ACTA TECHNICA CORVINIENSIS
– Bulletin of Engineering
Tome X [2017]
Fascicule 3 [July – September]
ISSN: 2067 – 3809

[1.]Ján ĎURECH, [2.]Mária FRANEKOVÁ,
[3.]Peter LÜLEY, [4.]Emília BUBENÍKOVÁ

SAFETY ASPECTS OF PKI ARCHITECTURE WITHIN C-ITS AND THEIR MODELLING

[1-4.] Department of Control and Information Systems, University of Žilina, 010 26 Žilina, SLOVAKIA

Abstract: The authors of this contribution focus on analysis of C2C communication in Cooperative - Intelligent Transportation Systems (C-ITS). In paper is proposed PKI (Public Key Infrastructure) secure architecture on the base of ECDSA (Elliptic Curve Digital Signature Algorithm) for several EC types. The experimental part is focused on worst case scenario of C2C communications for four-lane intersection, which model was realized via OPNET MODELER with OpenSSL libraries. From obtained results the influence of used elliptic curve and size of message to performance of the VANET network was analyzed.
Keywords: VANET; cooperative-intelligent transportation system; C2C; authentication protocols, traffic scenario, modelling

INTRODUCTION

The key aspect of cooperative intelligent transport systems (C-ITS) implementation to the real operation is the communication safety therefor it attracts the attention of research teams for long-time [1], [2]. C-ITS systems mostly use the wireless short-range communication through open transmission channel (so-called VANET network). This communication is introduced in order to improve the road safety by increasing the situation awareness of drivers. Vehicles communicate among themselves and with static units placed alongside infrastructure by critical and non-critical messages. These messages may contain data on vehicle location, its direction, speed, acceleration and other information such as special events that can occur during real traffic.

Development of C-ITS applications, which are using data obtained from vehicles and nodes placed alongside car to car, car to infrastructure respectively car to X communication (C2C, C2I or C2X), is supported by states around the world with links to car industry. Nowadays, there are within the EU an increasing number of projects dealing with C-ITS applications [3].

The most important applications for C-ITS are addressing the safety which uses VANET communication among surrounding entities (vehicles, road infrastructure) in order to reduce the number of accidents and also applications for the drivers and pedestrians protection against various dangers. Messages transmitted between vehicles can be repeated periodically (awareness messages) - so-called CAM (Cooperative Awareness Messages) or the messages are generated only when triggered by particular event (event driven messages) - so-called DENM (Decentralized Environmental Notification Messages).

Nowadays, based on outputs from various research projects in the EU and USA [4], [5], [6] are the C-ITS applications addressing safety divided in many categories respectively classes.

All these applications are designed to trigger alert before an accident (crash type).

The immediate reaction performed by the driver after receipt of unauthorized or altered (in any way) message can have negative impact on formation of traffic collisions. Therefore it is necessary to transmit messages of these applications secured by modern, computationally secure cryptographic algorithms. Providers of service (confidentiality, integrity and authorization) must guarantee the credibility of received messages and fulfillment of the application requirements (throughput respectively total network delay) even in the most unfavorable conditions (traffic-jam).

These services are in most cases realized by the cryptographic techniques and mostly with the link to asymmetric systems and Public Key Infrastructure (PKI) in connection with Certificate Authority (CA).
In the Figure 1 is shown the overview of digital signature cryptographic operations (only generation and verification part) respectively encryption in network or transport layer of communication protocol.

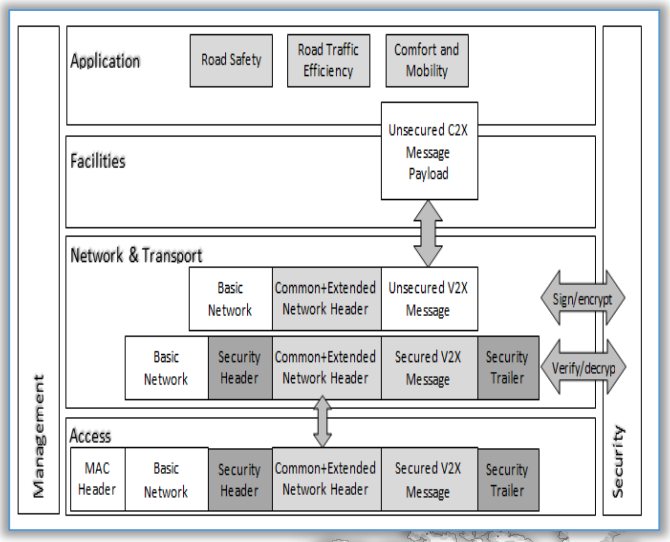

Figure 1. Safety ensured by the use of cryptographic mechanisms in the communication protocol

