ACTA TEHNICA CORVINIENSIS – Bulletin of Engineering
Tome VIII [2015] Fascicule 1 [January – March]
ISSN: 2067 – 3809

[1.] Ján ĎURECH, [2.] Marián HRUBOŠ, [3.] Mária FRANEKOVÁ, [4.] Aleš JANOTA

IMPLEMENTATION OF DATA FROM THE MOBILE MEASUREMENT PLATFORM TO VANET APPLICATION

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

Abstract: *The paper deals with an idea of informing the car drivers on problem of road degradation via sending of warning messages from road side units. The initial part of the paper summarized the up–to–now realized concept of the mobile measurement platform (MMS) and its mathematical principles showing how detailed data on road surface may be obtained. The main part of the paper is aimed at design of integration of data from MMS into the VANET application. Practical realisation is based on the warning message generation with GPS coordinates which is assuring by digital signature ECDSA cryptography algorithm via OpenSSL tool.*

Keywords: *point cloud; 3D model; data fusion; VANET; C2C; C2I, vehicular communications; cryptography; OpenSSL*

INTRODUCTION

In the field of road transport currently many countries are facing the problem of degradation especially of older roads. Constantly raising intensity of road traffic has negative effect on quality of road communications. Various sorts of defects of road surfaces such as cracks, potholes, longitudinal and transverse bumps, ripples of surface, local falls or beaten tracks have negative effects on driving comfort and cause greater wear of some parts of motor cars.

For measurement of deformations which can occur on the road surface several measurement methods and devices have been created. Generally, manual methods for measurement of surface attributes are being replaced with methods based on electronic measuring devices. One big group of measuring devices used for measurement of road deformations is based on utilization of the laser measurement systems. They measure flight of time of laser impulses to find out what is a distance between the laser scanner and road surface.

For detection of road texture there have been many methods developed so far, resulting in a number of various coefficients and attributes proposed to define surface roughness in an optimal way.

In the Slovak Republic devices of VIDEOCAR and Profilograph GE are currently being used for measurement of surface roughness. The Progilografh GE (see Figure 1) measures the texture and gives data on an average depth of texture. At the same time it is also used as a volumetric method for determining of an average texture depth. VIDEOCAR is a device which is used for fast visual inspection of the road surface. Data are collected using the VW Caravelle vehicle type. Basic task of fast visual survey is to collect data about state of road surface and determine defects attributes for the following purposes:

- ✓ *Data collection and filling databases of the Road databank for consecutive rating of individual sections of selected roads further utilized in the Road management system.*
- ✓ *Search engine, which serves for processing of detailed visual inspection if needed.*
- ✓ *Solutions of the research projects and projects of scientific–technological development.*

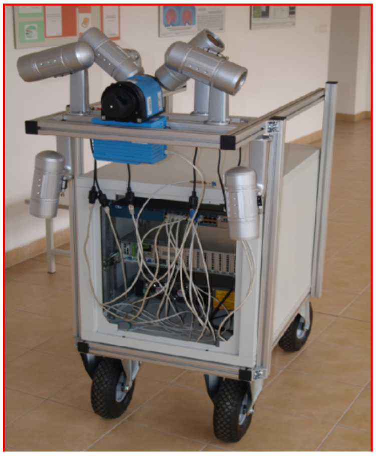


***Figure 1**. Mobile measurement platform (MMP)*

Basic conditions required for data collection are good optical conditions and dry unpolluted surface of the road. However, these methods do not provide all necessary information about the measured road and its surrounding area.

In the context of ITS (Intelligent Transport Systems) development integration of other offered services into one complex service package seems to be one of actual tasks. Some of those services may require communication connections based on C2C and/or C2I communication using wireless communication standards, through VANET (Vehicular Ad Hoc Networks) [1], which additionally requires authentication of services provided.

For measuring of attributes of road surface and surrounding areas the authors proposed the solution shown in Figure2 consisting of the MMP (Mobile Measuring Platform), It should be capable of storing scanned data about potholes positions into server connected to the

RSU (Road Side Unit) and thought VANET networks transmitting warning messages to all vehicles finding themselves in a communication range. To ensure authenticity and integrity of such messages a cryptography method is used to generate digital signature on the base of elliptic curve mechanism.

