Computer Networks 143 (2018) 74–81

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

A novel security scheme for Body Area Networks compatible with smart vehicles☆

Junchao Wang[a], Kaining Han[a], Anastasios Alexandridis[a], Zeljko Zilic[a], Yu Pang[b,*], Wei Wu[c], Sadia Din[d], Gwanggil Jeon[e]

[a] Electrical and Computer Engineering Department, McGill University, Montreal, Quebec, Canada
[b] Chongqing University of Posts and Telecommunications, Chongqing, China
[c] Sichuan University, Chengdu, Sichuan, China
[d] School of Computer Science and Engineering, Kyungpook National University, Daegu, Republic of Korea
[e] Incheon National University, Incheon, Republic of Korea

ARTICLE INFO

Article history:
Received 28 November 2017
Revised 7 June 2018
Accepted 2 July 2018
Available online 5 July 2018

Keywords:
Body Area Network
Vehicle Area Network
Security scheme
Authentication
Encryption

ABSTRACT

The growth of Body Area Networks (BANs) has caused significant academic and industrial research attention, as the concept of BANs provides a feasible solution for real-time health condition monitoring. Meanwhile, Vehicle Area Networks (VANs) support communications in smart vehicles and intelligent traffic systems. In practical situations, the two areas overlap in multiple circumstances and their combination could offer a variety of services that benefit from their complementary nature. The rapid development of BAN and VAN requires advanced security techniques to protect communications since both BANs and VANs are transmitting increasingly mission-critical and private data. Therefore, a novel security scheme consisting of enhanced authentication and encryption solutions, which is dedicated in the overlapping area of VAN and BAN, is proposed in this paper. The key aspects of the security scheme were implemented and evaluated in a Field-Programmable Gate Array (FPGA). The evaluation results illustrate that the proposed security scheme has the advantages of low power consumption, low latency, and low resource utilization.

1. Introduction

As reported in the "Canadian Motor Vehicle Traffic Collision Statistics:2015" by the Transport Canada's National Collision Database (NCDB), there were over 118,000 traffic casualties in Canada during 2015 [1], on which 1800 people died and 161,000 people were injured. However, with the development of smart vehicle systems, Internet of Things (IoT), and advanced sensors, an increasing number of modern techniques can be applied to assist drivers in making better decisions when driving.

In recent years, VANs have attracted huge academic and research attention by defining and regulating the communication protocols in smart vehicles. As a result, a huge new area opens up for intelligent applications. More precisely, an intelligent VAN consists of four types of communications [2]. The first one is the intra-VAN communication, which is a network inside the vehicle; data collected from the sensors attached to the passengers or vehicle need to be exchanged under this network. Furthermore, Vehicle-to-Vehicle communication is the network exchanging data between various vehicles. Third, communication of Vehicle-to-Broadband Cloud is a network exchanging data between the cloud and the vehicle. Lastly, there is a Vehicle-to-Road Infrastructure communication, in which the vehicle communicates with intelligent infrastructures, such as smart traffic lights.

In this paper, we focus on interfacing the intra-VAN network. The goal of intra-VAN is to provide information collected by sensors, or from a central hub in the network to the driver, and fa-

☆ This work is partially supported by the National Science Foundation of China (grant nos. 61471075, 61671091), University Innovation Team Construction Plan Funding Project of Chongqing (Smart Medical System and Key Techniques, CXTDG201602009), Chongqing Key Laboratory Improvement Plan (Chongqing Key Laboratory of Photoelectronic Information Sensing and Transmitting Technology, cstc2014pt-sy40001), Chongqing Research Program of Basic Research and Frontier Technology (cstc2017jcyjBX0057). Junchao Wang and Kaining Han want to thank the China Scholarship Council for partial support of their research.

* Corresponding author.
E-mail address: pangyu@cqupt.edu.cn (Y. Pang).

https://doi.org/10.1016/j.comnet.2018.07.005
1389-1286/

cilitate decision making while driving. In terms of existing works, [3] proposed an approach that analyzes the driver behavior state, such as being sleepy, according to the speech emotion, such that the drivers can recognize their physical behavior state while driving. In addition, the health status of drivers with chronic conditions, such as diabetes, can be monitored with the help of sensors to prevent accidents. In the case of diabetes, if the blood glucose approaches a dangerous level, the driver will be notified and the accident will be prevented. However, some challenges are restricting the development of VAN, such as the lack of car-suited physiological sensors [2].

Meanwhile, the development of Body Area Network (BAN) is growing rapidly since BAN was found to meet the requirements for efficient, economical, and uninterrupted health condition monitoring. Various types of biometric data such as Electrocardiography (ECG) [4], heart rate [5], and blood pressure [6] can be collected conveniently and relatively accurately by sensors designed for BAN. As it can be noticed, some of the issues and restrictions mentioned above with regards to the intra-VAN could be resolved with the help of BAN. For this reason, applying BAN in intra-VAN environments would help drivers understand their own physical condition, and contribute towards improved driving decision making, as well as prevent health-related accidents, based on biometric data collected by BAN nodes. Unlike conventional BAN hub devices such as a smartphone, in this case, a central embedded system such as the electronic control unit (ECU) of the vehicle has the potential to be the hub, which collects data from nodes, analyzes it, then gives feedback to the driver.