Aim of this article is to examine cryptographic safety solutions of Elliptic Curve Digital Signature Algorithm (ECDSA) digital signature scheme (for various algebraic structures a various types of Elliptic Curve (EC)) by modelling in the software tool OPNET Modeler in combination with open source cryptographic libraries and by the use of mathematical calculations.
These solutions can be used in C-ITS. Secondary aim is to compare how these solutions meet the requirements on the secure communication in VANET network (for critical scenarios – e.g. traffic jam at the intersection) depending on actual risks and potential safety incidents during the communication among mobile nodes.

RECOMMENDED CONCEPT OF PKI ARCHITECTURE AND ECDSA DIGITAL SIGNATURE SCHEMES

There exist several proposals of safety architectures for C2C, C2I communication through VANET networks [7], [8]. There are some deviations in countries of EU (represented mostly by C2C organization) and in countries of USA (represented for example by National Highway Traffic Safety Administration (NHTSA) [9], [10]. The common element is the conception based on PKI architecture with asymmetric cryptographic system in connection with certificate authorities. In the Figure 2 is shown the proposal of PKI architecture [7].

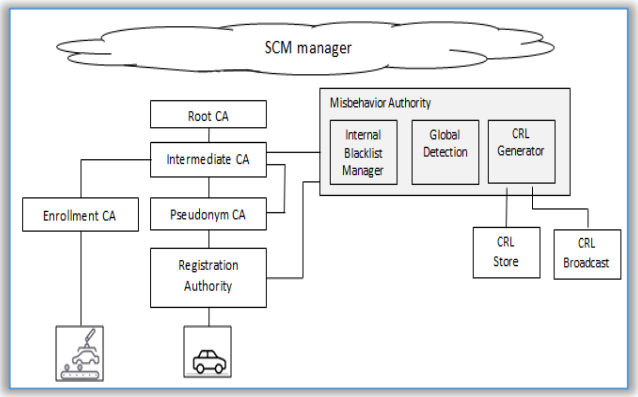

Figure 2. Recommended concept of PKI architecture

In the Figure 2 is shown general concept of PKI architecture. This concept can differ from actual implementation especially on the beginning when the number of vehicles equipped with on-borad unit (OBU) will be small (some levels of certificate authorities can be merged together). Proposed concept includes following parts:

- Security Credentials Management System (SCMS) – the highest control system which manages all iterations among components based on the machine to machine principle. These processes are performed automatically.
- Root Certificate Authority (RCA) – the highest authority on which is built the confidentiality of the PKI system. RCA signs certificates for itself therefor these certificates do not contain ID of signatory. Private key created by RCA is used to sign the certificates of other CAs or certificates of other parts of PKI. It is likely that RCA will work offline because compromising this authority can affect the safety of whole system.
- Intermediate Certificate Authority (ICA) – extension of RCA. Communication with ICA is protected against direct access to the internet (for example by Virtual Private Network (VPN) tunnel). Intermediate CAs can certify other subject and provide the system flexibility because they remove the need to establish connection between highly protected RCA and all other subjects.
- Misbehavior Authority (MA) – processes erroneous messages and develops/publish the list of cancelled certificates Certificate Revocation List (CRL).
- Pseudonym Certificate Authority (PCA) – issues short-term certificates to ensure the user privacy. Pseudonyms lifetime is variable but it is in minutes. Variability ensures worse predictability and more difficult vehicle tracking.
- Registration Authority (RA) – receives requests for pseudonyms allocation from OBUs and sends those requests to PCA. To ensure the privacy the RA mixes the requests from various OBUs to prevent creation of links between the user ID and certificates. RA also creates and manages blacklist of certificates.

