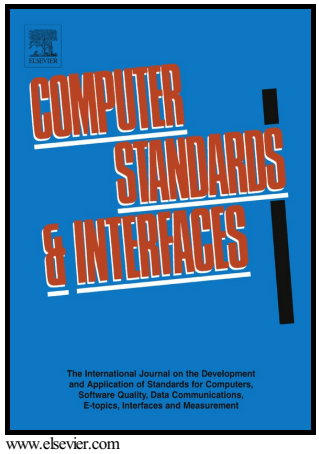
Formal Verification of LTE-UMTS and LTE-LTE Handover Procedures

Piergiuseppe Bettassa Copet, Guido Marchetto, Riccardo Sisto, Luciana Costa



www.elsevier.com

PII: S0920-5489(16)30071-X
DOI: http://dx.doi.org/10.1016/j.csi.2016.08.009
Reference: CSI3130

To appear in: *Computer Standards & Interfaces*

Received date: 9 February 2016
Revised date: 20 July 2016
Accepted date: 30 August 2016

Cite this article as: Piergiuseppe Bettassa Copet, Guido Marchetto, Riccardo Sisto and Luciana Costa, Formal Verification of LTE-UMTS and LTE-LTE Handover Procedures, *Computer Standards & Interfaces* http://dx.doi.org/10.1016/j.csi.2016.08.009

Formal Verification of LTE-UMTS and LTE-LTE Handover Procedures

Piergiuseppe Bettassa Copet[a], Guido Marchetto[a,*], Riccardo Sisto[a], Luciana Costa[b]

[a] *Dipartimento di Automatica e Informatica, Politecnico di Torino - Corso Duca degli Abruzzi, 24 - 10129 Torino, ITALY*
[b] *Telecom Italia Information Technology, Italy*

Abstract

Long Term Evolution (LTE) is the most recent standard in mobile communications, introduced by 3rd Generation Partnership Project (3GPP). Most of the works in literature about LTE security analyze authentication procedures, while handover procedures are far less considered. This paper focuses on the procedures that are activated when a mobile device moves between different LTE cells and between LTE and the older Universal Mobile Telecommunications System (UMTS) networks and completes previous results with a deeper formal analysis of these procedures. The analysis shows that security properties (secrecy of keys, including backward/forward secrecy, immunity from off-line guessing attacks, and network components authentication) hold almost as expected in nominal conditions, i.e. when all backhaul links are secured and all backhaul nodes are trusted. The paper also analyses how these security properties are affected by possible anomalous situations, such as a compromised backhaul node or a misconfiguration by which a backhaul link becomes not protected and can be accessed by an attacker. The analysis shows that some security properties hold even in these adverse cases while other properties are compromised.

Keywords: LTE; UMTS; security; formal verification; ProVerif; handover

*Corresponding author
Email addresses: piergiuseppe.bettassa@polito.it (Piergiuseppe Bettassa Copet), guido.marchetto@polito.it (Guido Marchetto), riccardo.sisto@polito.it (Riccardo Sisto), luciana.costa@it.telecomitalia.it (Luciana Costa)