5G Handover: When Forward Security Breaks

Navya Sivaraman[a] and Simin Nadjm-Tehrani[b]
Department of Computer and Information Science, Linköping University, Sweden

Keywords: 5G Xn Handover Protocol, Forward Security, Protocol Verification, Formal Analysis.

Abstract: 5G mobility management is dependent on a couple of complex protocols for managing handovers, based on the available network interfaces (such as Xn and N2). In our work, we focus on the 5G Xn handover procedure, as defined by the 3GPP standard. In Xn handovers, the source base station hands the user equipment (UE) over to a target base station through two different mechanisms: horizontal or vertical key derivation. To ascertain the security of these complex protocols, recent works have formally described the protocols and proved some security properties. In this work, we formulate a new property, forward security, which ensures the secrecy of future handovers following a session key exchange in one handover. Using a formal model and the Tamarin prover, we show that forward security breaks in the 5G Xn handover in presence of an untrusted base station. We also propose a solution to mitigate this counter-example with a small modification of the 3GPP Xn handover procedures based on the perceived source base station state.

1 INTRODUCTION

In cellular networks, mobility management plays a vital role in maintaining mobile services with minimal latency while a user is moving from one location to another. Cellular networks rely on handover procedures to achieve this functionality (Bitsikas and Pöpper, 2021). Handover helps to transfer the User Equipment (UE) from one cell to another.

A handover is initiated by the source base station (source gNB in the 3GPP terminology) either when the current serving network is incapable of serving the UE or when the user moves along a continuous path towards a new gNB (which is known as target gNB). UE helps the source gNB to make a handover decision by providing signal measurements to the network via reports when it detects a more appropriate gNB (target gNB) (Bitsikas and Pöpper, 2021). These reports are known as measurement report.

We consider the handover procedures within a standalone fifth generation of mobile networks (5G) network, i.e., intra-system handover with 5G Radio Access Network (RAN) and 5G core. In comparison with other type of handovers, Xn handovers aim to be of lower latency due to less interaction with the 5G core network. However, security is also a key factor to be considered. Therefore, we mainly focus on the security properties of Xn handovers.

Our work aims to thoroughly study the different session key generation procedures during the 5G Xn handover. We use formal methods and the Tamarin prover, to create an abstract model of the 5G Xn protocol for the security analysis. Our work is not limited to verifying the secrecy of a single communication session during handover. Rather, we formulate a new security property (informally defined by the 3GPP standard), known as *forward security*, to verify the secrecy of future handovers. To the best of our knowledge, we are the first to formally define and verify the *forward security* property for 5G Xn handovers.

The contributions of this work are as follows:

- We provide an overview of how a strong adversary with access to a key generated at a base station can use the 3GPP standard operations to derive all future keys when the UE is outside its range.
- We formalize the threat model, security properties for Xn handovers, including the forward security property, and show how it breaks in this context using the Tamarin prover.
- We mitigate the threat, based on adopting of a slightly modified key derivation, depending on the perceived honesty of the base stations.

[a] https://orcid.org/0000-0003-0123-1970
[b] https://orcid.org/0000-0002-1485-0802

Sivaraman, N. and Nadjm-Tehrani, S.
5G Handover: When Forward Security Breaks.
DOI: 10.5220/0012128400003555
In *Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT 2023)*, pages 503-510
ISBN: 978-989-758-666-8; ISSN: 2184-7711

2 BACKGROUND

Cellular communication divides the geographical area into hexagonal cells. Each cell includes a base station (gNB) that serves the network. We use the term RAN interchangeably for gNB in this paper, i.e., SRAN and TRAN for source gNB and target gNB. The 3GPP defines the 5G Core Network (CN) architecture. It is a service-based architecture that constitutes several network functions (NF), such as Authentication Server Function, Access and Mobility Management Function (AMF), and so on (3GPP TS 33.501, V17.7.0, 2022).

