototype running on macOS with Apple Silicon (16GB RAM), processes 103.0 messages/second with 9.7ms average detection latency, consuming 22.9 MB peak memory and 39.6% average CPU utilization. The measured performance characteristics suggest feasibility for mobile deployment, though actual mobile device performance requires further evaluation.

Keywords: False Base Station, Signal Overshadowing, Specification-based Cellular Attack Detection, Cellular Security, Protocol Compliance, Formal Verification, Detection Framework

1 Introduction

The proliferation of mobile communications has transformed cellular networks into critical infrastructure supporting emergency services, financial transactions, and essential societal functions. However, this pervasive connectivity has created new attack vectors that threaten individual privacy and national security. Techniques such as false base station attacks and advanced

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. 63, December 16-18, 2025, Sapporo, Japan.

signal overshadowing can enable adversaries to track UE location, eavesdrop on communication, denial of service, and manipulation of UE behavior through rogue signaling messages [1].

Current detection approaches predominantly utilize artificial intelligence and machine learning solutions, achieving high accuracy rates but suffering from significant limitations including computational overhead, poor battery efficiency on mobile devices, and lack of interpretability that hinders forensic analysis and regulatory compliance. While the 3GPP standardization effort has introduced frameworks for cellular security monitoring, current implementations remain primarily network-centric and do not fully exploit UE-level detection capabilities. This emphasizes the critical need for lightweight, interpretable, and UE-resident security mechanisms that can complement the current network-based solutions while enabling real-time threat detection and response to evolving threats.

Specification-based cellular attack detection offers a compelling alternative by monitoring UE protocol behavior against 3GPP specifications, providing deterministic detection with explainable results and predictable performance characteristics. However, existing specification-based cellular attack detection approaches lack extensive behavior rule frameworks that systematically address cellular attack vectors. The integration of formal verification methods using UPPAAL enables formal-model assurances about detection behavior and system correctness, while modern mobile devices provide the computational capabilities for real-time protocol monitoring.

This research addresses the need for systematically developed and formally verified behavior rules that can detect cellular attacks through UE-side protocol monitoring. The proposed approach develops an extensive set of behavior rules based on 3GPP Radio Resource Control (RRC) and Non-Access Stratum (NAS) protocol specifications, with core security requirements derived from the standards and detection thresholds chosen as reasonable engineering parameters. Each behavior rule maps security requirements to specific threats and establishes detection criteria, providing a structured framework for protocol compliance monitoring. These behavior rules undergo rigorous formal verification using UPPAAL model checking to provide formal-model assurances of detection correctness. The key contributions of this paper are:

- Development of twelve behavior rules (BR1-BR12) that address critical security vulnerabilities derived from 3GPP security requirements, including authentication bypasses, message integrity violations, identity harvesting, service disruption, network spoofing, and connection state management attacks
- Formal verification of the behavior rule models using UPPAAL model checking, providing formal-model assurances of correctness for detecting the implemented attack patterns
- Establishment of a specification-based cellular attack detection framework that combines protocol compliance monitoring with formal verification, enabling deterministic and explainable security decisions for UE-side detection

2 Related Work

2.1 Specification-Based Cellular Attack Detection

Specification-based cellular attack detection systems monitor UE protocol behavior in line with 3GPP specifications, detecting deviations that indicate cellular security violations such as false base station attacks and signal overshadowing [2]. This approach provides deterministic detection with explainable results, making it suitable for environments where protocol compliance can be clearly defined.

Unlike anomaly-based approaches that require extensive training data, specification-based cellular attack detection methods offer predictable performance characteristics and can be deployed immediately [2]. In cellular networks, this approach is valuable for detecting protocol-level attacks that manipulate RRC and NAS signaling procedures [3].

The application of specification-based cellular attack detection to communication protocols has shown promising results in detecting protocol misbehaviors and state machine violations [3]. However, existing approaches have primarily focused on traditional network protocols rather than the complex signaling procedures inherent in cellular networks. The unique characteristics of RRC and NAS protocols, including their interdependencies, timing requirements, and security context management, necessitate specialized behavior rule development that addresses the specific vulnerabilities of cellular communication systems such as false base station attacks and signal overshadowing.

2.2 Formal Verification in Network Security

Formal verification provides rigorous analysis of system models against specified properties through mathematical techniques [4]. The UPPAAL model checker, based on timed automata theory, has emerged as an effective tool for analyzing real-time systems with timing constraints, making it well-suited for cellular protocol verification [5].

Recent applications of UPPAAL in protocol security verification have demonstrated its effectiveness in analyzing wireless security protocols, including IEEE 802.11i authentication mechanisms and Internet of Things (IoT) protocols [6]. These studies have shown that timed automata provide an appropriate formalism for modeling the temporal characteristics of security protocols, enabling verification of properties such as authentication correctness, message ordering constraints, and timing-sensitive security requirements [7]. The ability to model concurrent processes with shared variables and synchronization channels makes UPPAAL particularly suitable for cellular protocol analysis [8].

While formal verification has been applied to various network security problems, its application to UE-side cellular attack detection is less explored [6]. The development of formally verified behavior rules provides a systematic approach to specification-based cellular attack detection. The integration of formal verification with specification-based cellular attack detection provides formal-model assurances of detection correctness, enabling precise characterization of security properties and extensive verification of system behavior.

3 Background

3.1 Cellular Protocol Stack

Modern cellular networks operate through a hierarchical protocol stack where Layer-3 signaling protocols manage critical communication functions [9], as illustrated in Figure 1. RRC operates between UE and radio access network (RAN) components, handling radio bearer establishment, security mode setup, and mobility procedures [9].

NAS manages communication between UE and core network functions, controlling authentication, security context establishment, and session management [10]. NAS protocols handle mobility management, session management, and security procedures that are independent of the radio access technology [11].

RRC messages are transmitted over Signaling Radio Bearers (SRBs), with SRB0 for initial access, SRB1 for RRC messages including piggybacked NAS, and SRB2 for dedicated NAS communications after security activation. The interdependency between RRC and NAS protocols creates potential attack vectors through protocol manipulation and timing exploits. Understanding these protocol interactions is essential for developing effective behavior rules that can detect sophisticated attacks targeting multiple protocol layers simultaneously.

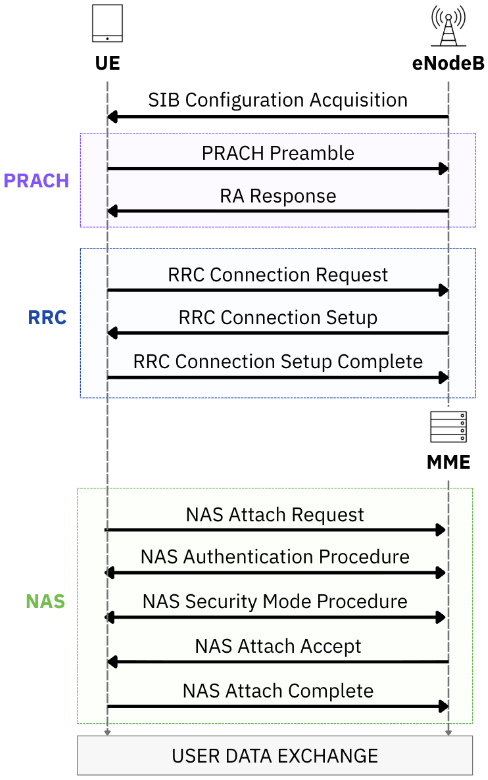


Figure 1: Cellular Protocol Stack showing RRC and NAS message flows between UE, RAN, and Core Network with security procedures.

3.2 Attack Vectors

False base station (FBS) attacks exploit the asymmetric authentication model in cellular networks where user equipment (UE) devices do not authenticate base stations [16]. Attackers deploy rogue infrastructure that broadcasts stronger signals to attract UE connections, enabling International Mobile Subscriber Identity (IMSI) catching, location tracking, and communication interception [3].

