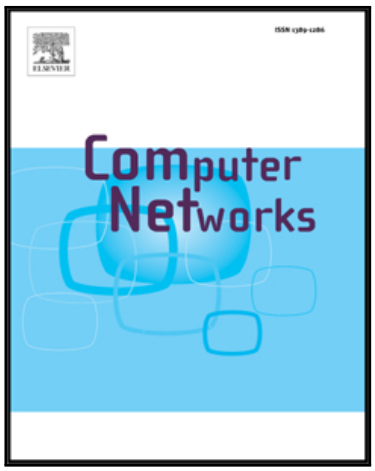

Trust-based Security Adaptation Mechanism for Vehicular Sensor Networks

Muhammad Awais Javed, Sherali Zeadally, Zara Hamid

PII: S1389-1286(18)30118-X
DOI: 10.1016/j.comnet.2018.03.010
Reference: COMPNW 6437

To appear in: *Computer Networks*

Received date: 25 December 2017
Revised date: 21 February 2018
Accepted date: 14 March 2018

Please cite this article as: Muhammad Awais Javed, Sherali Zeadally, Zara Hamid, Trust-based Security Adaptation Mechanism for Vehicular Sensor Networks, *Computer Networks* (2018), doi: 10.1016/j.comnet.2018.03.010

Trust-based Security Adaptation Mechanism for Vehicular Sensor Networks

Muhammad Awais Javed*, Sherali Zeadally† and Zara Hamid*
*COMSATS Institute of Information Technology, Islamabad, Pakistan
†University of Kentucky, United States
{awais.javed@comsats.edu.pk, szeadally@uky.edu, zarahamid@comsats.edu.pk}

***Abstract*—Vehicular Sensor Networks (VSNs) are foreseen as a promising technology that can provide safe and reliable road travel in smart cities. By establishing pervasive connectivity among vehicles and infrastructure units on the road, various intelligent transport applications could be realized. Efficient network security for VSNs thus becomes a key challenge to reliably implement these applications. However, robust security techniques incur high security overhead and processing delays which significantly impact Quality of Service (QoS) particularly in a dense traffic scenario. In this paper, we propose a trust-based security adaptation mechanism to improve the QoS of safety applications in VSNs. The trust level is calculated using connectivity duration, security level and centrality metrics of nearby vehicles. The simulation results we have obtained with our proposed research shows an improvement of $25-65\%$ in terms of safety awareness and $33-53\%$ improvement in terms of packet inter-arrival time of safety applications in VSNs.**

I. Introduction

Vehicular Sensor Networks (VSNs) provide connectivity between vehicles using wireless transceivers, Global Position System (GPS), and various other sensors. By sharing mobility and traffic related data with each other, vehicles construct a database known as Local Dynamic Map (LDM) that facilitates better awareness of the neighborhood traffic (which is defined as all vehicles within one hop transmission range). Many promising applications for VSNs are anticipated including safety, infotainment and traffic management [1], [2].

To enable safety applications in VSNs, the IEEE and the ETSI standards have devised a framework for data generation and transmission [3], [4]. Periodic broadcast transmission of Cooperative Awareness Messages (CAMs) is a key requirement to establish an up-to-date LDM by the vehicles [5]. A CAM is composed of GPS data of the transmitting vehicle along with other mobility data such as its speed, heading, and so on. Based on information in the received CAMs, vehicles make intelligent driving decisions such as lane change, applying brakes and crossing intersections.

CAMs are transmitted by every vehicle at a rate of 10 packets per second to regularly update LDM i.e., one packet every 100ms [6]. Moreover, the communication range of these messages vary from 300 meters to 1000 meters [6]. Since the broadcast mechanism is used to transmit CAMs, each vehicle receives a large number of messages (up to hundreds of these messages per second) from their neighborhood, particularly in a dense traffic scenario.

For vehicle safety applications to provide accurate information to the drivers, it is imperative to disseminate CAMs with a high delivery ratio (good QoS) and robust security mechanism [7]. VSN could be subject to various security threats that can cause network congestion or data corruption. Security mechanisms such as Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Integrated Encryption Scheme (ECIES) are recommended by the IEEE and the ETSI standards to ensure the reliability of VSN applications. These security mechanisms improve defense against privacy threats but cause an increase in packet size (to implement the security procedure). Moreover, security support also takes more time in signature/encryption processing at the transmitter and verification/decryption processing at the receiver [8].

Since QoS and security are conflicting goals, a key challenge in VSNs is to determine the trade-off between both in order to maximize vehicle safety [9]. To overcome this challenge, vehicles need to adapt their communication parameters such as transmit power, and packet generation rate (i.e., reduced QoS) so that they can operate at highest level of security [10], [11]. An alternative approach is to adaptively vary the security level so that vehicle's QoS could be maintained based on the application's requirements [12].

In this paper, we propose a trust-based adaptive security mechanism to enhance QoS in VSNs. The key idea behind the proposal is to evaluate trust level a vehicle has in its neighborhood based on the quality of their past interactions. As the vehicle's trust level in the neighborhood grows, it can reduce its security level to allow vehicles operate at lower security overhead and security processing times.

The trust level is computed by using metrics such as connectivity duration, current security level and centrality of the neighborhood vehicles. The computed trust level is then mapped to a security level which is then used for future CAM transmissions. Simulation results with the NS-3 simulator demonstrates that the proposed mechanism achieves significant improvements in terms of various QoS metrics.

The rest of the paper is organized as follows. Section II reviews the current literature related to QoS enhancement and adaptive security in VSNs. Section III presents our proposed trust based adaptive security mechanism. Section IV describes the simulation methodology and performance evaluation of the proposed mechanism for VSN safety applications. Finally, we make some concluding remarks in Section V.