AMF is a network function within the control plane that handles access authentication and authorization of handovers. This function is responsible for managing registration, detach procedures, paging, and services related to registration, connection, and mobility (Hussain et al., 2019). UE and RAN are separate entities from the 5G core architecture, thus unable to communicate directly with the AMF. Hence, they use secure network interfaces to communicate with AMF. For example, N1 is a network interface that allows interaction between the UE and AMF.

The handovers may differ according to how the source gNB and target gNB interact during the handover. Whenever the source gNB initiates a 5G intra-system handover request, it decides on either an Xn or N2 handover procedure based on the available interface. The availability of the network interface depends on the configuration that an operator chooses for running its RAN. The intention is that, the source gNB and the target gNB have minimal interaction with the 5G CN during the Xn handover.

2.1 5G Xn Handover Protocol

Every standard Xn inter gNB handover consists of three distinct stages, *Handover Preparation*, *Handover Execution*, and *Handover Completion*.

- *Handover Preparation*: During the *Handover Preparation* stage, the source gNB initiates transferring a UE to the target gNB through a *Handover Request* message. The *Handover Request* consists of the newly derived session key (K_{gNB*} and the target gNB ID). Then, the target gNB performs admission control and transmits a *Handover Acknowledge* message to the source gNB if the handover request is acceptable (3GPP TS 38.423, V17.1.0, 2022; 3GPP TS 33.501, V17.7.0, 2022).
- *Handover Execution*: The *Handover Execution* phase begins when the source gNB transmits the *Handover Command* message to UE (3GPP TS 33.501, V17.7.0, 2022), and this message contains information about the target gNB, such as target gNB ID. Once the UE receives the *Handover Command* message, it attempts to recompute the same session key K_{gNB*} and updates the signaling with the target gNB through the *Radio Resource Controller (RRC) Reconfiguration completion* message by encrypting with the session key K_{gNB*}.
- *Handover Completion*: In the final stage the UE content release and implementation of final bearers occur (Bitsikas and Pöpper, 2021). In this stage, the target gNB interacts with the AMF within 5G CN using *NGAP PATH SWITCH Request* and *NGAP PATH SWITCH Acknowledge* message to collect the the keying material. Thus, the AMF will compute the new next hop (NH) and next hop chaining counter (NCC) parameters for a future handover. Finally, the source gNB releases the UE content (3GPP TS 33.501, V17.7.0, 2022).

2.2 Session Key Generation

The generation of session key (K_{gNB*}) is a critical stage within the 5G handover procedure. The session key generation procedure may vary depending on the available keying parameters within the source gNB. There are two procedures, namely horizontal key derivation (hkd), and vertical key derivation (vkd).

2.2.1 Horizontal Key Derivation

In hkd, a new session key (K_{gNB*}) is derived from the source base station's key (K_{gNB}).

```
KgNB* = KDF (KgNB || TRAN_ID )
```

The key derivation function (KDF) takes the current key of the source base station (K_{gNB}) and the target base station's identifier (TRAN_ID) as input to derive the new session key K_{gNB*}.

2.2.2 Vertical Key Derivation

In vkd, a new session key (K_{gNB*}) is derived using the intermediate NH parameter transferred from AMF.

```
KgNB* = KDF (NH || TRAN_ID)
```

Hence, KDF takes the NH and TRAN_ID to derive K_{gNB*}. NCC acts as a counter of NH and increments after each handover.

In legitimate Xn-based handovers, the first session key is derived using hkd, followed by the vkd for future handovers if the source gNB has an unused $\{$ NH,NCC $\}$ pair (3GPP TS 33.501, V17.7.0, 2022).

2.3 The Tamarin Prover

The Tamarin prover is a state-of-the-art verification tool designed to analyze security protocols (Basin et al.,)(Peltonen et al., 2021)(Meier et al., 2013). Security protocols are programs that rely on cryptographic primitives to achieve secure communication over insecure networks. To prove the correctness of a security protocol, it is represented mathematically, either using a symbolic model or a computational model (Blanchet, 2012). The default underlying threat model of Tamarin is Dolev Yao (Dolev and Yao, 1983), a strong threat model with a powerful attacker who will be able to tamper with any publicly available information.