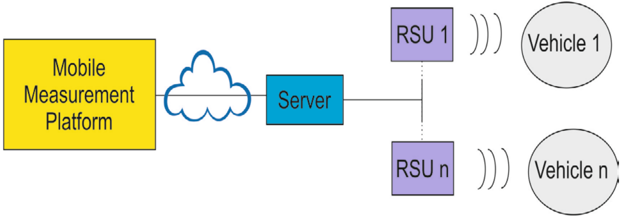


***Figure 2**. Interconnection of MMP with VANET application*

MATHEMATICAL PRINCIPLE USED IN THE MOBILE MEASUREMENT PLATFORM

The MMP is primary dedicated for measuring of geometric changes of road surface. The secondary assignment of this platform is measuring surrounding areas around the road itself.

The conception of the MMP is based on gathering of data characterizing a measured road and its surrounding areas and on its fast processing and graphical interpretation appropriate for next analysis. Processing of data obtained from the laser scanner is principally performed by off–line methods. It means that all measured data are first saved to the hard disk and after surveying the whole intended road section the computing algorithm is being initiated to calculate and get coordinates of all measured points [2].

The MMP illustrated in Fig1 can be used in generally for creation of the 3D model of real objects within road infrastructure such as roads, buildings, bridges or tunnels. By fusion of data coming from multiple sensors integrated in the MMP we are able to generate the 3D model of the real environment with its texture. Thus we are able to merge for example data from the laser scanner and a GPS receiver and generate the 3D model consisting of cloud of points.

Subsequently the algorithm for creation of surfaces in the points cloud may be applied to obtained data as a precondition of the following step – application of texture itself. Textures data are obtained from a set of cameras integrated in the MMP and monitoring the whole space around.

To calculate cloud of points the equations (1) may be used, designed on the base of analysis of data gathered from the following data sources: laser scanner, GPS receiver and INS (Inertial Navigation System) [3].

Thanks to data from the laser scanner we can obtain the following quantities [4]:

- ✓ *Starting angle α_{0n},*
- ✓ *Sequence number of a current point i,*
- ✓ *Angle increment $\Delta\alpha_n$,*
- ✓ *Measured distance between an object and the laser scanner d_{in}.*

After re–calculations of GPS receiver data we get position of the MMP in the form of coordinates x_{0n}, y_{0n} and z_{0n}.

The INS helps us to get data on rotation of the MMP in each axis α_{rn}, β_{rn} and γ_{rn}.

$$x'_{in} = d_{in} * \sin\left[\frac{(\alpha_{0n} + i * \Delta\alpha_n + \alpha_{rn} + 90) * \pi}{180}\right] * \cos\left[\frac{\beta_{rn} * \pi}{180}\right] + x_{0n}$$

$$y'_{in} = d_{in} * \cos\left[\frac{(\alpha_{0n} + i * \Delta\alpha_n + \alpha_{rn} + 90) * \pi}{180}\right] + y_{0n}$$

$$z'_{in} = d_{in} * \sin\left[\frac{(\alpha_{0n} + i * \Delta\alpha_n + \alpha_{rn} + 90) * \pi}{180}\right] * \sin\left[\frac{\beta_{rn} * \pi}{180}\right]$$

$$r'_{in} = \sqrt{y'^{2}_{in} + z'^{2}_{in}}$$

$$\gamma'_{in} = \arccos\left[\frac{y'_{in} * 180}{r'_{in} * \pi}\right]$$

$$x_{in} = x'_{in} \tag{1}$$

$$y_{in} = r'_{in} * \cos\left[\frac{(\gamma_{rn} + \gamma'_{in}) * \pi}{180}\right]$$

$$z_{in} = r'_{in} * \sin\left[\frac{(\gamma_{rn} + \gamma'_{in}) * \pi}{180}\right] + z_{0n}$$

The problem of calculations and needed data conversions is discussed in more details in [5]. Trajectory of the MMP can be also calculated by tracking the center line as the main road surface marking. Such an idea can also be found implemented in e.g. the LDWS (Lane Departure Warning System) where different methods of image processing based on computer vision are used to detect the line– for more details see e.g. [6].

For searching of defects on the road surface one must know the height of the laser scanner head situated at the MMP. In our case the laser scanner is located in the height of 108 cm above the road surface. Defects are searched in a programmable way by systematic searching of points whose distances from the laser scanner are greater than 108 cm. The algorithm provides an output in the form of output file which contains data on GPS position of identified defect, its length and depth. The 3D model may be used to create a visualized model of road surface that can make the process of subsequent road maintenance easier.

