VANET Security Framework for Trusted Grouping using TPM Hardware

Asif Ali Wagan[1], Bilal Munir Mughal[2] & Halabi Hasbullah[3]
Department of Computer and Information Sciences
Universiti Teknologi PETRONAS
Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia.
[1]*asifwaggan@gmail.com,* [2]*bilalmunirmughal@gmail.com,* [3]*halabi@petronas.com.my*

***Abstract*— Vehicular Ad hoc Network (VANET) is a network of vehicles on the roads, of which the success of its applications is highly dependent upon the underlying security mechanism. The default trial asymmetric PKI/ECDSA security mechanism is known for its high computational cost, thus lacking applicability in life-critical safety messaging. Alternative security schemes, such as symmetric methods provide faster communication at the expense of reduced security. Hence, hybrid and hardware based solutions were proposed by researchers to ease the issue. However, these solutions either do not support the existing VANET PKI standard or have larger message size. In this paper, we present a hardware-based security framework that uses both standard asymmetric PKI and symmetric cryptography for faster and secure safety message exchange. The proposed framework is expected to improve security mechanism in VANET by developing trust relationship among the neighboring nodes, hence forming trusted groups. The trust is established via Trusted Platform Module (TPM) and group communication.**

Keywords-VANET; asymmetric cryptography; symmetric cryptography; trusted group; Trusted Platform Module.

I. INTRODUCTION

Vehicular Ad hoc Networks (VANET) is receiving a lot of interest due to the variety of services that they can offer. The most important goal is to enable public safety applications that can potentially save lives and improve traffic conditions. Non-safety services are also envisaged to provide comfort, convenience and infotainment to road users, such as geo-location information, weather reports, on-line gaming, etc.

Effort to finalize VANET communication standards such as Wireless Access in Vehicular Environment (WAVE), IEEE 1609.x and 802.11p is in progress. WAVE is a trial layered architecture used by IEEE 802.11 devices to operate in the DSRC band for vehicle-to-vehicle (V2V) communication, as well as for vehicle-to-roadside (V2R) communication. In the USA, FCC has allocated DSRC spectrum at 5.9 GHz, which the spectrum is structured into seven of 10 MHz wide channels. Channel 178 (5.885-5.895GHz) is the control channel (CCH), which the primary use is for safety communications. The two extreme channels are reserved for future safety applications, i.e. advanced accident avoidance applications. The rest are service channels (SCH) that can be used for both safety and non-safety applications [1].

Several ongoing issues of VANET have attracted the attention of industry and academia. Safety communication is one of such issue that has been subject of a number of research papers. In VANET, vehicles exchange safety messages to keep the neighboring vehicles aware of the road and potential hazardous situations. Safety messages can be categorized into periodic safety messages and event-driven safety messages. Periodic safety messages are exchanged several times per second among neighboring vehicles and contain information regarding vehicle location, speed, direction, etc. Event-driven messages are initiated when a hazardous situation is sensed on the road, for example accidents, hard breaking, etc. On one hand, as lives are at stake, safety information needs to be delivered to all concerned vehicles in a speedy and secure way. On the other hand, a false message or a minute delay can lead to hazardous situations, such as collisions. Accordingly, IEEE 1609.2 asymmetric Public Key Infrastructure with Elliptic Curve Digital Signature Algorithm (PKI/ECDSA) has been proposed as a default trial security mechanism for VANET.

However, the asymmetric ECDSA is known for its high computational cost, which can lead to longer delay in message delivery [2]. Hence, researchers have proposed alternative symmetric VANET security solutions like [3] and [4] that do provide faster communication, but at the expense of reduced security. In view of this, hybrid methods can be exploited by taking advantage of both the asymmetric and symmetric cryptography to provide optimal security implementation. Nevertheless, tradeoffs still exist between secure (asymmetric) and faster (symmetric) safety messaging, such as trust building. Both requirements cannot be satisfied equally at the same time. In balancing the need, a trust must be established, particularly when good security level cannot be provided.

In the light of the abovementioned security demand, we define our research question as follow: How to build trust among neighboring vehicle nodes, to form a trusted group when there is a need to achieve fast and secure transmissions of the event-driven safety messages through symmetric method.

978-0-7695-3961-4/10 $26.00 © 2010 IEEE
DOI 10.1109/ICCSN.2010.115

Based on the identified research issues, we set the objectives of this research work in two folds. First, to make use of hardware integrated asymmetric and symmetric cryptography modules for safety messaging. Second, to develop trust among vehicle nodes in vicinity. These two objectives would lead to the development of a VANET security framework that is able to transfer safety messages using both cryptographic schemes.

