A Study on Tachograph based Security Network

Sania Yaqoob[1], Changhoon Lee[2] and Taeshik Shon[3]

[1,3]Department of Computer Engineering, Ajou University
Woncheon-dong, Yeongton-gu, Suwon, Korea
[2]Department of Computer Science and Engineering,
Seoul National University of Science and Technology (SeoulTech), Korea
sania.yaqoob86@gmail.com, chlee@seoultech.ac.kr, tsshon@ajou.ac.kr

Abstract

Tachographs are used in vehicles for keeping track of driver's hours and for other purposes of fraud detection, overspeeding and accident investigation.Their usage and benefits are in danger beacuse of increasing levels of frauds and manipulation.Tachograph fraud and tampering has become very common due to which the driver's hours and speed regulation are spurned on a large level.Most of these frauds are stimulated by economic pressure on vehicle operators and can be reduced if improved tachograph systems are introduced.Tachographs are used in vehicular environments.Vehicular communication networking is a promising approach to facilitate traffic mangement, road safety and infotainment dissemination for drivers and passengers.With the advancements in vehicular ad hoc networks, transporation safety and efficiency are at stake. Due to this fact, the security, privacy and protection of a private user have became rudimental part of the deployment of technology.The flaws in security of vehicular ad hoc networks can be exploited by even common users, who can interrupt or disable it if some strong and practical security enhancing features are not applied.In this paper we are proposing a new network for vehicular communications based on improved tachographs.The advance features in the tachographs can be helpful in the security and wireless communication vehicular Ad hoc networks.

Keywords: *VANETS, Tachometer, Biometrics, Heterogeneous Networks*

1. Introduction

The advanced and wide deployment of wireless networks has totally revolutionized the lifestyle by providing access to internet services and various communication applications. Telecommunication authorities and vehicle manufacturing companies are equipping every vehicle with the technology that allows users from different vehicles to communicate with each other. For recording vehicle related stats, a certain equipment is used called Tachograph. A tachograph is a device which is fitted in a vehicle that automatically records and archives its speed and distance, along with the driver's activity selected from a choice of modes. The drive mode is activated automatically when the vehicle is being driven, when the vehicle is stationary, it comes to other work mode. A tachograph system consists of a sender unit mounted to the vehicle gearbox, the tachograph head and a recording medium. Tachograph heads are of either analogue or digital types. The recording medium for analogue heads are wax coated paper discs. For digital heads, there are digital driver cards containing a microchip with flash memory. Digital driver cards store data as a .ddd file that can be imported into

[1] First author
[3] Corresponding author

tachograph analysis software. Vehicle drivers are legally required to accurately record their activities, keep the records and present them on demand to transport authorities who are charged with enforcing regulations governing drivers' working hours. Tachographs can be tampered with, in various ways due to which the security and authenticity of the vehicle’s data can be in danger. The example of tampering with tachograph is ghosting, which is another common trick when false driver information is entered onto a second chart to give the appearance that there is a second driver present in the cab for long distance runs that cannot be completed within a single driver's daily driving period.

For the enhancement of transportation efficiency and safety, wireless communication between vehicles and from vehicles to road-side infrastructures (RSUs) is deployed. These types of communications can be used for warning messages for environmental hazards, weather conditions for areas at distance, traffic, road conditions, and congestion and construction sites. But the problem with this type of communication is that a malicious vehicle owner can generate false hazard messages which can cause all the traffic to divert from a certain path which is perfectly clear or cause any other serious misinterpretation. Another type of attack can be to tamper with safety beacons of a vehicle to track vehicle id, location and other important information which can be very dangerous. Because of these threats, there are already many security schemes which are introduced for V2V and V2I communication [3-6].

In this paper, we propose a new network design in which the communication is based on improved Tachographs with advanced features [2], used to give vehicle stats for analysis and security purposes of different authorities like police or vehicle manufacturing companies.

The paper is organized as follows. In Section 2, related work is discussed. In Section 3 proposed features of tachograph and new network architecture is discussed. Finally, in Section 4, the conclusion and future research direction are discussed.

2. Related Work

In this section we are going to discuss some existing protocols and methods used for vehicle related communications.

