

IMPACT OF RELIABILITY FACTORS ON THE PROBABILISTIC MODEL PROPERTIES OF IFF RECOGNITION IN A NETWORK-ORIENTED ENVIRONMENT

Radoslav MASNICA, Jozef ŠTULRAJTER

Abstract: In the information age soldiers need to control combat operations, other than weapons, they need information and analytical tools for effective command in combat operations. This article focuses on the description of the properties of a probabilistic model for processing of sensor signals using a probabilistic model of recognition Custom/Foreign (Identification Friendly or Foe - IFF) and access to the current intelligence picture of the commander in the common operational picture (COP) for C4I2 systems. This view defines a comprehensive approach to processing of signals from the sensors using a probabilistic model of recognition Custom/Foreign (Identification Friendly or Foe - IFF) and access to current intelligence picture of the commander and the ability to use full access to information, use of common communication and information environment within systems to support command and control in the environment NEC to describe the relative information superiority.

Keywords: Network Enabled Capabilities (NEC), Command, Control, Communications, Computing, Intelligence and Information Systems - C4I2, sensors, information superiority, IFF, reliability factors.

HIERARCHICAL MODEL OF DECISION ACCEPTANCE IN INTELLIGENT MANET CONTROL SYSTEM

Oleg Y. SOVA, Valery A. ROMANYUK, Anton V. ROMANYUK,
Oleksandr I. LYSENKO, Inga V. URYADNIKOVA

Abstract: The new approaches of OSI level functioning in the self-organizing wireless networks MANET are proposed. They consist in the implementation of new methods and radio network management functions, coordination and intellectualization of the methods, corresponding to different OSI-model levels, and also coordination of the network resource management purposes distribution.

Keywords: Mobile radio network, intelligent control system, intelligent agent, multiagent system.

CRYPTOGRAPHY AND GENETIC ALGORITHMS

Martin JAVUREK, Marcel HARAKAL

Abstract: The genetic algorithm is used in cryptography, mainly for deciphering cipher, but may be also used as the random number. This article is a brief overview of genetic algorithms. The genetic algorithms are used as generators of random numbers. They are also used in cryptanalysis and for training and designing of artificial neural networks. The summary describes the advantages and disadvantages of genetic algorithms.

Keywords: Genetic algorithm (GA), Tree parity machine (TPM), Artificial Neural Network (ANN), cryptography.

SEARCHING FOR CRYPTOGRAPHICALLY SECURE ELLIPTIC CURVES OVER PRIME FIELDS

Rafal GLIWA, Janusz SZMIDT, Robert WICIK

Abstract: Elliptic curves over finite fields are applied to construct public key cryptosystems and to realize a digital signature. The security of these systems is based on computational intractability of the discrete logarithm problem in the group of points on an elliptic curve over a finite field. Elliptic curve cryptosystems provide security comparable to that of the RSA cryptosystem but with cryptographic keys of smaller size. This note presents conditions which cryptographically secure elliptic curves over prime fields have to satisfy and methods to generate such curves following the standard [3].

Keywords: Public key cryptography, elliptic curves over prime fields, security conditions, generation of elliptic curves, probabilistic analysis.

SECURITY IN MILITARY CLOUD COMPUTING APPLICATIONS

Miroslav ĎULÍK, Miroslav ĎULÍK Junior

Abstract: Cloud computing presents a significant technology trend not only in public sector but also in military sphere. It has become a smart solution for providing a flexible computing environment for military applications. This paper describes types of cloud computing models and cloud service model SPI (Software, Platform and Infrastructure). Consequently we describe the private cloud security model based on the private cloud reference model. This paper shows the security technologies and mechanisms for implementing security in private cloud applications, where the high levels of security is necessary and proper.

Keywords: Military Cloud, Private Cloud, Private Cloud Security Model, Security Technologies.

EFFECTS OF WELL - KNOWN FORMS OF IMPROVISED EXPLOSIVE DEVICES USING HOME – MADE ANFO EXPLOSIVES

Lucia FIGULI, Zuzana ZVAKOVÁ, Vladimír KAVICKÝ, Štefan JANGL, Miroslava VANDLÍČKOVÁ

Abstract: The paper is focused on the research of effects of improvised explosive devices (in the form of suicide belt, vest, car etc.) using home-made ANFO (Ammonium Nitrate and Fuel Oil) explosives as a body of the IED. ANFO explosive is chosen due to its spread using in the terroristic attacks. Field test of ANFO explosives are described in the paper. The effect of such IED is compared with the IEDs made from the TNT explosives.

Keywords: Blast wave, ANFO explosives, improvised explosive devices, stand-off distances.

EVALUATION OF THE UNIFORM LINEAR MICROPHONE ARRAY FOR DETECTION SYSTEMS

Roman BEREŠÍK, Jozef PUTTERA, Jozef JURČO

Abstract: Array signal processing methods have been applied in many applications like radars, acoustic and seismic sensor systems. Beamforming, or spatial filtering, is a one of the essential array signal processing methods used for discrimination among different signals coming from different directions and increasing of the signal to noise ratio. The use of microphone arrays as a part of a multisensor system have restrictions in terms of a microphone array dimension, type of microphones, number of channels used for signal processing and also requirements for array signal processing algorithms. The paper deals with simulations of the uniform linear microphone array as a basic configuration of the sensor array for detection of events in monitored area. In conclusion, outcomes of simulations are evaluated and also further research in the field of sensor arrays and array signal processing is outlined.

Keywords: Uniform linear array, array response, acoustic sensor system.

THE IMPORTANCE OF REPLICATION IN THE APPLICATION LOGIC

Lubomír SEMANČÍK

Abstract: This paper describes possibilities of using replications for updating database applications. This approach is based on the fact that each database application can be divided into three main parts: presentation functions, application functions and data management. Application functions represent logic of the application (data processing in the database application) and they can be implemented by means of DataBase Management Systems (DBMS), i.e. stored procedures, triggers, user defined functions and rules. Next the paper characterizes the replications and describes their categorization and properties. Considering that the replications in distributed DBMS allow to send to the remote node not only tables with data, but also selected stored procedures, triggers, user defined functions and rules, the update of the entire database application can be executed using replications. In the conclusion the paper compares the update of a database application using SQL scripts and replications.

Keywords: Database application, distribution of data, database, replications, stored procedures.

MONITORING OF DEPARTMENT NETWORK – ADMINISTRATOR VIEW

Július BARÁTH

Abstract: IT infrastructure primary consists of end devices, communication links and networking devices and all of them are prone to misconfiguration errors and vulnerable to attacks. To prevent poor performance, instability of the systems used and to fight with attackers – effective monitoring is a part of everyday admin’s duties. The paper answers basic questions: how to collect, normalize and process log and audit information; what is essential information to log across the platforms used; and how to monitor network attached devices in the department network. Collected and filtered data is then indexed with Splunk where data analysis and visualization is performed using queries or preconfigured dashboards. Only when full understanding of problem is achieved, proper reaction to fix the problem can be taken. A simple example is provided to better illustrate the process of finding and fixing a misconfiguration problem.

Keywords: Splunk, monitoring, audit, network infrastructure.

VEHICLES ELECTROMAGNETIC EMISSIVITY ANALYSIS

Stanislava GAŽOVOVÁ, František NEBUS, Vladimír BELÁK

Abstract: Recent vehicles are equipped with a great number of communications – information systems, sensors, actuators and electronic devices with maximally suppressed electromagnetic emissivity. The nature of emitted signals is rather ultra-wide band noise and some stationary stochastic signals. The article deals with analysis of personal vehicles electromagnetic emissivity, which is one of the possible characteristics useful for vehicles classification and recognition. The signals analysis, based upon emissivity measurement in anechoic chamber, is investigated in the frequency range from 100 kHz to 35 MHz, concluded with some specific classification characteristics.

Keywords: Vehicle, electromagnetic emissivity, classification, recognition, digital signal processing.

IMPACT OF RELIABILITY FACTORS ON THE PROBABILISTIC MODEL PROPERTIES OF IFF RECOGNITION IN A NETWORK-ORIENTED ENVIRONMENT

Radoslav MASNICA, Jozef ŠTULRAJTER

Abstract: In the information age soldiers need to control combat operations, other than weapons, they need information and analytical tools for effective command in combat operations. This article focuses on the description of the properties of a probabilistic model for processing of sensor signals using a probabilistic model of recognition Custom/Foreign (Identification Friendly or Foe - IFF) and access to the current intelligence picture of the commander in the common operational picture (COP) for C4I2 systems. This view defines a comprehensive approach to processing of signals from the sensors using a probabilistic model of recognition Custom/Foreign (Identification Friendly or Foe - IFF) and access to current intelligence picture of the commander and the ability to use full access to information, use of common communication and information environment within systems to support command and control in the environment NEC to describe the relative information superiority.

Keywords: Network Enabled Capabilities (NEC), Command, Control, Communications, Computing, Intelligence and Information Systems - C4I2, sensors, information superiority, IFF, reliability factors.

1 INTRODUCTION

In the transformation of the army in the Information Age army needs to conduct combat operations in addition to weapons, information, and analytical tools to streamline the chain of command in combat operations. This concerns in particular the knowledge systems of combat situations and sensors and instruments to analyse the information. This article aims to describe properties of a probabilistic model for processing the sensor signal and this article follows the description probabilistic model referred to in the article "Signal processing with using a probabilistic model for recognition identification friendly or foe - IFF" [2].

The article describes the impact factor of reliability in the probabilistic model and its relationship to, and their impact on results in the fight in the NEC network-oriented environment. This model can be used also in other procedures for the description of relative information superiority. The network-oriented environment and environment to achieve information superiority is necessary to achieve the highest level of efficiency of deployment of sensors and sources in proportion to the quality and completeness of the information.

2 PROBABILISTIC MODEL FOR THE PROCESSING OF SIGNALS FROM SENSORS

In the model, to simplify the description, assume that the only element information is information from our own sensors. The sensors acquire the position information of the opponent's goals and identify application IFF.

Suppose that a common operational picture COP consists only of placing targets (or critical subset of them, such as the location of his vehicles). Suppose that the commander has messages from the sensors. The sensors acquire the position information of the

opponent's goals and their identification application (IFF).

Suppose we have a random variable $V \in \{0, 1, 2, 3, 4, \dots, n\}$, which represents the number of units detected by a sensor in the area of interest of a commander. Then, $P(V = v)$ is the probability that the sensor detects and recognizes v units in the enemy units standing against his own troops.

However, this number is conditioned by the total number of units deployed in the area of interest of the enemy commander, which describes the conditional probability $P(V = v | U = u)$.

For using simple sensor in one observation, in a single cycle tracking of targets, which is able to detect and identify targets in area of interest with probability q , without false detection is:

$$P(V = v | U = u) f(x) = \begin{cases} \binom{u}{v} q^v (1 - q)^{u-v} & \text{for } v \leq u \\ 0 & \text{other} \end{cases} \quad (1)$$

When using multiple sensors in the network-oriented environment, we can then determine the probability of detection and identification of the target within the given cycle. Suppose that our sensors are able to make k measurements in the area of interest in the decision cycle of the commander.

This means that sensors can perform k measurements of the area of interest before the enemy commander move their unit. In each of these measurements, v_{di} enemy units are detected, where $i = 1, 2, 3, \dots, k$. Furthermore, we presume that the probability estimates are gradual and that the cycle time is small enough to create the report.

Using Bayes' formula we obtain:

$$P(U = u|V = v_{di}) = \frac{P(U = u|V = v_{d(i-1)}) \binom{u}{v_{di}} (1 - q)^u}{\sum_{j=v_{di}}^n P(U = j|V = v_{d(i-1)}) \binom{j}{v_{di}} (1 - q)^j} \quad (2)$$

Where is $i=1,2,\dots,k$, and for $v_{d0} = 0$ applies $P(U = u|V = v_{d0}) = P(U=u)=1/n+1$.

The result is that a subsequent detection and identification, which exhibit fewer units than the previous one, are completely ignored. Probability $P(U = u|V = v_{di})$ determines the probability of objective findings.

To evaluate the use of pieces of information for the commander, we need to determine the degree of uncertainty, therefore, to determine the likelihood that the commander has true picture of the number and identification of units arranged against him in his area of interest in the COP.

Information entropy $H(i)$ is the amount of uncertainty in probability distributions. Description of the use of entropy is shown in [3].

The residual knowledge of the following applies:

$$K(U, V = v_d) = \frac{\ln(n+1) - H(U|V = v_d)}{\ln(n+1)} \cdot \frac{\ln[\sum_{i=v_d}^n P(U = i|V = v_d - 1)]}{\ln[P(U = n|V = v_d - 1)]} \quad (3)$$

Now a similar formulation can be used also for the knowledge of the operation:

$$K(U_1 | V = v_{d1}, U_2 | V = v_{d2}, \dots, U_m | V = v_{dm}) = \frac{\sum_{t=1}^m [\ln(n_t+1) - H(U_t | V=v_{dt})]}{\sum_{t=1}^m \ln(n_t+1)} \cdot \frac{\sum_{t=1}^m \ln[\sum_{i=1}^{n_t} P(U_t = i | V=v_{dt}-1)]}{\sum_{t=1}^m \ln[P(U_t = n_t | V=v_{dt}-1)]} \quad (4)$$

3 IMPACT OF RELIABILITY FACTORS ON PROBABILISTIC MODEL OF SIGNAL PROCESSING FROM SENSORS

The initial probability distribution of U depends on the information available to the commander from his sensors and sources. When first started, the information available from the reconnaissance is processed.

After receiving the identification and reporting of the sensors, the probability distribution changes. However, in reality, the location of some of the objectives will not be known with certainty at the time of the decision of the commander.

Probability distribution $P(U = u)$ can be influenced by several factors:

1. Number of confirmed and unconfirmed reports from sensors;
2. Reliability of sensors and sources;
3. Terrain conditions;
4. Multiple confirmation;
5. Time lag of information gathered.

The next section will focus more on describing the impact factor of the reliability of sensors and sources for the probability distribution detection of objectives in the interest area of the commander.

In some cases, evaluation of the reliability is subjective, especially in evaluating the results of the visual observation.

In the case of technical sensors, their reliability varies with environmental conditions; unreliable messages are therefore ignored, which affects the probability distribution, and reduces the probability of recognition and detection and identification of target IFF.

On the reliability factor, we can look from different angles. The reliability factor is the reliability of the sensors, reliable information processing, but the reliability factor is also representing the quality of the information processing chain information network reliability. In the network where sensors are separated from the location information processing associated impact on the overall quality of the connection reliability of the sensor as a whole. We can generalize this approach to different perspectives and levels of the NEC.

To describe the factor, we can use analogy of the approach used in applied probability models, namely the use of Bayes phrases and properties of probability. Let $P(U)$ be the probability of detection of targets which are located within the range of sensors and let $P(P)$ be a factor of reliability of the sensor in the range $<0, 1>$. On the reliability factor of the sensor, we can watch as the probability of transmitting information from the sensor (connection quality). Then for the overall probability of detection targets with a confidence factor $P(S)$ holds:

$$P(S) = P(P \cap U) = P(A_1) \cdot P(A_2|A_1) = P(A_2) \cdot P(A_1|A_2) \quad (5)$$

only applies to $P(U) \neq 0$ or $P(P) \neq 0$.

This approach can be generalized to any number of intrusion penetration probabilities. In general:

$$P\left(\bigcap_{i=1}^n A_i\right) = P(A_1) \cdot P(A_2|A_1) \cdot P(A_3|A_2 \cap A_1) \dots \dots P(A_n \bigcap_{i=1}^{n-1} A_i) \quad (6)$$

where $i = 1, 2, \dots, n$, and $P(A_i)$ is probability of detection, the transmission of information and so on.

Using the Bayes Theorem for application brings relationship for the i -th observation, the overall probability of detection of targets with a confidence factor is:

$$P(S)_i = \frac{P(P) \cdot P(U = u | V = v_{d(i-1)}) \binom{u}{v_{di}} (1 - q)^u}{\sum_{j=v_{di}}^n P(P) \cdot P(U = j | V = v_{d(i-1)}) \binom{j}{v_{di}} (1 - q)^j} \quad (7)$$

To illustrate this formula, let's look at simple Example 1, for $n = 3$ units. Suppose that the observations were three different sensors, in three subsequent cycles through a sensor to pursuing the probability of detection: $q = 0,9$. The value of probability of detection sensor q has been selected as indicated by the producer probability of detection radars for ground exploration example. PSNR-5 (1RL133), Credit 1E (1M), EL / M-2140NG, SQUIRE, ARSS, MSTAR (AN / PPS-5C), ARS-2000 for effective reflecting surface target 1 square meter in optimum conditions of electromagnetic wave propagation.

Similarly, you can use probability of detection q , for different kinds of sensors or detection targets. The sensors are able to detect any target with probability q and probability of transmission of information from the sensor is $P(P)$. Parameters $P(P)$ and q are optional for each sensor used depending on the properties and applications. Table 1 presents the results of probability finding targets $P(U|V)$ for the individual measurements in each cycle of measurement. Table 1 shows probability of detection targets used $q = 0,9$ for the individual sensors, and probability of the transmission of information from the sensor $P(P) = 0,9$ and $P(P) = 0,5$ and for comparison without the probability the transfer of information from the sensor $P(P) = 1$.

Tab. 1 Total degree of uncertainty for Example 1

v	P(U=0 V)	P(U=1 V)	P(U=2 V)	P(U=3 V)	PP=1		PP=0,9		PP=0,6	
					H(U V)	K(U V)	H(U V)	K(U V)	H(U V)	K(U V)
-	0,25	0,25	0,25	0,25	1,3862	0	1,343	0,031	1,0397	0
0	0,9	0,09	0,009	0,0009	0,3602	0	0,184	0,86	0,5267	0
1	0	0,99	0,0198	0,0003	0,0899	0,3071	0,1767	0,8725	0,3951	0,1484
2	0	0	0,995	0,0044	0,0292	0,4695	0,121	0,9127	0,361	0,3698
3	0	0	0	1	0	1	0,0948	0,9316	0,3466	0,75

The first line is the assessment of the probability $P(U|V)$, provided that at the beginning we have complete ignorance of the situation.

Similarly, we can determine the use of the information for assessing the commander degree of uncertainty, therefore, to determine the probability that the commander has true picture of the number and identification of units, arranged against him in his area of interest in the COP. Uncertainty in the probability distributions is informational entropy $H(i)$ and residual knowledge. To determine the extent of knowledge, residual degree of uncertainty destination - a standardized form of entropy we use the equation:

$$K(U, V = v_d) = \frac{\ln(n+1) - H(U|V = v_d)}{\ln(n+1)} \cdot \frac{\ln[\sum_{i=v_d}^n P(U = i | V = v_d - 1)]}{\ln[P(U = n | V = v_d - 1)]} \quad (8)$$

The last three columns in Table 1 contain data of the entropy $H(U|V)$ and residual uncertainty destination - a standardized form of entropy $K(U|V)$ based on each observation and the mean of a factor in the reliability and without the offsetting impact factor of reliability - the probability of transmission of information from the sensor $P(P) = 1,0$, $P(P) = 0,9$ and $P(P) = 0,5$. Figure 1 shows the results graphically.

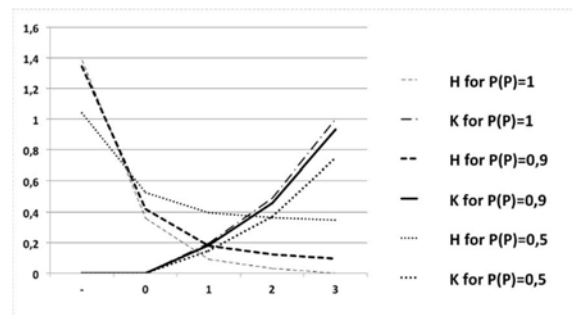


Fig. 1 Effect of the probability transmission of information from the sensor to the entropy
Source: author.

Impact of reliability factors on the probabilistic model - the probability of transmission information from the sensor $P(P)$ from 1 to 0,4 on entropy $H(U|V)$ is presented in Table 2.

Tab. 2 Impact of reliability factors on entropy $H(U|V)$

v	P(P)=1	P(P)=0,9	P(P)=0,8	P(P)=0,7	P(P)=0,6	P(P)=0,5	P(P)=0,4
	H(U V)	H(U V)	H(U V)	H(U V)	H(U V)	H(U V)	H(U V)
-	1,3863	1,3425	1,2876	1,2201	1,1383	1,0397	0,9210
0	0,3602	0,4190	0,4667	0,5018	0,5226	0,5267	0,5106
1	0,0900	0,1768	0,2523	0,3152	0,3636	0,3951	0,4062
2	0,0292	0,1211	0,2018	0,2700	0,3239	0,3610	0,3780
3	0,0000	0,0948	0,1785	0,2497	0,3065	0,3466	0,3665

Figure 2 shows the results graphically.

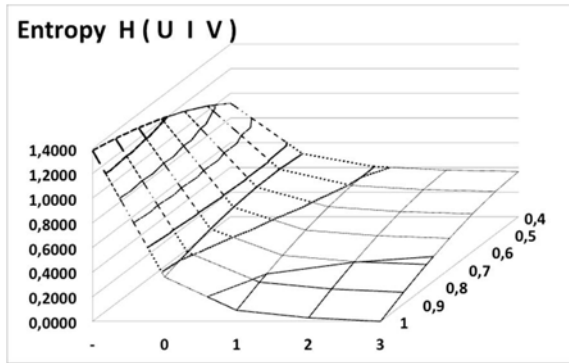


Fig. 2 Effect of the probability transmission of information from the sensor on the entropy
Source: author.

Impact of reliability factors on probabilistic model - the probability of transmission of information from the sensor $P(P)$ from 1 to 0,4 to the standardized entropy $K(U|V)$ is presented in Table 3.

Tab. 3 Effect of the probability transmission of information from the sensor to the standardized entropy and entropy for example 1

	$P(P)=1$	$P(P)=0,9$	$P(P)=0,8$	$P(P)=0,7$	$P(P)=0,6$	$P(P)=0,5$	$P(P)=0,4$
v	$K(U V)$	$K(U V)$	$K(U V)$	$K(U V)$	$K(U V)$	$K(U V)$	$K(U V)$
-	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
0	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
1	0,1941	0,1811	0,1698	0,1603	0,1531	0,1484	0,1467
2	0,4895	0,4563	0,4272	0,4026	0,3832	0,3698	0,3637
3	1,0000	0,9316	0,8712	0,8199	0,7789	0,7500	0,7356

Figure 3 shows the results graphically.

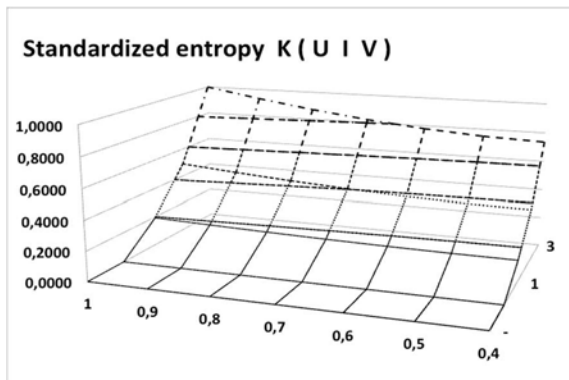


Fig. 3 Effect of reliability factors on the standardized entropy $K(U|V)$
Source: author.

Table 4 shows the impact of the probability transmission of information from the sensor on the overall understanding of the operation according to the conditions of use of a sensor in each cycle of detection.

Tab. 4 Overall knowledge of the operation detection / identification

				For $P(P)=1,0$	For $P(P)=0,9$	For $P(P)=0,5$			
t	q_t	v_{dt}	n_t	$H(U V)$	$K(U V)$	$H(U V)$	$K(U V)$	$H(U V)$	$K(U V)$
1	0,8	2	5	1,096	0,088	1,081	0,1073	0,8947	0,2215
2	0,7	4	5	0,3665	0,4883	0,4626	0,4713	0,6684	0,4523
3	0,9	2	4	0,6968	0,179	0,7218	0,23	0,6946	0,2607
4	0,7	1	3	0,9783	0,0609	0,9752	0,0781	0,8353	0,1874
5	0,9	3	3	0	1	0,0948	0,9316	0,3465	0,75

Table 4 shows a summary of the overall knowledge of the operation depending on the conditions of use of a sensor in each cycle of detection. The operation of detection / identification is made up of 5 cycles. At each cycle t is the probability of detection q_t depending on the conditions of use of the sensors varies depending on the conditions attached in the area of operations, the probability transmission of information from the sensor is $P(P)$, the number of detected units are v_{dt} and the maximum size of enemy units is given as n_t . The last three columns show the residual uncertainty for regulated probability distribution of information available from detection v_{dt} enemy units, a "probability" that the commander has an accurate overview of the number of enemy units in its area of interest.

Detection probability q_t and the probability of transmitting information from the sensor $P(P)$ changes are depending on detection conditions on the battlefield in time t so in order to reflect the changing conditions for a sensor input. Table 2 shows the influence of factors of reliable information transfer on the knowledge of the commander.

The aim is to increase knowledge of the impact on the result of the operation.

The use of entropy to evaluate the results of operations in COP leads to a better understanding of the distribution of enemy units, recognized and effective decisions using its own commander and units.

The procedure of determining the entropy and the probabilistic model, together with complexity theory are used to design a method to increase the level of information in COP and recognition of targets on the battlefield with application of identification (IFF) using new methods of network-oriented environment (Network Enabled Capability - NEC).

4 CONCLUSION

Knowledge of the situation on the battlefield - common operational picture (COP), detection of units - Custom/Foreign (IFF) thus represents the understanding of intentions of the enemy.

The aim of this contribution has been a description of the properties of a probabilistic model for processing of sensor signals using a probabilistic model of recognition Custom / Foreign (Identification Friendly or Foe - IFF) and access to the current intelligence picture of the commander in the common operational picture (COP) for C4I systems.

For the description probabilistic models were used and for determining of explicitness the Bayes model was used. Conditional probabilities were used for the description of a complex cybernetic system.

The probability model shows the impact of the reliability factor - the likelihood of transmission of information from the sensor to the overall knowledge of the operation depending on the conditions of use of sensors in each cycle of detection.

Such modeling allows design and verification of hypothetical assumptions, modeling and simulation processing reconnaissance information from sensors in the process of command and control with the aim to enhance the efficiency, effectiveness using NEC for obtaining information superiority.

For military practice use entropy increase of the level of information in COP and recognition of targets on the battlefield with using new methods of Network Enabled Capability.

Modeling allows to design and determine the conditions, technological change to qualitative change in the terms of command and determine the conditions for the effective use of C4I2 systems and improvement knowledge of the situation on the battlefield - Common Operational Picture. Properties of such systems will be determined on the basis of theoretical analysis of probabilistic models.

References

- [1] MASNICA, R.: Common operational picture and a probabilistic model for recognition identification friendly or foe – IFF. In: *Science & Military 1/2014*. Liptovský Mikuláš : Akadémia ozbrojených síl, 2014. s. 38-42. ISSN 1336-8885.
- [2] MASNICA, R., ŠTULRAJTER, J.: Signal processing with using a probabilistic model for recognition identification friendly or foe – IFF. In: *Medzinárodná vedecká konferencia NTSP 2014*. [CD ROM]. Tatranské Zruby : Akadémia ozbrojených síl, 2014. s. 78-82. ISSN 1339-1445.
- [3] MOFFAT, J.: *Complexity Theory and Network Centric Warfare*. Washington, DC : CCRP Publication Series, 2003. 160 s. ISBN 1-893723-11-9.
- [4] MOFFAT, J.: *Command and Control in the Information Age: Representing its Impact*. The Stationery Office. London, 2002. UK.
- [5] DARILEK, R., PERRY, W. et al.: *Measures of Effectiveness for the Information Age Army*. USA, Santa Monica, CA : RAND, 2001.
- [6] PERRY, W., BUTTON, R. W. et al.: *Measures of Effectiveness for the Information-Age Navy: The Effects of Network-Centric Operations on Combat Outcomes*. USA, Santa Monica, CA : RAND, 2002.
- [7] PERRY, W., MOFFAT, J.: *Measuring the Effects of Knowledge in Military Campaigns*. J. Opl Res. Soc 48. 1997. pp. 965-972.
- [8] STARK, H., WOODS, J. W.: *Probability, Random Processes and Estimation Theory for Engineers*. USA : Prentice Hall, 1986.
- [9] BLAHUT, R. E.: *Principles and Practice of Information Theory*. USA, MA : Addison-Wesley, 1987.
- [10] ZUREK, W. H. ed.: *Complexity, Entropy and the Physics of Information*. Vol III, Santa Fe Institute Studies in the Sciences of Complexity Series. USA : Addison Wesley, 1990.
- [11] KULLBACK, S.: *Information Theory and Statistics*. USA, Dover. New York : 1968.

Eng. Radoslav MASNICA
CSBC Company Ltd.
Roľnícka 10
831 07 Bratislava
Slovak republic
E-mail: masnicar@csbc.sk

Prof. Eng. Jozef ŠTULRAJTER, CSc.
Department of Informatics
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak republic
E-mail: jozef.stulrajter@aos.sk

SEARCHING FOR CRYPTOGRAPHICALLY SECURE ELLIPTIC CURVES OVER PRIME FIELDS

Rafal GLIWA, Janusz SZMIDT, Robert WICIK

Abstract: Elliptic curves over finite fields are applied to construct public key cryptosystems and to realize a digital signature. The security of these systems is based on computational intractability of the discrete logarithm problem in the group of points on an elliptic curve over a finite field. Elliptic curve cryptosystems provide security comparable to that of the RSA cryptosystem but with cryptographic keys of smaller size. This note presents conditions which cryptographically secure elliptic curves over prime fields have to satisfy and methods to generate such curves following the standard [3].

Keywords: Public key cryptography, elliptic curves over prime fields, security conditions, generation of elliptic curves, probabilistic analysis.

1 INTRODUCTION

Elliptic curves over finite fields have applications in public key cryptography for key agreement, encryption, digital signatures and pseudo-random generators. The security of the corresponding cryptosystems is based on intractability of the elliptic curve discrete logarithm problem (ECDLP) in the group of points on an elliptic curve over a finite field. One of the main benefits of Elliptic Curve Cryptography (ECC) in comparison with non-ECC cryptography is the same level of security provided by keys of smaller size. For example, a 256-bit ECC public key provides comparable security to a 3072-bit RSA public key. The U.S. National Institute of Standards and Technology (NIST) has endorsed ECC in the set of recommended algorithms, specifically Elliptic Curve Diffie-Hellman (ECDH) algorithm for key exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) for signatures. The U.S. National Security Agency (NSA) allows their use for protecting information classified up to secret with 384-bit EC keys.

This note presents the results of searching for elliptic curves over finite prime fields F_p satisfying the security conditions of the Brainpool Standard [3]. We have conducted numerical experiments showing how many cryptographically secure curves one can choose from a given set of random elliptic curves over a fixed prime field F_p . Two sets of curves are considered: those generated from seeds coming from expansion of π and e , as in the Brainpool Standard, and those generated from random seeds obtained by our random number generator [5]. We also provide one 384-bit elliptic curve generated from a random seed which satisfies all security and implementation requirements of the Brainpool Standard [3]. A new consideration about security of ECC is given in [2].