The rest of this paper is organized as follow. Section II discusses related work, Section III proposes a security framework, Section IV analyzes the proposed security framework, and finally, conclusion and future work are given in Section V.

II. RELATED WORK

PKI has been proposed as default trial asymmetric security mechanism for VANET, along with ECDSA. Computational overhead remains a key element of concern for real-time applications, such as the transmission of event-driven safety messages. Asymmetric methods are known to be extremely resource hungry and can incur processing delay [2]. Alternative symmetric methods provide a way for faster processing that suits life-safety messaging due to its innate requirement of minimal processing resources. However, faster processing comes at the expense of reduced security, i.e. lack of trust and non-repudiation. Consequently, emergence of hybrid solutions, such as [4] and [5] was inevitable. In the following, we summarized some of the already proposed solutions with regard to secure message communication in VANET.

A comprehensive study of work on VANET security can be found in [2]. The authors provide comparison between NTRU method with that of ECDSA method. The result showed that NTRU provides faster verification, but due to its large size, it is not suitable for VANET applications, which will not tolerate to delays.

According to [3], TESLA is a symmetric cryptography method that provides faster communication. TESLA uses code delayed key disclosure to provide message authentication. However, the main problem with TESLA is that receiver store all messages sent by sender and wait until the sender discloses the key. This may lead to vulnerability against possible memory attacks.

In [4], group signature scheme is presented, where there exist one signature for a group. Any group member can use it and send message accordingly, by which the group leader can track back the source node in case of any dispute. In [6], scheme of vehicle position verification is implemented using two methods: Convoy Member Authentication (CMA) and Vehicle Sequence Authentication (VSA). Authors in [7] give the concept of blind signature scheme. In this signature scheme, sender sends the message and message signer signs the message without knowing what the actual content of the message is. Kerberos proxy method as described in [8] presents a highly famous mutual authentication process, but due to its on-line real-time security requirements, it may not be suitable for VANET. This is due to possible delays or disconnections, which could lead to a network wide calamity. VANET Authentication using Signatures and TESLA++ (VAST) presents a hybrid solution without any hardware support [3]. However, in this solution each message contains both symmetric TESLA++ and ECDSA signature, which leads to larger packet size.

It is anticipated that VANET security mechanism can be improved with help of Trusted Platform Module (TPM) hardware chip. A previous work by [9] on TPM uses RSA method, which is large in size and takes longer time to generate signature. Performance analysis of RSA and ECC was given in [10], which resulted that ECC is faster in signing and key generation, while RSA only provides faster verification.

Therefore, there is an opportunity to find a solution for secure messaging among vehicle nodes in VANET by using TPM hardware. Specifically, the TPM chip could be utilized to establish trust among vehicular groups, such that secure safety messaging is allowed between them.

III. PROPOSED FRAMEWORK

Security is a prime concern for successful deployment of VANET applications. Periodic and event-driven safety messages are of great importance in this regard, particularly for life-safety applications, which their transmissions must be fast and secure.

Based on the requirement to provide hybrid cryptography scheme, we proposed a VANET security framework with support of TPM chip. The framework consists of three basic components: hardware entity (TPM chip), Group Entity, and Group Communication. To achieve trusted safety messaging in VANET, all the components are working collaboratively with each other as illustrated in Figure 1 to create a trusted group.

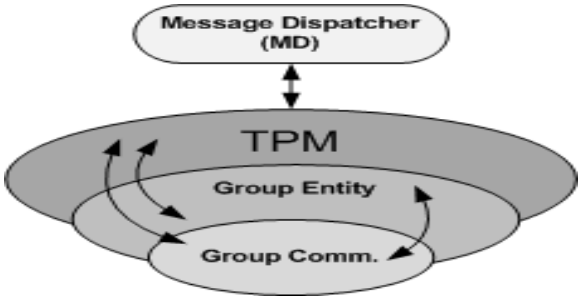

Figure 1. The proposed VANET security framework

A. Hardware Entity

Figure 2 illustrates the TPM hardware architecture, in which the chip is further divided into several sub-modules. The TPM is also interacting with its input/output components.

