Revista Brasileira de Computação Aplicada, November, 2025

DOI: 10.5335/rbca.v17i3.16506
Vol. 17, Nº 3, pp. 52–63
Homepage: seer.upf.br/index.php/rbca/index

ORIGINAL PAPER

A Coloured Petri Nets Model of the 5G Authentication and Key Agreement Protocol

José Sávio Gama Macêdo[1], Antônio Carlos de Oliveira Bezerra[1], Álvaro Sobrinho[1], Leandro Dias da Silva[2], Dalton C. G. Valadares[3], Danilo F. S. Santos[4], Angelo Perkusich[4]

[1]Federal University of the Agreste of Pernambuco, Garanhuns, Pernambuco, Brazil, [2]Federal University of Alagoas, Maceió, Alagoas, Brazil, [3]Federal Institute of Pernambuco, Caruaru, Pernambuco, Brazil, [4]Federal University of Campina Grande Campina Grande, Paraíba, Brazil

*savio.gama09@gmail.com; antonio.carlosb@ufape.edu.br; alvaro.alvares@ufape.edu.br; leandrodias@ic.ufal.br; dalton.valadares@caruaru.ifpe.edu.br; danilo.santos@virtus.ufcg.edu.br; perkusic@virtus.ufcg.edu.br

Received: 2024-11-23. **Revised:** 2025-10-25. **Accepted:** 2025-11-26.

Abstract

Background: The security in 5G networks must safeguard network functions and other components responsible for end-to-end communications, intending to provide confidentiality, integrity, availability, authenticity, and non-repudiation. Some security functions that protect 5G networks are built into relevant protocols, such as the 5G Authentication and Key Agreement (5G-AKA). However, the 5G-AKA protocol has some limitations, becoming susceptible to attacks such as replay and man-in-the-middle. **Results:** Aiming to analyze the 5G-AKA protocol regarding security properties and help to identify possible vulnerabilities and threats, we used coloured Petri nets to model the protocol's components, their interactions, and an example of an attack scenario. We validated the model using simulations and model-checking. **Conclusions:** This model may help improve the security of 5G networks by validating properties and behaviors using simulations and formal verification. The proposed 5G-AKA model can be a relevant tool for identifying vulnerabilities and proposing mitigation measures for different 5G topologies.

Keywords: 5G-AKA; formal modeling, security, formal verification.

Resumo

Background: A segurança nas redes 5G deve proteger as funções de rede e outros componentes responsáveis pelas comunicações ponta a ponta, visando garantir confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio. Algumas funções de segurança que protegem as redes 5G fazem parte de protocolos relevantes, como o 5G *Authentication and Key Agreement* (5G-AKA). No entanto, o protocolo 5G-AKA apresenta algumas limitações, tornando-se suscetível a ataques, como os de repetição e *man-in-the-middle*. **Resultados:** Com o objetivo de analisar o protocolo 5G-AKA em relação às propriedades de segurança e ajudar a identificar possíveis vulnerabilidades e ameaças, redes de Petri coloridas foram usadas para modelar os componentes do protocolo, suas interações e um exemplo de cenário de ataque. O model foi validado por meio de simulações e a técnica de verificação automática de modelos. **Conclusões:** O modelo pode contribuir para melhorar a segurança das redes 5G ao validar propriedades e comportamentos por meio de simulações e verificação formal. O modelo proposto do 5G-AKA pode ser uma ferramenta relevante para identificar vulnerabilidades e propor medidas de mitigação em diferentes topologias de 5G.

Palavras-Chave: 5G-AKA; modelagem formal; segurança; verificação formal.

1 Introduction

5G is the latest generation of mobile communication technology that aims to improve, for example, the wireless network's coverage, with the potential to revolutionize vertical applications (Wen et al., 2022). 5G networks provide high data transfer speeds, low latency, low power consumption, increased system capacity, and enable connectivity with a massive number of devices. However, new challenges exist, as with any new technology (e.g., security (Li et al., 2021)). One primary concern regarding 5G networks is the increase in attack surfaces, given that many components are software now, with the introduction of technologies such as network slicing, software-defined networks, and network function virtualization (Khan et al., 2020; Valadares et al., 2023).

In this sense, some components and protocols must incorporate security mechanisms and techniques to ensure communications remain secure and to protect the information and the assets involved. The 5G Authentication and Key Agreement (5G-AKA) is an example of a protocol to ensure security in 5G networks (Edris et al., 2020). This protocol provides authentication and establishes security keys between User Equipments (UEs) and the 5G network infrastructure. Proper authentication is essential to guarantee the confidentiality and integrity of communications and prevent attacks.

However, the 5G-AKA protocol is vulnerable to attacks such as replay, spoofing, and Man-in-the-Middle (MITM) (Basin et al., 2018; Sobrinho et al., 2024). One way to address such threats, aiming to mitigate or avoid them, is to apply formal methods to verify behavior and security properties. Formal methods provide a systematic, mathematically rigorous approach to analyzing and validating security methods and techniques, helping detect security flaws, identify potential vulnerabilities, and ensure that specified policies are correctly implemented, thereby contributing to the reliability and robustness of security systems. Furthermore, applying formal methods enables accurate and detailed verification of expected behaviors in a system, process, or protocol, providing a solid basis for compliance assessments and security audits.

In this regard, Coloured Petri Nets (CPN) can be a relevant solution to modeling and formal verification of security solutions such as the 5G-AKA protocol (Jensen and Kristensen, 2015a; Valadares et al., 2021). CPN is a graphical formal modeling language extensively used for validating complex and concurrent systems (Fernandes Costa et al., 2022). This formal modeling language can help analyze the protocol's behavior and identify vulnerabilities.

Therefore, in this paper, we propose a CPN model to formally analyze the 5G-AKA protocol. We modeled and validated the protocol using simulations and formal verification with the CPN Tools[1]. The formal verification considered the ASK-CTL library (Cheng et al., 1997), which implements a Computation Tree Logics (CTL)-like logic. The ASK-CTL enabled an exhaustive search of the state space of the 5G-AKA model to verify the validity of temporal logic formulas that represent the desired requirements. Based on our proposed model, formal verification can also help identify vulnerabilities in 5G network deployments based on the 5G-AKA protocol.

The main contributions of this paper are listed below:

- We present and describe a CPN model of the 5G-AKA protocol, considering its main components and their communication flow;
- We present the Message Sequence Charts generated when executing simulations with the CPN model, verifying that the communication flow represents well the 5G-AKA protocol;
- We present an evaluation of the model with a formal verification (model checking), considering some desired properties of the protocol.

The remaining sections are organized as follows. Section 2 describes a background on the main concepts of CPN. Section 3 discusses related works and limitations. Section 4 presents the proposed CPN model. Section 5 presents the model simulation results, while Section 6 presents the formal verification using ASK-CTL. Section 7 discusses an example of attack scenario. Section 8 concludes the papers and discusses future works.

2 Background

CPN is a high-level Petri net that combines the theory of Petri nets with the resources of a functional programming language, namely, CPN ML (Jensen and Kristensen, 2009). The CPN ML language is an extension of Standard ML (SML) designed to make Petri net modeling more intuitive, enabling users to create more sophisticated and complex Petri net models. A *coloured Petri net module* is a tuple $CPN_M = (P, T, A, \Sigma, V, C, G, E, I, T_{sub}, P_{port}, PT)$ (Jensen, 1981; Jensen and Kristensen, 2015b):

i. P is a finite set of places.
ii. T is a finite set of transitions such that $P \cap T = \theta$.
iii. $A \subseteq P \times T \cup T \times P$ is a set of directed arcs.
iv. Σ is a finite non-empty set of colors.
v. V is a finite set of typed variables such that $Type[v] \in \Sigma$ for all variables $v \in V$.
vi. $C : P \rightarrow \Sigma$ is a color set function that assigns a color set to each place.
vii. $G : T \rightarrow EXPR_V$ is a guard function that assigns a guard to each transition t such that $Type[G(t)] = Bool$.
viii. $E : A \rightarrow EXPR_V$ is an arc expression function that assigns an arc expression to each arc a such that $Type[E(a)] = C(p)_{MS}$, where p is the place connected and MS refers to "multiset". to the arc a.
ix. $I : P \rightarrow EXPR_\theta$ is an initialisation function that assigns an initialisation expression to each place p such that $Type[I(p)] = C(p)_{MS}$.
x. $T_{sub} \subseteq T$ is a set of substitution transitions.
xi. $P_{port} \subseteq P$ is a set of port places.
xii. $PT : P_{port} \rightarrow IN,OUT, I/O$ is a port type function that assigns port types to places.