2 BASIC DEFINITIONS

Let $p > 3$ be a prime number and let F_p or $GF(p)$ denote the finite field of p elements

$$F_p = \{0, 1, \dots, p-1\}$$

with addition and multiplication modulo p . An elliptic curve over the field F_p is the set of solutions of an equation

$$E : y^2 = x^3 + Ax + B \pmod{p} \quad (1)$$

together with a “point at infinity” O , where the coefficients $A, B \in F_p$ satisfy

$$\Delta = 4A^3 + 27B^2 \neq 0 \pmod{p}.$$

This set forms an abelian group with neutral element O and the addition law given for example in [4]. The group $E(F_p)$ of points of the elliptic curve (1) defined over the finite field F_p has order $\#E(F_p)$ which satisfies the Hasse inequality

$$p + 1 - 2\sqrt{p} \leq \#E(F_p) \leq p + 1 + 2\sqrt{p}.$$

The exact value of $\#E(F_p)$ can be calculated using the SEA-algorithm whose optimized implementation is available in the package Magma [7].

3 CRITERIA FOR ELLIPTIC CURVES OVER PRIME FIELDS

We consider here only elliptic curves over finite fields F_p , where p is a prime number of suitable size in bits. These curves must satisfy suitable conditions to ensure resistance against known attacks on ECDLP which are the main security requirements. We have searched for cryptographically secure elliptic curves over prime fields F_p according to the ECC Brainpool Standard [3]. We have considered the bit lengths 160, 192, 224, 256 and 384 of the basic primes p which were generated according to the algorithm given in [3] from the Brainpool seeds which were chunks of the hexadecimal representation of the number $\pi * 2^{1120}$ and from our seeds which were produced by a random number generator [5]. The elliptic curves were chosen according to the following conditions.

C1. The group order $q = \#E(F_p)$ of the elliptic curve is a prime number in order to prevent a small-subgroup attack [4]. Every non-identity point on such a curve is a generator of the group of points on this curve. The curves with prime group order have no points of order 2 and therefore no points with y -coordinate 0.

C2. Assuming the inequality $q < p$ one avoids overruns in implementation since in some cases even the bit-length of q can exceed the bit-length of p . Elliptic curves with $q = p$ are called trace one curves or anomalous curves. Satoh and Araki [6] proposed an efficient solution to the ECDLP on trace one curves.

C3. Immunity to attacks using the Weilpairing or Tatepairing. These attacks allow the embedding of the elliptic curve group $E(F_p)$ into the group of units of an extension $GF(p^l)$ of degree l of the field F_p , where subexponential attacks on DLP exist. Here we have $l = \min\{t: q \mid p^t - 1\}$, i.e. l is the order of p modulo q . The requirement is that $(q-1)/l < 100$; this means that l is close to the maximal possible value. This requirement also excludes supersingular curves.

C4. We define the number u from the equation $q = p + 1 + u$ and set $d = (4p - u^2)/v^2$, where $v = \max\{a : a^2 \mid 4p - u^2\}$, i.e., d is the square-free part of $4p - u^2$. Let $K = \sqrt{-d}$ be the imaginary quadratic number field. One of the requirements imposed in [1] is that $d > 2^{100}$, which means that the discriminant of the field K is sufficiently large.

C5. The ring of isogenies of the elliptic curve over the finite field (an isogeny is a transformation between elliptic curves which preserves the orders of groups of points on the curves) is isomorphic to a lattice in the ring of integers in the quadratic field $K = \sqrt{-d}$. The requirement formulated in the Brainpool Standard [3] is that the class number of the field K is greater than 10 000 000. It is time consuming to calculate the exact value of this class number, so the Standard [3] proposes an algorithm to assert the required inequality.

The requirements C4 and C5 are sophisticated, they are related to possible improvements of the algorithms solving ECDLP.

4 EXPERIMENTAL RESULTS

The following experiments have been carried out. We have generated random elliptic curves for fixed length of the base prime p according to the algorithm of Brainpool Standard [3] until 100 or 1000 curves satisfying condition C1 have been found. The second columns of the tables give the total numbers of the curves checked. The next columns of the tables give the numbers of curves satisfying the indicated conditions or times of calculation. Tables 1÷4 concern the elliptic curves generated from the Brainpool seeds which were the numbers π and e ,

and Tables 5÷8 the curves obtained from seeds generated by a random number generator [5]. All computations have been done in Magma [7].

Tab. 1 The numbers of elliptic curves satisfying the security conditions (the curves generated from Brainpool seeds)

	All curves	C1	C1+C2	C1+C2+C3+C4+C5
160 bit	19604	100	51	51
192 bit	24432	100	57	57
224 bit	22227	100	51	51
256 bit	36349	100	45	44

Tab. 2 The times (in minutes) of generation of the curves satisfying the given conditions

	All curves	C1	C1+C2+C3+C4+C5
160 bit	19604	29	66
192 bit	24432	64	109
224 bit	22227	120	173
256 bit	36349	246	297

Tab. 3 The numbers of elliptic curves satisfying the security conditions (the curves generated from Brainpool seeds)

	All curves	C1	C1+C2	C1+C2+C3+C4+C5
160 bit	206021	1000	502	498
192 bit	229840	1000	501	493
224 bit	264196	1000	487	479
256 bit	356036	1000	524	514

Tab. 4 The times (in hours) of generation of the curves satisfying the given conditions

	All curves	C1	C1+C2+C3+C4+C5
160 bit	206021	5.46	9.12
192 bit	229840	11.68	14.00
224 bit	264196	25.47	27.84
256 bit	356036	39.81	47.75

Tab. 5 The numbers of elliptic curves satisfying the security conditions (the curves generated from random seeds)

	All curves	C1	C1+C2	C1+C2+C3+C4+C5
160 bit	22693	100	52	52
192 bit	32851	100	46	46
224 bit	25684	100	57	56
256 bit	42211	100	47	47

Tab. 6 The times (in minutes) of generation of the curves satisfying the given conditions

	All curves	C1	C1+C2+C3+C4+C5
160 bit	22693	35	63
192 bit	32851	77	96
224 bit	25684	127	151
256 bit	42211	255	327

Tab. 7 The numbers of elliptic curves satisfying the security conditions (the curves generated from random seeds)

	All curves	C1	C1+C2	C1+C2+C3+C4+C5
160 bit	253914	100 0	512	503
192 bit	310477	100 0	503	500
224 bit	290629	100 0	528	523
256 bit	396279	100 0	503	496

Tab. 8 The times (in hours) of generation of the curves satisfying the given conditions

	All curves	C1	C1+C2+C3+C4+C5
160 bit	253914	5.5	9.45
192 bit	310477	9.87	14
224 bit	290629	18	23.5
256 bit	396279	32.64	44.69

To end this note we present an elliptic curve over the prime field F_p , where p is a randomly generated 384-bit prime number, A, B are the coefficients of the curve, $P = (x_0, y_0)$ is a randomly chosen point on this curve, q the order of the group of points on the curve, l the value from condition C4 and d the value from condition C5. This 384-bit elliptic curve satisfies all security conditions of the Brainpool Standard [3].

$p = 0x85552AE413E218FE96407A08D375AB7122EFE40643672D7803BB9E729E6C9F117815B2B0CC058F986CB31DACB9144FEB,$

$seed_random = 0x629991099D8BA5241BF1601E3A7EFA3F16992B48,$

$A = 0x7E650093A9E415324F3879F5EC1F9A89C21F89701B9F117C4D33FB5C2A50D2EC647EE715E5BC0C63C5FEBF84DC7F8AC,$

$B = 0x3C5FEBF84DC7F8ACC5B466EF0C1E9C2F135E17980B3BEEDABAB4A7550D0DDD684928AD038BEEEC841CA26F18727E243F,$

$x_0 = 0x8405BD74DAB1F3B41658E114F29F78B28E3EF60AAAD118D4A5345BC3320209945F5D23049BB570F4EF053F07FBBD5287,$

$y_0 = 0x35F0E509942B5D426682BDC7ABE0EB48CADBD544ECCA71F0C40C185955CBFE62D5F0EC84862D062695FD2AE0B0B8793,$

$q = 0x85552AE413E218FE96407A08D375AB7122EFE40643672D77E0FDE8B5BF6D64F7C0E58B569CD741BFCE2AB46E804B51BF,$

$l = 20521778549493474636638036249022264275456139090355823129913433068048175326645666326171333114344393525607648679645630,$

$(q-1)/l = 1,$

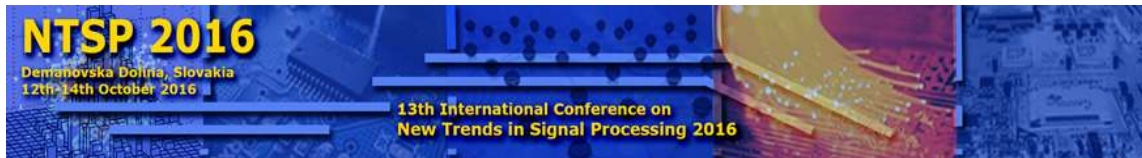
$d = 361606528384249306009928355546154169990169998377694594494439706622033872901623212387088049726004905487037408505123.$

Time of generation: 5343,6 seconds.

References

- [1] BERNSTEIN, D. J., LANGE, T.: *SafeCurves: choosing safe curves for elliptic-curve cryptography*. Available at: <http://safecurves.cr.yyp.to>
- [2] BERNSTEIN, D. J., CHOU, Tung, CHUENGSAIANSUP, Ch., HUELSING, A., LANGE, T., NIEDERHAGEN, R., Van VREDENDAAL, Ch.: *How to manipulate curve standards: a white paper for the black hat*. Cryptology ePrint Archive, 2014/571. Available at: www.iacr.org
- [3] ECC Brainpool. ECC Brainpool Standard Curves and Curve generation, 2005. Available at: <http://www.ecc-brainpool.org/download/Domain-parameters.pdf>
- [4] HANKERSON, D., MENEZES, A., VANSTONE, S.: *Guide to Elliptic Curve Cryptography*. Springer, 2004. ISBN 0-387-95273-X.
- [5] LEŚNIEWICZ, M.: *Sprzętowa generacja losowych ciągów binarnych*. Warszawa : Wojskowa Akademia Techniczna, 2009. ISBN 978-83-61486-31-2.
- [6] SATOH, T., ARAKI, K.: *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves*. Comm. Math. Univ. Sancti Pauli, 47, pp. 81-92, 1998.
- [7] Magma Computational Algebra System. Available at: www.magma.math.usyd.edu.au

Ph.D. Rafal GLIWA
 Ph.D. Janusz SZMIDT
 Ph.D. Robert WICIK
 Military Communication Institute
 05-130 Zegrze Poludniowe
 Poland
 E-mail: r.gliwa@wil.waw.pl
j.szmidt@wil.waw.pl
r.wicik@wil.waw.pl



ARMED FORCES ACADEMY OF GENERAL M. R. ŠTEFÁNIK
 and
 SLOVAK ELECTROTECHNICAL SOCIETY

invites you to

13th International Scientific Conference

**THE INTERNATIONAL CONFERENCE ON NEW TRENDS IN SIGNAL
 PROCESSING 2016**

12th– 14th October 2016

The International Conference on New Trends in Signal Processing 2016 (NTSP 2016) provides a space for a presentation of new advances and research results in the field of theoretical, experimental, and applied analog and digital signal processing. The conference covers main topics: **Signal Processing; Applied Electronics; Information and Communication Engineering; Microwave Engineering; Signal Processing in Military Applications.**

Contact adress: NTSP 2016
 Department of Electronics
 Armed Forces Academy of general M. R. Štefánik
 Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic
 E-mail: ntsp2016@aos.sk

HIERARCHICAL MODEL OF DECISION ACCEPTANCE IN INTELLIGENT MANET CONTROL SYSTEM

Oleg Y. SOVA, Valery A. ROMANYUK, Anton V. ROMANYUK,
Oleksandr I. LYSENKO, Inga V. URYADNIKOVA

Abstract: The new approaches of OSI level functioning in the self-organizing wireless networks MANET are proposed. They consist in the implementation of new methods and radio network management functions, coordination and intellectualization of the methods, corresponding to different OSI-model levels, and also coordination of the network resource management purposes distribution.

Keywords: Mobile radio network, intelligent control system, intelligent agent, multiagent system.

1 INTRODUCTION

MANET (*Mobile Ad-Hoc Networks*) [1] class mobile radio network (MRN) control features are: radio network control system (CS) consists of multiple CS nodes, that interact during the data transmission; dynamic nature of MRN leads to necessity of hierarchical architecture of their CS (master nodes and slave nodes) [2]. CS nodes make decisions based on gathering and processing of large volumes of service information about both node and entire MRN status; it is impossible to have full MRN status information in real time, therefore CS must make decisions in uncertain conditions.

MRN control process main requirement is that all management decisions for node and network resources must be carried out automatically by independent mobile nodes. Furthermore, during the management process every node's CS must consider not only its own goal function, but the goal function of all neighboring nodes [3], whose information is stored on the master node. In this scenario, MANET class radio network CS management decisions must be based on the intelligent ability to recognize and analyze different situations (on either node or network level).

Modern approach for intelligent node control system (ICS) design in view of the MANET class MRN functioning and mentioned above requirements is the use of the intelligent agents (IA) technology and multi-agent systems (MAS) [4]. Main feature of this technology is that an agent is considered as a hardware and software system, that can make decisions in uncertain conditions. That is, IA and MAS can adapt to the changes in surrounding environment they interact with, even in the case when said changes are not defined in their behavior schemes.

There are many examples of IA and MAS used for gathering and processing information, as well as automatic management of different complex systems and processes [5]. But existing models of IA and MAS are designed using the intelligent methods that do not account for the MANET class network control features, and the lack of a method for designing

corresponding models for ICS nodes delays the process of MRN development.

Therefore, the *purpose* of this article is to develop the hierarchical model for intelligent agents interaction for the MANET class radio network control system development.

2 INITIAL DATA FOR THE MODEL

According to the concept [2], MRNICS is an aggregation of interacting node ICS that are deployed using the IA technology [6]. In this case, IA stands for a software product able to act to achieve a given goal and in addition to the main features (reactivity, proactivity, sociality) has [7]:

Mobility – IA can carry out its functions on another node on behalf of the initiator node;

Intelligence – the main feature of IA, that presume its ability to self-learn in the process of the mobile node operations so that it can find optimal behavior patterns for cases not foreseen at the design phase.

Every IA of a node ICS is designed for a specific type tasks (performs different functions, depending on OSI model levels) (Fig. 1), can interact with other IA for information exchange and make coordinated decisions, forming the executive layer of network ICS.

The coordination of IA operations on executive layer is managed by metaagents of node ICS. Multiple metaagents form the node layer of network ICS. In turn, coordination of metaagents' decisions of node ICS is managed by a master node. Any node of the network can be a master node, depending on its hardware or geographic location.

As seen on Fig. 1, main management agents of the node ICS of the network can be distinguished as follows: functional agent, system agent, monitoring agent, diagnostics agent, foresight agent. Though, the quantity and composition of IA can vary drastically depending on the network node (mobile node, base station or sensor device) [8].

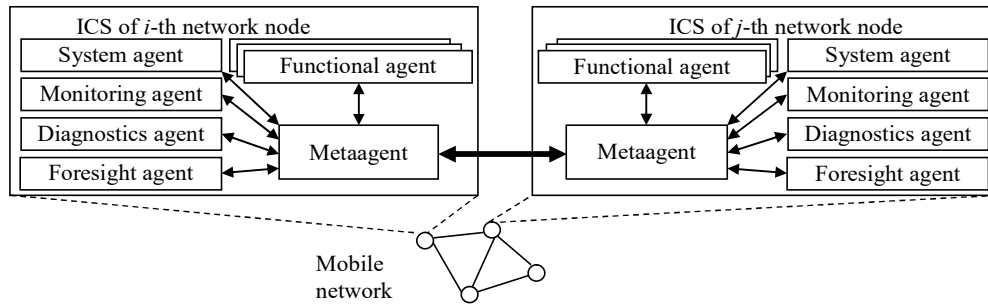
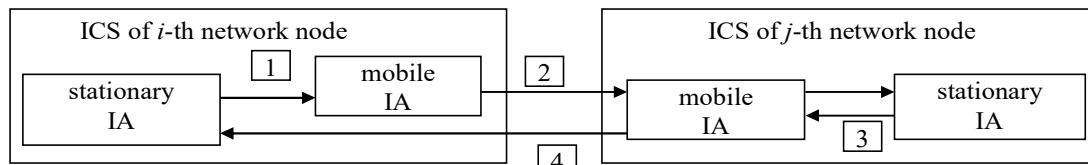


Fig. 1 Interaction of IA in the intelligent network control system
Source: authors.



1 – node i generates a MIA. 2 – MIA relocation. 3 – data collection and processing. 4 – return to the node i

Fig. 2 MIA life cycle
Source: authors.

Metaagent takes care of coordination of IA operations to achieve common management goals using the management decision made by local agents and metaagents of neighboring nodes. Metaagent analyzes network information by communicating with neighboring nodes so that it is able to make a decision to provide a certain level of QoS.

System agent. Its main functions are: maintaining a database of neighboring node and network status (available resources), mobile node locations (topographic information); forming a knowledge base with rules of “behavior” of the given node under different circumstances; self-learning of the mobile node.

Monitoring agent – implements continuous monitoring of the network key performance indicators in real time; identifies different situation on the MRN, determines current and potential problems; gathers and analyzes service information (statistics).

Diagnostics agent – determines, localizes and analyzes nod malfunctions; runs tests of main functions of all of the mobile node’s modules.

Foresight agent – uses the rules and algorithms of network performance analysis on all its layers to make a forecast of node and MRN status in the near future.

Functional agents – implements control methods for every layer of OSI model: topology management, routing management, data streams management, queue management, message priority and security, spectrum allocation, power allocation etc.

Most of the aforementioned IA are stationary, they are located on the node permanently. But for some functions (network zone monitoring,

information route planning, etc.) system agent can generate a mobile IA (MIA). MIA is relocated to another network node, collects (and processes if necessary) the information of the given node and returns to the source node with a report (or, if necessary, is relocated to a new node). MIA life cycle is illustrated on Fig. 2.

Therefore, in view of the hierarchical concept of network ICS design [2] and aforementioned functional structure of node ICS with IA, formal description of MANET class radio network ICS can be presented as multiple IAs on different layers, that interact with each other by exchanging service information that is used to make management decisions. To achieve this, we need to solve two problems: combine heterogeneous IA in the hierarchical network ICS and set up information exchange between IA in this structure. To solve these problems an hierarchical model of IA interaction is proposed, whose structure corresponds to the hierarchical network ICS design concept.

3 HIERARCHICAL MODEL OF IA INTERACTION

Formal description of the network ICS functional structure (with decentralized management) can be represented as a hierarchical IA structure with vertical relations between them. Given relations define the subordination of task that are resolved by IA at each layer [2]:

Zero (executive) layer – resolves management tasks according to the OSI model (routing, resource management, data streams management, security,

etc.) by selecting the required values of node ICS subsystem parameters;

First (node) layer – consists of node ICS meta-agents that coordinate the zero layer IA by selecting optimal set of management actions and their implementation sequence on all node ICS subsystems;

Second (network) layer – consists of the master node that corrects the goal functions of first layer meta-agents in view of network status, as a whole, or its part.

Using graph theory we can picture the given functional structure as shown on Fig. 3. Located at the root of the tree is a master node subsystem (I_2, U_2) , at the vertices that are one edge away from the root are subsystems $(I_{11}, U_{11}), \dots, (I_{1q}, U_{1q}), \dots, (I_{1Q}, U_{1Q})$ that represent Q meta-agents of node ICSs. Every mentioned subsystem of network ICS contains a control (identification) block I and management block U .

In turn, every first layer subsystem $(I_{1q}, U_{1q}), q = \overline{1, Q}$ is connected to multiple functional subsystems of zero layer $P_{qr}, q = \overline{1, Q}, r = \overline{1, R}$, that are located on two edges distance from the root. These subsystems represent IA interaction processes of every functional subsystem of node ICS [9]. This interaction consists of service information exchange and management decisions of each IA.

For q-th management subsystem of the first layer $(I_{1q}, U_{1q}), q = \overline{1, Q}$ let us denote the following:

$X_{1qr}(k)$ - multiple state vectors of the qr-th IA, where the size of $X_{1qr}(k) = \{x_{1qr}^a(k)\}, a = \overline{1, a_{1qr}}$ is $a_{1qr} \times 1$;

$\tilde{X}_{1q}(k)$ - multiple generalized estimated state vectors of q-th subsystem of the first layer (e.i. mobile node), where the size of $\tilde{X}_{1q}(k) = \{\tilde{x}_{1q}^a(k)\}, a = \overline{1, a_{1q}}$ is $a_{1q} \times 1$;

$U_{1qr}(k)$ - multiple management vectors of q-th subsystem of the first layer, that are directed to r-th IA of the zero layer, where the size of $U_{1qr}(k) = \{u_{1qr}^b(k)\}, b = \overline{1, b_{1qr}}$ is $b_{1qr} \times 1$;

$Y_{1q}(k)$ - multiple management vectors of q-th subsystem of the first layer, that are directed to the upper layer management subsystem (master node), where the size of $Y_{1q}(k) = \{y_{1q}^d(k)\}, d = \overline{1, d_{1q}}$ is $d_{1q} \times 1$;

$Z_{1q}(k)$ - multiple estimated state vectors of q-th subsystem of the first layer, that are directed to upper

layer management subsystem (master node), where the size of $Z_{1q}(k) = \{z_{1q}^d(k)\}, d = \overline{1, d_{1q}}$ is $d_{1q} \times 1$.

For the second layer management subsystem (I_2, U_2) (master node), let us denote:

$\tilde{X}_2(k)$ - multiple generalized estimated state vectors of the first layer subsystems (metaagents of the node ICS), where the size of

$$\tilde{X}_2(k) = \{\tilde{x}_2^l(k)\}, l = \overline{1, l_r} \text{ is } l_r \times 1 = \left(\sum_{q=1}^Q a_{1q} \right) \times 1;$$

$Y_{2q}(k)$ - multiple management vectors of control variables, that are sent to lower layer management subsystems (metaagents of the node ICS), where the size of $Y_{2q}(k) = \{y_{2q}^d(k)\}, d = \overline{1, d_{2q}}$ is $d_{2q} \times 1$;

$Z_{2q}(k)$ - multiple management vectors of variable estimated states, that are sent to the lower layer management subsystem (metaagents of the node ICS), where the size of $Z_{2q}(k) = \{z_{2q}^d(k)\}, d = \overline{1, d_{2q}}$ is $d_{2q} \times 1$;

Finally, for qr-th subsystem of the zero layer $P_{qr}, q = \overline{1, Q}, r = \overline{1, R}$ let us denote:

$C_{rp}^q(k)$ - multiple connections vectors (service information exchange between IA and their management decisions), where $C_{rp}^q(k) = \{c_{rp}^{qm}(k)\}, m = \overline{1, m_r}, n = \overline{1, n_r}$ between r-th and p-th subsystems $(r, p = \overline{1, Q}, p \neq r)$;

$\Pi_{qr}(k)$ - multiple external effects vectors, that are been measured by r-th IA of the q-th mobile node, where the size of $\Pi_{qr}(k) = \{\pi_{qr}^l(k)\}, l = \overline{1, l_q}$ is $l_{qr} \times 1$.

Wherein, multiple vectors of q-th IA states $X_q(k) = \bigcup_{r=1}^R X_{1r}(k)$ can be of different type depending on their state variables, that affect the channel quality and mobile node or network efficiency. Some of them are:

Network information load parameters vector

$$\Lambda(k) = \|\Lambda_1(k), \dots, \Lambda_q(k), \dots, \Lambda_Q(k)\|^T;$$

Information messages delays vector

$$H(k) = \|H_1(k), \dots, H_q(k), \dots, H_Q(k)\|^T;$$

Network radiofrequency environment parameters

$$\aleph(k) = \|\aleph_1(k), \dots, \aleph_q(k), \dots, \aleph_Q(k)\|^T;$$

Network spectrum resources vector

$$\Im(k) = \|\Im_1(k), \dots, \Im_q(k), \dots, \Im_Q(k)\|^T$$

Network energy resources vector

$$\Re(k) = \|\Re_1(k), \dots, \Re_q(k), \dots, \Re_Q(k)\|^T;$$

Hardware resources vector (processor, battery capacity, RAM, etc.)

$$A(k) = \|A_1(k), \dots, A_q(k), \dots, A_Q(k)\|^T,$$

etc.

As shown in the model (Fig. 3), any q -th management subsystem of the first layer (I_{1q}, U_{1q}), $q = \overline{1, Q}$ can be characterized by:

Mapping that describes the object being managed (metaagent of q -th mobile node)

$$O_1^{(1)}: \tilde{X}_{1q} \times U_{1q} \times C_{qp} \times \Pi_q \rightarrow Y_{1q} \times Z_{1q}; \quad (1)$$

Mapping that describes the criteria used by q -th mobile node metaagent to determine the estimated state V_q and control influence W_q

$$O_2^{(1)}: \tilde{X}_{1q} \times Z_{1q} \rightarrow V_q, \quad (2)$$

$$O_3^{(1)}: U_{1q} \times Y_{1q} \rightarrow W_q; \quad (3)$$

Mapping that describes the generalized information Φ_q that arrives to upper layer subsystem (master node)

$$O_4^{(1)}: Y_{1q} \times Z_{1q} \rightarrow \Phi_q \quad (4)$$

Mappings that determine the constraints of input variables vectors Θ_q and control influence vectors Ψ_q , respectively

$$O_5^{(1)}: X_{1qr} \rightarrow \Theta_q, \quad (5)$$

$$O_6^{(1)}: U_{1q} \rightarrow \Psi_q. \quad (6)$$

Second layer subsystem (I_2, U_2) can be characterized by:

Mapping that describes the formation of the generalized estimated states vector of the mobile network

$$O_1^{(2)}: \Phi \rightarrow \tilde{X}_2, \quad (7)$$

where $\Phi = \bigcup_{q=1}^Q \Phi_q$;

Mapping that describes the criteria used by the (I_2, U_2) subsystem (master node) to determine the control influence destined for (I_{1q}, U_{1q}), $q = \overline{1, Q}$

$$O_2^{(2)}: U \times \tilde{X}_2 \rightarrow W, \quad (8)$$

where $U = \bigcup_{q=1}^Q Y_{2q}$;

Mappings that determine the constraints for generalized state and control vectors

$$O_3^{(2)}: \tilde{X}_2 \rightarrow \Theta, \quad (9)$$

$$O_4^{(2)}: U \rightarrow \Psi. \quad (10)$$

The functioning of the ICS of all mobile network elements (mobile or sensor nodes, mobile base station or network control center) [9] can be described by time intervals, as follows:

T_{1q} - time interval for performing management and control tasks (1 – 6) by metaagents of every node ICS ((I_{1q}, U_{1q}) subsystems);

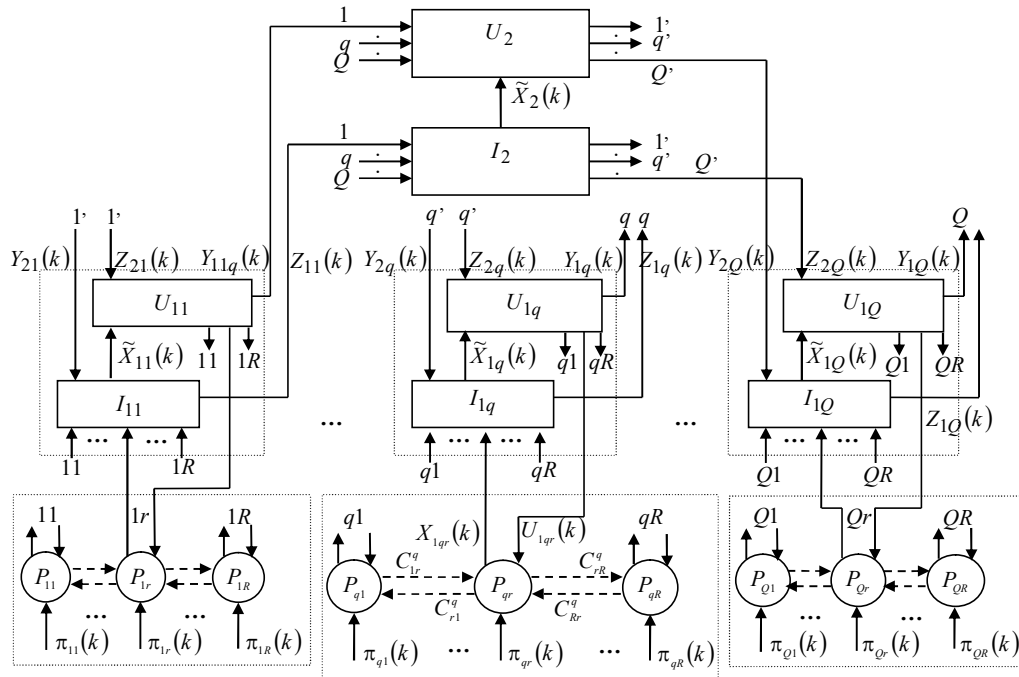


Fig. 3 Hierarchical model of IA organization of network ICS

Source: authors.

$T_{1q}^{(2)}$ - time interval of generalized information transmission from metaagents (I_{1q}, U_{1q}) to the master node (I_2, U_2) subsystem);

T_2 - time interval for performing the control and management tasks (7 – 10) by the master node.

The length of T_{1q} time interval is determined by the external influence vector $\Pi_{qr}(k)$ change rate, change of the control influences $Y_{2q}(k)$ and $Z_{2q}(k)$ from the master node (I_2, U_2) , and the change of interconnection matrix $C_{rp}^q(k)$ structure. The length of $T_{1q}^{(2)}$ time interval is determined entirely by the methods and protocols of interaction between (I_{1q}, U_{1q}) and (I_2, U_2) subsystems, defined at appropriate levels of the OSI model.

Based on the information received by node ICS metaagents $(I_{1q}, U_{1q}), q = \overline{1, Q}$, the master node (I_2, U_2) checks the restraints (9), (10) and calculates the values of the indicator in (8) with control influences $U(k) = \{U_{1qr}(k)\}$, that are defined by subordinate node ICS on the previous time interval. If constraints are observed or a criterion has a deviation from the required value, a higher layer task is performed again, which defines the length of time interval T_2 .

For a three layered network ICS (Fig. 3) the ratio between the aforementioned time intervals is as follows [9]:

$$T_2 \geq T_{1q}^{(2)}, T_2 \gg T_{1q}, T_{1q}^{(2)} \geq T_{1q}, \text{ for } \forall q = \overline{1, Q}.$$

During those time intervals every element of the network ICS implements corresponding methods and algorithms of mobile network management, from mathematical methods and algorithms of link management (physical level of OSI model) to methods and algorithms of application level management (security management, power consumption management, QoS management, etc.).

