Modelling of Security Principles within Car-To-Car Communications in Modern Cooperative Inteligent Transportation Systems

Jan DURECH, Maria FRANEKOVA, Peter HOLECKO, Emilia BUBENIKOVA

Department of Control and Information Systems, Faculty of Electrical Engineering, University of Zilina,
Univerzitna 1, 010 26 Zilina, Slovak Republic

jan.durech@fel.uniza.sk, maria.franekova@fel.uniza.sk, peter.holecko@fel.uniza.sk,
emilia.bubenikova@fel.uniza.sk

DOI: 10.15598/aeee.v14i1.1279

Abstract. *Intelligent transportation systems (ITS) bring advanced applications that provide innovative services for various transportation modes in the area of traffic control, and enable better awareness for different users. Communication connections between intelligent vehicles with the use of wireless communication standards, so called Vehicular Ad Hoc Networks (VANETs), require ensuring verification of validity of provided services as well as services related to transmission confidentiality and integrity. The goal of this paper is to analyze secure mechanisms utilised in VANET communication within Cooperative Intelligent Transportation Systems (C-ITS) with a focus on safety critical applications. The practical part of the contribution is dedicated to modelling of security properties of VANET networks via OPNET Modeler tool extended by the implementation of the OpenSSL library for authentication protocol realisation based on digital signature schemes. The designed models simulate a transmission of authorised alert messages in Car-to-Car communication for several traffic scenarios with recommended Elliptic Curve Integrated Encryption Scheme (ECIES). The obtained results of the throughput and delay in the simulated network are compared for secured and no-secured communications in dependence on the selected digital signature schemes and the number of mobile nodes. The OpenSSL library has also been utilised for the comparison of time demandingness of digital signature schemes based on RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorithm) and ECDSA (Elliptic Curve Digital Signature Algorithm) for different key-lengths suitable for real time VANET communications for safety-critical applications of C-ITS.*

Keywords

Authentication protocol, C-ITS, C2C communications, digital signature schemes, modelling, OPNET Modeler, security, throughput, traffic scenarios, VANET networks.

1. Introduction

Traffic control under its constantly growing volume cannot get along without the support of information and communication technologies provided by the Intelligent Transportation Systems [1]. Currently, a significant role is played by the development of a new generation of Cooperative Intelligent Transportation Systems which, together with wireless communication infrastructure, provides important information directly to a driver in a moving vehicle [2].

C-ITS introduce a technology which allows cars to communicate with each other or more precisely to communicate with the infrastructure. The reason of implementing such technology is to increase safety on the roads through raising awareness of the situation. Vehicles communicate with each other and with static units located along infrastructure by broadcasting critical and non-critical messages. These messages can contain information e.g. about location of vehicles, their speed and the information about unusual events on the road.

Many currently operating commercial systems of this type work on the principle of image information analysis, for example the Lane Departure Warning Systems (LDWS) [3], [4], [5], [6], which are based on a machine vision technology and monitor the position of a vehicle in the driving lane and alert the driver if the vehicle is departing or is going to depart the track [7].

Currently the problem of integration of the offered ITS services into a large complex is very actual [8]. While implementing these goals it is necessary to form communication connections between intelligent vehicles with the use of wireless communication standards, so called Vehicular Ad Hoc Networks (VANETs), which also requires to ensure verification of validity of the provided services as well as the services related to the transmission confidentiality and integrity.

The Car 2 Car Communication Consortium (C2C-CC) [8] was established in Europe in 2004 by six European car companies (Audi, BMW, DaimlerChrysler, Fiat, Renault and Volkswagen) with the goal to create an open standard for inter-vehicle communication using a wireless technology (IEEE 802.11 standard). The communication in VANETs is realised using an On Board Unit (OBU) and a Road Side Unit (RSU). The OBU is a transceiver/receiver operating on a principle of Dedicated Short Radio Communications (DSRC). Typically, it is installed inside the vehicle or on the vehicle. Portable OBUs are also being considered. The OBU can be operational while the vehicle or the person is moving or is idle. The On Board Unit transmits data on a single or several channels. The OBUs installed within a vehicle communicate with the RSUs and with other OBUs. The RSU is a short-range DSRC transceiver/receiver (typically tens of meters) which is installed along a road or sidewalk. It can operate only in a stationary mode. The RSU transmits data into the OBUs or exchanges data with the OBUs in its communication areas. The RSU also performs a function of an access point according to IEEE 802.11 with other DSRC functions. Several research groups are currently participating in VANET development in distinct projects, for example CARLINK, SeVeCom, CAR 2 CAR, Safespot, CVIS, Watch – Over, Aktiv, PRECIOSA, simTD etc [9], [10], [11], [12], [13], [14]. Generally, the applications utilising VANET can be categorised into: traffic control applications, logistics and freight traffic control, safety applications and safety-critical applications, maintenance and operational applications. The security of C2C communication in VANET is primarily dependent on the cryptographic algorithms and on the overall robustness of security mechanisms, including security protocols and organisational measures. Cryptographic algorithms and schemes are fundamental blocks of a security solution. The recommendations with orientation to secure services implemented in C-ITS and its application are described in IEEE 1609.2 [15].

The authors focus only on the safety oriented applications which require to ensure the nonrepudiation service and freshness of message, which is in many cases combined with the service of confidentiality and the integrity is provided by distinct cryptographic constructions and must be realized in real time.