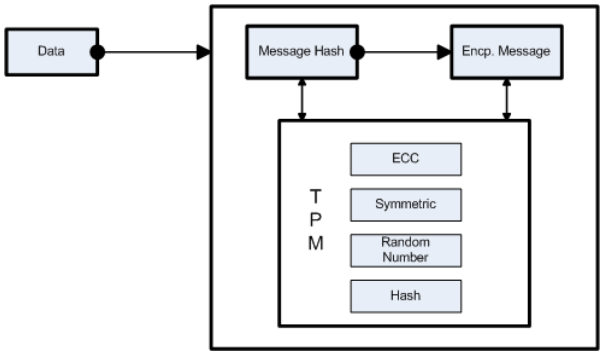

Figure 2. TPM hardware sub-modules and its security operations

Trusted Platform Module (TPM): Trusted computing chip come into the security arena to ensure that the trusted platform provides security features during the transmissions of safety messages. Its main role is to check that every component, as explained below, is working accordingly in perfect order without tempering [9]. TPM consists of many cryptographic engines: Asymmetric (ECC), Symmetric, Random Number Generator, and Hash. This is quite similar to module presented in [10].

Asymmetric module (ECC): The asymmetric acceleration engine generates elliptic curve cryptography (ECC), by which it also generates digital signature. The size of the digital signature is small, and can provide same level of security as that of the RSA or ECDSA. We use ECDSA as default.TPM uses endorsement key which is divided in two parts public key part and private key part. Private part burn into TPM chip by manufacturer and public key part is distributed to the users [9].

Symmetric module: The symmetric engine uses 128-bit cipher for encryption and decryption. The symmetric performance is very fast then the asymmetric, potentially hundreds or even thousand times faster.

Random Number Generator (RNG): Random number generator will generate the seed numbers.

Hash module: Hash engine will produce hash value using the Secure Hash Algorithm (SHA1).

TPM receives data from Message Dispatcher (MD) and converts it into hash value using the Hash engine. Next, by using ECC engine, it generates digital signature. Symmetric key also encrypted and send to receiver. At the receiving vehicle, it reverses the process and decrypts the received message using ECC engine and Hash engine.

When a node is selected as Group Leader (GL), TPM randomly selects a symmetric key from pre-loaded set of keys, by using Symmetric engine and RNG. The generated symmetric key is first converted into hash value, then it is encrypted with Attestation Identity Key (AIK) of GL, and subsequently shared among the group members via on-board unit (OBU). The receiving vehicle will first compute the hash value before decrypting and storing the key for symmetric event-driven message communications.

B. Group Entity

In VANET, it is possible to form groups of nearby vehicles in many ways. Common approaches are to geographically divide the road into segments, also known as cells (fixed), or make groups on the fly by using different clustering techniques. However, the underlying group formation process is beyond the scope of this study and we are concerned with behavior of the common group components like group leader and members. Hence, we assume that vehicles on a highway going in the same direction form group in order to share neighborhood information to achieve cooperative safety. Group consists of Group Leader (GL), Group Members (GMs), and a certain geographical area of fixed size. The GL selection can be made in different ways, e.g. on basis of node position [6]. Furthermore, we also assume that all the vehicles have been embedded with hardware chip entity, which is a tamperproof device.

C. Group Communication

Once a group has been established, communication is allowed among the group members. Figure 3 illustrates the working of a group communication by executing the following two processes.

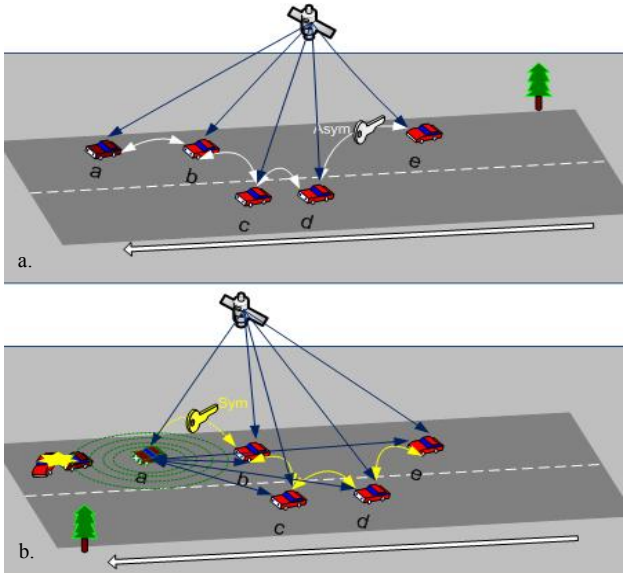

Figure 3. Group communications model a) asymmetric b) symmetric

Key generation: A GL generates a one-time symmetric key using TPM symmetric engine and distributes it to members via secure asymmetric communication. Each newly elected GL generates a new group key. Furthermore, one symmetric key is used for only one event-driven safety message.

