Partial Signature for Cooperative Intelligent Transport Systems

Hacene Fouchal, Alain Ninet

Partial Signature for Cooperative Intelligent Transport Systems

Hacène Fouchal[1] and Alain Ninet [2]
[1]CReSTIC, [2]LMR
Université de Reims Champagne-Ardenne, France
hacene.fouchal@univ-reims.fr, alain.ninet@univ-reims.fr

Abstract

On C-ITS (Cooperative Intelligent Transport Systems) vehicles send and receive sensitive messages informing about events on roads (accidents, traffic jams, etc, ..). The authentication of these messages is highly recommended in order to increase the users confidence about this system. This authentication ensures that only messages coming from trusted vehicles are accepted by receivers. An adapted PKI (Public Key Infrastructure) for C-ITS provides certificates for each vehicle. The certificate will be used to sign messages. This principle is used within deployed C-ITS solutions over the world. This solution is easy to implement but has one major flaw: each message needs to be sent with its signature and its certificate. The size of the message to send becomes high. In the meantime, for many C-ITS use cases, each message is sent many times for robustness reasons. The communication channel could be overloaded. In this paper, we propose to split the signature into some equal parts. When a message has to be sent, it will be sent with one of these parts. A receiver will save the received message with its actual part. For each reception, it will collect the remaining signature parts until all the signature parts are received. Our solution is implemented in a C-ITS architecture working through Bluetooth protocol using the advertising model. The solution is applicable for vehicle speeds reaching 130 km/h. We have proved, through a set of real experimentations, that our solution is possible.

***Index Terms*—C-ITS, VANETs, security, authenticity.**

I. Introduction

The deployment of C-ITS is a hot challenge in the era of smart cities. Urban roads and highways are often crowded. The dissemination of relevant information about traffic jams, accidents and road works help users to reduce their travel and to travel in safer conditions. A dedicated WIFI has been designed for connected vehicles: IEEE 802.11p (denoted also ETSI ITS-G5). The deployment of ITS-G5 hotspots (denoted RSU-Road Side Units) is on-going in many cities. V2V (vehicle-to-vehicle) and V2I (vehicle to infrastructure) communications become possible. The penetration rate of such technologies is still very low which makes the coverage of such technology very limited. In a previous work [1] we have used the BLE protocol (Bluetooth Low Energy) on smartphones used as receivers on vehicles. In this paper, we use the same environment for our experimentations.

We need to consider the authentication of senders in order to avoid untrusted drivers to notify fake events. It is recommended to handle PKI in charge of distributing certificates to all trusted vehicles in the eco-system. All messages are sent with their signature computed using their certificates. The certificate is also sent within the payload message.

Over ITS-G5, the message size could reach 1500 bytes. Most of usual notification messages (DENM: Decentralized Event Notification Messages) have a payload size between 200 and 300

978-1-7281-4905-9/20/$31.00 ©2020 IEEE

bytes where the size of the signature and the certificates is about 300 bytes.

Many solutions have been proposed to reduce this size; some of them have been deployed in ETSI standards as sending certificates only on-demand, sending the hash of the certificates.

The main contribution of this paper is to propose an additional mechanism: splitting the signature into many equal parts (partial signature). In each message only a partial signature is sent. When a message has to be sent, it will be sent with one of these parts. A receiver will save the received message with its actual part. For each reception, it will collect the remaining signature parts until all signature parts are received. Since messages are sent many times, we only modify the signature part in each sent message.

We have proven in [1] that BLE could be used with efficiency with vehicles, our present contribution is to experiment our splitting mechanism within the BLE protocol. Indeed, in the version 4.2 of this protocol (and later versions), the packet size could be 32 bytes for the advertising option. We have already proposed an architecture based on this protocol where the signature size is 16 bytes. But the whole signature size is 64 bytes (using the ECDSA algorithm: Elleptic Curve Digital Signature Algorithm). For our experimentations we split the signature into 4 parts. We have shown that for a speed of 130 km//h the vehicle is able to receive more than 20 messages during the receiving slot time (nearly 6 secondes). It is able to rebuilt the original message with all received messages and to verify the message signature even if some of these parts are dropped.