2. Principle of Message Authentication in Car-to-Car Communications

Research work in the sphere of vehicular networks is concentrated mainly on the following areas: routing protocols, power of antennas, elimination of error rate, control of mobility, realisation of database systems [?] but also on the solution of security architecture on the base of modern cryptographic constructions using PKI (Public Key Infrastructure) and CAs (Certification Authorities). The security architecture of VANET for C-ITS consists of several elements. It is concerned with widespread range of mechanisms located in a particular section of C-ITS. A more detailed description of it can be found e. g. in [16].

In the contribution, we present a secure architecture of V2V and V2I only for securing safety-related message transmissions in safety-critical applications.

According to the chosen digital signature scheme, the vendor assigns each node a pair of cryptographic keys, the public and the secret vehicle key $K = PK_V, SK_V$. These are the long-term keys. The Certification Authority (CA) assigns a long-term certificate for the public vehicle key PK_V. Secret keys are stored in the vehicle in a so called Hardware Security Module (HSM), which at the same time provides a secure time base when generating the time-stamps for the digital signature. The HSM also manages all cryptographic operations with keys. In case of threatening this sensitive information they should be deleted from the HSM module. Digital signature schemes in contrary to common commercial applications (banking systems) utilise the pseudo-anonymous identification when authorising messages within vehicular communication networks, thus providing security and anonymity of the vehicle owner. In order to obtain a pseudonym, a set of key pairs is generated within the vehicle and public keys are sent to the corresponding CA via a secure communication channel. Then the certification authority signs each of the public keys and generates a set of pseudonyms for each vehicle. Each pseudonym contains an identifier of the CA, lifetime of the pseudonym, the public key and the signature of the CA, hence no information on vehicle identity is provided [17].

The frequency of pseudonym changes depends on the degree of the vehicle protection, input parameters (position, speed) and system settings. To ensure other pseudonyms, so called pseudonyms sets are being used.

These pseudonyms are periodically supplemented from CA. In the moment, when a node transits from the pseudonym set 1 to the pseudonym set 2, it is no longer allowed to utilise any pseudonym from the set 1.

Before sending a safety related message a digital signature is generated in the security unit of the vehicle V_1 using its secret key SK_{V1}. The signature is a function of message M as well as the header H, as in the principle depicted in Fig. 1.

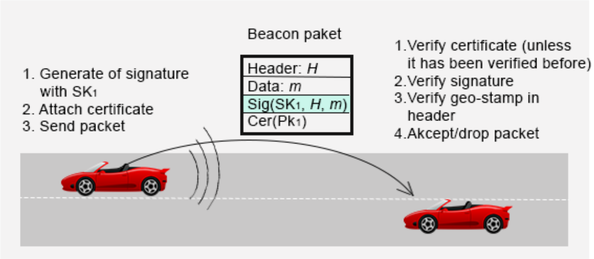


Fig. 1: The transmission of authorized messages between vehicles.

This way created cryptographic number is attached to the message together with the certificate *Cert*, which is coupled on the i-th anonymous sender public key PK_{iV1}, which is certified by the corresponding CA. On the side of vehicle V_2, the received certificate is validated first (if not done before) and the received digital signature is verified using the i-th public vehicle key PK_{iV1}, which is downloaded in periodic intervals by the vehicle V_2 (or other vehicles). Simultaneously, the *geo stamp* information is verified from the header H and after these procedures the safety relevant message is accepted or not.

The process of generation of digital signature by vehicle V_1 can be mathematically described as follows:

$$V_1 \rightarrow * : M, H, Sign_{SK_{iV1}} \left[(M, H) \mid T \right], \ldots \\ Cert_{PK_{i1}}, \tag{1}$$

where: M represents the sending safety relevant message, H represents message header, SK_{iV1} is a short-term secret vehicle key of vehicle V_1 in i-th moment, PK_{iV1} is a short-term public vehicle key of vehicle V_1 in i-th moment, T is a time-stamp, $Cert$ is a short-term certificate of vehicle V_1 (for anonymous public key PK_{i1}), represents the number of receivers (in case the message is sent to several vehicles).

The current certificate of vehicle V_1 valid in the i-th moment for the anonymous public vehicle key (PK_{i1}) contains:

$$Cert^i_{V1} \left\lfloor PK^i_1 \right\rfloor = \\ = PK^i_{V1} \mid Sign_{SK-CA} \left\lfloor PK^i_{V1} \mid ID_{CA} \right\rfloor, \tag{2}$$

where: $Sign_{SK-CA}$ represents the certificate signature of the corresponding certification authority based on its secret key $SK - CA$, ID_{CA} represents a unique identification number of the corresponding certification authority.

A conceptual design of security functions for vehicular communications within a single node is presented in Fig. 2.

