[1.]Alžbeta KANÁLIKOVÁ, [2.]Mária FRANEKOVÁ, [3.]Emília BUBENÍKOVÁ

TRENDS IN THE AREA OF SECURITY WITHIN C2C COMMUNICATIONS

[1-3.]University of Žilina, Faculty of Electrical Engineering, Department of Control and Information Systems, Žilina, SLOVAKIA

Abstract: The article deals with current and recent research in the VANET networks. The focus is on the secure car to car communication. The article lists possible cryptographic attacks. A possible security solution against attacks in the VANET network is the design of protocols and cryptographic architecture based on ETSI (European Telecommunications Standards Institute), C-ITS (Cooperative-Intelligent Transportation Systems), and NHTSA (National Highway Traffic Safety Administration). In order to guarantee integrity and authentication message in the transmission, is the most suitable security architecture based on PKI (Public Key Infrastructure). Integrity and authentication of the message transmission between C2C (Car-to-Car) vehicles are appropriate to be secured through ab digital signature algorithms. Appropriate digital signature schemes are schemes based on the RSA algorithm or elliptic curves. Elliptical curve schemes of digital signature are less demanding for the size of the key and the size of the encrypted message. Practically, car-to-car encrypted communication has been implemented through a digital signature based on elliptic curves. The simulation tool was the OPNET MODELER with the OpenSSL library. The simulations identified network throughput and network latency in the highway scenario.
Keywords: C-ITS systems, C2C, VANET Network, security attacks, PKI architecture, integrity and authenticity of message, digital signature, authorization messages, cryptographic library, OPNET MODELER

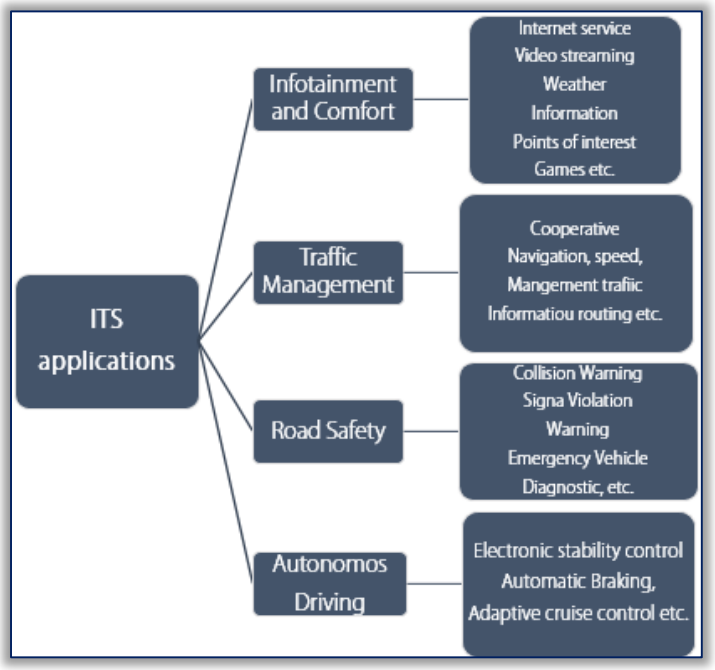
1. INTRODUCTION

The development of Cooperative-Intelligent Transportation Systems (C-ITS) represents an important aspect of the deployment of these systems into real-world. The reason for the implementation of C-ITS communication is to increase the road safety by increasing situation awareness of drivers. The vehicles communicate between each other and between static units located along the infrastructure by transmitting critical and non-critical messages. These messages can contain data like vehicle position, vehicle velocity, information on exceptional events and so on [1], [2].

The development of C-ITS communication architectures is heading towards the utilization of mobile ad-hoc networks. The reason is a simpler infrastructure in comparison to access-point based networks. The VANET networks (*Vehicular Ad-hoc Networks*) represent a specific mobile ad-hoc networks subgroup providing communication between vehicles (*Car-to-Car, C2C*) or between vehicles and infrastructure (*Car-to-Infrastructure, C2I*).

C-ITS applications that are used to communicate Car-to-Car or Car-to-Infrastructure in VANET network are divided [1] to:

- Infotainment and comfort application – These applications are focused on delivering value-added services to the driver, increasing his driving experience. These services are provided by trusted providers. Typical examples are remote diagnostics and vehicle maintenance. Convenient applications include, for example, providing video, audio stream, or games.
- Traffic management applications – these applications are based on a global data exchange from global traffic map databases that contain travel information - road overload, route speed, recommended routes, and more.
- Road safety applications – road traffic applications use wireless communication between entities (vehicles, road infrastructure) to reduce traffic accidents and protect drivers from the various dangers that are on the road.
- Autonomous driving - new technologies for autonomous vehicle control, which make several technical facilities conditional, cameras, sensors, navigation receivers systems on the vehicle and the like.