4 DECISION MAKING IN THE NETWORK INTELLECTUAL CONTROL SYSTEM

In the general scenario, management decision making in the network ICS means providing a given quality of information exchange in MANET by determining the values of control variables of node ICS based on the analysis of current state of the radio network. But, as mentioned before, every node ICS is characterized by its own goal function, that is formed based on multiple factors:

Resources and hardware/software capabilities of the node, i.e. the totality of the devices for reaching

the goal (RAM, processor performance, battery capacity, etc.);

Managed parameters: on physical level – transmitter power, modulation, transmission rate, etc., on channel level – access protocol, on network level – routing method, on transport level – transfer method, etc.

Uncontrollable parameters: set exchange protocols, topology dynamics, network size, interference level, etc.:

Requirements for information exchange quality for different types of traffic (data, voice, video, graphics).

It leads to the inability to achieve global optimization of the entire mobile network in the case of decentralized management environment and with presence of contradiction between the optimal node ICS awareness and the timeliness of control influences. Thereby, it was proposed in [10] to decompose the main goal of mobile network management to multiple simpler goals. To achieve this, in the design phase of node ICS a goal structure (GS) is formed as a graph, where the vertices are goals, and edges are the influences of achieving a goal in a subgoal (Fig. 4).

In the previous research it was shown, that in an uncertain environment, where a mobile network functions, to describe a situation and make a management decision by the subsystems of node ICS it is advisable to use the methods of fuzzy logic [11]. Therefore, the goal structure (Fig. 4) can be mathematically interpreted as a list of fuzzy management goals of different levels L_1, \dots, L_k , that are connected by [10, 12]:

$$\begin{aligned} \text{GS} = \{ & C_1, R_{2m_{(1)}} \{ C_{21}, C_{22}, \dots, C_{2m_{(2)}} \}, \\ & R_{3m_{(2)}} \{ C_{31}, C_{32}, \dots, C_{3m_{(3)}} \}, \dots, \\ & R_{km_{(k)}} \{ C_{k1}, C_{k2}, \dots, C_{km_{(k)}} \} \} \end{aligned} \quad (11)$$

where C_1 – global goal of the network ICS, that is determined by the master node; $C_{il}, i = \overline{1, k}$,

$l = \overline{1, m_{(i)}}$ – l -th subgoal of i -th level of the goal structure, that is determined by the metaagent of the corresponding node ICS; $R_{ij}, i = \overline{1, k}, j = \overline{1, m_{(i-1)}}$ – fuzzy relationship between the lax advantage of the objects on the i -th level over every object at the upper $i-1$ level.

If R_{ij} describes the relationship only between the subgoals of neighboring levels, we should talk about a goal tree, other wise the goal structure degenerates to a network.

Let the goal system consist of k levels and every L_i level $i = \overline{1, k}$ consists of m_i objects (for first level $m_1 = 1$):

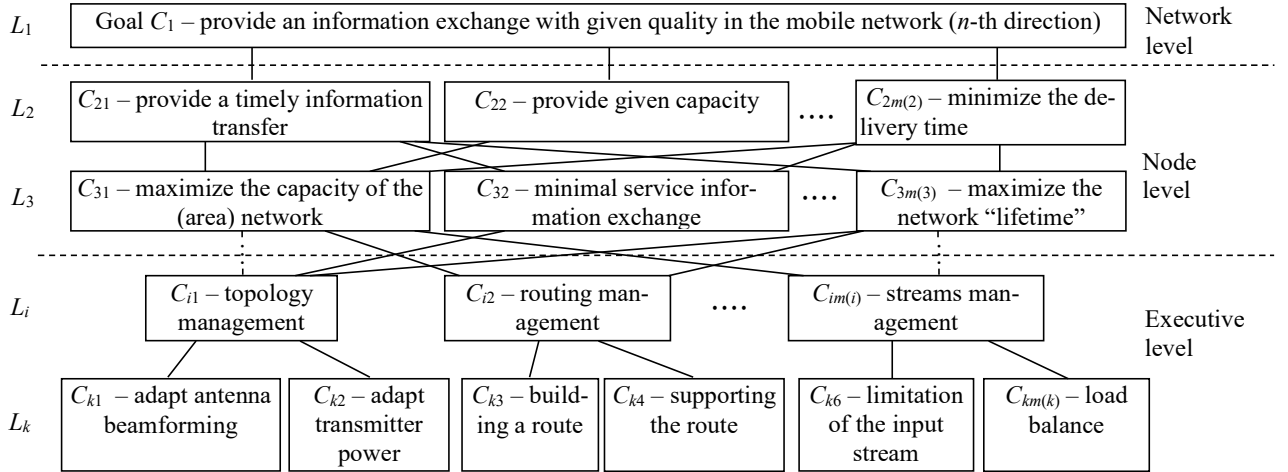


Fig. 4 Fragment of the goal structure of the network ICS

Source: authors.

$$L_i = \{C_{i1}, C_{i2}, \dots, C_{im(i)}\}.$$

Goal structure (Fig. 4) can be described as a multiple of levels L_i :

$$GS = \bigcup_{i=1}^k L_i = \bigcup_{i=1}^k \bigcup_{l=1}^{m_i} C_{il}.$$

As seen on Fig. 4, different elements of the goal structure are united under a global goal C_1 , that can be described as providing the information exchange with given quality in the network. As mentioned before, a binary fuzzy relationship of a lax advantage R_{ij} is used to describe the relationship between global goal and lower level goals, that is given by a membership function $\mu_{R_{ij}}(C_{il}, C_{ir})$, $i = \overline{2, k}$, $j = \overline{1, m_{(i-1)}}$, $l, r = \overline{1, m_i}$.

It should be noted, that depending on the hierarchy layer (Fig. 3) there can be two types of relationship:

“goal - subgoal” relationship – appear between the elements of the network and node layers (between master node and subordinate nodes of a mobile network or its area) and create a goalforming part of the GS;

“subgoal – means to reach the goal” relationship – appear between elements of the node layer (metaagents of node ICS) and the elements of the executive layer (IA of corresponding functional subsystems) and create an implementing part of the GS.

And so, beginning with the second hierarchy layer (11), at every i -th layer there are as many fuzzy relationship of advantage R_{ij} as there are objects at $i - 1$ level of GS. In the general case, these relationships can be described as a matrix:

$$R_{ij} = \begin{pmatrix} 1 & \mu(C_{i1}, C_{i2}) & \dots & \mu(C_{i1}, C_{im(i)}) \\ \dots & 1 & \dots & \dots \\ \mu(C_{im(i)}, C_{i1}) & \dots & \dots & 1 \end{pmatrix},$$

where $\mu_{R_{ij}}(C_{il}, C_{ir}) \in [0; 1]$, $i = \overline{2, k}$, $j = \overline{1, m_{(i-1)}}$, $l, r = \overline{1, m_i}$.

As a result, tasks of decision making of the network ICS are reduced to receiving of the priority vector of the lower layer elements in relationship to the global goal – the element of the first layer. To cope with this task in [12] it is proposed to use a weighting procedure of the hierarchy analysis method or fuzzy relationship convolution algorithm.

5 CONCLUSIONS

Thereby, to respond to the features of the management in the MANET class mobile networks, the management system must have intellectual capabilities to recognize and analyze the situations in the radio network, and based on this, make management decisions to control the node and network resources. To design such management system, it is proposed to use the technology of intellectual agents and multiagent systems, that suggests that all subsystems of node ICS are implemented using multiple IA, that are defined by management functions depending on the level of the OSI network model.

To combine different IA in an intellectual network control system a hierarchical model of IA interaction was proposed in this article, whose essence lies in describing the network ICS as a hierarchical structure with vertical links, that indicate the subordination of management tasks.

The novelty of the model lies in using the graph theory to make a formal description of the functional subsystems of the network ICS (vertices of the graph) and their interaction processes (edges of the graph). Using the proposed model can accelerate and systemize the network design process considering their functioning environment and hierarchical structure of their ICS. Using the intellectual agents technology and multiagent systems allows to minimize the service traffic and use network and node resources more efficiently.

During future research a model for information resources organization of network ICS will be developed, to describe the circulation, processing and storage of the service information, that is used by the methods and protocols of corresponding subsystems for making management decisions in the mobile network.

References

- [1] CONTI, M.: Mobile ad hoc networking: milestones, challenges, and new research directions. Conti, M., Giordano, S. *Communications Magazine*, IEEE. Vol. 52, Issue 1. P. 85–96.
- [2] ROMANYUK, V.: *Concept of hierarchical design of intelligent control systems of MANET class tactical radionet works*. Sova, O., Romanyuk, V., Zhuk, P., Romanyuk, A.: 22nd international conf. “UHF and telecommunication technologies” Crimico-2012. Sevastopol : Crimico, 2012. pp. 265 – 266.
- [3] ROMANYUK, V.: Target functions of operational control of tactical radio networks. Romanyuk, V.: *Collection of scientific work of MITI NTUU “KPI”*. 2012. № 1. PP. 109 – 117.
- [4] RUSSEL, S.: *Artificial intelligence. A modern approach*. Russel, S., Norvig, P. Williams, 2007. 1408 c.
- [5] BUGAICHENKO, D.: *Design and implementation of methods considering formal and logical specifications of self-tuning multiagent systems with time constraints*: PhD thesis: 05.13.11 Bugaichenko Dmitrii Yurievich. SPb., 2007. 259 p.
- [6] ROMAYUK, V.: *Analysis of possibilities of intelligent agents usage for building the node control systems for MANET*. Sova, O., Simonenko, O., Romanyuk, V., Umanec Y. *Collection of scientific work of MITI NTUU “KPI”*. 2013. № 1. P. 76 – 84.
- [7] GAVRILOVA, T.: *Knowledge bases of intelligent systems*. Gavrilova, T., Horoshevski, V.: SPb. Piter, 2000. 384 p.
- [8] ROMANYUK, V.: Architecture of MANET control systems. Romayuk, V., Sova, O., Zhuk, O.: *Conf. “Problems of telecommunications - 2011”*. K.:ITSNTUU “KPI” 2011. p. 77.
- [9] MINOCHKIN, A.: Objective, multiagent model of operational control of mobile component of anew generation military network. Minochkin, A., Shacilo, P.: *Collection of scientific work of MITI NTUU “KPI”*. 2008. № 3. pp.107–118.
- [10] MINOCHKIN, A.: Methods of decision making in amobileradio network control system. Minochkin, A., Romanyuk, V. *Collection of scientific work of MITI NTUU “KPI”*. 2006. № 1. PP. 66 – 71.
- [11] ROMANYUK, V.: Methods of process in the know ledge about a situation in MANET network for building intelligent node control systems. Sova, O., Romanyuk, V., Minochkin, D., Romanyuk, A. *Collection of scientific work of MTI STU*. 2014. № 1. pp. 97 – 110.
- [12] BLUMIN, S.: *Methods of decision making in anuncertain environment*. Blumin, S., Shuikova, I., Lipetsk: LEGI, 2001. 138 p.

Oleg Y. SOVA, PhD.
 Prof. Valery A. ROMANYUK, PhD.
 Military Institute of Telecommunications
 and Informatization
 Moskovska str. 45/1
 010 11 Kyiv
 Ukraine
 E-mail: soy135@ukr.net
 rom-v-a@yandex.ua

P.G. Anton V. ROMANYUK
 Prof. Oleksandr I. LYSENKO, PhD.
 National Technical University of Ukraine
 Peremogy av. 37
 030 56 Kyiv
 Ukraine
 E-mail: anton.romaniuk@gmail.com
 lysenko.a.i.1952@gmail.com

Assoc. Prof. Inga V. URIADNIKOVA, PhD.
 Odessa National Polytechnic University
 Shevchenko av. 1
 650 44 Odessa
 Ukraine
 E-mail: ingavictory@gmail.com

CRYPTOGRAPHY AND GENETIC ALGORITHMS

Martin JAVUREK, Marcel HARAKAI

Abstract: The genetic algorithm is used in cryptography, mainly for deciphering cipher, but may be also used as the random number. This article is a brief overview of genetic algorithms. The genetic algorithms are used as generators of random numbers. They are also used in cryptanalysis and for training and designing of artificial neural networks. The summary describes the advantages and disadvantages of genetic algorithms.

Keywords: Genetic algorithm (GA), Tree parity machine (TPM), Artificial Neural Network (ANN), cryptography.

1 INTRODUCTION

The genetic algorithm is a search algorithm based on the mechanics of natural selection and natural genetics. A population of individuals should behave like a natural system in order to adapt to some environment. Survival and reproduction of an individual is promoted by the elimination of useless features and by rewarding useful behavior. The genetic algorithm belongs to the family of evolutionary algorithms, along with genetic programming, evolution strategies, and evolutionary programming. Evolutionary algorithms can be considered as a broad class of stochastic optimization techniques. An evolutionary algorithm maintains a population of candidate solutions for the problem at hand. The population is then evolved by the iterative application of a set of stochastic operators. The set of operators usually consists of mutation, recombination, and selection or something very similar. Globally satisfactory, if sub-optimal, solutions to the problem are found in much the same way as populations in nature adapt to their surrounding environment.

There are some groups of problems for which a GA can be very useful. The application of a genetic algorithm (GA) in the field of cryptography is rather unique. Only few works exist on this topic. This nontraditional application is investigated to determine the benefits of applying a GA to a cryptanalytic problem, if any. If the GA-based approach proves successful, it could lead to faster, more automated cryptanalysis techniques. However, since this area is so different from the application areas where GAs developed, the GA-based methods will likely prove to be less successful than the traditional methods [11].

2 GENETIC ALGORITHM

The Genetic algorithm is based on the Charles Robert Darwin's theory of evolution. It is adaptive heuristic exploration algorithm based on mechanics of the theory of natural selection and natural genetics [1], [2].

The main idea of genetic algorithm is to replicate the randomness from nature where population of

individuals adapts to its surroundings over natural selection process and behavior of natural system. Survival and reproduction of an individual is promoted by the elimination of unwanted characteristics [2].

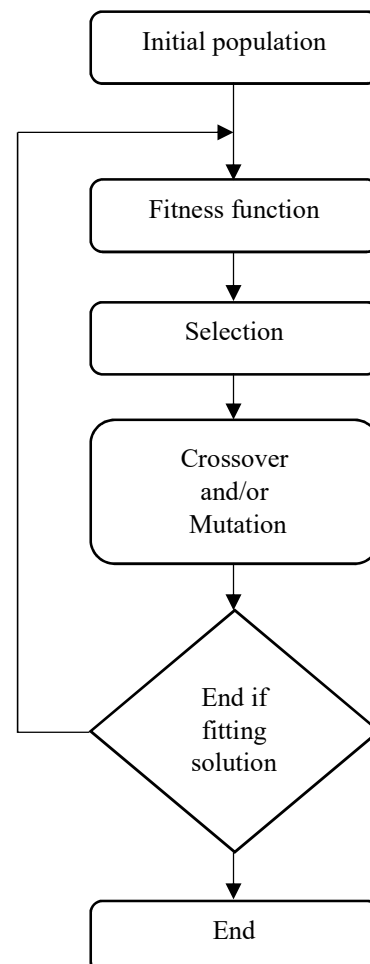


Fig. 1 Genetic algorithm
Source: authors.

Genetic algorithm is required to initialize a population of suitable size and suitably selected fitness function which is essential to achieve a suitable outcome. And subsequently used by three operators to transform a population (chromosomes) into the new population with better fitness:

1. Selection.
2. Crossover.
3. Mutation.

Initial population is also called chromosomes. Genetic algorithm needs initial population with some population size which remains constant from generation to generation. Determining the size of the population is a crucial factor. Too small population size increases risk of converging prematurely to local minima. Initial population can be determined randomly or by using some heuristic [2].

Fitness function is very important for guiding genetic algorithm. It can help to explore the search space more effectively and efficiently, but if the fitness function is bad, it can easily make genetic algorithm get trapped in a local optimum solution and lose the discovery power. Fitness function can be classified as constant fitness function and mutable fitness function [2].

Selection is the stage of the genetic algorithm in which individual chromosomes are chosen from a population for reproduction. It is a quantitative criterion based on fitness value. The chromosome with higher fitness value will be considered better in order to implement proportionate random choice [1], [2].

Crossover is a genetic operator which takes two chromosomes and new child is generated by taking some attributes of first chromosome and rest from second chromosome [1], [2].

Mutation is a genetic operator which changes one or more bits in the chromosome. It is used to maintain genetic diversity from one generation to the next. It is similar to biological mutation. It is performed on the child after crossover. Mutation allows the algorithm to avoid local minima by preventing the population chromosomes from becoming too similar to each other [1], [2].

We do not need to use both operators but there is a question what is better crossover or mutation? There are some pluses and minuses which can help us to decide [4]:

1. Only crossover can combine information from two parents.
2. Only mutation can introduce new information.
3. Crossover does not change the frequencies of the population.

According to these advantages and disadvantages, the easiest answer is to use both operators.

3 GENETIC ALGORITHM AS RANDOM NUMBER GENERATOR

Genetic algorithm in cryptography can be used for generating the key. Key generation in cryptography is the most important part of encoding data. If the key is randomly chosen and non-repeating used than this cypher is called one time pad (or one time system). The one time pad is theoretically unbreakable [1], [3]. The one of the most used one time pad is in Vernam cipher. Vernam cipher is a stream cipher where plaintext is converted into cipher text by using XOR operation between plaintext and the key [1], [3].

One of the possible methods of generating the key is described in the work [3]. It consists of:

1. Generating binary population. For this step, pseudo random number generator can be used.
2. Selection. Where the two parents will be chosen for reproduction.
3. Crossover. From parents by using crossover operator we gain child.
4. Mutation. After crossover we applied mutation operator.
5. Fitness function. If value from fitness function is satisfactory random chromosome is selected as the key else process is repeated.

4 GENETIC ALGORITHM IN CRYPTOANALYSIS

One of the most used genetic algorithms is in cryptanalysis. Cryptanalysis is the process of recovering the plaintext or key from a cipher [4]. Genetic algorithm can be used in genetic attack in neural cryptography and often in attacks on the transposition cipher. In breaking transposition cipher are used four main attack models where difficulty of a successful attack relates to the quantity of information that attacker has. Those models are sorted by the amount of information that the attacker has [5]:

1. Ciphertext only.
2. Known plaintext.
3. Chosen plaintext.
4. Chosen ciphertext.

4.1 Known plaintext attack

The main idea in this model is that attacker knows a sample plaintext for a corresponding encrypted text. Attacker now needs to reconstruct key, knowing encryption function, decryption function, substring of the plaintext and substring of the ciphertext, in order to read all encrypted messages. Given the complexity of encryption and decryption function it is not a trivial problem [5].

4.2 Chosen plaintext attack

There the attacker knows substring of the plaintext, chosen by him, and gets an access to encryption that uses the key, without knowing the key, thus generating the corresponding substring of the ciphertext. The attacker now needs to reconstruct the key, knowing encryption function, decryption function, substring of the plaintext and substring of the ciphertext, in order to read all future encrypted messages. And again, encryption and decryption functions are very complex. However, the attacker's ability to select substring of the plaintext has useful statistical or mathematical properties. In the Chosen Plaintext Attack, the attacker may use the useful properties of substring of the plaintext in order to implement the attack, as is the case with differential cryptanalysis. The difference is input as a parameter to the system and the system automatically generates a plaintext of that difference [5].

4.3 Brute force attack

All technique for breaking a cipher must be compared to a Brute Force Attack. The main idea in the Brute Force Attack is that all possible keys are trying to break the cipher. Practically every cipher is vulnerable to this attack type on the key, but the time for these attacks to be successful is unacceptable. Average at least half of the key space must be tried before the key is found. The goal of security through cryptography is not to keep a message secure forever, but to make the cost of breaking the cipher in terms of time so large that the data is worthless when found, or so costly in terms of computing resources that the gains from the intelligence are less than the cost expended for breaking it. This principle is known as a cipher being computationally secure [5].

4.4 Genetic algorithm for breaking transposition cipher

Brute Force attack has high computational complexity. In order to overcome this complexity, the Meta heuristic search techniques like Genetic Algorithm are used [4]. It consists of Initialize algorithm variables [4], [6]:

1. The maximum number of generations to consider.
2. The solution pool size.
3. And any other problem dependent variables.
4. Generation of an initial solution pool containing candidate solutions.
5. Using the current pool for number of generation iterations.

Then the genetic algorithm continues by selecting a pool from the current solution and pair parents. For each pair of parents it generates a pair of children using suitable crossover function and applies

a mutation operator. Then it evaluates the fitness function for each of the children and on the base of the fitness of each of the children and the fitness of each of solutions in the pool, it decides which solution will be placed in the new solution pool. Next, it replaces the current solution pool with the new one. And, in the end, it chooses the fittest solution of the final generation as the best solution. The technique to compare candidate key is next used in genetic attack. The main idea in this technique is to compare n-gram statistic of the decrypted message with those of the language [4]. General formula (1) is used to determine the suitability of a proposed key [4].

$$C^k = \beta \cdot \sum_{i,j \in A} |K_{(i,j)}^b - D_{(i,j)}^b| + \gamma \cdot \sum_{i,j,k \in A} |K_{(i,j,k)}^t - D_{(i,j,k)}^t| \quad (1)$$

Where A is the using language alphabet, K is known language statistics, D is decrypted message statistic, b is bigram statistics, t is trigram statistics. And the value of β and γ allows assigning of different weights to each of the two n-gram types.

The complexity of determining the fitness is $O(N^3)$ (where N is the alphabet size). To calculate the cost associated with the transposition cipher key the proposed key is used to decrypt the ciphertext and then the statistics of the decrypted message are then compared with statistics of the language. Improvement of this method is in using only subset of the most common bigrams and trigrams instead of using all possible bigrams and trigrams [4].

4.5 Genetic algorithm for attack on neural cryptography

Safety of the neural exchange protocol is based on the fact that two ANN (A, B) communicating with each other are synchronized faster than the third network (E) (attacker's) which is trained only to capture the input and outputs from the synchronizing ANN from the public channel. The attacker does not know the topology of the ANN and what output values are in the each hidden neuron so that the most of attacks are based only on estimate status of hidden neurons. There are four basic attacks: Simply attack, Geometric attack, Majority attack and Genetic attack.

In the genetic attack, the attacker starts with only one TPM but is permitted to use M TPMs. Because the most challenging issue in the mutual learning process is to predict the internal representation of either TPMA or TPMB, the genetic attack directly deals with this difficulty. For a specific value of oA/B , there are $2K-1$ different internal representations to reproduce this value. The genetic attack handles all these possibilities in a parallel fashion. The genetic attack proceeds as follows [7], [8]:

- If $\sigma^A = \sigma^B$ and E has at most $M/2^{K-1}$ TPMs, 2^{K-1} TPMs are generated and each updates its weights based on one of the possible internal representations. This step is known in genetic algorithms as the mutation step.
- If E has more than $M/2^{K-1}$ TPMs, the mutation step will be essentially an overhead due to the exponential storage needed. Therefore, the attacker must discard some of the TPMs to avoid exponential storage increase. As a genetic algorithm, the discarding procedure is based on removing the TPMs with the least fitting function. The algorithm uses two variables U and V as the fitting functions. The variable U represents the number of correct prediction of σ^A in the last V training steps.

And if $\sigma^A \neq \sigma^B$ the attacker's networks remain unchanged, because A and B do not update the weights in their tree parity machines.

5 GENETIC ALGORITHM FOR TRAINING

Next genetic algorithm can be used for training or designing artificial neural network. It has some advantages in comparison with classical learning methods. For example, backpropagation has some disadvantages.

First is the scaling problem. Backpropagation works well on the simple training problems. However as the problem complexity increases the performance of backpropagation falls off rapidly. Second drawback is to compute a gradient requires differentiability. Therefore backpropagation cannot handle discontinuous optimally criteria or discontinuous node transfer functions. This precludes its use on some common node types and simple optimality criteria [12].

Genetic algorithms should not have problem with scaling as backpropagation. One reason for this is that they generally improve the current best candidate monotonically. They do this by keeping the current best individual as part of their population while they search for better candidates. Secondly, genetic algorithms are generally not bothered by local minima. The mutation and crossover operators can step from a valley across a hill to an even lower valley with no more difficulty than descending directly into a valley [12].

Genetic algorithm is algorithm for optimization and learning based loosely on several features of biological evolution. It requires five components [12]:

1. A way of encoding solutions to the problem on chromosomes. The weights (and biases) in the neural network are encoded as a list of real numbers.
2. An evaluation function that returns a rating for each chromosome given to it. Assign the weights

on the chromosome to the links in a network of a given architecture, run the network over the training set of examples, and return the sum of the squares of the errors.

3. A way of initializing the population of chromosomes. The weights of the initial members of the population are chosen at random with a probability distribution. This is different from the initial probability distribution of the weights usually used in backpropagation, which is uniform distribution between -1 and 1.
4. Operators that may be applied to parents when they reproduce to alter their genetic composition. Included might be mutation, crossover (i.e. recombination of genetic material) and domain-specific operators.
5. Parameter settings for the algorithm, the operators and so forth. There are a number of parameters whose values can greatly influence the performance of the algorithm.

Given these five components a genetic algorithm operates according to the following steps [12]:

1. The population is initialized. The result of the initialization is a set of chromosomes.
2. Each member of the population is evaluated. Evaluations may be normalized and important thing is to preserve relative ranking of evaluations.
3. The population undergoes reproduction until a stopping criterion is met. Reproduction consists of a number of iterations. One or more parents are chosen to reproduce. Selection is stochastic, but the parents with the highest evaluations are favored in the selection. Then the operators are applied to the parents to produce children. And in the end, the children are evaluated and inserted into the population. In some versions of the genetic algorithm, the entire population is replaced in each cycle of reproduction. In others, only subsets of the population are replaced.

6 ADVANTAGES AND DISADVANTAGES OF GENETIC ALGORITHM

There are a lot of advantages and of course disadvantages of using genetic algorithm. The main pro is that it efficiently searches the whole model space in order to find global minimum. There is no needed linearization of the problem and no needed partial derivatives. So it needs only finite knowledge of the physical system. Genetic algorithm can help avoid a danger of trapping in local maximum or minimum and can be applied in wide variety of optimization problems [9], [10].

And most important cons are: there is no guaranty to find the best solution because sometimes there is a problem finding the exact global optimum. Next there is long time to evaluate the individuals, because

genetic algorithm requires large number of fitness function evaluations [9], [10].

7 CONCLUSION

The genetic algorithm can be very helpful for solution of some groups of problems. One of them is application in the cryptography. It is usually used in cryptanalysis, but it can be used for the random number generators or for training and designing artificial neural networks. The random number generator is a very important part of any cryptographic system and artificial neural network is used in cryptography, too. The main reason for using the genetic algorithm in cryptanalysis is its efficient search of the whole model space in order to find global minimum. There is no needed linearization of the problem and no needed partial derivatives. What is more, this ability increases suitability of training or designing of artificial neural networks.

References

- [1] GOYAT, S.: Cryptography Using Genetic Algorithms (GAs). In: *IOSR Journal of Computer Engineering (IOSRJCE)*, 1(5), pp. 06-08 Identification of Common Molecular Subsequences. *J. Mol. Biol.* 147, 195-197. 2012.
- [2] MISHRA, S., BALI, S.: Public key cryptography using genetic algorithm. In: *International Journal of Recent Technology and Engineering*, 2(2), pp. 150-154. 2013.
- [3] KHAN, F. U., BHATIA, S.: A novel approach to genetic algorithm based cryptography. In *International Journal of Research in Computer Science*, 2(3), pp. 7-10. 2012.
- [4] TOEMEH, R., ARUMUGAM, S.: Breaking Transposition Cipher with Genetic Algorithm. In: *Elektronika ir Elektrotechnika*, 79(7), pp. 75-78. 2015.
- [5] BROWN, J. A., HOUGHTEN, S., OMBUKI-BERMAN, B.: Genetic algorithm cryptanalysis of a substitution permutation network. In: *Computational Intelligence in Cyber Security*, 2009. CICS'09. IEEE Symposium on. pp. 115-121. 2009)
- [6] TOEMEH, R., ARUMUGAM, S.: Applying Genetic Algorithms for Searching Key-Space of Polyalphabetic Substitution Ciphers. In *Int. Arab J. Inf. Technol.*, 5(1), pp. 87-91. 2008.
- [7] RUTTOR, A., KINZEL, W., NAEH, R., & KANTER, I.: Genetic attack on neural cryptography. In: *Physical Review E*, 73(3), 036121. 2006.
- [8] PRABAKAN, N., VIVEKANANDAN, P.: A New Security on Neural Cryptography with Queries. In: *Int. J. of Advanced Networking and Applications*, Volume: 02, Issue: 01, pp. 437-444. 2010.
- [9] UZEL, Ö., KOC, E.: *Basics of Genetic Programming*. Doctoral dissertation, Dissertação (Mestrado) - Cankaya University. 2012.
- [10] SUMATHI, S., HAMSAPRIYA, T., SUREKHA, P.: *Evolutionary Intelligence: An Introduction to Theory and Applications with Matlab*. 1. edition. Springer, 2008. ISBN: 9783540751588.
- [11] DELMAN, B.: *Genetic algorithms in cryptography*. Thesis. Rochester Institute of Technology. Available at: <http://scholarworks.rit.edu/theses/5456>. 2004.
- [12] MONTANA, D. J., DAVIS, L.: Training Feedforward Neural Networks Using Genetic Algorithms. In: *Proceedings of the International Joint Conference on Artificial Intelligence*. San Francisco, Vol. 89, pp. 762-767. 1989.

Eng. Martin JAVUREK
ITC Department
Armed Forces Academy of General. M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: martin.javurek@aos.sk

Assoc. Prof. Eng. Marcel HAKAKAL, PhD.
Department of Informatics
Armed Forces Academy of General. M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: marcel.harakal@aos.sk

SECURITY IN MILITARY CLOUD COMPUTING APPLICATIONS

Miroslav ĎULÍK, Miroslav ĎULÍK Junior

Abstract: Cloud computing presents a significant technology trend not only in public sector but also in military sphere. It has become a smart solution for providing a flexible computing environment for military applications. This paper describes types of cloud computing models and cloud service model SPI (Software, Platform and Infrastructure). Consequently we describe the private cloud security model based on the private cloud reference model. This paper shows the security technologies and mechanisms for implementing security in private cloud applications, where the high levels of security is necessary and proper.

Keywords: Military Cloud, Private Cloud, Private Cloud Security Model, Security Technologies.

1 INTRODUCTION

Cloud computing is still an evolving technology paradigm. Its definitions, used cases, underlying technologies, issues, risks, and benefits will be refined in a spirited debate by the public and private sectors. These definitions, attributes, and characteristics will evolve and change over time. The cloud computing industry represents a large system of many models, vendors, and market niches. This definition attempts to encompass all of the various cloud approaches.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

2 ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING

The Cloud can provide the following security benefits:

- Centralized data storage.
- Segmented data/applications
- Better logging/accountability.
- Standardized images for asset deployment.
- Better resilience to attack & streamlined incident response.
- More streamlined audit and compliance.
- Better visibility to process.
- Faster deployment of applications, services, etc.