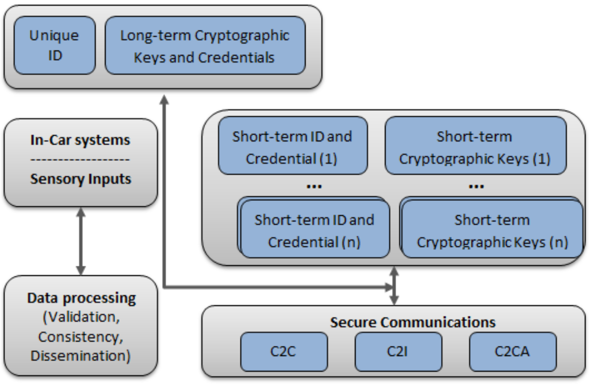

Unique ID
Long-term Cryptographic Keys and Credentials
In-Car systems
Sensory Inputs
Short-term ID and Credential (1)
Short-term Cryptographic Keys (1)
...
...
Short-term ID and Credential (n)
Short-term Cryptographic Keys (n)
Data processing (Validation, Consistency, Dissemination)
Secure Communications
C2C
C2I
C2CA

Fig. 2: Conceptual secure VC view: node functionality [17].

3. Analysis of Attacks to Car-to-Car Communications

Before designing the security architecture of C2C using VANET, it is necessary to address the analysis of risks which can occur during transmission of information messages in a wireless environment. Regarding an open transmission system, the number of network attacks is a variable which has to be monitored because the progress in cryptographic transmission development also implies the increase of development in possible attacks and related cryptographic attacks. It is necessary to consider attackers who do not attack only outside from network side, but directly in vehicle (inside attackers). To mention a few of them [18]:

- Denial of Service (DoS) attack: A type of attack where the attacker either disrupts the communication channel or overloads computational resources of the vehicle. The attack can be performed by overloading the communication band or overloading by transmitting high number of messages.

- Message manipulation: The attacker injects fake messages into communication or holds the retransmission of messages. One motivation can be sending messages about road congestion and thereby forcing other vehicles to use an alternative route and clearing the road for the attacker. Another case can be faking a priority vehicle and thereby accelerating attackers drive.

- Retransmission of messages and tunnel attack: The attack is similar to the previous by retransmitting a message after some time or in a different place via a tunnel using an external communication channel.

- Eavesdropping: The attack is based on capturing messages and their analysis. The attack violates privacy.

- Privacy violation: The attacker can monitor vehicles and drivers via their communication. The attack can be based on monitoring the RF fingerprint for identification and recognition of the vehicle.

- Masking and Sybil's attack: In masking the attacker impersonates themselves as another vehicle using fake identification, while in Sybil's attack they presents themselves as several vehicles. The attacker can generate data on road congestion or if the removal of corrupt devices is based on voting, they can vote with all fake identities for the removal of certain vehicle from the network.

- Discovery of secret keys: The attacker can gather secret keys from OBU or RSU. The attack is based on memory retrieval or utilisation of side-channel.

In this example of forgery attack attackers diffuse wrong information in the network to affect the behavior of other drivers (e.g., to divert traffic from a given road and thus free it for them, as illustrated in Fig. 3).

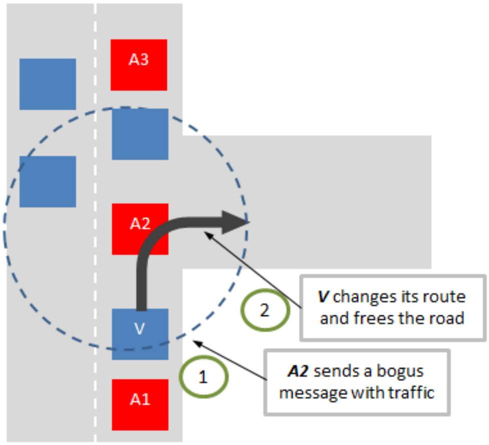

A3
A2
V
A1
1
2
V changes its route and frees the road
A2 sends a bogus message with traffic

Fig. 3: Example of forgery attack [19].

4. Parameters of Efficient and Robust Digital Signatures Schemes for Car-to-Car Authentication

Digital signatures are used for secure communications in VANETs. Messages are signed with the private keys corresponding to the current pseudonym. The messages in the schemes of digital signatures also contain the time stamps, the sender's clock value, geo stamps and the sender's coordinates at the sending time.

Currently, in the commercial sphere, following asymmetric cryptography digital signature schemes are being utilised [20]:

- Digital signature scheme with the Rivest, Shamir, Adleman (RSA) algorithm.

- Digital Signature Algorithm (DSA) with the modified El Gamal's algorithm.

- Digital Signature Algorithm (ECDSA) scheme with the elliptic curve algorithm.

In the process of selection of digital signature schemes for car-to-car messages authentications, the following parameters are important: total message size, size of safety message, size of cryptographic overhead, throughput of vehicular network, number of communicating vehicles, message rate and maximum tolerable processing delay per message.

According to DSRC standard messages within VANET communications are transmitted with a periodicity of 100 to 300 ms. From this the upper bound on the processing time overhead T_{OH} is defined by:

$$\begin{gathered} T_{OH} = T_{Sign}\left(M\right) + \\ T_{TX}\left(M \mid SIG_{prKV}\left[M\right]\right) + T_{Ver}\left(M\right), \end{gathered} \tag{3}$$

where $T_{Sign}\left(M\right)$, $T_{TX}\left(M \mid SIG_{prKV}\left[M\right]\right)$, T_{Ver} are necessary durations for signage, transmission and verification of the message. $T_{sign}\left(M\right)$ is the time required for singing M, T_{Ver} is the time required for verifying M, $Sign_{PrKv}\left[M\right]$ is the signature of message M from sender V and contains the key signed by Certification Authority and $T_{tx}\left(Sign_{PrKv}\left[M\right]\right)$ is the time required for transmitting a signature.