Modern FBS attacks employ advanced techniques such as bidding down attacks that manipulate NAS reject messages and RRC release procedures to force connections to less secure network generations [3]. Advanced adversaries also use signature reshaping strategies, modifying non-critical message fields and temporal sequences to evade detection while maintaining attack functionality [16].

Signal overshadowing represents an evolution beyond traditional FBS attacks, achieving high success rates with minimal power advantages through precisely timed signal injection [20].

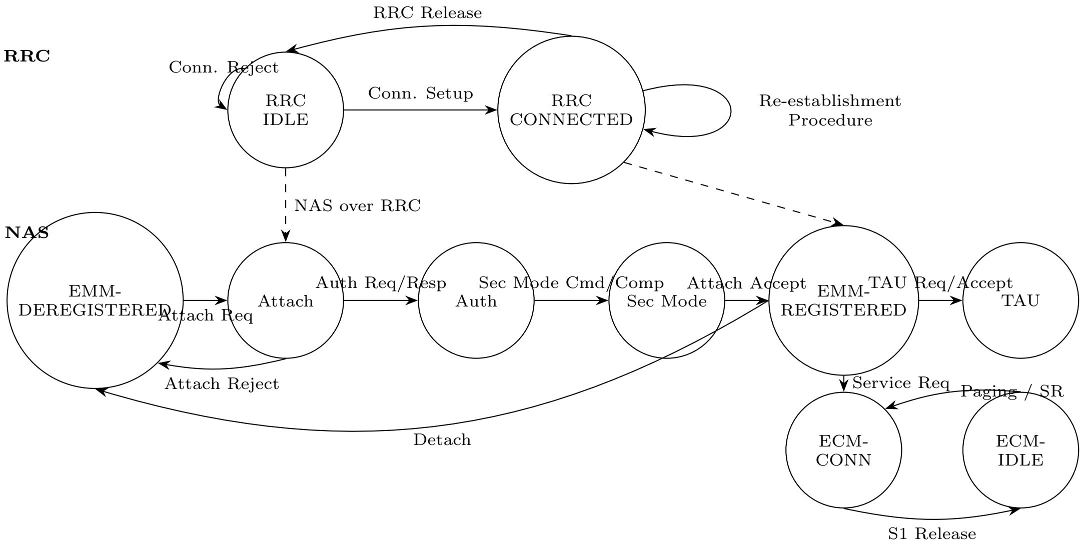


Figure 2: RRC/NAS State Machine (4G LTE/EPS): Normal protocol progression showing RRC states (IDLE/CONNECTED), EMM registration sequence (Attach, Authentication, Security Mode), ECM connection states, and TAU mobility procedures per TS 36.331 and TS 24.301.

These attacks exploit the capture effect in wireless communication, targeting multiple protocol layers simultaneously with microsecond-level temporal precision, requiring sophisticated detection mechanisms that can identify subtle timing anomalies and message sequence violations.

4 Proposed System

4.1 Adversarial Model

The adversarial model considers attackers with capabilities to establish false base stations using software-defined radio equipment, enabling them to impersonate legitimate network infrastructure and manipulate UE communication protocols. These attackers possess the technical expertise to implement sophisticated attacks targeting multiple protocol layers, including RRC connection procedures, NAS authentication sequences, and security mode establishment processes.

Attackers primarily exploit vulnerabilities in the NAS and RRC signaling protocols through several attack vectors [9]. They can intercept and modify authentication messages to bypass security procedures, inject malicious service reject messages to force service disruption, and conduct identity tracking attacks through repetitive false identity requests [18]. Advanced attackers can manipulate sequence numbers to break protocol synchronization and spoof network identity parameters to redirect UEs to malicious networks [16].

The attackers' intentions range from passive surveillance through International Mobile Subscriber Identity (IMSI) catching and location tracking to active service denial by forcing UEs to detach from legitimate networks [19]. Man-in-the-middle attacks position attackers between the UE and legitimate network to intercept sensitive communications, while more sophisticated attacks attempt to replay previous authentication sequences or manipulate protocol state transitions to gain unauthorized access [3].

These attack vectors directly violate the security assumptions embedded in 3GPP specifications regarding message integrity, authentication sequences, and network identity consistency [11]. The systematic nature of these attacks necessitates the derivation of behavior rules that can detect deviations from expected protocol behavior patterns defined in the standards. The behavior rules must address both obvious protocol violations and subtle anomalies that indicate sophisticated attack attempts.

4.1.1 UPPAAL Adversarial Behavior Representation

The formal verification framework models adversarial behavior through dedicated UPPAAL templates that systematically inject attack patterns into the protocol state space. Attackers are represented as non-deterministic processes with states for normal operation (IDLE), attack initialization (ATTACK_INIT), active execution (ATTACK_EXEC), and sustained malicious behavior (ATTACK_MAINTAIN).

Each attack vector is formalized as UPPAAL transitions with timing constraints, including authentication bypass through malformed AUTH REQUEST messages, identity harvesting via out-of-context IDENTITY REQUEST messages, service disruption through manipulated reject messages, and network spoofing via MCC/MNC parameter manipulation.

Advanced techniques incorporate precise temporal modeling, such as microsecond-level signal overshadowing timing, NAS sequence number progression disruption, and session state-aware attack execution based on UE RRC connection states.

This non-deterministic adversarial model enables comprehensive verification of behavior rules against diverse attack patterns while maintaining mathematical precision in representing real-world cellular attack capabilities.

4.2 3GPP Specification Analysis and Behavior Rule Derivation

The behavior rules were systematically derived through comprehensive analysis of 3GPP technical specifications, focusing on protocol security requirements and potential attack vectors. The derivation process involved three key phases: specification review, security requirement identification, and threat mapping.

First, we conducted a thorough review of key 3GPP specifications including TS 24.501 Release 18 (NAS protocol for 5G) [10], TS 33.501 Release 18 (Security Architecture) [11], TS 24.301 Release 18 (NAS protocol for EPS) [12], TS 33.401 Release 18 (EPS Security) [13], and TS 38.331 Release 17 (RRC protocol) [9][1]. LTE-specific procedures referenced in Table 1 utilize TS 36.331 [14] and TS 36.304 [15]. Each specification was analyzed to identify security-critical protocol behaviors and requirements that must be enforced to maintain cellular network security.

Second, we identified specific security requirements from these specifications that define expected protocol behavior under normal operating conditions. These requirements establish the baseline for legitimate network operation and provide the foundation for detecting anomalous behavior.

Third, we mapped these security requirements to potential attack vectors, creating a systematic threat-to-specification mapping.

[1] TS 38.331 Release 17 was used as RRC protocol changes in Release 18 do not affect the behavior rules.

4.2.1 Distinction Between Specification Requirements and Detection Thresholds

While the core security requirements and behavioral expectations are derived directly from 3GPP specifications, certain detection thresholds represent reasonable engineering choices based on empirical analysis of typical network behavior patterns. These researcher-defined thresholds are necessary because 3GPP specifications often define general requirements (e.g., ”shall not request permanent identity unnecessarily”) without specifying concrete numerical limits. The thresholds used in UE-Guard are chosen to balance security effectiveness with tolerance for legitimate network variations, retransmissions, and timing uncertainties.

