TEAM 2016

Proceedings of the 8th International Scientific and Expert Conference

19th – 21st October 2016, Trnava, Slovakia
TEAM 2016, Proceedings of the 8th International Scientific and Expert Conference

19th – 21st October 2016, Trnava, Slovakia

Organizers International TEAM Society and Slovak University of Technology, Faculty of Materials Science and Technology in Trnava, Slovakia

All papers are reviewed.

Place of edition: Trnava
Editor: AlumniPress
Year of edition: 2016
Edition: 1st
Pages: 360

Reviewers:
Prof. Ing. Miloš Čambál, CSc.
Prof. Ing. Milan Marônek, CSc.
Assoc. prof. Ing. Mária Dománková, PhD.
Assoc. prof. Krunoslav Mirosavljević, Dr. Sc.

EAN 9788080962371
Honorary Committee

Prof. dr. sc. Dražan Kozak  
Prof. dr. sc. Ivan Samardžić  
Prof. dr. sc. Antun Stoić  
mr. sc. Josip Jukić  
Prof. Dr. Lóránt Kovács  
Prof. Dr. Ing. Jozef Peterka  
Prof. Ing. Jozef Zajac, CSc.  
Prof. dr. sc. Vlado Guberac  
Prof. Dr. Radivoje Mitrović  
Prof. Dr. Aleksandar Sedmak

Scientific Committee

Prof. Zoran Radakovic  
Dr. Vojislav Simonovic  
Dr. Zorana Golubovic  
Prof. Aleksandar Sedmak  
Dr. Nenad Mitrovic  
Dr. Milos Milosevic  
Dr. Sanja Petronic  
Dr. Katarina Colic  
Prof. Snezana Kirin  
Dr. Srdjan Tadic  
Dr. Zsolt Csaba Johanyák  
Dr. Lorant Kovács  
Dr. Erika Török  
Dr. Judit Pető  
Dr. Árpád Ferencz  
Prof. dr. sc. Ivan Samardžić  
Prof. dr. sc. Dražan Kozak  
Prof. dr. sc. Antun Stoić  
Prof. dr. sc. Želiko Ivandić  
Prof. dr. sc. Goran Šimunović  
Prof. dr. sc. Vlado Guberac  
Prof. dr. sc. Sonja Marić  
Prof. dr. sc. Zvonko Antunović  
Prof. dr. sc. Darko Kiš  
Prof. dr. sc. Jasna Šoštarić  
mr. sc. Josip Jukić  
Assoc. prof. dr. sc. Krunoslav Miroslavljević  
dr. sc. Teuta Benković-Lačić  
dipl. Ing. Ivica Lacković  
Milan Stanić  
Prof. Ing. Milan Maroňek, CSc.  
Assoc prof. Ing. Mária Dománková, PhD.  
Prof. Ing. Miloš Čambál, CSc.  
Prof. Ing. Alexander Čaus, DrSc.  
Prof. Ing. Maroš Soldán, PhD.
Prof. Ing. Jozef Zajac, CSc.  Slovakia
Assoc prof. Ing. Ján Piteľ, CSc.  Slovakia
Assoc prof. Ing. Peter Monka, PhD.  Slovakia
Prof. RNDr. Dušan Knežo, CSc.  Slovakia
Dr.hc. prof. Ing. Karol Vasilko, DrSc.  Slovakia
Prof. Ailer Piroska  Hungary
Prof. Nicolae Balc  Romania
Dr. Mislav Balković  Croatia
Dr. Jozef Bártta  Slovakia
Prof. Sladana Benković  Serbia
Prof. Pavel Beňo  Slovakia
Prof. Ivana Bilić  Croatia
Prof. Zlatan Car  Croatia
Prof. Somnath Chattopadhyaya  India
Prof. Robert Čep  Czech Republic
Prof. Ante Ćikić  Croatia
Prof. Dražena Gašpar  Bosnia and Herzegovina
Prof. Nenad Gubeljak  Slovenia
Prof. Fuad Hadžikadunić  Bosnia and Herzegovina
Prof. Sergej Hloch  Slovakia
Prof. Grzegorz Królczyk  Poland
Prof. Leon Kukielka  Poland
Prof. Stanislaw Legutko  Poland
Prof. Marin Milković  Croatia
Prof. Mirjana Pejić Bach  Croatia
Prof. Marko Rakin  Serbia
Prof. Pero Raos  Croatia
Prof. Alessandro Ruggiero  Italia
Prof. Bahar Sennaroğlu  Turkey
Prof. Stevan Stankovski  Serbia
Prof. Mladen Šercer  Croatia
Prof. Udo Trauernigg  Austria
Prof. Vlado Tropša  Croatia
Prof. Nicolae Ungureanu  Romania
Prof. Jan Valíček  Czech Republic
Prof. Djordje Vukelić  Serbia

