World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:12, No:06, 2018

Security Issues in Long Term Evolution-Based Vehicle-To-Everything Communication Networks

Authors : Mujahid Muhammad, Paul Kearney, Adel Aneiba

Abstract : The ability for vehicles to communicate with other vehicles (V2V), the physical (V2I) and network (V2N) infrastructures, pedestrians (V2P), etc. – collectively known as V2X (Vehicle to Everything) – will enable a broad and growing set of applications and services within the intelligent transport domain for improving road safety, alleviate traffic congestion and support autonomous driving. The telecommunication research and industry communities and standardization bodies (notably 3GPP) has finally approved in Release 14, cellular communications connectivity to support V2X communication (known as LTE – V2X). LTE – V2X system will combine simultaneous connectivity across existing LTE network infrastructures via LTE-Uu interface and direct device-to-device (D2D) communications. In order for V2X services to function effectively, a robust security mechanism is needed to ensure legal and safe interaction among authenticated V2X entities in the LTE-based V2X architecture. The characteristics of vehicular networks, and the nature of most V2X applications, which involve human safety makes it significant to protect V2X messages from attacks that can result in catastrophically wrong decisions/actions include ones affecting road safety. Attack vectors include impersonation attacks, modification, masquerading, replay, MiM attacks, and Sybil attacks. In this paper, we focus our attention on LTE-based V2X security and access control mechanisms. The current LTE-A security framework provides its own access authentication scheme, the AKA protocol for mutual authentication and other essential cryptographic operations between UEs and the network. V2N systems can leverage this protocol to achieve mutual authentication between vehicles and the mobile core network. However, this protocol experiences technical challenges, such as high signaling overhead, lack of synchronization, handover delay and potential control plane signaling overloads, as well as privacy preservation issues, which cannot satisfy the adequate security requirements for majority of LTE-based V2X services. This paper examines these challenges and points to possible ways by which they can be addressed. One possible solution, is the implementation of the distributed peer-to-peer LTE security mechanism based on the Bitcoin/Namecoin framework, to allow for security operations with minimal overhead cost, which is desirable for V2X services. The proposed architecture can ensure fast, secure and robust V2X services under LTE network while meeting V2X security requirements.

Keywords : authentication, long term evolution, security, vehicle-to-everything
Conference Title : ICICS 2018 : International Conference on Information and Communications Security
Conference Location : San Francisco, United States
Conference Dates : June 06-07, 2018