- **Network Identity Spoofing** (BR1): Prevent MCC/MNC and TAC manipulation through SIB consistency validation
- **Connection State Attacks** (BR2, BR3): Maintain RRC state machine integrity through connection flood prevention and state transition validation
- **Service Disruption** (BR4, BR11): Detect malicious reject messages and attach flooding attacks
- **Protocol Sequence Bypass** (BR5): Enforce complete EMM procedure sequence to prevent authentication and security mode skipping
- **Security Mode Bypass** (BR6): Enforce proper encryption and integrity algorithms, preventing null cipher downgrade
- **Message Integrity Violations** (BR7, BR11): Prevent injection of unprotected NAS messages through MAC presence validation and reject message integrity
- **Protocol Synchronization Attacks** (BR8): Identify sequence number manipulation and replay attacks
- **Identity Harvesting** (BR9, BR10): Block unauthorized IMSI/IMEI collection through context validation and frequency control
- **Mobility Tracking** (BR12): Block unauthorized tracking area updates and location harvesting

Each behavior rule is systematically derived from 3GPP specifications through a rigorous specification-to-detection mapping process. The derivation methodology involves: (1) identifying security requirements from 3GPP TS 24.501 (NAS protocol), TS 33.501 (Security architecture), and TS 38.331 (RRC protocol); (2) extracting normative clauses that define mandatory protocol behaviors using keywords ”shall” and ”shall not”; (3) translating these protocol requirements into observable message patterns and timing constraints; and (4) defining detection criteria that identify deviations from specified behavior. Table 1 provides the specific 3GPP technical specifications and clauses that establish the core security requirements implemented by each behavior rule. Note that while the fundamental security principles (e.g., integrity protection, identity minimization) are directly derived from 3GPP specifications, specific detection thresholds and parameters may represent reasonable engineering choices based on empirical analysis, as detailed in the behavior rule descriptions.

Table 1: 3GPP Specification Alignment for Behavior Rules

Behavior Rule	**3GPP Spec**	**Section**	**Key Security Clause**
RRC Layer - Idle and Connection Establishment			
BR1	TS 38.331	§6.3.1	UE shall consider system information valid for cell where it was acquired
BR1	TS 36.304	§5.2.4	SIB changes trigger cell reselection evaluation
BR2	TS 38.331	§5.3.3	Network shall reject RRC connection requests only for valid reasons such as congestion
BR2	TS 36.331	§5.3.3.2	UE shall follow T300/T303 timer specifications for connection attempts
BR3	TS 38.331	§5.3.8	Network may release RRC connection at any time
BR3	TS 38.331	§5.6.8	While in RRC_CONNECTED state, UE shall not receive paging
BR3	TS 38.331	§5.3.7	Network shall reject RRC re-establishment requests only for valid reasons
NAS Layer - Initial Registration and Security (TS 24.501 / TS 24.301)			
BR4	TS 24.501	§5.5.1.2.2	If registration request rejected, UE shall start timer T3346 with random value
BR4	TS 24.301	§5.5.1.2.2	Attach reject handling starts backoff timer T3346 for EPS
BR4	TS 24.501	§8.2.7	Network may reject registration attempts that exceed reasonable limits
BR5	TS 24.501	§5.1	UE shall follow mandatory registration state machine progression
BR5	TS 24.501	§5.1.1	Authentication and security activation required before registration completes
BR5	TS 24.301	§5.1	UE shall follow EPS attach state machine progression
BR6	TS 33.501	§6.7	Network shall not select NULL encryption NEA0 or NULL integrity NIA0 except emergency
BR6	TS 24.501	§5.4.3	Security mode command shall be sent only after successful authentication
BR6	TS 33.501	§7.2	Single security mode command per session
BR6	TS 33.401	§7.2	EPS security mode shall not use EEA0/NIA0 outside emergency services
BR7	TS 24.501	§4.4.4	Receiver shall verify integrity of NAS messages when security header indicates protection
BR7	TS 24.501	§4.4.4.3	MAC-I presence mandatory when integrity protection active
BR8	TS 33.501	§6.4.3	NAS COUNT shall be incremented by one for each NAS message sent
BR8	TS 33.501	§6.5	Receiver shall discard NAS messages received out of sequence
NAS Layer - Post-Registration and Mobility (TS 24.501 / TS 24.301)			
BR9	TS 24.501	§5.4.4.3	Network shall initiate identity request only when UE identity cannot be derived
BR9	TS 24.301	§4.3.2.4	Identity request allowed only in specific EPS contexts
BR9	TS 24.501	§5.4.4.2	Identity requests restricted to authentication failure scenarios
BR10	TS 33.501	§6.1.3	Network shall minimize collection of subscriber identities
BR10	TS 33.401	§5.4.3	EPS identity protection requires minimal disclosure
BR10	TS 33.501	§6.1.3	Repeated identity requests indicate privacy violation
BR11	TS 24.501	§5.5.1.2.5	REGISTRATION REJECT with persistent causes shall be integrity protected
BR11	TS 24.301	§5.5.1.2.5	ATTACH REJECT with persistent causes shall be integrity protected
BR11	TS 24.501	§5.6.1.5	SERVICE REJECT messages shall be integrity protected when security active
BR11	TS 24.501	§8.2.7	Reject messages with persistent effects require integrity protection
BR12	TS 24.501	§5.5.3	UE shall perform mobility registration update only in registered state
BR12	TS 24.501	§5.5.3.2.2	Mobility registration update triggered by periodic timer expiry or network command
BR12	TS 24.301	§5.3.3	TAU shall occur only in EMM-REGISTERED state with valid triggers

4.3 Behavior Rule Specifications

UE-Guard implements a framework of twelve behavior rules (BR1-BR12) that operate as an integrated detection system aligned with the underlying RRC and NAS state progression (Figure 2 shows the normal path). The rules function collectively to provide comprehensive protocol monitoring, where each rule addresses specific state-dependent vulnerabilities while contributing to overall system integrity. This approach increases the likelihood that attacks violating multiple protocol layers or exploiting state transition boundaries trigger coordinated rule violations rather than being evaluated in isolation.

RRC Layer - Idle and Connection Establishment Phase:

- **BR1 (System Information Block Consistency)** [TS 38.331 §6.3.1, §5.2.2]: *State Context: RRC_IDLE during cell selection/reselection.* Validates consistency of broadcast System Information Blocks (SIB1, SIB2) to detect illegitimate base stations manipulating cell identity parameters (MCC, MNC, TAC). Positioned first as SIB decoding is the UE's initial interaction with the network before RRC connection establishment. Detects cell ID spoofing and rogue base station deployment by monitoring for SIB modifications without corresponding handover or reselection events specified in TS 36.304.

- **BR2 (RRC Connection Request Flood Prevention)** [TS 38.331 §5.3.3]: *State Context: RRC_IDLE → RRC_CONNECTED transition.* Monitors the frequency of RRC connection establishment attempts, releases, and rejections to detect resource exhaustion attacks. Placed at the RRC connection phase as this is the entry point to network access. Enforces rate limiting per TS 36.331 §5.3.3.2, preventing attackers from overwhelming eNodeB resources through rapid connection flooding that violates T300/T303 timer specifications.

- **BR3 (RRC State Transition Validation)** [TS 38.331 §5.3.8, §5.6.8]: *State Context: RRC_CONNECTED state management.* Enforces valid RRC state machine transitions between RRC_IDLE, RRC_CONNECTED, and RRC_INACTIVE states. Positioned after connection establishment to monitor ongoing connection integrity. Detects anomalous state manipulations including unexpected RRC Release messages, extended T302 reject timers, and illegitimate paging while in RRC_CONNECTED state—violations that indicate denial-of-service or lullaby attacks. This aligns with NR paging rules in TS 38.331 and LTE paging behavior in TS 36.331, where paging is not delivered while the UE remains in RRC_CONNECTED.

NAS Layer - Initial Registration and Authentication Phase:

- **BR4 (Attach/Registration Request Rate Limiting)** [TS 24.501 §5.5.1.2.2, TS 24.301 §5.5.1.2.2]: *State Context: EMM-DEREGISTERED / 5GMM-DEREGISTERED, initiating attach/registration.* Tracks attach/registration request frequency per GUTI/TMSI/SUCI to prevent flooding attacks. Positioned at NAS layer entry as attach/registration requests are the first NAS signaling messages sent after RRC connection. Enforces T3346-style backoff compliance for both EPS and 5GS contexts, detecting rapid attempts that exhaust core resources or trigger battery depletion.