An approximate comparison of key lengths (in bits) for the most widely used patterns of digital signature using asymmetric algorithms is introduced in Tab. 1.

A short key-length (in comparison with RSA and DSA schemes) and the related low computational demandingness predestines the ECDSA for deployment in

Tab. 1: Comparison of key lengths for digital signature schemes.

Asymmetric algorithm			Security
DSA	**RSA**	**ECDSA**	**until year**
L=1024, SK=160	N=1024	n=160–223	2010
L=2048, SK=224	N=2048	n=224–255	2030
L=3072, SK=256	N=3072	n=160–233	2030
L=7680, SK=384	N=7680	n=384–511	2030
L=15360, SK=512	N=15360	n=512– more	2030

Note: L, N, n are parameters of public keys of DSA, RSA and ECDSA

devices with limited computational capacity and limited memory, which includes intelligent vehicle applications. In order to accelerate the computation (for mathematically complex schemes utilising asymmetric cryptographic algorithms), the tendency of integrated schemes is pushed forward. These perform two or three security functions in a single algorithm. This direction has also been chosen by the researchers in the SeVeCom project, who recommend to use not the original, but the modified ECDSA scheme [21].

Within the SeVeCom project, the hybrid ECDSA scheme – Elliptic Curve Integrated Encryption Scheme (ECIES) has been selected within the digital signature scheme implementation, which supported secure services authentication of messages with the combination of confidentiality and message integrity.

5. Model Realisation of an Authentication Processor

For model realisation of an authentication processor which simulates a part of HSM module in OBU units within C2C communications, the authors utilised the OPNET Modeler tool [22]. The OPNET software supports libraries written in C or C++ languages. This enables the utilisation of distinct libraries source codes related to security, for example the OpenSSL library. In this work, the OpenSSL-1.0.1f version has been used for models design.

In the OpenSSL library, we use our modified C-code for signing messages using ECIES scheme, which was recommended as effective cryptography scheme for VANET applications [23].

Figure 4 shows the placement of security blocks within the designed model. The „Authentication processor“ block controls the entire data flow from the source (moving vehicle) into VANET and performs security operations (encryption and digital signature using the ECIES). The „Verification processor“ block on the receiver side (in vehicle or Road Side Unit) controls the data flow from the network to a node and performs the verification of received messages.

Functions performed in the authentication processor:

- Generation of hash code H-MAC (Hash – Message Authentication Code) on the base of SHA-1 (Secure Hash Alhorithm) - **digest**.
- Authentication of this output by the ECDSA algorithm, resp. generation of digital signature - **signature**.

The model of the authentication processor designed in the process editor is shown in Fig. 4. It is a state diagram consisting of two states **St_0** and **St_1**.

The generation of hash code is performed in state 0 (**St_0**) and the digital signature is generated in state 1 (**St_1**). State 0 is implicit and its output value is a hash code (the **digest** variable in source code) and return value **hmac_done**. The variable **hmac_done** acquires value 1 in case of a successful hash code generation. After getting this value, the condition for a transition to state 1 is valid. If this state occurs, the generated hash code is signed and output variables **signature** and **state** are created. The signature variable represents the signature attached to a message and the state variable after getting value 1 passes the condition to perform the **MAC_PACKET_HANDLE** function. This function forwards the message into the next level (**ARP, wireless_lan_MAC, wlan_port**), which consequently sends it to VANET.

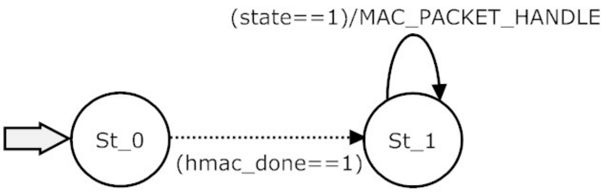


Fig. 4: Authentication processor model.

Functions performed in the verification processor:

- Generation of hash code from the message using H-MAC – **digest**.
- Signature verification - **verify**.

The state diagram of verification processor is shown in Fig. 5. It is composed of two states. In state 1 (**St_1**), the same operation is performed as in the authentication processor, i.e a hash code is generated from the received message using H-MAC (SHA-1). After generating the hash code the condition for transition into state 2 (**St_2**) is valid and the signature verification operation can be performed - **verify**. The input variables of this function are the key (**eckey**), hash code (**digest**) and the signature (**signature**). The return value of this function is the variable **ret**. In case of value 1, the signature has been evaluated as valid and a transition is activated, which enables to perform the **IP_PACKET_HANDLE** action. This action enables access to the message from the lower level (in Fig. 6 denoted **Internet Protocol**). In case the **ret** variable gets another value, the **DROP_PACKET** action is performed – the signature is not valid. This action also deletes the invalid message.

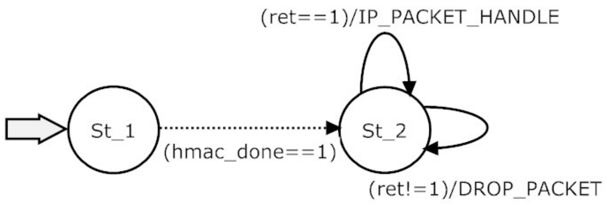


Fig. 5: Verification processor model.