2.1. Common V2X Network

Wireless Access for Vehicular Environments (WAVE) involves IEEE 802.11p, IEEE 1609.1-4 and SAE 2735 standards. According to the research in this field, main goals for V2X are to provide information on conditions for remoter areas such as traffic jam around a curve 5 km away while there’s still time to act. V2X “communication supports the existing vehicle sensors and can provide additional information. Also V2X communication will allow cars to move at higher speeds with less space between them, which allow for greater fuel efficiency, improved traffic flow, and reduced emissions as vehicles spend more time moving and less time sitting in traffic. IEEE 802.11p is an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE). It defines enhancements to 802.11 (the basis of products marketed as Wi-Fi) required to support Intelligent Transportation Systems (ITS) applications. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz). IEEE 802.11p is based on IEEE 802.11a PHY: OFDM modulation, IEEE 802.11 MAC: CSMA/CA and IEEE 802.11e MAC enhancement: message prioritization.802.11p allows communication patterns like roadside units and mobile radio units (Vehicle-2-Infrastructure), mobile units (Vehicle-2-Vehicle) or portable units and mobile units (Vehicle-2-Pedestrian). Different countries use different V2X frequency bands.

Infrastructure of V2X involves Roadside Units (RSUs), Gantries (e.g. tolling gantries), Poles, traffic lights, Mobile/Portable equipment such as On-board Unit (OBU). In 802.11p there is multichannel communication. First is Control Channel (CCH) which involves Broadcast communication, and is dedicated to short, high-priority, data and management frames. Second is Service Channel (SCH) which involves Two-way communication between RSU and OBU or between OBUs. For specific applications, e.g. tolling, internet access different kinds of applications can be executed in parallel on different service channels. It requires the setup of a WAVE Basic Service Set (WBSS – "Ad-hoc group") prior to usage of the SCH.

IEEE 1609.4 is a functional extension to IEEE 802.11e MAC to enable multi-channel coordination. It has functions like Channel routing, Data buffers (queues), Prioritization and Channel coordination. IEEE 1609.3 is WAVE Short Message Protocol (WSMP).It is a networking protocol specifically designed for V2X communications. SAE J2735 is Dedicated Short Range Communication (DSRC) Message which defines set Dictionary, ASN.1 representation of message structures and Hierarchical definition of messages and substructures. The vision of the ITS America Connected Vehicle Task Force is deployment of a nationally interoperable, wireless communications system that transforms the way vehicles interact with each other and our highway network.

2.2. CTS, Existing Bus and Taxi Network

While transport systems have generally been essential to human civilizations, their impact on society and economy has vastly grown in recent decades due to technological advancements. Modern transportation systems are expanding growth of cyber physical systems that are becoming increasingly intelligent and complex. These cyber transportation systems (CTS), i.e., automotive, avionics, maritime, and rail systems, will greatly improve essential transport attributes such as energy-efficiency, greenhouse gas emission, independent operation, reliability, and crash avoidance while also providing a new experience to the users in terms of safety, comfort, interactions, and entertainment. Modern vehicles include several Electronic Control Units (ECUs) that form an in-vehicle distributed networked embedded system.

Future ITS involves communication between the vehicles as well as the communication between vehicle and external entities. Although the introduction of new communication technologies offers an exceptional number of new opportunities, the integration of communication technologies in transportation systems also simultaneously increases the complexity of the CTS and demands new analysis of security and privacy requirements. Another great source of vulnerability stems from the weaknesses in the electronic and transportation components supply chain management such as determining the authenticity of parts. Gaps in authenticating parts and cost constraints could result in integration of less reliable and possibly malicious counterfeit, fake or Trojan components in the system during manufacturing or repair. The evolving nature of CTS complexity and attack possibilities suggests that a continuous flow of research and development is needed before modern CTS can be efficiently designed, and safely operated.

In recent times, few existing European efforts and initiatives are taken in vehicular and CTS safety and security domains. First project is EVITA. The EVITA project's objective is to design, verify and prototype an architecture for automotive on-board networks that protects security-related components and sensitive data. It focuses on secure intra-vehicle communication and complements other e-safety related projects that focus on the secure vehicle-to-X communication. The project plans on hardware-based security investigation and aims to develop hardware security modules that can be provided as extensions to automotive controllers/ ECUs or as dedicated security controller chips. Another project is CyberMove.

This project considers the development of CTS to overcome problems with traditional transportation systems such as road congestion, energy expenditure, noise, and pollution that degrade the quality of life in urban life. CyberCars-2 project is extension of CyberCars project and focuses on vehicle-to-vehicle and vehicle-to-infrastructure communication as well as vehicle coordination.