- **BR5 (NAS Procedure Sequence Integrity)** [TS 24.501 §5.1, TS 24.301 §5.1]: *State Context: Full attach/registration state progression.* Validates the attach (EPS) and registration (5GS) procedure sequence from DEREGISTERED through authentication and security mode establishment to REGISTERED. Placed here to monitor the entire initial sequence. Detects security bypass attacks where attackers skip authentication or security mode command procedures, violating the mandatory ordering defined in TS 24.501 §5.1.1 and TS 24.301 §5.1.

- **BR6 (Security Mode Command Context Validation)** [TS 33.501 §6.7, TS 24.501 §5.4.3, TS 33.401 §7.2]: *State Context: EMM-DEREGISTERED, security activation procedure.* Validates Security Mode Command messages to prevent null encryption (EEA0/NEA0) and null integrity (EIA0/NIA0) algorithm selection outside emergency sessions. Positioned during security establishment phase to ensure cryptographic protection is activated before sensitive data transmission. Detects downgrade attacks and excessive security mode flooding that violates single-command-per-session constraints in TS 33.501 §7.2 and TS 33.401 §7.2 for EPS.

- **BR7 (NAS Message Authentication Code Presence)** [TS 24.501 §4.4.4]: *State Context: Post-security activation, all protected NAS messages.* Validates presence of Message Authentication Code (MAC-I) in NAS security headers when integrity protection is active. Positioned after security mode completion to enforce cryptographic protection requirements. Detects message injection attacks where adversaries send unprotected NAS messages (security header type 0x00) after security context establishment, violating mandatory MAC inclusion per TS 24.501 §4.4.4.3.

- **BR8 (NAS Sequence Number Monotonicity)** [TS 33.501 §6.4.3]: *State Context: Post-security activation, ongoing NAS signaling.* Validates monotonic progression of NAS sequence numbers (NAS COUNT/uplink sequence number) to maintain synchronization. Placed in active security context monitoring as sequence numbers are incremented with each protected message. Detects replay attacks and synchronization failures by flagging sequence number gaps ¿5, which violate the incremental progression required by TS 33.501 §6.5.

NAS Layer - Post-Registration and Mobility Management Phase:

- **BR9 (Identity Request Legitimacy Validation)** [TS 24.501 §5.4.4.3, TS 24.301 §4.3.2.4]: *State Context: EMM-REGISTERED / 5GMM-REGISTERED state, identity verification.* Validates that Identity Request messages (for IMSI, IMEI, IMEISV) occur only in legitimate contexts: authentication failure recovery, initial registration without GUTI/SUCI resolution, or network-initiated IMEI checks. Positioned post-registration to detect IMSI/IMEI catching attacks where rogue base stations request identities while UE is already authenticated and registered—a violation of TS 24.501 §5.4.4.2 and TS 24.301 §4.3.2.4 which restrict identity requests to specific failure scenarios.

- **BR10 (Identity Request Frequency Control)** [TS 33.501 §6.1.3, TS 33.401 §5.4.3]: *State Context: EMM-REGISTERED / 5GMM-REGISTERED state, identity harvesting prevention.* Monitors frequency of Identity Request messages per session to prevent excessive identity collection. Placed alongside BR9 to add rate-limiting to context validation. Detects identity harvesting attacks by enforcing maximum request limits ($\leq$2 requests per 60-second window), as legitimate procedures rarely require repeated identity disclosure per TS 33.501 and TS 33.401 privacy requirements.

- **BR11 (Rejection Message Integrity Validation)** [TS 24.501 §5.5.1.2.5, §5.6.1.5; TS 24.301 §5.5.1.2.5]: *State Context: EMM-DEREGISTERED ← EMM-REGISTERED / 5GMM-DEREGISTERED ← 5GMM-REGISTERED, rejection procedures.* Validates that Attach/Registration Reject, TAU Reject, and Service Reject messages with persistent cause codes include integrity protection when sent during active security contexts. For EPS, this covers Attach/TAU causes such as #3, #6, and #7; for 5GS, persistent Registration/Service reject causes likewise require protection. Positioned in rejection handling to detect false base station attacks that use unprotected rejection messages to force UE de-registration. Enforces the requirement that reject messages with persistent effects must be integrity-protected to prevent attacker manipulation in both EPS and 5GS contexts.

- **BR12 (TAU / Mobility Registration Update Context Validation)** [TS 24.501 §5.5.3, TS 24.301 §5.3.3]: *State Context: EMM-REGISTERED / 5GMM-REGISTERED state, mobility management.* Validates that Tracking Area Update (4G EPS) or Mobility Registration Update (5G) requests occur only in registered state and in response to legitimate triggers (e.g., periodic timer expiry, network command, or mobility event). Both procedures share common security requirements: they must be initiated only when UE is in registered state, must include valid triggering conditions per TS 24.301 §5.3.3 (4G TAU) and TS 24.501 §5.5.3 (5G mobility update), and must maintain proper security context. Positioned last in the state sequence as these mobility procedures represent steady-state operations. The UPPAAL formal verification validates the state-context and trigger logic using TAU as the representative mobility procedure; the 5G mobility registration update follows identical state-context principles (registered-state prerequisite and legitimate trigger validation per 3GPP specifications), making the verification approach applicable to both 4G and 5G mobility management.

The behavior rules operate as an interconnected detection system rather than independent checks. Rules are designed with deliberate dependencies: BR1-BR3 establish baseline RRC layer trust before NAS procedures begin; BR5's EMM state tracking provides context for BR6-BR8's security validation; BR9-BR10 combine contextual and frequency-based identity protection; BR11 leverages security context from BR6-BR8 to validate rejection integrity. This systemic design increases the likelihood that sophisticated attacks attempting to exploit protocol layer boundaries or state transition vulnerabilities trigger multiple coordinated rule violations, increasing detection confidence and reducing false negatives inherent in isolated rule evaluation.

