Hindawi
Security and Communication Networks
Volume 2021, Article ID 4498324, 15 pages
https://doi.org/10.1155/2021/4498324

Research Article

Towards 5G Security Analysis against Null Security Algorithms Used in Normal Communication

Run Zhang,[1] WenAn Zhou ,[1] and Huamiao Hu[2]

[1]*School of Computer Science (National Pilot Software Engineering School), Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*Science and Technology on Communication Information Security Control Laboratory, Jiaxing 314003, Zhejiang, China*

Correspondence should be addressed to WenAn Zhou; zhouwa@bupt.edu.cn

Received 29 June 2021; Revised 27 September 2021; Accepted 29 September 2021; Published 20 October 2021

Academic Editor: Weizhi Meng

mailto: 5G network makes our lives delicate and more pleasant, and its security will impact the operation of the entire society. Compared with the LTE network, 5G brings up many new security features and possesses more sophisticated and robust security mechanisms, while there are still many potential security issues with the 5G network. Therefore, the security analysis of the 5G network is highly crucial. Null security algorithm (i.e., NEA0 and NIA0) is used in normal communication, a security vulnerability that exists and has not been fully addressed in the LTE network, but in the 5G network, no studies have been performed to demonstrate whether this security vulnerability still exists so far. Therefore, in this paper, we apply a systematic approach based on the principle of model checking to verify. We conduct an in-depth analysis of the signaling interaction and security mechanism for the attach procedure in the 5G network. And then, we model UE and AMF into two synchronous communication finite-state machines, extract the desired properties from 3GPP relevant specifications, and construct an adversary model to test the system's security. By observing the operation of state machines and analyzing relevant protocol behavior, we discover that faulty security algorithm selection could result in the acceptance of the null security algorithm (i.e., NEA0 and NIA0) on the side of the core network, and attackers can exploit this to trigger IP spoofing attacks and SUPI catching attacks on the victim UE. We analyze the root cause of these network attacks and propose an anomaly detection method to avoid these network attacks from being launched effectively.

1. Introduction

5G is the fifth-generation wireless technology for digital cellular networks, with widespread deployment which began in 2019, and it was used commercially in 2020. In comparison to current 4G LTE networks, the vision of next-generation 5G wireless communications is to provide very high data rates (typically of the Gbps order), extremely low latency, a massive increase in base station capacity, and a significant improvement in users' perceived quality of service (QoS). 5G is expected to connect people, things, data, applications, transportation systems, and cities in smart networked communication environments, and it can enable new applications such as smart homes and buildings, smart cities, 3D videos, cloud work and play, remote medical services, and virtual and augmented reality. It brings a revolution that makes all aspects of social and economic life increasingly intelligent and has created much enthusiasm in both industry and academia.

However, 5G, such as the power and energy infrastructures on which we currently rely, is an infrastructure, and its security will impact the operation of the entire society. When we more and more rely on 5G, its security issues become more and more serious. Although, compared with the 4G LTE network, the 5G network is designed with highly sophisticated and robust security architecture and cryptographic algorithms to defend against the overwhelming majority of malicious adversarial attacks, it does not mean that the 5G network is secure. There are still many potential security issues with the 5G network.

The 3GPP security working group has studied and dissected the most known LTE protocol security vulnerabilities in 5G security specification 3GPP TS 33.50, and it finds that most of the demonstrated LTE protocol vulnerabilities which have not been fully addressed remain potential security threats in the 5G network. There are many edge cases of network insecurity caused by many security features and procedures outside the scope of protocol specifications in the 5G network. Therefore, when the combination of the protocols that support insecure edge cases and implicit trust of preauthenticated messages, it will lead to a large number of LTE protocol security vulnerabilities being activated. Network attackers can exploit that and launch network attacks, posing a threat to network security. Table 1 summarizes some of the most relevant LTE protocol exploits that are not fully addressed in the open literature and are still a potential threat in the 5G network.

Null security algorithm (i.e., NEA0 and NIA0) is used in normal communication, a security vulnerability that exists and has not been fully addressed in the LTE network. Generally, null security algorithms (i.e., NEA0 and NIA0) are only applicable for UE in the limited service mode. They are just security algorithms informal and cannot provide any encryption protection or integrity protection for the control plane signaling messages in the NAS layer and AS layer. However, when a UE initiates the normal attach procedure to access a cellular network, the core network selects null security algorithms to establish the security context, and the control plane signaling messages will deliver between UE and the core network in the plaintext. Malicious attackers can exploit it to launch network attacks. Chlosta et al. [12] described the threat of eavesdropping and message forgery by inducing null ciphering after testing about twelve commercial LTE networks in European countries. The fundamental problem of this vulnerability is network misconfiguration. Compared with the LTE network, 5G brings up many new security features and possesses more sophisticated and robust security mechanisms, while similar to the LTE network, some of the upcoming 5G security features will be configured by the provider. Because there is a persistent discrepancy between the specified and configured security in the network system, this vulnerability may continue in the 5G network. However, in the 5G network, no studies have been performed to demonstrate whether this security vulnerability still exists so far.

However, the 5G network has not been deployed on a large scale, and there is no open-source 5G protocol stack that can be used to analyze network vulnerabilities in a tested platform. Currently, there are only a handful of studies on the 5G network security, and the researchers conducted the study employing a systematic approach based on the principle of model checking which lazily combines a symbolic model checker and a cryptographic protocol verifier in the symbolic attacker model.

Hussain et al. [4] first presented this approach, exploited it to analyze three critical procedures (i.e., attach, paging, and detach procedures) of the 4G LTE network, and uncovered ten new attacks and nine prior attacks in the LTE network. And then, Hu et al. [13] used this systematic approach to study the registration procedure, authentication procedure, deregistration procedure, security mode command procedure, service request procedure, and identification procedure in the 5G network for analyzing the NAS layer signaling security. In addition to considering these traditional communication procedures, they also studied some new security features in the 5G network, such as enhanced home network control and asymmetric encryption of SUPI. They identified ten new 5G protocol vulnerabilities for 5G nonaccess stratum signaling security and proposed a defense method utilizing the existing public-private key pair adopted by 3GPP. Afterward, Hussain et al. [6] employed this approach to verify 5G NAS layer procedures (i.e., initial registration, deregistration, paging, configuration update, handover, and service request procedures) and the corresponding RRC layer procedures against relevant security and privacy properties. They discovered 11 design weaknesses resulting in attacks having security and privacy implications in the 5G network. This systematic approach can effectively analyze the security of communication networks, and it has attracted the attention of academics, but no studies have been performed to conduct an in-depth analysis of the signaling interaction and security mechanism for the attach procedure in the 5G network by using this systematic approach. No studies have been performed to demonstrate whether the security vulnerability (i.e., the null security algorithm is used in the normal communication) exists in the 5G network by using this systematic approach and whether this security vulnerability poses a risk to the communication network security by using this systematic approach.

Hence, in this paper, we apply this systematic approach to conduct an in-depth analysis of the signaling interaction and security mechanism for the attach procedure in the 5G network and demonstrate that the null security algorithm (i.e., NEA0 and NIA0) used in normal communication exists and remains a security threat in the 5G network. We find that it can trigger IP spoofing attacks and SUPI catching attacks. In addition, we analyze the root cause of these attacks and propose an anomaly detection method against this vulnerability which was presented. The anomaly detection method restricts the use of null security algorithm (i.e., NEA0 and NIA0) in normal communication and ensures that the malicious attackers cannot bypass security mechanisms via enabling the null security algorithm (i.e., NEA0 and NIA0) to trigger attacks.

We focus on the security algorithm selection of the network as an integral component of 5G security. One of the consequences of a network misconfiguration is that attackers could launch a man-in-the-middle attack against the network and impersonate users. Therefore, it is essential to ensure the deployment of secure configurations in 5G networks. In particular, we make the following contributions:

Table 1: Major LTE protocol exploits, threats, and their impact on 5G.