- Enrolment Certificate Authority (ECA) – performs the initial enrolment. It connects OBU and SCMS by providing OBU with long-term key. Enrolment can be performed during vehicle production.

In order to ensure the message transmission credibility in C-ITS applications addressing safety there are recommended signature schemes which have simple key distribution among mobile nodes and fast message verification process either on demand or on a periodic basis (including the certificate generation by CAs). Another requirement is short cryptographic header which is in C2C communication added to transmitted messages (important role has the length of generated digital signature attached to the messages from various CAs – see Figure 2). PKI objects shown in Figure 2 are creating following cryptographic outputs.

One of the main delays reason in the C2C communication (C2I) is the cryptographic header and therefore it is very important to select effective digital signature schemes in order to guarantee signatures verification from multiple sources in one vehicle (broadcast message type). The processing time of cryptographic safety header and cryptographic tailer $T_{HT}(M)$, which are attached to the message M (see Figure2), consists of the time needed to generate the signature, time needed to sign the message (including the attachment of timestamp $T_{sign}(M)$, time needed to transfer signed message including addition of certification data from appropriate CA $T_{tx}(Sign_{PrKv}[M])$ and time needed to verify one message T_{verify} (M) (respectively more messages). This processing time is defined as follows:

$$T_{HT}(M) = T_{sign}(M) + T_{tx}(Sign_{PrKv}[M]) + T_{verify}(M) \quad (1)$$

From this point of view are group digital signature schemes an important part of the PKI architecture because it is possible to verify within the C2C respectively C2I communication the signatures of several unique private keys within the particular group of nodes SK_1, SK_2,..., SK_n by just one private key (of the group) PK_G. Digital Signature Algorithm (DSA) signature scheme with modified El Gamal algorithm or ECDSA signature scheme with Elliptic Curve Cryptosystem (ECC) algorithm can be included in the group digital signature schemes. Short key lengths (compared to RSA (Rivest Shamir Adleman) or DSA schemes) and related small computational complexity makes ECDSA cryptographic schemes ideal for the use in devices with limited computational capacity and limited memory, where are included also C-ITS applications.

– **Safety elements of ECDSA scheme**

There exist several recommended standards of ECDSA schemes in the field of automotive industry [11], [12] but there is still an ongoing development in the process of finding new modification of ECDSA in various groups GF(2^m) respectively GF(p). It is a preferred trend in cryptography with better results (in many parameters) than commonly used asymmetric schemes (e.g. RSA).

The main advantage of elliptic cryptosystems is the speed and small hardware and software demand which is very useful in ad-hoc vehicles networks. Development is currently focused on the implementation of ECDSA algorithm and mostly deal with implementation of ECDSA algorithm of chosen EC on the parallel solving of discrete logarithm problem in additive group because the discrete logarithm is the fundamental safety part of ECC algorithms.

Solution of this problem depends on the effective implementation of arithmetic in the group of EC points. For the development and effective implementation of curve arithmetic is needed mainly knowledge from the finite fields theory. There exist more algorithms which solve the Elliptic Curve Discrete Logarithm Problem (ECDLP) problem (with various efficiency).

The most used is the Pollard's rho method [13] with complexity $(\pi . n/2)^{1/2}$ steps. If n=256 bits it makes approximately 2^{128} steps what is approximately the safety level of symmetric block cipher AES-128 (Advanced Encryption Standard) which is currently unsolvable problem. If the discrete logarithm problem (DLP) task is performed in parallel on N processors we get complexity $\frac{(\pi n/2)^{\frac{1}{2}}}{N}$, what is for large r still difficult task. To better understand the DLP problem we describe the process of key generation, message signing and message verification. All this operations are performed in OBU in special co-processor which performs cryptographic operations and key management independently from other tasks. Built-in computers in vehicles have processors with limited processing performance and memory. For example OBU from company Savari [17] uses 500MHz processor, 256MB main memory and 512MB data storage.

Public and private keys of the vehicle are certified by relevant CA. Private keys are stored in HSM (Hardware Security Module) safety module of the vehicle which also provides secure time base for the digital signature timestamps. HSM module manages all cryptographic operations with private keys. In case of threats this module should be erased. HSM is not a part of OBU. It is using the Short Term Identity (STI) in order to ensure the user anonymity. STI is an anonymous key pair derived from ELP (Electronic License Plate) parameters with shorter lifetime. Short-term vehicle identification is carried out by pseudonyms.

