Accepted Manuscript

A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs

SK Hafizul Islam, Mohammad S. Obaidat, Pandi Vijayakumar, Enas Abdulhay, Fagen Li, M Krishna Chaitanya Reddy

PII: S0167-739X(17)30843-9
DOI: http://dx.doi.org/10.1016/j.future.2017.07.002
Reference: FUTURE 3532

To appear in: *Future Generation Computer Systems*

Received date : 1 May 2017
Revised date : 4 June 2017
Accepted date : 1 July 2017

Please cite this article as: S.H. Islam, M.S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, M.K.C. Reddy, A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.07.002

A Robust and Efficient Password-based Conditional Privacy Preserving Authentication and Group-Key Agreement Protocol for VANETs

SK Hafizul Islam [a], Mohammad S. Obaidat (**Fellow of IEEE and Fellow of SCS**)[b], Pandi Vijayakumar[c], Enas Abdulhay[d], Fagen Li[e], M Krishna Chaitanya Reddy[f]

[a]Department of Computer Science and Engineering, Indian Institute of Information Technology, Kalyani 741235 West Bengal, India
[b]Department of Computer and Information Science, Fordham University, NY, USA
[c]Department of Computer Science and Engineering, University College of Engineering, Tindivanam, Melpakkam, Tamilnadu 604001, India
[d]Department of Biomedical Engineering, Jordan University of Science and Technology, Irbid, Jordan
[e]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[f]LatentView Analytics Pvt. Ltd., Ramanujan IT City,Taramani, Chennai, Tamilnadu 600113, India

Abstract

With the rapid growth of information and communication technology (ICT) and Internet of things (IoT), the concept of smart-city is recently introduced by the government of many countries to improve the living environment of urban people. In city areas, the numbers of vehicles are increased exponentially day-by-day. Therefore, it is very difficult to control and manage the city traffic caused by tens of thousands vehicles. The Vehicular Ad-hoc Network (VANET) is used to communicate with the vehicles to give alert for weather conditions, road defects, traffic conditions, etc. and the conditions of the vehicle including location, speed, traffic status, etc. Therefore, the traffic efficiency and safety of the vehicles can be improved with the help of VANET. To serve this purpose, in the literature, many conditional privacy preserving authentication (CPPA) protocols based on CA-PKC (certificate authority-based public key cryptography), and ID-PKC (identity-based public key cryptography) have been put forwarded. In addition, some of these CPPA protocols use elliptic curve or bilinear-pairing for their implementation. The computation cost for bilinear-pairing and elliptic curve is very high compared to the cryptographic general hash function. Therefore, all the earlier protocols suffer from the heavy computational burden and some security weaknesses as well. Therefore, bilinear-pairing-free, robust and efficient CPPA with group-key agreement protocol for VANETs is essential. This paper presents a password-based conditional privacy preserving authentication and group-key generation (PW-CPPA-GKA) protocol for VANETs. Our protocol offers group-key generation, user leaving, user join, and password change facilities. Our protocol is lightweight in terms computation and communication since it can be designed without bilinear-pairing and elliptic curve.

Keywords: VANET; Group-key; Conditional privacy; Road-side-unit; On-board-unit; Hash function.

1. Introduction

In the recent years, the governments of different countries concentrated on the development of smart-city to improve the different services to make citizens' life comfortable and secure. The vision of smart-city is to develop the urban areas with the help of ICT and IoT so that the citizens of the city can get better living facilities such as medical, schools, libraries, transportation systems, power plants, water supply management, waste management, law enforcement, etc. To provide secure and fast transportation facilities in smart-city, the management of traffic systems in efficient manner is now becoming a challenging issue. Recently, the concept of intelligent transportation system is developed to manage the traffic of the city, where Vehicular Ad-hoc Network (VANET) is used to provide road safety [1, 2, 3, 4, 5, 6, 7, 8, 9]. A VANET is a continuously self-configuring and infrastructure-less wireless mobile network, where the vehicles behaves like mobile node [5, 6, 7, 8, 9]. A VANET mainly consists of three components, called TA (Trusted Authority), OBU (On-board-unit) and RSU (Road-side-unit). The TA provides the necessary

[a]Corresponding author: hafi786@gmail.com; Ph.:+91-8797369160