LTE protocol exploit	Threat	Impact on 5G
IMSI catching	Privacy threat, location leaks, SS7 leaks, etc. [1–6]	Potential for IMSI/SUPI catching in some protocol edge cases, such as when an unauthenticated emergency call is maliciously triggered
Device fingerprinting using exposed device capabilities	Identification attacks, bidding down attacks, and battery draining attacks [7]	Exploiting unprotected device capabilities' information identification attacks, bidding down attacks, and battery drain attacks against cellular devices
Location tracking	Location leaks [7]	Link device fingerprints to SUPI and track user's location
Silent downgrade to GSM	Man-in-the-middle attacks, SMS snooping, and phone call [2, 4, 6, 7]	Silent GSM downgrade using preauthentication messages from a malicious base station broadcasting a Mobile Country and Network Code (MCC-MNC) of a network with no public key provisioned in the USIM
Attach/Tracking Area Update (TAU) request	DoS [2, 4, 6]	DoS of 5G mobile devices caused by malicious base stations broadcasting a valid MCC-MNC combination for a network with no public key provisioned in the USIM
Wireless eavesdropping	Eavesdropping attacks [8–11]	Eavesdropping attacks exploit unsecured network communications to gain access to data as they are sent or received by their target

(1) We apply a systematic approach based on the principle of model checking to have a deep analysis of the signaling interaction and security mechanism for the attach procedure in the 5G network and verify that the null security algorithm (i.e., NEA0 and NIA0) is used in the normal communication in the 5G network, and it can trigger IP spoofing attacks and SUPI catching attacks

(2) We analyze the root cause of these attacks and propose an anomaly detection method to avoid these network attacks being launched effectively

The remainder of the paper is organized as the following: Section 2 introduces the 5G network architecture and attach procedure focusing on the NAS security mechanism and AS security mechanism. Besides, we describe the selection process of security algorithms in 5G networks. In Section 3, we introduce the systematic approach used to analyze the security of the 5G network. In Section 4, we show the modeling, the desired properties, and the components of the test platform in our work. Section 5 describes the attack discovered through our method in detail. Section 6 shows the root causes of the discovered attacks and gives a countermeasure against this vulnerability. Finally, we discuss the conclusion and the future work.

2. Technical Background

2.1. 5G Network Architecture. We provide a brief overview of 5G. We simplify the network architecture significantly for clarity (see Figure 1) and only focus on the aspects relevant to the attach procedure. As illustrated in Figure 1, the 5G network is made up of three parts: user equipment (UE), 5G access network (NG-RAN), and 5G core network (5GC).

UE. UE is the cellular device equipped with a universal subscriber identity module known as USIM. In the 5G network, SUPI (Subscription Permanent Identifier) is a user's permanent identity. Each USIM is uniquely identified by its SUPI, similarly to 3G and 4G networks, and USIM was identified by its IMSI (International Mobile Subscriber Identity). SUPI is never transmitted in the open-air interface to avoid leakage.

5G-RAN. In 5G, a geographical area is divided into hexagonal cells, with each cell served by a gNB (5G base station), which connects nearby cellular devices to the internet via the carrier's core network.

5G-CN. The 5G core network, as defined by 3GPP, employs cloud-aligned, service-based architecture (SBA) that spans all 5G functions and interactions, including authentication, security, session management, and traffic aggregation from end devices. We now describe those 5G components relevant to our discussion, i.e., the AMF (Access and Mobility Management Function) and the UDM (Unified Data Management).

(1) AMF: AMF is one of the essential network elements in the 5G core network, which is responsible for registration management, connection management, reachability management, and mobility management in 5GS, as well as NAS message ciphering and integrity protection

(2) UDM: UDM is primarily in charge of generating 3GPP AKA authentication credentials, storing and managing all user identity information (SUPI) in the 5G system, and decrypting SUCI

2.2. Attach Procedure with NAS Security and AS Security. 5G divides UE management into nonaccess stratum (NAS) and access stratum (AS). The NAS layer protocol manages the connection between UE and the core network (AMF), whereas the AS layer protocol manages the radio layer between UE and gNB using the Radio Resource Control (RRC) protocol. NAS security ensures that the signaling between UE and AMF can be transmitted securely on the control plane, while AS security aims to deliver RRC messages and IP packets securely.

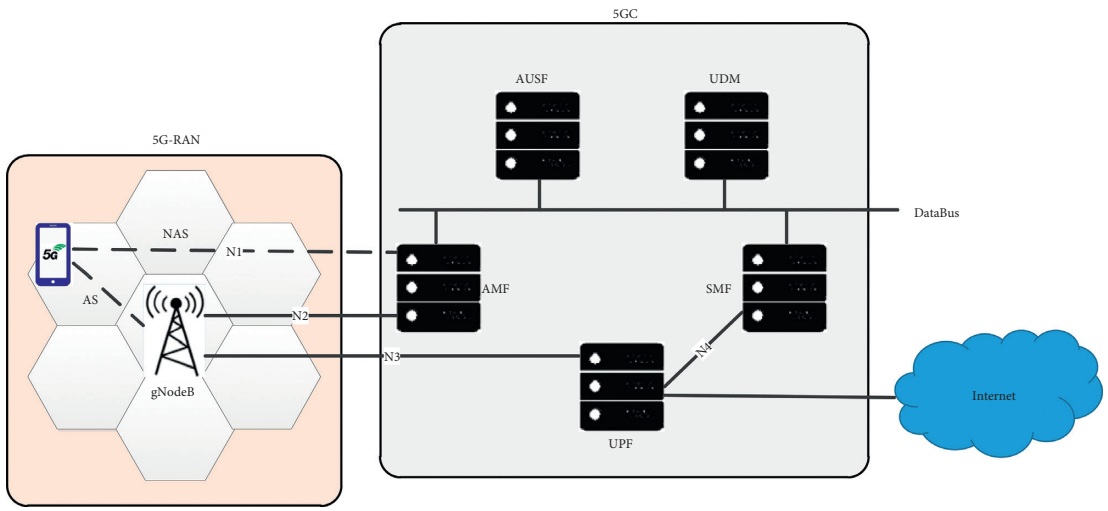

Figure 1: The 5G network architecture.

The UE must perform an initial attach procedure to access the 5G network, initiating all protocol layers from the NAS layer up to the AS layer. We assume that the UE and the gNB already established a radio connection in terms of our proposal. Figure 2 depicts the initial attach procedure with NAS security and AS security, which runs as follows:

(1) The UE initially sends the Attach Request message with the SUPI or SUCI to identify and the supported security algorithms included in the Security Capabilities.

(2) The authentication and key agreement establishes mutual authentication. The AMF sends an Authentication Request message that contains a random nonce (RAND) and an authentication token (AUTN) to the UE when it receives an authentication challenge generated by the UDM. The UE verifies the authentication token, computes, and returns the network-verified response RES.

(3) To enable the NAS security mechanism, the AMF selects ciphering and integrity algorithms based on the UE Security Capabilities, generates the NAS Security Mode Command message via the selected security algorithms, and sends the integrity-protected NAS Security Mode Command message to the UE. The UE confirms with a NAS Security Mode Complete message. Notice here that the NAS Security Mode Command message is integrity protected but not ciphered. Besides, it indicates the selected security algorithms and a replay of the original UE Security Capabilities to prevent algorithm downgrade attacks.

(4) The network finally assigns an IP address with the Attach Accept message and contains UE Security Capabilities in the Attach Accept message to initiate the AS security mechanism.

(5) For initiating the AS security mechanism, the gNB generates the AS Security Mode Command message based on the selected security algorithms contained in the Attach Accept message and sends it to the UE. The UE acknowledges with an AS Security Mode Complete message. One thing to note here is that the AS Security Mode Complete message is integrity protected but not ciphered.

2.3. Security Algorithm Selection. According to the above analysis, we can see that the selection of security algorithm is significant for the security protection of the air interface signaling. 5G supports three ciphering and integrity protection algorithms, known as New radio Encryption Algorithm (NEA) and New radio Integrity Algorithm (NIA). NEA1 and NIA1 use the SNOW 3G cipher, NEA2 and NIA2 lean upon AES, and NEA3 and NIA3 rely on ZUA. The null algorithms NEA0 and NIA0 disable security, allowing data to be transmitted unprotected. They enable emergency calls to be made in the absence of a valid USIM and, as a result, a valid key. Integrity protection is crucial to ensure the authenticity of exchanged messages, and it continuously demonstrates that both parties have valid keys.

3. Applied Systematic Approach

In this section, we will describe the systematic approach applied to analyze 5G network vulnerabilities.