In [1] is defined cloud model, which is composed of essential characteristics, service models, and deployment models. For characterization of the basic principle cloud computing these characteristics are inherent:

- *On-demand self-service.* A consumer can be unilaterally provisioned computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

- *Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- *Rapid flexibility.* Capabilities can be flexible provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- *Measured service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

The existing computing paradigms e.g. Distributed computing, SOA (Service-Oriented Architecture), networking etc. are building blocks of cloud computing. There are numerous issues associated with these computing paradigms and some new challenges emerged from cloud computing are required to be addressed properly in order to realize the cloud to its full extent. Current cloud adoption is associated with numerous challenges.

In the next part we offer insight into challenges that organizations has to face with adopting cloud with a focus on what it means to face these challenges

and realize business opportunity once these challenges are understood and resolved [2].

- *Cost of Entry.* Implementing a cloud in the organization will require a significant entry cost to satisfy the needs of virtualization and the management layers that compose the fabric to deploy, operate, and monitor the environment. These costs must be realized in each step of the deployment process from prototyping to production. Over time these costs will turn to cost benefits as shared resource usage wins over traditional forms of resource allocation on a per application instance basis.
- *Data Location.* When discussing cloud computing, the challenge of data location within the cloud surfaces as an impediment to adoption. This is likely the prime reason that drives the private cloud deployment model into the discussion, because it alleviates the concern of placing enterprise data in the public cloud. In a private cloud deployment model, enterprise data remains in-house but due to the management characteristic of a private cloud the infrastructure required to satisfy data storage is largely commoditized.
- *Security.* Designing for a secure environment is always a challenge as new threats continue to emerge on a regular basis. In that sense this is not a new concern for cloud computing, but the attack surfaces and vectors are different in cloud computing and must be understood. Private clouds mitigate many of these attack surfaces since the entire operation is in-house, however organizational concerns still exist when meeting compliance requirements.
- *Compliance.* In any IT organization the goals of IT must be met while maintaining conformance to organizational and regulatory compliance requirements. This compliance will drive cloud computing deployment models and the management layers to establish and implement management boundaries for sensitive data storage and transmission throughout the cloud infrastructure.
- *Application Programming Models.* When considering cloud computing adoption within the organization, a challenge will likely surface around the existing application programming model and tools for development and test. This will drive an evaluation of the migration effort to move legacy application to the cloud and ongoing development of new applications for the cloud.

2.1 Cloud computing in military sphere

Cloud computing is based mainly on Internet (protocol TCP/IP) and offers cost reduction, flexibility, reliability, availability and energy-saving,

and these gain has become a solution for flexible computing applications.

Cloud technology has great utilization in military domain. Transitioning to cloud based solutions and services advances the military's long term objective to reduce cost ownership, operation and sustainment of hardware and other commoditized IT. Procuring these as services will allow the military to focus resources more effectively to meet evolving mission needs. Over time it will significantly boost IT operational efficiency, increase network security, improve interoperability with mission partners, and posture the military to adopt innovative technology more quickly at lower cost.

The importance of this trend for military is proved for example in USA DoD (Department of Defense) strategy "Cloud Computer Strategy" [3] issued in July 2012 and Army document "Army Cloud Computing Strategy", issued in March 2015 [4].

According to US Army researchers, this move will provide mobility, scalability, resource sharing, automation, and cost savings which will be available in diverse platforms. Previous command and control systems developed were usually using proprietary protocols thus it was very difficult to share data with the other organizations. Based on tactical cloud computing, new services can be developed using toolkits, software development kit, and a common framework which can be easily distributed and implemented.

This new development, various command and control systems can be interrelated thereby allowing seamless exchange of information via web services. These new systems must still comply with the security and standards guidelines.

Presents command and control systems send rare information to big data centres tens or hundreds of kilometers away. However, real time access is not very possible with limited network connectivity and low bandwidth. Thus, the modern military information systems (for example cloud placed directly on battlefield) with limited resources in tactical environments can still be flexible and robust, and similar to that of enterprise capabilities like inter-cloud federation, cloud integration with military communications, security, fault tolerance, load balancing, rapid provisioning, and resource management.

The military will continuously assess and weigh the potential benefits of various cloud deployment models against potential risks, such as:

- Increased technical complexity.
- System performance and outages.
- Competitive, congested and contested cyber electromagnetic environment.
- Data storage and information security.
- Changes in vulnerability attack vectors.
- Government data storage legal compliance.

2.2 Types of cloud computing deployment models

In cloud computing, we define cloud computing into two distinct sets of models:

- *Deployment Models:* This refers to the location and management of the cloud's infrastructure.
- *Service Models:* This consists of the particular types of services that user can access on a cloud computing platform.

There are four primary Deployment Models. A deployment model defines the purpose of the cloud and the nature of how the cloud is located [5]:

- *Private cloud.* The private cloud infrastructure is operated for the exclusive use of an organization. The cloud may be managed by that organization or a third party. Private clouds may be either on- or off-premises.
- *Community cloud.* A community cloud is one where the cloud has been organized to serve a common function or purpose. It may be for one organization or for several organizations, but they share common concerns such as their mission, policies, security, regulatory compliance needs, and so on. A community cloud may be managed by the constituent organization(s) or by a third party.
- *Public cloud.* The public cloud infrastructure is available for public use alternatively for a large industry group and is owned by an organization selling cloud services.
- *Hybrid cloud.* A hybrid cloud combines multiple clouds (private, community, or public) where these clouds retain their unique identities, but are bound together as a unit. A hybrid cloud may offer standardized or proprietary access to data and applications, as well as application portability.

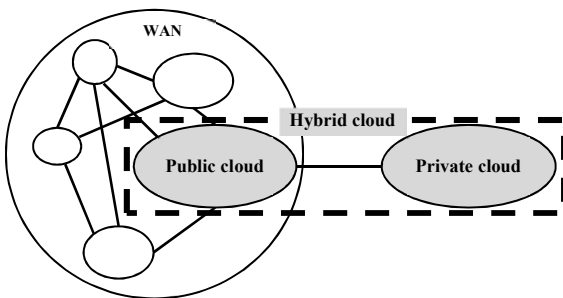


Fig. 1 Types of clouds
Source: [6]

Individuals typically use public clouds-such as those provided e.g. by Amazon.com, Google, and Apple. Large entities with vast amounts of sensitive data have turned to private, "secure" clouds. The most concerned users, current and future, are government agencies, especially the military, processing high sensitive data [7], [8].

Due to the special security needs of military applications cloud computing (e.g. CCC - Combat Cloud Computing [9], COMBAT – mobile-Cloud-based cCompute/communications infrastructure for BATtlefield applications [10]) desire to create a secure and reliable system is the most proper the private cloud version [11].

The main advantages of Private Cloud Computing [11]:

- Highly available, fault-tolerant architecture.
- Military grade datacenter security, hosted on multi-tiered private infrastructure.
- More secure than public, community or hybrid cloud offerings.

Concise comparison of public and private clouds:

Public cloud:

- Low investment hurdle;
- Negative loss and control over data;
- Higher risk of multi-tenancy data transfer.

Private cloud:

- High investment hurdle;
- IT organization (military) retains control over data;
- IT organization (military) control security technologies implementing.

3 PRIVATE CLOUD COMPUTING AND SECURITY

In private or hybrid cloud implementations, rather than remove the perimeter network altogether, it is possible place all other networks outside the perimeter into the untrusted zone. Figure 2 provides a conceptual representation of this change.

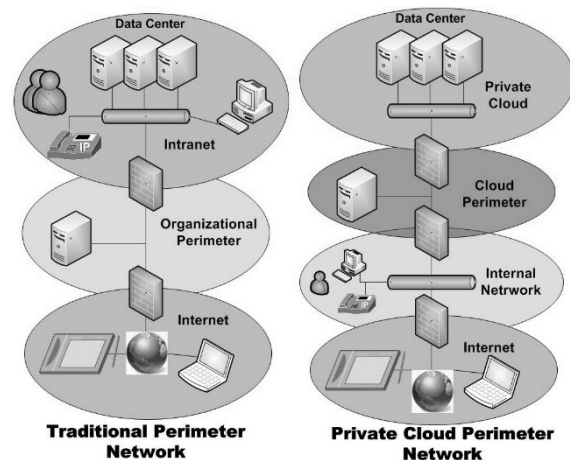


Fig. 2 Perimeter network in private cloud
Source: [12]

3.1 SPI model of cloud computing

The cloud provides options for approach, sourcing, and control. It delivers a well-defined set of services, which are perceived by the customers to have infinite capacity, continuous availability, increased agility, and improved cost efficiency. To achieve these attributes in their customers' minds, IT must shift its traditional server-centric approach to a service-centric approach. This implies that IT must go from deploying applications in silos with minimal leverage across environments to delivering applications on pre-determined standardized platforms with mutually agreed upon service levels.

A hybrid strategy that uses several cloud options at the same time will become the norm as organizations choose a mix of various cloud models to meet their specific needs.

Cloud options typically are categorized by the following SPI (Software, Platform and Infrastructure) service models [13]:

- *Cloud Software as a Service (SaaS)*. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based

email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- *Cloud Platform as a Service (PaaS)*. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- *Cloud Infrastructure as a Service (IaaS)*. The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer doesn't manage or control the underlying cloud infrastructure but has control over operating system, storages, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

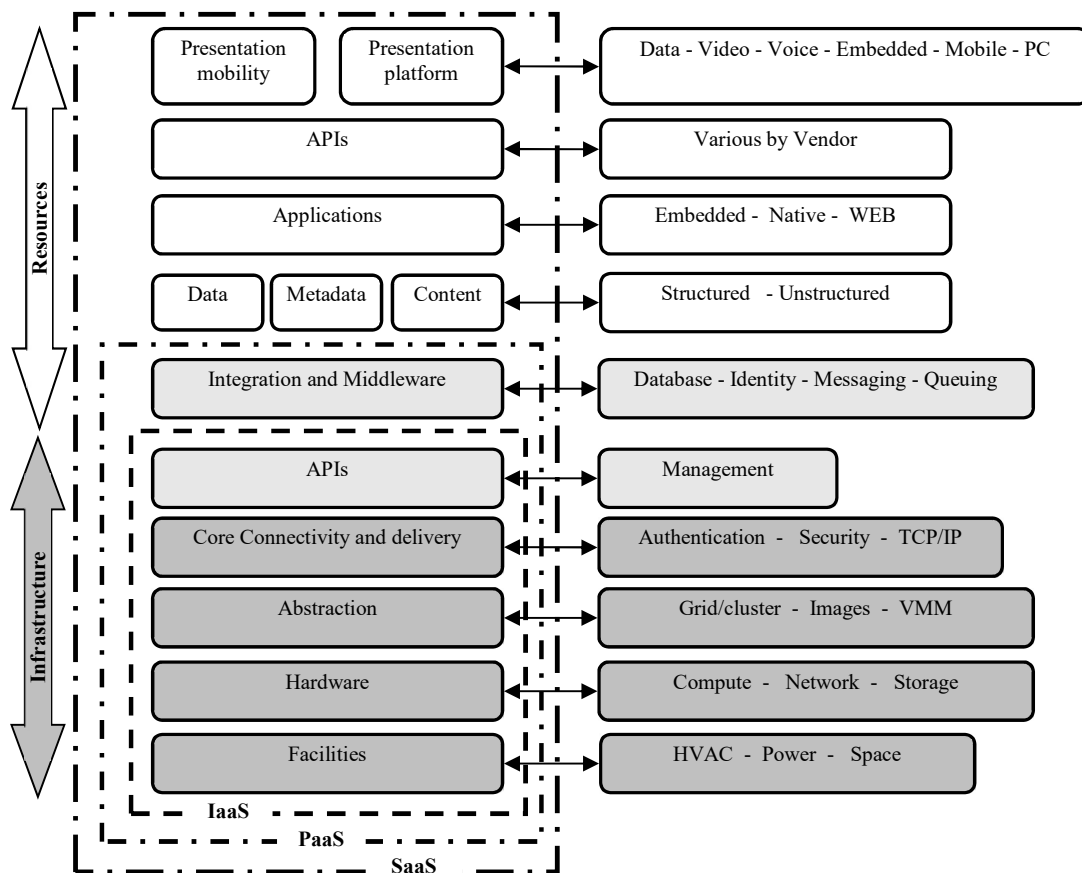


Fig. 3 Cloud computing service reference model and underlying cloud infrastructure

Source: [6]

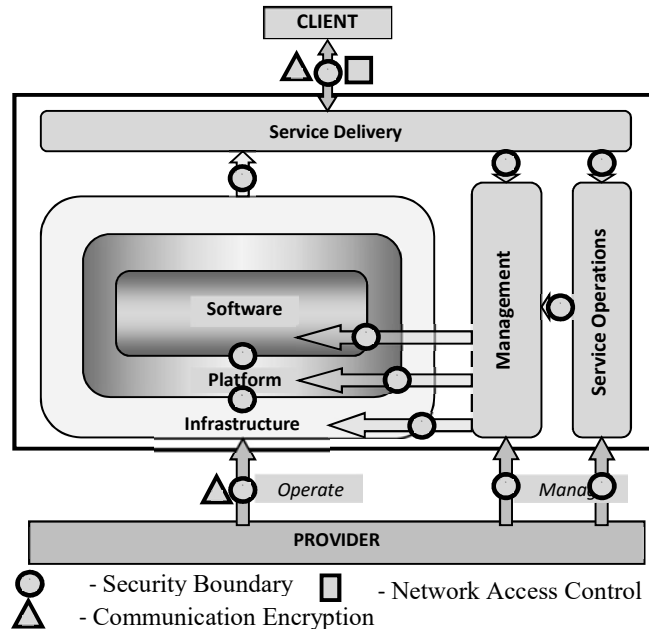


Fig. 4 The simplified private cloud security model and security components
Source: [14]

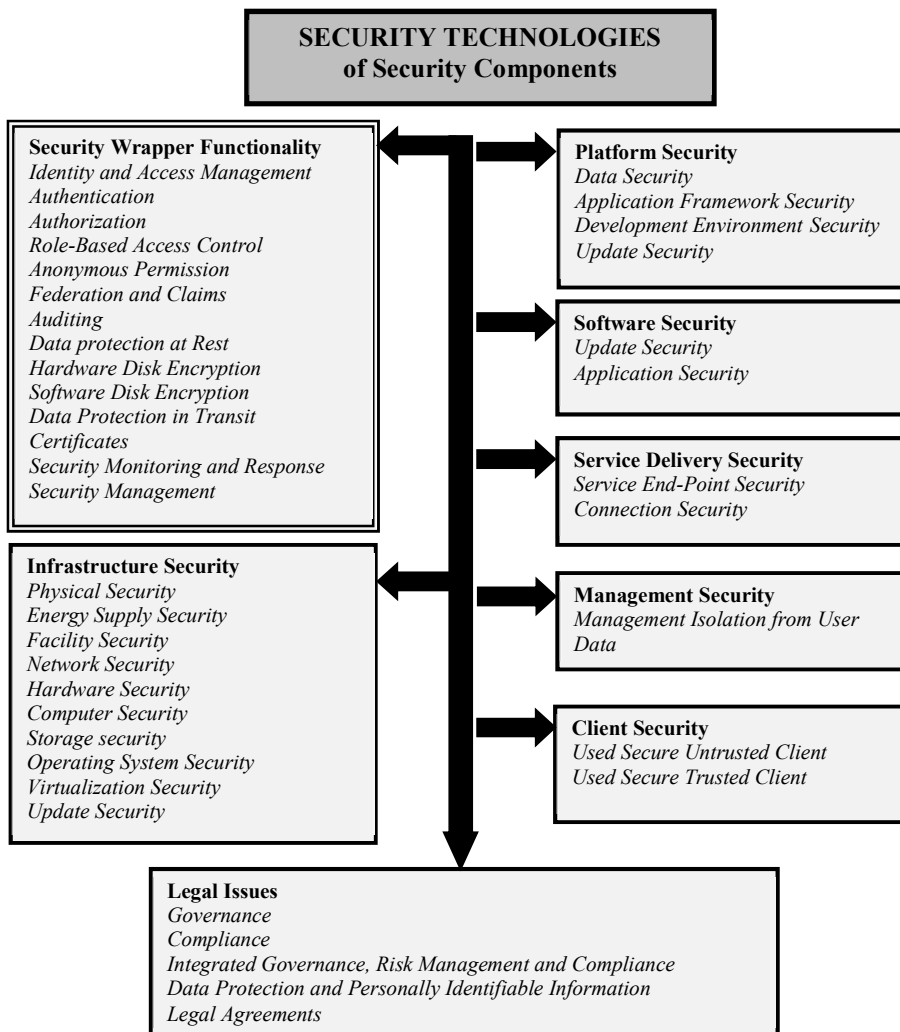


Fig. 5 Security technologies of security components in a private cloud security model
Source: authors.

It is useful to think of cloud computing service models in terms of a hardware/software stack. One such representation of the cloud reference model is shown in Fig. 3 [6]. At the bottom of the stack is the hardware or infrastructure that comprises the network elements. As we move upward in the stack, each service model inherits the capabilities of the service model beneath it. IaaS has the least levels of integrated functionality and the lowest levels of integration, whereas SaaS has the most.

3.2 The private cloud reference and security model

The private cloud security model uses the same design as the private cloud reference model but replaces the capabilities with mechanisms for implementing security. Fig. 4 shows how these relations between components relate in a concise

form [14]. To explain these relations in detail see Fig. 5. In addition to basic relations, this figure illustrates challenges, functions and underlying technologies to be implemented. To implement and verify security model, this figure could serve as a more detailed resource and list of required security features.

The next part of this paper presents this security model by considering each component of the private cloud reference model and analyzing the factors that apply at each layer and stack and includes the security components [14]:

- Infrastructure security.
- Platform security.
- Software security.
- Service delivery security.
- Management security.
- Client security.
- Legal issues.

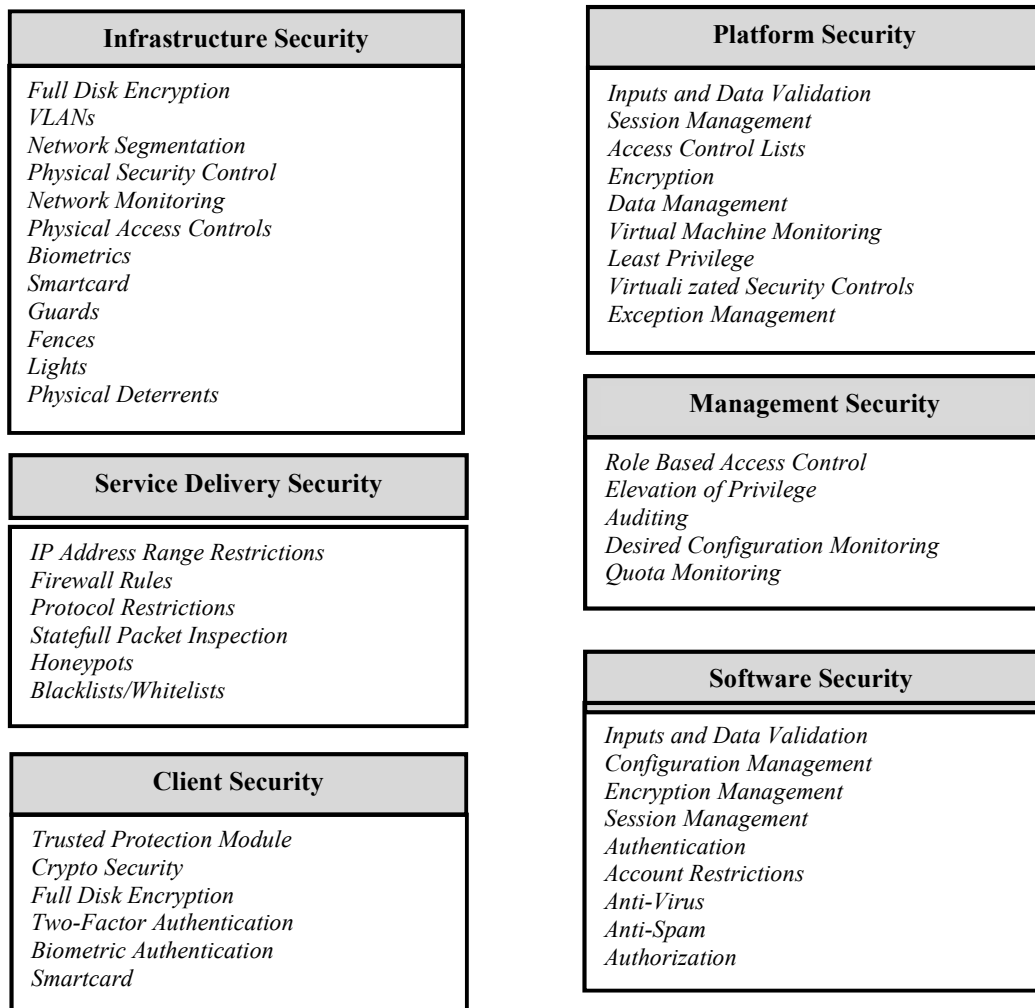


Fig. 6 Security mechanisms and services in security components of private cloud security model
 Source: authors.

Not only these challenges have to be solved. When implementing such a system, security must be resolved on several layers – from the hardware layer to end-user application layer. Security questions concern both client and server-side software, taking into account numerous threats regarding both inside and outside malicious attacks. To implement security on all layers, see Fig. 6 demonstrating all kinds of security measures, spanning from bottom to top layers, including hardware and software fields.

This section presents a wide spectrum of security issues that organization should consider for information security in private cloud, but it should not be considered exhaustive. More about cloud security threats and countermeasures is available in [15].

4 CLOUD COMPUTING SURVEY

Private Cloud-only strategies are in decline, and Hybrid Cloud is evolving and growing. But IT organizations still aren't sure what Hybrid Cloud means or how best to use it. Over the past 5 years, the focus of IT organizations has significantly shifted from Private Cloud strategies (-48.4%) to Hybrid Cloud (+19.2%) or Public Cloud (+43.3%) consumption models. IT organizations are looking to evolve beyond basic IaaS services (SDN – Software Defined Network, PaaS, DBaaS – Database-as-a-Service). As Public Cloud providers such as AWS, Azure and Google continue to add new services, more companies are beginning to experiment with emerging Cloud technologies such as SDN (23%), PaaS (52%) and DBaaS (38%). This highlights that IT organizations are being pushed by development teams to keep up with the pace of innovation in the Public Clouds [16].

Answer Options	2015 [%]	2014 [%]
IaaS Compute	66,9	30
IaaS Storage	66,6	40
PaaS	63,5	29
DBaaS	57,0	39
SDN	41,9	25
SaaS	77,5	61
None	5,1	-

Fig. 7 Cloud technologies and deployment in companies
Source: [16]

5 CONCLUSION

Based on previous studies and the definition of a private cloud, private clouds would seem to be more secure than public clouds because of infrastructure

design. It gives the organization more control over their policies and security. According to NIST, the internal private cloud is more suitable deployment models that offer an organization greater oversight and authority over security and privacy. Private cloud also better limits the types of tenants that share platform resources, reducing exposure in the event of a failure or configuration error in a control.

Private clouds are built for the exclusive use of one client, providing the highest control over data, security and quality of service. The company owns the infrastructure and has control over provided applications. Private clouds may be also deployed in an enterprise datacenter, or at a co-location facility.

References

- [1] MELL, P., GRANCE, T.: *The NIST Definition of Cloud Computing*. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-145. 7 p. Gaithersburg, Maryland : 2011, USA.
- [2] *Private Cloud – A Technical Perspective*. Available at: <https://technet.microsoft.com/en-us/cloud/hh147296.aspx>.
- [3] *Cloud Computing Strategy*. Department of Defense, Chief Information Officer, 44 p. DoD, USA, July 2012.
- [4] *Army Cloud Computing Strategy*. Office of the Army Chief Information Officer/G-6. U. S. Army. Version 1. March 2015. 40 p.
- [5] BADGER, L. et al.: *Cloud Computing Synopsis and Recommendations*. NIST Special Publication 800-146. 81 p. Maryland, USA : 2012.
- [6] SOSINSKY, B.: *Cloud Computing Bible*. Wiley Publishing, Inc., Indianapolis, USA : 2011. 531 p. ISBN 978-0-470-903356-8.
- [7] WILSON, J. R.: *The challenge of a secure military cloud*. November 14, 2013. Available at: <http://www.militaryaerospace.com/articles/print/volume-24/issue-11/technology-focus/the-challenge-of-a-secure-military-cloud.html>
- [8] FORIKA, K. T.: *Application of cloud computing in the defense industry: An academic and practical viewpoint*. AARMS, Vol. 11, No. 2, 2012. 12 p. Budapest, Hungary : National University of Public Service, 2012.
- [9] GOZTEPE, K., CEHRELI, I., SENSOY, S. E.: *A Decision Framework for Combat Cloud Computing Strategy*. 6th International Information Security & Cryptology Conference. Proceedings. 4 p. 20-21 September 2013, Ankara, Turkey.

- [10] SOYATA, T. et al.: *COMBAT: mobile-Cloud-based compute/communications infrastructure for Battlefield applications*. Proceedings of SPIE, vol. 8403-20, 13 p. Apr 2012, Baltimore, USA.
- [11] SIMMONDS, D., WAHAB, A.: *Public Cloud Computing vs. Private Cloud Computing: How Security Matters*. Research Paper. 14 p. Lawton, Oklahoma : Cameron University, 2012.
- [12] *Cloud security Challenges*. Microsoft, 2015. Available at: <http://social.technet.microsoft.com/wiki/contents/articles/6651.cloud-security-challenges.aspx>
- [13] *What is Infrastructure as a Service?* Microsoft, 2015. Available at: <http://social.technet.microsoft.com/wiki/contents/articles/4633.what-is-infrastructure-as-a-service.aspx>
- [14] *Private Cloud Security Model*. Microsoft, 2015. Available at: <http://social.technet.microsoft.com/wiki/contents/articles/6653.private-cloud-security-model.aspx>
- [15] MEIER, J. D.: *Cloud Security Threats and Countermeasures at a Glance*. Jul 2010. Available at: <http://blogs.msdn.com/jmeier/archive/2010/07/08/cloud-security-threats-and-countermeasures-at-a-glance.aspx>
- [16] *Insights from the 2015 Future of Cloud Computing Survey*. Available at: <http://wikibon.com/insights-from-the-2015-future-of-cloud-computing-survey/>

Eng. Miroslav ĎULÍK, PhD.
Department of Informatics
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: miroslav.dulik@aos.sk

Eng. Miroslav ĎULÍK, PhD. Junior
Faculty of Electrical Engineering
Institute of Aurel Stodola
University of Žilina
J. Nálepku 1390
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: dulik@lm.uniza.sk

EFFECTS OF WELL - KNOWN FORMS OF IMPROVISED EXPLOSIVE DEVICES USING HOME – MADE ANFO EXPLOSIVES

Lucia FIGULI, Zuzana ZVAKOVÁ, Vladimír KAVICKÝ, Štefan JANGL, Miroslava VANDLÍČKOVÁ

Abstract: The paper is focused on the research of effects of improvised explosive devices (in the form of suicide belt, vest, car etc.) using home-made ANFO (Ammonium Nitrate and Fuel Oil) explosives as a body of the IED. ANFO explosive is chosen due to its spread using in the terroristic attacks. Field test of ANFO explosives are described in the paper. The effect of such IED is compared with the IEDs made from the TNT explosives.

Keywords: Blast wave, ANFO explosives, improvised explosive devices, stand-off distances.

1 INTRODUCTION

Europe influenced by the refugee crisis due to the conflict in Syria, Iraq, Afghanistan, Yemen and the other gets to the political and security crisis in these days. European politicians cannot respond to the potential arrival of terrorists from the Islamic State, Al Qaeda and Al Nasr to Europe, their integration from the existing structures or to the manifestations of right-wing extremism, xenophobia and racism. All these factors create the conditions of the increased activity from the both sides of this very specific conflict that could lead to terroristic attacks. The largest group of technical means used in terrorist acts are firearms weapons and explosives respectively IEDs. While firearms are mainly obtained from illegal trade, much of explosives can be prepared with the available chemicals, commonly used in industrial and agricultural sectors.

Transport infrastructure is often chosen as a potential target of terrorist activities, mainly due to the large number of people who are predictably concentrated (time and space) to a certain place. Any organized terrorist = antisocial action has the potential to cause massive loss of life, health and property, but also to provoke a negative psychological effect on society. One of the most destructive action of terrorist groups is the using of improvised explosive device. Their consequences are often fatal and it is necessary to know the mechanisms of distribution and ways to protect against them, not only people but also objects of transport infrastructure.

2 EFFECTS OF WELL-KNOWN FORMS OF IMPROVISED EXPLOSIVE DEVICES ANFO EXPLOSIVES

2.1 ANFO EXPLOSIVES

ANFO explosive is a widely used explosive mixture. It can be prepared industrially or it can also be made at home very easily.

From the chemical-technological point of view it is possible to differentiate three different versions of ANFO explosives:

- ammonium nitrate + fuel,
- ammonium nitrate + fuel + powder metal (usually aluminium or magnesium) and
- ammonium nitrate + fuel + wooden powder - delaborated TNT.

ANFO explosives are very popular among the terrorists due to their simplicity of preparation. These types of explosives are very dangerous for the society. Prices of needed components are very low; the preparation does not require specialised knowledge and components for the preparation are freely available. Described explosives can be made by fertilizer based on ammonium nitrate used for agricultural purposes. Availability of fertilizers and oils (oil, fuel oil, kerosene) is not controlled. A malaxer for the production of chocolate or a concrete mixer can be used as mixing machines.

Attainability of means of domestic production of certain types of explosives, particularly ANFO explosives, puts to the foreground questions related with effects of explosions of known types of improvised explosive devices in case of this way made explosives as their filling. To find out what effect can be expected in the explosion of such improvised explosive devices, it is necessary to know the quantity of non-standard ANFO explosives contained in them.

2.2 Forms of improvised explosive devices











There is a group of the form of IED commonly used in terroristic attacks in the past. The list of the known types of improvised explosive devices and containing maximum amount of TNT explosive is in the Tab.1.

In the table there is presented the greatest amount of TNT that is able to place into such explosive system. The minimum distance from the building is the smallest distance which the building is constructed at, from common building materials capable to resist an explosion in such way so as the supporting structure not to be damaged. Minimum outdoors distance is the minimum distance that determines a level of injury and danger in an area where injuries happen caused by flying rubble,

shrapnel and loose building materials. Using TNT as an explosive body of IEDs is very improbable due to the restrictions of the EU. 95 % of the terroristic attacks is done using home-made ANFO explosives.