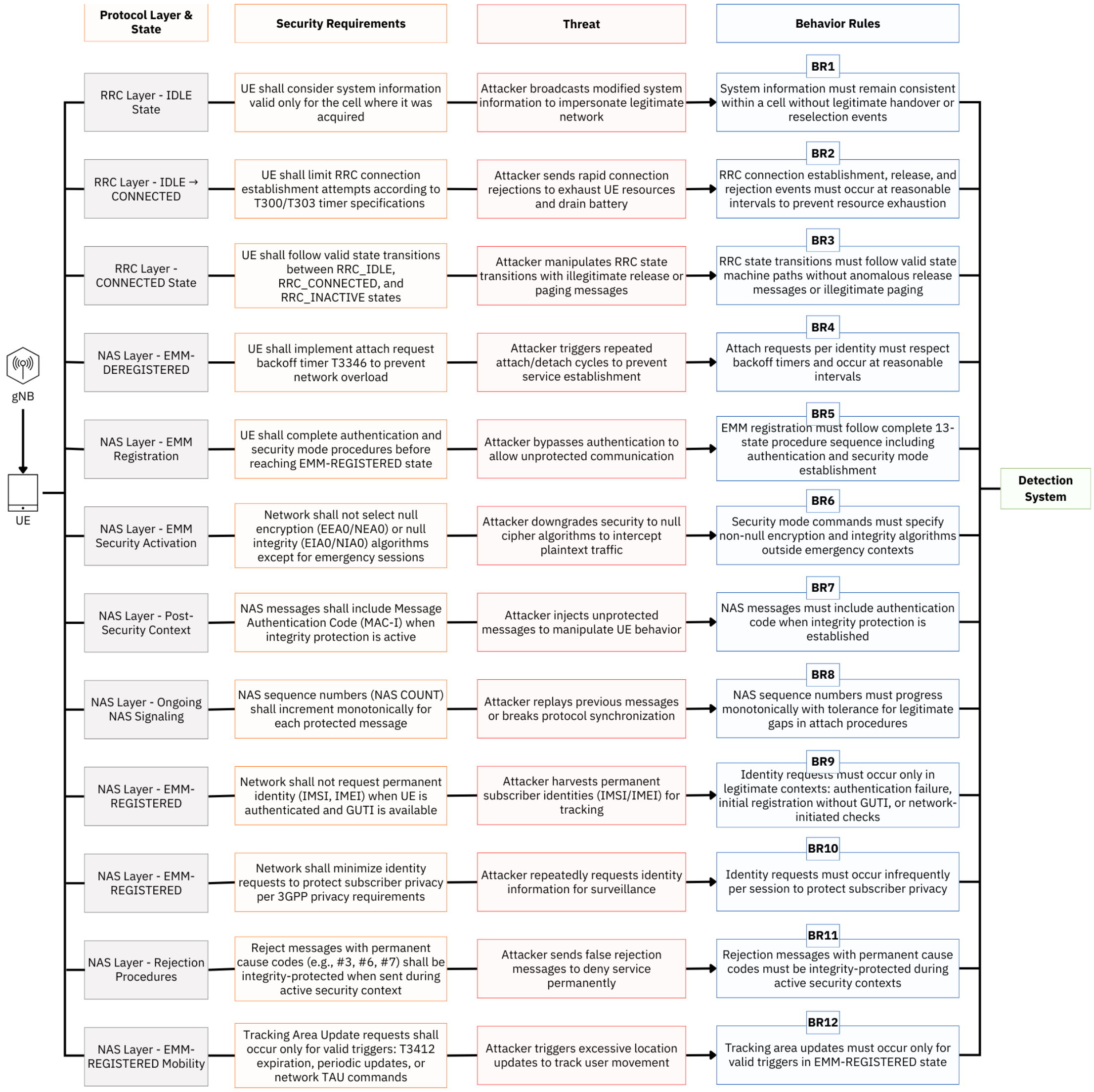
Figure 3 provides a visual overview of these behavior rules, organized by security requirements, associated threats, and specific detection criteria.

4.4 Formal Verification Framework

4.4.1 UPPAAL Model Implementation

This research employs UPPAAL model checking to provide formal-model assurances about the formal model's correctness and detection capabilities [5]. UPPAAL extends timed automata with real-valued clocks to model timing-sensitive systems, making it suitable for cellular protocol verification where temporal constraints are critical [4].

Each behavior rule is implemented as a validation function using simple conditional logic to check specific protocol compliance conditions on individual messages. The implementation focuses on per-message validation to detect specific attack patterns while maintaining compatibility with legitimate protocol operations. The verification framework implements the components consisting of:



Protocol Layer & State	Security Requirements	Threat	Behavior Rules
RRC Layer - IDLE State	UE shall consider system information valid only for the cell where it was acquired	Attacker broadcasts modified system information to impersonate legitimate network	BR1 System information must remain consistent within a cell without legitimate handover or reselection events
RRC Layer - IDLE → CONNECTED	UE shall limit RRC connection establishment attempts according to T300/T303 timer specifications	Attacker sends rapid connection rejections to exhaust UE resources and drain battery	BR2 RRC connection establishment, release, and rejection events must occur at reasonable intervals to prevent resource exhaustion
RRC Layer - CONNECTED State	UE shall follow valid state transitions between RRC_IDLE, RRC_CONNECTED, and RRC_INACTIVE states	Attacker manipulates RRC state transitions with illegitimate release or paging messages	BR3 RRC state transitions must follow valid state machine paths without anomalous release messages or illegitimate paging
NAS Layer - EMM-DEREGISTERED	UE shall implement attach request backoff timer T3346 to prevent network overload	Attacker triggers repeated attach/detach cycles to prevent service establishment	BR4 Attach requests per identity must respect backoff timers and occur at reasonable intervals
NAS Layer - EMM Registration	UE shall complete authentication and security mode procedures before reaching EMM-REGISTERED state	Attacker bypasses authentication to allow unprotected communication	BR5 EMM registration must follow complete 13-state procedure sequence including authentication and security mode establishment
NAS Layer - EMM Security Activation	Network shall not select null encryption (EEA0/NEA0) or null integrity (EIA0/NIA0) algorithms except for emergency sessions	Attacker downgrades security to null cipher algorithms to intercept plaintext traffic	BR6 Security mode commands must specify non-null encryption and integrity algorithms outside emergency contexts
NAS Layer - Post-Security Context	NAS messages shall include Message Authentication Code (MAC-I) when integrity protection is active	Attacker injects unprotected messages to manipulate UE behavior	BR7 NAS messages must include authentication code when integrity protection is established
NAS Layer - Ongoing NAS Signaling	NAS sequence numbers (NAS COUNT) shall increment monotonically for each protected message	Attacker replays previous messages or breaks protocol synchronization	BR8 NAS sequence numbers must progress monotonically with tolerance for legitimate gaps in attach procedures
NAS Layer - EMM-REGISTERED	Network shall not request permanent identity (IMSI, IMEI) when UE is authenticated and GUTI is available	Attacker harvests permanent subscriber identities (IMSI/IMEI) for tracking	BR9 Identity requests must occur only in legitimate contexts: authentication failure, initial registration without GUTI, or network-initiated checks
NAS Layer - EMM-REGISTERED	Network shall minimize identity requests to protect subscriber privacy per 3GPP privacy requirements	Attacker repeatedly requests identity information for surveillance	BR10 Identity requests must occur infrequently per session to protect subscriber privacy
NAS Layer - Rejection Procedures	Reject messages with permanent cause codes (e.g., #3, #6, #7) shall be integrity-protected when sent during active security context	Attacker sends false rejection messages to deny service permanently	BR11 Rejection messages with permanent cause codes must be integrity-protected during active security contexts
NAS Layer - EMM-REGISTERED Mobility	Tracking Area Update requests shall occur only for valid triggers: T3412 expiration, periodic updates, or network TAU commands	Attacker triggers excessive location updates to track user movement	BR12 Tracking area updates must occur only for valid triggers in EMM-REGISTERED state

Figure 3: Twelve Behavior Rules (BR1-BR12) with Security Requirements, Threat Descriptions, and Detection Criteria for UE-Guard Cellular Attack Detection Framework

Detection_Agent: This component monitors UE protocol messages against behavior rules BR1-BR12, maintaining security contexts, message sequences, and timing constraints. Figure 4 shows the UPPAAL template that detects when an abnormal state is reached by violating the defined behavior rules.

The Detection_Agent implements each behavior rule as a validation function using conditional logic to check protocol compliance conditions. Each rule monitors specific aspects of 3GPP protocol behavior, transitioning to violation states when security requirements are breached.

The Attack State Indicator (ASI) uses a bitwise system to track violations, where each behavior rule maps to a specific bit (BR1: bit 0 through BR12: bit 11). Violations are aggregated using bitwise OR operations and communicated to the Checker component.