Picture 1. C-ITS communication applications [1]

In the field of safety are on the centerpiece is mainly applications on road safety. These applications monitor road traffic. For some applications, it is also necessary to guarantee system parameters for example reliability, delay, reach, packet frequency, and so on. Road safety apps include

applications that provide information, for example, warnings against standing or slow vehicles, dangers on the road, accident information, road trip alerts, and more. The main focus of our research is on secure communication in C-ITS. Within safe communication, several research projects were solved, for example between older research projects addressed to 2010-2011 [10]:

- COMeSafety – focused mainly on the development of standards for C-ITS deployment and active safety (implemented by 2010).
- SAFESPOT – the project focusing on the development of a safety assistant to improve road safety (implemented by 2010).
- SEVECOM - the project focused on the full definition, design and implementation of security requirements (implemented by 2010).
- C&D – A Dutch project which designed an adaptive cruise control using the IEEE 802.11p standard for C2C and C2I communications.
- EVITA-The project aimed at creating and implementing a hardware security module (HSM) for onboard network security of the car.
- Group of standard IEEE 802.11p – The group that has developed a standard for WLANs, specifically for wireless access in vehicular environments (standard built in 2010).

The later C-ITS security projects and groups include, for example:

- SAFERTEC - project seeks to in-depth explore the involved vulnerabilities of connected vehicles, apply innovative techniques for attack modelling, experimentally validate the quantification of security assurance levels and also contribute to relevant standards. [3]
- SCOOP - pilot project for the deployment of cooperative intelligent transport systems. SCOOP aims at deploying alert services such as road works warning, information about current interventions of road maintenance agents and on-board signaling of hazardous and dangerous events. The exchange of information between the vehicles and the infrastructure is based on ITS G5 [4].
- CODECS – the project aimed at unifying and coordinating scientific approaches to C-ITS implementation, security topics are its content [5].
- Amsterdam Group – the strategic alliance of committed key stakeholders with the objective to facilitate the joint deployment of cooperative ITS in Europe [6].
- HIGHTS - project addresses these problems by combining traditional satellite systems with an innovative use of on-board sensing and infrastructure-based wireless communication technologies (e.g., Wi-Fi, ITS-G5, UWB tracking, ZigBee, Bluetooth, LTE etc.). This platform will increase the safety level of vulnerable road users (motorcycles, scooters, pedestrians) through bi-directional danger detection. [7]
- ROADART – this project deals with communication, detection, localization and others techniques between truck to truck [8].

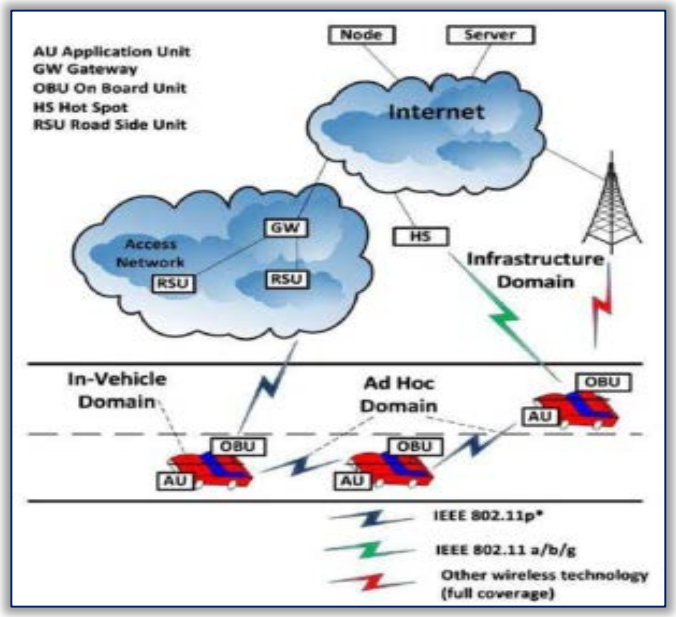
2. VANET NETWORK AND ATTACKS TO VANET NETWORK

C – ITS communication is performed via open channel in ad hoc network – VANET (Vehicular ad hoc Network).