The Tamarin prover builds on symbolic modeling. It takes the formal model of the protocol, which includes the formalization of the threat model, and the properties to be verified as input. The tool attempts to prove the property by constructing a proof of correctness or returning a counter-example.

3 RELATED WORK

Various security features of 5G handover protocols, including the Xn handover, have been analyzed and formally verified. However, most of the recent works have been focusing on authentication and key secrecy features in 5G Xn handover.

Huang et al., and Yan et al., propose a new secure handover authentication protocol for 5G handovers based on the Chinese Remainder Theorem and formally prove its correctness using Burrows–Abadi–Needham logic (BAN logic) and Scyther tool (Yan and Ma, 2021)(Huang and Qian, 2020).

Peltonen et al. present the first comprehensive formal verification model of 5G handovers (Peltonen et al., 2021). They uphold a strong assumption by considering honest entities throughout the operational life of their system model. They then formally verify the authentication and key secrecy of 5G handovers, including injective agreement.

Gupta et al. propose a Secrecy and Efficiency Aware Inter-gNB handover Authentication and Key Agreement protocol (AKA) to achieve session key secrecy and authenticity (Gupta et al., 2022). Formal security analysis and verification is performed with the Random Oracle Model and AVISPA tool.

Nyangaresi and Rodrigues extend the protocol for selection of the target gNB using a multilayer neural network. They prove the privacy and security properties, such as forward and backward key secrecy during handover authentication, using BAN logic (Nyangaresi and Rodrigues, 2022).

In addition to the handover, Miller et al. propose a combined model for 5G registration and 5G AKA protocol (Miller et al., 2022). They formally model and verify the handover authentication and key secrecy, including multiple threat models, using the Tamarin prover. However, the security enhancement of protocol data unit sessions with smart filtering are the main focus of this work.

From the literature study, it is evident that the authentication, session key secrecy, forward secrecy, backward secrecy, and availability (resistance to desynchronization or replay attack) features of 5G handover have been formally verified. Huang et al., Yan et al., Gupta et al., and Nyangaresi and Rodrigues, cover performance analysis, computational overhead, and energy consumption, as well as comparing the proposed protocols with the existing 3GPP standard. Evidently, the proposed protocols are slightly different from the standardized handover procedure. Peltonen et al., and Miller et al., adopt the standardized 5G handover procedure, as defined by the 3GPP, in their model. To the best of our knowledge, we are the first to formally define and verify the forward security property in 5G Xn handovers.

4 OUR SYSTEM AND THREAT MODEL

This section introduces the relevant actors within our Xn handover model in accordance with the 5G Xn handover, defined by 3GPP. In addition, our threat model reflects plausible adversary capabilities within the modeled protocol.

4.1 System Model

There exist different variations of Xn handover in the 3GPP standard. In our system model, we consider a conventional Xn handover model that consists of two base stations, i.e., source gNB and target gNB, UE, and AMF as shown in Figure 1.

The AMF NF within 5G CN remains unchanged in this model. The source gNB and target gNB are connected with an Xn interface. The network interface N1 is used for the communication between UE and 5G CN. On the other hand, N2 is a network interface used for communication between gNBs and 5G CN.

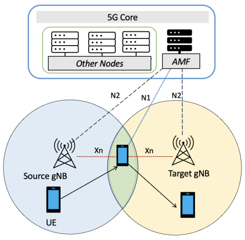

Figure 1: System model of 5G Xn handover.

4.2 Threat Model

The main goal of the attacker is to potentially create a massive service disruption or service compromise for an arbitrary set of users. That is, the attacker may intercept or modify legitimate messages to the users during emergencies. In our threat model, we consider a powerful attacker who has complete protocol knowledge and access to some sensitive information within a base station (e.g., within compromised equipment or a malicious insider). We assume that the base stations are protected by physical security as the 3GPP standard stipulates. Access to any clear text data is limited except when the attacker is an insider or has obtained unauthorized remote access to the base station equipment by exploiting potential vulnerabilities, or a misconfiguration. If all sensitive data is stored in an encrypted manner within the base station, then the attacker is assumed to possess the capability required to access some sensitive information within a base station, such as the temporary session keys used for local storage. The critical information, such as long-term keys, is assumed to be secure and thus inaccessible to the attacker. In our threat model, our attacker can compromise temporary session keys from the base station, and by using these session keys he/she will be able to compromise not only the current session but also the future handover sessions of an arbitrary number of UEs. That is, he/she will be able to eavesdrop, modify, drop, or may reuse the information to perform malicious actions in the future.