To obtain a pseudonym the car C_i generates the set of key pairs $\{SK_{1v}, PK_{1v}\}$,..., $\{SK_{nv}, PK_{nv}\}$ and sends the public keys to corresponding CA through a secure communication channel. Vehicle uses its long-term identification for authentication within the CA. CA then signs all public keys PK_{nv} and generates a set of pseudonyms for

mentioned vehicle. Each pseudonym contains CA identifier, information on the pseudonym lifetime, public key and the CA signature. It does not contain any information about the vehicle identity.
The frequency of pseudonyms change is irregular and depends on the vehicle protection degree, on input parameters (position, speed) and on the system settings. To obtain next pseudonyms are used so-called sets of pseudonyms. These pseudonyms are periodically supplemented by CA. After the node moves from the set of pseudonyms 1 to the set of pseudonyms 2 it can no longer use any pseudonym from the set 1.
The process of message signing (message is generated by vehicle C_i) is be mathematically expressed as:

$$C_i \rightarrow *: M, HT, Sign_{SKVi}[(M, HT)|T], Cert_{PKVi} \quad (2)$$

Where: M represents safety-related message, HT represents the cryptographic header and tailer of the message, SK_{Vi} is the secret (private) key of vehicle C_i, PK_{Vi} is public key of vehicle V_i, T is timestamp, Cert is certificate valid for the vehicle C_i (signed by anonymous public key PK_{Vi}) and * represents number of receivers (in case the message was sent to more vehicles).
Current certificate of V_i vehicle signed in point of time j by anonymous public key of vehicle C_i (PK_i) contains:

$$Cert_{Ci}[PK_j] = PK_j \,|\, Sign_{SK-CA}[PK_{Vj}|ID_{CA}], \quad (3)$$

where: $Sign_{SK-CA}$ represents corresponding CA certificate signature based on its private key $SK - CA$ and ID_{CA} represents unique identification number of particular CA..

– **Implementation of the signature based on EC in C-ITS**

It must be noted that ECDSA scheme of digital signature is just a curvilinear domain of DSA signature scheme therefore their signature generation and signature verification phases are nearly identical.
For C-ITS are recommended the elliptic curves E over the group GF(p), where p is a large prime number [14].
Elliptic curves over these algebraic structure are defined by the set of points$P[x_p, y_p]$, where x_p, y_p are coordinates of GF(p)and by distinguished point O (at infinity). Elliptic curve $E_p(a, b)$ constructed over GF(p) must satisfy the equation:

$$y^2 \equiv x^3 + ax + b \ (mod p), \quad (4)$$

where a, b are coefficients (constants) of elliptic curve $E_p(a, b)$, p is prime number and x, y are coordinates.
Calculation of individual operations of ECDSA algorithm is performed on the set of parameters known as system parameters. These system parameters are: type of elliptic curve $E_p(a, b)$, point on elliptic curve which is order of prime number n for which is valid $n.P = O$.

Note: various point on the curve, which is satisfying the equation (4), have different order (it is so-called infinite loop operation when by multiplying the point is the infinity achieved for the first time in the GF(p). For practical application is currently preferred p = 224 or256 bits [14] where is the order of EC high what is used for DLP problem.
In the next step is in the particular HSM module of the vehicle C_i selected random number d from the interval $(1, n-1)$ and on the elliptic curve $E_p(a, b)$ is calculated new point Q:

$$Q = d.P, \quad (5)$$

where d is private key of the vehicle C_i. Points P and Q can be disclosed.
Then the private and public keys of particular vehicle C_i using the ECDSA scheme with $E_p(a, b)$ are:

$$PK_{Ci} = \{E_{p(a,b)}, n, P, Q\} \quad SK_{Ci} = \{d\}. \quad (6)$$

After key pair PK_{Ci} and SK_{Ci} generation is in the HSM module of the C_i vehicle realized the calculation of digital signature and signed message using generated random number k (since it is a stochastic scheme of digital signature). For each message M is generated new random number. ECDSA digital signature consists of the calculation of two parameters r and s as mathematically expressed in equations (7) and (8).