The objective of TransCyber workshop, which is a great attempt to address problems in CTS, is to identify and address the issues concerning real time safety, reliability, availability, and security for upcoming generations of transportation systems. The workshop will bring together International experts from industry, government, defense, and research domains to highpoint the existiing challenges in this area and discuss the various approaches/initiatives needed for addressing these challenges. The TransCyber workshop focuses on a number of unique characteristics, which were not addressed by the previously held workshops and meetings in this domain. The workshop plans to bring together top International professional and experts from various levels of transportation manufacturers and authorities, government and defense agencies, platforms and tool providers, and industrial and academic researchers to identify the rising trends and challenges in CTS domain. In particular, the workshop places emphasis on the new business opportunities created by safe and reliable CTS, while investigating the pressing issues of forged parts detection and protection in components supply chain, secure software updates, and digital rights management for transportation systems. The longer-term impact of the TransCyber workshop and its accompanying initiatives is creation of better/safer CTS and several new business opportunities in this domain.

Existing Taxi networks involve different levels of services such as booking answering, Failure to connect with customers, delivery (pick-up waiting time limit) and no car availability time limit. There are standards defined for everything related to the taxi network. There are rules and regulation for becoming authorized taxi-cab network provider. Taxi-cab Network Services Standards have lots of rules and regulation involving service levels, booking service, Supervision and compliance with network rules and by-laws, directions, driver training, driver safety, Electronic Toll Tags, advertising, Livery and uniforms, fares, Government subsidy schemes, Offloading bookings, Monitoring, Customer service, reporting and sanctions. This system lacks the ITS benefits, which if applied can benefit the existing taxi network a lot.

City buses are the most common means of transportation. They are frequent, reliable and probably the most inexpensive way of getting around. There are lots of long-distance and short distance buses running all throughout different countries. As a rule of thumb, buses run every 15 minutes to 1 hour. However, there are usually no regular timetables, and departure times can vary throughout the day. Buses always leave on time or sometimes even too early. Bus routes are usually color coded and depict the distance they travel. The buses used for inter-city travel have different color than those used for intra city travel. Fares vary depending on the kind of bus you are taking. Payment card is usually used for bus travel. Also money can be given directly. Bus stops are usually after reasonable distance and are not very far from each other. Currently, there are no special ways of communication applied in this network by which all buses or taxis are connected with each other for sharing of important news or details about each other. This shortcoming can be overcome by making them a part of ITS.

3. Improvements in Tachograph and Proposed Network

In this paper we are going to give some important points to improve the Tachometer usage and then we propose a network architecture based on Tachographs for security purposes.

Improvements in Tachographs:

To avoid breach of laws, as frequently done by different drivers by changing tachographs stats, there can be some changes in the basic tachograph architecture. For these purposes biometrics can play important role. We can make changes in tachometer by providing security using biometrics. For tachograph of a certain route vehicle, the thumbnail impression for all drivers of that route is taken. It can also be made mandatory for a driver to give his thumbnail impression in the digital tachometer at the start and end of its duty time. The stats whether the thumbnail impression was given for starting and ending of the duty time are also recorded. For example, if on a certain route one driver can only drive for 12 hrs., then for starting of the shift and after 12hrs, thumbnail impression of the driver should be provided .In this way, the problem of 'ghosting'__ manipulating tachograph chart, can be avoided. Still there are many other methods to tamper with the smart card and the tachometer itself.

The second problem for tachometers is that the tachometer data is extracted not on regular basis. Although the provision of data is not easy and has different criteria for different users, like, for police the different details can be extracted from smart card and for the maintenance company the extracted data will be different from tachograph. The solution to this problem is that if we develop a system in which the Tachograph data can be sent to a central authority periodically or on predefined intervals, the tampering problems with tachograph data can be avoided. The reason is that when the data will be sent periodically to some server which will store the data and will also be analyzing it, then the unusual stats can be identified. For this purpose there should be an analyzing authority to point out the unusual or abnormal stats it is getting as shown in Figure 2. Some algorithms can be devised for this process so that the process does not become very exhaustive. For sending data periodically to a central authority from high speed vehicles is not easy task because of their high mobility and changing wireless conditions. For overcoming this problem the vehicles should be equipped with at least one long range and one short range radio interfaces, whereas regular nodes (clients) only need a short range radio interface. By regular nodes we mean the Roadside infrastructures such as traffic signals. The environment considered for this scenario is heterogeneous. Now-a-days communication is possible from different wireless channels, so we can consider our network as heterogeneous network. Data from vehicles can be sent to central authority from any type of network like 2G, 3G, 4G and Wi-Fi etc. The data sending process is done by tachometer.