Organising Committee

Prof. Milan Marônek, PhD.
Ing. Jozef Bártta, PhD. (Chairperson)
Ing. Ivan Buransky, PhD.
Ing. Ingrid Kovaříková, PhD.
Ing. Beáta Šimeková, PhD.
Ing. Martin Bajčičák, PhD.
Assoc. Prof. Erika Hodúlová, PhD.
Prof. Koloman Ulrich, PhD.
PhDr. Kvetoslava Rešetová, PhD.
PaedDr. Dáša Zifčáková
CONTENT

TECHNICS SECTION
Using the Ant Colony Optimization method to find an optimal solution in drilling process............. 8
Numerical examination of a system model with a nonlinear component........................................... 12
Distributed congestion detection and classification method for the analysis of velocity......................... 17
Development of the Lower Body of Assistive Humanoid Robot MARKO .............................................. 23
Optimization of Planetary Gear Trains with Spur, Helical and Double Helical Gears ......................... 29
Optimal Synthesis of the Loader Bucket Mechanism ........................................................................... 35
Analysis of the Mechanism of Complex Structures with High Class Kinematic Group ......................... 41
Investigation of Ultrasonic Assisted Milling of Nickel Alloy Monel .................................................... 47
Influence of selected parameters on the machining of sintered carbide by WEDM ............................... 53
Review of Anomaly-Based IDS Algorithms ......................................................................................... 58
Survey on SDN Programming Languages ............................................................................................ 64
Chip formation mechanizm during composite materials machining...................................................... 71
Estimation of statistical parameters of electric appliances based on environmental measurements ...... 75
Manufacturing of Twist-Free Surfaces by MAM Technologies ............................................................... 79
Coefficient of friction in the design of non-metallic brittle interference fit parts ................................. 84
Control system design of the parallel kinematics mechatronic press ..................................................... 88
Comparison of laser beam cutting and milling of plastics materials made from PMMA focusing on mechanical properties of the material................................................................. 94
Statistical process control in the gear wheel manufacturing .................................................................. 99
Cutting analysis of CFRP composites ..................................................................................................... 107
Development of On-line monitoring system for monitoring main welding parameters ...................... 111
Dilatometric testing of maraging steel ................................................................................................. 118
Design and calculation of cylindrical industrial air filter device with use of CFD analysis .............. 124
Equalization of stress distribution on threaded connection optimizing pitch geometry .................... 134
Influence of the mini - dental implants diameter on stress in the surrounding bone ....................... 141
The impact of cutting speed and pressure on surface quality during plasma cutting ..................... 147
Finite Elements Investigation of Laser Welding in a keyhole Mode ....................................................... 151
A Study of Laser Sheet Bending with Finite Elements Method ............................................................. 155
Structural integrity assessment of a pressure vessel ............................................................................ 160
Risk based management of pressure equipment safety ....................................................................... 165
Procedures and evaluation of the stress strain fields on the Locking Compression Plates .................... 171
Hardness and metallographic tests of repaired starting vessel used in thermal power plant tent B .......... 180
The influence of electron beam welding process on properties of superduplex stainless steel S32507 weld joints ............................................................. 185
Wizardry of water – ram pump ......................................................... 190
Development and construction of machine for fused deposition modeling ............................................. 195
Numerical simulation of metal cutting using the software DEFORM 2D ............................................. 201
Kerf Variation Analysing After Cutting With Abrasive Water Jet of a Steel Part ..................................... 211
Experimental determination of Tensile Strain-Hardening Exponent and Strength Coefficient of the S355J2+N steel grade ........................................................................... 218
Specifics of the possible applications of polyester laminates considering mechanical properties ...... 224
Design, 3d model and calculation of pelleting machine ............................................................................ 229
Selecting Image Feature Points Based on the Object Contour Curvature ........................................... 237
Design of polymeric electrolyte membrane reformer ............................................................................. 241
Initial Sensitivity Analysis of Packed-bed Methanol Steam Reforming Reactor ...................................... 245
Structural Integrity Assessment of a Pressure Vessel ............................................................................. 251
Flat Die Sliding Model with Variable Contact Pressure in Deep Drawing Process ................................ 255
Thermal Analysis of Packed-bed Methanol Steam Reforming Reactor ................................................... 259