— VANET network

VANET network is very dynamic with little access to the network infrastructure and offering multiple services. The system architecture of VANET network consists of 3 basic domains [9]:

1. In-Vehicle domain – this domain consists of ECU (*Engine Control Units, ECU*), of the OBU (*On-Board Units, OBU*), unit TPM (*Trusted Platform Module*), and one or multiple AUs (*Application Unit, AU*) and unit GNSS (*Global Navigation Satellite System, GNSS*). ECUs collect data about the vehicle's dynamics (location, speed, direction, vehicle dimensions, etc.) and control the vehicle's functionality. The AU is responsible for running one or multiple applications, which are offered by remote service providers (*Service Providers, SPs*), and communicates with other nearby C- ITS entities. Each connected vehicle is also equipped with a TPM to enable secure and efficient



Picture 2. VANET infrastructure and communication [11]

communications and to manage the different keys and certificates.

2. Ad hoc domain - consists of vehicle OBUs and road-side units (*Road-Side Units, RSUs*) deployed along the roads. In this domain, the information collected at the vehicles is the exchange in real time between OBUs with nearby C-ITS entities (C2C communication), communication between OBU and RSU.
3. Infrastructure domain - Infrastructure includes RSU and Wireless Hotspot Points (HS) that allow vehicles to access applications. While is the RSU drive is connected to the Internet via an infrastructure manager or other authority, the access point may be private and less secure. Unless there is a direct connection to the RSU or access point, the OBU can also communicate via the Global System for Mobile Communications, the Universal Mobile Telecommunications System (UMTS) and the 4G (4 Generation) if integrated into the OBU.

Car to Car communication in the VANET network and the individual domains of its system infrastructure are shown at Picture 2.

— VANET security attacks

The communication in C-ITS performed via an open channel which properties enable a wide scale of transmission attacks. The main threats and attacks on communications security are focused on several basic security services:

- Availability
- Identity and authenticity
- Confidentiality
- Integrity of data and credibility
- Nonrepudiation

To the listed services exist following attacks [11]:

≡ Attacks on availability: in such attacks, the attacker shuts down the entire network and the node has no access to the information. For example:

- Denial of service (*DOS*) or distributed denial of service (*DDOS*) - it hijacks the network totally, slows down the entire process and interrupts the services of the network. The intruders send many fake or bogus requests, reply to the network, and impersonate themselves as a normal vehicle OBU or RSU, and the network seems busy or out of reach, not responding to the genuine vehicles). Identity revealing: disclosing details of the individual vehicle can put security at danger. Later character revealing must be avoided.
- Jamming - the attacker senses the physical channel and gets the information about the frequency at which the receiver receives the signal. Then he transmits the signal on the channel so that channel is jam.
- Other attacks for example attack using malware, black hole attack, attack by overflow network etc.

≡ Attacks on authentication: identification of vehicles is mandatory to rectify the genuine sender and receiver, confirm identity first to kick out intruders, and reduce the chance of information loss. For example attacks:

- Sybil attack - it is an attack when one node is issued simultaneously for several nodes with a valid identity. Such behaviour may lead to network congestion and lead to the generation of false messages about the number of nodes present in the network, which can cause unnecessary and unjustified vehicle manoeuvers.
- GPS spoofing attack - GPS spoofing attack attempts to deceive a GPS receiver by broadcasting incorrect GPS signals, structured to resemble a set of normal GPS signals, or by rebroadcasting genuine signals.
- Tunneling attack - GPS satellite simulator generates signals that are stronger than those generated by the actual satellite system are, an attacker can produce false readings in the GPS to deceive vehicles to think that they are in a different location.
- Key or certificate replication attack - An attacker duplicates a key pair and/or certificates to create ambiguities, which can prevent authorities from identifying a vehicle in disputed situations.

≡ Attacks on confidentiality: the information should be confidential between the authorized users and kept hidden or encrypted from the intruders to avoid traffic analysis or snooping attacks. For example attack on confidentiality:

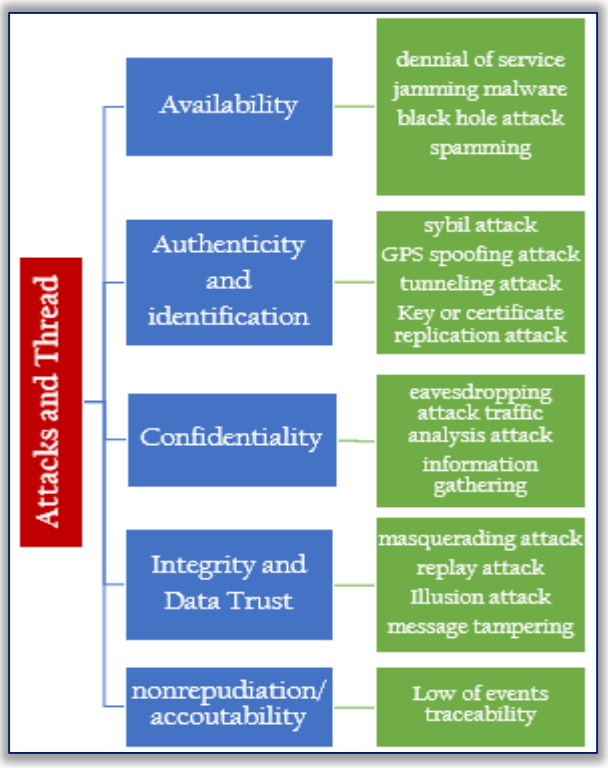
- Eavesdropping attack - Listening to the media is an attack easy to carry out and through this attack can be collected such as location data that can be used for tracking vehicles.
- Traffic analysis attack - The attacker analyzes collected information after a phase of listening to the network, it tries to extract the maximum of useful information for its own purposes.

≡ Attacks on integrity: the intruder should change the data by deletion, insertion, and modification of data according to his requirements and benefits. Data integrity keeps away repudiation and replaying attacks. Attacks on integrity:

- Masquerading attacks - In this attack, the attacker is hidden using a valid identity (called a mask), and tries to form a black hole or produce false messages. For example, to slow down the speed of a vehicle or require it a lane changes. A malicious node attempts to act as an emergency vehicle.

- Replay attack - attack it consists in replaying (broadcast) a message already sent to take the benefit of the message at the moment of its submission. This attack can be used e.g. to replay beacons frames, so the attacker can manipulate the location and the nodes routing tables.
- Message tempering - this attack is against integrity it consists in modifying, deleting, constructing or altering existing data. The attacker falsifies received data indicating that the route is congested, and changes them to deceive users.
- Illusion attack – attack it consists in placing voluntarily sensors which generate false data. These data can move normally in the network and require driver interaction to make decisions.

≡ Attacks on nonrepudiation: The ability to confirm that the sender and receiver of the message are authentic users and at the end, they cannot refuse to acknowledge. In VANET it should be always possible to verify all hardware and software changes in security settings and applications (update, modification, addition, etc.). In VANET is attack loss of events traceability. This non repudiation attack consists of taking action, allowing subsequently an attacker to deny having made one or more actions.



Picture 3. Attacks in VANET network [11]

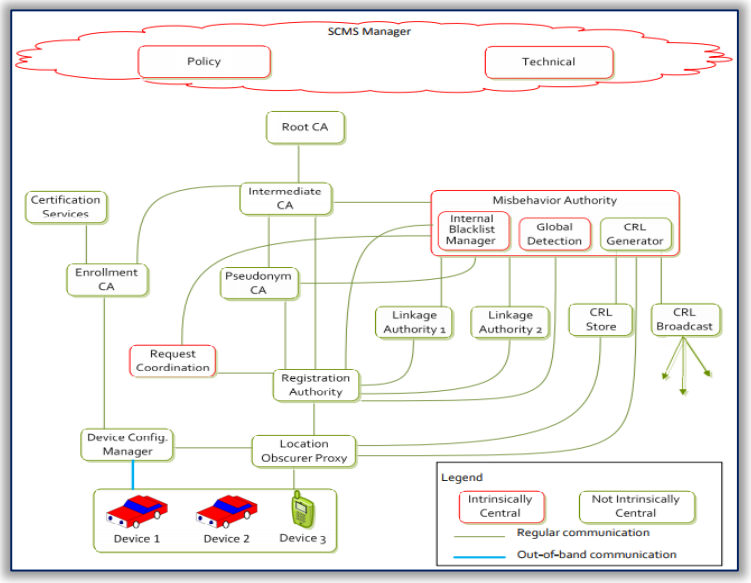
3. SECURITY PROTECTIONS ON THE BASE OF CRYPTOGRAPHY

For the VANET network, many groups have investigated the security architectures and infrastructures. These groups generated either security standard protocols or have defined security architecture of VANET network. For example, ETSI and NHTSA (*National Highway Traffic Safety Administration*) propose security services [12]:

- Authentication - NHTSA authenticates via digital signature and encryption. ETSI via signed messages.
- Confidentiality - NHTSA and ETSI via symmetric and asymmetric encryption.
- Integrity - NHTSA assures the integrity via Message Authentication Code. ETSI check the value of the signed message.
- Liability identification - NHTSA via Misbehavior Authority. ETSI via accountability and remote management.
- Message security - NHTSA and ETSI use PKI. NHTSA uses ECDSA.
- Non-repudiation ETSI and NHTSA have EDR (*Event Data Recorder*) for tracing.
- Privacy NHTSA uses an anonymizer proxy and privacy-preserving revocation via MA (*Misbehavior Authority*).