The paper is focused on the research for finding effects of well-known form of IEDs using ANFO explosives. For the defining of effects of such IEDs it is essential to know the characteristics of the home-made ANFO explosives (blast pressure, detonation velocity, density etc.). Consequently the ratio of efficiency both explosives could be set. The field test were done for the measurement of home-made ANFO explosives characteristics.

Tab. 1 Basic types of improvised explosive devices [4]

Type of improvised explosive device	Amount of explosive [kg]	Minimum distance from building ¹ [m]	Minimum outdoors distance [m]
 Tubular explosive	2,3	21	259
 Suicide belt	4,5	27	330
 Suicide vest	9	34	415
 Hand luggage/suitcase	23	46	564
 Vehicle type of coupé	227	98	457
 Vehicle type of sedan	454	122	534
 Vehicle type of microbus	1 814	195	838
 Delivery truck/Small truck	4 536	263	1 143
 Tank	13 608	375	1 982
 Truck with trailer	27 216	475	2 134

2.3 Field tests

The set of field tests took place at the development and testing set of the Ministry of Defence of the Slovak Republic called Military Technical and Testing Institute Zahorie. Methodology of the measurement is based on [3]. Maximum overpressure was measured using blast pressure sensors type 137A23 and 137A24 PCB Piezotronics. The explosive charge was positioned at a wooden base in the height of 1.6 m over the ground, i.e. in the height of human chest. Sensors were placed in the distances of 2, 5, 10 and 20 meters from the source (see Fig. 1).



Fig. 1 Blast sensors used in the field tests
Source: authors.

2.4 ANFO characteristics

The mixture of ANFO was made from GPN HD Ammonitrate 33.5 (composed of 33.5 % of ammonium nitrate - 16.7 % of nitric nitrogen and 16.8 % of ammoniacal nitrogen) and fuel oil Extra M2T (5 % of charge weight) (see Fig. 2) were used for the preparation of ANFO explosives for the blast tests.

Detonation characteristics used in the simulation, compared with standard TNT explosion, are in the Tab. 2.

Tab. 2 Detonation characteristics

Explosive	Explosive detonation velocity [m/s]	Density [g/cm ³]	Explosive pressure [GPa]
TNT	6800	1.58	18.4
ANFO	2872	0.9	6,14



Fig. 2 Ammonium nitrate used for the home-made ANFO and the form of charge
Source: authors.

2.5 Simulation of maximal blast wave

In our previous research work [2] there was mentioned the relationship for the analytical simulation for the overpressure setting in the distance R for $1 \leq Z \leq 10$ for ANFO explosives (Kavicky-Figuli model):

$$P_+ = \left(\frac{0,202}{Z} + \frac{0,224}{Z^2} + \frac{1,182}{Z^3} \right) 0,5e^{0,03R}; \quad (1)$$

2.6 Effects of IEDs using ANFO explosives

On the basis of the present relationship amount of non-standard ANFO explosives with similar effect as in the explosion of stated amount of TNT was found. It is necessary to pay attention on the volume placing explosives in the package. Using the volume of TNT contained in known forms of improvised explosive devices it was identified amount of abnormally produced 6 % ANFO explosives that can be placed in it (see Tab. 3).

The effects of the explosion of improvised explosive devices at using non-standard ANFO explosives 6 % are presented in the tab. 4. It was found out that they are describing the pressure generated by the explosion in the nearest way to the real values. The pressure at different distances from the point of explosion were calculated.

Figure 3 graphically shows the predicted distribution of pressure in the explosion of a tubular explosives, hand luggage and vehicle type coupe produced by using non-standard ANFO explosives.

The damage description arising from the explosion of explosives:

- The objects suffer from minor damage. It is characterized by varying degrees of glazing damage up to glazing breakage, by varying degrees of roof damage and thin walls, deformation and damage of the door and window hinges and frames, serious damage up to destruction of the light walls of porous

materials and formation of smaller damages in the structure of the objects.

- Medium-sized damage. It is characterized by damage of light structures, formation of cracks in brick walls, damage of the major bonds lining and severe damage of reinforced concrete ceiling panels.

Tab. 3 Basic types of improvised explosive devices and amount of non-standard 6 % ANFO explosives contained in them

Improvised explosive system	Amount of explosive TNT [kg]	Equivalent amount of ANFO 6 % [kg]	Max. amount of ANFO 6 % at compliance of improvised explosive devices volume [kg]
Tubular explosive	2,3	3,66	1,30
Suicide belt	4,5	7,20	2,57
Suicide vest	9	14,49	5,15
Hand luggage/suitcase	23	37,02	13,23
Vehicle type of coupé	227	365,36	130,01
Vehicle type of sedan	454	730,71	259,93
Vehicle type of microbus	1 814	2 919,64	1 038,50
Delivery truck/Small truck	4 536	7 300,71	2 596,68
Tank	13 608	21 902,13	7 790,04
Truck with trailer	27 216	43 804,25	15 580,07

Tab. 4 Basic types of improvised explosive devices and amount of non-standard 6 % ANFO explosives contained in them

Improvised explosive devices	Maximum amount of ANFO 6 [kg]	The distance from the explosion point [m]			
		2	5	10	20
		Pressure [kPa]			
Tubular explosive	1,30	140,48	31,59	15,4	4,9
Suicide belt	2,57	230,85	44,41	20,26	6,4
Suicide vest	5,15	398,54	65,07	27,25	8,29
Hand luggage/suitcase	13,23	882,9	116,6	42,29	24,04
Vehicle type of coupé	130,01	3645,82	658,7	159,4	66,51
Vehicle type of sedan	259,93	6236,26	989	260,63	96,13
Vehicle type of microbus	1 038,50	20496,52	2269,4	783,7	225,96
Delivery truck/Small truck	2 596,68	47789,9	4386,7	1115,6	436,85
Tank	7 790,04	136679,6	10731,65	2173,91	1053,39
Truck with trailer	15 580,07	268519,4	19758,48	3533,91	1912,9

Tab. 5 Nature of the damage caused by the pressure blast

Interval [kPa]	Damage extend
<0;0,5)	No damage
<0,5;5)	Little-sized damage
<5;20)	Medium-sized damage
<20;50)	Large-sized damage
<50;90)	Very large-sized damage
<90;150)	Very large-sized damage and total destruction
<150;3052)	Total destruction of objects

- Large-sized damage. It is characterized considerable damage of urban multistoried buildings, damage of internal light walls, falling of wooden telephone poles, disruption of steel frame of buildings and its separation from the ground, falling of non-bearing walls, serious damage of bearing elements of masonry structures and roof forfeitures, damage of unreinforced brick walls and overturning of loaded train wagons.
- Very large-sized damage. It is characterized by falling of less resistant stone, brick and wooden buildings and the collapse of a part of supporting elements of masonry structures, damage of the power supply and of light reinforced concrete buildings, damage of normal outer brick walls and severe damage of the walls and roofing of buildings consisting of reinforced concrete or steel skeleton and serious cracks in masonry buildings with massive brick walls.
- Very large-sized damage up to complete destruction of the objects. It is characterized by the damage of the reinforced concrete walls, puncturing of the block walls, building collapse with massive reinforced concrete and brick walls and complete destruction of masonry structures. Total destruction of buildings occurs, except of reinforced concrete special structures, concrete cracking appear and falling of the heavy wooden buildings occur.
- Total destruction of the objects appear. It is characterized by damage of reinforced concretespecial constructions and steel bridges, by severe damage up to the collapse of massive reinforced concrete structures and by perforation of concrete panels.

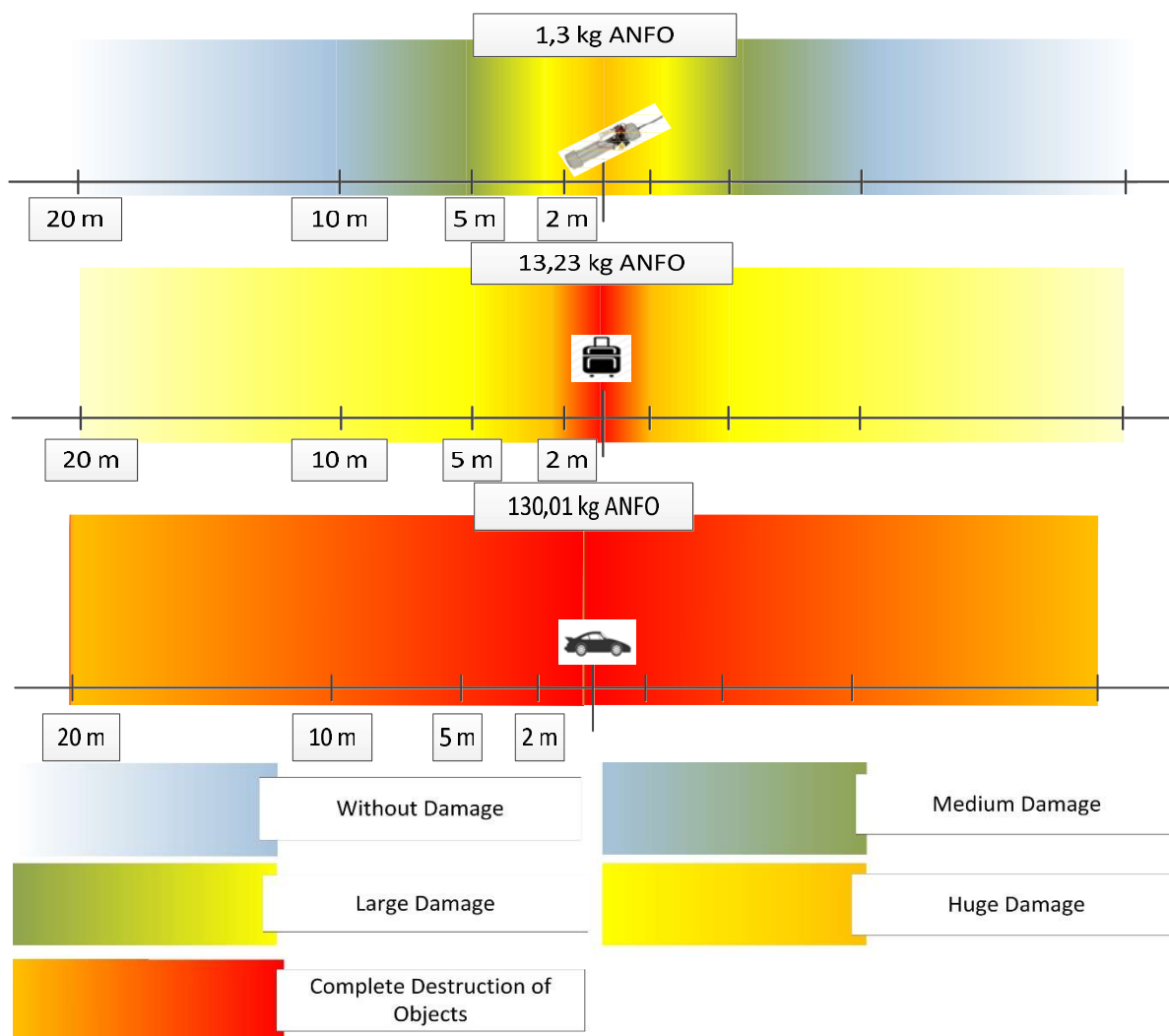


Fig. 3 Predicted distribution of pressure extension in the explosion of a tubular explosives, hand luggage and vehicle type of coupe produced by using non-standard ANFO explosives
Source: authors.

5 CONCLUSIONS

The presented research identified an amount of home-made ANFO 6 % explosives, which can be placed in known forms of improvised explosive devices. These explosive devices can be used in various anti-social activities, especially in organized crime and terrorist acts.

The explosion of tube bomb causes damage from small-scale to very large scales. It was found that just using a suicide belt, the second smallest known form of IED, the threshold of 150 kPa indicating the complete destruction of objects is surpassed at the distance of 2 meters from the explosion source. The scale of damage declines with the increasing distance from major damage to the medium ones at the distance of 20 m from the place of explosion. A similar situation also arises in the case of a suicide vest. In the case of placing explosives in hand

luggage, there would be the complete destruction of objects caused by an explosion at the distance of 2 m. Furthermore, the scale of damage would be reduced to very large damage at a distance of 20 m from the explosion source. In the case of placing IED in the car of type coupe and sedan, there will be occurred a complete destruction of the object at the distance of 10 m. IED in the other form of vehicles - van, light truck, tank truck and semi-trailer, the explosion would cause the complete destruction of objects up to a distance of 20 meters or more from the explosion source.

Based on these findings, it can be conclude that the known types of improvised explosive devices can be effectively used even if the explosive material used there will be home-made produced ANFO 6 %.

Acknowledgement

This work has been supported by VEGA grant No. 1/0240/15 named „Process model of critical infrastructure safety and protection in the transport sector“

Eng. Štefan JANGL, PhD.
University of Žilina
Faculty of Security Engineering
Univerzitná 8215/1
010 26 Žilina
Slovak Republic
E-mail: stefan.jangl@fbi.uniza.sk

References

- [1] JANGL, Š., KAVICKÝ, V.: *Ochrana pred účinkami výbuchov výbušnín a nástražných výbušných systémov*. Žilina : ŽU, 2012. str. 93-94. ISBN 978-80-9711108-0-2.
- [2] KAVICKÝ, V., FIGULI, L., JANGL, S., LIGASOVÁ, Z.: *Analysis of the field test results of ammonium nitrate: fuel oil explosives as improvised explosive device charges*. WIT Transactions on the Built Environment, Vol 141, pp 297-309, WIT Press, 2014.
- [3] ITOP 4-2-822: *Electronic Measurement of Airblast Overpressure and Impulse Noise*. 2000.
- [4] Available at: www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf

Eng. Miroslava VANDLÍČKOVÁ, PhD.
University of Žilina
Faculty of Security Engineering
Univerzitná 8215/1
010 26 Žilina
Slovak Republic
E-mail: miroslava.vandlickova@fbi.uniza.sk

Eng. Lucia FIGULI, PhD.
University of Žilina
Faculty of Security Engineering
Univerzitná 8215/1
010 26 Žilina
Slovak Republic
E-mail: lucia.figuli@fbi.uniza.sk

Eng. Zuzana ZVAKOVÁ, PhD.
University of Žilina
Faculty of Security Engineering
Univerzitná 8215/1
010 26 Žilina
Slovak Republic
E-mail: zuzana.zvakova@fbi.uniza.sk

Eng. Vladimír KAVICKÝ, PhD.
University of Žilina
Faculty of Security Engineering
Univerzitná 8215/1
010 26 Žilina
Slovak Republic
E-mail: kavickya@gmail.com

EVALUATION OF THE UNIFORM LINEAR MICROPHONE ARRAY FOR DETECTION SYSTEMS

Roman BEREŠÍK, Jozef PUTTERA, Jozef JURČO

Abstract: Array signal processing methods have been applied in many applications like radars, acoustic and seismic sensor systems. Beamforming, or spatial filtering, is a one of the essential array signal processing methods used for discrimination among different signals coming from different directions and increasing of the signal to noise ratio. The use of microphone arrays as a part of a multisensor system have restrictions in terms of a microphone array dimension, type of microphones, number of channels used for signal processing and also requirements for array signal processing algorithms. The paper deals with simulations of the uniform linear microphone array as a basic configuration of the sensor array for detection of events in monitored area. In conclusion, outcomes of simulations are evaluated and also further research in the field of sensor arrays and array signal processing is outlined.

Keywords: Uniform linear array, array response, acoustic sensor system.

1 INTRODUCTION

Array signal processing methods have been applied in many applications such as detection, identification, localization of events and enhancement of a signal to noise ratio of detected signals. Advances in sensor array technologies and availability of high performance digital signal processor systems allow utilizing of acoustic arrays in telecommunication systems and as systems for automatic speech recognition and speakers localization as well. The main drawback of the single microphone is that it captures not only the desired acoustic signal but also the certain level of noise. Furthermore, in many cases it is exposed to reverberation effect, which subsequently limits the effectiveness and performance of single channel noise suppression algorithms. In order to increase signal to noise ratio and limits reverberation effect, microphones are arranged into microphone arrays.

Multisensor systems as a part of Unattended Ground Sensor (UGS) systems [1], can consist of microphones [2], seismic [3], image and magnetic sensors arranged into sensor arrays. The target detection, classification and localization are main tasks fulfilled by UGS systems. Microphone arrays are able to provide a spatial and temporal sampling of wave-field and have an ability to resolve multiple point sources such as events in monitored area [4]. They can also be used in speech recognition systems to allow distant-talking interaction, acoustic echo cancellation and reduction, microphone-array hearing aids, joint audio-video signal processing for object localization and tracking [4]. The use of microphone arrays in military and security applications requires solving several problems. Firstly, signals which describe single events can be generated by variety of sources. From the military point of view, the most common sources of acoustic signals are persons [5], wheeled and tracked vehicles.

Sensors create part of perimeter protection systems [6] and they can also be involved in

information fusion process [7]. In contrast of seismic and image sensor systems, acoustic sensor systems formed by MEMS microphones and MEMS microphone arrays provide a dimension efficient way for design of UGS systems [2]. Several beamforming techniques can be applied in order to form the microphone array [4, 8]. Main parameters which define the beamforming method of a microphone array are the bandwidth of an acoustic signal and its character, the character of an area where the microphone array will be deployed and chosen tasks which will be fulfilled by sensor systems.

The presented paper is devoted to simulations of small size uniform linear microphone arrays where the dimension of the microphone array and the signal to noise ratio are main concern. We conclude this paper with the evaluation of simulation results and the further research in the field of microphone sensor arrays is outlined.

2 PROBLEM DESCRIPTION AND SIGNAL MODEL OF MICROPHONE ARRAY

In general, there are several microphone array geometries which can be used in military sensor systems. The most frequently used sensor array is a uniform linear array (ULA), where microphones are arranged into line with the same distance between adjacent microphones. Microphones can also create a uniform circular array (UCA), which is mainly used for acoustic signal localization. Above mentioned array geometries are widely used in systems deployed on the ground surface in parallel way with a horizontal plane. Some applications, like acoustic antennas, require arranging of sensors into an equispaced rectangular grid.

In the most of beamforming applications, two assumptions simplify the analysis of microphone arrays:

1. Signals are narrowband.
2. Signal sources are located in such a distance that the far-field assumption is valid for particular situations.

In spite of the fact that the far-field assumption is valid for most of security and military applications, the assumption that signals are narrowband is never valid [4]. The Fig. 1 shows the typical time, frequency and time-frequency representation of the broadband acoustic signal generated by a moving vehicle. The amount of the acoustic signal power can be identified in the frequency span between 60-1200 Hz [9]. The detection of events base on acoustic signatures generated by movement of a vehicle is a specific problem, because signal signatures have a specific character in terms of amplitude and frequency characteristics.

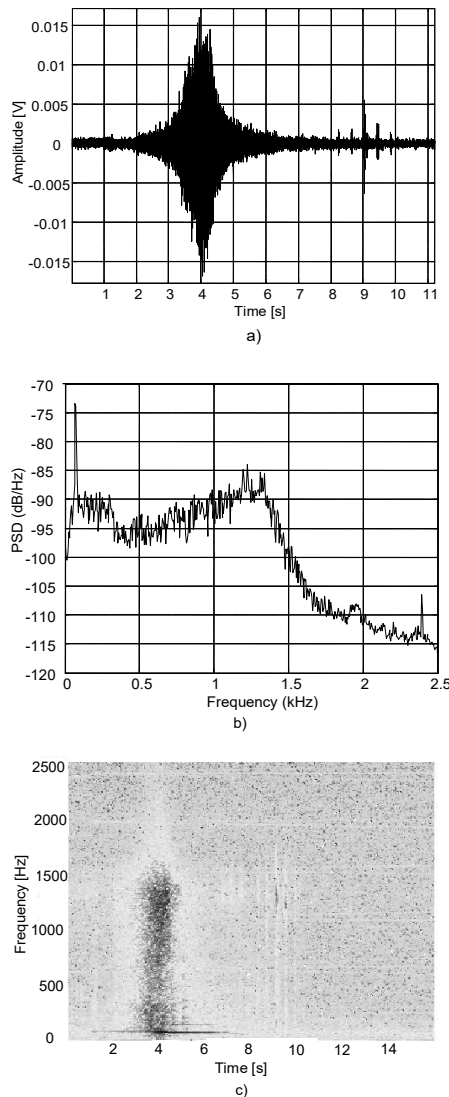


Fig. 1 Time (a), frequency (b) and time-frequency (c) representation of the acoustic signal generated by the moving vehicle
Source: authors.

Similarly, the Fig. 2 shows the time, frequency and time-frequency representation of the acoustic signal recording of a small charge explosion at the distance of 200 m from the position of microphone. This acoustic event can be characterized as broadband signal as well, with main frequency components located in the frequency span between 70-1800 Hz [12]. From the Fig. 1 and Fig. 2 also imply that the main portion of the acoustic signal power, which described the event, is concentrated in the frequency band from 60 Hz to 100 Hz with the power spectral density (PSD) equal to -73 dB/Hz (Fig. 1b) and -68 dB/Hz (Fig. 2b). There are also additional frequency components, which can be used not only for detection purposes but also for classification of events, located in frequency span between 1 kHz to 1.5 kHz. However, these frequency components have significantly lower PSD (from 15 to 20 dB/Hz) in comparison of frequency components mentioned in previous case.

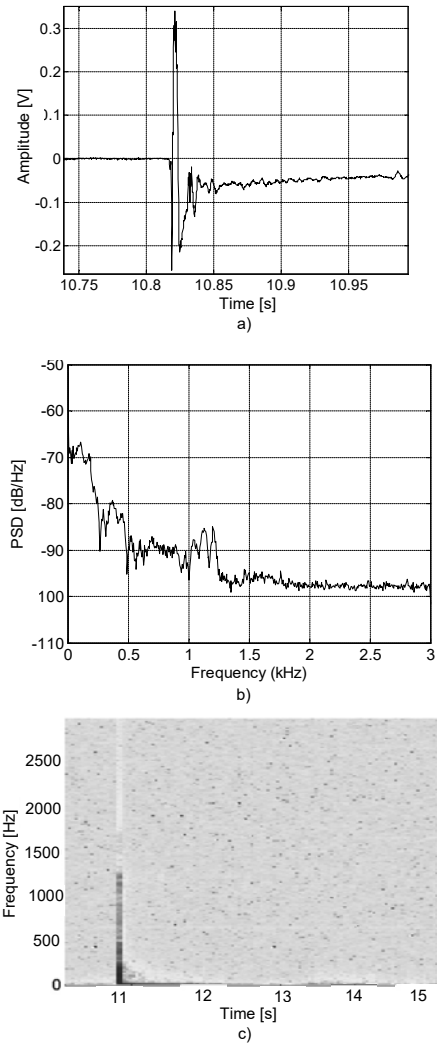


Fig. 2 Time (a), frequency (b) and time-frequency (c) representation of the small charge explosion
Source: authors.

In many cases, it is not main concern to determine the direction of acoustic signal arrival, but it is required to enhance the signal to noise ratio (SNR) of incoming signal from the specific sector and subsequently to increase the probability of event detection and its classification. The design of microphone array and subsequent application of signal processing algorithms can provide the solution for these problems. The type of microphone array pattern, among other things, depends on the end-user application, parameters of signals and the hardware configuration of digital signal processing means. There is also concern to keep the configuration of the acoustic sensor system as simple as it is possible.

There are three major research areas for array signal processing [9]:

1. Detecting the presence of an impinging signal and determine the signal numbers.
2. Finding the direction of arrival angles of the impinging signals.
3. Enhancing the signal of interest coming from known/unknown direction and suppress the interfering signals.

As it was mentioned previously, the primary purpose of simulations is to analyze small-aperture microphone array which consists of up to four microphones. The Fig. 3 represents possible scenario of microphone arrays utilization when detection of acoustic signatures of events is primary task.

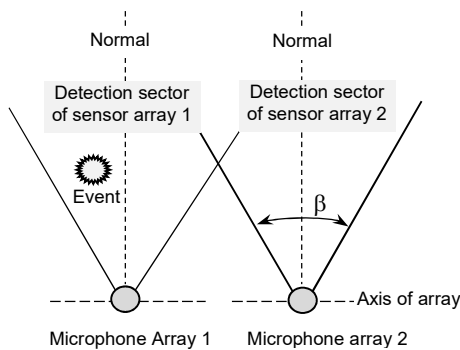


Fig. 3 Typical scenario of sensor array deployment
Source: authors.

This scenario represents placement of two adjacent microphone arrays with overlapped coverage sectors defined by angle β (for example, up to 75°) and the axis of the array heading to the direction of interest (Fig. 3, Normal).

In general, the beamforming is the process when the sensor beam pattern is focused to desired direction, so signals from this direction overlap constructively. As a basis for simulations, the ULA

of microphones was selected. In spite of the fact that the ULA is not appropriate choice for applications where signals have a wideband character, since the directivity of ULA is strongly frequency dependent, the primary concern of simulations was to determine limitations of the small-aperture ULA regarding to its use for detection purposes. The basic configuration of ULA is shown in Fig. 4. Acoustic signals which characterize certain events (i.e. vehicle movement) are mostly positioned in area perpendicular to the microphone array axis y shown in Fig. 4. The microphone array geometry displayed in signal model (Fig. 4), is called the broadside linear microphone array.

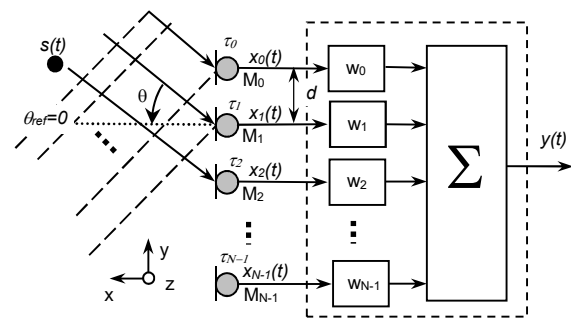


Fig. 4 Signal model of the beamforming process
Source: authors [similar in 4].

There are assumptions related to signal model of the microphone sensor array:

- All sensors exhibit same characteristics in terms of the magnitude and phase.
- All sensors in sensor array are assumed to be point-like.
- Far-field assumption is valid for microphone sensor array.

The angle of incidence (θ) is measured with the respect to the normal of the array aperture (Fig. 3 and 4). The signal model shown in Fig. 4 assumes, that the one sample of the discrete input sequence $x(t)$ at each microphone consists of the delayed (τ_i) and attenuated (a_i) version of the desired signal $s(t)$. The given situation can be described by equation [4],

$$x_i(t) = a_i s(t - \tau_i) + v_i(t), i = 0 \dots N - 1, \quad (1)$$

where N denotes the number of microphones integrated into microphone array and v_i denote a noise component with arbitrary spatial statistics. The signal model can also be expressed as follows

$$\begin{pmatrix} x_0(t) \\ x_1(t) \\ x_2(t) \\ \vdots \\ x_{N-1}(t) \end{pmatrix} = \begin{pmatrix} a_0 s(t-\tau_0) \\ a_1 s(t-\tau_1) \\ a_2 s(t-\tau_2) \\ \vdots \\ a_{N-1} s(t-\tau_{N-1}) \end{pmatrix} + \begin{pmatrix} v_0(t) \\ v_1(t) \\ v_2(t) \\ \vdots \\ v_{N-1}(t) \end{pmatrix}, \quad (2)$$

Subsequently, we assumed that neither noise component (v_i) nor additional interferences are present in the model shown in Fig. 4 and described by equation (1). It is also assumed that the value of attenuation (a_i) is also omitted, therefore the output signal of each microphone is equal to the component of the source signal $s(t-\tau_i)$ captured by single microphones M_i . All captured waves can be summed and this process is expressed by following equation

$$y(t) = \sum_{i=0}^{N-1} x_i(t) w_i^* = \sum_{i=0}^{N-1} s(t-\tau_i) w_i^*, \quad (3)$$

The delay of signal for the single signal component is given by

$$\tau_i = \frac{d_i \sin \theta}{c}, \quad (4)$$

where c denotes the speed of the sound, θ is the angle of the acoustic signal arrival and d_i is spacing between two adjacent microphones. The weight vector for the microphone array holds complex conjugate coefficients of sensors, given by [10],

$$w_i = [w_0 \ w_1 \ w_2 \ \dots \ w_{N-1}]^T. \quad (5)$$

For simulations of the small-aperture ULA, following assumptions were considered. The output signal is given by equation (3) and for data-independent operations the weights are chosen as scalar given by,

$$w_i = \frac{1}{N}, \quad (6)$$

The corresponding directivity pattern for the linear equally spaced array of identical microphones is given by [11],

$$D(f, \theta) = \sum_{i=1}^N w_i(f) e^{j(i-1) \frac{2\pi f}{c} d \sin \theta - \Psi}, \quad (7)$$

where Ψ is the initial phase difference of signals at two adjacent microphones. The following equation expresses a sound capture model of microphone array

$$D_i(f, \theta) = e^{j(i-1) \frac{2\pi f}{c} d \sin \theta - \Psi}, \quad (8)$$

Applying the equation (6) to (7) we get the following equation

$$D(f, \theta) = \frac{1}{N} \sum_{i=1}^N (f) e^{j(i-1) \frac{2\pi f}{c} d \sin \theta - \Psi}, \quad (9)$$

From the equation (9) implies that the directivity pattern depends upon:

1. The number of array elements N .
2. The inter-element spacing d .
3. The frequency f .

A design of microphone arrays has to consider the problem of spatial aliasing when for a single sensor pair; the resulting delay is identical for two or more directions for given frequency. For this reason the distance between two microphones of the sensor pair is given by,

$$d = \alpha \frac{\lambda_{\min}}{2}, \quad (10)$$

where λ_{\min} is the minimal wave length of the acoustic signal and the coefficient α is equal to $\alpha \leq 1$. The directivity pattern as one of the microphone array characteristics is shown in Fig. 5.

In order to analyze performance of the microphone array, several parameters can be used:

1. Bandwidth (B), which is described as region of the main-lobe where the signal is decreased by 3 dB.
2. Relative side-lobe level, which can be described as relative height of the first side-lobe with the respect to the main-lobe.
3. Peak-to-zero distance is described as the region from the maximum of the main-lobe to its first minimum [8].

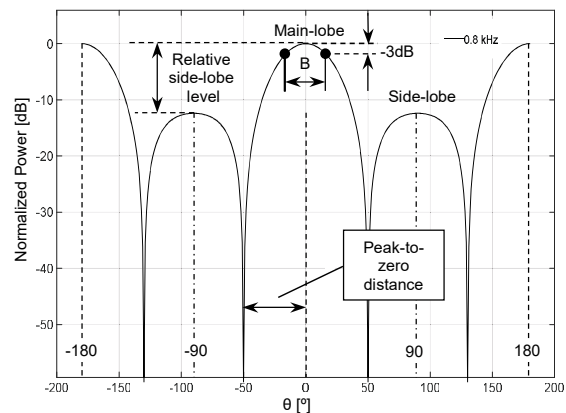


Fig. 5 Directivity pattern of ULA with $N=4$ at the frequency of 800 Hz and $d=0.139$ m

Source: authors.