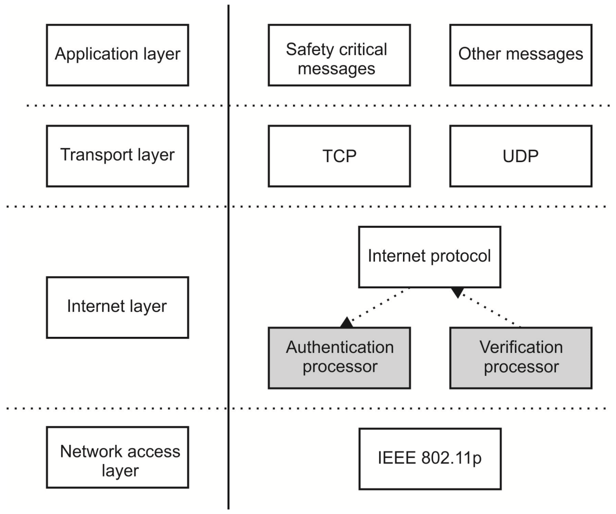


Fig. 6: Implementation of security blocks at the IP layer.

For the encryption of the message, we utilised the **aes_cbc.c** source code from the OpenSSL project to create a hash code **hmac.c**. The source code includes functions not only for signature generation, but also for the verification of integrated digital scheme – the **ecdsa.h** function. The source code with predefined parameters for digital signatures operations was joint to output data from the previous state (H_MAC output, keys). For a proper operation of these subprograms, it is necessary to include the used libraries (**INCLUDE**) into the OPNET installation directory. A link to these libraries has to be inserted into the header block, not directly into the individual states. These subprograms are able to operate within the separated signature and authentication part (with modifications), but also within a single unit (see Fig. 7).

The OpenSSL project contains several predefined elliptic curves. A list of all available elliptic curves can be found in [20]. For the simulation purpose, we chose the P-384 elliptic curve, in OpenSSL denoted as follows: **secp384r1: NIST/SECG curve over a 384 bit prime field**. It is the elliptic curve (EC) $E_p(a,b)$ defined over a finite body F_p (p=384), where p is an even prime number and represents the key length. According to [21], the prime number EC is more advantageous for the software implementation in comparison to EC over a finite body F_2^m or Koblitz curves.

The overall communication security model using the ESCIS scheme is shown in Fig. 7.

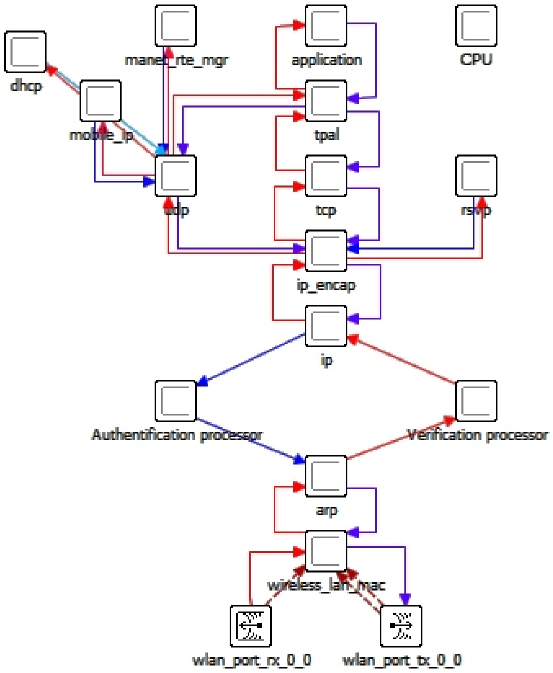


Fig. 7: Demonstration of overall communication security model in OPNET Modeler.

6. Obtained Results

The authors in parallel performed a comparison of time demandingness of ECDSA scheme generation and verification in dependence on key length on simulated OBU units.

We created a simple simulation to demonstrate the computational demandingness of chosen digital signatures. It has been tested on a computer with Intel Dual Core processor with frequency of 2.3 GHz. We performed the calculations using a virtual device that we created for this purpose using the VirtualBox software and additional software, needed for the proper OpenSSL operation. We focused on the ECDSA digital signatures with key length 160, 192, 224, 256, 384 and 521 bits for several types of elliptic curves (EC) on the base prime field, binary Koblitz curve and pseudorandom curves. Within the simulation, the message with a predefined length was signed by a private key with a measured length and the number of signatures during the 10-second interval has been noted. Consequently, the message verification using a public key during the 10-second interval has been done.