Many groups in Europe and USA build their own security architectures based on PKI. In Europe ETSI its security architecture for C-ITS and USA build security architecture within Vehicle Safety Consortium.

NHTSA proposed security architecture [13] based on PKI. Entities of the NHTSA architecture and PKI scheme are shown in picture 4. The communication consists of two types of messages: BSM (Basic Safety Message) and security information message. For the communications between vehicles is used for confidentiality asymmetric encryption digital signature ECDSA (*Elliptic Curve Digital Signature Algorithm*). For the Communications inside (entity to entity) is used the symmetric encryption AES-CCM (*Advanced Encryption Standard-Counter with CBC-MAC*) is used for confidentiality with MAC (*Message Authentication Code*) for integrity and together they provide authenticity.



Picture 4. PKI scheme and security architecture of NHTSA [13]

The IEEE 1609.2 security standard [16,19] presents methods to secure message formats, application messages, and messages processing used by WAVE (Wireless Access in Vehicular Environments) devices.standard

From the standards, the IEEE 1609.2 security standard [14] presents methods to secure message formats, application messages, and messages processing used by WAVE (*Wireless Access in Vehicular Environments*) devices. All these security issues are based on PKI using keys and certificates management.

— Security based on integrity and authentication

Appropriately combined cryptographic algorithms and schemas are provided by the following services: confidentiality, integrity, authentication, identification, indisputable, access control. Of these services of the VANET network is a service of integrity and authentication is very important.

In the VANET network are used digital signature cryptographic techniques for integrity and authentication of messages between mobile nodes. Authentication techniques of digital signature schemes are based on the PKI scheme and certification authority (*Certification Authority, CA*) (Picture 4). Each CA is responsible for its assigned region in the road infrastructure and manages the identification of all moving nodes (vehicles). In road infrastructure, the certification authority is called the GTA (*Government Transportation Authority*). Each GTA is responsible for its assigned region in the road infrastructure and manages the identification of all moving nodes (vehicles). Each intelligent vehicle is equipped with OBU and is identified by an electronic identifier with unique parameters.

Vehicle identification can be divided into [10]:

- LTI (*Long Term Identity*) - This is an electronic identification, also known as the ELP (*Electronic License Plate*), issued by the manufacturer of the vehicle manufacturer to each vehicle.
- STI (*Short Term Identity*) - an anonymous key pair that derives from ELP parameters. It has a shorter duration and serves to ensure the anonymity of the vehicle user.

Current vehicle certificate C1 signed at anonymous time point public vehicle key C1 (*PKi*) contains:

$$CertC1[PKi] = PKi \,|\, SignSK{-}CA[PKCi \,|\, IDCA] \quad (1)$$

SignSK-CA represents the signature of the certificate by the appropriate CA at based on its private key SK-CA,
IDCA represents the unambiguous identification number of the relevant certification authority.

For digital signatures in C-ITS, it is important that the values of the following parameters are as small as possible with respect to the duration generation and verification of signature:

- digital signature size,
- size of the public key,
- digital signature generation time,
- digital signature verification time.

Currently, are used various digital signature schemes in the commercial sphere. The most used ones are:

- deterministic schemes based on the RSA algorithm,
- stochastic schemes based on DSA and ECDSA.

— Digital signature RSA scheme

RSA digital signature is deterministic scheme but it is slow in the signature generation and signing operation.

Mathematical description this scheme is [15]:

1. Initialization, create key for encrypt and decrypt:
   N = p.q , where *p, q* the big prime number (50 – 100)
   ϕ(N) = (p-1).(q-1) , Euler function
   e: 1<s< ϕ(N) *e* – encryption exponent, condition indivisible whit Euler ϕ*(N)* function
   d: 1<t< ϕ(N) *d*– decryption exponent, inverse element of e - e.d = 1 mod ϕ(N)
   K_E {e,N} Public key
   K_D {d,N} Secret key
2. Create Digital signature:
   $\sigma = H(M)^d \mathrm{mod} N$ /create digital signature with hash function of message M.
   $\sigma^e \mathrm{mod}\ N = H(M)$ /verification digital signature - is correct if the result is a hash of original message.

