Accepted Manuscript

Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks

P. Vijayakumar, Victor Chang, L. Jegatha Deborah, Balamurugan Balusamy, P.G. Shynu

PII: S0167-739X(16)30663-X
DOI: http://dx.doi.org/10.1016/j.future.2016.11.024
Reference: FUTURE 3230

To appear in: *Future Generation Computer Systems*

Received date: 24 August 2016
Revised date: 1 November 2016
Accepted date: 21 November 2016

Please cite this article as: P. Vijayakumar, V. Chang, L. Jegatha Deborah, B. Balusamy, P.G. Shynu, Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks, *Future Generation Computer Systems* (2016), http://dx.doi.org/10.1016/j.future.2016.11.024

Computationally Efficient Privacy Preserving Anonymous Mutual and Batch Authentication Schemes for Vehicular Ad Hoc Networks

P.Vijayakumar[a,*], Victor Chang[b], L. Jegatha Deborah[a], Balamurugan Balusamy[c], P.G.Shynu[c]

[a]Department of Computer Science and Engineering, University College of Engineering Tindivanam, Melpakkam, Tamilnadu, India-604001.

[b]International Business School Suzhou, Xi'an Jiaotong Liverpool University, Suzhou, China-215123

[c]School of Information Technology and Engineering, VIT University Vellore, Tamilnadu, India- 632014.

Mail: vijibond2000@gmail.com, ic.victor.chang@gmail.com, blessedjeny@gmail.com, balamuruganb@vit.ac.in, pgshynu@vit.ac.in

Abstract: In the near future, it is envisioned that vehicular Ad hoc networks (VANETs) will be making use of long-distance communication techniques, such as cellular networks and Worldwide Interoperability for Microwave Access (WiMAX), to get instant Internet access for making the communication between vehicles and fixed road side infrastructure. Moreover, VANETs will also make use of short-distance communication methods, such as Dedicated Short-Range Communications (DSRC) and Wireless Fidelity (Wi-Fi) to perform short range communication between vehicles in an ad hoc manner. This Internet connection can provide facility to other vehicles to send traffic related messages, collisions, infotainment messages other useful safety alerts. In such a scenario, providing authentication between vehicle to infrastructure and vehicle to vehicle is a challenging task.
In order to provide this facility, in this paper, we propose a computationally efficient privacy preserving anonymous authentication scheme based on the use of anonymous certificates and signatures for VANETs in making them an important component of Internet of Things (IoT) and the development of smart cities. Even though there are several existing schemes available to provide such anonymous authentication based on anonymous certificates and signatures in VANETs, the existing schemes suffer from high computational cost in the certificate revocation list (CRL) checking process and in the certificate and the signature verification process. Therefore, it is not possible to verify a large number of messages in a particular period in VANETs which would lead to increased message loss. Hence, we use a computationally efficient anonymous mutual authentication scheme to validate the message source as well as to verify the integrity of messages along with a conditional tracking