$$k.P = (x_1, y_1); r = x_1 \bmod n, \quad (7)$$

$$s = k^{-1}(H(M) + d * r) \bmod n. \quad (8)$$

Note: H(M) is the hash code of selected computationally secure hash function (e.g. SHA-256).
In the C_i vehicle (respectively in all vehicles in the range) is performed verification of the signature attached to message M' which was created using the ECDSA scheme. It means there are verified received cryptographic signatures r' and s' attached to the message. This is realized by calculation of auxiliary variables w, u_1, u_2 and v as it is mathematically expressed in equations (9) to (11).

$$w = (s')^{-1} \bmod n \text{ and } H(M'), \quad (9)$$

$$u_1 = (H(M').w) \bmod n; \ u_2 = r'.w \bmod n, \quad (10)$$

$$u_1.P + u_2.Q = (x_0, y_0); v = x_0 \bmod n. \quad (11)$$

If *v=r´* the message verification was performed and the message is considered as credible.

PRACTICAL PART

In the practical part we compared the amount of verified messages received within the period of 1s for different types of elliptic curves in ECDSA cryptographic scheme. Experiment was conducted using the OPEN SSL library

on two different computes. One computer equipped with processor Pentium Dual-Core E5500 2,8GHz, second computer equipped with processor i5-2500 3,3GHz.
Let's assume the worst case scenario (traffic-jam) on a four-lane intersection as shown in Figure 3. Furthermore let's assume that all vehicles shown in Figure 3 are equipped with C-ITS applications and contain communication module for C2C communication with ECDSA digital signature scheme messages authorization. We analysed the amount of verified CAM messages within the defined time period (1s) from the point of view of the vehicle V_i.
The vehicle is receiving all messages in the range. For the 300m range (what is the usual range according to IEEE 802.11p [14]) it represents for the defined scenario reception and verification of messages from up to 800 vehicles. We assume that the CAM messages are generated every 300ms (according to ETSI TS 102 637-2 [15]). It means that the vehicle V_i must verify each second 2400 messages.

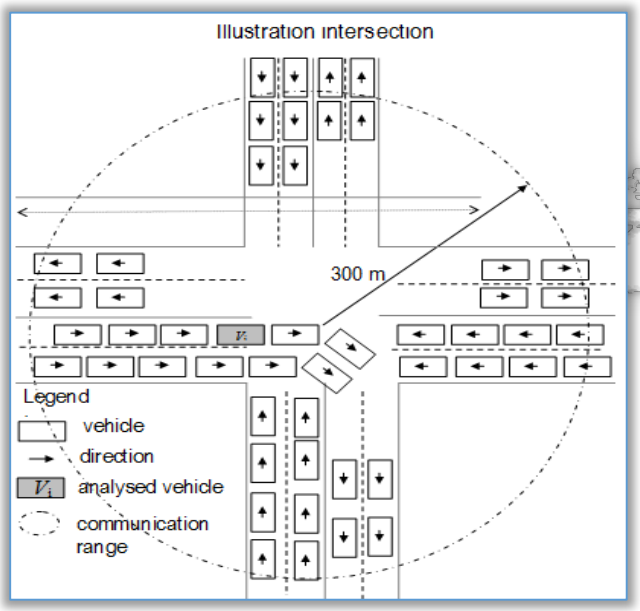

Figure 3. Analyzed scenario of intersection

In order to evaluate the secure transmission effectiveness as well as to evaluate the real possibilities of verification of the amount of safety-critical messages we follow the recommendations in standard IEEE 1609.2 for the elliptic curve type selection for the ECDSA scheme which recommends the use of NID_secp224r1 (where the value 224 bits represents the size of selected prime number in ECDSA scheme). According to realized experiments the message length do not affect the signature verification time. Verifications were performed for messages with lengths 100B, 300B and 1024B and the verification time was identical.
Results of realized experiment with the use of OPEN SSL (Secure Sockets Layer) cryptographic library and processor Pentium Dual-Core E5500 2,8GHz has shown the verification time of 2400 messages for selected elliptic curve 2.66s. It means that the vehicle can verify during one second only 902 messages what represents only 37,5% of all received messages.
Results indicate overloaded communication what could adversely affect the reaction of the driver which is needed in real time (within 100ms). If we use the same scenario with ECDSA scheme and NID_secp160r2 curve (with shorter key) the vehicle V_i would manage to verify 60% or received messages.
With the reduction of the EC key length is the percentage of verified messages increasing (for example for the NID_secp128r2 it would be 83%) but the transmission safety is decreasing. During the selection of appropriate key length of ECDSA scheme is necessary to follow the recommendations for computational safety in the process of solving discrete logarithm as mentioned in the theoretical part of this article (the recommended curve length is greater than 160B).
We also conducted experiment in order to examine the ability of the vehicle V_i to verify messages for a selected period of time and we determined the amount of verified messages during 1s for different types of elliptic curves (Figure 4). Experiment was conducted for the same length of useful message (payload) 300B.