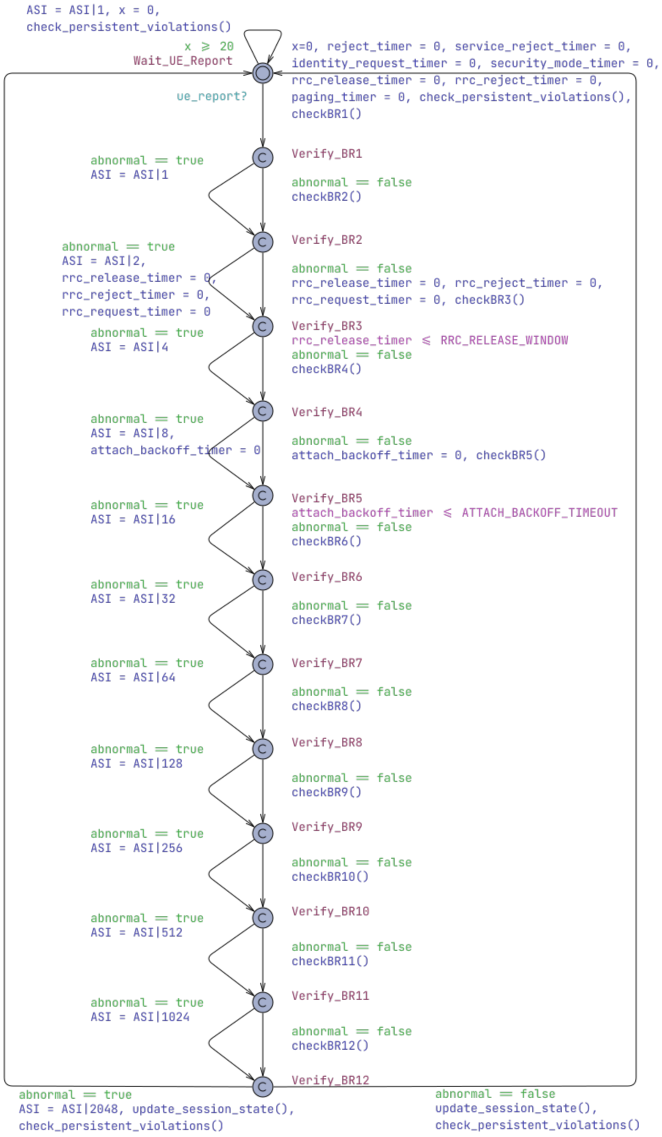


Figure 4: Detection_Agent template in UPPAAL showing the monitoring engine that checks for abnormal states by applying behavior rules BR1-BR12 and using the Attack State Indicator (ASI) to track violations.

Checker: The Checker component validates the Detection_Agent's detection decisions against mathematical specifications. The Checker operates in two distinct states that determine verification outcomes:

- **No_Error State**: Indicates successful detection where the Checker reaches this state when the Detection_Agent correctly identifies and flags attack patterns, confirming that the behavior rule violations are properly detected

- **Error State**: Represents verification scenarios where either legitimate protocol behavior is incorrectly flagged as malicious (false positive) or actual attacks are missed (false negative)

Using Timed Computation Tree Logic (TCTL) formulas, the Checker verifies critical properties including deadlock freedom, attack pattern reachability, and timing constraints. Each behavior rule is associated with specific TCTL queries that support verification of the rule's correctness, as demonstrated in Figure 5.

The verification queries are designed to ensure extensive coverage:

- **Reachability Queries (`E<> checkerN.No_error`)**: Verify that there exists at least one execution path where each behavior rule checker reaches the No_error state, confirming that attack patterns are detectable

- **Safety Queries (`A[] not deadlock`)**: Verify that the formal model does not contain deadlock states, ensuring the detection system can operate continuously

- **Invariant Queries**: Validate that specific conditions (such as timing constraints and counter thresholds) are maintained throughout all possible executions

These query formulations are appropriate because they directly test the formal properties required for reliable cellular attack detection: attack pattern detectability, system stability, and temporal correctness.

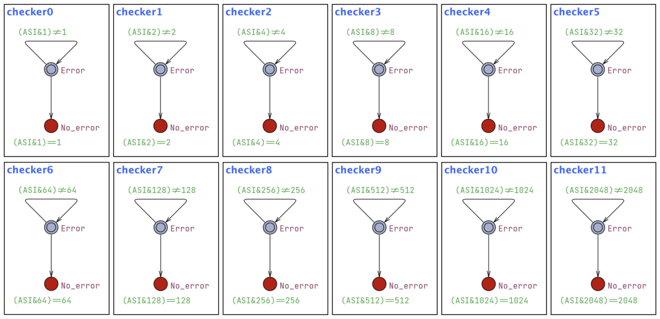


Figure 5: Checker template in UPPAAL demonstrating formal verification of temporal logic properties for attack detection correctness.

5 Experiments

5.1 Experimental Setup

Execution platform: All performance measurements reported in the abstract and Section 5 were obtained from the Python prototype implementation running on macOS with Apple Silicon and 16GB RAM. Timing used `time.perf_counter()` and memory profiling used `memory_profiler`.

5.1.1 Dataset Processing and Pipeline

The framework was evaluated using 51 cellular signaling datasets captured from real network environments. The dataset comprises attack datasets (44 files) generated by the authors and supplemented with scenarios from Karim et al.'s public repository [17], along with normal traffic baselines (7 files) generated and collected by the authors using standard cellular protocol capture methodologies.

Raw cellular signaling data was captured in PCAP format and processed through a multi-stage pipeline to extract RRC and NAS protocol messages for analysis. The processing pipeline consists of three main stages: packet extraction, protocol parsing, and structured formatting.

First, PCAP files were processed using tshark to generate PDML XML format, which provides detailed protocol dissection of LTE/5G signaling messages. The PDML XML was then filtered to retain only relevant cellular protocols, removing extraneous network traffic and focusing on RRC and NAS message content.

Second, the filtered XML files were parsed to extract essential protocol fields using a specialized preprocessor that handles both LTE and 5G message formats. The preprocessor extracts critical signaling information including basic packet metadata (timestamp, message index, packet type, direction), network identity parameters (MCC/MNC values from GUMMEI, TAI, and RRC contexts), protocol discriminators, RRC message types (UL/DL CCCH/DCCH messages), and comprehensive NAS fields (EMM/ESM message types, security headers, sequence numbers, authentication codes, identity information, cause codes, and TMSI values). These extracted fields form a structured dataset with 43 protocol-specific attributes essential for behavior rule evaluation.

Third, the extracted data was converted to CSV format with standardized field naming and data types suitable for automated analysis. This structured format enables efficient processing by the UE-Guard detection system while preserving all essential protocol information for comprehensive attack pattern analysis.

Table 2 provides a comprehensive overview of the processed datasets used in the experiments, including packet counts and attack distributions after PCAP to CSV conversion.

5.1.2 Performance Measurement Setup

Performance metrics were collected using a Python-based prototype implementation of the behavior rule validation logic on a macOS system with Apple Silicon processor and 16GB RAM. Timing measurements used Python's `time.perf_counter()` with microsecond precision across all processed messages. Memory profiling employed the `memory_profiler` library to track peak memory consumption during dataset processing. These measurements establish feasibility baselines for mobile deployment, though actual mobile device performance will be evaluated in future work (Section 8).

5.2 Packet-Weighted Detection Results

The experimental evaluation demonstrates UE-Guard's detection performance through coordinated rule violations. Packet-weighted detection reaches 97.57% (16,179 of 16,582 attack packets), preserving the operational goal of detecting attack campaigns while reflecting their packet volume. Table 3 summarizes the packet-weighted detection effectiveness.