This paper is composed as follows: Section II describes some works dedicated to vehicular networks and security of exchanged messages. In section III we present the unsual security mechanism handled in C-ITS. Section IV presents the experimental environment of the study. V is dedicated to detailed processes used in this solution. Section VI give some conclusions and ideas about future enhancements of the study.

II. Related works

[2] presents another alternative to WAVE/DSRC. It mixes three technologies: Wi-Fi Direct, ZigBee and Cellular Network. Wi-Fi Direct is used as a direct link between nodes. ZigBee is used to connect roadside sensors and Cellular Network for long distance communications. [3] uses the same principle, however this paper does not take into account the hybridation between ITS-G5 and Cellular Network.

In [4], the authors propose a new network architecture deployed in Spain on vehicles switching between 802.11p and 3G, depending on the availability of RSUs.

[5] presents a detailed study on performance evaluation of IEEE 80211.p networks versus LTE (Long Term Evolution) vehicular networks. The authors have measured some performance indicators as the end-to-end delay for both networks in different scenarios (high density, urban environments, etc.). Many important issues have been measured as network availability and reliability. The authors have proved through simulations that LTE solution meets most of the application requirements in terms of reliability, scalability, and mobility. However, IEEE 802.11p provides acceptable performance for sparse network topologies with limited mobility support.

[6] studies throughput of VANETs with unidirectional traffic for different conditions and transmission ranges of wireless equipments. All studied vehicles are randomly connected. The paper gives few results of simulation studies achieved on NS-2 toolbox. They have measured performances indicators in case of congestion.

In [7], an evaluation of vehicular communication networks through car sharing scenarios is detailed. They adopted a specific mobility model which has been imported to a simulator. They have worked on a grid Manhattan network and they have observed some performance parameters such as delay, packet loss, etc. They have shown that vehicular communication are realistic under some conditions.

Some recent studies have proposed various solutions either for privacy [8], [12], [13], [11]

and authenticity [10], [13].

III. Security architecture

A. Preliminaries

In the area of C-ITS (Cooperative Intelligent Transportation System), a protocol stack has been defined and standardized by the ETSI standardisation institute in Europe [14]. Over the *Transport-Networking* layer (defined as geo-networking layer), the *Facilities* layer has been designed in order to be an efficient interface between the application layer (close to the driver and the vehicle sensors) and the *Transport-Networking* layer. Many types of messages are provided by this layer. In this paper will focus only on one main message, DENM (Decentralized Environmental Notification Message). A vehicle sends DENM messages in order to inform of any event (i.e. accident, traffic jam, etc.). The event could be triggered automatically thanks to the connexion to the vehicle CAN (Controller Area Network) Bus. In fact, some smart rules are run on the OBU (On-Board Unit) which generates automatically appropriate messages. It could also generates manual messages for sensitive cases as animal on the road.

B. Privacy and authenticity

C-ITS security considers two main aspects:

- Authenticity: this aspect allows to consider only messages coming from trusted drivers.
- Privacy: this aspect allows to protect drivers data and avoid driver tracking.

Each involved vehicle in the eco-system has to subscribe to the PKI server. The subscription allows to provide a long term certificate (LTC) to the vehicle (signed by a root PKI).

A vehicle could sign its messages using this LTC by means of a TPM (Trusted Plateform Module) which embeds cryptographic processes and private keys with safety. Authenticity is very well ensured. But with such a mechanism, privacy is not guaranteed at all. Indeed, from a unique LTC we could extract private informations which give the opportunity to external observers to track drivers. In order to ensure privacy, it is usual to work with a set of pseudonym certificates (PCs)[3] for small periods. A vehicle should have a pool of PCs which should be up to date in order to be able to switch to another PC.

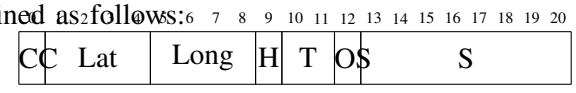
IV. BLE environment

In this section, we first propose the experimentation environment used in this paper. BLE advertising mechanism is used in the experimentations of our solution. The principle is to send beacons (16, 32, 64 or 128 bytes). BLE has been designed in order to advertise data wide areas in order to inform users about any product (in particular in restaurants, shopping centers, museums, ...). The communication is unidirectional without any connection between the sender and receivers. The adverser broadcasts an « Advertising » BLE message composed of Beacon code (which is a value fixed by the sender about the product to advertise) and any other relevant information. The receiver should run BLE scanner able to accept any BLE beacon and is able to wake-up a dedicated application according to the Beacon code value.