DESIGN OF INTEGRATION OF DATA FROM THE MMP INTO THE VANET APPLICATION

The authors have extended the concept of the MMP and the idea of recording defects in road surface in this paper for application of the warning system RHCN (Road Hazard Control Notification), In case of detection of potentially dangerous situations (pothole, ice, ...) this system can send through the VANET all nearby vehicle warning message, informing drivers about dangerous situation or dangerous spot on road communication / infrastructure. The principal scheme of this idea is shown in Figure3.

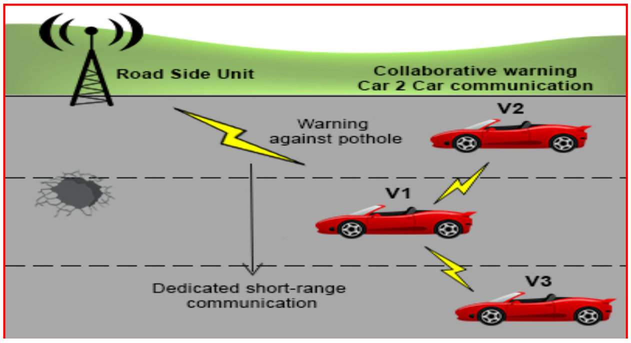
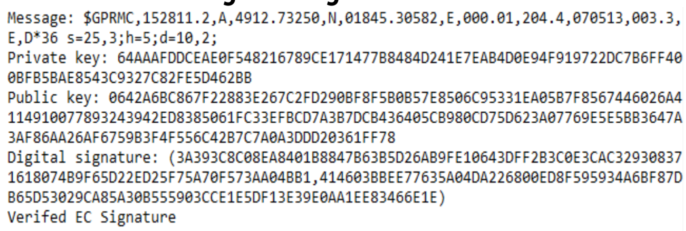


***Figure 3**. Warning system in VANET network*



```
Message: $GPRMC,152811.2,A,4912.73250,N,01845.30582,E,000.01,204.4,070513,003.3,
E,D*36 s=25,3;h=5;d=10,2;
Private key: 64AAAFDDCEAE0F548216789CE171477B8484D241E7EAB4D0E94F919722DC7B6FF40
0BFB5BAE8543C9327C82FE5D462BB
Public key: 0642A6BC867F22883E267C2FD290BF8F5B0B57E8506C95331EA05B7F8567446026A4
1149100778932439342ED8385061FC33EFBCD7A3B7DCB436405CB980CD75D623A07769E5E5BB3647A
3AF86AA26AF6759B3F4F556C42B7C7A0A3DDD20361FF78
Digital signature: (3A393C8C08EA8401B8847B63B5D26AB9FE10643DFF2B3C0E3CAC32930837
1618074B9F65D22ED25F75A70F573AA04BB1,414603BBEE77635A04DA226800ED8F595934A6BF87D
B65D53029CA85A30B555903CCE1E5DF13E39E0AA1EE83466E1E)
Verifed EC Signature
```

Figure 4. Example of signed message
with using ECDSA algorithm realised via OpenSSL

As explained in the previous chapter, the MMP after computing all sensed data evaluates which data represent defects in road surface and record data about their positions to the server connected to the roadside unit RSU. The RSU through short range communication DSRC (Dedicated Short Range Communication) sends warning message to vehicles available in range of the relevant RSU. The proposed concept can be used also for warning drivers about blind spots and other dangerous situations. This is a modified method of C2C communication, respectively C2I where in the case of the proposed application the road infrastructure (relevant RSU) communicates with vehicles.

Considerations of wireless communication bring higher possibility for abuse and potential existence of attacks to the communication system. If a vehicle (respectively RSU unit) doesn't have security features implemented in the control unit, other vehicles may not consider and mark received warning messages as secured, it means there is no warranty about authentication of sent messages. Security solutions of C2C and C2I communication are actually solved by the C2C–CC organization [7]. The use of IPv6 (Internet Protocol v6) protocol is being advocated actually there. IPv6 according to the set configuration solves the following security requirements for the communication in the VANET:

- ✓ Authentication of message and its integrity – protection of message prior to its modification, the ability to identify the sender.
- ✓ Non–repudiation of messages – the sender cannot deny that he sent the message.
- ✓ The timeliness of reports – the recipient can be sure that the message is fresh and was generated within the specified interval.
- ✓ Access control – a decision which nodes in the network can perform their assigned actions.
- ✓ Confidentiality of message – preservation of content messages secret from unauthorized parties.