Even though applying BAN into the intra-VAN improves the functionality of VAN, maintaining a secure communication is a critical issue that needs to be investigated, since the biometric data of human beings is relatively private and significant. Therefore, a novel security scheme that works for BAN, which is applied in intra-VAN situations, is proposed. The scheme has the advantages of low power consumption, small latency, and small resource utilization.

The remainder of this paper is organized as follows. Section 2 presents the previous related work on the security of VAN and BAN. Afterward, Section 3 illustrates the proposed cooperating security scheme between BAN and VAN. The implementation and evaluation of the proposed scheme in a Field-Programmable Gate Array (FPGA) are demonstrated in Section 4. The last section concludes the performed work and discusses the potential future work for this project.

2. Related work

As mentioned, one priority issue that needs to be resolved in combining intra-VAN and BAN is ensuring secured communications. A few proposed methods to resolve the security issues in intra-VAN and BAN will follow.

In terms of security solutions of intra-VAN, a set of experiments were performed by Koscher et al. [7] in 2010 to illustrate potential security issues in the communication of smart vehicles. A few security solutions have been proposed to ensure a secured intra-VAN communication. For instance, an authentication method involving certificate and encryption design was proposed by Wolf et al. [8] for secured automotive communication. In 2009, Groll and Ruland [9] proposed a security solution which divides the communication among ECU and sensors into secured and unsecured groups. More precisely, communication involving confidential and private data can only take place in a closed group, which consists of authentic controllers holding a certificate signed by the manufacturers. Moreover, considering data exchanging between each node may cause information leakage in the network, in order to preserve the privacy of vital data, Schulze et al. [10] suggested applying a Data Management System (DMS) for data storage in the intra-VAN. DMS only allows data exchange between a specific node which stores all the data and normal nodes. Multiple security mechanisms, such as access control, are utilized to protect the data. Further, Oguma et al. [11] proposed an attestation-based security architecture for in-vehicle communication, which executes a hash function in the ECUs to accomplish the attestation process.

On the other hand, there are specific requirements in BAN security processes. As it is mandated by the IEEE standard 802.15.6, three security levels, level 0, level 1, and level 2, have been specified to classify the communication process [12]. The security level of a specific communication is determined by data type and privacy level. For the lowest security level (level 0), the plaintext is directly transmitted and no authentication is required. In the case of level 1, authentication is required before the node gets access to the network while the data transmission is still in plaintext, which provides a medium level of security in data exchanging. A communication of security level 2 needs to have both authentication and encryption, such as Elliptic Curve Cryptography (ECC), which provides the highest protection during the data exchange in BANs. On the basis of the security and power constraints of BANs, light-weight data authentication schemes have been proposed in [13,14]. Compared to other proposed protocols such as SPINS and BROSK, these schemes achieved up to 98% and 67% less power consumption respectively, which makes them more feasible in node sides that are limited by the power supply and computational ability. Moreover, ECG and other biometric data are involved as dynamic factors in the design schemes of Zhang et al. [15] and Ramli et al. [16]. Biometric data is utilized to generate keys used for data authentication and encryption, which simplifies the system while maintaining its security level and properties.

In terms of hardware implementations, Banerjee et al. [17] designed and implemented an FPGA-based hardware security add-on solution for the BAN, while Selimis et al. [18] proposed a security scheme for BAN operated on a customized microprocessor optimized for the Advanced Encryption Standard (AES) encryption, with integrated vector functional units and cryptographic instructions to accelerate the process of the encryption.

Meanwhile, data storage is also a significant problem for both the intra-VAN and BAN systems due to the vast amount of data produced. Cloud storage is an effective method to solve the data storage issue, however, research on the security and search scheme of the cloud storage is required. A smart content-aware search scheme for the problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE) is used in [19] to encrypt the cloud data. Based on rigorous privacy analysis and an experiment on real-world datasets, the scheme is shown to be secure and efficient. Furthermore, an innovative semantic search scheme, based on the concept hierarchy and the semantic relationship between concepts in the encrypted datasets, is proposed in [20], which is used in the cloud storage. The experimental results, again based on real-world datasets, show that this scheme is more efficient than the previous one. Shen et al. proposed a framework for urban data sharing, achieved by exploiting the attribute-based cryptography in cloud computing. Experimental results and comparisons demonstrate that this scheme is secure and can resist possible attacks [21]. A similarity search method for encrypted documents, based on simhash, is proposed in [22]. Ren et al. [23] present the first evidential quality preserving scheme of electronic records, based on Diffie–Hellman key agreement, and provable data possession for cloud storage, which ensured the authenticity, integrity, and reliability of electronic records. Furthermore, Shen et al. proposed an efficient public auditing protocol with global and sampling blockless verification, as well as batch auditing. Numerical analysis and real-