EDUCATION SECTION
The difference in somatotype between football and not football players .................................................. 263
Effectiveness indicators and ensuring conditions in dual training ......................................................... 268
Functions associated with the weighted mean and median .................................................................... 275
Overdetermined systems of linear equations .......................................................................................... 280
Optimal nuber of clusters provided by K-means and E-M algorithm ...................................................... 286

AGRICULTURE SECTION
Comparative analysis of features in computer vision for apple quality monitoring ................................ 292
Ambrosia artemisiifolia allelochemicals and relationship to pollen allergy with air pollution ............... 297
Weed control of potato with herbicide containing the active substance metribuzin .................................. 302
Economic evaluation of different technology in the corn growing in Hungary .................................... 307
Effect of nitrogen on the growth and ingredients of celery .................................................................... 312
Familiarity of Honey Products in Slavonski Brod .................................................................................. 317

MANAGEMENT SECTION
Financial analysis – indicator of business success ................................................................................ 322
The impact of the economic crisis on youth leaving Croatia ................................................................. 326
Youth Entrepreneurship ......................................................................................................................... 330
Emotional intelligence in business ................................................................. 334
Importance of managing communication process in crisis situations ..................... 338
Diversification as growth strategy for small enterprises ...................................... 344
Company size and employee training: Case of Vojvodina Manufacturing Industry .......... 350
Is Economy of Vojvodina ready for joining EU ? ............................................ 355
Review of Anomaly-Based IDS Algorithms

László Göcsa, Zsolt Csaba Johanyák, Szilveszter Kovácsb

a Department of Information Technology, Pallas Athena University, GAMF Faculty of Engineering and Computer Science, Kecskemét, H-6001 Pf. 91, {gocs.laszlo, johanyak.csaba}@gamf.kefo.hu

b Department of Information Technology, University of Miskolc, Miskolc-Egyetemváros, Miskolc, H-3515, Hungary, szkovacs@iit.uni-miskolc.hu

Abstract

Intrusion detection systems (IDSs) can provide an effective solution for the information security needs of a company. Well configured IDSs are able to automatically recognize attacks that target either networks or hosts. IDSs can be categorized based on different aspects or properties. The intrusion detection approach is one of the most important properties of the IDS algorithms. Based on it one can identify signature based and behaviour based solutions. While the signature based approach tries to recognize attacks by using a database of known attack signatures, the behaviour based one first learns the normal behaviour of the supervised system and after finishing the learning process tries to identify anomalies, i.e. significant deviations from the normal behaviour.

In this paper, after presenting the main ideas of the functioning of behaviour based IDSs we do a survey on the currently most important anomaly detection types. Thus key features of statistical based, knowledge based, and computational intelligence based techniques are introduced. In the latter case methods applying fuzzy logic, neural networks, and clustering are described as well. Advantageous and disadvantageous features of the different approaches are also presented.

Keywords: information security, signature based IDS, behaviour based IDS, Anomaly-Based IDS, fuzzy logic, neural networks, clustering.

1. INTRODUCTION

An intrusion detection system (IDS) is a software or hardware solution that automates the monitoring and analysis of the network traffic and user activities to strengthen the security of an information system. The intrusion detection consists of two basic processes, i.e. monitoring the underlying system activities and analysing the resulting log data [1]. Generally, IDSs can be classified into two types based on the considered information source, i.e. Host based Intrusion Detection Systems (HIDS) and Network based Intrusion Detection Systems (NIDS) [2]. While members of the first group mainly work with local (operating system related) information IDSs belonging to the second group monitor network related events. This paper focuses on the latter type.

An NIDS contains one or more sensors connected to network interface cards that acquire information about network traffic volume, used protocols, source and destination IP addresses, service ports, etc. [7]. This IDS type usually is deployed in a segment or on the border of a network, and mainly investigates the network traffic. Usually it is capable to monitor and protect several systems and devices.

The type of the applied analysis is the most important aspect taken into consideration for the categorization of NIDSs. Conform to it one can
identify anomaly detection and signature detection based IDSs [3].