The systematic approach applied is based on the principle of model checking. Model checking is an automated verification technology for analyzing dynamical systems that state transition systems can model. It verifies the desired behavioral property of a reactive system over a given system (the model) through exhaustively enumerating (explicitly or implicitly) all the states reachable by the system and the behaviors that traverse through them. Compared to simulation, testing, and other formal verification methods, the model checking method enjoys the following remarkable advantages: (a) it is entirely automated, and its use requires no user supervision or knowledge of mathematical disciplines such as logic and theorem proving. (b) When a design fails to satisfy the desired property, the model checking

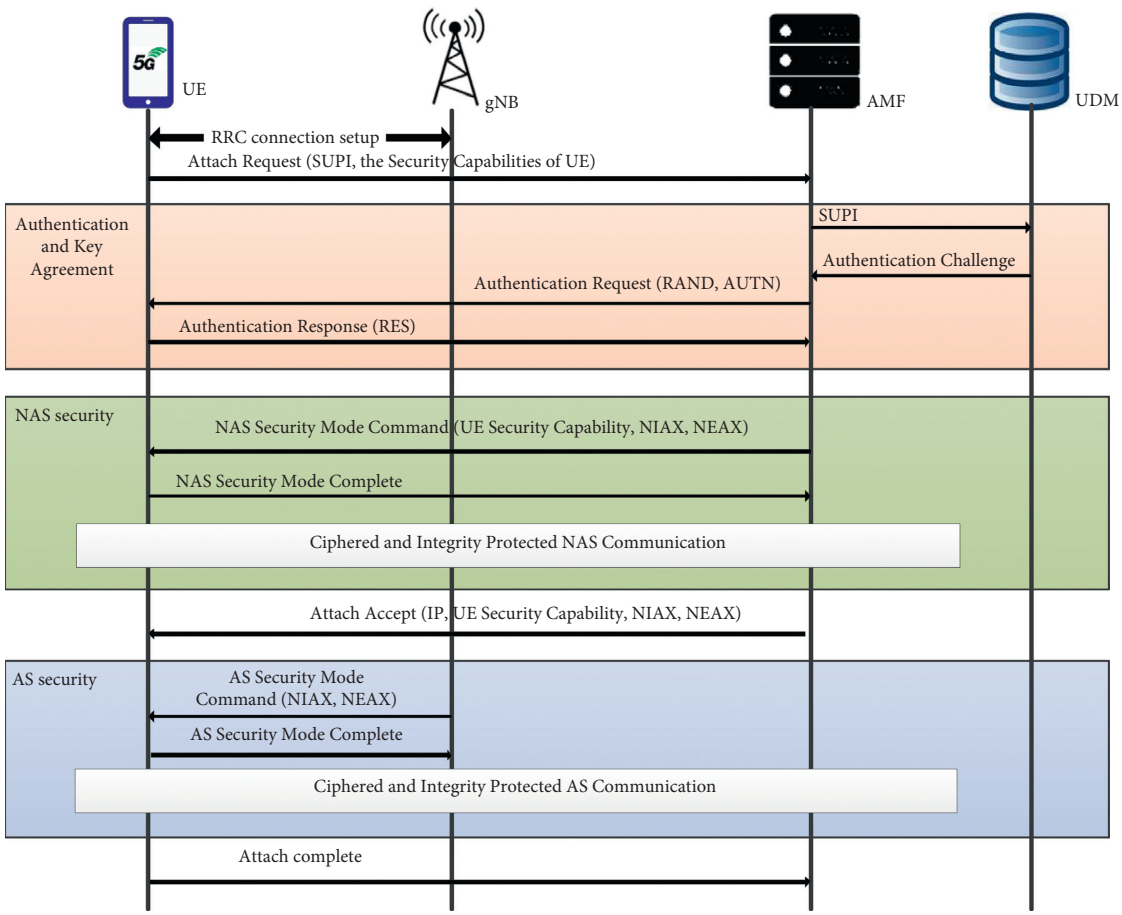

Figure 2: 5G attach procedure with NAS security and AS security.

process consistently produces a counterexample demonstrating behavior that falsifies the property. This faulty trace provides invaluable insight into the actual cause of the failure and crucial clues for resolving the issue.

These two significant advantages and the advent of symbolic model checking, which allows exhaustive implicit enumeration of an astronomical number of states, completely revolutionized the field of formal verification and transformed it from a purely academic discipline into a viable, practical technique that can potentially be integrated as an additional valuable method for design validation within many industrial development processes. Therefore, the model checking method is widely concerned by the academic. Moreover, it has been applied in many technical fields to verify the security and reliability of the system.

To analyze the security and reliability of the communication network efficiently and conveniently, the researchers designed a systematic approach based on the principle of the model checking method and used it to discover the design weaknesses resulting in attacks having security implications in the communication network. We lucubrate the work of literature [4, 6, 13] and summarize the operation flow of this approach. Figure 3 shows the operation flow of this approach. From Figure 3, we can see that this approach can be used to analyze the security and reliability of the network according to the following steps:

(1) *Modeling*. Firstly, we need to select the components of the network to be used to model synchronous communication finite-state machines (FSMs in Figure 3) according to the concerned procedure of the analyzed network protocols from 3GPP specifications. And then, abstract the protocol model according to the analyzed network protocols' behavior stipulated in the 3GPP specification (Step ① in Figure 3). Secondly, we select an adversary model (Step ② in Figure 3). Finally, we take the protocol model and modify it to incorporate the presence of an adversary to obtain a new model called threat model instrumentor (Step ③ in Figure 3).

(2) *Extract the Desired Property*. We need to combine 3GPP specifications to lucubrate the concerned procedure of the analyzed network protocols and figure out what properties we require. And then, we extract the desired properties from 3GPP specifications (Step ① in Figure 3).

(3) *Discover Attacks*. Firstly, we took the threat model instrumentor and desired property extracted into the model checker (Step ④ in Figure 3). Secondly, we used the model checker to verify whether there is an execution of the model which violates the property. If there was an execution that violates the execution

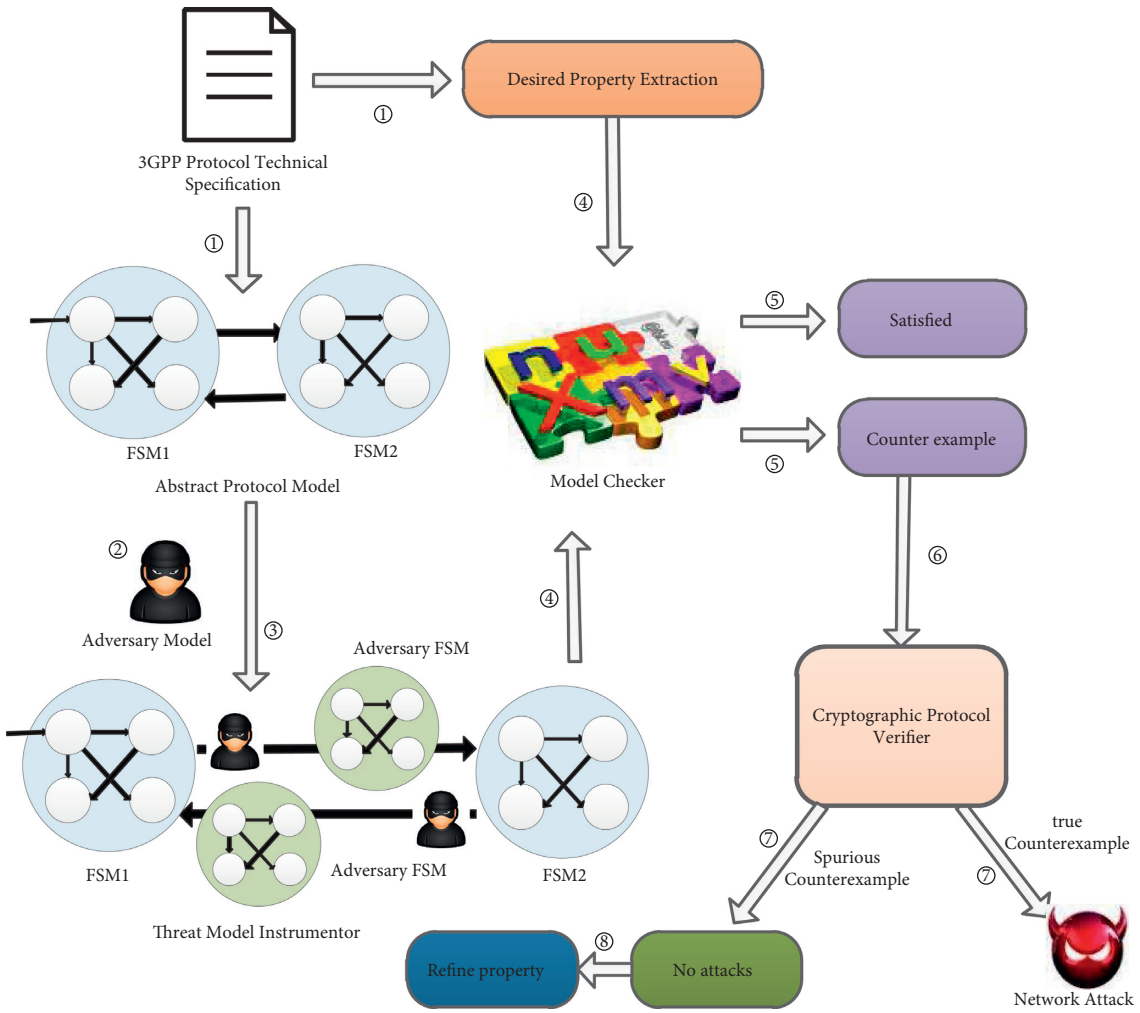

Figure 3: The operation flow of the applied systematic approach.

of the model, it provides a counterexample. Otherwise, we adjudicate the property to be satisfied by the model (Step ⑤ in Figure 3). Because of the abstraction, this counterexample may be spurious, so we need to distinguish it with a cryptographic protocol verifier CPVerif (Step ⑥ in Figure 3). If it confirms that all the actions included in the counterexample conform to the cryptographic assumptions and all adversarial actions can be proven feasible, the counterexample is recognized as an attack path (Step ⑦ in Figure 3). Otherwise, we conclude that it is a spurious counterexample, and we rule it out by refining the property (Step ⑧ in Figure 3).