Safety messaging: All periodic beacon exchange shall be made using asymmetric method. On the other hand, event-driven messages are delivered using symmetric key, which can improve message delivery time to the application, and thus giving more reaction time to driver. A new symmetric key is generated whenever a new GL is elected.

IV. ANALYSIS OF THE FRAMEWORK

As mentioned earlier, the final goal of the framework is to develop a trusted group of vehicle nodes in vicinity. With the trusted communication model, an enhanced level of relationship between nodes in a group is created, thus a trusted group is established. This is achievable when the symmetric key distribution for trust grouping is done via standard PKI security mechanism. In fact, the symmetric key is only used when a real safety-related event happening along the road.

An example of implementation of trusted group communication could be derived from Figure 3a. A group of vehicles is moving in the same direction along a highway, and the vehicles are exchanging periodic asymmetric safety beacon messages. Security method in this case is asymmetric, such as ECDSA. In Figure 3b, as soon as vehicle "a" detects a hazardous situation on the road, it immediately broadcasts event-driven safety messages using pre-loaded symmetric keys among the group members. This gives more reaction time to the drivers of the following vehicles.

The core differences between our and the other proposed TPM framework can be viewed from two points. First, the previous TPM framework support RSA, which provides fast signature verification but requires longer message transmission time. This is due to its size, which is about nine times larger than the ECDSA, as discussed in [2] and [10]. In comparison, our proposed framework supports ECDSA, which already been used in VANET. ECDSA is smaller in size but is slower in signature generation and verification. This can be an issue in event-driven safety messaging. To counter this, we proposed to use symmetric encryption method along with the ECDSA, which is inherently faster as compared to asymmetric methods. However, for periodic safety messaging, the ECDSA remains the first choice. Second point, the previously proposed symmetric solutions did not provide group trust relationship among the VANET vehicle nodes, which without this component a trusted group could not be established. Additionally, the proposed TPM-based security framework is also providing tampering protection not only from other vehicle nodes, but also from the transmitting vehicle node itself.

V. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a TPM-based security framework employing a unified hybrid security solution that takes advantage of TPM hardware chip, asymmetric and symmetric security keys distribution for fast and secure safety messaging in VANET. Importantly, the proposed framework is intended to achieve trusted group communication among the vehicle nodes within a group.

For future work, we intend to perform simulation tests to validate the expected outcomes from the proposed TPM-based VANET security framework.

ACKNOWLEDGMENT

The authors would like to thank Department of Computer and Information Sciences of Universiti Teknologi PETRONAS (UTP) for providing grant and facility for the research.

REFERENCES

[1] Jiang, D., Taliwal, V., Meier, A., Holfelder, W. & Herrtwich, R., "Design of 5.9 GHz DSRC-based vehicular safety communication," IEEE Wireless Communications, vol.13, no.5, pp.36-43, October 2006.

[2] M. Raya & J.P. Hubaux, "The security of vehicular ad hoc networks," Proc. of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN'05), 2005.

[3] A. Studer, F. Bai, B. Bellur & A. Perrig, "Flexible, Extensible and Efficient VANET Authentication", Proc. of the 6th Embedded Security in Cars (ESCAR) Workshop, November, 2008.

[4] M. Raya, A. Aziz & J.P. Hubaux, "Efficient secure aggregation in VANETs", VANET '06, Proc. of the 3rd. International workshop on Vehicular ad hoc networks, 2006

[5] G. Calandriello, P. Papadimitratos, J.P. Hubaux & A.Lioy, "Efficient and robust pseudonymous authentication in VANET" VANET '07, Proc. of the 4th. ACM international workshop on Vehicular ad hoc networks, 2007.

[6] .S. Ahren, L. Mark & P. Adrian, "Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs" Proc. of the SecureComm'07, 2007.

[7] T.L. Chun, S.H. Min & P.C. Yen, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks" ACM, vol.31, no.12, pp.2803-2814 2008.

[8] H. Moustafa , G. Bourdon & Y. Gourhant, "AAA in vehicular communication on highways with ad hoc networking support: a proposed architecture", Proc. of the 2nd ACM international workshop on Vehicular ad hoc networks, September 2005.

[9] G. Guette & C. Bryce, "Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs)", IFIP International Federation for Information Processing, 2008.

[10] Z. Huanguo, Q. Zhongping & Y. Qi, "Design and Implementation of the TPM Chip J3210," Trusted Infrastructure Technologies Conference (APTC '08), 3rd. Asia-Pacific , vol., no., pp.72-78, 14-17 Oct. 2008.