In comparison to other existing works (Peltonen et al., 2021) (Miller et al., 2022), we have proven the new security requirement in presence of a stronger insider threat model. This helps to identify the impacts of new attack surfaces.

5 SECURITY ASSUMPTIONS AND REQUIREMENTS

In this work, we reuse some useful fragments of the existing formal model from (Peltonen et al., 2021). The 5G AKA procedure is a prerequisite for a UE to authenticate itself with the CN. We begin our model with Xn handover by assuming that UE has successfully authenticated itself with the CN beforehand.

5.1 Initial Security Assumptions

Our work mainly focuses on the in-depth analysis of key generation during the 5G handover. We next describe the used notions from the 5G key hierarchy adopted in our model.

5.1.1 Keys in 5G Key Stack

Here, we provide a brief overview of keys modeled in our formal model from the 5G key stack and define certain assumptions to reduce model complexity. Figure 2 presents the keys within the 5G key stack.

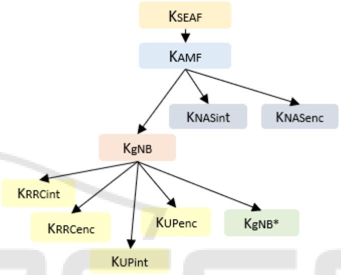

Figure 2: Keys in 5G Key Stack.

K_{SEAF} is the anchor key generated during the primary 5G AKA procedure between UE and CN. All the subsequent security keys are derived using this K_{SEAF} key. K_{AMF} is the long-term key, from which all the session keys are derived by the SRAN and UE during handover. The K_{NASint} and K_{NASenc} are the keys for protecting the Non-access stratum (NAS) signaling between UE and AMF. The key K_{gNB} is the session key derived from the long-term key K_{AMF} during the 5G AKA procedure. The key K_{gNB*} is the session key derived by the SRAN using hkd or vkd for each session during handover. The communication between UE and RAN is secured by four keys: K_{UPenc}, K_{UPint}, K_{RRCenc} and K_{RRCint} and they are derived from session key K_{gNB} to enable encryption and integrity protection of user plane traffic and RRC signaling.

In our model, we consider the anchor key K_{SEAF} and the long-term key K_{AMF} is assumed to be secure. That is, the attacker will not be able to compromise any long-term keys in the 5G key stack. To avoid the complexity in modeling, we use the K_{AMF} for encryption and integrity protection instead of K_{NASint} and K_{NASenc} keys. In addition to this, the keys K_{UPenc}, K_{UPint}, K_{RRCenc} and K_{RRCint} keys are substituted with K_{gNB*} for encryption and integrity protection.

5.1.2 Network Interfaces for Communication

We recall here the claims of secure network interfaces from the 5G standard. The NFs like AMF, within the 5G core, can communicate directly with each other. On the other hand, RAN and UE are separate entities from the 5G core architecture, thus unable to communicate directly with the AMF. Hence, they use secure network interfaces to communicate with the AMF. Therefore, we assume that the N1, N2, Xn, and air interfaces are secure during the handover.

5.2 Security Requirements

The security requirement for 5G Xn handovers is not explicitly stated in the 3GPP standard (3GPP TS 33.501, V17.7.0, 2022). The three security requirements for 5G Xn handover protocol that can be considered are (1) injective agreement of re-derived keys, (2) secrecy of all keys and identifiers used during a handover, and (3) forward security, which ensures the secrecy for future handovers.