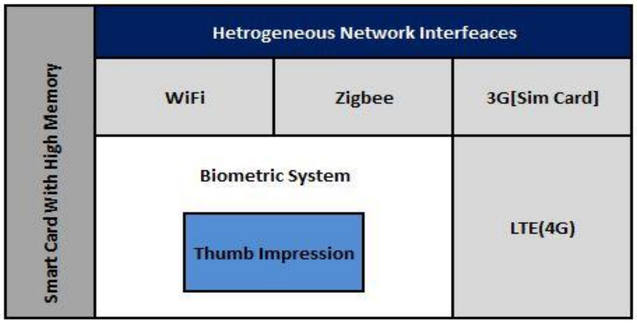

Figure 1. Advance Features for Tachograph

For this type of network, the tachometers should have the capability to have multiple interfaces for different types of wireless networks as shown in Figure 1.The short range radio channels of the tachometer can communicate with the roadside infrastructures and other vehicles which come within range. The long range channels are used to send data directly to the Central authority. The reason to have multiple types of channel is that, in our network, there will be multiple types of communication due to high mobility scenario in vehicles. Currently, we are aware of a large variety of wireless access networks, including the emerging vehicular ad hoc networks (VANETs). For tachometer to be connected with Central authority either directly with a radio channel or indirectly, via a central entity such as roadside infrastructure, to continuously sending driving stats, the demand for features such as real-time connectivity, high-availability, and even instantaneous high-bandwidth is increased. Therefore, when tachometer has the ability to communicate through multiple radio channels in heterogeneous network, it is vital for network service providers to make the best possible use of the combined resources of available heterogeneous networks (wireless area networks (WLANs), Universal Mobile Telecommunications Systems, VANETs, Worldwide Interoperability for Microwave Access (WiMAX), *etc.*) for connection support. When connections need to transfer between heterogeneous networks for performance and high-availability reasons, seamless vertical handoff (VHO) is an obligatory step. So for effective connectivity in this tacchograph network, vehicular and other mobile applications are expected to have seamless VHO between heterogeneous access networks. For VHO performance, Algorithm development is already in progress for connection management and optimal resource allocation for seamless mobility. There are already much research work is going on for developing a VHO decision algorithm that enables a wireless access network to not only balance the overall load among all attachment points (*e.g.*, base stations and access points) but also maximize the collective battery lifetime of mobile nodes (MNs). In addition, when ad hoc mode is applied to 3/4G wireless data networks, VANETs, and IEEE 802.11 WLANs for a more seamless integration of heterogeneous wireless networks, many route-selection algorithms are also devised for forwarding data packets to the most appropriate attachment point to maximize collective battery lifetime and maintain load balancing.

Therefore, if we develop such a network based on tachograph with functionalities of multiple radio interfaces and biometrics functionalities applied, then not only some security issues can be addressed but also high connectivity and availability of vehicle data, location and other information extraction is easily available for analysis anytime.

Figure 2 shows the network we are proposing. Every vehicle has tachometer which has multiple radio interfaces to communicate with all devices in a heterogeneous network.

We can define types of communication we want. For example we can design an ad hoc mode in which tachograph uses short range communication such as Zigbee, to communicate with other vehicle passing by. With this type of communication we can communicate or broadcast information to all vehicles within certain range of zigbee/ Wi-Fi mode for informing about some accident or traffic conditions nearby.

