A Comprehensive Formal Analysis of 5G Handover

Secure Systems Demo Day 2021

Aleksi Peltonen[1], Ralf Sasse[2], David Basin[2]

[1]Aalto University, Espoo, Finland
[2]ETH Zurich, Zurich, Switzerland

June 15, 2021

Accepted to ACM WiSec 2021

A Comprehensive Formal Analysis of 5G Handover

Aleksi Peltonen
Department of Computer Science
Aalto University
Espoo, Finland
aleksi.peltonen@aalto.fi

Ralf Sasse
Department of Computer Science
ETH Zurich
Zurich, Switzerland
ralf.sasse@inf.ethz.ch

David Basin
Department of Computer Science
ETH Zurich
Zurich, Switzerland
basin@inf.ethz.ch

ABSTRACT

5G has been under standardization for over a decade and will drive the world's mobile technologies in the decades to come. One of the cornerstones of the 5G standard is its security, also for devices that move frequently between networks, such as autonomous vehicles, and must therefore be handed over from one network operator to another. We present a novel, comprehensive, formal analysis of the security of the device handover protocols specified in the 5G standard. Our analysis covers both handovers within the 5G core network, as well as fallback methods for backwards compatibility with 4G/LTE. We identify four main handover protocols and formally model them in the security protocol verification tool Tamarin. Using these models, we determine for each protocol the minimal set of security assumptions required for its intended security goals to be met. Understanding these requirements is essential when designing devices and other protocols that depend on the reliability and security of network handovers.

CCS CONCEPTS

• **Networks** → **Protocol testing and verification**; **Mobile networks**.

KEYWORDS

5G, handover protocols, protocol verification, formal analysis

ACM Reference Format:
Aleksi Peltonen, Ralf Sasse, and David Basin. 2021. A Comprehensive Formal Analysis of 5G Handover. In *Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '21), June 28–July 2, 2021, Abu Dhabi, United Arab Emirates.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3448300.3467823

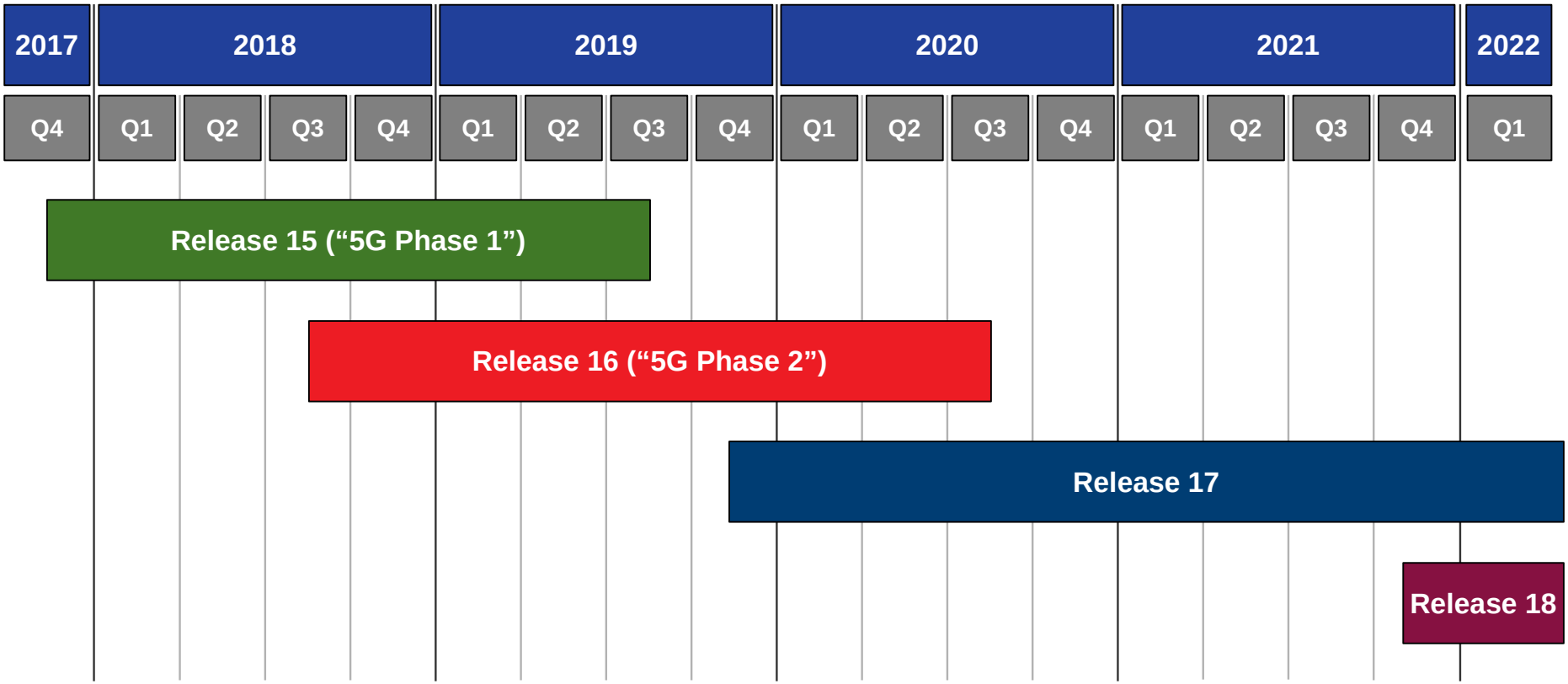
commonly known as 5G. This technology is intended to provide fast, reliable, and secure device mobility across different networks and technologies.