4. Experiment

Section 3 has described the systematic approach applied in detail. Therefore, in this section, we will depict the process of modeling in our work and exhibit the desired properties extracted for analysis. Besides, we state the components of the test platform and their tasks in detail, respectively.

4.1. Modeling. In this section, we will elaborate on the process of modeling in our work. Firstly, we abstract the 5G protocol model from 3GPP specifications. Secondly, we select the Dolev–Yao-style network adversary as the adversary model through consulting the literature. Finally, we take the 5G protocol model and modify it to incorporate the presence of an adversary to obtain a new model called threat model instrumentor. The threat model instrumentor will be used to take into the model checker for detection.

4.1.1. Protocol Model. In the process of verifying the security and reliability of the system via using the model checking, building the system model is the first and the most crucial step. Clarke mentioned in [14] that if the refinement degree of the model is too high, in other words, too many details contained in the model, it will lead to the explosion of state space. As a result, there may be too many spurious counterexamples, which will reduce the checking efficiency. On the contrary, if the refinement degree of the model is too low, the accuracy and validity of the checking will be reduced. Therefore, the system model should present the real system

exactly and eliminate the details that have nothing to do with the nature to be tested but would complicate checking.

Our research work focuses on selecting the security algorithms, i.e., we verify whether the security vulnerability that NEA0 and NIA0 can be used in the normal communication procedure still exists in the 5G mobile communication system. Because the 5G mobile communication system is an amalgamation of multiple protocols, it is very complex. So, we just only choose UE and AMF as the major participants of the system protocol model and model them into two synchronous communication finite-state machines (FSMs) M_{UE} and M_{AMF}, respectively. Because the UE and the AMF communicate with each other by sending messages through a public bidirectional communication channel in the real system, we model this bidirectional channel with two unidirectional channels between M_{UE} and M_{AMF}; one from M_{UE} to M_{AMF} and another from M_{UE} to M_{AMF}. Notice here that the reason we model the public channel between UE and AMF with two unidirectional channels between M_{UE} and M_{AMF} but not a bidirectional channel between M_{UE} and M_{AMF} is the following: (a) for modeling convenience; (b) for effortlessly modeling the weaker adversary model during adversary model instrumentation.

Although there are other protocol participants, such as gNB and UDM, for ease of modeling, we combine their functionality within the AMF as their identity distinction does not affect the analysis of the selection of security algorithms.

In our work, we study the security of relevant protocol behaviors of the attach procedure in the 5G mobile communication network by analyzing the signaling interaction process and security mechanism. We model signaling messages as a possible message type for ease of research instead of modeling message data with arbitrarily large domains. For example, the Attach Request message can contain SUPI as data, and we can model the value of the SUPI as a data domain. However, this is not how our model is designed. In our model, we model it with a possible message type. In addition, we model message data-dependent conditions as environment-controlled Boolean variables. For instance, we capture the integrity verification of each message that can have integrity protection with a unique Boolean variable mac failure, the value of which is nondeterministically set by the environment during model checking. For the sake of elaboration, Figure 4 shows the state transition of the part of our model. As we can see from Figure 4, transition labels are of the form "condition/actions," in which the condition component is a propositional logic formula that specifies the condition under which the transition will be triggered. In contrast, the actions component is a sequence of actions that the FSM will perform (in their appearance order) after the transition is taken.

4.1.2. Adversary Model. In order to facilitate the security analysis of the security algorithm selection in the 5G mobile network, we consider using the Dolev-Yao-style network adversary [15] as the adversary model. This model can drop, inject, or modify any messages in the public communication channel and impersonate a legitimate protocol participant in case of adhering to cryptographic assumption. In addition, cryptographic constructs are considered to be perfectly secure in our model.

4.1.3. Threat Model Instrumentor. The threat model instrumentor takes a general protocol model M as the input and obtains another new model M_{adv} that is an extension of M incorporated in the presence of an adversary. Given a public unidirectional channel C_1 between M_1 and M_2, we assume that the instrumentor introduces a new state machine M_{a} to capture the adversary's behavior. In other words, for a given input message signaling, the adversary can randomly delete or change the received message signaling, and the adversary can choose any strategy to attack the network protocol. The state machine M_{a} uses two unidirectional channels $C_{1\mathrm{a}}$ and $C_{\mathrm{a}2}$ to replace C_1, and channel $C_{1\mathrm{a}}$ carries data from the state machine M_1 to M_2, while $C_{\mathrm{a}2}$ transmits data from the state machine M_2 to M_1. Figure 5 shows the threat model instrumentor.

4.2. Property Extraction Principles. We need to verify properties that include authenticity, availability, integrity, encrypt, privacy, and replay protection. Therefore, we extract the properties that need to be checked from 3GPP specifications. Our work has three types of properties: state transition, authentication, and signaling message security protection. We describe how we extract these properties in the following.

For state transition properties, usually, the state machine of the 5G protocol participating entities can perform state transition so that 3GPP promises without being interrupted, disturbed, or cheated. So, we extract state transition properties based on the transfer relationship between the state machines that we had built in the previous steps. For example, we can extract a property that a UE in the disconnected state will enter the state of waiting for an authentication request.

For authentication properties, we extract the principles concerning TS 33.501 [16] in the following: (1) the serving network needs to authenticate the SUPI in the process of authentication and key agreement between UE and network in subscription authentication. (2) The serving network identifier must be authenticated by the UE using implicit key authentication in serving network authentication. (3) The UE must be authorized by the serving network using the subscription profile obtained from the home network, and the authenticated SUPI is used for UE authorization in UE authentication. (4) The network shall ensure that UE can connect to the access network authorized by the service network and provide services to the UE. This authorization is necessary in order to establish access network security successfully. The authorization of access networks applies to all types of access networks.

For signaling message security protection properties, we extract the principles concerning TS 33.501 [16] and TS 24.501 [17] in the following: (1) the UE needs support ciphering of the signaling and support integrity protection and replay