In the practical part of the paper, the authors deal only with issues of authentication of message and its integrity.

Currently in modern cryptography cryptographic authentication protocols are based on scheme of digital signature mostly based on asymmetric cryptography. In commercial applications there are currently expanded several types of digital signature schemes:

- ✓ RSA (Rivest, Shamir, Adleman) digital signature scheme,
- ✓ DSA (Digital Signature Algorithm),
- ✓ ECDSA (Elliptic Curve Digital Signature Algorithm).

The most important parameters of digital signatures in the transport system are: the size of the signature, public key size, generation time of signature and time of signature verification.

Matter of choosing an efficient digital signature schemes for authentication purposes in VANET networks is devoted to a number of projects. Project SeVeCom [8] supports the use of a modified version of a digital signature scheme based on ECDSA.

PRACTICAL REALISATION

The authors have chosen the ECDSA digital signature scheme to ensure the credibility of message transmission from MMP which is also supported by the results of testing three schemes of digital signatures: RSA–1024, DSA–1024 and ESDSA–160 from the perspective of time sessions for generating and verifying signatures (see Table 1) which was implemented in the OpenSSL tool.

All three schemes were applied to the message of the same length on one type of PC with Intel Dual Core processor with frequency of 2.3 GHz.

Given the large number of tests performed in several projects with different results always the best and the worst case of available data is given in the table. Additional crucial parameter for choosing an algorithm is the size of the key.

As shown in Table 1 in the case ECDSA scheme compared with other schemes the process of signature generating and certificating is very fast, which predetermines the algorithm used in applications with a focus on performance, which can also include sensor networks.

Table 1. Time demands of algorithms RSA, DSA, ECDSA

	Generating of signature	Verification of signature	Size of signature [Byte]	Size of public key [Byte]
RSA – 1024	15 – 154.5	1	128	128
DSA – 1024	8.7 – 80	9.9 – 97.72	40	128
ECDSA 160	0.9 – 6.94	1.382 – 14.01	40	20

Before sending safety–relevant messages (in our application – "RHCN") a digital signature (Figure5) is generated in the RSU using its private key SK_1 which is function of message M and message header H. The header may contain, for example, information about location of roughness on the road.

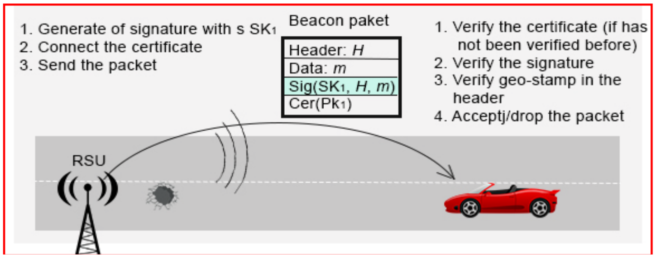

1. Generate of signature with s SK1
2. Connect the certificate
3. Send the packet
Beacon paket
Header: H
Data: m
Sig(SK1, H, m)
Cer(Pk1)
1. Verify the certificate (if has not been verified before)
2. Verify the signature
3. Verify geo-stamp in the header
4. Acceptj/drop the packet
RSU

Figure 5. Authorized transfer of messages between RSU
and vehicle via VANET network

Thus created cryptographic number is attached to the message simultaneously with a certificate Cert, which is tied to the i–th anonymous public key of the sender VK^{i}_{1}, which certifies the corresponding CA (Certification Authority). On the side of the vehicle V the received certificate is validated first (if it was not done before) and the received digital signature is verified using the i–th public key *of the vehicle VK^{i}_{V1}, that is downloaded by the vehicle V (resp. other vehicles) in regular intervals. At the same time information of geostamp type (about position of place where emergency condition happened) is verified from the header H and after completing these procedures the safety–related message is either accepted or rejected.*

The process of generating a digital signature in RSU can be mathematically expressed:

$$RSU \longrightarrow \; : M, H, Sign_{SK^i}[(M,H)|T], Cert_{RSU}. \qquad (2)$$

where: M represents sent safety–relevant message,

H represents the message header,

SK^i is a short–term private key RSU in the i–th moment,

VK^i is a short–term public key RSU, in the i–th moment,

T is the time stamp,

Cert is a short–term certificate of the RSU (for the anonymous public key pre VK^{i}_{1}), represents the number of receivers (in the case, that message was sent to multiple vehicles in mode „broadcast“).