As it was mentioned above, these parameters are function of the number of microphones, frequency and microphone array geometry.

Following assumptions were given for our simulations:

1. The steering direction of ULA is equal 0° .
2. The ULA consists of 2, 3 and 4 microphones placed symmetrically around axis y and with steering direction aligned with the axis x (Fig. 6).
3. The inter-element spacing of ULA is given by (10).

3 RESULTS OF SIMULATIONS

An important quantity describing a performance of the microphone array and beamformer is the directivity pattern of ULA (sometimes called beam pattern, Fig. 5). It quantifies the spatial selectivity of a beamformer with the respect to the plane-wave impinging from the direction θ at given frequency. Additionally, there is another quantity describing the performance of the microphone array called the array response (Fig. 7a, 8a and 9a), which uses same parameters as directivity pattern. However, the array response also describes effects of the varying frequency on the beamformer response. It can be described as a sum of the steering direction absolute values for each frequency component and the direction.

Properties of microphone arrays were evaluated for the frequency range from 20 to 1200 Hz with the frequency step of 20 Hz and angles in range of $-180^\circ \leq \theta \leq +180^\circ$ (Fig. 7c, 8c, 9c) and $-90^\circ \leq \theta \leq +90^\circ$ (Fig. 7a, 7b, 8a, 8b, 9a, 9b) with step of 3° . The maximum frequency of the signal used for simulations was chosen according to the frequency band of the recorded acoustic signal generated by the moving vehicle (Fig. 1) during the experiments described in [8]. The arrangement of ULAs used for simulations is expressed by Fig. 6. The microphones of the simulated ULA are equally spaced at inter-element distance equal to 0.139 m (Fig. 4, Fig. 6). The Fig. 7, 8 and 9 illustrate the directivity pattern and the array response of simulated ULAs.

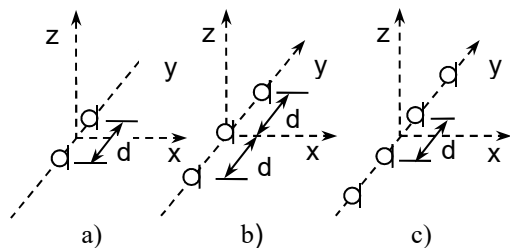


Fig. 6 Arrangement of ULA which consists of even (a, c) and odd number of microphones (b)

Source: authors.

The Fig. 7 represents performance characteristics of ULA which consists of two microphones. The main lobe of the array response has a bandwidth equal to 62° (at the frequency of 1200 Hz) and the maximum gain of the main lobe is equal to 2.98 dB. Neither side lobes nor gratings lobes can be observed in the array response shown on Fig. 7a, c. By decreasing the frequency, the bandwidth of directivity pattern becomes wider and the gain decreases too. This situation can be clearly seen in array response shown on Fig. 7a and Fig. 7c, which represents distribution of the normalized power as a function of the angle θ at frequencies equal to 400 Hz, 800 Hz and 1200 Hz. The bandwidth and gain of two-microphone ULA for given frequencies are shown in Tab. 1.

Tab. 1 Bandwidth and gain of two-microphone ULA at specific frequencies

	Frequency [Hz]		
	400	800	1200
B [°]	-	100	62
Gain [dB]	0.377	1.45	2.98

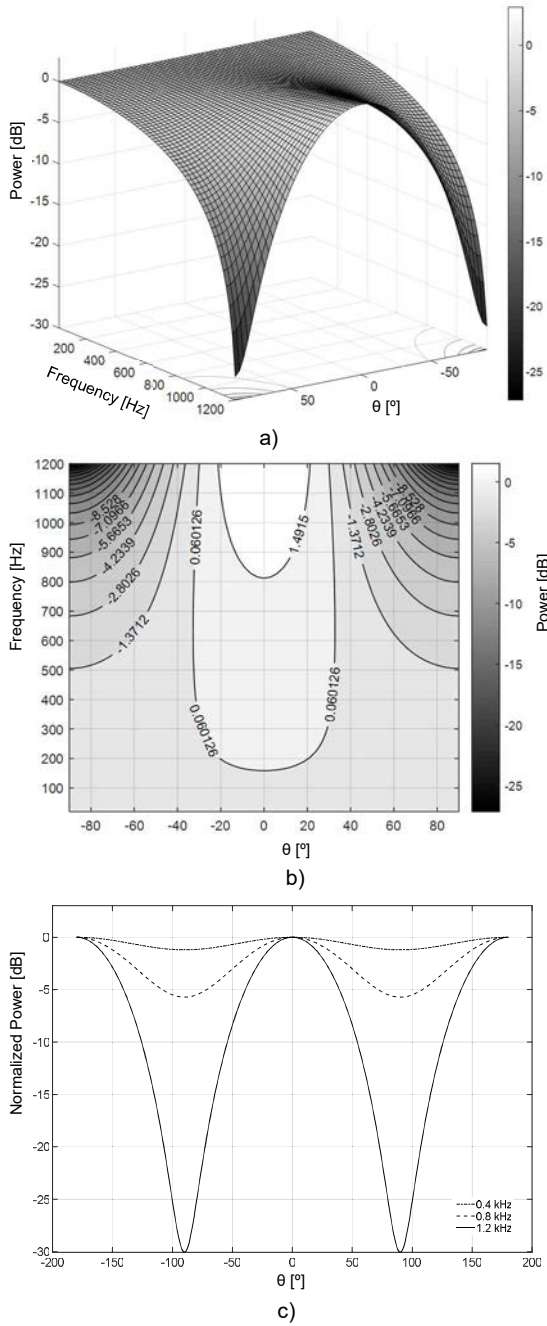
The bandwidth of two-microphone ULA at the frequency 400 Hz cannot be determined due to the fact that the directivity pattern of the microphone array nears to directivity pattern of the omnidirectional microphone. In the frequency range below 40 Hz, ULA characteristics are same as omnidirectional microphone ones.

Fig. 8 represents performance characteristics of ULA which is comprised of three microphones.

The array response exhibits main lobe with the bandwidth equal to 38° and gain of 4.71 dB at the frequency of 1200 Hz. In contrast to the two-microphone ULA (Fig. 7), side lobes appear at angles equal to $\pm 90^\circ$ and the frequency of 1200 Hz (Fig. 8c). Similarly, the performance of the three-microphone ULA at given frequency range can be analyzed base on array response shown on Fig. 8a and Fig. 8c. The Fig. 8c represents the distribution of normalized power as a function of the angle θ at frequencies equal to 400 Hz, 800 Hz and 1200 Hz.

The bandwidth and gain of three-microphone ULA beam pattern for particular frequencies are shown in Tab. 2. The Fig. 9 displays performance characteristics of ULA with four microphones linearly spaced along the y axis.

From the Fig. 9 implies that by adding another microphone to the sensor array, the bandwidth of the main lobe is decreased to 28° (at the frequency of 1200 Hz) (Fig. 9a, 9c), which improves spatial selectivity of simulated ULA.



Tab. 2 Bandwidth and gain of three-microphone ULA at specific frequencies

	Frequency [Hz]		
	400	800	1200
B [°]	148	58	38
Gain [dB]	0.9	3.1	4.71

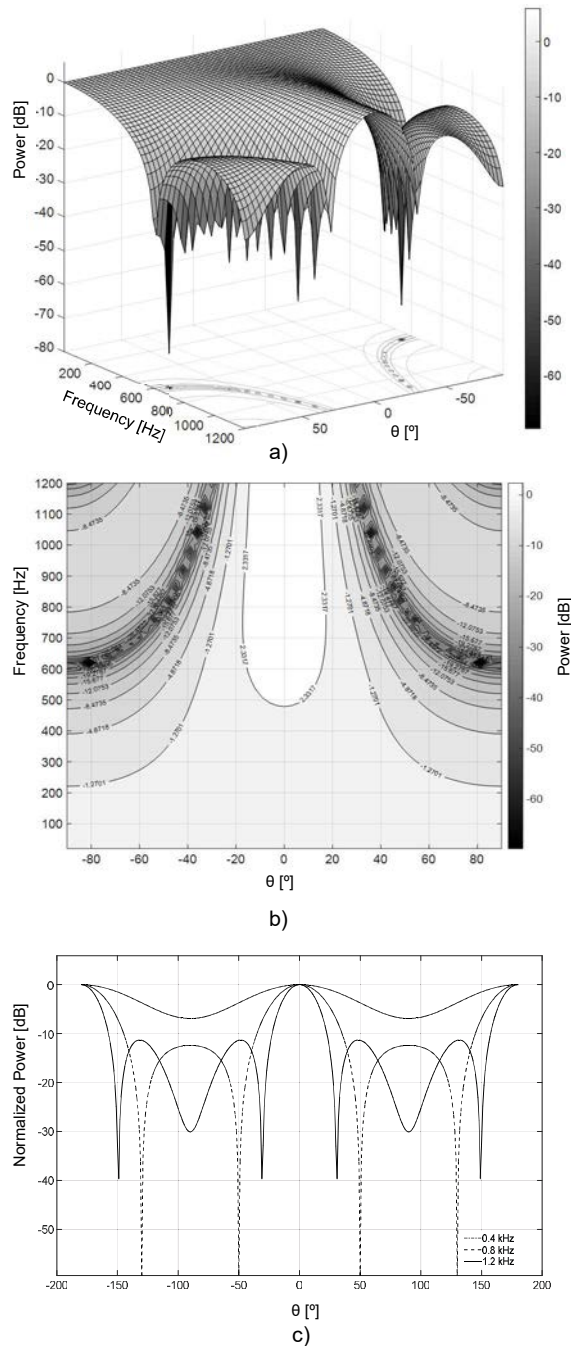


Fig. 9 Microphone array response (a) and directivity pattern (b, c) of four-microphone ULA with $d=0.139$ m
Source: authors.

The maximum gain, given by main lobe, is equal to 5.93 dB which is about 1.22 dB higher than the gain of three-microphone ULA (Fig. 8a). The bandwidth and gain of four-microphone ULA beam pattern for particular frequencies are shown in Tab. 3.

Tab. 3 Bandwidths and gain of the four-microphone ULA at specific frequencies

	Frequency [Hz]		
	400	800	1200
B [°]	90	42	28
Gain [dB]	1.72	4.44	5.93

From the Fig. 7, 8, 9 imply that by increasing number of microphones without changing the inter-spacing distance between neighboring microphone elements, the microphone array performance is better in higher frequency range in terms of the spatial selectivity. It is proved by the comparison of two, three and four-microphone ULA main lobe bandwidths (Tab. 1, 2, and 3). A minimum configuration of the microphone array requires two microphones. The maximum gain of ULA with this configuration is about 2.98 dB at the frequency of 1200 Hz. On the one hand, by adding additional two microphones to the ULA (four-microphone ULA) the gain is doubled and base on simulation results it is equal to 5.93 dB. On the other hand, better spatial selectivity and higher gain of ULA will cause that higher number of microphone arrays will be required for covering of monitored area in comparison to two-microphone ULA (Fig. 3).

As it was mentioned above, simulations were made for the microphone array with the inter-element spacing d equal to 0.139 m. The dimension of simulated microphone arrays for the specific number of microphones is summarized in Tab. 4.

Tab. 4 Dimensions of simulated ULAs with $d=0.139$ m

	Number of microphones		
	2	3	4
Dimension of ULA [m]	0.139	0.278	0.417

Modern trends in design of acoustic sensor systems used in military and security applications show that these systems become portable and easily deployable in real environment. Typical example is, when microphone array is integrated into sensor node as a part of the wireless sensor network. The dimension of the sensor node is usually several centimeters; therefore the dimension of microphone array can be critical. In order to evaluate the properties of ULAs with inter-spacing dimension d reduced to $\lambda/4$ ($d=0.07$ m with $\alpha=0.5$), several simulations were performed. The results of simulations for two, three

and four-microphone ULA are shown in Fig. 10. The decreasing of inter-spacing dimension between two adjacent microphones makes microphone arrays more compact in terms of the total dimension. However, this modification also decreases the gain and spatial selectivity of microphone ULAs. When the higher SNR of detected signal is required, the minimization of the ULA dimension is not applicable.

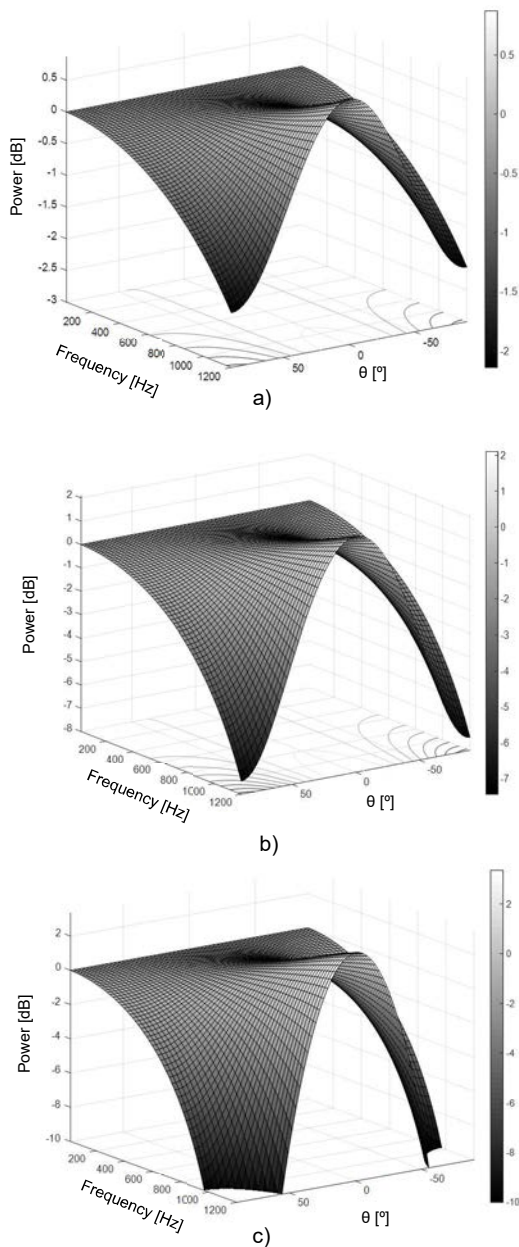


Fig. 10 Microphone array response of two-microphone ULA (a), three-microphone ULA (b) and four-microphone ULA (c, enlarged part) with $d=0.07$ m
Source: authors.

The following table (Tab. 5) represents comparison of two, three and four-microphone ULAs in terms of the bandwidth and gain.

There is another fact which should be taken into account. When beamforming method is applied to the uniform linear arrays, the sensor array forms two main lobes.

Tab. 5 Bandwidths and gain of two, three and four-microphone ULA with $d=0.07$ m, $f=1200$ Hz

	Number of microphones		
	2	3	4
B [°]	172	72	54
Gain [dB]	0.87	2.1	3.35

The first main lobe can be observed on steering direction equal to $\theta=0^\circ$ and the second main lobe on angle $\theta=180^\circ$. The first main lobe is a product of the constructive overlapping of incoming waves from the direction of interest (in our case $\theta=0^\circ$). The second main lobe occurs due to the front-back ambiguity. This fact can cause problem when localization of event is vital. The front-back ambiguity can be ignored in the case that the acoustic sensor system is deployed as early warning detection system in monitored area when each detected event is considered as signature of threat.

4 CONCLUSION

The outcomes of simulations show that when the number of microphones is doubled the bandwidth of the main lobe is decreased twice. This situation is valid for ULAs which comprise of two and four microphones. When the higher spatial selectivity for the better spatial separation of acoustic signal sources is required, the high number of microphones has to be used. The disadvantage of increasing of the microphones number is that higher numbers of side lobes can be presented in array response. Moreover, it causes increasing of the sensor array size which can complicate the design of portable UGS systems. The outcomes of simulations also show that there are no grating lobes, which can cause the false identification of the direction of arrival of acoustic signals. Future experiments will be focused on simulations of non-uniform arrays and also differential acoustic arrays in order to explore possible advantages for their implementation in military and security applications.

References

- [1] PAKHAMOV, A., GOLDBURT, T.: Seismic Systems for Unconventional Target Detection and Identification. In: *Sensors, and Command, Control, Communication, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense V*, Proceedings of SPIE, vol. 6201, 2006.
- [2] ZHANG, X., HANG, J., SONG, E., LIU, H., LI, B., YUAN, X.: Design of Small MEMS Microphone Array Systems for Direction Finding of Outdoors Moving Vehicles. In: *Sensors 2014/14*, pp. 4384-4398. ISSN 1424-8220.
- [3] WILIAMS, P. E., HOFFMAN, M. W.: Classification of the Military Ground Vehicles Using Time Domain Harmonics' Amplitudes. In: *IEEE Transaction on Instrumentation and Measurement*, vol. 60, No. 11, November 2011.
- [4] BRANDSTEIN, M., WARD, D.: *Microphone Arrays-Signal Processing Techniques and Applications*, Chapter 2, Springer, 2010. ISBN 978-3-642-07547-6.
- [5] DAMARLA, T., MEHMOOD, A., SABATIER, J.: Detection of People and Animals Using Non-Imaging Sensors. In: *14th International Conference on Information Fusion*. July 2011, pp. 429-436.
- [6] ANDRASSY, V., GREGA, M.: Možnosti optimalizácie informačných procesov v bezpečnostnom systéme. In: *Košická bezpečnostná revue* [elektronický zdroj]. Roč. 5, č. 2 (2015), on-line, s. 11-18. ISSN 1338-6956.
- [7] NEČAS, P., GREGA, M.: *Simulation technologies: implications for security management and training*. In: *Security and Defense* [electronic source]: quarterly. - ISSN 2300-8741. - No. 2 (2013), online, s. 149-159.
- [8] TEUTSCH, H.: *Modal Array Signal Processing: Principles and Applications of Acoustic Wavefield Decomposition*, Chapter 4, Springer, 2007. ISBN-10 3-540-40893-2.
- [9] BEREŠÍK, R., PUTTERA, J.: Seismic-Acoustic Sensor system for vehicle and persons detection. In: *Proceedings of the International Conference New Trends in Signal Processing 2014*. Tatranské Zruby, 2014. pp. 6-13. ISSN 1339-1445.
- [10] LIU, W., WEISS, S.: *Wideband Beamforming Concepts and Techniques*, John Wiley & Sons, Ltd., 2010. ISBN 9780470713921.
- [11] KURTY, J., NEBUS, F.: *Antenna array signal processing*. Košice : Mercury-Smékal, 2002. ISBN 80-89061-58-3.
- [12] BEREŠÍK, R., PUTTERA, J., ŠOSTORNEK M., NEBUS, F., JURČO, J.: Sensors, sensors systems in military and security applications. In: *Final report of project*. Liptovský Mikuláš : 2015.

Maj. Eng. Roman BEREŠÍK, PhD.
Electronics Department
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: roman.beresik@aos.sk

Assoc. Prof. Eng. Jozef PUTTERA, CSc.
Electronics Department
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: jozef.puttera@aos.sk

Eng. Jozef JURČO
Electronics Department
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: jurci0@yahoo.com

THE IMPORTANCE OF REPLICATION IN THE APPLICATION LOGIC

Eubomír SEMANČÍK

Abstract: This paper describes possibilities of using replications for updating database applications. This approach is based on the fact that each database application can be divided into three main parts: presentation functions, application functions and data management. Application functions represent logic of the application (data processing in the database application) and they can be implemented by means of DataBase Management Systems (DBMS), i.e. stored procedures, triggers, user defined functions and rules. Next the paper characterizes the replications and describes their categorization and properties. Considering that the replications in distributed DBMS allow to send to the remote node not only tables with data, but also selected stored procedures, triggers, user defined functions and rules, the update of the entire database application can be executed using replications. In the conclusion the paper compares the update of a database application using SQL scripts and replications.

Keywords: Database application, distribution of data, database, replications, stored procedures.

1 INTRODUCTION

Software of a database application includes three basic components [4, 8]:

- Presentation functions – provide interactions between users and database applications, represent presentation of results of selected tasks to users and provide an interface to application control (provide an user interface);
- Application functions – provide application logic (represent data processing in the application – performing necessary computations with data obtained from the database);
- Data management – provide administration and data manipulation in the database.

Nowadays the client – server architecture is the most used architecture for information systems and database applications. The database servers of this architecture have a possibility to define [3, 4]:

- Stored procedures – precompiled sequences of SQL commands stored in a database;
- User – defined functions;
- Triggers - stored procedures (means), which automatically start during execution of DML commands – INSERT, DELETE, UPDATE;
- Rules for values and records.

Stored procedures, user – defined functions, triggers and rules are an option of implementation of application logic (application functions) [6].

The definition of the client – server architecture is based on distribution of processing between several processes, where at least one process is a client that requests services from a server [4].

For client – server systems the following subgroups have been defined (Tab. 1) [4, 8]:

- DP – Distribution Presentation (Interface Distribution);
- RP – Remote Presentation (Interface Separation);
- DF – Distributed Application Function (Application Distribution);

- RDM – Remote Data Management (Data Separation);
- DD – Data Distribution.

These subgroups are based on the distribution of functions between the client and the server [4, 6, 8].

Tab. 1 Distribution of components between client and server and subgroups (models) of client – server systems

		Subgroups of client – server systems				
		DP	RP	DF	RDM	DD
Components of a database application	Data Management	Server	Server	Server	Server	Server and Client
	Application Functions	Server	Server	Server and Client	Client	Client
	Presentation Functions	Client and Server	Client	Client	Client	Client

The subgroups DP (Distribution Presentation) and RP (Remote Presentation) have implemented the application functions on a server, wherefore the use of stored procedures, user – defined functions, triggers and rules are preferred in these models.

2 DISTRIBUTED DATABASE SYSTEM

A distributed database system is a set of interconnected computer network nodes, where each node contains a separate database system and the

nodes can access the data stored on another nodes as if they were placed in their own node (Fig. 1) [3, 5].

Distributed database is thus a set of interconnected databases, which are located on different nodes so that the user is handled as in the case of a centralized database [3, 5].

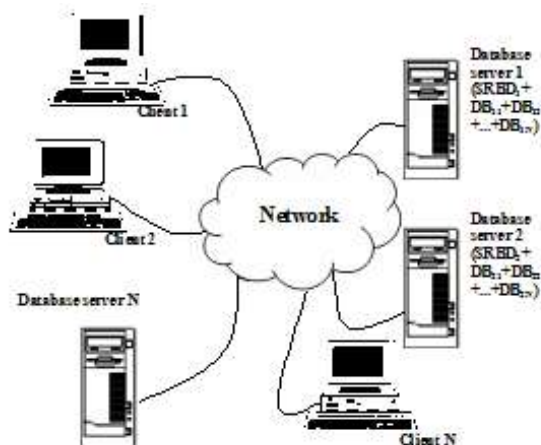


Fig. 1 A distributed database system
Source: author.

The distributed data processing is linked with various forms of organization of data maintained by a distributed database management system.

In principle, possible ways of distributing of data stored in the databases are the following [3, 4, 5]:

- Replication of data – all nodes contain the same data (the selected part of the same data);
- Fragmentation of data – all nodes contain different data.

2.1 Replication

Data replication allows distributing data from a source database on one or more servers [7].

The basic idea of replication is to create a local database, which is identical with the central database (this database is redundant).

The replication is a generation and reproduction of multiple copies of data in one or more locations [1]. This allows access to current data for users at the right time and location and improves the performance of data processing, when central resources are overloaded [1].

Replication is used for administration of data on multiple servers on a periodic basis. If you need to create a copy of the data only once, the replication is not needed [7].

The data that are distributed during replication are called articles. Articles are the basic units of replication. These articles contain tables, fragments of tables, stored procedures, etc. A publication is a collection of articles [2, 5, 7].

Reasons for use of replications are [7]:

- Synchronization of changes in the remote database with a central database;
- Creating multiple instances of a database in order to distribute the loading;
- Distribution of some data sets from the central server to other servers;
- Editing of data and their distribution to multiple users.

An importance of replication is [5]:

- A higher level of data accessibility;
- A higher level of data security.

Replication increases [3]:

- System performance;
- System availability.

Replication can be divided into [1,7]:

- Continuous;
- Periodic;
- Synchronous;
 - Replicated data is updated immediately after updating of source data - commit transaction closes the replication;
 - These are used when full data synchronization is required;
 - They represent heavy loading for the network;
 - It is impossible to terminate a transaction when any location is not accessible;
- Asynchronous;
 - The target database is updated after updating of entire source database (not after updating of source data);
 - These are used when full data synchronization is not required;
 - Time delay of restoring of consistency can be seconds to hours.

Other requirements related to replications [1]:

- Specification of a replication scheme – authorized users determine what data and objects will be replicated;
- Subscription – authorized users determine what data and objects will be available for replication;
- Initialization – possibility to initiate the target replicas;
- Scalability – possibility to process small as well as large volumes of data;
- Mapping and transformation – possibility to process replications between different platforms;
- Replications of objects – possibility to replicate other objects than the data (tables), e.g. stored procedures, triggers;
- Simplified administration.

Replication architecture consists of [2, 5, 7, 9]:

- Replication components – data and server components used for replications:
 - Publisher – the database server, which provides data and objects for replication (database tables, views, stored procedures, user – defined functions, etc.), keeps the information about data changes and information about the source database;
 - Distributor – the database server, which distributes replicated data, this server controls the replication and contains distribution database, metadata, historical data and records about transactions;
 - Subscriber – the database server (one or more), which synchronizes data, objects or transactions with publisher (subscribe data from publisher).
 - Replication agents – applications that are used during a replication:
 - Snapshot agent
 - creates a snapshot of data;
 - updates information in the distribution database;
 - is started on the Distributor and it connects to the Publisher;
 - Distribution agent
 - moves data from snapshot or transactional replication to Subscriber;
 - is started on the Distributor or Subscriber;
 - Merge agent
 - synchronizes changes after creation of the first snapshot;
 - is started on the Publisher or Subscriber;
 - is used in merge replications;
 - Agent for reading of transaction logs
 - moves transactions for replications from transaction logs to the Publisher or Distributor;
 - is started on the Distributor and connects to the Subscriber;
 - is used in transactional replications;
 - Variants of replications – types of replications, which can be set:
 - Snapshot replication
 - represents the current snapshot of data at a certain time;
 - this snapshot will replace the data on one or more subscribers;
 - increases network traffic;
 - is started periodically, therefore the Subscriber does not contain actual data;
 - may be used to initialize merge replication or transactional replication;
 - Transactional replication
 - is used in the server – server environment;
 - the snapshot is sent to the Subscriber after starting of replication, then transactions are sent to the Subscriber;
 - can be started continuously or periodically;
 - Merge replication
 - is suitable for replication of large amount of data or when low latency is required between the Publisher and the Subscriber;
- The replications consist of the next steps [5, 7]:
- choosing the type and model of replication;
 - execution of preliminary operations;
 - configuration of the Distributor and setting permissions for the Publisher and the Subscribers;
 - creating of publication (selection of objects for replication);
 - creating of subscriptions.
- Let us denote these steps as a configuration of replication.
- Related with replication, the following types of ownership of data are known [1]:
- Master/slave (asymmetric replication)
 - asynchronously replicated data are owned by one locality (master locality, primary locality);
 - any locality can read these data;
 - to avoid conflicts, only one locality can update these data;
 - Workflow
 - the rights of updating of data could be transferred from one locality to another;
 - only one locality can update these data at a time;
 - Update anywhere (peer-to-peer, symmetric replication)
 - more sites have the same rights to update the replicated data;
 - locations can work autonomously when other localities are unavailable;
 - there may be conflicts between localities;
 - comparing the records on the source and destination locations, timestamps, priorities and manual intervention are used for conflict resolution.

3 UPDATE OF DATABASE APPLICATION

As it has been already mentioned, application functions in database applications are realized by stored procedures, user – defined functions, triggers and rules.

We prepare a simple database application. We will update this application (i.e. change processing of data into application) through updating of stored procedures.

Let's have two database servers SQL_1 and SQL_2 with the databases data_1 on SQL_1 and data_2 on SQL_2.

We can prepare the necessary parts of the database application, e. g. tables and stored procedures on the database server SQL_1 in the database data_1 [6]:

```
CREATE TABLE tab1 (... , data ...)

CREATE TABLE ...

CREATE PROCEDURE proc1 @param1 INTEGER
AS
...
... WHERE id = @param1
...
GO

CREATE PROCEDURE ...
```

3.1 Update of database application using SQL scripts

We execute experiments in which we are going to update the above mentioned application through SQL scripts (SQL script is a sequence of SQL commands, which will be run step by step in the database, in which the script is running). The user has the right to run SQL scripts in the database data_1 on SQL_1 and data_2 on SQL_2, too.

We create a table for recording times in the experiments

```
CREATE TABLE tab_audit (id SMALLINT
PRIMARY KEY, time DATETIME2(7))
```

and stored procedures

```
CREATE PROCEDURE procA AS
...
SET @stringA = N'alter procedure proc1 as ... '
INSERT INTO tab_audit (id, time) VALUES
(@var1, SYSDATETIME())
EXECUTE sp_executesql @stringA
SET @var1 = @var1 + 1
INSERT INTO tab_audit (id, time) VALUES
(@var1, SYSDATETIME())

CREATE PROCEDURE procB AS
...
SET @stringB = N'alter procedure proc1 as ... '
INSERT INTO tab_audit (id, time) VALUES
(@var1, SYSDATETIME())
EXECUTE sp_executesql @stringB
SET @var1 = @var1 + 1
INSERT INTO tab_audit (id, time) VALUES
(@var1, SYSDATETIME())
```

where @stringA ≠@stringB.

INSERT INTO tab_audit ... command writes the current system time into the table tab_audit.

EXECUTE sp_executesql @stringA (EXECUTE sp_executesql @stringB) commands execute a command, which is registered in the variable @stringA (@stringB), where commands for updating the stored procedure proc1 (ALTER PROCEDURE) are located in variables @stringA (@stringB).

The reason for using of EXECUTE sp_executesql command is the fact that the command CREATE PROCEDURE must be usually executed as the first command in the SQL script, but INSERT INTO command for recording time is executed as the first command in the procedures procA (procB).

We started the commands execute procA and execute procB in the loop. It was executed 1000 repeated cycles.

The stored procedures procA and procB, along with the loop in which the procedures procA and procB are started, represent SQL script.

It does not matter whether the script is started on the server SQL_1 or on the server SQL_2 in this experiment.

It results from the experiments, that the change of stored procedures takes several milliseconds.

3.2 Up date of database application using replication

Replication in distributed databases allows to send the stored procedures, user – defined functions, triggers and rules between computer network nodes. Then an update of some types of database applications can be realized by means of replication [6].

We executed experiments to update the database application through replication in accordance to the above described application.

The user has the right to access the databases data_1 on SQL_1 and data_2 on SQL_2, too.