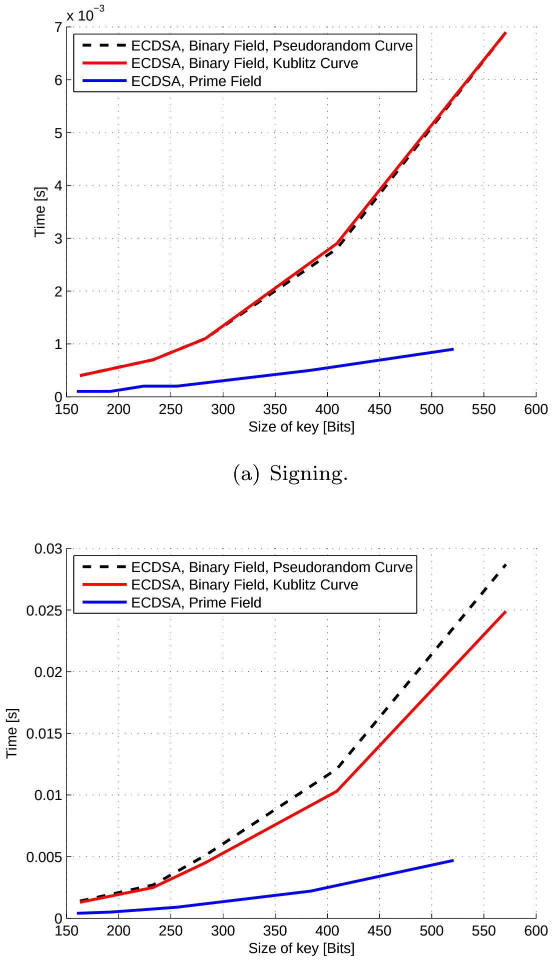
At first, we compared demandingness of different EC in the process of signing and verification, where we found out that ECDSA prime field curves are the fastest (Fig. 8(a) and Fig. 8(b)). Next we chose ECDSA Prime field curve and compared it to RSA, DSA cryptographic schemes.

The obtained results of measured time of generation and verification are presented in Tab. 2 which contains (from the left): the algorithm name, the key length, the number of messages signed during 10 seconds, the number of messages verified during 10 seconds, the average time of signing of one message and the average time of verification of one message in seconds. The graphical results for three selected digital signatures schemes (RSA, DSA and ECDSA) are shown in Fig. 9(a)) - generation and Fig. 9(b)) - verification.

Tab. 2: The results of measured time for generation and verification of digital signature.

	Key	**Private**	**Public**	**Sign [s]**	**Verify [s]**
RSA	512	73148	789777	0.000137	0.000013
RSA	1024	13272	254362	0.000747	0.000039
RSA	2048	2045	64246	0.004873	0.000155
RSA	4096	268	17040	0.037068	0.000574
DSA	512	74480	68644	0.000134	0.000145
DSA	1024	24869	21805	0.000401	0.000459
DSA	2048	6469	5545	0.001533	0.001802
ECDSA	160	92305	24595	0.0001	0.0004
ECDSA	192	73776	18892	0.0001	0.0005
ECDSA	224	57669	14097	0.0002	0.0007
ECDSA	256	47598	10836	0.0002	0.0009
ECDSA	384	22111	4551	0.0005	0.0022
ECDSA	521	11311	2122	0.0009	0.0047

From the obtained results we can see that the RSA scheme is faster in the verification process, which is important because vehicle will be signing just its own messages, but it needs to verify messages from all vehicles which are within the range. RSA is now one of the fastest algorithms in the verification process, but by the increase of key length during the next 30 years, RSA starts to be slower (Fig. 10). This is one of the reasons why ECDSA is deployed to the VANET networks as a perspective cryptographic scheme.



(a) Signing.

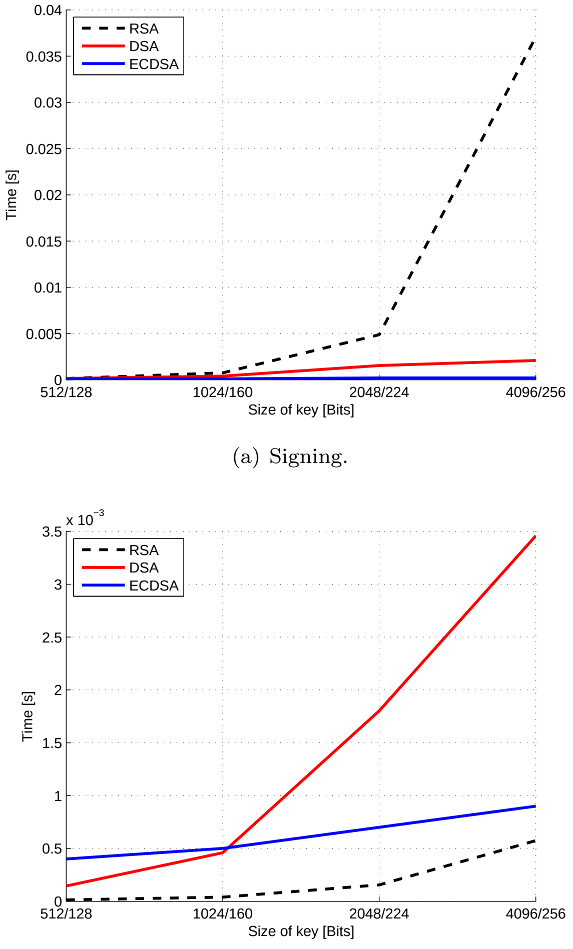
(b) Verification.

Fig. 8: Comparison of elliptic curves.

The second reason for using ECDSA is to save the frequency band of communication. From Fig. 11 we can see how the frequency band is loaded when several vehicles communicate using different size of messages.

7. Conclusion

With the development of intelligent transportation systems, it is necessary to handle the problems of transmission security in the C2X applications. Several cryptographic constructions have to be used; they have to be computationally secure and fast at the same time and do not load the VANET composed of a variable number of moving nodes. Nowadays, the development of integrated cryptographic schemes is being promoted, including several security services. The authors implemented a model of an authentication processor



(a) Signing.