Current certificate of the RSU valid in the i–th point of time for the anonymous public key RSU V_1 (VK^{i}_{1}) includes:

$$Cert^{i}{}_{V1}\left[VK^{i}{}_{1}\right] = VK^{i} \,|\, Sign_{SK-CA}\left[VK^{i} \,|\, ID_{CA}\right]. \qquad (3)$$

where: $Sign_{SK-CA}$ represents signature of certificate signed by relevant certification authority based on its private key SK–CA, ID_{CA}represents the unique identification number of the certification authority.

When the MMP finds a pothole on the road, respectively other roughness, it generates a message that consists of GPS coordinates and by using the selected cryptographic algorithm (in our case ECDC scheme) sign and send the message to the nearest RSU unit. The experiment has been realized using MMP in the University of Žilina Campus. We walked through the campus with MMP and after recording the potholes, message containing its GPS coordinates has been generated. Subsequently the message was signed. The process of signing the message has been simulated using the OpenSSL in which elliptic curve over a 384 bit prime field has been chosen. We have chosen prime field curve because of more effective implementation in the software implementation. Digital signature is shown in Figure4. Next step would be adding signature and send message with public key to the vehicle. Subsequently vehicle can verify message using public key, and if the vehicle verify the message, warning can be shown.

CONCLUSION

The aim of this paper was to describe integration of the RHCN system into the C2I communication. An initial part of the paper shows the concept of data fusion that helps us reach a 3D model covered with surfaces where surface textures may be applied. One of the tasks potentially covered by the presented concept of the MMP is detection of road surface deformations. Data on these findings may be further used to calculate and send warning messages to passing vehicles, signed by digital signature within the VANETs. Described methods and algorithms of data fusion have been implemented in MATLAB programming environment. Example of the digital signature scheme ECDSA has been realized with the help of the OpenSLL library.

Furthermore, the realized software applications of detecting potholes can be amendment to detection of transverse and longitudinal tracks.

Choosing a digital signature scheme with focus on elliptic curve algorithm ECDSA has been chosen on the basis of comparison of the effectiveness signing scheme e.g. referred to [9] due to the described applications where except security performance of the used digital signature scheme is also an important parameter.

Acknowledgment

The paper has been written with the partial support of the project ITMS–26220220089 "New methods of measurement of physical dynamic parameters and interactions of motor vehicles, traffic flow and road" [50%] and partial support of the Educational grant agency KEGA within the project Nr: 024ŽU–4/2012 "Modernization of educational technologies and methods with focus on cryptography for safety relevant applications" [50%].

References

[1.] Hartenstein, H., Laberteaux, K., P.: VANET: Applications and Inter–Networking Technologies. WILEY. ISBN 978–0–470–74056–9

[2.] Halgaš, J., Hruboš, M., Pirník, R., Janota, A.: Determination of Formulas for Processing of Measured Points Representing Road Surface Deformations. Archives of Transport System Telematics, vol. 5, No. 1, 2012, ISSN 1899–8208, pp. 7–10.

[3.] Hruboš, M.: A Tool to Detect Status of Road Degradation over Time.In: Slovak. MSc. thesis, No. 28260220122010, University of Zilina, 2012

[4.] https://www.mysick.com/saqqara/im0031422.pdf

[5.] Šimák, V., Nemec, D., Hrbček, J.: Calculation of robot position utilizing accelerometers in non–inertial frame of reference. In: Proc. of the 9th International Conference ELEKTRO 2012, May 21 – 22, 2012, IEEE Catalog Number: CFP1248S–ART, ISBN 978–1–4673–1179–3

[6.] Bubeníková, E., Muzikářová, Ľ., Halgaš, J.: Application of Image Processing in Intelligent Transport Systems, In: 11 th IFAC/IEEE International conference on programmable Devices and Embedded Systems, Brno, May 23th–25th 2012, ISBN: 978–3–902823–21–2, ISSN 14746670

[7.] Car2Car Communication Consortium. In: http://www.car–2–car.org/M.

[8.] SeVeCom: Security Vehicle Communication. In: http://www.sevecom.org/

ACTA Technica CORVINIENSIS
BULLETIN OF ENGINEERING
ISSN:2067-3809