Abstract

A vehicular ad-hoc network (VANET) is a wireless network formed by bringing smart vehicles and road side fixed infrastructures for exchanging various information among multiple stake holders to improve traffic congestion, make responsible, reliable and comfortable safe road journey. Each moving vehicle can be characterized as a node in VANET allowing inter-vehicle distance approximately 100m to 300m. Implementing a sophisticated VANET can bring a countless benefits to its users. Ensuring security for highly scalable, dynamic fifth generation (5G), there are many challenges specifically to restrict unauthenticated users access and proper key agreement with fine-grained access control. Further, 6G cellular technology is going to support diverse connectivity requirements at microsecond speed with 1000 times faster latency compared to 5G and greater capacity via higher radio frequency. 6G networks includes most of the features of 5G viz. software defined networking (SDN), network slicing, multi-access edge computing (MEC) and network functions virtualization (NFV). Therefore, most of the security concerns and requirements still remain the most challenging in 6G. Avoiding free flow of information is also a crucial challenge keeping untouched the promising objectives of future generation technology. These 5G and 6G technologies aim to connect devices in milion/sqkm range with the improved performance, incredible transmission speed (terabit), and cost to serve vast transformative diverse automobile sector. VANET and intelligent transport system (ITS) together form a highly sophisticated dynamic complex system of systems (SOS) that provides data access infrastructure to mobility objects, basic stand-alone static elements to highly sophisticated dynamic elements to provide data access as per real-time need for modern traffic management and optimization. To ensure user's core security concern over crucial data in transit, it essentially demands a foolproof user authentication scheme for accessing desired services from VANET clouds. Critical life threatening occurrence of important and urgent high priority events have to traverse unprotected and insecure public/private networks. This openly shared information faces various serious security and privacy challenges. Recently various schemes have been designed to address numerous security concerns but very few schemes have concentrated to address all major attacks with efficiency and in compliance with functional and general security requirements of VANET. Fundamentally, VANET solves security challenges in centralized approach where

centrally trusted unit experiences single point failure issues and most of the traditional VANET approaches may not support high scalability in such dynamic hostile scenarios.

In this thesis, we focus to explore novel security in the area of design and analysis of access control schemes, scalable user authentication, lightweight blockchain-based authentication and suitable key agreement with fine-grained access control for VANET.

First, we propose a lightweight anonymous key agreement scheme (AKAS) with fine-grained authentication feature to address challenges related to restriction of unauthenticated users access and proper key agreement with fine-grained access control specifically for vehicle-to-vehicle (V2V) communication in VANET. In the proposed scheme, registered and authorized users can access services/information as per access privilege only. We have performed formal security analysis using real-or-random (ROR) model. Moreover, we have simulated our scheme using automated validation of internet security protocols (AVISPA) tools, simulation of urban mobility (SUMO), and objective modular network testbed in C++ (OMNET++). We have used the widely accepted AVISPA tool to study formal security verification for intrusion detection and attack mitigation accuracy. SUMO is a mobility simulator to simulate the dynamic behavior of VANET protocols. The ROR is used to proof formerly the security of cryptographic aspects of protocols. Whereas, a modular and component-based network simulation-bed can be developed by OMNET++ tool. Analysis and simulation results show that our scheme is secured against various well-known attacks. Further, we have compared the security and efficiency of our scheme with the existing schemes available in the literature and found that our proposed protocol is more secure, lighter, 5G, 6G friendly, scalable and even faster than the other related schemes.

Secondly, we propose a dynamic lightweight biometric-based authentication protocol for vehicle-to-vehicle (V2V) communication networks where user after successful registration can directly login from any local mobile terminal and access his /her services/information directly from the authentication servers. We have done the security analysis of our scheme and prove that our scheme provides location privacy, mutual authentication for averting spoofing attack, user anonymity and resistance against replay attack, modification and forgery attacks. We also compare the efficiency of our scheme with other related schemes and show that our authentication scheme is more secure and performs faster than other schemes available in the literature. In addition, our proposed scheme provides scalability as there is no limitations on number of user terminal but only the genuine user needs to be registered once for taking the services. No multiple registration or session based registrations are required.

In third study, we propose improved and enhanced Rabin cryptosystem based authentication mechanism to address all known major attacks with robustness keeping efficiency, scalability and dynamicism in picture. We have rigorously carried out security analysis by AVISVA and Proverif tools. The analysis has shown that our scheme guarantees positional privacy, user anonymity and mutual authentication to prevent spoofing attack, password guessing attack, insider privilege attack and temporal session attack. The comparison of protocol with available relevant schemes reveals that the proposed protocol is more efficient with efficacy. It supports light weight authentication process for legitimate users. This proposed scheme supports scalability as this does not depend on the volume of user access point and valid user requires to register only once for accessing the VANET services. Thus, session based and duplicate registration can be avoided by the proposed scheme.

At last, we propose lightweight blockchain-based secure authentication and fine-grained access control (LBAFA) for VANET users. We have defined a framework with edge computing and mobile edge computing to offload computation intensive tasks as well as optimization of data processing before sending it to blockchain based VANET network. We have done security analysis by Proverif tool and formally proved security strength using BAN logic. The security analysis shows that the proposed scheme resists various known security threats. Moreover, the performance analysis proves that our scheme faster and more efficient compared to other available relevant protocols. In addition, in the proposed scheme (LBAFA), we have incorporated blockchain technology to introduce decentralization and parallel computing over traditional centralized VANET. We have also used ECC to optimize the computation cost and CP-ABE to impose access control over the data in fine-grained manner based on user attributes.
The effectiveness of VANET heavily depends on smart traffic management, efficient user interaction and data transmission, collision detection and prevention, road safety, high scalability for large networks, avoiding the free flow of information, and addressing known security attacks with robustness. The critical performance

analysis, simulation results, formal security verification by simulation tools, and mathematical models including informal cryptographic analysis show that most of our proposed protocols are highly effective for VANET applications.

Keywords: Vehicular ad-hoc network (VANET); Intelligent transport system (ITS); Key agreement; User authentication, Biometrics; Blockchain; Fine-grained access control; Security.