(b) Verification.

Fig. 9: Example of time relations in RSA, DSA, ECDSA digital schemes.

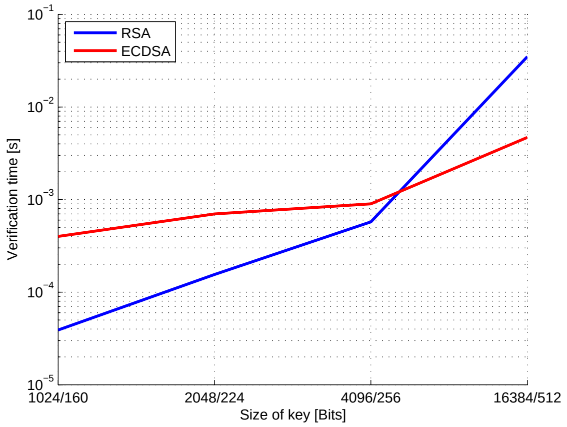


Fig. 10: Comparison of verification time in RSA, ECDSA scheme for equivalent key length.

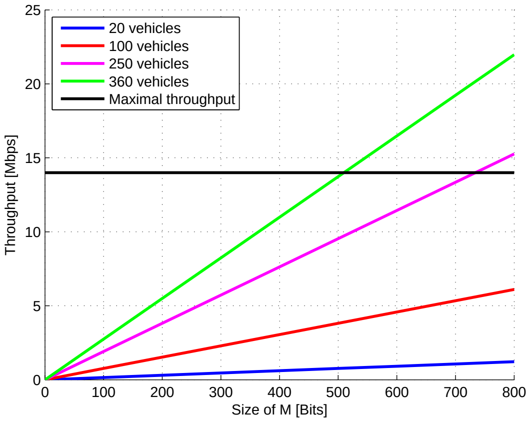


Fig. 11: Message size vs. system throughput.

via OPNET Modeler which was used for generation and verification of messages transmitted between C2C modified ECIES cryptography construction. Using the OpenSSL libraries, the authors analysed the performance and time demandingness of the ECDSA scheme for different key lengths and different shapes of elliptic curves as well as a comparison of time relation of digital signature schemes RSA, DSA and ECDSA has been performed. For several transport scenarios for a given number of vehicles the throughput parameter of VANET network was determined in dependence on message size.

Acknowledgment

This work has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number: 024ZU-4/2012: Modernization of technology and education methods orientated to area of cryptography for safety critical applications.

References

[1] ISO 14813-1:2007. *Intelligent transport systems – Reference model architecture(s) for the ITS sector – Part 1: ITS service domains, service groups and services*. Geneva: ISO, 2007.

[2] FAZIO, P., F. D. RANGO and A. LUPIA. Vehicular Networks and Road Safety: an Application for Emergency/Danger Situations Management Using the WAVE/802.11p Standard. *Advances in Electrical and Electronic Engineering*. 2013, vol. 11, no. 5, pp. 357–364. ISSN 1804-3119. DOI: 10.15598/aeee.v11i5.890.

[3] MIHAL, R. and I. ZOLOTOVA. Incidents, alarms and events in information and control systems. In: *2014 IEEE 12th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*. Herlany: IEEE,

2014, pp. 371–374. ISBN 978-1-4799-3442-3. DOI: 10.1109/SAMI.2014.6822442.

[4] HRUBOS, M. and A. JANOTA. Algorithm for Surface Creation from a Cloud of Points. In: *13th International Conference on Transport Systems Telematics (TST 2013)*. Katowice: Springer, 2013, pp. 42–49. ISBN 978-3-642-41646-0. DOI: 10.1007/978-3-642-41647-7_6.

[5] MACHACEK, Z., R. SLABY, R. HERCIK and J. KOZIOREK. Advanced System for Consumption Meters with Recognition of Video Camera Signal. *Electronics and Electrical Engineering*. 2012, vol. 18, no. 10, pp. 57–60. ISSN 2029-5731. DOI: 10.5755/j01.eee.18.10.3062.

[6] BUBENIKOVA, E., J. DURECH and M. FRANEKOVA. Security Solutions of Intelligent Transportation System's Applications with using VANET Networks. In: *Proceedings of the 2014 15th International Carpathian Control Conference (ICCC)*. Velke Karlovice: IEEE, 2014, pp. 63–68. ISBN 978-1-4799-3527-7. DOI: 10.1109/CarpathianCC.2014.6843570.

[7] BUBENIKOVA, E. *Detection of lanes in control applications of road transport*. Zilina, 2014. Dissertation. University of Zilina. Supervisor Prof. M.Sc. Maria Franekova, Ph.D.

[8] BUBENIKOVA, E., FRANEKOVA, M. and P. HOLECKO. Secure Solution of Collision Warning System Integration with Use of Vehicular Communications within Intelligent Transportation Systems. In: *12th IFAC Conference on Programmable Devices and Embedded Systems*. Velke Karlovice: IFAC, 2013, pp. 78–83. ISBN 978-3-902823-53-3. DOI: 10.3182/20130925-3-CZ-3023.00011.