5.2.1 Injective Agreement

Injective agreement, also simply known as ”agreement”, is a key security requirement that needs to be accomplished among the communicating entities during a handover (in our study) or specifically during a key agreement. We use Lowe's definition to formally define injective agreement (Lowe, 1997).

During the Xn handover, both the UE and target gNB must agree upon the same key K_{gNB*} for the session. It is important to satisfy the injective agreement between the UE and target gNB to eliminate replay attacks.

5.2.2 Secrecy

Secrecy ensures the confidentiality of the information exchanged during a key exchange procedure. During an authentication key exchange procedure, secrecy is considered an indispensable security requirement for protecting data from being disclosed to unauthorized entities.

During the 5G Xn handover, the secrecy of session keys, such as K_{gNB} and K_{gNB*}, as well as the communication channels (i.e., the network interfaces used for communication) need to be verified to ensure the confidentiality of information exchanged during the handover.

5.2.3 Forward Security

The 3GPP (3GPP TS 33.501, V17.7.0, 2022) standard presents the semi-formal definition of forward security. It refers to the fulfillment of the property that for an entity a, with the knowledge of K_m, used between a and a second entity b, it should be computationally infeasible to predict any future keys K_{m+n},$(n > 0)$ used between a third entity c and entity b.

Forward security plays an inevitable role during 5G Xn handovers to ensure the secrecy of future handovers. If forward security holds for a base station gNB_1 with the knowledge of the key K_{gNB_1}, shared with a UE, it is computationally infeasible to predict any future K_{gNB_i} $(i > 1)$ that will be shared between the same UE and another base station node gNB_i.

Furthermore, the n hop forward security is defined as the property where a gNB is unable to compute the keys that will be used between any UE and another gNB to which the UE is connected after n or more handovers $(n >= 1)$.

6 FORMAL VERIFICATION

Formal analysis of a protocol requires resolving three sub-problems: how to model a protocol, the threat model or adversary knowledge, and security properties. All three may vary depending on the choice of the proof tool that will be used.

In our approach, we use the Tamarin prover, one of the most prominent security protocol verification tools for formal analysis. In this section, we describe how we can model the protocol, adversary capabilities, and security properties using the Tamarin prover, and conclude by summarizing our results.

6.1 Protocol Modelling

In the Tamarin prover, the protocols and the adversary knowledge are modeled using a multi-set rewriting rule. The security properties are defined using first-order logic and they are denoted by lemmas.

Rules operate on the system's state, which is represented using a multiset (i.e., a bag) of facts. The rules are comprised of premises, action facts, and conclusions. The execution of rules shows the system's state transition from the premises, a set of facts, to the conclusions, i.e., a potentially different set of facts. The actions during protocol state transitions are captured by action facts that appear in the traces. The trace of a system or protocol is a sequence of events that starts from an empty state, and consists of a sequence of labeled actions, captured by the action facts for a sequence of rules that were applied.

The rules in the Tamarin prover for protocol modeling are represented as follows:

```
[p] --[a]-> [c]
```

where p is the premise, a is the action fact, and c is the conclusion.

Let us consider a rule to initialize the UE with the serving network in our protocol model. We present a simplified version of the actual rule here.

```
rule init_UE:
  [ !UE(~SUPI, ~CN_ID)]
--[ KeyDerived( K_gNB, ~K_SEAF, K_AMF, ~SUPI)
  ]-> [ Session_key(~SUPI, ~SRAN_ID, K_gNB)]
```

The rule init_UE is comprised of several facts: !UE(...) is a fact in premises, KeyDerived(...) is an action fact, and Session_key(...) denotes a fact within conclusions. The symbol ! with a fact (!UE(...)) indicates that the fact is persistent. Each fact contains one or more terms, such as (~SUPI,~CN_ID). The symbol ~ denotes the freshness of the terms.

The rule init_UE states that a new UE is initialized or registered with the CN (with the identifier ~CN_ID) using the UE's Subscription Permanent Identifier (SUPI). Each ~SUPI value will be unique for each UE. This UE will derive a new session key K_gNB from the long-term key K_AMF, which is derived using the anchor key ~K_SEAF, and the UE identifier ~SUPI. This action is captured by the action fact KeyDerived(...). The fact Session_key(...) in the conclusion indicates that the UE and source gNB (~SRAN_ID) derive the same session key K_gNB.