Therefore, a *hierarchical coloured Petri net* is a four-tuple $CPN_H = (S, SM, PS, FS)$ (Jensen and Kristensen, 2009):

[1]https://cpntools.org/

i. S is a finite set of *modules*. Each module is a *Coloured Petri Net Module* $s = ((P^s, T^s, A^s, \Sigma^s, V^s, C^s, G^s, E^s, I^s), T^s_{sub}, P^s_{port}, PT^s)$. It is required that $(P^{s_i} \cup T^{s_i}) \cap (P^{s_j} \cup T^{s_j}) = \theta$ for all $s_i, s_j \in S$ such that $i \neq j$.

ii. $SM : T_{sub} \rightarrow S$ is a *submodule* function that assigns a submodule to each substitution transition, requiring that the *module hierarchy* is acyclic.

iii. PS is a port-socket relation function that assigns a *port-socket relation* $PS(t) \subseteq P_{sock}(t) \times P^{SM(t)}_{port}$ to each substitution transition t, requiring that $PT(p) = PT(p')$, $C(p) = C(p')$ and $I(p)\langle\rangle$ for all $(p, p') \in PS(t)$ and all $t \in T_{sub}$.

iv. $FS \subseteq 2^P$ is a family of non-empty *fusion sets* such that $C(p) = C(p')$ and $I(p)\langle\rangle = I(p')\langle\rangle$ for all $p, p' \in fs$ and all $fs \in FS$.

This formal modeling language is widely used for analyzing and ensuring the compliance of complex and non-deterministic systems with desired properties. Therefore, formalism is relevant for modeling and analyzing ML results. The CPN Tools are used to develop and analyze CPN models, enabling editing, simulation, and state-space analysis.

The state-space analysis of CPN models is a process that examines the structure and behavior of CPN models. The analysis process relates to identifying a model's reachable states and state changes. The CPN Tools automatically report state-space statistics and main behavioral patterns, such as liveness, boundedness, fairness, and home properties. Thus, using state space allows the developer to verify the satisfiability of the model with respect to system safety properties.

However, one limitation of state-space analysis is the state explosion problem, which occurs when modeling a system with many possible states. For instance, the state-space explosion problem can happen when there are many variables in the system, as each additional variable significantly increases the number of possible states (Clarke et al., 2018).

3 Related Works

Various methods have been proposed to enhance and better understand the security of protocols, especially as the rollout of 5G gains momentum (Piqueras Jover and Marojevic, 2019). For example, Ouaissa and Ouaissa (2020) highlighted vulnerabilities in the 5G-AKA protocol, pointing to potential threats to user data protection and privacy. They introduced a refined version of the 5G-AKA protocol to address these issues. Their solution was verified with the AVISPA tool, showcasing the enhanced protocol's security verification and authentication capabilities.

Edris et al. (2020) provide a particularly relevant perspective as they conduct a detailed formal analysis of the 5G-AKA protocol. They used ProVerif to perform a comprehensive systematic assessment of the 5G-AKA protocol. The authors identify that the existing protocol does not achieve critical security properties and that previous studies have overlooked some crucial flaws. Based on this, they offer recommendations to address the issues identified in their security analysis.

Yan, Gu, Gu and Huang (2021) focus on the formal specification and security verification of 5G-AKA. They identify three potential attack methods on the protocol and propose an enhancement scheme to mitigate them. CPN enabled them to create a clear graphical representation of the protocol and attacks, facilitating understanding and vulnerability identification. In another study, Yan, Gu and Huang (2021) focused on preventing location-tracking attacks in the 5G-AKA protocol. For this purpose, they proposed a novel scheme that utilizes a trust-based networking approach. Similarly to the previous work, they applied CPN to model the protocol and attacks.

However, previous studies have some limitations. For example, studies such as those presented in Edris et al. (2020) and Ouaissa and Ouaissa (2020) do not provide a graphical, executable model to enable simulations of the 5G-AKA protocol. Additionally, the studies of Yan, Gu, Gu and Huang (2021); Yan, Gu and Huang (2021) require a more detailed specification of the 5G-AKA components and convincing evidence of the protocol's precise representation. For instance, they represent some 5G network functions using color sets and Standard Modeling Language (SML) functions that could be too simplified. Formal verification using ASK-CTL needs to be included in such studies. The authors use only simulations and manual state-space analysis based on a sample of the state space.

Thus, our study goes two steps further: (1) we provide a more detailed CPN model for the 5G-AKA protocol, and (2) we formally verify the model using ASK-CTL. The following sections detail these contributions.

4 CPN Model

The first step in modeling the 5G-AKA authentication protocol using CPN was to identify the fundamental elements involved in the authentication procedure. For this task, we used the formal specification document provided by the European Telecommunications Standards Institute as a reference source (ETSI, 2020). The document guided the specification of the security architecture of the security procedures executed in the 5G system.

Fig. 1 presents the main module of the 5G-AKA protocol model. Considering the `Serving Network` and `Home Network` substitution transitions, we can observe relevant components, including the UE, the Security Anchor Function (SEAF), the Authentication Server Function (AUSF), and the Authentication Credential Repository and Processing Function (ARPF). Hierarchical CPN enabled a more explicit representation of component encapsulation, providing modularity and adaptability. Fig. 2 and Fig. 3 present the submodules for the SN and HN, respectively. The SN submodule contains the SEAF function, while the HN contains the AUSF and the ARPF functions.

The hierarchical CPN model also allows the addition of new instances of relevant components, such as the UE. Fig. 4 illustrates the 5G-AKA model considering two UEs. Defining different configurations can enable analyses using specific 5G topologies. The source of the CPN model

