An efficient authentication and key agreement protocol for 4G (LTE) networks

ABSTRACT

Long Term Evolution (LTE) networks designed by 3rd Generation Partnership Project (3GPP) represent a widespread technology. LTE is mainly influenced by high data rates, minimum delay and the capacity due to scalable bandwidth and its flexibility. With the rapid and widespread use LTE networks, and increase the use in data/video transmission and Internet applications in general, accordingly, the challenges of securing and speeding up data communication in such networks is also increased. Authentication in LTE networks is very important process because most of the coming attacks occur during this stage. Attackers try to be authenticated and then launch the network resources and prevent the legitimate users from the network services. The basics of Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) are used in LTE AKA protocol which is called Evolved Packet System AKA (EPS-AKA) protocol to secure LTE network, However it still suffers from various vulnerabilities such as disclosure of the user identity, computational overhead, Man In The Middle (MITM) attack and authentication delay. In this paper, an Efficient EPS-AKA protocol (EEPS-AKA) is proposed to overcome those problems. The proposed protocol is based on the Simple Password Exponential Key Exchange (SPEKE) protocol. Compared to previous proposed methods, our method is faster, since it uses a secret key method which is faster than certificate-based methods, In addition, the size of messages exchanged between User Equipment (UE) and Home Subscriber Server (HSS) is reduced, this reduces authentication delay and storage overhead effectively. The automated validation of internet security protocols and applications (AVISPA) tool is used to provide a formal verification. Results show that the proposed EEPS-AKA is efficient and secure against active and passive attacks.

Keyword: EEPS-AKA; EPS-AKA; LTE; SPEKE