![Intrusion Detection Approach](image1)

**Fig. 1. Categorization of IDSs based on the applied analysis**

While signature based IDS solutions look for the existence of known patterns or signatures the anomaly detection technics compare the actual behaviour of the system to its estimated “normal” behaviour. The advantage of the latter approach lies in the potential capability to recognize new intrusion types [7]. Being an intensively investigated and developing area our paper focuses on the anomaly detection based approaches.

The rest of this paper is organized as follows. Section 2 presents the main ideas of anomaly based IDSs as well as the three main subtypes. Section 3 is entirely dedicated to the computational intelligence based BIDSs.

2. ANOMALY DETECTION BASED IDSs

Although there are some differences between the anomaly detection based IDS (also called Behavior based IDSs - BIDS) subtypes but generally they can function on two different modes (see Fig. 2). In case of the training mode the system is fed with sensor data that describes the typical (normal) network and user behaviour. This input is transformed and formalized into the so called normal behaviour profiles by the parameterization module. Based on these profiles the training module creates a normal behavioural model for the network automatically, manually or in a combined way. Next, the BIDS is switched into the detection mode when it is used for its main purpose, i.e. the strengthening of the network security.

In the detection mode the actual sensor data is converted into actual profile by the parameterization module and the detection module compares it with the previously created model. Based on the acquired knowledge the detection module strives to determine whether the analysed activity is harmful to the system or not.

![BIDS functional architecture](image2)

**Fig. 2. BIDS functional architecture [7]**

BIDSs create statistics for the logon time, the time a user was logged in, the usually accessed files, as well as for the frequency of the modification and movement of these files, etc. The advantage of the anomaly based approach is its fast and dynamic adaptation capability to unknown attack types.

The disadvantage of BIDSs is that they alert the administrator and take counter measures more often than knowledge-based IDSs due to their high rate of false alarms [9]. Additionally, a BIDS is less efficient in case of systems whose behaviour pattern is not static enough for the creation of statistics or in case of systems where user activity is not monotonous. One has to take extra precautions in course of the learning period to avoid the possibility of “learning” an actual intrusion as a normal behaviour [4].

BIDSs can be classified into three main categories based on the data processing mode, i.e. statistical based, knowledge based, and computational intelligence based. The following three subsections describe them briefly.

2.1. Statistical based BIDSs

Statistical based BIDSs monitor the network traffic, examine the communication speed, the used protocols and IP addresses focusing on the differences from the allowed values. It examines the current profile by comparing it to the normal profile. If an anomaly occurs in the network the anomaly measure is also calculated. If it exceeds a predefined threshold an alarm is activated.
This IDS type follows different activities and creates reports about malicious activities using statistical methods. Its shortcoming is its relative high rate of categorizing an attack occurring in course of the normal traffic as a normal activity [5].

2.2 Knowledge based BIDSs

Knowledge based BIDSs work with a database containing information about previous attacks. It is decided based on this samples whether the monitored activity is categorized as a hostile one or not. Actually this is the most used BIDS model. Its advantage is that it blacklists mistakenly significantly less traffic than the other approaches. Furthermore, in almost all of the cases it uses standard alerts that are easily understandable for system administrators. However, its demand on continuous update and maintenance of the sample database can be considered as a drawback. Moreover, this type of IDS cannot recognize new attack types. This shortcoming can result in whitelisting a new, previously unknown attack type and allowing it access to the system.

2.3 Computational Intelligence based BIDSs

Computational intelligence (CI) based BIDSs can recognize and define rules and regularities independently or with human help based on sample data. They not only learn samples but also became capable of making decisions on their own in case of previously unseen data. CI based BIDSs also use statistical analysis techniques to improve their performance. However, they usually require big computational resources owing to the huge amount of data to be processed.

3. COMPUTATIONAL INTELLIGENCE BASED BIDS APPROACHES

Computational Intelligence (CI) comprises a family of nature inspired heuristics methods that support various calculations related to artificial intelligence tasks [8]. Frequently used tools from this family are fuzzy logic, artificial neural networks as well as clustering and several optimization techniques. In this section, three CI based BIDS approaches are presented, namely artificial neural networks, fuzzy logic and clustering based BIDSs.

3.1 Artificial Neural Network

ANNs are the most commonly used soft computing technique in IDSs. An ANN is a processing system that is inspired by the biological nervous systems. It is composed of a large number of highly interconnected processing elements (called neurons) that are working together to solve specific problems. Each neuron is basically a summing element followed by an activation function.