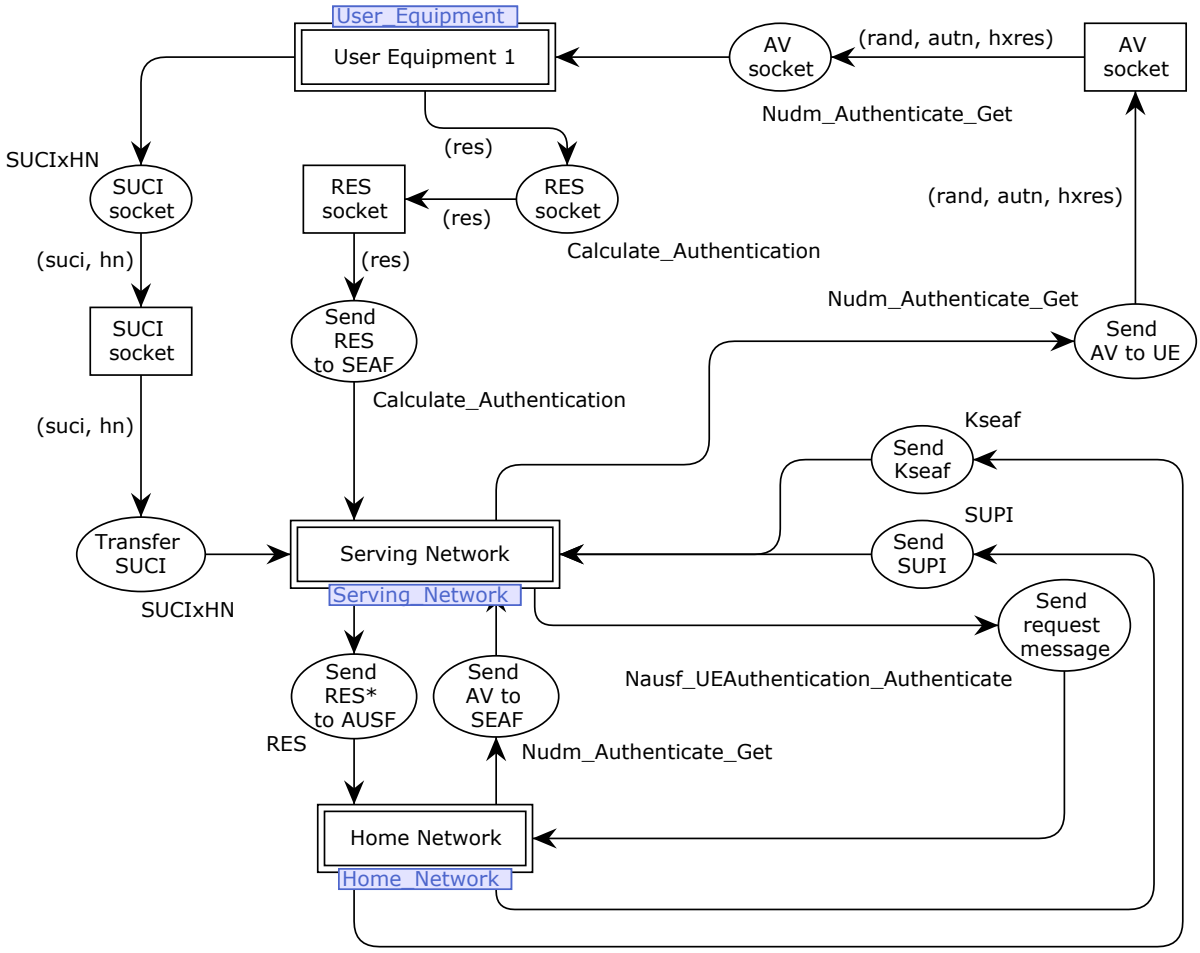

Figure 1: Main module of the 5G-AKA protocol model.

presented in this article is available online for reuse[1]. The source provides a more detailed presentation of all elements of the CPN model, including color sets, variables, and implemented SML functions. The following sections address specific 5G-AKA elements present in the previous illustrated modules (Fig. 1, Fig. 2, Fig. 3, and Fig. 4).

4.1 UE Modeling

The UE can connect to the 5G Core (5GC) and the evolved packet core and is attached to a gNB that is linked to both cores. The UE can select which core to connect to. If the UE chooses the 5GC, it will follow security procedures based on key agreement concepts.

The primary authentication and key agreement procedures provide mutual authentication between the UE and the network. These procedures also generate ciphering material that can be used in subsequent security processes between the UE and the Serving Network (SN). The key derived from the primary authentication and key agreement procedure is used to generate an anchor key, KSEAF. This key is provided by the AUSF of the home network to the SEAF of the SN.

Therefore, the UE performs two main tasks. The first is to initiate the protocol by requesting authentication. In this step, the UE encrypts the Subscription Permanent Identifier (SUPI) and sends it as the Subscription Concealed Identifier (SUCI) to the SN. This preserves the confidentiality of user information during transmission, preventing undue exposure of sensitive data. Fig. 5 presents a sample of the 5G-AKA CPN model, focusing on the first authentication procedures performed by the UE. The `Encrypt SUPI` represents the conversion of the SUPI to the SUCI identifier.

Fig. 6 presents the Authentication Vector (AV) verification procedure and the UE's response generation. After sending the SUCI, the UE awaits the SN's response, which includes the transmission of the Random Challenge (RAND) and the Authentication Token (AUTN). Upon receiving these parameters, the UE initiates the second task: verifying the 5G AV update and calculating the response (RES*).

The UE verifies the provided AUTN by comparing it with the value stored in 5G AV. This verification is essential to ensure the authenticity of the AUTN and,

[1]https://doi.org/10.5281/zenodo.8257009

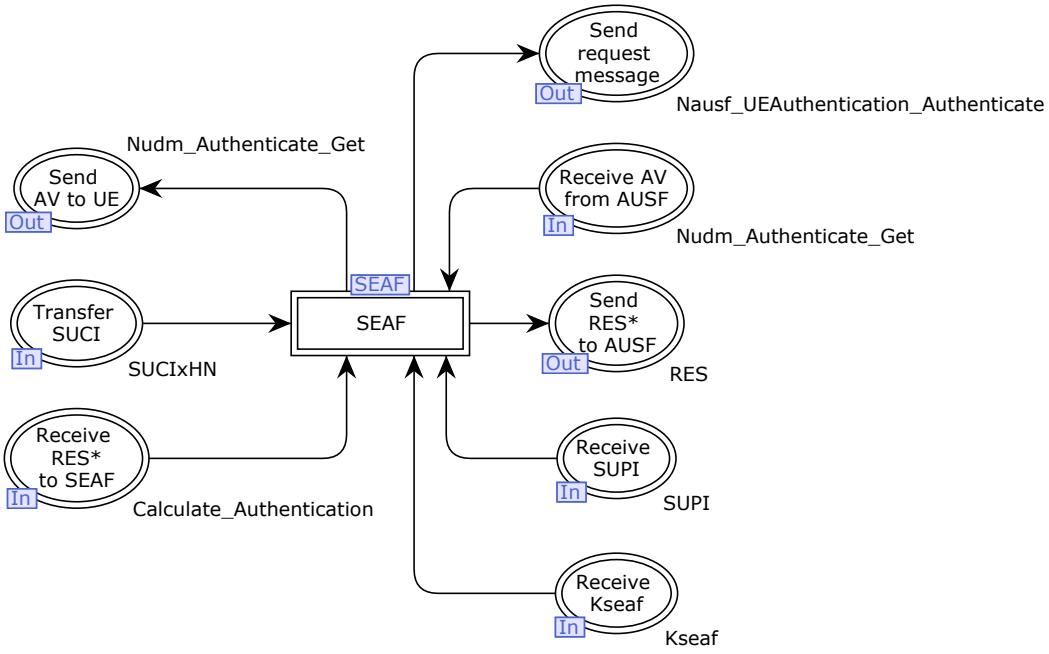

Figure 2: SN submodule of the 5G-AKA model.

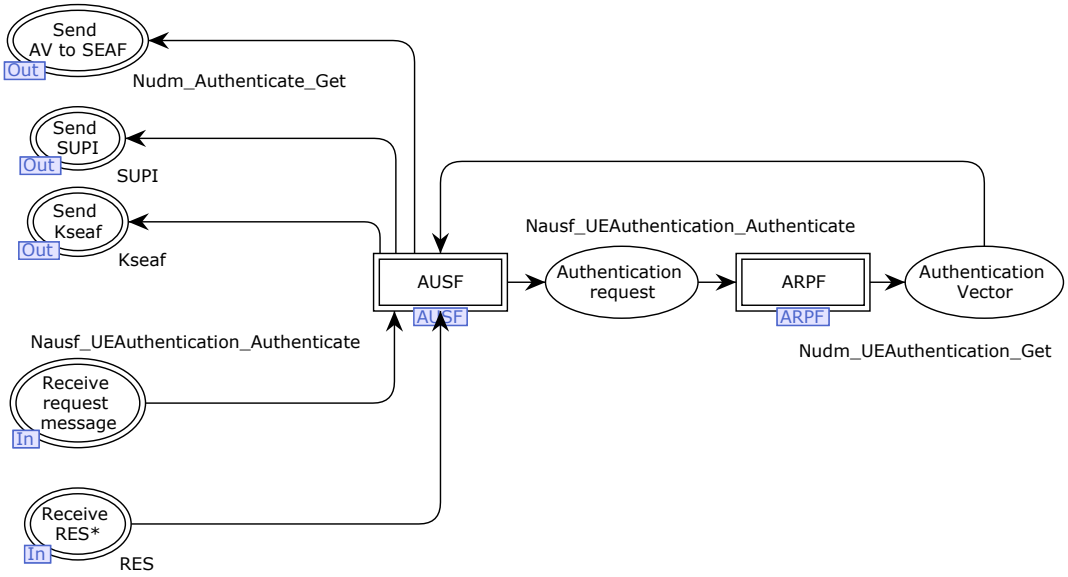

Figure 3: HN submodule of the 5G-AKA model.

consequently, the security of the protocol. If the AUTN is validated, the UE uses the received RES to calculate RES*. RES* represents the UE's response to the authentication challenge and ensures the continuity of the process.