The senders denoted BLETransmitter, are deployed on roads and are connected to road operator management servers which monitor them by sending all relevant informations on roads.

A. Adapted notification message

We have defined a message format (inspired from the standard DENM format) containing the minimum information required to notify any event on the road. We only keep the mandatory fields defined in the ETSI standard. Our format is defined as follows:



Each field is defined as follows: **Cause Code CC)** or Event Cause Code mixed with its sub cause code (A translation table has been defined to match with the DENM standard codes) ; **Latitude Lat / Longitude Long** for The GPS Location ; **Heading (H)** - defines the angle between the vehicle's direction and the North side ; **Timestamp (T)** - defines the instant where the message has been produced ; **Offset (OS)** - defines the offset

of the signature part ; **Signature(S)** - defines the signature part of the message.

V. A proposed authentication solution

In this section, we give details of our contribution: splitting a signature into equal parts and insert a partial signature in each message to send.

A. Principle

We consider a message M to send. The signature S is provided by the signature algorithm embedded on the C-ITS station. We split S into N parts such as $S = S1, S_2, ..., S_N$. Each part S_i could be included at anytime in the whole message to send.

B. Communication algorithms

The algorithm 1 describes the actions to be run by each sender. When a message is valid, it has to be sent in a continuous way. But at each time, the signature field changes. One part among all parts is selected randomly and is inserted in this field of message. The sending of messages ends when the message is no more relevant (when it is not valid for instance).

The algorithm 2 describes the actions to be run by each receiver. The receiver catchs the first message and keeps receiving the same message but selects the received part of the signature, it is sorted in a temporary variable. The next time the same message is received, the signature part is also selected. When all the signature parts are received, the verification of the signature is run. If the signature is valid, then the message is accepted.

Algorithm 1 : Sender Algorithm

1: **Begin**
   - M *: Message*
   - S *: Signature parts*= $S = S1, S_2, ..., S_N$
   - VT *: Validity slot time of the event*
2: **while** (VT is valid) **do**
3: sends $M + Random(S, N)$
4: **end while**
5: **End**

Algorithm 2 : ReceiverAlgorithm

1: **Begin**
   - M_i *: Message* i
   - RS *: ReceivedSignatureSave contains the signature parts*
2: **while** (MessageVerified(M_i) == FASE) **do**
3: Receives M_i
4: Extracts S_j from M
5: Insert S_j into RS
6: **if** (RS is full and signature verified) **then**
7: MessageVerified(M_i) = TRUE
8: **end if**
9: **end while**
10: **End**

C. Experimentation with BLE

We have experimented the message sending with various vehicle speeds. Figure 1 shows how many times the message is received in the slot window of the sender. In fact this number depends on the protocol range. Indeed, the BLE protocol is supposed to have range of 100-500 meters. When a fixed sender broadcasts its message, it will cover a range of distance D. A vehicle driving through D will receive the message as long as it in D. When the speed increases, the time slot where the vehicle is in D is shorter, then the number of received beacons is lesser. In our experimentation, we need to split the signature into 4 parts in order to fit with the defined structure of the adapted notificationpacket. Then if the vehicle speed is less than 130 km/h, this decomposition is possible and the vehicle is able to rebuilt the entire signature.

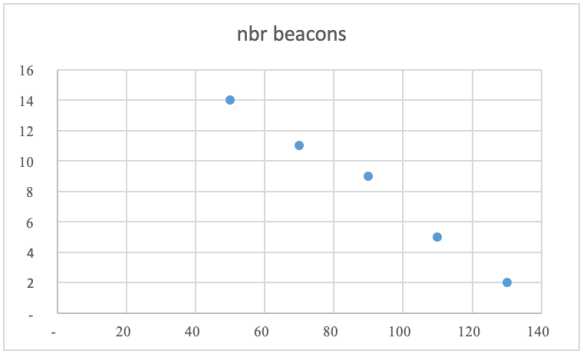


Figure 1: Number of beacons vs. speed

VI. Conclusion

In this paper we have proposed a simple solution for reducing the signature size of messages in the area of C-ITS. Indeed, the main idea is to split the signature in small parts. We only insert one part in each sent message. The messages will be repeated many times but with other signature parts.