We also formalize the adversary capabilities using rules in the Tamarin prover, as follows:

```
rule reveal_session_key_k_gnb:
  [ Session_key(~SUPI, ~SRAN_ID, K_gNB) ]
--[ InsiderAttacker(K_gNB)
    , Rev(<'K_gNB', K_gNB>)]-> [ Out(K_gNB) ]
```

Similar to the rule init_UE, the rule reveal_session_key_k_gnb is comprised of three facts, Session_key(...) is the premise, InsiderAttacker(...) and Rev(...), the action facts, and Out(...) is the conclusion fact. The terms 'K_gNB', K_gNB included within the <> represents association of the label ('K_gNB') with the term (K_gNB) itself. In the Tamarin prover, labels are strings within single quotes enclosed within angle brackets (<>).

The special facts, In() and Out() are used to send and receive messages over the network, modeling information which can be intercepted by the attacker.

The rule reveal_session_key_k_gnb states that if an insider attacker obtains access to the session key (captured by the action fact InsiderAttacker(K_gNB)), then he/she will be able to reveal this session key (using action fact Rev(...)). As a result, the session key (K_gNB) is considered as sent out to the public.

6.2 Formalizing Security Properties

In this section, we specify the security properties described in subsection 5.2 as relevant for the 5G Xn handover protocol. We use lemmas to formalize the following security properties using the Tamarin prover.

6.2.1 Injective Agreement

We define the lemma of the injective agreement by following the standard formula definitions within the Tamarin prover manual (in detail). During the 5G Xn handover, we want to guarantee the injective agreement property, that is the agreement between the UE and target gNB (TRAN) on the key K_{gNB^*} (i.e., K_gNB_star in the lemma). We used the action facts Commit(...) and Running(...) to formulate injective agreement, as defined in the Tamarin prover manual.

6.2.2 Secrecy

Our work mainly focuses on the session key derivation and exchange during the 5G Xn handover, we formulate the following lemma to require its secrecy.

```
lemma secret_KgNB :
" All p #i. Secret (<'K_gNB', p>) @i
== > (not (Ex #j. K ( p ) @j))
        | (Ex A #j1. Rev( A, p)@j1
            & InsiderAttacker(A) @i )"
```

The lemma secret_KgNB with the action fact Secret(...) indicates the fact that any key p, which is labelled as K_gNB, and is considered to be secret at any time (#i), requires that no attacker has knowledge (K(...)) about the key p at another time point (#j), nor is there an insider attacker A, denoted by the action fact InsiderAttacker(A), at the same time point (#i), who can reveal (Rev(A, p)) the key. The inbuilt action fact K(...) within the Tamarin prover denotes the attacker's knowledge.

6.2.3 Forward Security

Forward Security is the key property of 5G Xn handover, and it is important to verify this property for both hkd and vkd during the 5G Xn handover.

```
lemma forward_securtiy:
  " not ( Ex q #i1 #j1.
            ForwardSecuritySecret(
                <'K_gNB_star', q>) @i1
            & K(q) @#j1
            & not ( Ex p #r.
                    Rev(<'K_gNB', p>)@r
                    & #r < #i1) & #j1 < #i1) "
```

The lemma `forward_security` states that there is no forward security secret at any time (`#i1`), which is known to the attacker at any time point `#j1` and is exposed by the session key (`K_gNB`), being revealed (`Rev(...)`) at some time point `#r`. The term `q` denotes the forward security secrect, i.e., the key `K_gNB_star`, and the action fact `ForwardSecuritySecret(...)` is used to capture this in a trace.

6.3 Results

Our formal model is used to verify the lemmas, Secrecy, injective agreement, executability (not shown here), and forward security. Here, we mainly focus on the forward security lemma from our results, which has not been verified in any other 5G protocol model. Our results showed that forward security breaks for 5G Xn handovers if the session key is derived using hkd. Therefore, the Tamarin prover returns a counter-example.