Subsequently, the UE returns the RES* to the SEAF in a non-access stratum message called an authentication response. This message contains the necessary information to proceed with authentication and establish a secure connection between the UE and the network.

4.2 SEAF Modeling

Fig. 7 presents a sample of the model with the authentication request. The SEAF is a key component in the 5G-AKA protocol, facilitating secure communication between the UE and the SN. Upon receiving the authentication request from the UE, the SEAF undertakes a series of tasks to ensure the process is secure.

The SEAF's initial task is to receive the UE's request and forward it to the Home Network (HN). Additionally, the SEAF is responsible for transmitting the SUCI to the

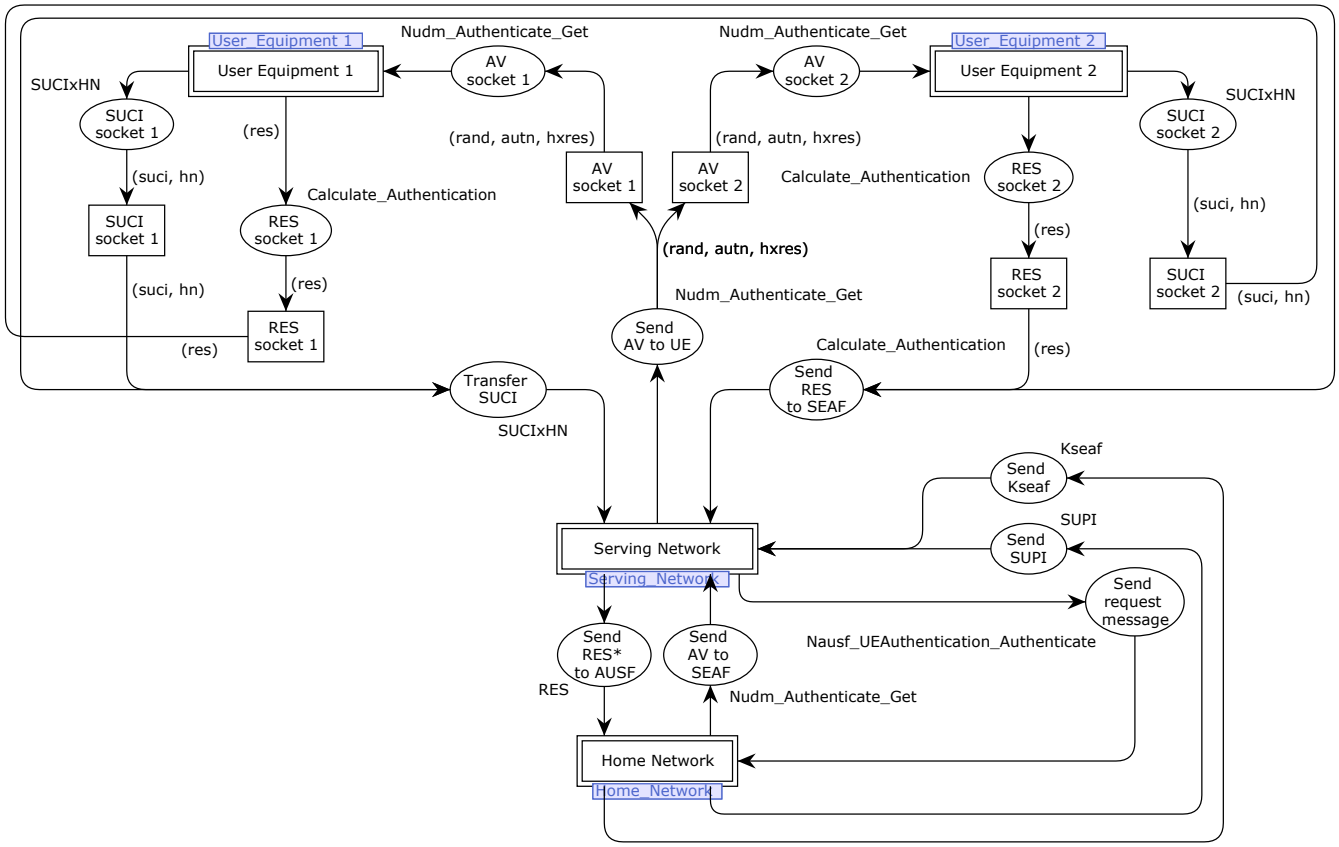

Figure 4: CPN model of the 5G-AKA protocol with two instantiated UEs.

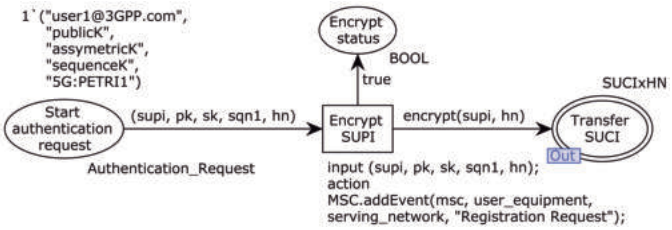

Figure 5: Model with the first UEs' authentication procedures

HN, which is used to identify the UE securely.

After receiving the RAND and AUTN parameters from the AUSF, the SEAF generates a message containing these parameters and sends it back to the UE, enabling it to perform the necessary calculations for authentication. At the same time, the SEAF stores the HXRES* for future comparisons of the response challenge.

Upon receiving the RES* from the UE, the SEAF promptly computes the Hash of RES* (HRES*) and compares it with the previously stored HXRES* to determine whether they are identical. In the event of identical values, the SEAF considers the authentication successful from the SN's perspective. Fig. 8 presents the verification process of challenge-response. After successful verification, the SEAF transmits the RES* from the UE to the AUSF.

If authentication is successful, the SEAF awaits a response from the AUSF. Upon successful authentication, the SEAF receives the KSEAF key and the SUPI in the message. The KSEAF key is critical to ensure security in communications between the UE and the SN. Fig. 9 presents the final authentication procedure considering the SEAF.

4.3 AUSF Modeling

The AUSF provides authentication and authorization services for the UE and the SN (Fig. 10). Its functions encompass temporary information storage, the generation and manipulation of authentication vectors, and the validation of network responses to determine the success or failure of authentication.

Upon receiving the XRES* temporarily along with the SUCI or SUPI, the AUSF stores these values. Subsequently, it generates the 5G AV by utilizing the 5G HE AV received from the ARPF, calculating the HXRES* and KSEAF. The AUSF replaces the XRES* with the HXRES* and the KAUSF with the KSEAF in the 5G HE AV. Following the manipulation of 5G AV, AUSF removes the KSEAF and returns the authentication vector, containing RAND, AUTN, and HXRES*, back to the SEAF. Fig. 11 presents the authentication and authorization process of the AUSF.