Many of the anticipated use cases for 5G, like autonomous vehicles and IoT devices [17, 24], require reliable connections with low latencies, even when the devices are moving at high speeds. In practice, this means that not only must the serving network provide fast and reliable connectivity, but also that switching between different networks must be seamless and not break any ongoing data connections. This includes both moving between different base stations within the 5G Core Network (5GC), as well as connecting to networks implementing older standards, such as LTE.

Transferring an ongoing connection from one network (or base station) to another is commonly called a *handover* in mobile communication. Handovers in cellular networks can further be divided into intra- and inter-system handovers. An intra-system handover is performed when the source and the target network share a common Radio Access Technology (RAT), i.e., when they implement the same network standard, such as 5G. In contrast, an inter-system handover is required when the networks implement different standards, such as when switching from a 5G to an LTE network or vice versa. In this paper, we use formal methods to model and analyze the security of both intra- and inter-system handovers in 5G. Since the interaction between 5G and networks implementing standards older than LTE is currently not supported [6], we limit our analysis of fallback methods to LTE.

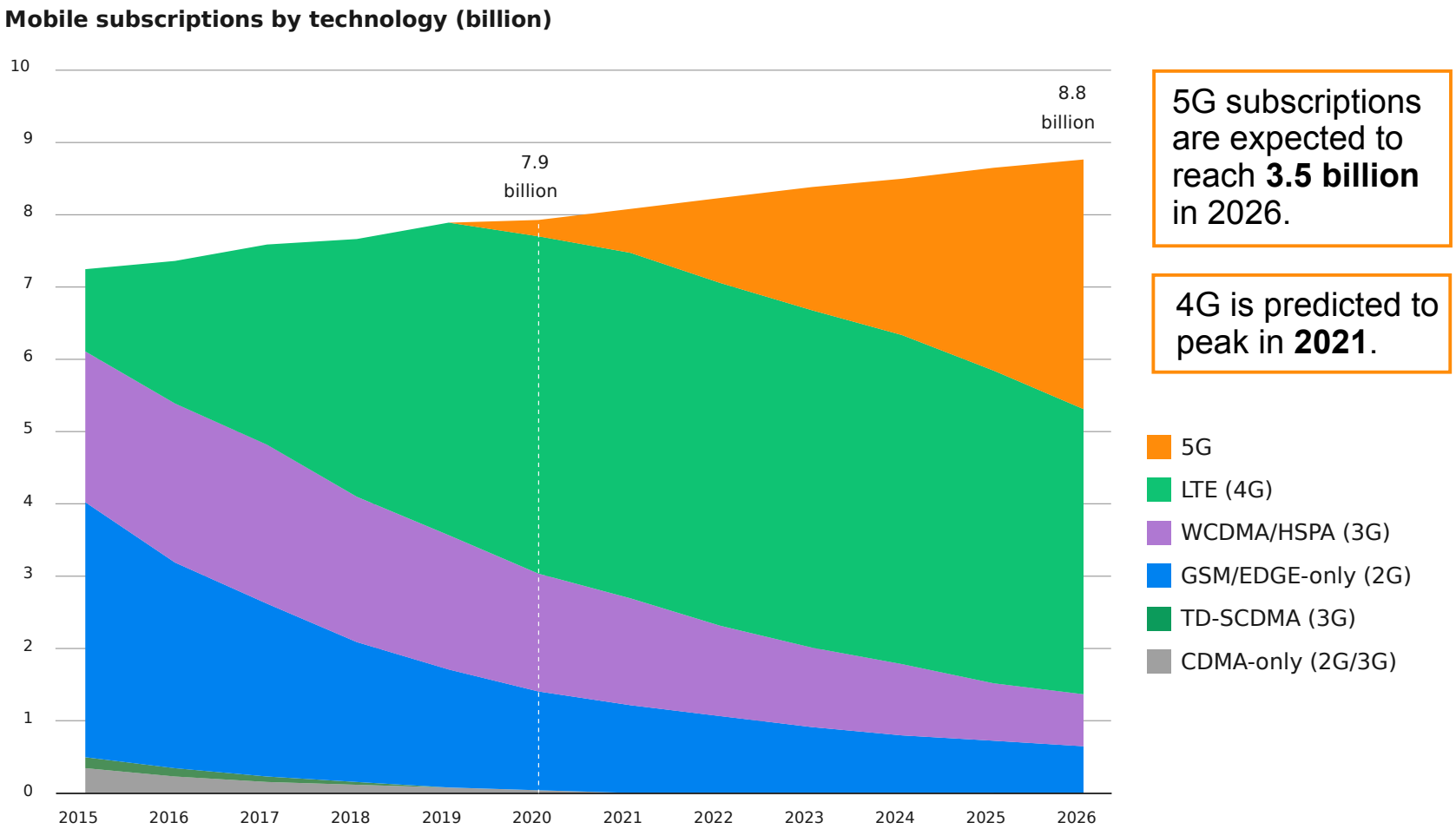
Contributions. Our main contributions are as follows. First, the 5G standard has considerable complexity and is divided over a large number of documents. For both intra- and inter-system handovers we extract and concisely summarize from the relevant standardization documents the handover protocols, their security