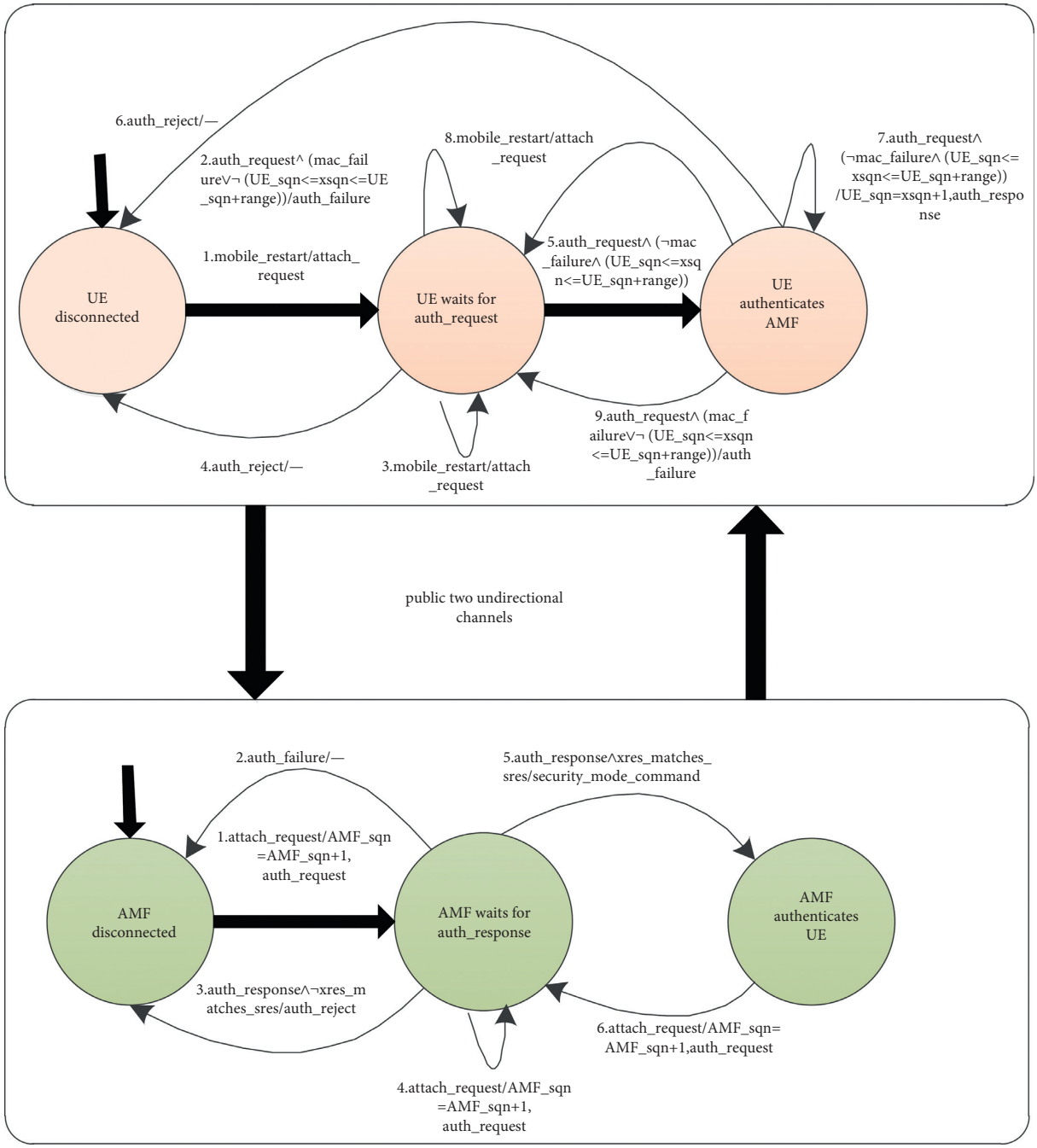

Figure 4: Simplified protocol model schematic.

protection of the signaling. (2) Confidentiality protection of the signaling is optional to use. (3) Except for routing information, such as the Mobile Country Code (MCC) and Mobile Network Code, the SUPI should not be transmitted in clear text over NG-RAN (MNC). (4) Within the UE, the long-term key of the subscription certificate (i.e., K) should be encrypted and integrity protected using tamper-proof security hardware components, and the long-term key of the subscription certificate should never be obtained explicitly outside of the tamper-proof security hardware components. (5) Mobile devices shall support the null scheme. (6) Attach Request message sent by the UE to the network is not protected by encryption and integrity in the attach procedure. (7) The Attach Reject message sent by the core network to UE can be accepted by the UE without any integrity protection.

4.3. Test Platform

4.3.1. Model Checker. In our work, the model checker takes the threat model instrumentor M_{adv} and a desired abstract property ϕ as the input and checks whether all possible executions of M_{adv} satisfy ϕ while considering all possible values of the environmental variables. If the model checker finds an execution of M_{adv} which violates ϕ, it outputs this

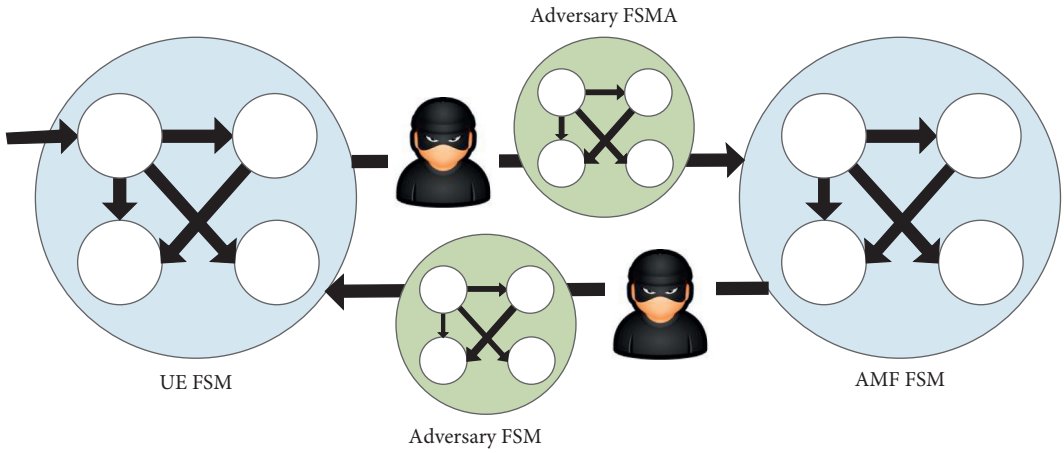

Figure 5: Threat model instrumentor.

execution as the counterexample. This execution of M_{adv} includes the adversary actions used to violate ϕ, and it can be regarded as the attack strategy. To model check our state machine presentation, we use nuXmv [18] to finish that. nuXmv is a new symbolic model checker based on the development of NuSMV, which can be verified on finite-state systems using some algorithms of SAT and on infinite-state systems (such as systems containing real or integer variables) using SMT technology for verification.

4.3.2. Cryptographic Protocol Verifier. This counterexample may be spurious due to the abstraction, so we need to use the cryptographic protocol verifier to rule out the spurious counterexample. For a given counterexample, it includes the adversary actions used to violate the desired abstract property used to model check, so we verify whether all adversarial actions can be proven feasible. If so, the counterexample is presented as a feasible attack. However, if the ProVerif adjudicates one of the actions taken by the adversary to be infeasible, we refine the property to assure that the adversary does not perform the infringing action in subsequent verification iterations. The verification loop is repeated until the model either fulfills the property or finds a realizable counterexample. In our work, we use ProVerif [19] as the cryptographic protocol verifier. ProVerif is a formal automatic verification cryptographic protocol tool based on the Dolev–Yao model, and it can support unbounded parallel sessions, cryptographically sophisticated adversaries, and rich constructs.

5. Experiment Result

This section details the attacks discovered by our applied systematic approach and introduces each attack from four aspects: adversary assumptions, vulnerability, attack procedure, and implications.

5.1. IP Spoofing Attack

5.1.1. Adversary Assumptions. For successfully carrying out this attack, the adversary is required to set up a malicious gNB and a malicious UE. When the network attacker wants to launch an attack against victim UE, it will adsorb the victim UE to the fake base station with strong signal power. Note that the attacker does not initially own any information about the victim UE, such as SUPI and the encryption key.

5.1.2. Vulnerability. Through the study of 3GPP TS 33.501 [16] and 3GPP TS 24.501 [17], we can find that the Attach Request message sent by UE to the core network is not protected by encryption and integrity, and the Attach Reject message sent by the core network to UE can be accepted by the UE without any integrity protection. Therefore, we model check M_{adv} against these properties and the state transition properties relevant to the NAS security mechanism. It is trivially violated by a counterexample in which the adversary can manipulate the Security Capabilities of the victim UE when the victim UE sent the Attach Request message to the core network, and the adversary can set the highest priority of the null security algorithm (i.e., NEA0 and NIA0) or delete other nonnull security algorithms and only keep the null security algorithm. Afterward, when the AMF receives the Attach Request message manipulated, the NAS security mechanism will be initiated, and the network guarantees the secure transmission of NAS signaling by establishing the security context. However, because the core network does not perceive the Attach Request message has been manipulated by the adversary, it will configure network parameters according to the security algorithm included in the Attach Request message received, select null security algorithm (i.e., NEA0 and NIA0) as the security algorithm of signaling, and complete the NAS security mechanism. Because null security algorithm (i.e., NEA0 and NIA0) is only a security algorithm informal, it cannot provide any encryption protection or integrity protection. So, the use of null security algorithm (i.e., NEA0 and NIA0) in normal communication can make control plane signaling messages free from encryption protection and integrity protection, in which the network attackers will exploit it to launch network attacks. In addition, when the victim UE receives the Attach Reject message sent by the adversary, it will be disconnected from the network until it is rebooted.

5.1.3. Attack Procedure. The complete attack procedure is shown in Figure 6. To prepare for the attack, the adversary first needs to construct a malicious UE and a malicious gNB, and then it uses strong signal power adsorbing the victim UE. First, the victim UE initiates the attach procedure by sending the Attach Request message to the core network, but because the Attach Request message does not have any encryption protection and integrity protection, at this time, the adversary manipulates the parameter, which is the Security Capabilities included in this message and changes the supported algorithms to NIA0 and NEA0 or sets the priority of the null algorithm to the highest. After doing this, the adversary sends this message to the AMF. Then, the core network sends the Authentication Request message to initiate the authentication procedure. The adversary transmits this message and Authentication Response message, in which the victim UE sends when it completes the authentication between the victim UE and the core network. Afterward, the core network selects NEA0 and NIA0 as the security protection algorithms and uses them to generate the NAS Security Mode Command message. Therefore, the subsequent communication does not need to have any valid key, and the adversary exchanges the signaling message with the core network in the plaintext without any encryption protection and integrity protection. The core network eventually assigns an IP address included in the Attach Accept message sent by the AMF to the victim UE, and then the malicious gNB obtains the Attach Accept message and establishes an IP connection with malicious UE. Meanwhile, the adversary sends the Attach Reject message to the victim UE, causing the victim UE to disconnect from the core network until it restarts or reinstalls the SIM card. However, the malicious UE gets the internet services, while the mobile data charging center will charge the victim UE according to the usage of these network services.