After successful authentication, the AUSF stores the

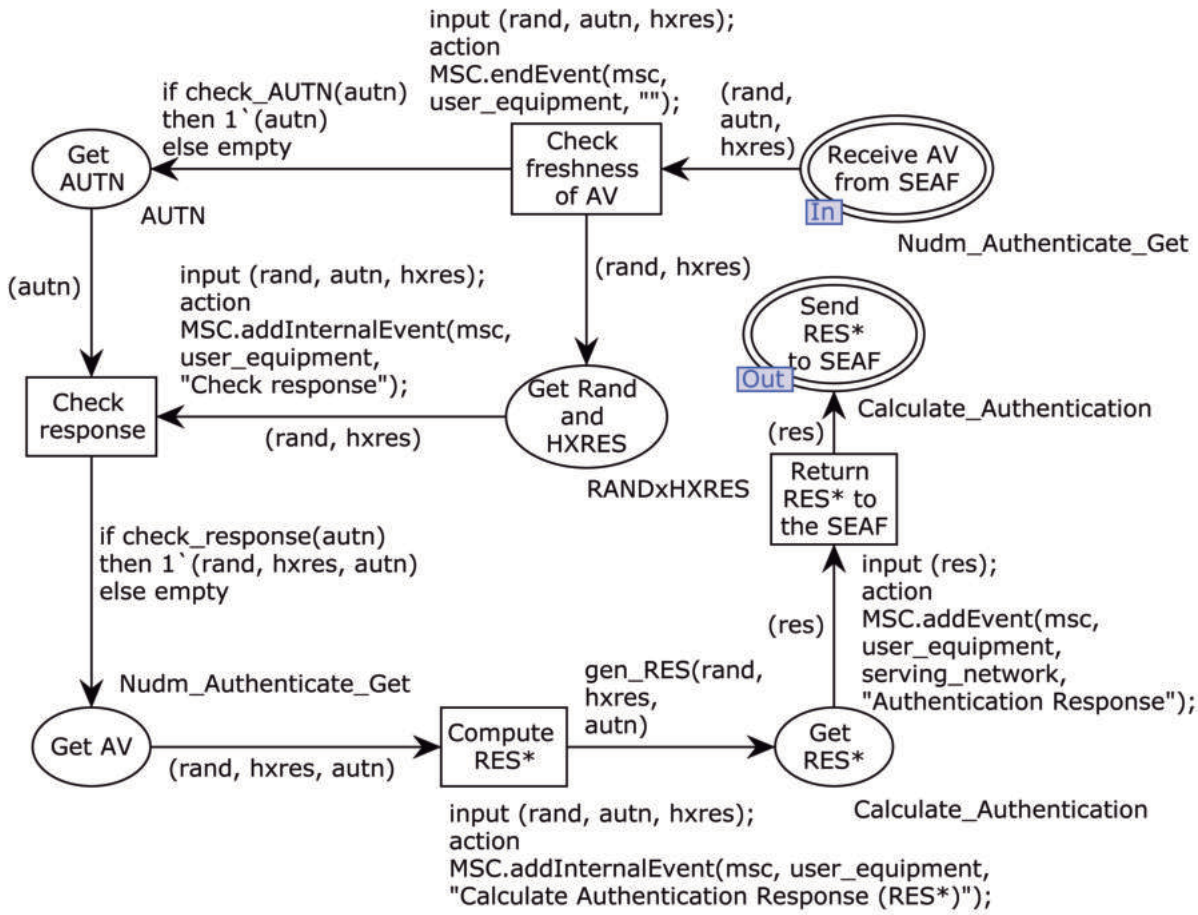

Figure 6: Sample of the model with the verification procedure and response.

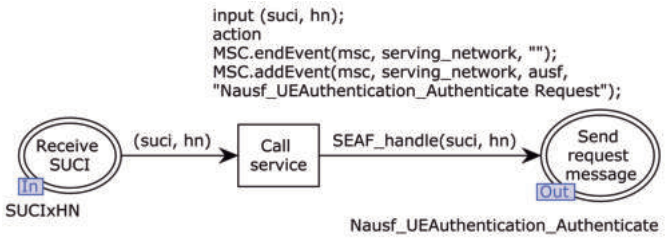

Figure 7: Sample with the authentication request.

KAUSF and compares the received RES* with the stored XRES*. If these values match, the AUSF considers the authentication successful from the home network's perspective. If the authentication is successful, the KSEAF is returned to the SEAF. The AUSF also includes the SUPI in the response message to the SEAF, ensuring accurate identification and association of the UE with its permanent identifier during authentication.

4.4 ARPF Modeling

Upon receiving a request, the ARPF initiates the process by creating a 5G Header Encryption Authentication Vector (5G HE AV). Subsequently, the ARPF derives the Key Agreement for the AUSF (KAUSF) and calculates the Expected Response (XRES*). Lastly, the ARPF generates a new 5G HE AV containing the parameters RAND, AUTN, XRES*, and KAUSF, which will be used in subsequent protocol steps. Fig. 12 shows the ARPF creating the authentication vector.

The ARPF is relevant in generating authentication keys and parameters and ensuring the process's security. By creating and providing 5G HE AV containing crucial information such as RAND, AUTN, XRES*, and KAUSF, the ARPF contributes to establishing a reliable and secure authentication between the UE and the service network. This modeling of the steps executed by the ARPF is essential to ensure the proper execution of the 5G AKA authentication protocol and enhance communication security in the 5G network.

5 Model Simulation

We conducted many simulation steps to analyze the CPN model presented in Section 3. To bolster our confidence that the CPN model accurately represents the 5G-AKA protocol, we also generated Message Sequence Charts (MSCs) by model simulation. The MSC is a graphical tool

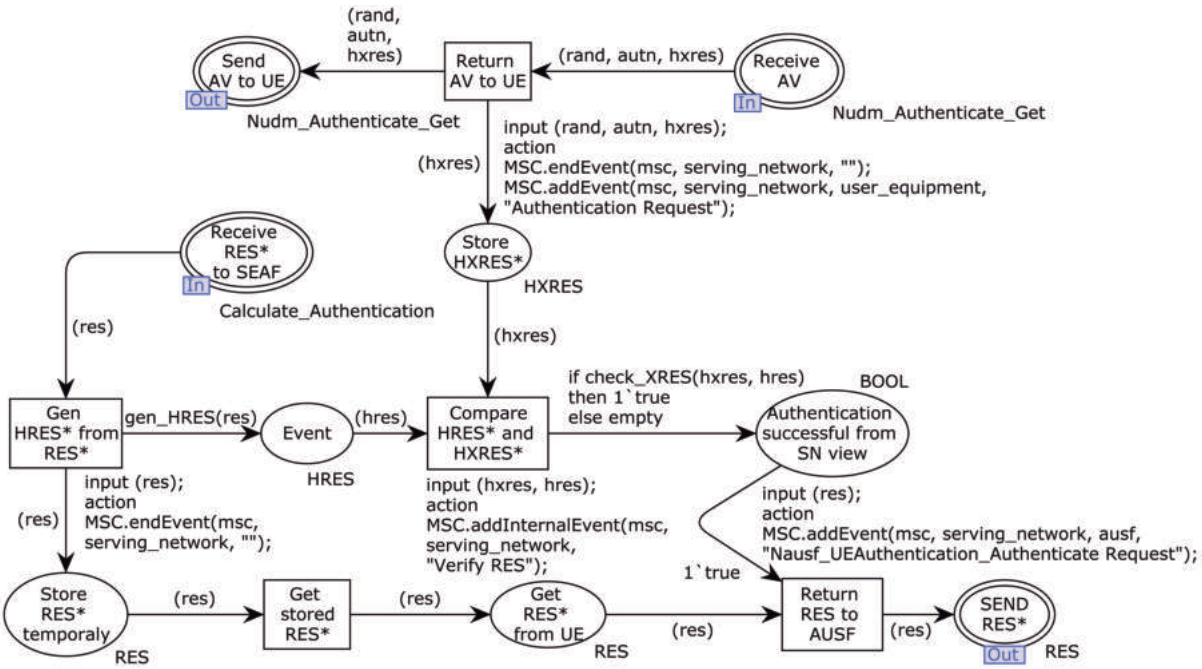

Figure 8: Sample of the model with the challenge-response verification.