Table 2: Dataset Summary: 51 Datasets Evaluated Across Attack Categories and Normal Baseline Traffic

Dataset Category	**Files**	**Total Packets**
Attack Datasets (44 files)		
Identity Catching	2	311
Encryption/Security	9	1,586
Service Rejection	7	1,801
Network Downgrade	5	1,648
Resource Depletion	3	4,225
State Manipulation	9	2,442
Location/Tracking	4	3,249
Protocol Failures	5	1,320
Attack Subtotal	**44**	**16,582**
Normal Traffic Datasets (7 files)		
Normal Baseline (normal_data 1-7)	7	514
Normal Subtotal	**7**	**514**
Grand Total	**51**	**17,096**

Table 3: Packet-Weighted Detection Effectiveness with Attack Distribution

Attack Category	**Files**	**Total Packets**	**Packet-Weighted Detection**
Identity Catching	2	311	91.6% (285/311)
Encryption/Security	9	1,586	86.3% (1,368/1,586)
Service Rejection	7	1,801	100.0% (1,801/1,801)
Network Downgrade	5	1,648	100.0% (1,648/1,648)
Resource Depletion	3	4,225	100.0% (4,225/4,225)
State Manipulation	9	2,442	100.0% (2,442/2,442)
Location/Tracking	4	3,249	95.1% (3,090/3,249)
Protocol Failures	5	1,320	100.0% (1,320/1,320)
Attack Subtotal	**44**	**16,582**	**97.57% (16,179/16,582)**
Normal Baseline	**7**	**514**	**100.0% specificity (0/514)**
Total Datasets	**51**	**17,096**	—

5.3 Performance Characteristics of Specification-Based Detection

5.3.1 Detection Effectiveness

The experimental evaluation validates the effectiveness of the specification-based approach across comprehensive attack scenarios:

- **Attack Detection**: The behavior rules detected protocol violations across 16,179 of 16,582 attack messages (97.57%)

- **Normal Traffic Validation**: The framework correctly processed all 514 baseline normal cellular signaling packets without false alarms (100% specificity), ensuring legitimate network operations remain unaffected

- **Deterministic Decisions**: The framework provides binary decision outcomes (compliant/non-compliant) based on explicit 3GPP specification requirements, eliminating uncertainty inherent in probabilistic classification models

5.3.2 Computational Performance

Table 4 summarizes the key performance metrics measured during evaluation of UE-Guard.

Table 4: UE-Guard Framework Performance Characteristics

Performance Metric	Detection Latency	Memory Usage	CPU Utilization	Throughput
UE-Guard Framework	9.7 ms	22.9 MB	39.6%	103.0 msg/sec

5.3.3 Deployment Advantages for Mobile Environments

The specification-based approach addresses key limitations of machine learning methods for mobile cellular security:

Explainable Detection: Unlike black-box AI models, each detection is directly traceable to specific violations of 3GPP specifications, enabling forensic analysis and regulatory compliance.

Real-Time Processing: The framework processes 103.0 messages per second with 9.7ms average latency per message, demonstrating computational feasibility for real-time UE deployment. The rule-based approach ensures consistent execution with bounded computational complexity.

Resource Efficiency: With a 22.9 MB peak memory footprint and 39.6% average CPU utilization measured on the evaluation platform, the framework demonstrates reasonable resource consumption. The absence of computationally intensive operations such as matrix multiplications or neural network inference suggests lower power consumption compared to neural network approaches.

Immediate Deployment: The approach requires no training phase, enabling deployment using established 3GPP protocol knowledge without extensive data collection cycles.

These characteristics suggest specification-based detection as a feasible approach for cellular attack detection, offering deterministic and transparent security decisions while warranting further evaluation on actual mobile hardware.

6 Verification Results

6.1 UPPAAL Formal Verification Methodology

The behavior rules underwent rigorous formal verification using UPPAAL 4.1.26, a model checker based on timed automata theory [5]. The verification framework models the UE-Guard detection system as a network of timed automata, consisting of a Detection_Agent that implements all twelve behavior rules and Checker components that validate detection correctness against formal specifications.

The verification employs Timed Computation Tree Logic (TCTL) formulas to establish three critical properties: completeness (BR1-BR12 protocol violation patterns are detectable), correctness (detection logic correctly sets violation indicators when threshold conditions are met), and temporal compliance (3GPP timing requirements are satisfied). The model uses a 16-bit Attack State Indicator (ASI) with bitwise operations to track violations across all behavior rules simultaneously, enabling verification of both individual and combined detection capabilities.

6.2 UPPAAL Query Verification Results

All 20 temporal logic properties were successfully verified, confirming the correctness of the formal model's detection logic. Table 5 provides a categorical summary of verification results, while Table 6 details individual query outcomes. The verification encompasses five dimensions: system safety (1 query), individual behavior rule completeness (12 queries), combined detection capability (1 query), detection logic soundness (5 queries), and 3GPP temporal compliance (1 query).

Table 5: UPPAAL Formal Verification Summary (20/20 Queries Verified)

Verification Category	**Queries**	**Verified**	**Result**
System Safety	1	1	✓Success
Completeness (Individual BR)	12	12	✓All Success
Completeness (Combined)	1	1	✓Success
Correctness (Logic Soundness)	5	5	✓All Success
Temporal (3GPP Compliance)	1	1	✓Success
Total	**20**	**20**	**100% Success**

Table 6: UPPAAL Query Verification Results (20/20 Successful)

Property	**Type**	**Query**	**Result**
System Deadlock Freedom	Safety	`A[] not deadlock`	Success
Completeness Verification - Individual BR Detection			
BR1: SIB Consistency	Reachability	`E<> checker0.No_error`	Success
BR2: RRC Request Flooding	Reachability	`E<> checker1.No_error`	Success
BR3: RRC State Transitions	Reachability	`E<> checker2.No_error`	Success
BR4: Attach Request Flooding	Reachability	`E<> checker3.No_error`	Success
BR5: EMM Sequence Integrity	Reachability	`E<> checker4.No_error`	Success
BR6: Security Mode Command	Reachability	`E<> checker5.No_error`	Success
BR7: NAS MAC Presence	Reachability	`E<> checker6.No_error`	Success
BR8: NAS Sequence Monotonicity	Reachability	`E<> checker7.No_error`	Success
BR9: Identity Request Context	Reachability	`E<> checker8.No_error`	Success
BR10: Identity Request Frequency	Reachability	`E<> checker9.No_error`	Success
BR11: Reject Message Integrity	Reachability	`E<> checker10.No_error`	Success
BR12: TAU / Mobility Registration Update Context	Reachability	`E<> checker11.No_error`	Success
Combined BR Detection	Reachability	`E<> (checker0.No_error && ... && checker11.No_error)`	Success
Correctness Verification - Detection Logic Soundness			
BR2: RRC Request Flooding	Invariant	`A[] (rrc_request_count > MAX_RRC_REQUEST imply (ASI&2)==2)`	Success
BR3: Paging in CONNECTED	Invariant	`A[] (paging_count > MAX_PAGING imply (ASI&4)==4)`	Success
BR10: Identity Request Frequency	Invariant	`A[] (identity_request_count > MAX_IDENTITY_REQUESTS imply (ASI&512)==512)`	Success
BR11: Reject Message Flooding	Invariant	`A[] (reject_count >= RAPID_REJECT_THRESHOLD imply (ASI&1024)==1024)`	Success
BR12: TAU During Attach	Invariant	`A[] ((attach_in_progress && msg_type == TAU_REQUEST) imply (ASI&2048)==2048)`	Success
Temporal Verification - 3GPP Timing Compliance			
BR5: Attach Backoff Timer	Invariant	`A[] (da.Verify_BR5 imply attach_backoff_timer <= 3240)`	Success

The verification results establish three scoped assurances for the formal model of the UE-Guard detection framework:

Completeness Assurance: Thirteen reachability queries (`E<>`) confirm that violations of each behavior rule (BR1-BR12) are individually detectable, and the combined query verifies that all rules can detect violations simultaneously. This ensures that the framework provides coverage across the specified BR1-BR12 protocol violation patterns within the formal model.

Correctness Assurance: Five invariant queries (`A[]`) with implication properties establish that the detection logic in the formal model is sound—whenever threshold conditions are met (e.g., `rrc_request_count` > MAX_RRC_REQUEST for BR2, `paging_count` > MAX_PAGING for BR3, `identity_request_count` > MAX_IDENTITY_REQUESTS for BR10, `reject_count` ≥ RAPID_REJECT_THRESHOLD for BR11), the corresponding Attack State Indicator (ASI) bit is correctly set in all verified execution paths.

Temporal Compliance Assurance: One timing query validates temporal properties of the formal model. The BR5 query (`A[] (da.Verify_BR5 imply attach_backoff_timer <= 3240)`) verifies that the attach backoff timer remains bounded by 3240 seconds, aligned with 3GPP TS 24.501 T3346 specifications. This timing constraint ensures the formal model respects protocol-defined temporal limits, while BR5's detection logic identifies rapid consecutive attach attempts that violate backoff requirements.

