5G Handover: When Forward Security Breaks

Navya Sivaraman
Navya.sivaraman@liu.se
Linköping Universitet, Sweden

Simin Nadjm-Tehrani
Simin.nadjm-tehrani@liu.se
Linköping Universitet, Sweden

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 handovers the user equipment (UE) to a target base station through 2 different mechanisms: horizontal or vertical key generation. Although showing the security of these protocols is complex, 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 with a dishonest base station. We also propose a solution to mitigate this counterexample with a small modification of the 3GPP Xn handover procedures based on the source base station state.

Keywords: 5G Xn handover protocol, forward security, protocol verification, formal analysis