Chapter 8
Mobile Network Forensics: Emerging Challenges and Opportunities

ABSTRACT

Mobile networks are evolving towards the fifth generation, with radical changes in the delivery of user services. To take advantage of the new investigative opportunities, mobile network forensics need to address several technical, legal, and implementation challenges. The future mobile forensics need to adapt to the novelties in the network architecture, establish capabilities for investigation of transnational crimes, and combat clever anti-forensics methods. At the same time, legislation needs to create an investigative environment where strong privacy safeguards exist for all subjects of investigation. These are rather complex challenges, which, if addressed adequately, will ensure investigative continuity and keep the reputation of mobile network forensics as a highly effective discipline. In this context, this chapter elaborates the next-generation of mobile network forensics.

INTRODUCTION

This chapter discusses the future of mobile network forensics as of the emerging challenges and investigative opportunities. The complete redesign of the 5G network architecture with new deployment scenarios, control and user plane separation, and flexibility for network slicing bring a whole new layer of complexity for implementation of the mobile network forensics mechanisms. The cross-border investigations are also discussed as a unique challenge.

DOI: 10.4018/978-1-5225-5855-2.ch008
that warrants joint utilization of interception mechanisms from operators belonging to different jurisdictions. Mobile network forensic investigations are effective in yielding evidence with high probative value that criminals and attackers are trying to diminish or eliminate completely. The anti-forensics challenges and opportunities for detection are also discussed as of the types, tools, and common actions taken to preserve the normal acquisition, analysis and interpretation of potential mobile network evidence. Lastly, the privacy protection by design for LI and LALS is discussed to prevent illicit and unauthorized use of mobile network data.

5G Mobile Network Forensics

5G Deployment Scenarios

To meet the International Telecommunication Union (ITU) IMT-2020 requirements, the 3rd Generation Partnership Project (3GPP) envisions a fifth generation (5G) with a support for new radio access technologies, control and user plane separation, network slicing, and network sharing. The new 5G air interface is required to provide a marked improvement in the Quality-of-Experience (QoE) as of 20 Gb/s for downlink and 10 Gb/s for uplink peak data rates, 4 milliseconds latency for user traffic and 10 milliseconds latency for control traffic, and continuous service support for one million users per km² connection density.

The 5G radio access is also required to support internetworking with satellite networks next to the LTE-WLAN Aggregation (LWA) and LTE WLAN Radio Level Integration with IPsec Tunnel (LWIP) introduced with LTE-Advanced. 3GPP introduces new deployment scenarios that include: indoor hotspots, high urban density, high speed vehicles and trains, extreme long distance coverage in low density areas, urban coverage for massive Machine Type Communication (mMTC), connected cars, commercial air-to-ground service, and service for light aircraft/helicopters (3rd Generation Partnership Project, 2017b).

From a forensics perspective, the 5G access is required to extend the support for LALS and enable definition/measurement of the scenario-specific KPIs so investigators are able to use target positioning and predict any smart attacks in the radio networks. For LALS, 3GPP retains the current positioning techniques explained in Chapter 6 but also enables for new positioning based on Bluetooth, WLAN, Terrestrial Beacon Systems (TBS), or sensors (3rd
A Unique Method of Constructing Brand Perceptual Maps by the Text Mining of Multimedia Consumer Reviews
www.igi-global.com/article/a-unique-method-of-constructing-brand-perceptual-maps-by-the-text-mining-of-multimedia-consumer-reviews/209387?camid=4v1a

Reconnaissance Attack on IPv6 to IPv4 Tunneling
www.igi-global.com/article/reconnaissance-attack-ipv6-ipv4-tunneling/76392?camid=4v1a