The receiver will collect all messages and rebuilt the entire signature with all different parts. When all parts are recovered, the message could be verified and could be computed.

We have experimented this mechanism with the BLE protocol. This protocol is suited for such environment: beacons are sent continuously (the frequency could be 10 hz). We have shown that for the BLE protocol the vehicle speed has an impact on the obtained results. The splitting is different. More the speed is high, less the number of signature parts is.

We intend to investigate if we could verify the validity of the message without getting all the signature parts. Indeed, in this study we assume that all different messages are properly received. As a future works, we intend to test better the scalability of our system by launching simulations. In the meantime we intend to analyse the security performances of signing and verifying processes.

Acknowledgement

This work was made possible by EC Grant No. INEA/CEF/TRAN/A2014/1042281 from the INEA Agency for the SCOOP project. The statements made herein are solely the responsibility of the authors.

References

[1] Kevin Thomas, Hacène Fouchal, Stephane Cormier, Francis Rousseaux: Intelligent Transport System Based on Bluetooth. Nets4Cars/Nets4Trains/Nets4Aircraft 2019, pp: 50-59, Lecture Notes in Computer Science 11461.

[2] S. U. Bhover, A. Tugashetti and P. Rashinkar, V2X communication protocol in VANET for co-operative intelligent transportation system," International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, 2017, pp. 602-607.

[3] S. Jeong, Y. Baek and S. H. Son, A Hybrid V2X System for Safety-Critical Applications in VANET, 2016 IEEE 4th International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA), Nagoya, 2016, pp. 13-18.

[4] Jose Santa, Pedro J. Fernandez, Fernando Perenaguez-Garcia. Deployment of vehicular networks in highways using 802.11p and IPv6 technologies. IJAHUC 24(1/2): 33-48 (2017)

[5] Z. H. Mir and F. Filali. LTE and IEEE 802.11p for vehicular networking: a performance evaluation. *EURASIP J. Wireless Comm. and Networking*, 2014:89, 2014.

[6] W. Lu, Y. Bao, X. Sun, and Z. Wang. Performance evaluation of inter-vehicle communication in a unidirectional dynamic traffic flow with shockwave. In *Proceedings of the International Conference on Ultra Modern Telecommunications, ICUMT 2009, 12-14 October 2009, St. Petersburg, Russia*, pages 1–6, 2009.

[7] W. Lu, L. D. Han, and C. R. Cherry. Evaluation of vehicular communication networks in a car sharing system. *Int. J. Intelligent Transportation Systems Research*, 11(3):113–119, 2013.

[8] Hyunbum Kim, Jalel Ben-Othman and Lynda Mokdad, UDiPP: A framework for differential privacy preserving movements of unmanned aerial vehicles in smart cities, *IEEE Transactions on Vehicular Technology*, 68(4), 3933–3943, 2019

[9] Hacène Fouchal, Emilien Bourdy, Geoffrey Wilhelm, Marwane Ayaida: Secured Communications on Vehicular Networks over Cellular Networks. ICDCIT 2019: 31-41, Lecture Notes in Computer Science 11319, Springer 2019,

[10] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan. Vehicular ad hoc networks (vanets): status, results, and challenges. *Telecommunication Systems*, 50(4):217–241, 2012.

[11] Hichem Sedjelmaci, Makhlouf Hadji, and Nirwan Ansari, Cyber Security game for Intelligent Transportation System", *IEEE Network Magazine, 2019*,

[12] Boualouache, S. M. Senouci and S. Moussaoui, A survey on pseudonym changing strategies for Vehicular Ad-Hoc Networks, *IEEE Communications Surveys & Tutorials,* vol. 20, no. 1, pp. 770-790, Firstquarter 2018. doi: 10.1109/COMST.2017.2771522

[13] H. Fouchal, J. Biesa, E. Romero, A. Araujo, O.N. Taladrez A security scheme for wireless sensor networks *2016 IEEE Global Communications Conference (GLOBECOM), 1-5*

[14] European Telecommunications Standards Institute (ETSI), Available at: http://www.etsi.org.