5G Timeline



Source: 3GPP.
https://www.3gpp.org/specifications/67-releases

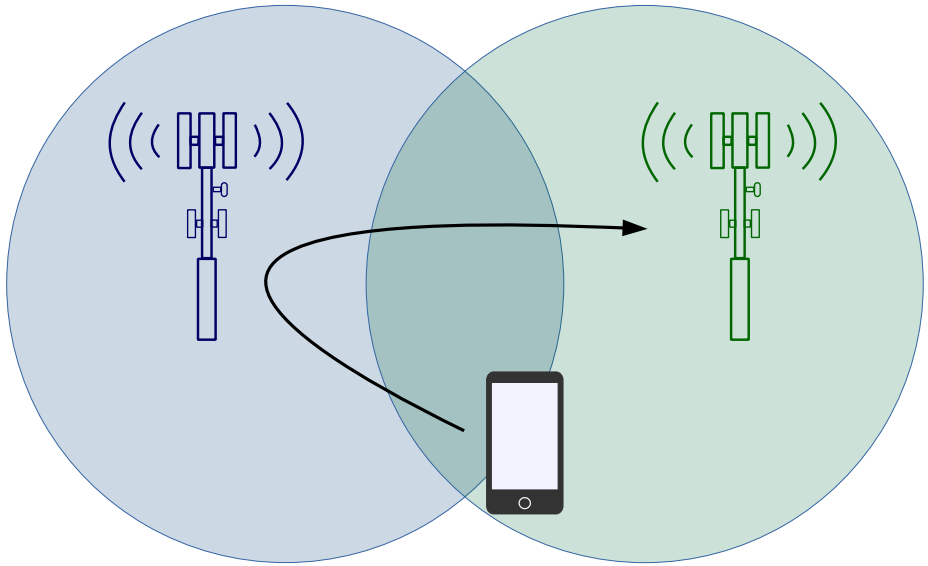
From 4G to 5G



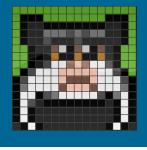
Source: Ericsson Mobility Report, November 2020.
`https://www.ericsson.com/4adc87/assets/local/mobility-report/documents/2020/november-2020-ericsson-mobility-report.pdf`

5G Handover

- A **handover** protocol transfers an ongoing data connection between two networks.
- Either from one 5G network to another, or fallback from 5G to 4G (or vice versa).
- Needs to be fast, reliable, seamless and **secure**.
- We identify four main handover protocols in the 5G specification.



Formal Verification with Tamarin Prover



- Tamarin is a state-of-the-art **verification tool** for the **symbolic modeling** and analysis of security protocols.
- Given a formal model of a protocol and its expected **properties** as input, the tool tries to either **prove** or **disprove** the properties.

```
lemma completion:
  exists-trace
  "∃ a b x y k_AB #i #j #k.
        (((DerviedKey( a, b, k_AB ) @ #i) ∧
          (Commit( a, b, <'I', 'R', x, y> ) @ #j)) ∧
         (Commit( b, a, <'R', 'I', y, x> ) @ #k)) ∧
        (¬(∃ #r. Reveal( a ) @ #r))"
simplify
solve( Commit( $A, $B, <'I', 'R', x, y>
       ) @ #j )
  case I_3
  solve( St_I_2( $A, $B, k_AB.1, x, y ) ▶₀ #j )
    case I_2
    solve( Commit( $B, $A, <'R', 'I', y, ~x>
           ) @ #k )
      case R_2
      solve( St_R_1( $B, $A, k_AB.2, ~x, y ) ▶₀ #k )
        case R_1
        solve( !KU( hmac(~x, ~k_AB.1) ) @ #vk )
          case I_2
          solve( !KU( hmac(~y, ~k_AB.2) ) @ #vk.2 )
            case I_2
            solve( !KU( ~x ) @ #vk.3 )
              case I_1
              solve( !KU( ~y ) @ #vk.3 )
                case R_1
                SOLVED // trace found
              qed
            qed
          qed
        qed
      qed
    qed
  qed
qed
```