The algorithm of digital signature on base RSA creates slowly a digital signature with respect to the long private key, which also increases the size of the digital description. VANET network applications are systems with limited performance and memory, and it is important that the signature scheme used is more efficient and produces short signatures. Therefore, the RSA digital signature scheme for fast authorization of messages in VANET networks is not the most appropriate and more convenient is the ECDSA elliptical curve scheme.

— Digital signature ECDSA scheme

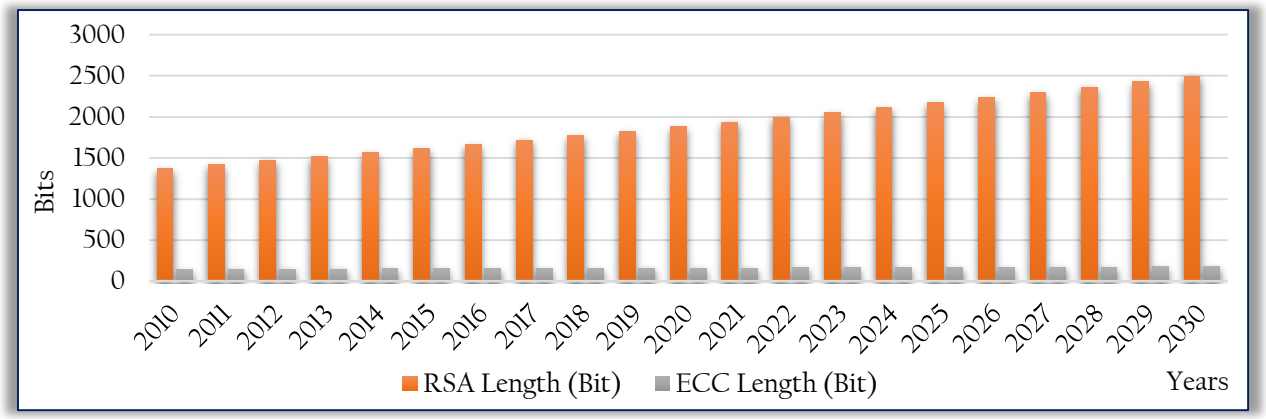
The ECDSA Digital Signature Scheme is a stochastic scheme. It is based on a discrete logarithm based on elliptic curves. The ECDSA signature scheme is composed of several processes [16]:

a) Generation and validation of domain parameters.
b) Generation and validation of a key-pair.
c) Generation of a signature.
d) Verification of a signature.

- Let us have points P, Q on an elliptic curve, for which we need to determine an integer d, while 0 ≤ d ≤ n-1, where n is the order of point P and for the point Q holds Q = d*p.
- In order to sign the message M performs the ECDSA signature generation (steps 1 to 7):
  1. Choose a random or pseudorandom integer k so that $1 \leq k \leq q-1$.
  2. Calculate: $k.G = (x_1, y_1)$, convert x_1 to integer $\overline{x_1}$.
  3. Calculate: $r = x_1 \bmod n$, if $r = 0$, go to step 1
  4. Calculate: $k^{-1} \bmod n$,
  5. Calculate: $h = H(M)$, convert this bit string to integer e.
  6. Calculate: $s = k^{-1}\{e + dr\} \bmod n$, if $s = 0$, go to step 1.
  7. Signature of vehicle C_1 for message M is (r, s).
- To verify the signature (r, s):
  1. It verifies that r and s are integers from the interval $[1, n-1]$.
  2. Calculate: $h = H(M)$, converts this bit string into an integer e.
  3. Calculates : $w = s^{-1} \bmod n$, $u_1 = ew \bmod n$, $u_2 = rw \bmod n$, $X = u_1 G + u_2 Q$
  4. If $X = O$, then it refuses the signature. Otherwise, it converts the x coordinate x_1 from X to an integer $\overline{x_1}$ and calculate $v = \overline{x_1} \bmod n$.
  5. Accept the signature if and only $v = r$.

— Comparison of ECC over RSA scheme

The RSA schema is slowly in creating a digital signature and fast in verifying digital signature. The reason is a long key. [11] In VANET networks, we need communication to be fast. Both academic and private organizations provide recommendations and mathematical formulas to approximate the minimum key size requirement for security [20]. Through the method of Arjen K. Lenstra [18] and results in portal https://www.keylength.com [20] we have recalculated the minimum length of key for RSA and ECC algorithms. The chart on Picture 5 presents the comparison, what key minimum lengths (bits) of each algorithm will provide a level of security measured in the years. Based on this comparison the ECDSA digital signature scheme with ECC algorithm is more effective with respect to the length of the key which has an impact on creation and verification time of digital signature.