In the hkd, each session key K_{gNB} is dependent on the previous session key. Therefore, if one key is revealed within this key dependency chain, it helps the attacker to generate the subsequent keys, such as K_{gNB*}, K_{UPenc}, K_{UPint}, K_{RRCenc} and K_{RRCint}. This breaks the forward security property, as a result of which the attacker can modify, intercept, or hinder the service during (any future) handover. In contrast, the vkd satisfies the forward security because of the unique NH parameter provided by the 5G CN. Thus, it is hard to compromise all future session keys without compromising the 5G CN.

6.4 Mitigation Method

Our proof clearly shows that the secrecy of future handovers strongly depends on the choice of session key generation, i.e., hkd or vkd, during handover. We can remove the counter-example for the forward security lemma during the protocol execution by using the mitigation method below.

To provide an effective solution to our problem, first, we need to distinguish an untrusted base station, which is accessible to an attacker, from a trusted one. For that, we consider the base stations have a designated state as honest or dishonest. The base stations with the dishonest state are those that may reveal the temporary session keys.

The terms `s1` and `s2` below denote the states of source gNB and target gNB during a handover.

```
predicates:
    HonestOrDishonestgNBhandovers  (s1,s2) <=>
    ((s1 = 'dishonest' & s2 = 'honest')
      |(s1 = 'honest'))
```

In addition, we add a rule `honest_dishonest` to indicate the possible states of gNBs.

```
rule honest_dishonest:
  [] -->
  [!H_or_DH('honest'), !H_or_DH('dishonest')]
```

Using the predicates and the rule `honest_dishonest` above, we modify the original rule `init_RAN`, in order to initialize the source gNB in the protocol model to honest or dishonest respectively. The state of the source gNB is traced using the action fact `RANState(...)`. The premise `!H_or_DH(s)` is a persistent fact that represents the state of the gNB. The label for a state `s` in `!H_or_DH(s)` can be either `'honest'` or `'dishonest'`.

```
rule init_RAN:
  [ Fr(~RAN_ID) ,!H_or_DH(s)]
--[ RadioAccessNetwork(~RAN_ID)
    , RANState(~RAN_ID, s) ]->
  [ !NG_RAN(~RAN_ID, s), Out(~RAN_ID) ]
```

In the Tamarin prover, embedded restrictions are used to enforce a restriction on the trace once a certain rule is invoked. Hence, we enforce the states of the source ('honest'/ 'dishonest') and target gNB ('honest') using a restriction `_restrict(HonestOrDishonestgNBhandovers ( s1, s2))` to cover both possible scenarios.

In addition, we implement two rules for hkd based on the state of the source gNB. If the state of the source gNB is `'honest'`, then the source and target gNB will engage in the standard Xn handover procedures, including hkd. On the other hand, if the source gNB is `'dishonest'`, then we invoke a different rule during the *Handover Execution* stage.

The modified rule includes the following steps:

- CN generates a unique key material (~Akey) in the *Handover preparation* stage.
- This key material (~Akey) is shared and stored within the UE, while the UE initializes itself with the CN.
- During the *Handover preparation* stage, the source gNB is identified by the target gNB as honest or dishonest when exchanging the session key K_{gNB*} through *Handover Request* message.
- When the Target gNB receives a *Handover Request* message from an untrusted gNB, it forwards this message to the 5G CN/AMF.
- AMF will derive the new session key (K_{gNB**}) and send it to UE, through *Handover Acknowledge* from Target gNB to Source gNB, and *Handover Command* from Source gNB to UE. The derivation of the new session key (K_{gNB**}) is modelled as:

  `K_gNB_star_star = KDF(K_gNB_star,~Akey)`

- After receiving the *Handover Command* message from Source gNB during the *Handover Execution* stage, UE will initially derive the session key K_{gNB*}, and then derive the unique session key (K_{gNB**}) using the key material (˜Akey) and K_{gNB*}.
- If the authentication is successful, then the UE will send the *RRC Reconfiguration Completion* message to the Target gNB.