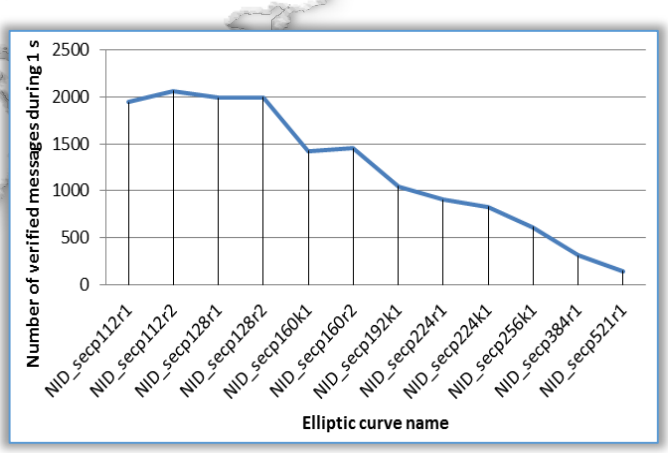

Figure 4. Comparison of the amount of verified messages for different EC curves (processor Pentium Dual-Core E5500 2,8GHz)

The results of experiment realized for the worst case of "crowded intersection" indicate that the network throughput must be addressed by additional measures. One solution could be dynamic implementation of different EC based on monitored load for example by the use the received messages counter in the vehicle. After the critical amount of received messages is reached the safety can be switched to weaker.
In order to maintain suitable level of safety there are needed OBU units with higher performance. We performed the same experiments with the same curves on better computer equipped with processor i5-2500 3,3GHz and the performance increased by 50%. The

amount of verified messages increased from 902 to 1307 (for the curve NID_secp224r1).

Performance of currently manufactured OBUs [16, 17] is not sufficient. The solution could be the use of supercomputer for intelligent vehicles Drive PX2 which was presented by company Nvidia on the CES 2016. Computing performance of this supercomputer is 24 TOPS (300x more powerful than computer used for our experiments). With this computer could be used for the same scenario EC with longer key, e.g. NID_secp521r1.

We realized the C2C communication model (Figure 5) for the same scenario of four-lane intersection in the SW tool OPNET Modeler [19] and investigated additional parameters such as network delay and network throughput for 800 vehicles.

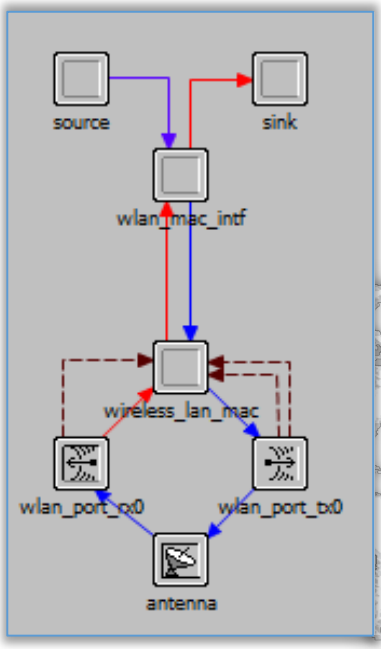

Figure 5. Model of vehicles communication without authentication

The node consists of four processors. The first one is the "source" which simulates the data transferred from higher layers. It is a simple source which generates packets with certain length and frequency and records statistics such as the length of generated packet and generation time which are used at the end of the simulation to calculate the total network delay, throughput and other parameters. Source will generate packets with length of 300 bytes and sends them with frequency 1 to 10 messages per second.