5.1.4. Implication. The adversary forces the victim to use NEA0 and NIA0 at the NAS layer, allowing the adversary to communicate with the core network without any valid keys and launch a network attack from that. The malicious UE can successfully establish an IP connection with the core network, surf the internet, and charge the victim UE. However, the victim UE is denied access to the core network until it restarts or reinstalls the SIM card.

5.2. SUPI Catching Attack

5.2.1. Adversary Assumptions. We assume that the adversary can construct a communication channel between the victim UE and the legitimate network via forging a malicious gNB and a malicious UE, and it already knows the C-RNTI of the victim UE.

5.2.2. Vulnerability. Through the study of 3GPP TS 33.501 [16] and 3GPP TS 38.331 [20], we can find the following: (1) the Attach Request message sent by the UE to the core network in the attach procedure does not have any encryption protection and integrity protection. (2) Moreover, if the base station requires the access stratum (i.e., AS layer or RRC layer) security context to be set up, the base station will eventually establish the security context. (3) The base station and UE continue using the security configuration before the reception of AS Security Mode Command message, neither NEA0 nor NIA0. However, 3GPP TS 33.501 mentions that the null integrity protection algorithm is used only for control plane messages and for UE in the limited service mode. Therefore, we mode check M_{adv} against these properties.

The model checker yields a counterexample in which the adversary can manipulate the UE Security Capabilities and make the victim UE enable the null security algorithms in normal communication so that the control plane signaling messages in the NAS layer and AS layer are free from encryption protection and integrity protection. And then, it can pretend to be the victim UE sending the AS Security Mode Failure message in response to the AS Security Mode Command message. We confirm this attack trace with the cryptographic protocol verifier and find that the adversary exploits the lack of integrity protection in the AS Security Mode Failure message. AS Security Mode Failure message is a signaling message that the victim UE sends to the base station when it cannot verify the AS Security Mode Command message. Using NEA0 and NIA0 in the AS layer allows the adversary to see and inject any control plane messages, which makes the adversary inject the AS Security Mode Failure message in the AS layer's security mode procedure. The adversary injects the AS Security Mode Failure message and sends it to the legitimate gNB. Meanwhile, it intercepts and discards the AS Security Mode Complete message sent by the victim UE. As a result, the AS security mechanism is not completed successfully, and the RRC messages (i.e., AS messages) delivered between UE and gNB after that are not integrity protected and encrypted protected. Furthermore, because the Identity Request message is transmitted in the plaintext, the adversary can expose the SUPI of the victim UE by injecting the Identity Request message to the victim UE. On account of this, SUPI is the unique subscription permanent identifier for UE in the 5G network. Therefore, when the adversary gets it, the adversary can use it to identify, locate, and track the victim UE, which leads to the disclosure of privacy.

5.2.3. Attack Procedure. Figure 7 depicts the complete attack procedure. In the first phase, the adversary deploys a malicious gNB near the target cell with a strong signal, and the victim UE will release the previous RRC connection and connect to it. Meanwhile, the adversary constructs a malicious UE to set up an RRC connection with the legitimate gNB. Thus, there is a communication channel between the victim UE and the legitimate network. In the second phase, when the victim UE sends the Attach Request message to initiate the attach procedure, the malicious gNB intercepts and modifies this message and sends the manipulated

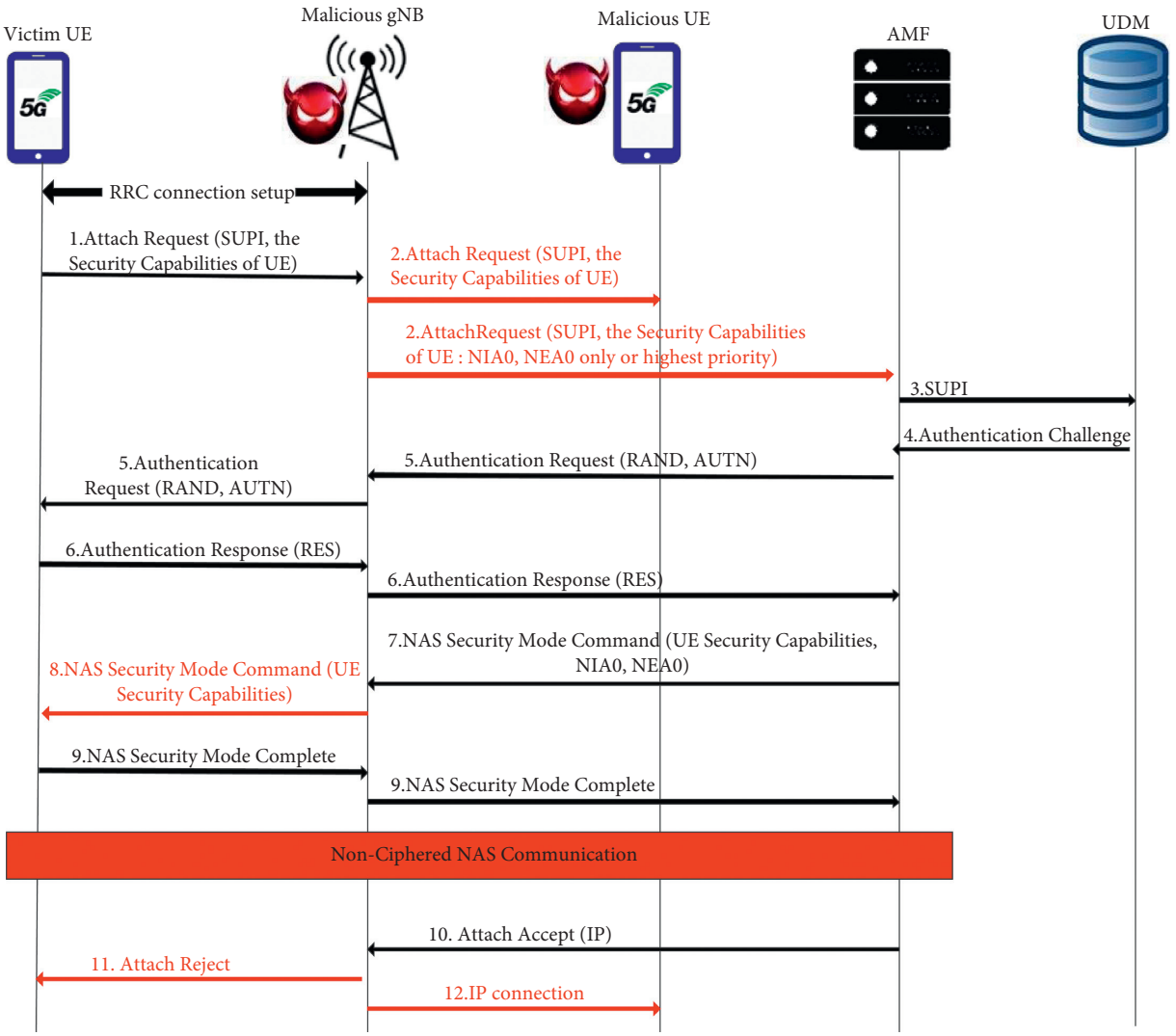

Figure 6: IP spoofing attack.

message to the malicious UE. Subsequently, the malicious UE sends this message to the legitimate gNB by pretending to be a legitimate UE and accomplishes the authentication procedure with the core network. This process will transmit the authentication request message received from the core network to the victim UE through the malicious gNB and deliver the Authentication Response message sent by the victim UE to the malicious gNB to the core network. Afterward, the AMF selects NEA0 and NIA0 as the security algorithms and initiates the NAS security mechanism with the null security algorithm. Hence, all the control plane signaling messages in the NAS layer and AS layer are not protected by any encryption and integrity. Therefore, the adversary can see and inject any control plane signaling messages in the AS layer. So, in the third phase, the adversary receives the AS Security Mode Command message sent by the legitimate gNB and delivers it to the victim. Hereafter, the adversary discards the AS Security Mode Complete message sent by the victim UE and injects the AS Security Mode Failure message to the legitimate gNB. Finally, the adversary injects an Identity Request message to the victim UE and obtains the SUPI of the victim UE. The adversary can use the SUPI to identify, locate, and track the victim UE and cause the privacy disclosure of UE.

5.2.4. Implication. The adversary compels the victim UE to use NEA0 and NIA0 at the AS layer by manipulating the UE Security Capabilities included in the Attach Request message, causing any control plane messages in the AS layer to be injected or seen by it. In this attack, the adversary sends the Identify Request message to the victim UE and makes the victim UE expose its SUPI in the plaintext. And then, the adversary can obtain the SUPI of the victim UE and use it to identify, locate, and track the victim UE, which leaks the victim UE identity.