Picture 5. Perspective minimum lenght bit key. Comparison RSA and ECC [17,20]

Based on this comparison and analysis of standards for safety of communications for inter-communications in C-ITS IEEE1609.2 and ETSI TS 103097, we decided to use a ECDSA scheme for creating and verifying digital signature in the practical part of our research.

4. PRACTICAL RESULTS OF SIMULATION

In our research, we focused on simulation security communications between two vehicles. Model of the cryptographic system was created in the OPNET Modeler tool. The model situation was a highway that consisted of 2 lanes in each direction of travel 1 km in length, with the number of vehicles 30 for low and 100 for high traffic density. The speed was simulated, in the case of low density, in right lanes at 80 km.h^{-1} and 130 km.h^{-1} in the left lane in the direction of travel. In the case of high traffic density, a velocity of 10 km.h^{-1} was defined in all lanes for simulate traffic congestion on the highway. Vehicle nodal models were configured to unsecured message size of 100 and 400 B. Global attributes were modified for secure communication so that the original unsecured message was as large that message in secure communication. At the application of cryptographic algorithms was used available open source library OPENSSL at version 1.02a. On the

recommendations in IEEE 1609 and ETSI TS 103097, was implemented the ECDSA signature scheme with parameters P-224 and P-256 for the digital signature. For simulation of security and authentication of the message was used processor Intel Core TM i5-2500 CPU, RAM 16GB, frequency 3.30GHz. In the simulated model, we focused on the comparison of delay and throughput without added cryptomodule for generating, signing and verifying the message and adding the module [19].

For both traffic scenarios: Highway with the low and high density of vehicles, we focused on determining network throughput and delay.

The throughput of the VANET network of T depends on the number communicating nodes - n, the size of the transmitted message M and the number of transmitted messages per second with a vehicle - R (Rate) (formula 2).

$$T = n.R.M.8/1024.1024[Mb/s] \quad (2)$$

The delay represents the difference in end times and the beginning of the cryptographic operation. In our case, the delay is caused by generating a signature at the sending node, verifying the signature contained in the pseudonym, and verifying the signature of the received message.

The simulation results are shown in Table 1.

Table 1. Results of average value end time delay and throughput

Scenario	Highway with the low density of vehicles delay [μs]	Highway with the low density of vehicles delay [μs]	Highway with the high density of vehicles delay [μs]	Highway with the high density of vehicles throughput [bit/s]
Unsecured communication 100 B message	199,940	38155	205,203	141719
Unsecured communication 400 B message	611,214	146797	647,923	567290
Secured communication ECDSA P256 100 B message	3038,701	120614	3094,693	435207
Secured communication ECDSA P256 400 B message	3379,285	237704	3559,599	858407
Secured communication ECDSA P224 100 B message	2594,472	114425	2715,530	417705
Secured communication ECDSA P224 400 B message	3075,245	234548	3141,580	842071

Results of the simulation of the scenarios show that total delay are caused by cryptographic operations and with the delay of transmission, which caused an increase in the size of a message. Results of measured network throughput in the selected scenarios indicate that addition of security also has increased overall network throughput. The simulation results could help to set and optimize VANET parameters, namely delays and network throughput when implementing secure message.

The proposed model should be improved by the following suggestions, for example:

- Implement algorithm to reduce the message header.
- Find a tool to better implement the IEEE 802.11p protocol.
- Implement appropriately the OPENSSL library and its other algorithms.

5. CONCLUSION

The VANET network has a many challenges and one of the important challenges is security. The article contains an overview of completed and ongoing projects in the VANET network, mainly in the field of security. The article also provides an overview of VANET network attacks, overview of security architectures, standards and overview particularly in the field of vehicle-to-vehicle communications, and special about authentication of received and sent messages. Currently, the most common mechanism used for cryptographic authentication is the digital signature that allows users to authenticate the origin of the received messages. The search for effective digital signature schemes that guarantee the V2V messages is still a priority research task for automotive companies. And practically we have worked on verifying the elliptical curve of a digital signature scheme that seems most effective. We have focused on optimal selection of signing scheme parameters in two scenarios - highway and crossroad. In most cases, it needs to make a compromise between the message generating and the speed of their verification and the selected key size. In the future work is very important to focus on a survey of the authentication and confidentiality of VANET messages and to verify some other models of message alert and authorization.

Acknowledgement

The paper has been written with the support of the project KEGA 016ŽU-4/2018 Modernization of teaching methods of management of industrial processes based on the concept of Industry 4. 0.