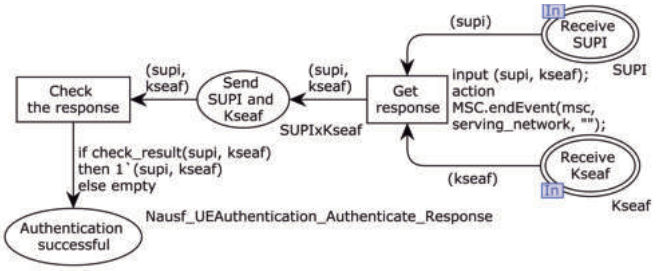

Figure 9: Sample with the final procedure for authentication.

for representing interactions in communication systems. Its intuitive nature aids not only representation but also validation of communication flows between entities.

By integrating MSCs into the CPN modeling, we can show that every communication flow is precisely mapped and aligned with the technical specifications. The MSC enhances the clarity of the system representation and provides a systematic approach for validation. Any deviation can be easily identified and corrected by comparing the MSC derived from the CPN model with the original protocol specifications. As shown in Fig. 13, the MSC generated by the CPN model improved the visual clarity of component interactions and provided behavioral validation. We compared the MSC generated by our CPN model with the 3GPP specifications to ensure that our model accurately represents the communication flows among all entities.

6 Formal Verification

We used the ASK-CTL library within CPN/Tools. This library employs an extension of CTL, a branching temporal logic that facilitates the expression of path-related properties in a model. The ASK-CTL library considers state and transition information, and its queries are structured directly in the SML[2] (Standard ML) functional programming language.

Formal verification entails the exhaustive traversal of all paths within the model's state space. We can evaluate whether the formal model upholds specific protocol properties. We have formally defined and verified six properties using ASK-CTL. These properties were designed to adhere to the privacy and confidentiality protection requirements of user identifiers (e.g., SUPI), ensuring (i) that only legitimate networks can initiate authentication processes, (ii) the integrity and authenticity of authentication vectors, (iii) the uniqueness of each session, and (iv) the successful completion of the authentication process, safeguarding the network against authentication failures.

Table Table 1 lists the ASK-CTL properties and descriptions. All the properties were satisfied using model checking. The first property verifies that, at some point in the future, the SUPI will be encrypted, and the network will initiate the authentication process. In the formula, it is possible to primarily identify the SML functions `encrypt` and `isEncrypted`, which verify the markings of the corresponding places. In contrast, the `service` function checks whether the `Call_service` transition fires with certain specific binding elements.

[2]https://cs.lmu.edu/ ray/notes/introml/

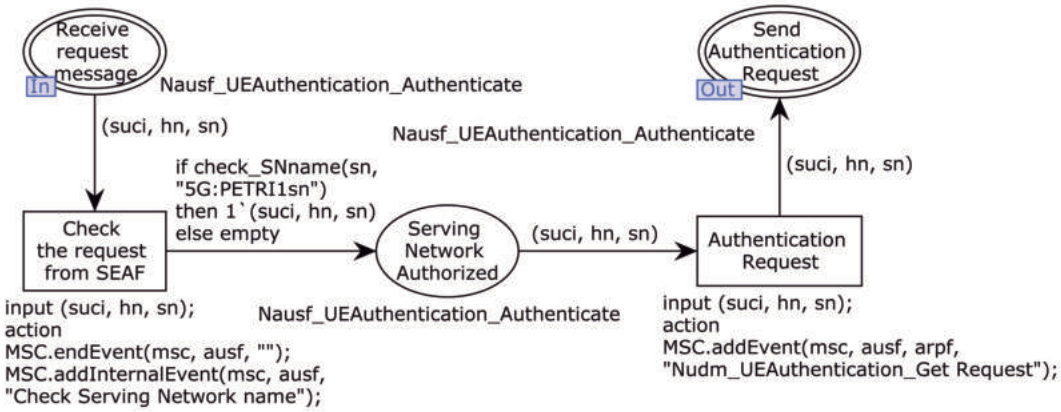

Figure 10: Sample with the verification of the request.

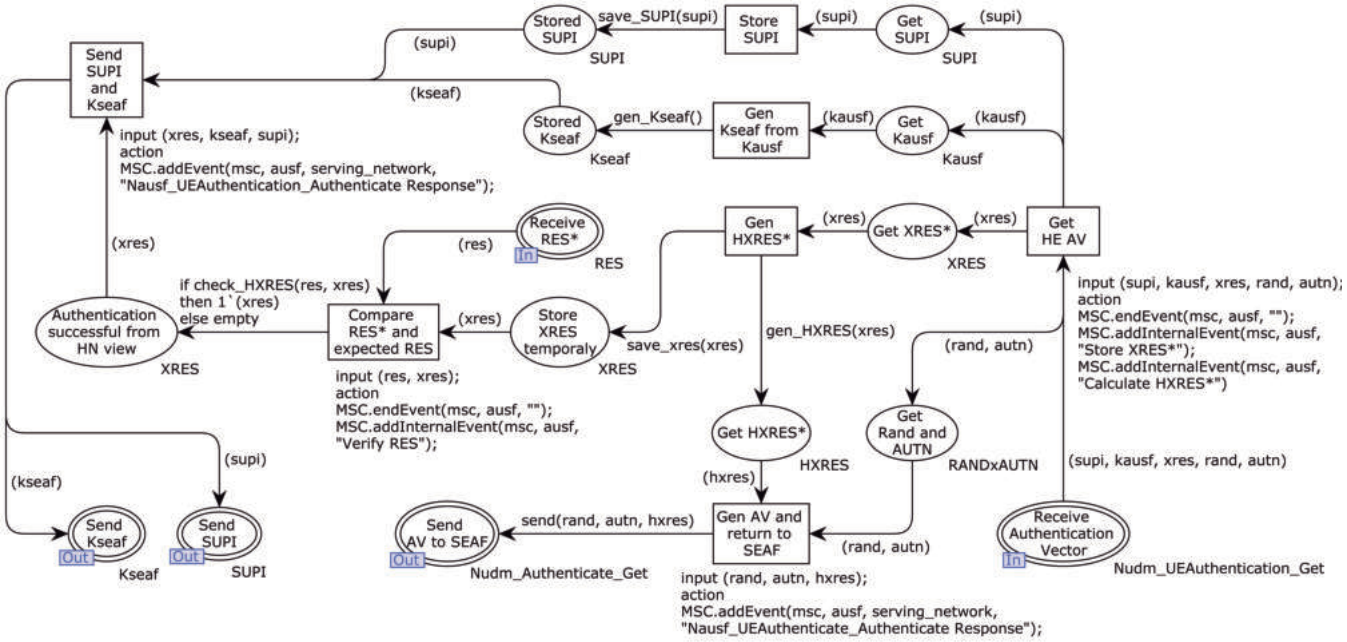

Figure 11: Sample of the model with the authentication and authorization.

The second property ensures that it is impossible to initiate an authentication process by providing an invalid HN. The function `request` checks for an invalid HN and returns "valid" for states where a request with the specified characteristics exists. On the contrary, the function `isAuthorizedFormula` verifies that authorization has not been granted.

The 5G-AKA protocol transmits data from the network to the UE, serving as the challenge-response that validates the user's identity. Thus, the third property verifies whether the SN sends all the necessary data for this purpose after the UE initiates the authentication request. The functions `service` and `return` verify whether a transition with the declared label is present on the arc they are analyzing.

The fourth property verifies whether the network has sent an authentication vector and received it by the UE while the network has temporarily stored an expected response. We defined two functions to verify specific conditions within the model. The first, `isXRESStored`, checks whether the expected response token is stored at the specified location. In contrast, `isAVReceived` verifies whether the authentication vector with specific values is present.

The fifth property ensures that the network generates and sends a random number, which the UE receives to continue the protocol. The RAND is relevant, as it is one of the elements that make up the AV used during the process. The function `randGenerated` serves the purpose of verifying whether a random value has been generated and associated with a specific arc in the network, identified by the index `i`, while the function `randReceived` checks whether the UE has received a random value in the instance `i2` of the model.