6. Root Cause and Countermeasure

This section will discuss the root causes of the vulnerabilities mentioned above and propose a countermeasure.

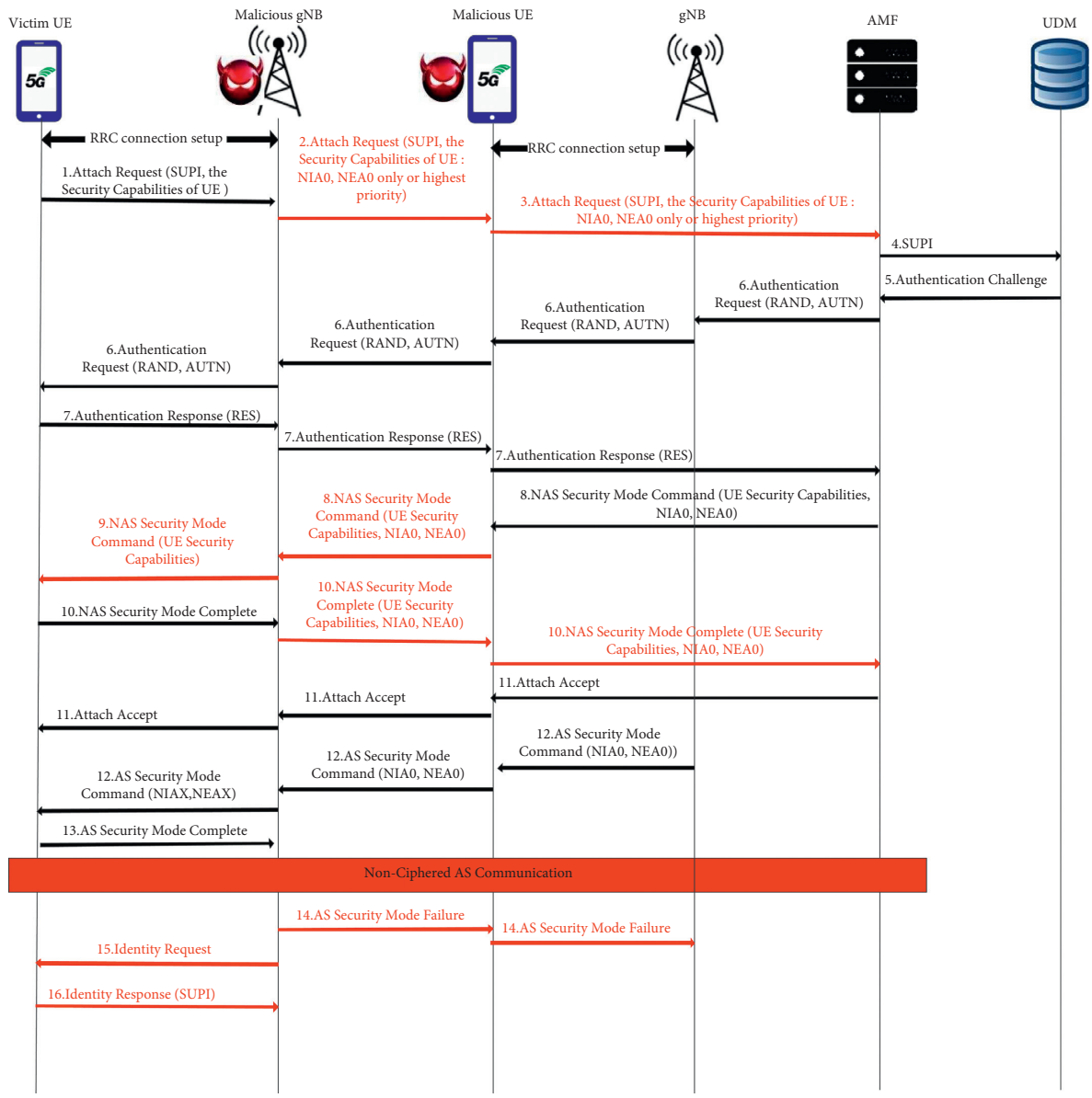

Figure 7: SUPI catching attack.

6.1. Root Cause Analysis. Technically analyzing the mentioned attacks, we discover that the root causes mainly remain in the following areas:

(1) The encryption and integrity algorithms of the wireless air interface channel are not strong enough. Before the authentication process of the mobile communication network, all signaling messages between the UE and the core network are not encrypted and do not have any integrity protection and any authentication.

(2) The UE and the core network are fully trusted so that the adversary can make malicious use of the signaling message during this period and launch network attacks. The mobile communication network is the central architecture of the network, and the majority of communication business decision-making processes are initiated and implemented by the core network. If the UE cannot verify the authenticity of the access network, the absolute trust of the UE to the core network will reduce the technical difficulty of the fake network deception quickly. Therefore, network attackers can infiltrate the core network by building fake base stations and launch network attacks, which are effective even in the current 5G network with a relatively perfect security mechanism.

(3) Almost all generational mobile communication network systems remain null encryption algorithm and null integrity protection algorithm, which are used to remove encryption measures in the case of poor wireless channel quality or in emergency communication scenarios to achieve communication tasks, such as UEA0 algorithm and UIA0 algorithm for the UMTS network, EEA0 algorithm and EIA0 algorithm for the

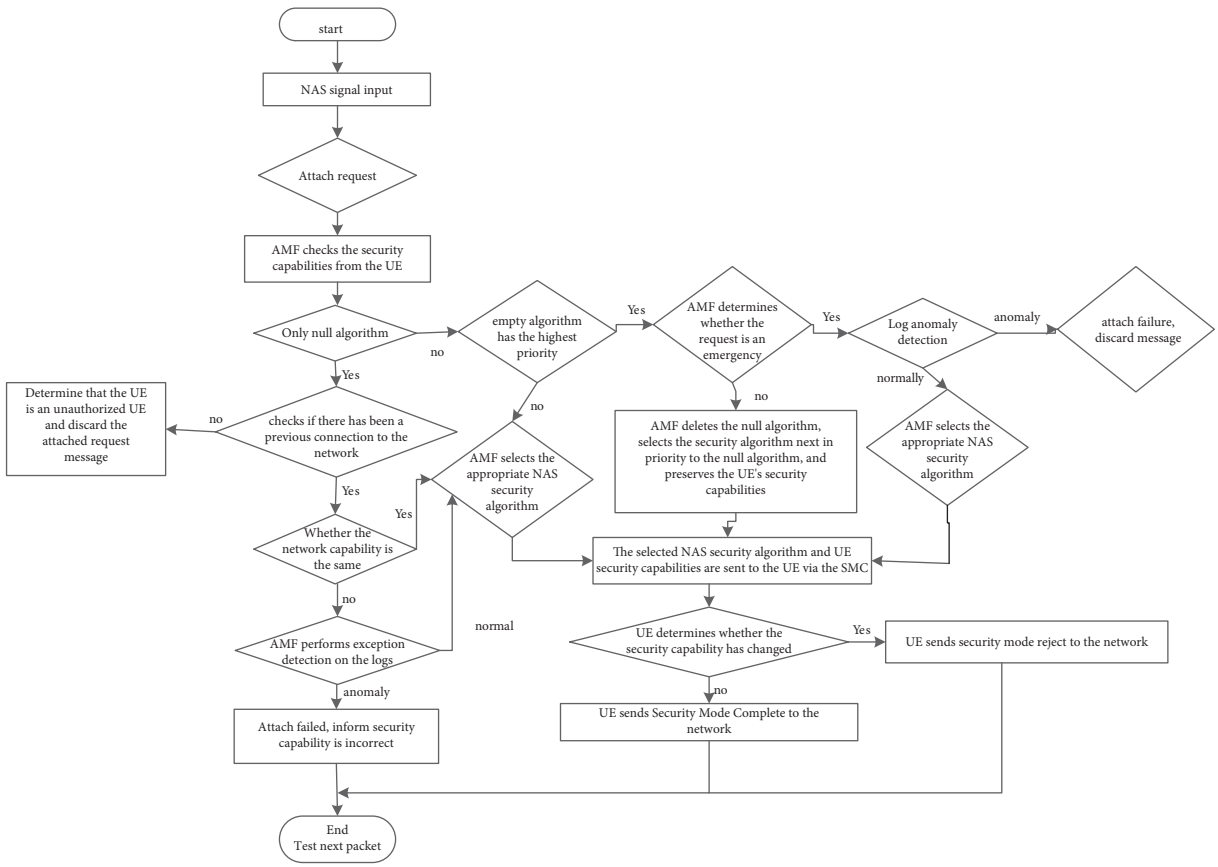

Figure 8: Flowchart of the anomaly detection method.