The successful verification of all properties provides formal-model assurances about correctness for the verified queries and confirms that the behavior rule models can identify the implemented attack patterns without introducing system deadlocks or timing violations within the modeled scope. The deadlock freedom property (`A[] not deadlock`) guarantees continuous monitoring capability in the formal model, ensuring the detection system remains responsive throughout all possible execution paths modeled in UPPAAL.

Verification Metadata: All verifications were performed using UPPAAL 4.1.26 on the formal model of the detection framework. The complete UPPAAL model file (`spec_verification.xml`) with embedded verification results is available as supplementary material, enabling independent verification by reviewers and researchers. The model includes 1197 lines of formal specifications, complete implementations of all twelve behavior rules, and all 20 verification queries confirming successful verification. Future work will verify correspondence between the formal model and actual implementation code through code-to-model tracing.

7 Discussion

The formal verification results validate the correctness of the UE-Guard formal model. All 20 temporal logic properties were successfully verified, confirming that the twelve behavior rules can reliably detect target attack patterns within the modeled scope without introducing system deadlocks or timing violations.

The framework focuses on NAS and RRC protocol violations, providing detection capabilities for attacks that violate 3GPP specifications. However, it may not detect sophisticated attacks that operate within protocol specifications through anomalous but legitimate message sequences. The timing constraints verified through UPPAAL provide sufficient windows for legitimate protocol operations while detecting malicious deviations in the formal model.

Applicability to 5G-Advanced and Beyond-5G Networks: The specification-based approach extends naturally to 5G Standalone (SA) architectures and evolving 6G networks. The behavior rule derivation methodology can be applied to emerging 5G security procedures defined in TS 33.501, including Subscription Permanent Identifier (SUPI) concealment verification (§6.12) and 5G Authentication and Key Agreement (5G-AKA) protocol monitoring (§6.1). The framework's formal verification approach remains applicable as 3GPP continues to standardize security mechanisms for network slicing and service-based architectures. Future beyond-5G networks may benefit from hybrid approaches that combine specification-based rules with complementary detection mechanisms while maintaining the deterministic guarantees and explainability that formal verification provides.

8 Conclusion

This paper presented a specification-based cellular attack detection framework that monitors UE behavior against 3GPP protocol specifications. The framework comprises twelve formally verified behavior rules that systematically map security requirements to specific threats and detection criteria, providing a structured approach to protocol compliance monitoring. The formal verification using UPPAAL model checker provides formal-model assurances of detection correctness, with all 20 temporal logic properties successfully verified across three verification dimensions (completeness, correctness, and temporal compliance), confirming deadlock-free operation and reliable detection of implemented attack patterns.

The next phase involves integrating the specification-based detection framework on the mobile device platform already developed by the researchers. This integration will leverage existing diagnostic interfaces such as Qualcomm's QXDM or equivalent protocol monitoring capabilities available on modern smartphones to capture RRC and NAS messages in real-time. The integrated system will evaluate battery consumption characteristics through continuous protocol monitoring, assess integration challenges with existing UE protocol stacks, and measure detection latency on resource-constrained mobile hardware. Furthermore, comprehensive comparative analysis will run the AI-based intrusion detection system alongside the specification-based framework, providing detailed performance comparisons evaluating detection accuracy, computational efficiency, memory usage, energy consumption, and real-time processing capabilities under identical experimental conditions.

Future work should expand the behavior rule set to address emerging attack vectors in 5G-Advanced and 6G networks, while cross-layer correlation between physical layer measurements and protocol behavior could enhance detection accuracy. The specification-based approach offers deterministic detection with explainable results [23], establishing a foundation for UE-side cellular attack detection that complements existing network-centric security mechanisms [2].

Acknowledgments

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No. RS-2024-00437252, Development of anti-sniffing technology for mobile communication and AirGap environments).

References

[1] Wani, M.S., Rademacher, M., Horstmann, T., Kretschmer, M.: Security vulnerabilities in 5G non-stand-alone networks: A systematic analysis and attack taxonomy. Journal of Cybersecurity and Privacy 4(1), 23–40 (2024).

[2] Y. Park *et al.*, "SMDFbs: Specification-Based Misbehavior Detection for False Base Stations," *Sensors*, vol. 23, no. 23, 9504, 2023.

[3] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE," in *Proc. Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, USA, February 2018.

[4] R. Alur and D. L. Dill, "A theory of timed automata," *Theoretical Computer Science*, vol. 126, no. 2, pp. 183–235, 1994.

[5] K. G. Larsen, P. Pettersson, and W. Yi, "UPPAAL in a nutshell," *International Journal on Software Tools for Technology Transfer*, vol. 1, no. 1-2, pp. 134–152, 1997.

[6] L. Aceto, A. Burgueño, and K. G. Larsen, "The quest for compositionality: Reflections on twenty years of research on timed automata," *Information and Computation*, vol. 264, pp. 101–117, 2018.

[7] D. Basin, S. Modersheim, and L. Viganò, "OFMC: A symbolic model checker for security protocols," *International Journal of Information Security*, vol. 4, no. 3, pp. 181–208, 2005.

[8] M. A. Rahman *et al.*, "A Formal Verification of a Reputation Multi-Factor Authentication Mechanism for Constrained Devices and Low-Power Wide-Area Network Using Temporal Logic," *Electronics*, vol. 12, no. 16, 2023.

[9] 3GPP, "Radio Resource Control (RRC) Protocol Specification," 3GPP TS 38.331, Release 17, 2022.

[10] 3GPP, "Non-Access-Stratum (NAS) protocol for 5G System (5GS)," 3GPP TS 24.501, Release 18, v18.4.0, September 2024.

[11] 3GPP, "Security Architecture and Procedures for 5G System," 3GPP TS 33.501, Release 18, v18.4.0, 2024.

[12] 3GPP, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)," 3GPP TS 24.301, Release 18, v18.4.0, 2024.

[13] 3GPP, "Security Architecture for Evolved Packet System (EPS)," 3GPP TS 33.401, Release 18, v18.3.0, 2024.

[14] 3GPP, "Radio Resource Control (RRC) Protocol Specification (LTE)," 3GPP TS 36.331, Release 18, 2024.

[15] 3GPP, "User Equipment (UE) Procedures in Idle Mode (LTE)," 3GPP TS 36.304, Release 18, 2024.

[16] I. Karim *et al.*, "Gotta Detect 'Em All: Fake Base Station and Multi-Step Attack Detection in Cellular Networks," *arXiv preprint arXiv:2401.04958*, 2024.

[17] I. Karim *et al.*, "Dataset for Gotta Detect 'Em All: Fake Base Station and Multi-Step Attack Detection in Cellular Networks," Zenodo, DOI: 10.5281/zenodo.15337578, 2024.

[18] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," in *Proc. Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, USA, February 2016.

[19] N. Golde *et al.*, "Let Me Answer That for You: Exploiting Broadcast Information in Cellular Networks," in *Proc. 22nd USENIX Security Symposium*, 2013, pp. 33–48.

[20] D. Rupprecht *et al.*, "AdaptOver: Adaptive Overshadowing Attacks in Cellular Networks," in *Proc. ACM Conference on Computer and Communications Security*, 2022, pp. 2845–2859.

[21] A. David *et al.*, "UPPAAL SMC tutorial," *International Journal on Software Tools for Technology Transfer*, vol. 17, no. 4, pp. 397–415, 2015.

[22] G. Behrmann, A. David, and K. G. Larsen, "A tutorial on UPPAAL," in *Proc. 4th International School on Formal Methods for the Design of Computer, Communication and Software Systems*, 2004.

[23] R. Mitchell and R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 16–30, 2014.