

A theoretical analysis of securing LTE backhaul network using host identity protocol

C.S. Weliwita^{1,2}, S.N. Karunarathne^{2*} and M. Sandirigama²

¹*Department of Math and Computer Science, The Open University, Sri Lanka,*

²*Department of Computer Engineering, Faculty of Engineering, University of Peradeniya, Sri Lanka*

**namal@ce.pdn.ac.lk*

Long Term Evolution (LTE) is expected to provide end-to-end security with many other promising features. However, with unencrypted transmission in the backhaul network (network segment from evolved node B (eNB/eNodeB) to core network), end-to-end security guarantee is violated. Unlike in legacy standards, security standards for LTE do not specify backhaul security implementation and expects service providers to adapt backhaul security. Third Generation Partnership Project (3GPP) has recommended but not mandated implementing Internet Protocol Security (IPsec) with Internet Key Exchange v2 (IKEv2). Nevertheless, most vendors do not implement IPsec for on various reasons like implementation and maintenance cost, overhead, and lack of experience in security implementation.

To assure end-to-end security, backhaul needs to be protected. In order to implement backhaul security, we proposed a new backhaul architecture using Host Identity Protocol (HIP) (HIP-LTE backhaul). HIP is capable of authenticating end nodes in the base exchange process and transmit Internet Protocol (IP) packets using Encapsulated Security Payload (ESP) transport mode by providing encryption and adding integrity protection as ESP – Bounded End to End Transmission (ESP-BEET) mode packets. A Security Gateway (SeGW) is used at the core network and backhaul network interface to work as one end node to reduce overload in HIP processing at core network nodes. eNBs and SeGW are the only nodes needed to implement HIP.

We evaluated security of HIP-LTE backhaul network using analytical model based on ISO security architecture. In the study, we identified security mechanisms available and derived security services in HIP-LTE backhaul. Then we performed a compliance evaluation with 3GPP security requirements for LTE backhaul and found that all the security requirements are fulfilled by new architecture with additional security measures as resilience to DoS, MitM, Replay and flooding attacks. Thus HIP-LTE backhaul is capable of providing security in the backhaul segment without direct IPsec implementation. This reduces the operator effort to implement security in backhaul with less cost.

HIP-LTE backhaul network can be used as an alternative in securing LTE backhaul networks.