Finally, the fifth property ensures that the network will complete the authentication process successfully,

Table 1: ASK-CTL properties for 5G-AKA model.

ID	Property	Description
1	AND(AND(EV(MODAL(AF("encrypt",encrypt))),POS(NF ("isEncrypted",isEncrypted))),POS(MODAL(AF("service", service))))	The SUPI will be encrypted. Thus, the service network will initiate the authentication process.
2	FORALL_UNTIL(AF("Request",request),NOT((NF("Authorized", isAuthorized)))	It is not possible to start an authentication process with an invalid HN.
3	FORALL_MODAL(AF("Service",service), (AF("Return",return))	After an authentication request event, the SN sends all required data to enable the UE to proceed.
4	EXIS_UNTIL(POS(NF("XRESStored",isXRESStored)), NF("AVReceived", isAVReceived))	An authentication vector was sent and, afterward, received by the UE while the network temporarily recorded a response.
5	FORALL_UNTIL(POS(MODAL(AF("generated",randomGenerated))), POS(NF("received", randomReceived)))	A generated random number is sent by the network and received by the UE.
6	FORALL_UNTIL(AND(POS(NF("sn",snStatus)),POS(NF("hn", hnStatus))), POS(NF("process",process)))	If there exists an authentication process failure by the network during the challenge's response, the network will finish the process.

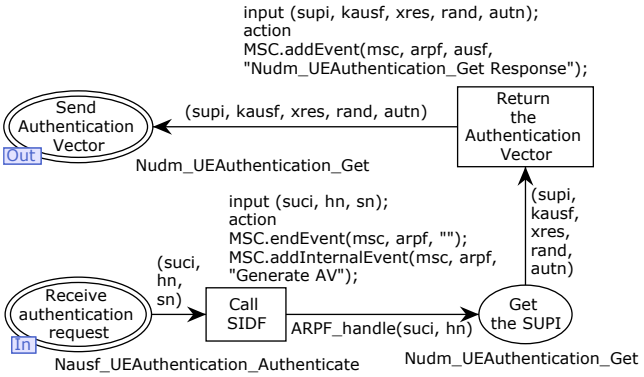

Figure 12: Sample with the authentication vector.

without failures in the service network or the HN during the challenge-response phase. The functions `snStatus`, `hnStatus`, and `process` verify the markings at the specified places.

In addition to validating the model against the desired properties of the 5G-AKA protocol as specified in the technical specifications, formal verification is relevant for analyzing the model with respect to various security aspects. For instance, the proposed model enables diverse network configurations with varying quantities of UE and distinct relationships. Additionally, modelers can extend our model to represent other network components within a specific 5G network configuration. Thus, they can ascertain whether the model satisfies the designated properties for each experimented configuration.

Given the protocol's specification, they can also analyze security threats in the 5G network. Examples of known threats to these networks include replay and MITM attacks. Such information on existing threats can serve as a basis for augmenting the model, which aims to provide mitigation measures. Afterward, the definition of new ASK-CTL properties can help modelers ensure that the included mitigation measures are effective.

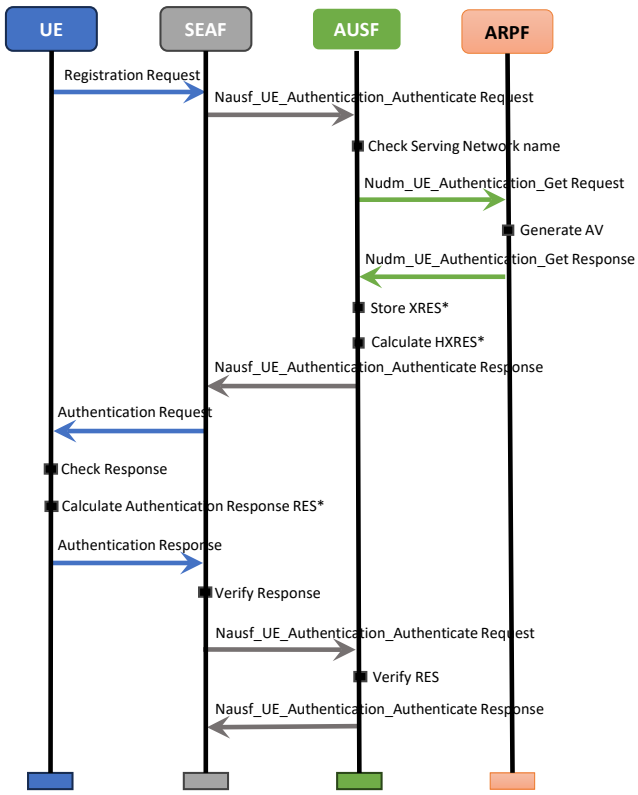

Figure 13: MSC from the simulation of the 5G-AKA model.

7 Example of Attack Scenario

We can consider an attack that occurs during UE authentication and involves the HN providing services. This passive attack monitors private data related to network traffic (from the UE to the service). Including an attack in our model highlights the importance of analyzing and mitigating problematic scenarios. Fig. 14 shows the main CPN module with the attack modeled. The substitution transition, Fake SN/UE, represents the lower-level details of the attack.

The attacker positions a Fake SN/UE to intercept and manipulate critical authentication messages exchanged

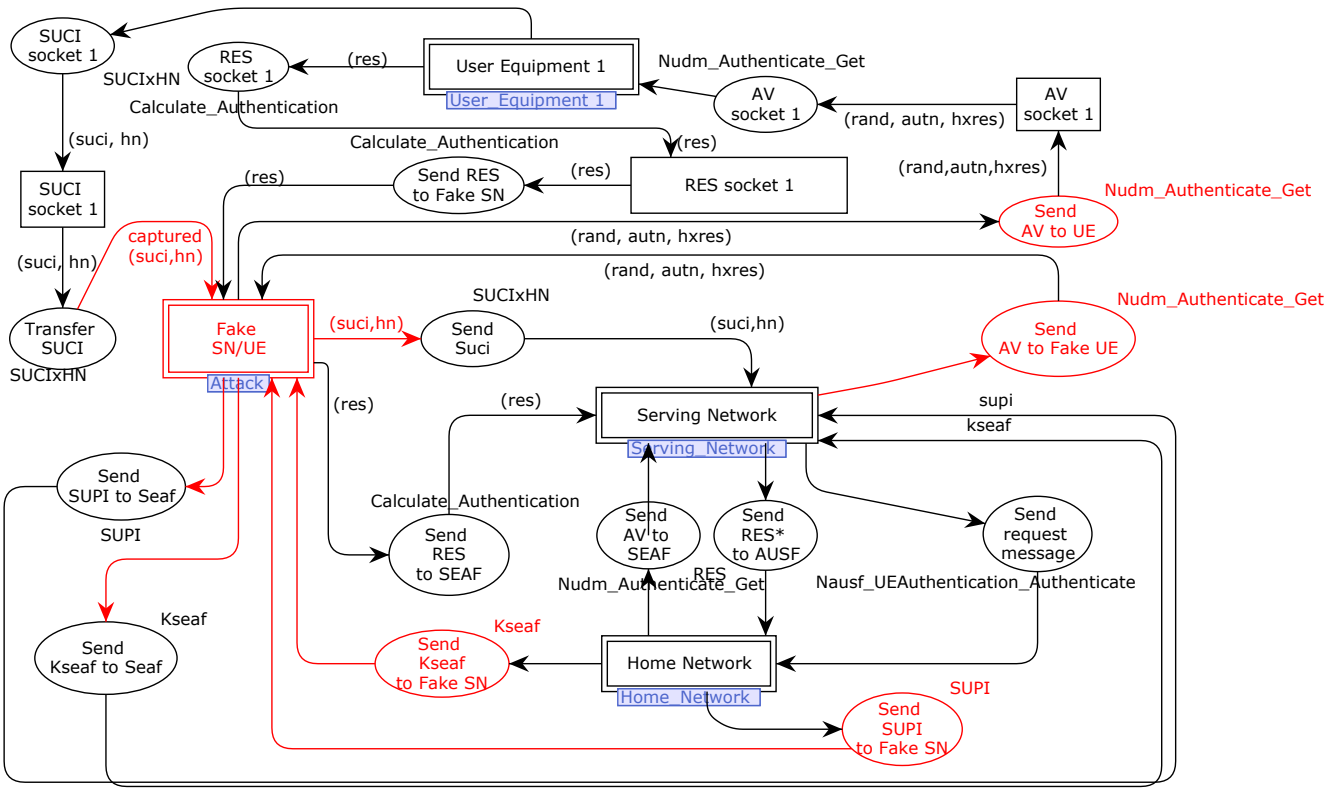

Figure 14: Example of an attack scenario considering the monitoring of network traffic.

among the UE, SN, and HN. The malicious node passively captures the SUCI during transmission and re-injects it into the network, triggering a parallel, fraudulent authentication workflow. Thus, it forces the legitimate network entities to generate and forward sensitive artifacts, exploiting the trust relationship.