Some IDS designers apply ANN as a pattern recognition technique [20]. Pattern recognition can be implemented for example by using a feed-forward neural network that has been trained with a sample data set. When the initial training process of the neural network is finished the ANN identifies the current input pattern and it outputs the corresponding class. In case of the lack of an exact match the neural network gives an output, which corresponds to the known input pattern that is the least different one from the given pattern [17].

For example Kukielska and Kotulski [18] proposed a distributed IDS system having three modules, i.e. the central module, the Net-LAN monitor and the H&N monitor. While the two monitors analize host log data and network data respectively, the central module is responsible for alerting the end user and retraining the system with new data vectors.

Ryan et al. presented anomaly neural network based intrusion detection system called NNID [21] of which presumption was that the user leaves a “print” when using a computer system. This “print” is described as a feature vector that contains among others the connections of a single user during a whole day and information
regarding the 100 most important commands they used. The vector can be learned by an ANN and so later the ANN can identify the current user. If the actual behaviour does not match the “print” a possible intrusion is in progress and the system administrator is alerted. NNID applied backpropagation ANN and achieved an accuracy of 96%

### 3.2 Fuzzy logic

Although on the surface there are always exact facts and numerical data the process of intrusion detection has to deal with vague boundaries between normal behaviour and anomalies. Besides being able to handle the inherent vagueness fuzzy logic based solutions also provide a self-explaining capability that can be a useful characteristic when analysing their functioning. Furthermore, they can easily incorporate human expert knowledge expressed in form of IF-THEN rules (see Fig. 4.).

```plaintext
IF unusual_connection_count is high AND
destination_host_count is high AND
observed_service_port_count is medium_low THEN
service_scan_possibility is high
```

Fig. 4. Example rule for the detection of a host scan on a given port aiming the identification of a server

There are several possible application areas for the fuzzy approach in the field of intrusion detection. For example Bridges et al. [12] proposed a system that in the training phase creates a fuzzy normal behaviour profile from intrusion free log data using data mining techniques and by creating fuzzy association rules. Later in the detection phase new association rules are created from the actual log data and the decision is made based on a similarity assessment. Anomaly detection can also be viewed as an outlier detection (exception mining) problem where the outlier points represent abnormal behaviour, i.e. a possible attack against the protected system.

Chimplee et al. [13] used fuzzy c-means clustering for the identification of intrusion attempts. They applied correlation analysis based feature selection in order to reduce the dimensionality of the problem. The fuzzy concept can find application at a higher level as well. Decision fusion can employ fuzzy logic (e.g. [14]) for making a final decision when more than one different techniques are used for intrusion identification purposes.

### 3.3 Clustering and identification of outliers

The goal of cluster analysis is to identify groups of objects in such a way that group members are more similar (close) to each other than to members of other groups. [11]. An outlier is an object that is distant from other objects and is not considered as member of any clusters. It can arise as a result of some kind of anomaly, which presents a potential applicability in intrusion system development.

![Fig. 5 Cluster and outliers](image)

Scherer et al. [15] investigated the usage of Farthest First Traversal (FFT), K-means and COBWEB/CLASSIT algorithms for clustering and support vector machine (SVM) for classification. Taking into consideration different attack types K-means based clustering ensured the best average results.

### 4. CONCLUSIONS

Intrusion detection systems have become a very important component of the defence systems of individual computers and computer networks facing various threats of malicious activities. Although the IDS technology has a long history with several approaches and solutions this field is in continuous development.

This paper presented a survey on a main category of IDSs, i.e. anomaly based intrusion detection approaches. Depending on the applied data processing mode three main BIDS categories were identified. Beside the classical
solutions the computational intelligence based approach has gained more and more attention recently. Here fuzzy logic and artificial neural networks proved to be two straightforward options especially due to the proper hardware resource ensured by the current devices.

5. ACKNOWLEDGEMENTS

This research was supported by the Foundation for the Development of Automation in Machinery Industry.

6. REFERENCES


[5] Davood Kheyri, Mojtaba Karami: “A Comprehensive Survey on Anomaly-Based Intrusion Detection in MANET”, Published by Canadian Center of Science and Education, Computer and Information Science; Vol. 5, No. 4; 2012, ISSN 1913-8989 E-ISSN 1913-8997


[10] SANS Institute InfoSec Reading Room: „Application of Neural Networks to Intrusion Detection”, SANS Institute, 2001