We create a table for recording times in the experiments and triggers for recording information about creating and updating of the stored procedure proc1.

```
CREATE TABLE tab_audit (id SMALLINT
PRIMARY KEY, activities CHAR(20), time
DATETIME2(7))
```

```
CREATE TRIGGER trig_db_1 ON DATABASE
FOR CREATE_PROCEDURE AS
```

```
...
INSERT INTO tab_audit VALUES (@max, 'create
procedure', SYSDATETIME())
SET @max = @max + 1
...
```



```

CREATE TRIGGER trig_db_2 ON DATABASE
FOR ALTER_PROCEDURE AS
...
INSERT INTO tab_audit VALUES (@max, 'alter
procedure', SYSDATETIME())
SET @max = @max + 1
...

CREATE TRIGGER trig_db_3 ON DATABASE
FOR DROP_PROCEDURE AS
...
INSERT INTO tab_audit VALUES (@max, 'drop
procedure', SYSDATETIME())
SET @max = @max + 1
...
Afterwards we create the procedure proc1:
CREATE PROCEDURE proc1 @param1 INTEGER
AS
...
... WHERE id = @param1
...
GO

```

We prepare snapshot replication on the SQL_1 (Publisher) for SQL_2 (Subscriber). The snapshot replication must be created before inserting of data into tables:

- include tables and stored procedures into publication;
- setup of subscriber (subscribers) – database data_2 on the database server SQL_2;
- start replication.

Table tab1 and procedure proc1 were replicated on the server SQL_2 into the database data_2.

We create triggers for recording information about creating and updating of stored procedure proc1 on the server SQL_2 in the database data_2, too:

```

CREATE TRIGGER trig_db_1 ON DATABASE
FOR CREATE_PROCEDURE AS
...
INSERT INTO tab_audit VALUES (@max, 'create
procedure', SYSDATETIME())
SET @max = @max + 1
...

CREATE TRIGGER trig_db_2 ON DATABASE
FOR ALTER_PROCEDURE AS
...
INSERT INTO tab_audit VALUES (@max, 'alter
procedure', SYSDATETIME())
SET @max = @max + 1
...

CREATE TRIGGER trig_db_3 ON DATABASE
FOR DROP_PROCEDURE AS
...

```

```

INSERT INTO tab_audit VALUES (@max, 'drop
procedure', SYSDATETIME())
SET @max = @max + 1
...

```

Then we start on SQL_1

```

ALTER PROCEDURE proc1 AS
...

```

and SELECT * FROM tab_audit

with results

```

1 create procedure      *****
2 alter procedure      *****

```

The new replication on SQL_1 can be created after the update of database application:

- only changed stored procedure has been included into the new publication;
- setup of the Subscriber (Subscribers) – database data_2 on database server SQL_2;
- start replication.

We start on SQL_2:

```

SELECT * FROM tab_audit

```

with results

```

1 drop procedure      *****
2 create procedure    *****

```

Commands DROP PROCEDURE and CREATE PROCEDURE (but not ALTER PROCEDURE) are registered through triggers into the table tab_audit during replication, thus the snapshot from SQL_1 replaced the stored procedure proc1 on the server SQL_2.

These experiments were also executed with transactional replication. These results also confirm the possibility to update a database application through transactional replication, too. Attention must be paid to the definition of publications in order to prevent unnecessary duplications of data after the change of procedures in the database data_1.

We used already created tables tab_audit and tab1, triggers trig_db_1, trig_db_2, trig_db_3, procedure proc1 and already prepared replications in further experiments.

We prepared new snapshot replication on SQL_1, which will include the stored procedure proc1 in the publication only.

We started periodically the next commands in the loop (replication of updated procedure):


```

DECLARE @var1 AS SMALLINT
DECLARE @var2 AS SMALLINT
...
DECLARE @max AS SMALLINT
SET @var1 = 1
...
WHILE @var1 <= @max
BEGIN
DECLARE @retA AS NVARCHAR(MAX)
DECLARE @retB AS NVARCHAR(MAX)
SET @retA = N'ALTER procedure proc1 as ... '
SET @retB = N'ALTER procedure proc1 as ... '
EXECUTE sp_executesql @retA
INSERT INTO tab_audit(id,time) VALUES (@var2,
SYSDATETIME())
SET @var2 = ...
EXECUTE          sp_startpublication_snapshot
@publication = 'publ'
INSERT INTO tab_audit(id, time) VALUES (@var2,
SYSDATETIME())
SET @var2 = ...
EXECUTE          sp_addpushsubscription_agent
@publication= 'publ',...
INSERT INTO tab_audit(id, time) VALUES (@var2,
SYSDATETIME())
SET @var2 = ...
EXECUTE sp_executesql @retB
INSERT INTO tab_audit(id, time) VALUES (@var2,
SYSDATETIME())
SET @var2 = ...
EXECUTE          sp_startpublication_snapshot
@publication = 'publ'
INSERT INTO tab_audit(id, time) VALUES (@var2,
SYSDATETIME())
SET @var2 = ...
EXECUTE          sp_addpushsubscription_agent
@publication= 'publ',...
INSERT INTO tab_audit(id, cas) VALUEs (@max,
SYSDATETIME())
SET @var2 = ...
SET @var1 = @var1 + 1
END

```

Where procedures:

- o sp_executesql - executes the commands stored in a Unicode string (retA);
- o sp_startpublication_snapshot - starts the Snapshot Agent that generates the initial snapshot for a publication;
- o sp_addpushsubscription_agent - creates the subscriptions programmatically.

It results from the experiments that the change of stored procedures through replication takes several seconds.

3.3 Evaluation of experiments

The above described experiments highlight several interesting features of replications for update

of database application compared to the use of SQL scripts:

- Time of update of database application is much higher for update using replication than for update using SQL scripts, if we don't consider the time of SQL script transmission;
- Replication requires a network connection between the source and target database server but transmission of SQL scripts is possible using removable storage media (DVD / USB storage), too;
- When the database application is being updated on multiple servers, distribution of scripts can be difficult. Since the replication is configured on one server, the proper script is not necessary to create;
- It is not required to perform any preliminary operations on updated servers for update of a database application using replication; but for update of a database application using SQL script, it is necessary to create this script on the source server, then this script has to be transferred to the target server and then run on it;
- No interventions are required on the updated servers in order to update the database application using replication;
- Difficulty of configuration of replication depends on the variants of replication – the configuration of snapshot replication is easy, but configuration of transactional replication is more elaborate than snapshot replication;
- Difficulty of configuration of replication depends on using of special tools for replication management or direct using of commands – the using of special tools is easy, but the using of commands is difficult.

These are shown in the table below (Tab. 2):

Tab. 2 Compare of replication and SQL script for update of database application

Property / Value (Result)	SQL script	Replication
Time of Update (change of stored procedure) [ms]	≈ 1	≈ 1000
Requirement for network connections between database servers	NO	YES
Requirement for preliminary operations on the updated servers	YES	NO
Requirement for intervention on the updated servers	YES - periodically at update of application	NO
Difficulty	Low	Low to high

4 CONCLUSION

This paper reviews possibilities of replication for updating of some types of database applications.

This is possible if the application logic of the database application is implemented on the database server only.

These are cases when the application logic is realized by means of stored procedures, user – defined functions, triggers and rules.

References

- [1] CONNOLLY, T., BEGG, C., HOLOWCZAK, R.: *Mistrovství – databáze. Profesionální průvodce tvorbou efektivních databází*. Brno : Computer Press, 2009. 1. vyd. 584 s. ISBN 978-80-251-2328-7.
- [2] KNIGHT, B.: *Microsoft SQL Server 2000 Pokročilé techniky*. Brno : Computer Press, 2004. 477 s. ISBN 80-251-0111-8.
- [3] MATIAŠKO, K., VAJSOVÁ, M., ZÁBOVSKÝ, M., CHOCHLÍK, M.: *Databázové systémy. Databázové technológie a aplikácie*. Žilina : EDIS – vydavateľstvo ŽU, 2008. 518 s. ISBN 978-80-8070-821-4.
- [4] SEMANČÍK, E.: *Databázové systémy*. Liptovský Mikuláš : Vojenská akadémia, 2004. 115 s. ISBN 80-8040-230-2.
- [5] SEMANČÍK, E., DEDERA, E.: *Distribúované spracovanie údajov v databázových aplikáciách*. Učebný text. Liptovský Mikuláš : Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2010. 67 s. ISBN 978-80-8040-411-6.
- [6] SEMANČÍK, E.: Update of Database Application Using Replication. In: *KIT 2015 [elektronický zdroj]*. Communication and Information Technologies, 8 th international Scientific Conference : Conference Proceedings: Tatranské Zruby – October 14th – 16th, 2015. Liptovský Mikuláš : Published by Armed Forces Academy of Gen. M. R. Štefánik, 2015. 6 p. ISBN 978-80-8040-508-3.
- [7] STANEK, W.R.: *Microsoft® SQL Server 2005. Kapesní rádce administrátora*. Brno : Computer Press, 2006. 1. vyd. 542 s. ISBN 80-251-1211-X.
- [8] TASCHNER, K.: Nebojte se databází. In: *Computer World*, č. 44/96, s.17-30.
- [9] WALTERS, R. E., COLES, M., RAE, R., FERRACCHIATI, F., FARMER, D.: *Mistrovství v Microsoft SQL Server 2008*. Brno : Computer Press a.s., 2008. 1. vyd., 864 s. ISBN 978-80-251-2329-4.

Eng. Ľubomír SEMANČÍK, PhD.
 Department of Informatics
 Armed Forces Academy of General M. R. Štefánik
 Demänová 393
 031 01 Liptovský Mikuláš
 Slovak Republic
 E-mail: lubomir.semancik@aos.sk

MONITORING OF DEPARTMENT NETWORK – ADMINISTRATOR VIEW

Július BARÁTH

Abstract: IT infrastructure primary consists of end devices, communication links and networking devices and all of them are prone to misconfiguration errors and vulnerable to attacks. To prevent poor performance, instability of the systems used and to fight with attackers – effective monitoring is a part of everyday admin’s duties. The paper answers basic questions: how to collect, normalize and process log and audit information; what is essential information to log across the platforms used; and how to monitor network attached devices in the department network. Collected and filtered data is then indexed with Splunk where data analysis and visualization is performed using queries or preconfigured dashboards. Only when full understanding of problem is achieved, proper reaction to fix the problem can be taken. A simple example is provided to better illustrate the process of finding and fixing a misconfiguration problem.

Keywords: Splunk, monitoring, audit, network infrastructure.

1 INTRODUCTION

Proper, timely, and effective reaction to misuse of IT resources and data thefts requires overall situational awareness and the correct information in the right place at the right time including historical logs. Information acquired from security network devices, operating systems and critical applications on the one hand and proper analysis and correct reaction by IT professional on the other hand is required to prevent intrusion, data thefts and violation of the security policy. Common, standardized, community and industry accepted protocols for reporting are required to accomplish vision of automated, real time and effective reaction to modern threats.

Both operating system and network/security device vendors provide tools to manipulate generated logs from their products with more or less success to import logs from other party products. Such approach usually ends with multiple and overlapping platforms for monitoring, inconsistencies in logs coverage and difficult manageability. Network and system admins, together with security professionals are asking for one universal, extendable platform for filtering, processing and visualization of logs. One of the products in this category is Splunk. The paper describes how, where and what data to collect and how to use them to answer every day admin questions about functionality and security in the department network.

2 BACKGROUND

ISO 27002 in section Communications and operations management subsection 10.10 Monitoring states that “Systems should be monitored and information security events should be recorded.

Operator logs and fault logging should be used to ensure information system problems are identified. An organization should comply with all relevant legal requirements applicable to its monitoring and logging activities. System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.” [1].

To accomplish the idea, the administrator should:

- configure audit logs to support future investigations and access control monitoring,
- monitor system use (authorized access, privileged operations, unauthorized access attempts, system alerts or failures, changes or attempts to change system security settings and controls),
- protect logging facilities and log information against tampering and unauthorized access,
- log system administrator and system operator activities,
- log and take an appropriate action on faults,
- guarantee that the clocks of all relevant information processing systems within an organization or security domain are synchronized with an agreed accurate time source [1].

Many “Best practices for network monitoring” exists and are available^{1,2}, some of them put accent on effectiveness and proactive approach using offsite applications, monitoring of both performance and availability of resources, providing of several different notification options, providing application specific alerts and reporting, providing hardware specific alerts or for example have robust reporting capabilities.

The question is how to properly size those capabilities, unify log formats coming from multiple environments, select software for analysis and reporting etc. In the next section we will discuss our approach to monitoring a department network.

¹ Available at: http://www.pcworld.com/article/144635/guide_network_management_monitoring.html

² Available at: <http://lanlogic.com/pdf/Lanlogic-Network-Monitoring-Best-Practices.pdf>

3 DEPARTMENT NETWORK AND MONITORING

The department oriented to IT research and education uses variety of server and desktop operating systems and applications, network infrastructure, peripherals and security devices (Fig. 1).

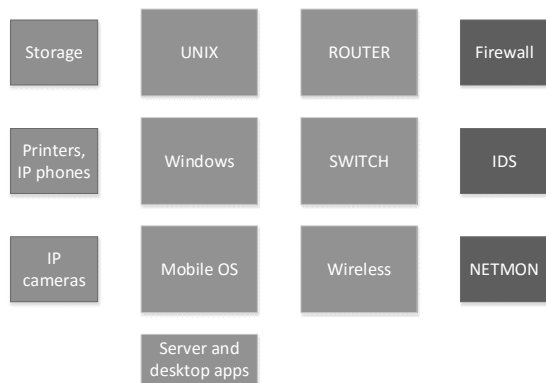


Fig. 1 Structure of resources used by a department
Source: author.

Any part of the infrastructure is a potential target for attacks, due to misconfigurations or software bugs not yet discovered and patched.

Based on number of used devices, the primary targets of attacks and misuses are desktop and server operating systems. Basic installation of MS Windows desktop operating system does not provide sufficient log and audit information and to fix it - group security policy should be used to force domain workstations to apply appropriate log and audit policies. Moreover, workstations use antivirus software with its own reporting capabilities and formats.

Question 1: What is essential information to log from servers?

Problem 1: Logs are stored locally and in a specific format.

Server (UNIX and MS Windows) operating systems have extended complexity of logging and auditing because of server applications with specific needs:

- web, mail, database servers,
- network services – DNS, DHCP, Active Directory, web applications,
- special services - Certification Authority, time service, Licensing servers ...,
- shared applications – licensed development products and more.

Both UNIX and MS Windows servers need to enforce security and configure logging and auditing specific to their configuration. Managing consistent

security policy across all servers can be difficult. Problem 1 applies here, too.

Question 2: What is essential information to log from servers and their applications?

Second possible target of attacks are network attached devices – some of them are disk storages, network printers, IP phones, IP video cameras, remotely operated door locks and more. Those devices have in most cases old firmware versions and limited or missing logging features.

Question 3: How to monitor network attached devices?

Third possible target of attacks are network infrastructure devices and monitoring devices. Routers, switches, firewalls, IDS and network monitors (if purchased as managed devices) have specialized operating systems and usually good logging capabilities. As any other hardware with an operating system, they should be secured, patched and remote logging should be configured.

Question 4: What is essential information to log from network infrastructure and monitoring devices?

To generalize, we should answer following questions:

- how to collect, normalize and process log and audit information,
- what is essential information to log across the platforms used,
- how to monitor network attached devices.

3.1 How to collect, normalize and process log and audit information?

To collect process and present data the Splunk³ software was chosen. “Splunk is the engine for machine data. Splunk can read data from just about any source imaginable, including student registration systems, learning management systems, networks, web servers, remote sensors, mobile and online learning applications, legacy applications, application servers and structured databases. By centralizing all this data into a single console, Splunk provides unparalleled insight into problems, usage patterns and trends across an entire campus IT infrastructure. In addition, institutional usage is not limited by the number of machines, data sources, or users—it is only limited by the total data volume that is indexed. This gives IT the ability to control utilization without being locked into a per-user or per-machine fee” [3].

Collection of data and its processing can be described using Fig. 2. As a prerequisite to collect useful data, all devices must have synchronized time and are managed by a local network administrator.

Desktops and **servers** are able to collect logs and audit information locally and send them to Splunk – Option 1 Fig. 2, but on the Splunk side we can filter less significant events and we are losing some logs

³ Available at: <http://www.splunk.com/>

specific for application servers or network services, because some DHCP logs on MS Windows servers are stored in local log files and not in the central event log system, SharePoint server produces logs differently, too, etc. Specialized Splunk client lite (with server/platform specific extensions) can be remotely installed on critical servers and its configuration file allows the administrator to select/filter what information is send, where it should be processed and provides identification of source. Information being send includes health, resource utilization, updates, security, change management and more.

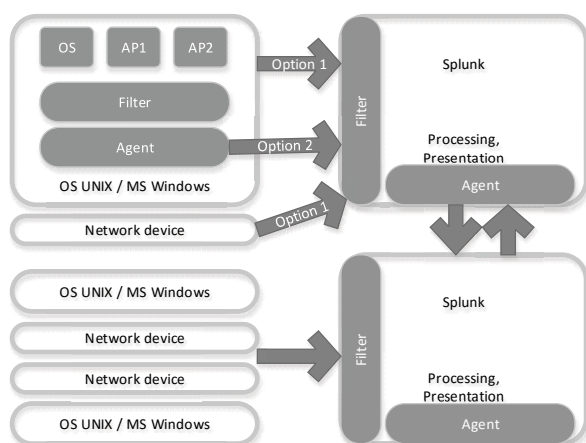


Fig. 2 Data collection and processing
Source: author.

Network and security devices (routers, switches, IDS, firewalls) manufactured by Cisco Systems are remotely manageable devices with appropriate log capabilities. Logs from these devices are sent directly to Splunk and no extra effort is needed to interpret them (thanks to plugins created and maintained by the company). Basic logging configuration of routers usually includes settings for the timestamps, the logging level and the logging syslog server.

More advanced monitoring options enable to:

- change characteristics of auditing,
- set up smart call home logging,
- monitor interface changes,
- utilize DHCP logging,
- utilize ACL logging,
- monitor MAC move notifications,
- utilize STP and IP SLA logging etc.

A short example of advanced monitoring configurations follows.

```
Advanced logging includes change auditing:
Archive
```

```
log config
  logging enable
  logging size 200

  notify syslog contenttype plaintext
  hidekeys
!
login on-failure log
login on-success log
logging userinfo
!
Smart call home logging includes:
ip http client source-interface
FastEthernet 0/0
!
service call-home
call-home
  contact-email-addr xy@aos.sk
  site-id "kti"
  profile "Splunk"
  destination transport-method http
  destination address http
http://XX.XX.XX.XX:YYYY
  subscribe-to-alert-group diagnostic
severity debug
  subscribe-to-alert-group
environment severity debug
  subscribe-to-alert-group inventory
  subscribe-to-alert-group inventory
periodic daily 20:00
!
```

3.2 How to monitor network attached devices?

This category of devices has specific needs, because not all of them support direct open interface to access logs. If the attached device is monitored by a server or a host based application, the Splunk client lite can be used to access logs. In other cases only L2-L7 communication monitoring can be used (via a specialized probe or monitor).

To monitor special communication channels like Locked-down VDI monitoring (printer and USB channels), see ExtraHop for Security and Compliance⁴. The ExtraHop platform analyzes wire data, which is all L2-L7 communications between systems including full bi-directional transaction payloads.

⁴ Available at: <https://splunkbase.splunk.com/app/1757/>

3.3 What is essential information to log across the platforms used?

General guidance for logging is provided by [1] where it is written that “Audit logs should include, when relevant:

- a) user IDs,
- b) dates, times, and details of key events, e.g. log-on and log-off,
- c) terminal identity or location if possible,
- d) records of successful and rejected system access attempts,
- e) records of successful and rejected data and other resource access attempts,
- f) changes to system configuration,
- g) use of privileges,
- h) use of system utilities and applications,
- i) files accessed and the kind of access,
- j) network addresses and protocols,
- k) alarms raised by the access control system,
- l) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.”

And monitoring system should record:

- a) authorized access,
- b) all privileged operations,
- c) unauthorized access attempts,
- d) system alerts or failures,
- e) changes to, or attempts to change, system security settings and controls.

The frequency how often the results of monitoring activities are reviewed should depend on the risks involved. Risk factors that should be considered include the following:

- a) criticality of the application processes,
- b) value, sensitivity, and criticality of the information involved,
- c) past experience of system infiltration and misuse, and the frequency of vulnerabilities being exploited,
- d) extent of system interconnection (particularly public networks),
- e) logging facility being de-activated [1].

For a MS Windows server it is easy to generate hundreds of thousands records per day per server and deeper understanding of the system is required to define audit and logging parameters in order to filter unwanted logs [4,5,7-9]. For UNIX systems we can generate periodic logs using system utilities (sar, tcpdump, iostat, mpstat, IP Traf etc) and then use them to extend “Slunk Universal Forwarder for Linux” or “Linux Auditd⁵” app capabilities. For detailed description how to route and filter data on Splunk installations, see [2].

4 PRESENTING DATA WITH SPLUNK

Once textual data (from switches, routers, firewalls, desktops, servers, web servers, databases, network services) is indexed by Splunk, it is analyzed by system and network administrators or security experts to find anomalies, configuration errors, and all sorts of breaches using Splunk’s Search Processing Language.

As we use Splunk to answer questions, we’ll find that we can break the task into three phases.

1. First, identify the data that can answer our question.
2. Second, transform the data into the results that can answer our question.
3. Third, display the answer in a report, interactive chart, or graph to make it intelligible to a wide range of audiences [6].

Nice thing about Splunk is that our findings may vary from the most common to the most unusual ones. Results can be summarized via statistics or represent accidents as group of events, providing necessary level of operational intelligence.

To find the needle in the haystack we use search app. Search lets us create search query, change time range, run query, refine search, save search and more. An alternative to type search commands is to use dashboards, followed by detail inspection of problems.

Fig. 3 shows 25 crashes of server-c in last 24 hours, using references in crashes the reason of problems is determined. Detail view with preconfigured search query helps with inspection.

```
eventtype="wineventlog_windows"
EventCode="1001" Event_Name="*"
host="*" | eval application=P1."
(version: ".P2.")" | search
application="7.6.7601.18804
(version: 80072ee2)"
```

Based on a detail view (not shown in the paper) we can quickly conclude that the problem comes from misconfiguration of the Windows update service. After fixing the problem we will not see such entries for server-c any more.

Dashboards are usually parts of specifically created applications from different vendors like Microsoft, Cisco etc. and if needed, we can create our own ones. It is very useful to create our own queries, transform them into events and run them automatically to detect possible configuration problems or violations of security policy. Such an approach automatizes routine actions and customizes working environment.

⁵ Available at: <http://splunkbase.splunk.com/app/2642/>

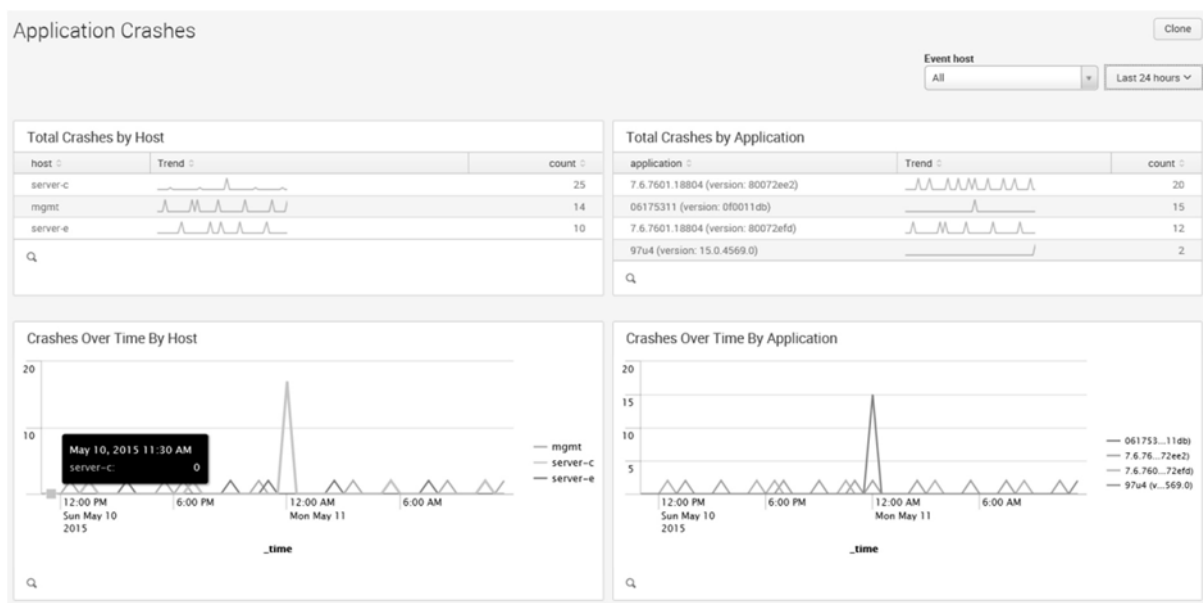


Fig. 3 Application crashes dashboard
Source: author.

5 CONCLUSION

Working with Splunk consists of gathering data, transferring them into answers and visualizing of review data to get answers. During the experimentation phase more than 66 million records from servers and routers were analyzed, many lesser or greater misconfigurations were fixed and a few security violation accidents were found. As any other technology on the market, when properly used by a trained professional, Splunk can help understand problems in our information infrastructure. It will not fix the problem; we must take proper actions to fix them. If we'll not regularly review collected data and actively search for new forms of attacks, our IT infrastructure and processed data will not be safe.

References

- [1] ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls. In: Switzerland: International Organization for Standardization.
- [2] Route and filter data [online]. [cited may 2015]. Available from: <<http://docs.splunk.com/Documentation/Splunk/6.2.2/Forwarding/Routeandfilterdatad>>.
- [3] Splunk for Higher Education and Universities [online]. [cited june 10 2014]. Available from: <http://www.splunk.com/web_assets/pdfs/secure/Splunk_for_Higher_Education.pdf>.
- [4] Planning and Deploying Advanced Security Audit Policies [online]. 2009 2015]. Available from: <[https://technet.microsoft.com/en-us/library/ee513968\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/ee513968(v=ws.10).aspx)>.
- [5] (T) Filtering or trimming Windows logs the right way, NOT by Event ID [online]. 2014 [cited may 2015]. Available from: <<http://hackerhurricane.blogspot.sk/2014/07/t-filtering-or-trimming-windows-logs.html>>.
- [6] CARASSO, D.: Exploring Splunk [online]. CITO Research, 2012. Available from World Wide Web: <<http://www.splunk.com/goto/book>>.
- [7] MELBER, D. *Windows group policy resource kit : Windows server 2008 and Windows vista*. Edtion ed. Redmond, WA : Microsoft Press, 2008. xxiv, 511 p. p. ISBN 9780735625143 (perfect bound).
- [8] Security Log Step-by-Step: Avoiding Audit Policy Configuration Pitfalls [online]. 2012 [cited may 2015]. Available from: <<https://www.ultimatewindowssecurity.com/blog/default.aspx?p=aa6c16dc-8bb8-40e3-aac9-d2c7eaa6c5f6>>.
- [9] TULLOCH, M. *Introducing Windows Server 2012 R2*. Edtion ed. Redmond, Washington : Microsoft, 2013. xi, 227 pages p. ISBN 9780735682788 (pbk.) 073568278X (pbk.).

Eng. Július BARÁTH, PhD.
Department of Informatics
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: Julius.Barath@aos.sk

VEHICLES ELECTROMAGNETIC EMISSIVITY ANALYSIS

Stanislava GAŽOVÁ, František NEBUS, Vladimír BELÁK

Abstract: Recent vehicles are equipped with a great number of communications – information systems, sensors, actuators and electronic devices with maximally suppressed electromagnetic emissivity. The nature of emitted signals is rather ultra-wide band noise and some stationary stochastic signals. The article deals with analysis of personal vehicles electromagnetic emissivity, which is one of the possible characteristics useful for vehicles classification and recognition. The signals analysis, based upon emissivity measurement in anechoic chamber, is investigated in the frequency range from 100 kHz to 35 MHz, concluded with some specific classification characteristics.

Keywords: Vehicle, electromagnetic emissivity, classification, recognition, digital signal processing.

1 INTRODUCTION

Electromagnetic security based on electromagnetic compatibility (interference - emissivity and susceptibility) theoretical basis is recently becoming fundamental task for car producers in conjunction with increasing number of used information technology (IT) and automation. Since IT-based parts of every new innovation have to be implemented on an Electronic Control Unit, there is an increasingly complex basis of ECUs contained in each car meanwhile building a core part of its electronic interior. While simple recent cars are equipped at least with 10 ECUs and several hundreds of m of cables distributed over the whole vehicle, some luxury vehicles currently have up to 80 ECUs.

Primary aim of the car producers from the EMC point of view is to guarantee the safe functionality of the car in standard environment (electromagnetic emissivity EMI) and not to be electromagnetically harmful to surrounding technology (electromagnetic susceptibility EMS) [1], [2], [3]. Those regulations are expressed in several international and EU regulations (CISPR 12, CISPR 25, EN 301 489-1, EN 50498, ISO 16750-2, ...). On the other hand the radiofrequency emissivity of the particular car has relation to the potentially harmful external electromagnetic field which may disrupts performance of the car control systems. This recent research is primarily performed in parallel with so called electromagnetic (or radiofrequency) weapons which are capable of remote electromagnetic disruption of electronics. Both emissions and external electromagnetic field characteristics are car's trade mark, construction, car engine and model dependent. From this point of view for potential external car control is electromagnetic characteristics analysis of the vehicles necessary in order to make required car classification and enable further proper safe external electromagnetic interference.

Car electronic system are operating in frequency range from zero to several GHz with power levels of units of mW to several tens of W.

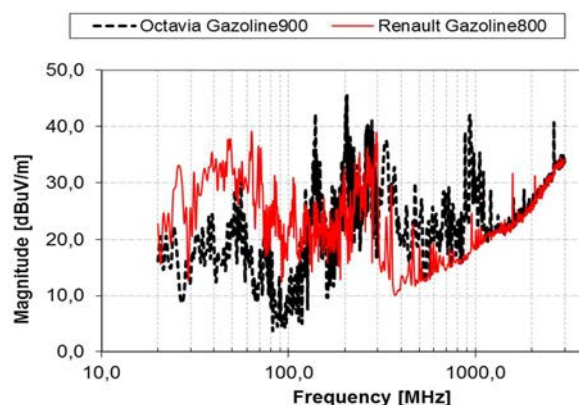


Fig. 1 Examples of electromagnetic emissions of personal vehicles measured inside anechoic chamber
Source: authors.

Majority of the stationary stochastic signals (communication systems) are very well EMC perfected, however it should be considered, that there are very short non-stationary signal or transient ones.

Electromagnetic emissivity is produced from four main areas of the vehicle:

- The ignition system - it is the largest source of electromagnetic emissivity, voltages up to 30 kV are now common and the peak current for a fraction of a second when the spark plug fires can peak in excess of 100 A, frequency range is above 30 MHz and the energy can peak, for fractions of a second, of the order of 500kW.
- The charging system produces electromagnetic emissivity because of the sparking at the brushes. Regulators with vibrating contacts can cause additional unwanted emissions.
- Motors, switches and relays produce some electromagnetic emissivity. A wiper motor and a heater motor are the most popular sources.
- Static discharges are due to friction between the vehicle and the air, and the tyres and the road [4].