8 Conclusion and Future Works

Using the CPN formal modeling language, we provide a detailed and reliable representation of the 5G-AKA protocol. Earlier formal analyses of the 5G-AKA protocol did not provide a graphical, executable, and parameterized model for simulating different 5G topologies. CPN model simulations and formal verification using ASK-CTL evidenced the precise representation of the protocol's components in our specification. Therefore, we can reuse our CPN model to identify and analyze vulnerabilities that compromise the security of 5G networks. Although some previous studies formally analyzed the 5G-AKA protocol, our formal CPN specification complements the literature by providing graphical and executable models that explicitly present the protocol's components and communication flow. Besides being relevant for conducting a formal analysis of security properties, the models can be reused as executable documentation for future protocol implementations. They can also be valuable for modifying the existing specification to enhance the protocol.

In future work, we aim to conduct a comprehensive security analysis of the 5G-AKA protocol using the CPN model presented in this paper. Simulations and formal verification using ASK-CTL can support the analysis, providing convincing evidence of the existence of vulnerabilities. We also plan to experiment with various 5G topologies for additional security analyses.

Acknowledgments

The authors acknowledge the support by the Project SafeSenseAI Base supported by Centro de Competência Embrapii Virtus em Hardware Inteligente Para Indústria—VIRTUS-CC, with financial resources from the Programa Prioritário (PPI) HardwareBR of the Ministério da Ciência, Tecnologia e Inovação (MCTI), signed with Empresa Brasileira de Pesquisa e Inovação Industrial (EMBRAPII), under Grant 055/2023.

References

Basin, D., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R. and Stettler, V. (2018). A formal analysis of 5g authentication, *Proc. of the SIGSAC Conference on Computer and Communications Security*, CCS '18, ACM, New York, NY, USA, p. 1383–1396. https://doi.org/10.1145/3243734.3243846.

Cheng, A., Christensen, S. and Mortensen, K. H. (1997).

Model checking coloured petri nets - exploiting strongly connected components, *DAIMI Report Series* **26**(519). https://doi.org/10.7146/dpb.v26i519.7048.

Clarke, E. M., Henzinger, T. A., Veith, H. and Bloem, R. (2018). *Handbook of Model Checking*, 1st edn, Springer Publishing Company, Incorporated. https://doi.org/10.1007/978-3-319-10575-8.

Edris, E. K. K., Aiash, M. and Loo, J. K.-K. (2020). Formal verification and analysis of primary authentication based on 5g-aka protocol, *2020 Seventh International Conference on Software Defined Systems (SDS)*, pp. 256–261. https://doi.org/10.1109/SDS49854.2020.9143899.

ETSI (2020). Security architecture and procedures for 5g system (3gpp ts 33.501 version 16.3.0 release 16). Available at https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf.

Fernandes Costa, T., Sobrinho, A., Chaves e Silva, L., da Silva, L. D. and Perkusich, A. (2022). Coloured petri nets-based modeling and validation of insulin infusion pump systems, *Applied Sciences* **12**(3). https://doi.org/10.3390/app12031475.

Jensen, K. (1981). Coloured petri nets and the invariant-method, *Theoretical Computer Science* **14**(3): 317–336. https://doi.org/10.1016/0304-3975(81)90049-9.

Jensen, K. and Kristensen, L. M. (2009). *Coloured Petri Nets: Modelling and Validation of Concurrent Systems*, 1st edn, Springer Publishing Company, Incorporated. https://doi.org/10.1007/b95112.

Jensen, K. and Kristensen, L. M. (2015a). Colored petri nets: A graphical language for formal modeling and validation of concurrent systems, *Commun. ACM* **58**(6): 61–70. https://doi.org/10.1145/2663340.

Jensen, K. and Kristensen, L. M. (2015b). Colored petri nets: a graphical language for formal modeling and validation of concurrent systems, *Commun. ACM* **58**(6): 61–70. https://doi.org/10.1145/2663340.

Khan, R., Kumar, P., Jayakody, D. N. K. and Liyanage, M. (2020). A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions, *IEEE Communications Surveys & Tutorials* **22**(1): 196–248. https://doi.org/10.1109/COMST.2019.2933899.

Li, Y., Yu, Y., Susilo, W., Hong, Z. and Guizani, M. (2021). Security and privacy for edge intelligence in 5g and beyond networks: Challenges and solutions, *IEEE Wireless Communications* **28**(2): 63–69. https://doi.org/10.1109/MWC.001.2000318.

Ouaissa, M. and Ouaissa, M. (2020). An improved privacy authentication protocol for 5g mobile networks, *2020 International Conference on Advances in Computing, Communication & Materials (ICACCM)*, pp. 136–143. https://doi.org/10.1109/ICACCM50413.2020.9212910.

Piqueras Jover, R. and Marojevic, V. (2019). Security and protocol exploit analysis of the 5g specifications, *IEEE Access* **7**: 24956–24963. https://doi.org/10.1109/ACCESS.2019.2899254.

Sobrinho, A., Vilarim, M., Barbosa, A., Candeia Gurjão, E., F. S. Santos, D., Valadares, D. and Dias da Silva, L. (2024). Challenges and opportunities in mobile network security for vertical applications: A survey, *ACM Comput. Surv.* **57**(2). https://doi.org/10.1145/3696446.

Valadares, D. C. G., de Carvalho César Sobrinho, A. A., Perkusich, A. and Gorgonio, K. C. (2021). Formal verification of a trusted execution environment-based architecture for iot applications, *IEEE Internet of Things Journal* **8**(23): 17199–17210. https://doi.org/10.1109/JIOT.2021.3077850.

Valadares, D. C. G., Will, N. C., Sobrinho, Á. Á. C. C., Lima, A. C. D., Morais, I. S. and Santos, D. F. S. (2023). Security challenges and recommendations in 5g-IoT scenarios, *Advanced Information Networking and Applications*, Springer, pp. 558–573. https://doi.org/10.1007/978-3-031-29056-5_48.

Wen, M., Li, Q., Kim, K. J., López-Pérez, D., Dobre, O. A., Poor, H. V., Popovski, P. and Tsiftsis, T. A. (2022). Private 5g networks: Concepts, architectures, and research landscape, *IEEE Journal of Selected Topics in Signal Processing* **16**(1): 7–25. https://doi.org/10.1109/JSTSP.2021.3137669.

Yan, Z., Gu, C., Gu, Y. and Huang, H. (2021). Security verification and improvement of 5g aka protocol based on petri-net, *2021 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 11–16. https://doi.org/10.1109/ICCC52777.2021.9580325.

Yan, Z., Gu, C. and Huang, H. (2021). Analysis for threat models and improvement scheme of 5g aka protocol based on petri-net, *2021 IEEE 21st International Conference on Communication Technology (ICCT)*, pp. 11–17. https://doi.org/10.1109/ICCT52962.2021.9657852.