Generated data are sent to next processor "wlan_mac_intf". This serves as interface between higher layers and MAC (Medium Access Control) layer. Its task is to send packets from the source to the "wireless_lan_mac" processor and to send packets received from this processor to "sink" processor which throws away packets from other nodes and makes statistics in order to allow calculation of network properties. It also inserts the addresses (in our case broadcast) in order to simulate the CAM messages exchange.

The "wireless_lan_mac" processor is used to simulate the MAC layer. It produces the frames and sends them to transmitting module "wlan_port_tx0" respectively to compose the message received from "wlan_port_rx0" module. There is implemented access method CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). The node model also contains modules for data transmission respectively data receipt "wlan_port_tx0" and "wlan_port_rx0" which simulate the channel settings for transmission and receipt and contain methods to calculate the number of erroneous bits, the noise impact and so on.

The receiving module also informs the processor "wireless_lan_mac" on the state of the media which is necessary for implementation of the access method. The last module is antenna. In our case we used isotropic antenna. Results of delay and throughput in VANET network are shown in Figure 6.

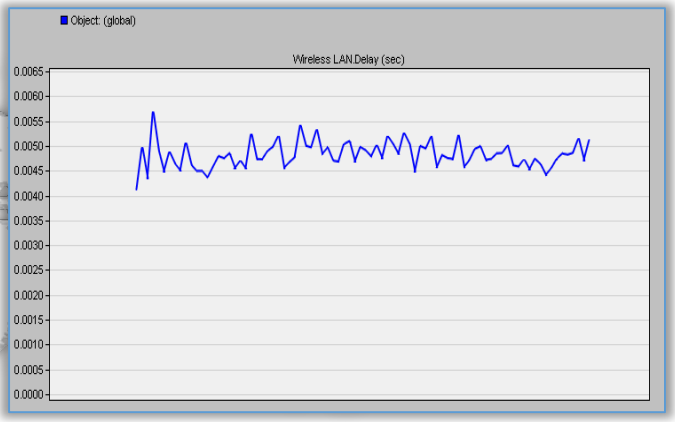

Figure 6. Delay in VANET network (model "four-lane intersection")

The results of the simulation indicate the average transmission delay of 300B long messages on the value of 0,5 ms while the load is 2,5Mbs. This delay does not include the time needed for signing and verification. The total delay of one message transmission when used recommended elliptic curve NID_secp224r1 can be calculated according to the equation (1), where:

$$T_{sign}(M) = 0{,}969 \text{ ms},$$
$$T_{tx}(Sign_{PrKv}[M]) = 0{,}5 \text{ ms},$$
$$T_{verify}(M) = 1{,}109 \text{ ms}$$

Than: $T_{HT}(M) = 2{,}758$ ms

We calculated the average delay of one message from its creation up to the receipt on the value of 2,758ms what is in line with requirement for a maximum delay in safety-critical applications which is 100ms.

We also examined the impact of message length on total message delay (in the same scenario). Results are presented in Figure 7.

In case of RSA signature scheme, which has greater key length, is the average delay of message transmission between nodes increased to 450ms. Such delay would have a great impact on the overall safety.

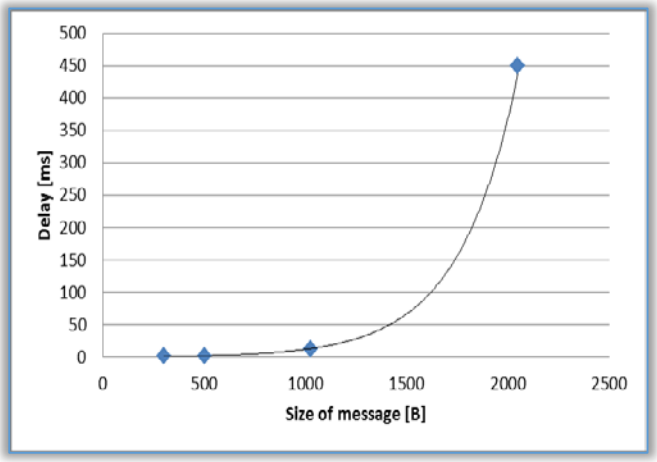

Figure 7. The impact of message size to the delay in transmission

CONCLUSIONS

Authors in the contribution present how type of elliptic curve and length of message influence performance of the network. In detail they are concentred of describing of PKI and ECDSA algorithm.