[9] RESTA, G., P. SANTI and J. SIMON. Analysis of multi-hop emergency message propagation in vehicular ad hoc networks. In: *Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing - MobiHoc '07*. New York: ACM Press, 2007, pp. 140–149. ISBN 978-1-59593-684-4. DOI: 10.1145/1288107.1288127.

[10] KROH, R., A. KUNG and F. KARGL. Secure Vehicle Communications. Deliverable 1.1. VANETS Security Requirements Final Version. In: *Transport Reserch and Innovation Portal* [online]. 2006. Available at: http://www.transport-research.info/sites/default/files/project/documents/20130605_103517_12197_Sevecom_Deliverable_D1.1_v2.0.pdf.

[11] STUBING, H. *Car-to-X Communication: System Architecture and Applications. Multilayered Security and Privacy Protection in Car-to-X Networks*. 1st ed. Wiesbaden: Springer Vieweg, 2013. ISBN 978-3-658-02530-4.

[12] WEISS, C. SimTD proven possitive: Car-to-x technology is ready for market. In: *Safe and Intelligent Mobility* [online]. 2015. Available at: http://simtd.de/index.dhtml/object.media/enEN/8022/CS/-/backup_publications/Informationsmaterial/simTD_presentation_2013_en_web.pdf.

[13] KADAS, G. and P. CHATZIMISIOS. Collaborative Efforts for Safety and Security in Vehicular Communication Networks. In: *15th Panhellenic Conference on Informatics*. Kastonia: IEEE, 2011, pp. 117–121. ISBN 978-1-61284-962-1. DOI: 10.1109/PCI.2011.75.

[14] BENGLER, K., K. DIETMAYER, B. FARBER, M. MAURER, C. STILLER and H. WINNER. Three Decades of Driver Assistance Systems: Review and Future Perspectives. *IEEE Intelligent Transportation Systems Magazine*. 2014, vol. 6, no. 4, pp. 6–22. ISSN 1939-1390. DOI: 10.1109/MITS.2014.2336271.

[15] IEEE Std 1609.2-2013. *IEEE Standard for Wireless Access in Vehicular Environments: Security Services for Applications and Management Messages*. New York: IEEE, 2013.

[16] HARTENSTEIN, H. and K. LABERTEAUX. *VANETs: vehicular applications and inter-networking technologies*. 1st ed. Hoboken: Wiley, 2010. ISBN 978-0-470-74056-9.

[17] PAPADIMITRATOS, P., L. BUTTYAN, J.-P. HUBAUX, F. KARGL, A. KUNG and M. RAYA. Architecture for Secure and Private Vehicular Communications. In: *7th International Conference on ITS Telecommunications*. Sophia Antipolis: IEEE, 2007, pp. 1–6. ISBN 1-4244-1177-7. DOI: 10.1109/ITST.2007.4295890

[18] KARGL, F., P. PAPADIMITRATOS and L. BUTTYAN. Secure vehicular communication systems: implementation, performance, and research challenges. *IEEE Communications Magazine*. 2008, vol. 46, no. 11, pp. 110–118. ISSN 0163-6804. DOI: 10.1109/MCOM.2008.4689253.

[19] ABOOBAKER, A. K. K. *Performance Analysis of Authentication Protocols in Vehicular Ad Hoc Networks (VANET)*. London, 2010. Technical Report RHUL-MA-2010-2, Royal Holloway University of London, Supervisor Dr. Stephen Wolthusen.

[20] LEVICKY, D. *Cryptography in communications security*. 1st ed. Kosice: Elfa, 2014, ISBN 978-80-8086-235-0.

[21] BASSHAM, L., D. JOHNSON and W. POLK. ANSI X9.62. *Internet X.509 Public Key Infrastructure - Representation of Elliptic Curve Digital Signature Algorithm (ECDSA) Keys and Signatures in Internet X.509 Public Key Infrastructure Certificates. American Bankers Association.* New York: American National Standards Institute, 1999.

[22] Opnet Modeler 17.5 Documentation, In: *OPNET TECHNOLOGIES* [online]. 2013. Available at: http://opnet-modeler-documentation.software.informer.com/.

[23] JANECH, J., E. KRSAK and S. TOTH. The Architecture of Distributed Database System in the VANET Environment. *Informatica.* 2014, vol. 38, no. 3, pp. 205–211. ISSN 0350-5596.

About Authors

Jan DURECH was born in Zlate Moravce (Slovakia) in 1989. He received his Master (M.Sc.) degree in 2013 from the University of Zilina. He is currently a Ph.D. student. His research interests include security solution of wireless communications in the field of intelligent transport systems.

Maria FRANEKOVA was born in Brezno (Slovakia) in 1961. She received her Prof. in 2011 in the field of Automation with orientation to “Safety-related Control and Communication Systems”. Her research interests include assessment of safety communications on the base of coding and cryptography tools within safety-related applications.

Emilia BUBENIKOVA was born in Martin (Slovakia) in 1969. She received her Ph.D. from the University of Zilina in 2014 in the field of Automation with orientation to „Detection of lanes in control applications in road transport“. Her research interests include methods of image digital processing and control systems.

Peter HOLECKO was born in Zilina (Slovakia) in 1981. He received his Ph.D. from the University of Zilina in 2012 in the field of Automation and specialisation on sensor networks. Currently he is an assistant and his research interests include security of information systems and sensor networks.