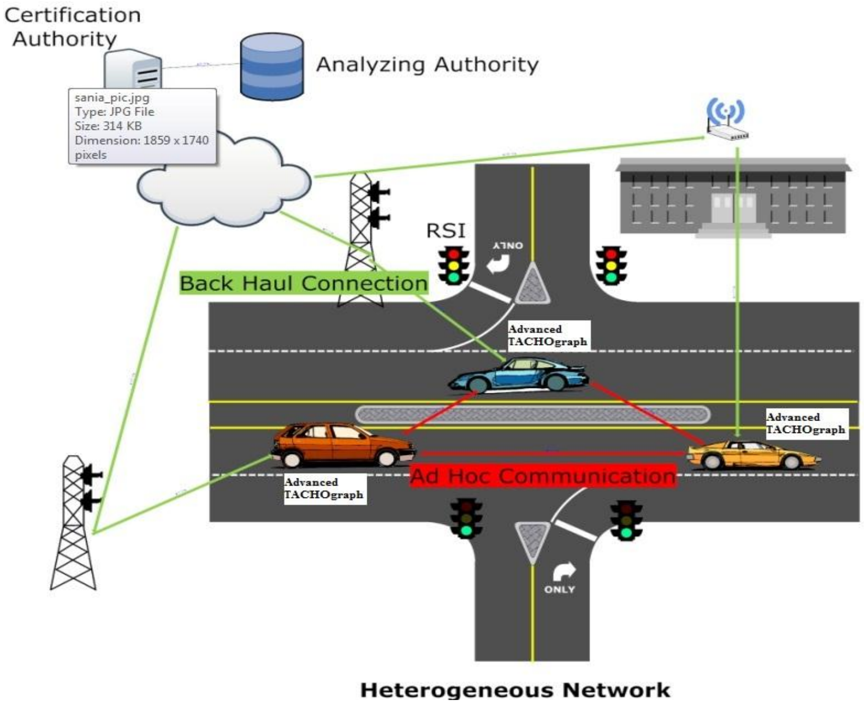

Figure 2. The Overall Architecture of Tachograph based Heterogeneous Network

In our network Tachograph can be in two modes. A Vehicular Ad-Hoc Network, or VANET, is a form of mobile ad-hoc network, which provides communications among nearby vehicles and between vehicles and nearby fixed devices, usually described as roadside equipment. It is enabled by short-range to medium range systems, which consists of vehicle-to-vehicle (V2V) or vehicle-to-roadside infrastructure (V2I) communications. Similarly the second mode of tachograph can be to send tachograph data to central authority periodically. The data which is to be sent periodically to central authority should be strictly limited to contents which has the threat to be modified by the driver of the vehicle or though other security attacks. This data is sent to central authority through 2G/3G/4G cellular systems or any other way of long range communication, as shown in Figure 2.This type of communication can be done by inserting a sim in tachograph, or by using any other techniques for long range communications. When this data is sent to the central authority, it is analyzed by analyzing authority for abnormal stats, as well as it is checked for any mischievous act like the drivers who try to remove the over speeding or jumps stats by tampering with tachograph.The strategy to this can be to find out if the stats of the vehicle remain normal for a long time with no over speeding or jumps data, which shows tampering with Tachograph. The analyzing authority can find other algorithms or ways to get information about abnormal or tampering with tachograh data. After that the issue can be resolved by informing police or related authority to check the vehicle and make the tachograph to work correctly again.

4. Conclusion

In this paper, new system architecture is proposed with communication done by Tachographs which have advanced features. Because of these advance features of tachograph, tampering with tachometer stats can be greatly reduced. For this time we have ignored the security schemes which can be used for V2V and V2I communication because this area is already been a part of research and many security schemes and algorithms are already proposed for this purpose. If we use any of the existing authentication schemes for Ad hoc communication between vehicles, other communication types for V2I and long range communication between vehicle and central authority, by using the proposed advanced features in Tachograph and the new heterogeneous network structure, we can guarantee improvement in communication between entities and tachograph security. Also if we used the advanced tachographs and apply advance communication techniques in existing bus or taxi network, the overall traffic and network performance will also improve.

Our future work will be made on the methodology and algorithms for authentication schemes in proposed heterogeneous network communication and novel security techniques for Tachograph data safety and integrity.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(No. 2012R1A1A1010667).

References

[1] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho and X. Shen, “Security in vehicular ad hoc networks”, Communications Magazine, IEEE, vol. 46, Issue 4, **(2008)**, pp. 88- 95.

[2] R. Anderson, “on the security of digital tachograph”, Computer Security- ESORICS 98, **(1998)**, pp. 111-125.

[3] M. Raya, P. Papadimitratos and J. -P. Hubaux, “Securing Vehicular Communications”, IEEE WIRELESS COMMUNICATIONS Journal, **(2008)**, pp. 8-15.

[4] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung and J. -P. Hubaux, “Secure vehicular communication systems: design and architecture”, Published in: IEEE Communications Magazine, vol. 46, no. 11, **(2008)**, pp. 100-109.

[5] http:// http://www.tachopak.co.uk/digital-tachograph-for-drivers.shtml.

[6] http://www.dft.gov.uk/vosa/publications/businesslinkwebpages/tachographsthebasics.htm.