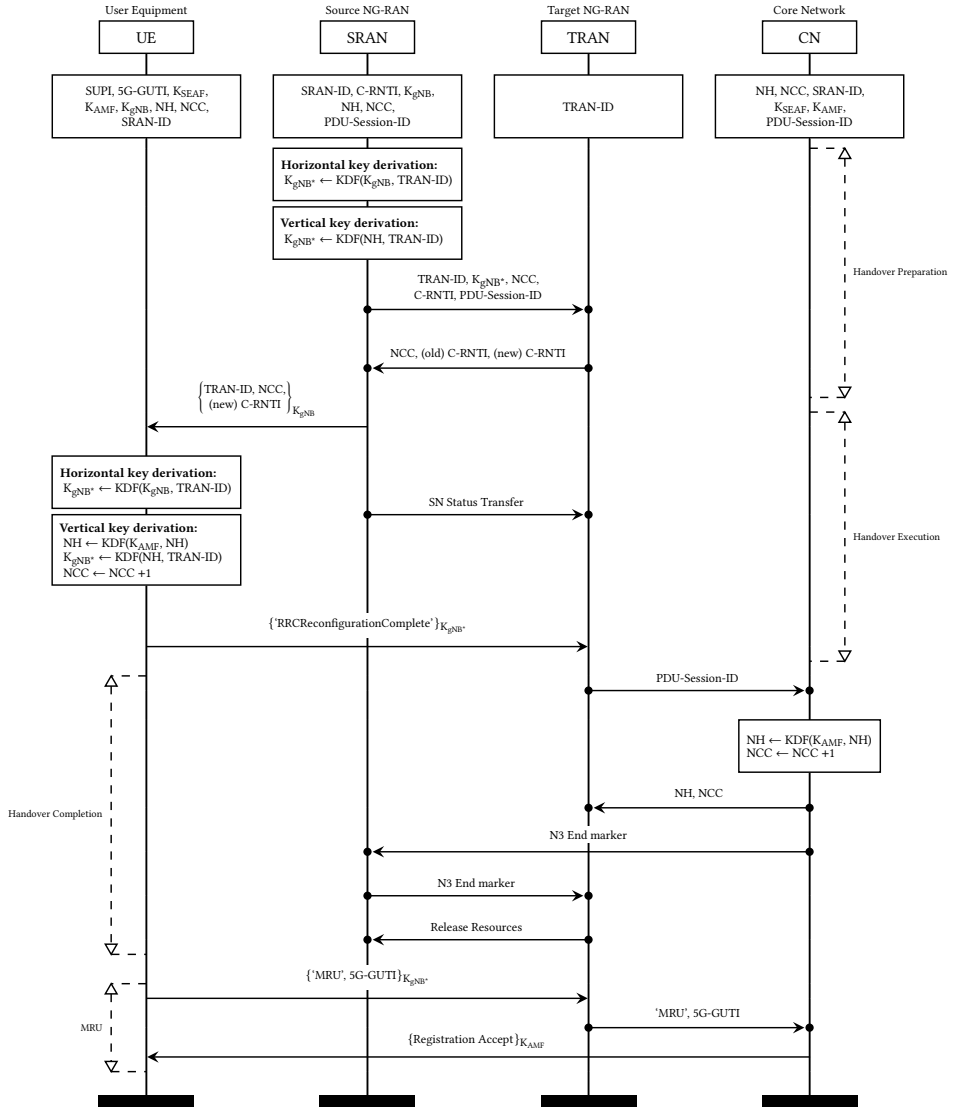
(a) Expected trace

```
lemma injectiveagreementINITIATOR:
  all-traces
  "∀ a b x y #i.
        (Commit( a, b, <'I', 'R', x, y> ) @ #i) ⇒
        ((∃ #j.
           ((Running( b, a, <'I', 'R', x, y> ) @ #j) ∧
            (#j < #i)) ∧
           (¬(∃ a2 b2 #i2.
               (Commit( a2, b2, <'I', 'R', x, y> ) @ #i2) ∧
               (¬(#i2 = #i))))) ∨
         (∃ X #r. (Reveal( X ) @ #r) ∧ (Honest( X ) @ #i)))"
simplify
solve( Commit( a, b, <'I', 'R', x, y>
       ) @ #i )
  case I_3
  solve( St_I_2( a, b, k_AB, x, y ) ▶₀ #i )
    case I_2
    solve( !KU( hmac(~x, ~k_AB) ) @ #vk )
      case I_2
      solve( !KU( ~x ) @ #vk.2 )
        case I_1
        SOLVED // trace found
      qed
    qed
  qed
qed
```

(b) Counterexample

Formalization and Formal Modeling

- As part of our modeling, we abstract away parameters and messages unrelated to security.
- Abstracted values include configuration parameters and other values provisioned for later use by other protocols within the 5G standard.
- We summarize the abstracted protocols as message sequence charts.



Summary

(a) Extended paper

(b) Tamarin models

a) https://research.aalto.fi/en/publications/a-comprehensive-formal-analysis-of-5g-handover
b) https://github.com/tamarin-prover/tamarin-prover/tree/develop/examples/wisec21-5G-handover