References

[1] E.B. Hamida, H. Noura, W. Znaidi, "Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures", 2015, ISSN: 20799292, [cit. 09/2018] Online: http://www.mdpi.com/2079-9292/4/3/380
[2] Janota et all. "Applied Telematic", EDIS University of Žilina, 2015, ISBN 978-80-554-1037.
[3] SAFERTEC - Security Assurance Framework for Network Vehicular Technology, European project of Horizon 2020 [cit. 10/2018] Online: www.safertec-project.eu

[4] SCOOP - The pilot project for the deployment of cooperative intelligent transport system [cit.10/2018] Online: http://www.scoop.developpement-durable.gouv.fr/en/project-r2.htmt
[5] CODES - Cooperative ITS Deployment Coordination Support, European project of Horizon 2020 [cit. 10/2018] Online: https://www.codecs-project.eu
[6] Amsterdam Group, the umbrella organisation for organisations who have the means to jointly develop and deploy cooperative ITS in Europe, [cit. 10/2018] Online: https://amsterdamgroup.mett.nl/default.aspx
[7] HIGH PRECISION POSITIONING FOR COOPERATIVE-ITS, European project of Horizon 2020, [cit. 10/2018] Online: http://hights.eu
[8] Roadart Project, Research On Alternative Diversity Aspects for Trucks, European project Horizon 2020, [cit. 10/2018] Online: http://www.roadart.eu
[9] M. Franeková, A. Kanáliková, E. Bubeníková, Modeling of inter-vehicular communications intention to authorization of messages, Sami 2018, IEEE 16th World Symposium on Applied Machine Intelligence and Informatics Dedicated to the Memory of Pioneer of Robotics, February 7-10, 2018, Košice, Herlany, Slovakia, ISBN 978-1-5386-4771-4
[10] J. Ďurech: Security solutions of VANET network for control of intelligent transport systems, Dissertation Thesis 2016, University of Žilina.
[11] M. Kaur, S. Mandeep, K. SaggiRanjeet, K. SandhuRanjeet, K. Sandhu, A Survey of Vehicular Ad Hoc network on Attacks & Security Threats in VANETs, Conference: International conference on Research and Innovations in Engineering and Technology (ICRIET 2014) on 19-20 December 2014, [cit. 10/2018] Online: https://www.researchgate.net/publication/295595335_A_Survey_of_Vehicular_Ad_Hoc_network_on_Attacks_Security_Threats_in_VANETs
[12] F. Sakiz, S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV, Ad Hoc Networks 61 (2017) 33–50 Contents lists available at ScienceDirect Ad Hoc cit. [10/2018] Online: https://www.sciencedirect.com/science/article/pii/S1570870517300562
[13] W. Whyte, A. Weimerskirch, V. Kumar, T. Hehn, A Security Credential Management System for V2V Communications, [cit. 10/2018] Online: https://www.researchgate.net/profile/William_Whyte/publication/271554151_A_security_credential_management_system_for_V2V_communications/links/566aeefe08ae1a797e396777.pdf
[14] H. Hasrouny, C. Bassil, A. Ellatif Samhat, A. Laouiti, Group-based authentication in V2V communications, [cit. 10/2018] Online: https://ieeexplore.ieee.org/document/7113193/
[15] M. Franeková, K. Rástočný, Cryptography in safety-relevant systems, EDIS Žilina, 203p., ISBN 978-80-554-1310-5, University of Žiina 2017.
[16] M. Franeková, P. Holečko, E. Bubeníková, A. Kanáliková, Transport scenarios analysis within C2C communications focusing on security aspects, IEEE 15th International Symposium on Applied Machine Intelligence and Informatics, January 26–28, 2017 Herlany, ISBN: 978-1-5090-5654-5
[17] Kerry Maletsky, RSA vs. ECC Comparison for Embedded Systems, [cit. 10/2018] Online:http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-8951-CryptoAuth-RSA-ECC-Comparison-Embedded-Systems-WhitePaper.pdf
[18] Arjen K.Lenstra: Selecting Cryptographic Key Sizes [online] [cit. 11/2018], https://infoscience.epfl.ch/record/164526/files/NPDF-22.pdf
[19] J. Fedor, Modeling the safety characteristic of communication of Cooperative Intelligent Transport systems in the OPNET Modeler Tools, Diploma Thesis, University of Žilina, 2016.
[20] Portal of key length cryptographic algorithm [online] [cit. 11/2018], https://www.keylength.com

ISSN 1584 - 2665 (printed version); ISSN 2601 - 2332 (online); ISSN-L 1584 - 2665