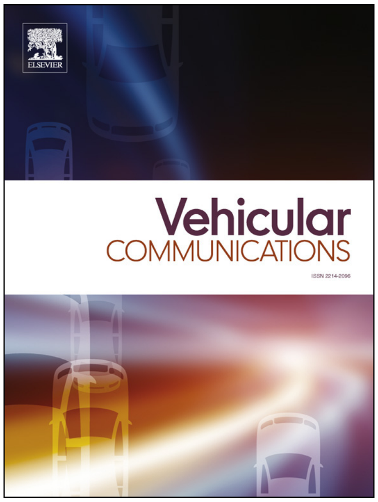

Design of authentication protocol for wireless sensor network-based smart vehicular system

Prerna Mohit, Ruhul Amin, G.P. Biswas

PII: S2214-2096(16)30112-7
DOI: http://dx.doi.org/10.1016/j.vehcom.2017.02.006
Reference: VEHCOM 82

To appear in: *Vehicular Communications*

Received date: 7 September 2016
Revised date: 26 December 2016
Accepted date: 23 February 2017

Please cite this article in press as: P. Mohit et al., Design of authentication protocol for wireless sensor network-based smart vehicular system, *Veh. Commun.* (2017), http://dx.doi.org/10.1016/j.vehcom.2017.02.006

Design of Authentication Protocol for Wireless Sensor Network-based Smart Vehicular System

Prerna Mohit[1], Ruhul Amin[2], G.P Biswas[1]

Abstract

The design of authentication protocol for a smart vehicle system is proposed, where vehicles are equipped with sensors and the sinks are placed along the road to receive and/or send data to sensors. The user monitors the vehicles by collecting data from sinks and performs analysis of the data by taking necessary action (if needed). Moreover, the system is using sensors in vehicles to provide a user-friendly platform to communicate with users. Now, the exchange of authentication message between authenticated entities are two important issues for successful implementation of a smart vehicular system. In the proposed vehicular system there are three entities involve namely users, sink and sensor and two set of communication between user to sink and sink to sensor are needed. In short, we have proposed an architecture of data traffic/movement in vehicular sensor network and authenticate the entities. In addition, we have analyzed our protocol with respect to security attacks and found that it is strongly protected against security attacks. Furthermore, the proposed protocol is relatively better in terms of overhead such as computation and communication.

Keywords: Authentication Technique, Wireless Sensor Networks.

1. Introduction

Internet of Things aims at bridging the gap between the physical world and its representation within the digital world. The term things refer to an object that have sensors attached to it, and can transmit data to internet, where it can be analyzed and used to make decisions, one such example is vehicle sensors. The vehicle sensors are placed in vehicles to monitor the vehicles and its surrounding. A sensor node in wireless sensor network (WSN) is able to process, gather sensory information and communicate with other connected nodes in the network as well as widely used in many applications such as health care, industry, vehicles, etc. due to their ability for monitoring and detecting problems. The sensor node is generally built of a small device, which has a processor, limited memory and limited battery life. The sensors can be classified as 1) static sensors and 2) dynamic sensors. The static sensors are immobile nodes in network that remains stable and do not get power from any electric source directly. The dynamic sensors, are mobile and energy efficient irrespective of whether energy sources of the sensor nodes can be replenished or not [1]. In this paper, we have assumed that the sensors are dynamic and energy efficient, which are connected with the battery of vehicles. Here, the vehicular system is designed in the environment of WSN to monitor and provide a solution for the vehicle related problems such as traffic congestion, speed, etc. in the offline mode. The vehicle sensor sense the real time data and forward it to the nearby sink node directly and the user outside the network can access the sensed data. As the communications are perform via insecure channel, the adversary can intercept the communicated message. Therefore, authentication and privacy of message are the prime concern in the process of message communication. In order to provide secure communication over the insecure channel, we proposed a smart vehicular system using WSN which provides an efficient authentication protocol for securing the sensor node to sink and sink to User. To design an

*Corresponding author. (Ruhul Amin)

Email addresses: prernamohit@outlook.com (Prerna Mohit[1]), amin_ruhul@live.com (Ruhul Amin[2]), gpbiswas@gmail.com (G.P Biswas[1])

[1] Department of Computer Science and Engineering, Indian Institute of Technology (ISM), Dhanbad-826004, India

[2] Department of Computer science and Engineering, Thapar University Patiala 147004, Punjab, India