The accrued situation leads to generation and sending an authorised warning message to the surrounding vehicles signed by a digital signature within vehicular networks. We analysed four lane overloaded intersection, where we found that it is necessary to making demands on OBU performance.

In practical part, the authors analysed how performance of OBU influence number of verified messages and how the length of message influence the performance of network. We compared two different common computer, where was 50% different in performance.

Also with increasing of message length is delay in network increasing from 0,5ms (300B message) to 450ms in (2kb message). Such a delay would have a major impact on the overall safety.

Acknowledgment

This work has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number: 008ŽU-4/2015: Innovation of HW and SW tools and methods of laboratory education focused on safety aspects of ICT within safety critical applications of processes control.

References

[1] E. B. Hamida, H. Noura and W. Znaidi, "Securtiy of cooperative intelligent transport systems: standards, Threats analysis and cryptographic countermeasures", in Electronics 2015 vol 4, pp. 380-423, ISSN: 20799292.

[2] S. Bhoi, P. Khilar, "Vehicular communication: A survey", in. IET Netw. 2014 vol 3, pp. 204–217.

[3] M. A. Lebre, F.L. Mouel, E. Menard, J. Dillschneider and R. Denis, "VANET applications: Hot use cases", in Technical Report hal-01024271; 2014, p. 1–36.

[4] http://www.preciosa-project.org

[5] http://www.evita-project.org

[6] G. Popov, M. Hristova and Hr. Hristov, "Method of increasing reliability of semi-ergatic systems in extreme situations", in: Latest Trends in Applied Informatics and Computing, 3rd International Conference on Applied Informatics and Computing Theory (AICT '12), Barcelona, Spain, (2012), ISBN: 978-1-61804-130-2, pp 225 – 231.

[7] J. Harding, "Vehicle-to-vehicle communications. Rediness of V2V technology for applications", Report No DOT HD 812 014, Washingtnon, DC, National Highway Traffic Administration, 2014, in: http://www.nhtsa.gov.

[8] J. Ďurech, P. Holečko, E. Bubeníková and M. Franeková: "Performance analysis of authentication protocols used within Cooperative - Intelligent Transportation Systems with focus on security", in: International conference TST 2015, Wroclaw, Poľsko. Selected paper in: CCIS (Communications in Computer and Information Science) 531 proceedings. Springer- Verlag, 2015, pp: 231-240, ISBN 978-3-319-24576-8

[9] J. Ďurech, M. Franeková, P. Holečko, "VANET throughput model scenarios for authorized V2V communication",in: IEEE conference INES 2015, 3.- 5. 9. 2015, Bratislava, pp.129-133, ISBN 978-1-4673-7938-0.

[10] S. Vaudenay, "A classical introduction to cryptography", Springer, ISBN 0-387-25880-9.

[11] N. W. Wang, Y. M. Huang and W. M Chen, "A novel secure communication scheme in vehicular adhoc networks" in: Computer Communications, 2008, 31, 2827–2837., cit 11/2015, http://www.sciencedirect.com/science/article/pii/S0140366407005178.

[12] N. Varshney, T. Roy and N. Chaudhary, "Security protocol for VANET by using digital certification to provide security with low bandwidth", in: Proceedings of the 2014 International Conference on Communications and Signal Processing (ICCSP), Melmaruvathur, India, 3–5 April 2014, pp. 768–772, 11/2015, cit.:11/2015, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6949947

[13] V. Klima and T. Rosa, "Kryptologie pro praxi-DSA, ECDSA", in: Chip 8/2002, p. 135-136.

[14] FIPS 186-3. The Elliptic Curve Digital Signature Algorithm, nIST publication, 2010.
[15] IEEE 802.11p
[16] ETSI TS 102 637-2
[17] Savari networks: "MobiWAVE – on board unit", in: http://www.savarinetworks.com/files/MobiWAVE
[18] Unex "OBU-201U", in: http://unex.com.tw/product/obu-201u
[19] Opnet Modeler 17.5 Documentation, 2013.

ISSN:2067-3809