LTE network, and NEA0 algorithm and NIA0 algorithm for the 5G network. Because the core network element AMF is responsible for selecting the encryption algorithms ultimately, UE does not perceive whether the encryption measures have been used. Therefore, all kinds of mobile communication network standards stipulate that UE should have encryption prompts, and there should be warnings if encryption measures are not used. However, virtually all mobile operators and terminal equipment manufacturers have not implemented these standard requirements.

6.2. Countermeasure. We now discuss the potential countermeasure to the vulnerabilities that we discovered. First, we propose an anomaly detection method to prevent the adversary from attacking the network that manipulates UE network capability and initiates NEA0 and NIA0 in normal communication. Figure 8 shows a flowchart of the anomaly detection method, and Table 2 summarizes the data used for it. When the network receives the Attach Request message from the UE, AMF checks the Security Capabilities of this message. Therefore, according to the parameters of UE security capability, the anomaly detection is divided mainly into the following three cases: normally, only the null algorithm, and the null algorithm has the highest priority.

If the Security Capabilities of this message support only the null encryption algorithm or null integrity algorithm, whether there are previous connection records is checked through the SUPI of the UE, and the previously received UE network capability and the current UE network capability are compared. If these capabilities are the same, the AMF will select the corresponding security algorithm to UE according to the Security Capabilities of the message, and the core network will send a Security Mode Command (SMC in Figure 8) that includes the selected security algorithm and UE Security Capabilities to UE. Then, UE estimates the Security Capabilities from core network changes; if not, UE will send a Security Mode Complete message to the core network. Otherwise, UE will send a Security Mode Reject message to the core network. If these capabilities are different, AMF will perform the anomaly detection (the required data are shown in Table 2), and if an exception is detected, attach procedure fails, and the system informs UE that the Security Capabilities are incorrect. Otherwise, the AMF will select the corresponding security algorithm to UE according to the Security Capabilities of the message, and the core network will execute the same operations described above.

If the Security Capabilities of this message support that the null encryption or null integrity has the premier priority, AMF decides whether this message is an emergency Attach Request message. If not, AMF will detect null encryption algorithm or null integrity algorithm, select the security algorithm whose

Table 2: Required data for anomaly detection.

Type	Field	Description
User information	SUPI	Identification of UE
	MSISDN (Mobile Station ISDN)	Phone number of UE
	User IP version	IP version of UE
	User IPv4	IPv4 address of UE
	User IPv6	IPv6 address of UE
	Tracking area identity (TAI) list	Base station list in which UE can access for analyzing the UE location
NAS message information	Attach request time	Time of the Attach Request message
	Attach reject cause	Cause of the Attach Reject message
	Attach request type	Type of Attach Request 1.5GS attach 2.combined 5GS/SUPI attach 6.5GS emergency attach
	Security Mode Command Time	Time of the Security Mode Command message
	Security Mode reject cause	Cause of the security mode reject message
	UE network capability	NEA, NIA configurations of UE
	Selected NEA/NIA	Selected NEA/NIA mode by AMF

priority is next only to the null encryption algorithm or null integrity algorithm, and save the UE Security Capabilities. Hereafter, the AMF will select the corresponding security algorithm to UE according to the Security Capabilities of the message, and the core network will send a Security Mode Command (SMC in Figure 8) that includes the selected security algorithm and Security Capabilities to UE. Then, UE estimates the Security Capabilities from core network changes. If not, UE will send a Security Mode Complete message to the core network. Otherwise, UE will send a Security Mode Reject message to the core network. Otherwise, AMF will perform the anomaly detection (the required data are shown in Table 2), and if an exception is detected, attach procedure fails and the system discards this message. On the contrary, suppose the anomaly detection does not discover an exception. In this case, the AMF will select the corresponding security algorithm to UE according to the Security Capabilities of the message, and the core network will execute the same operations described above.

If the above two cases do not occur in the core network, when AMF receives the Attach Request message sent by UE, the AMF will select the corresponding security algorithm to UE according to the Security Capabilities of the message. First, the core network will send a Security Mode Command (SMC in Figure 8) including the selected security algorithm and UE Security Capabilities to UE. Then, UE estimates the Security Capabilities from core network changes. If not, UE will send a Security Mode Complete message to the core network; otherwise, UE will send a Security Mode Reject message to the core network.

7. Conclusion

In this paper, we apply a systematic approach based on the principle of model checking to analyze the 5G security vulnerability. We model UE and AMF into two synchronous communication finite-state machines, extract the desired properties from 3GPP relevant specifications, and construct an adversary model to test the system's security. By observing the operation of state machines and analyzing relevant protocol behavior, we demonstrate that the null security algorithm (i.e., NEA0 and NIA0) used in normal communication exists and remains a security threat in the 5G network, and it can lead to IP spoofing attack and SUPI catching attack. In addition, we analyze the root cause of these network attacks and propose an anomaly detection method to avoid these attacks from being launched.

In the future, we will improve our 5G protocol model to make it amenable to automated reasoning by exploring different new forms of abstraction that achieve the right balance between behavioral accuracy and analysis scalability. In addition, because there is no open-source 5G protocol stack that can test our attacks in a testbed, we do not have access to any 5G commercial networks or cellular devices to verify our work attacks. Therefore, in the future, we will use open-source 5G protocol stack and 5G commercial networks to test the security vulnerabilities, verify network attacks, and test the performance of our proposed countermeasures against security threats.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Key Laboratory Fund (Grant no. 6142106200103).

References

[1] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information," in *Proceedings of*

the Network and Distributed Systems Security (NDSS) Symposium 2019, San Diego, CA, USA, March 2019.

[2] R. Piqueras Jover, V. Marojevic, and V. Marojevic, "Security and protocol exploit analysis of the 5G specifications," *IEEE Access*, vol. 7, pp. 24956–24963, 2019.

[3] 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 *Proceedings of the 23rd Annual Network Distribution System Security Symposium (NDSS)*, San Diego, CA, USA, January 2016.

[4] S. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "LTEInspector: a systematic approach for adversarial testing of 4G LTE," in *Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2018*, San Diego, CA, USA, February 2018.

[5] R. Borgaonkar, A. Shaik, N. Asokan, V. Niemi, and Jean, "LTE and IMSI catcher myths," Proc. of BlackHat Europe, 2015.

[6] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "5GReasoner: a property-directed security and privacy analysis framework for 5G cellular network protocol," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, London, November 2019.

[7] A. Shaik, R. Borgaonkar, S. Part, and J.-P. Seifert, "New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 221–231, Miami, FL, USA, May 2019.

[8] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2017.

[9] Y. Xu, J. Liu, Y. Shen, X. Jiang, Y. Ji, and N. Shiratori, "QoS-aware secure routing design for wireless networks with selfish jammers," *IEEE Transactions on Wireless Communications*, vol. 20, 2021.

[10] Y. Xu, J. Liu, Y. Shen, Y. Jun Liu, X. Jiang, and T. Taleb, "Incentive jamming-based secure routing in decentralized internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 3000–3013, 2020.

[11] J. D. V. Sánchez, L. Urquiza-Aguiar, M. C. P. Paredes, and D. P. M. Osorio, "Survey on physical layer security for 5G wireless networks," *Annals of Telecommunications*, vol. 76, no. 3, pp. 155–174, 2021.

[12] M. Chlosta, D. Rupprecht, T. Holz, and C. Pöpper, "LTE security disabled: misconfiguration in commercial networks," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, Miami, FL, USA, May 2019.

[13] X. Hu, C. Liu, S. Liu, W. You, Y. Li, and Y. Zhao, "A systematic analysis method for 5G non-access stratum signalling security," *IEEE Access*, vol. 7, pp. 125424–125441, 2019.

[14] E. Clarke, O. Grumberg, S. Jha, Y. Lu, and H. Veith, "Counterexample-guided abstraction refinement," in *Proceedings of the International Conference on CompSuter Aided Verification*, pp. 154–169, Springer, Chicago, IL, USA, July 2000.

[15] D. Dolev and C. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1981.

[16] "Security architecture and procedures for 5G system (release 15)," *Document TS*, 3GPP, vol. 33.501, 2019.

[17] "Non-access-stratum (NAS) protocol for 5G system (5gs)(release 15)," *Document TS*, 3GPP, vol. 24, 2019.

[18] R. Cavada, A. Cimatti, M. Dorigatti et al., "The nuXmv symbolic model checker," in *Proceedings of the International Conference on Computer Aided Verification*, pp. 334–342, Springer, Los Angeles, California, USA, July 2014.

[19] B. Blanchet, "An efficient cryptographic protocol verifier based on prolog rules," *Csfw*, vol. 1, 2001.

[20] Nr; Radio Resource Control (Rrc), "Protocol specification,(release 15)," *Document TS*, 3GPP, vol. 38.331, 2019.