In the final stage, *Handover Completion* stage, we follow the original Xn handover procedure.

7 CONCLUSIONS AND FUTURE WORK

Forward security plays a vital role in 5G Xn handovers. It guarantees security for future handovers. The failure of the proof of forward security during 5G Xn handovers reveals the strong attack surface that allows intercepting communications while remaining invisible or unnoticed. Our study shows that the secrecy of future handovers strongly depends on the choice of the session key generation, i.e., hkd, or vkd, during handovers.

We also present a possible solution to mitigate this kind of attack to enhance secrecy. While our model of an untrusted base station is a simplified binary one, and this classification may, in reality, be more complex policy-based decisions or signaling-based detection of rogue base stations.

We would like to recall and emphasize that 5G standards do mandate some security requirements but also leave some options to operators to promote flexibility. The operators implementing 3GPP standards that are aware of this security problem may have already implemented a mitigation of these effects as part of optional features of their systems. Any such solution could also be formalized and proved correct in a similar manner to what we did here. Therefore, future works may include the assessment of various other approaches for hardening the security of handover protocols using formal modelling and verification.

ACKNOWLEDGEMENTS

This work was funded by ELLIIT, Excellence Center at Linköping-Lund on Information Technology.

REFERENCES

3GPP TS 33.501, V17.7.0 (2022). 5G; Security architecture and procedures for 5G System. 3GPP TS 33.501.

3GPP TS 38.423, V17.1.0 (2022). 5G; NG-RAN; Xn Application protocol (XnAP). 3GPP TS38.423.

Basin, D., Cremers, C., Dreier, J., Meier, S., Sasse, R., and Schmidt, B. Tamarin-prover Manual Security Protocol Analysis in the Symbolic Model, 2019.

Bitsikas, E. and Pöpper, C. (2021). Don't hand it over: Vulnerabilities in the Handover Procedure of Cellular Telecommunications. In *Annual Computer Security Applications Conference*, pages 900–915.

Blanchet, B. (2012). Security protocol verification: Symbolic and Computational models. In *International Conference on Principles of Security and Trust*, pages 3–29. Springer.

Dolev, D. and Yao, A. (1983). On the security of public key protocols. *IEEE Transactions on information theory*, 29(2):198–208.

Gupta, S., Parne, B. L., Chaudhari, N. S., and Saxena, S. (2022). SEAI: Secrecy and Efficiency Aware Inter-gNB Handover Authentication and Key Agreement Protocol in 5G Communication Network. *Wireless Personal Communications*, 122(4):2925–2962.

Huang, J. and Qian, Y. (2020). A secure and efficient handover authentication and key management protocol for 5G networks. *Journal of Communications and Information Networks*, 5(1):40–49.

Hussain, S. R., Echeverria, M., Karim, I., Chowdhury, O., and Bertino, E. (2019). 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*, pages 669–684.

Lowe, G. (1997). A hierarchy of authentication specifications. In *Proceedings 10th computer security foundations workshop*, pages 31–43. IEEE.

Meier, S., Schmidt, B., Cremers, C., and Basin, D. (2013). The TAMARIN prover for the symbolic analysis of security protocols. In *International conference on computer aided verification*, pages 696–701. Springer.

Miller, R., Boureanu, I., Wesemeyer, S., and Newton, C. J. (2022). The 5G Key-Establishment Stack: In-Depth Formal Verification and Experimentation. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, pages 237–251.

Nyangaresi, V. O. and Rodrigues, A. J. (2022). Efficient handover protocol for 5G and beyond networks. *Computers & Security*, 113:102546.

Peltonen, A., Sasse, R., and Basin, D. (2021). A comprehensive formal analysis of 5G handover. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 1–12.

Yan, X. and Ma, M. (2021). NSEHA: a neighbor-based secure and efficient handover authentication mechanism for 5G networks. In *2021 9th International Conference on Communications and Broadband Networking*, pages 209–216.