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 HARAKAĽ

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

Ľubomír 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.