Above mentioned precondition and potential scenario, where vehicle is approaching check point with electromagnetic recognition system (some other sensors for data fusion are expected too)

and electromagnetic disruptive system give us preliminary constrains for measurement and signals analysis.

Electromagnetic emissivity measurement time is the critical requirement. It is very short, up to several tens of milliseconds, due to the speed limit of the vehicle is established at 50 kph (14 m/s) in build-up areas and vehicle detection distance 10 m. This acquisition time will ensure the preservation of stationary stochastic signals and also several engine revolutions and related non stationary signals. One part of the sensor system is the omnidirectional antenna with bandwidth from 100 kHz to 35 MHz. In real situation it is expected stationary electromagnetic scene except standard communication signals.

2 SIGNAL ANALYSIS

It is known a signal is a physical quantity, it brings some report. This report can contain a lot of information, but how much information contains, it depends on the receiver. The signal can be represented by the description of one parameter depending on other parameter or parameters. The analysis of signals is based on this fact. The signals can be processed within the time domain, frequency domain, time – frequency (spectrogram) domain. Each process in one domain has a corollary to the others, however time domain is the best for the transient signals representation, frequency domain with proper selection of correlation interval for the stationary stochastic signals and spectrogram for general overview. In the processing of measured data is necessary reduction of data redundancy and suppress unwanted interference. This process occurs before analysing the data in one of the domain. The most common tool is the filtration and downsampling.

2.1 Time domain

Time domain investigation of signals and systems is one of the most essential tool of electrical engineering. It is useful in short time, transient several times repeated signals. For vehicles EMI analysis we expect those kind of signals emitted from ignition system, especially sparks from petrol engines, fuel injectors from diesel engines eventually petrol engines too. Signal acquisition and triggering synchronisation is with such signals driving process for whole signal acquisition and signal analysis process.

In recognition process cross and autocorrelation is very often used. Correlation is based on similar period of time of investigated processes and in our case it is repetitive ignition between 800 and 2000rpm (Fig.2). It is known crosscorrelation function (between two signals $x[n]$ and $y[n]$) can be written as [5]

$$K_{12}[k] = \sum_{n=0}^{N-1} x[n]y[n-k] \quad (1)$$

where k is time index moving one signal over the other and N repetition period – correlation interval; and autocorrelation function given by [5]

$$K[k] = \sum_{n=0}^{N-1} x[n]x[n-k] \quad (2)$$

2.2 Frequency domain

Frequency domain refers to analysing a mathematical function or a signal with respect to the frequency. This method is optimal for stationary stochastic signal analysis. The most common transformation is the discrete Fourier transformation commonly used in digital signal processing, software defined radios defined in [5].

$$\bar{X}[k] = \sum_{n=0}^{N-1} x[n]e^{-j2\pi\frac{nk}{N}} \quad (3)$$

where $x[n]$ represents n -th sample in time. Final spectral resolution depends on number of samples, method and windowing, averaging, overlapping and sampling quality (bits number, sampling frequency). Those parameters became very important in situation, where signal to noise ratio (SNR) is very low and wanted signal is unknown. In our situation SNR it is below 15dB, in real situation with background noise is below 5dB. Each car situation sampled signal was 83886606 points vector, sampling frequency 125 MHz, counting 16 bit resolution, noise threshold -110dB. During the test we examined also some other methods, MUSIC, Covariance, Burgh estimator. Those methods are very effective for narrow band signals compound. The best resolution results we obtained with Welch's method, which is built on the averaged periodograms of 256 points overlapped, $N=2048$ and $N=4096$ Hamming windowed segments of a time series of signal.

$$P[k] = 20 \cdot \log_{10} \left| \frac{1}{L} \sum_{l=1}^L \left| \sum_{n=1}^N x^l[n]w^l[n]e^{-j2\pi\frac{lk}{N}} \right| \right| \quad (4)$$

It is good to know one attribute of Fourier transform. If used a long period of signal in time domain, it has an impact on the spectrum amplitude of non-stationary frequency components of $(X[k])$ are relative values and are reduced. Thus transient signals are rarely visible in such interpretation.

2.3 Time - frequency domain

The Fourier transform allows visibility only frequency components in the whole signal and it does not give a view about frequency components occurrence in time. For this view it is suitable to use spectrogram, also called waterfall.

$$P_l[k] = 20 \cdot \log_{10} \left| \sum_{n=1}^N x_l'[n] w_l'[n] e^{-j2\pi \frac{lk}{N}} \right|, \quad l = 1, \dots, L \quad (5)$$

The common tool for spectrogram is modification of the Fourier transform called Short Time Fourier Transform (STFT) with the window shifted over time gradually. We used it with two different parameters. In general signal characterization with 1024 points overlapped $N=16384$ Hamming windowed segments of a time series of signal. Second option for finding transients (ignition - injection mainly) was 36 points overlapped, $N=64$ Hamming windowed segments of a time series of signal and 512 sampling points for calculation the discrete Fourier transform.

3 THE VEHICLE MEASUREMENT AND ANALYSIS OF MEASURED DATA

Configuration of the workplace the measurement of shielding emissivity of personals vehicles was performed according to EMI standard MIL STD-285 and IEEE-299. The whole measurement was done in the Anechoic chamber that was prevented by the influence of other sources of electromagnetic fields. Anechoic chamber was with certified attenuation above 90 dB. The test bed consisted of spectrum analyzer Anritsu MS2667C, signal analyzer Agilent Infinium DSO 80804B and receiving antenna SAS-550-1B with antenna factor 0 in whole spectrum

range. There were seven vehicles under the test: Škoda Yeti (diesel engine); Škoda Octavia (diesel engine), Škoda Octavia (petrol engine), Ford Focus (diesel engine), Ford Mondeo (diesel engine), Fiat 500 (petrol engine) and Honda Civic (petrol engine).

3.1 Analysis in the time domain

It is necessary to find signals which are regularly repeated and which are specific for each class of vehicle in the time domain. Signals, occurred with a certain time period, are a precondition for classification or recognition of the vehicle. Examples can be the communication signals or transients caused by the ignition system, which depends on engine revolutions. It is a spark inside the cylinder for the vehicle with petrol engine and a fuel injection into the cylinders for vehicle with diesel engine common rail injection technology [6]. These two facts depend on engine revolutions. It is known if the engine revolutions are 2000 rpm, one of these facts shows every 0,015 seconds in the time domain or every 0,0375 seconds, if the engine revolutions is 800 rpm. There are pulses in Škoda Yeti's data in time domain (fig. 2), which depend on engine revolutions. The time period is 0,0379 second for 800 rpm and 0,01634 seconds for 2000 rpm (inaccuracy can be caused by fluctuation of engine revolutions or error on the display for engine revolutions in vehicle). However, the pulses are not 100 % identical, which can be caused by reducing transient because of they must show frequently. This fact can cause that the cross correlation is not 1.

On the other side, there can be also data of vehicle that shows no characteristic pulses or signals without filtering in time domain for example Škoda Octavia's (classic pump injector diesel engine) data (Fig.3).

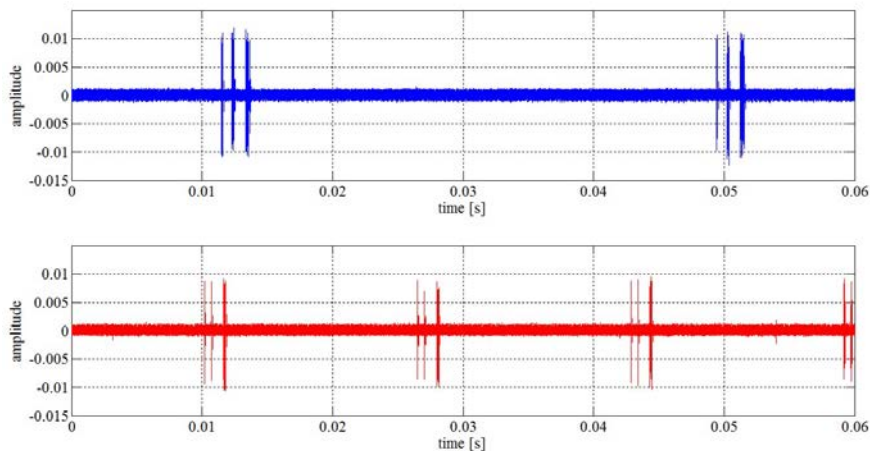


Fig. 2 Škoda Yeti (with diesel engine) data in time domain – top is 800 rpm, down is 2000 rpm
Source: authors.

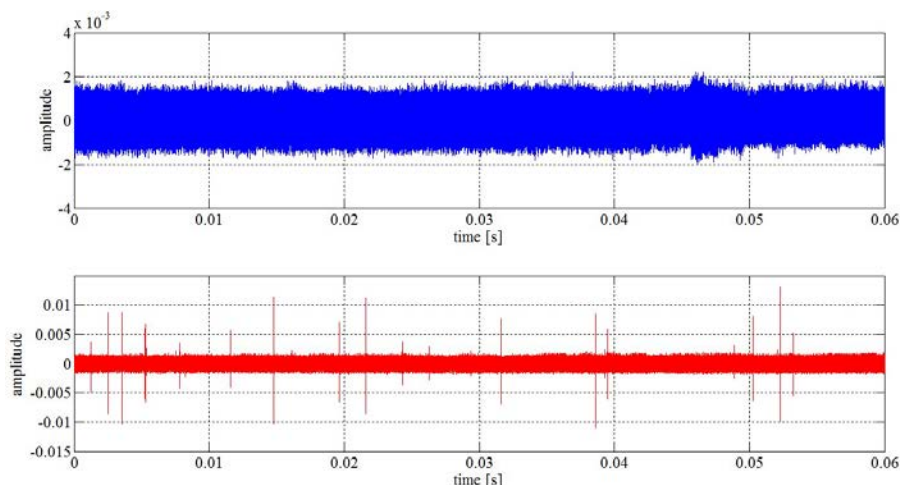


Fig. 3 Škoda Octavia’s (with diesel engine) data in time domain – top is 800 rpm, down is 2000 rpm
Source: authors.

The vehicle’s classification in time the domain is characteristic primarily for vehicles with petrol engines, where detectable are pulses dependent on engine revolutions - ignition. Analysis in the frequency domain shows their ultra-wideband characteristics. It can be appropriate to filter out

petrol vehicles pulses which are compared in the time domain with the diesel common rail ones. For example (Fig. 4) there are pulses of Škoda Octavia with petrol engine in the time domain before and after filtration in frequency band 3 MHz to 6 MHz.

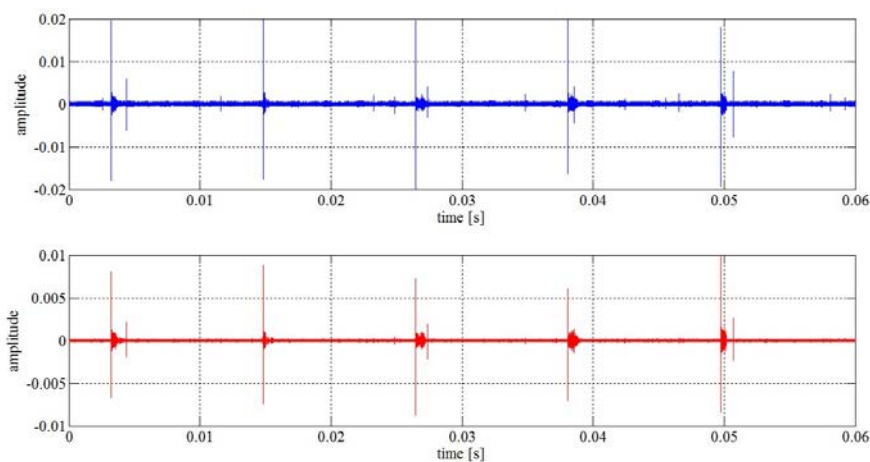


Fig. 4 Škoda Octavia’s (with petrol engine) data in time domain – top is before filtration, down after filtration
Source: authors.

3.2 Analysis in the frequency domain

The characteristic parameters determination of vehicle emitted signals for further classification in the time domain is possible as well as in the frequency domain. We can identify specific frequencies for different vehicle model which depend on particular electronics installed on vehicle board, but are not connected directly with engine type. Main feature of

vehicles with petrol engine is broad-spectrum signals with low levels. Noisy real environment with insufficient signal-to-noise ratio (especially for producers who strictly comply with emissivity regulations) can disrupt frequency characteristics and will lead into low detection probability.

On the other side, vehicles with diesel engine emit signal with a lot of frequency components with sufficient level.

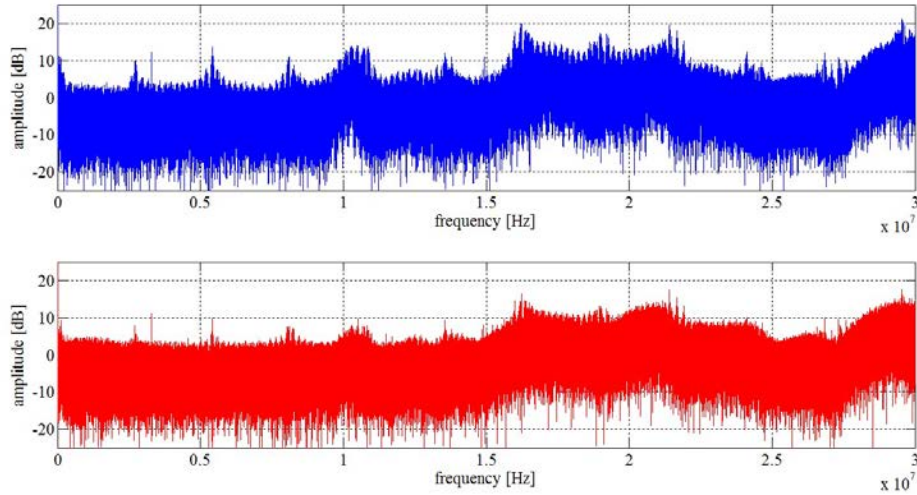


Fig. 5 Fiat 500's data in frequency domain – top is 800 rpm, down is 2000 rpm
Source: authors.

There is amplitude frequency spectrum of Fiat 500's data on Fig. 5. There are some similar frequency spectrums by radio pulse with carrier frequency. With that it is possible to identify frequency ranges in which filtering and detection for particular vehicle can be performed.

For demonstration there are amplitude frequency spectrums of Honda Civic (Fig. 6) with specific frequencies. Fiat 500 and Honda Civic are vehicles with petrol engine, on Fig. 7 there is vehicle with diesel engine.

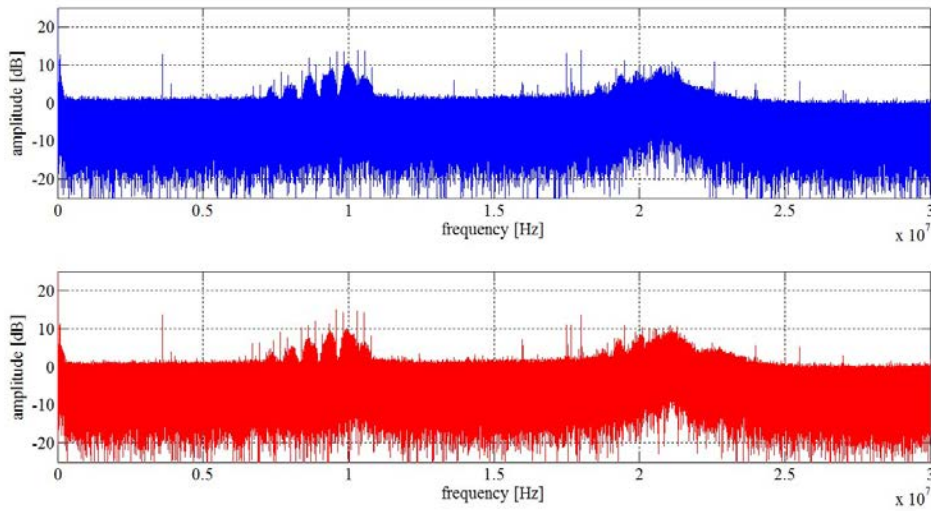


Fig. 6 Honda Civic's data in frequency domain – top is 800 rpm, down is 2000 rpm
Source: authors.

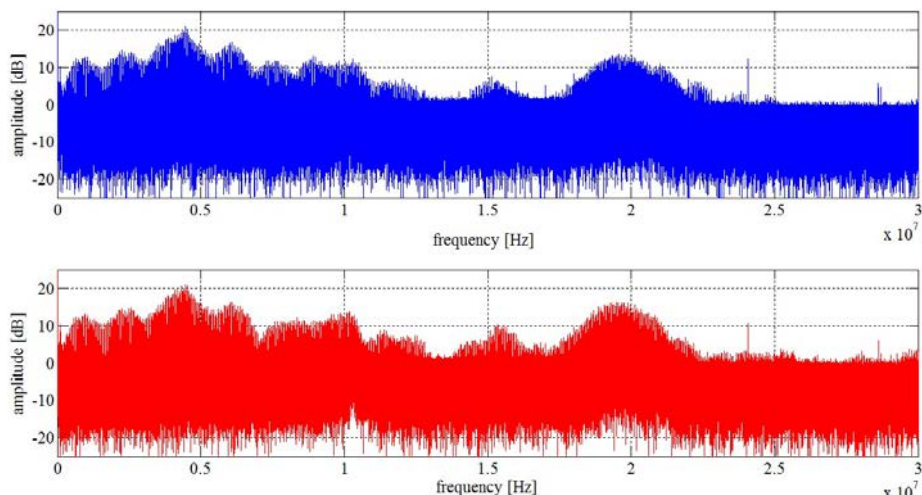


Fig. 7 Škoda Octavia's (with diesel engine) data in frequency domain – top is 800 rpm, down is 2000 rpm
Source: authors.

Tab. 1 Characteristic spectral parameters for analyzed car EMI signals

Vehicle	Frequency								
	Amplitude [dB]								
Ford Focus	6,75 kHz	24,69 kHz	374,3 kHz	469 kHz	748,4 kHz	3,543 MHz	8,5 MHz	10 MHz	11,68 MHz
	11,89	15,69	13,86	13,59	14,78	18,85	9,74	18,11	25,15
Ford Mondeo	24,94 kHz	473,7 kHz	648,2 kHz	3,295 MHz	10,01 MHz	20,81 MHz	21,21 MHz	21,61 MHz	25,36 MHz
	15,79	13,32	12,42	17,86	14,05	18,63	18,93	17,97	8,46
Honda Civic	3,614 MHz	7,416 MHz	7,655 MHz	8,373 MHz	8,613 MHz	8,852 MHz	9,33 MHz	9,569 MHz	
	13,68	6,77	9,2	10,43	10,85	11,95	11,45	15,02	
Fiat 500	5,417 MHz	7,673 MHz	13,57 MHz	14,91 MHz	21,42 MHz	21,52 MHz	26,83 MHz	29,54 MHz	
	10,01	4,242	6,815	6,839	17,48	13,31	9,962	17,63	
Skoda Octavia diesel	480,1 kHz	660,1 kHz	2,36 MHz	4,24 MHz	4,94 MHz	8,5 MHz	9,821 MHz	19,08 MHz	
	10,13	7,145	12,46	19,2	15,81	10,86	11,11	12,66	
Škoda Octavia petrol	4,952 MHz	8,109 MHz	16,1 MHz	17,49 MHz	18 MHz	20,13 MHz	22,17 MHz	24 MHz	
	4,51	10	7,76	14,84	13,3	12	9,01	18,07	
Škoda Yeti	656 kHz	2,416 MHz	4,24 MHz	4,944 MHz	5,408 MHz	5,472 MHz	8,109 MHz	8,8965 MHz	
	7,71	11,6	14,21	13,62	19,16	18,52	9,9994	11,05	

Every vehicle emits some signals carried by specific frequencies with any level. The tab. 1 shows the some dedicated frequencies for vehicles which were measured in the anechoic chamber. We should keep in mind, that characteristic frequencies are relevant for stationary and transient signals too and transient signals are investigated in following paragraph. There are yellow color marked frequencies intended for the detection and the

recognition of each type of vehicle. With that it can type of vehicle. With that it can be possible to makeclassification according to the vehicle manufacturer. For manufacturer Ford there is frequency $3,4 \text{ MHz} \pm 2 \text{ MHz}$ specific for both type of vehicle. For manufacturer Škoda there is frequency $4,5 \text{ MHz} \pm 0,5 \text{ MHz}$, but the signal level for the vehicle with petrol engine is smaller than for vehicles with diesel engine.

3.3 Analysis in the time - frequency domain

For the vehicle classification using the analysis of short non-stationary signals results it is better to specify the frequencies of the signal amplitude which are visible in the time - spectrogram.

Determination of the frequencies amplitude involved on the pulse over the time of pulse duration will lead into diesel – petrol engine and possibly particular car producer fingerprint. Pulse - fingerprint repetition frequency depends on the engine revolutions and some pulses are characteristic for particular vehicle without direct connection to engine revolutions.

Škoda Octavia with petrol engine has wideband pulses dependent on engine revolutions too, but it has a kind of pulses not discovered in the time or frequency domain and independent of engine revolutions. The first kind of pulses (Fig. 8) is emitted at 15,95 MHz and 16,1 MHz and the second kind of pulses (Fig. 9) is emitted at 20 MHz.

Each pulse can be specific for each vehicle; however there are commonalities for the pulses of petrol engines and diesel engines. Pulses, which are connected with engine revolutions, can be examined separately. For example the specific pulse for Honda Civic (the petrol engine) is on Fig. 11 (left side) and specific pulse for Škoda Yeti (the diesel engine) is on Fig. 11 (right side).

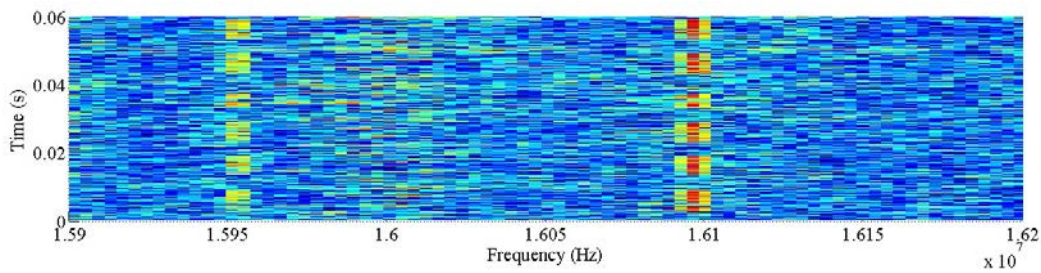


Fig. 8 Škoda Octavia (the petrol engine) specific pulses at 15,95 MHz and 16,1 MHz (800 rpm) after filtration
Source: authors.

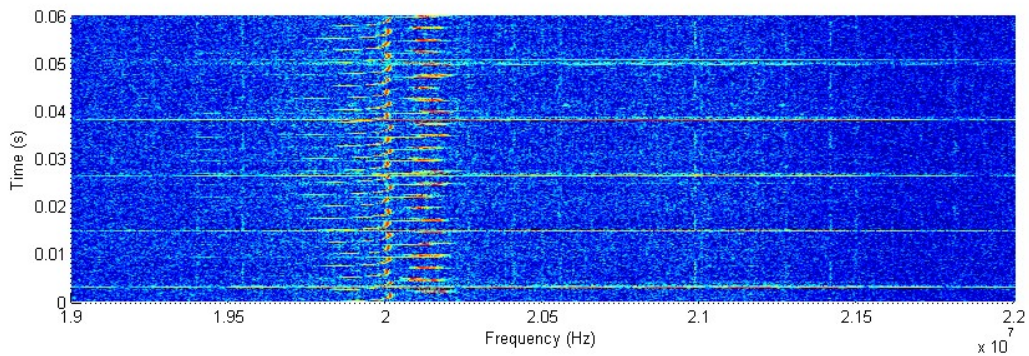


Fig. 9 Škoda Octavia (the petrol engine) specific pulses (2000 rpm) at 20 MHz band after filtration and five ultra-wide band ignition pulses
Source: authors.

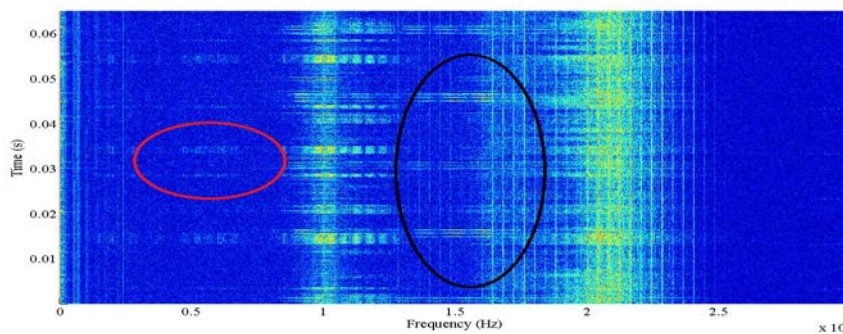


Fig. 10 Ford Mondeo (the diesel engine) spectrogram (2000 rpm) - ultra-wide band injection pulses are in the red circle, additional particular car ultra-wide band pulses in the black circle
Source: authors.

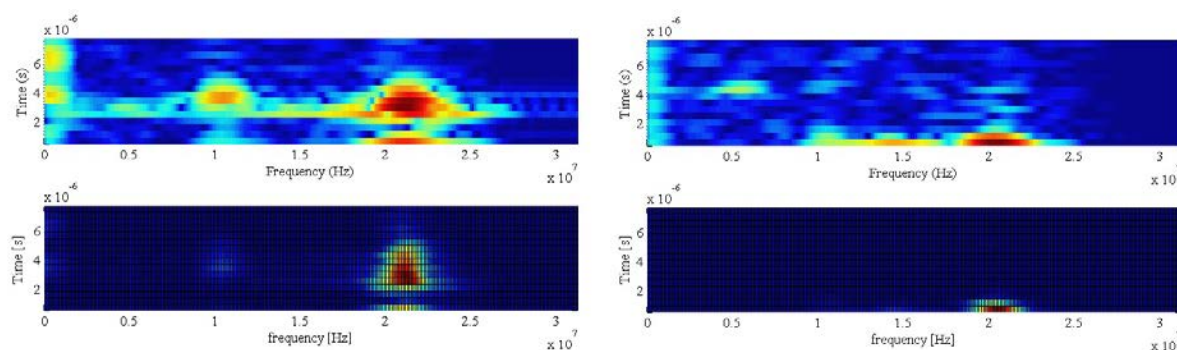


Fig. 11 Honda Civic's (the petrol engine)- up specific pulse dependant on engine revolutions, down statistical fingerprint (left side), Škoda Yeti's (the diesel engine) - up specific pulse dependant on engine revolutions, down statistical fingerprint (right side)

Source: authors.

It is possible to see, there are wideband pulses on these figures, however the pulse of diesel engine is shorter than the pulse of petrol engine, it is narrower in frequency and for common rail engines the burst of particular pulses sequence is always present. Each pulse is finally for recognition purposes represented with fingerprint of the time length $8,2 \mu\text{s}$. It gives us opportunity to compare vehicles.

3.4 Analysis conclusion

As mentioned in previous paragraphs, the largest source of electromagnetic emissivity and transient - short non-stationary signals is the ignition system. Also should be noted, that there are several particular vehicle characteristic stationary signals. These signals are visible in this analysis (Fig. 2, 3, 4). Ignition signal is ultra-wide band signal, for petrol engines single, for diesel (common rail) engine - injection signal it is the burst of mainly 2-3 similar ones, with delay characteristic for particular car producer. It is expected that the recognition of each producer of vehicle and particular model can be based on a combination of the frequency domain characteristics detection and time domain spectrograms formed fingerprints detection and further classification.

4 CONCLUSION

Analysis of personal vehicles electromagnetic emissivity is one of the possible approach for vehicles classification and recognition. There are used four typical vehicles with diesel engine and three typical vehicles with petrol engine. Every vehicle was equipped with specific electronic systems, for the classification purposes of measurement. The analysis was performed in the frequency range of 100 kHz to 35 MHz. Measured data were selectively processed

and evaluated in the time, frequency and time-frequency domain.

For proposed application scenario, with expected recognition time of several tens of milliseconds, selected frequency band and allows vehicle classification according to the type of diesel - petrol engine. Classification and engine revolution speed can be detected with the use of processed spectrogram fingerprints in selected wide frequency bands, very much the same for all producers of common rail diesel engines and very wide bands for petrol ones. The best fitting bands are around 10MHz and 20MHz. The classification according to the vehicle manufacturer is possible with use of detailed frequency matrix detection; however the probability of success in real environment might be low. The classification of a particular type of vehicle is possible in given scenario only in ideal environment. For slow classification purposes (several seconds) one may use emitted narrow band and low level signals from communication means (like CAN bus) and make interpretation of internal code.

Analytical investigation brought the database, which is primarily expected to be used for following automated car recognition. Algorithms for real time use with software defined radio or more robust recognition tool are the following program. Secondly the database of EMI characteristic have some relation to EMS characteristics of the particular car and knowledge will be used for blocking the particular electronics of the vehicle and further stopping the non-cooperative vehicle by electronic means.

Acknowledgement

This work is funded by the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement 285202, "Safe control of non-cooperative vehicles through electromagnetic means" (SAVELEC).

Eng. Vladimír BELÁK
Electronic Department
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: quido23@gmail.com

References

- [1] KODALI, V. P.: *Engineering Electromagnetic Compatibility: Principles, Measurement and technologies*. New York : IEEE PRESS, 1996. 369 p. ISBN 0-7803-1117-5.
- [2] PAUL, C. R.: *Introduction to Electromagnetic Compatibility (2nd edition)*. New Jersey : Wiley-Interscience, 2006. 989 p. ISBN-10-0-471-75500-1.
- [3] OTT, H. V.: *Electromagnetic Compatibility Engineering*. New Jersey : Wiley-Interscience, 2009. 843 p. ISBN 978-0-470-18930-6.
- [4] DENTOM, T.: *Automobile Electrical and Electronic System (3rd edition)*. Oxford : Elsevier Butterworth-Heinemann, 2004. 463 p. ISBN 0 7506 62190.
- [5] ONDRÁČEK, O.: *Signály a systavy*. Bratislava : STU, 1999. ISBN 80-227-1254.
- [6] GAŽOVOVÁ, S. NEBUS, F., BELÁK, V.: Analysis of Vehicles Electromagnetic Emissivity for Vehicles Classification Application. In: *Communication and Information Technologies 8th International Scientific Conference*. Liptovský Mikuláš : Armed Forces Academy of General M. R. Štefánik, 2015. CD-ROM. p. 1-12. ISBN 978-80-8040-508-3.

Eng. Stanislava GAŽOVOVÁ
Electronics Department
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: stana.gazovova@gmail.com

Assoc. Prof. RNDr. František NEBUS, PhD.
Electronics Department
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: frantisek.nebus@aos.sk