Received: January 24, 2018

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

An Intrusion Detection System for Network Security Situational Awareness Using Conditional Random Fields

Azhagiri Mahendiran[1]* **Rajesh Appusamy**[2]

[1]*Department of Computer Science and Engineering, St.Peter's Institute of Higher Education and Research, Chennai, Tamilnadu, Pincode 600054, India*
[2]*Department of Computer Science and Engineering, C.Abdul Hakeem College of Engineering and Technology, Melvisharam, Tamilnadu, Pincode 632509, India*
* Corresponding author's Email: azhagiri1687@gmail.com

Abstract: The huge proliferation of cyber economy, social media usage and online transactions has resulted in large volumes of data in the cyber space. This has led to an increase in concern over the security of confidential data in the cyber space. Network security situational awareness systems helps in effectively monitoring a network for suspicious activities and thwarting any attacks on the information stored in the network. In this paper, an intrusion detection system for network security situational awareness using conditional random field has been proposed. Conditional random fields being conditional models are capable of modeling inter relationships between the observed features. This results in greater accuracy in classification. Conditional random field's complexity increases with the number of features in the observation. To reduce this complexity, a feature selection method using oneR algorithm has been proposed. The ability of oneR algorithm to find the best attribute that result in optimal classification has been used for ranking the features in the observation. The proposed system was trained and tested using the bench mark NSL-KDD dataset. The proposed system on experimentation, exhibited higher accuracy (98%) in identifying an attack in general and also showed better performance (>93%) in identifying individual attack categories specifically.

Keywords: Network security situational awareness (NSSA), Intrusion detection system (IDS), Network security, Intelligent systems, Conditional random fields.

1. Introduction

Situational awareness in terms of military combat operations means "the ability to identify, process, and comprehend the critical elements of information about what is happening to the team with regards to the mission" [1]. In terms of computer networks, it is the ability to assess the current state of a network i.e. identify any malicious activities in the network by means of very concise and accurate information provided by various sensors at different levels of the network [2]. This is not a trivial task considering the volume of traffic found on any kind of network and the increase in sophistication of the kind of attacks experienced by these networks.

The functional requirements of Situational Awareness in Computer Network Security can be described at four different levels as in [3]:

- Perception – involves acquiring information such as security alerts from intrusion detection systems, firewall logs, scan reports along with their timing and source information. It also involves classifying the acquired information into appropriate representations for the comprehension, projection and resolution levels.
- Comprehension – involves techniques used to analyze, synthesize, correlate and determine the relevance of the evidences received from the perception level.
- Projection – predict future events based on the information received from the higher levels.

DOI: 10.22266/ijies2018.0630.21

- Resolution – actions required to address a security event when it happens.

As can be seen from the functional requirements, one of the main sources of information of malicious activity in a network is the "Intrusion Detection System (IDS)" deployed over the network. Intrusion detection is the process of identifying activities on a network that are violating the security policies of the network [4]. Intrusions tend to destabilize the network security, there by affecting the integrity, confidentiality of the information on the network and preventing accessibility of the information sources on the network [5, 6, 7]. Improving the effectiveness and accuracy of IDS will help in better Network Security Situational Awareness (NSSA). To meet this end, the focus of this research is to develop an IDS that is capable of detecting accurately the various attack categories so that it can be an effectively used in a NSSA system.

Our contributions in this research,

- The development of an IDS using Conditional Random Field (CRF), capable of detecting various attack categories with high accuracy.
- The development of a feature selection method using oneR mining algorithm for selecting optimal features that help in increasing the operational efficiency of CRF.

One of the systems in the literature [8] also uses CRF to detect attacks. The differences between their system and our proposed system are as follows:

- The system in [8] uses 4 layers of binary CRF classifier each capable of predicting one of the 4 attack categories whereas our system comprises of a single multi class CRF classifier capable of predicting all 4 attack categories.
- The system in [8] uses manual feature selection whereas our system uses an automatic feature selection method.

The rest of the paper is organized as follows: Section 2 describes several state of the art IDS in the literature. Section 3 gives an introduction to conditional random field. Section 4 explains the proposed system. Section 5 discusses the results obtained by the proposed system and Section 6 concludes this research.

2. Related work

In this section we have given a brief discussion about some of the more prominent IDS researched in the literature.

In [8] the authors have proposed a layered approach for intrusion detection using conditional random fields. The conditional random field helps in achieving high accuracy and layered approach helps in improving the efficiency of the detection process. The authors have conducted statistical tests to prove the higher detection accuracy of their method.

In [9] the authors propose a Multi-class SVM (Support Vector Machine) to detect intrusions along with Multi-Linear Dimensionality Reduction (ML-DR) process to reduce the feature dimensions there by reducing the training time.

In [10] the authors have used Synthetic Minority Oversampling Technique (SMOTE) to balance the dataset and eliminate the skewness of the class distribution. They have used the K-NN clustering technique along with Gower metric to handle mixed data in the dataset.

In [11] the authors have proposed a multiclass modeling technique using multiclass support vector machine to identify the various attacks on a network. They have also used the chi-square feature selection method to reduce the dimensionality of the dataset and choose appropriate attributes for building the model.

In [12] the authors have used a fuzzy based semi-supervised learning approach for IDS. The semi-supervised approach helped in efficiently utilizing the unlabeled samples with supervised learning algorithm to improve the performance of the IDS. A single hidden layer feed forward neural network is used for building the model. In the first stage, the unlabelled samples are categorized using a fuzzy quantification process. The neural network is then retrained by incorporating each of these categories separately into the original training set.

In [13] an anomaly based network intrusion system has been explored. The authors have proposed a meta-heuristic assessment model using feature correlation analysis and association impact scale to predict intrusions. The authors found that feature correlation significantly minimized the computational time of measuring association impact.

In [14] a multi-level hybrid intrusion detection model using support vector machine and extreme learning machine is proposed. The authors have also come up with a modified K means algorithm to significantly improve the quality of the training dataset. This high quality training dataset has led to reduction in training time of the classifiers and also resulted in improved performance of the IDS.

In [15] a modified optimum path forest algorithm [OPF] is used for detecting intrusions. The authors have used k-means clustering algorithm to partition the training samples into homogeneous training subsets. This has resulted in improved scalability, accuracy, detection rate, false alarm rate and execution time than traditional OPF.

In [16] the authors propose a fuzzy membership function which reduces considerably the computational complexity of the intrusion detection process and at the same increases the accuracies of the classifier algorithms.

In [17] an anomaly based intrusion detection system using hierarchically structured learning automata has been proposed. Learning automata learns to choose the optimal action through repeated interactions with the environment. Usage of the learning automata results in a highly resilient approach that excels in detecting unknown attacks.

In [18] the authors propose a hybrid feature selection method for intrusion detection. In the proposed approach the authors have used binary gravitational search algorithm with mutual information based filter for pruning the subset of features. The search direction is controlled using a two objective fitness function to maximize detection rate and minimizing false positive rate. This enhanced the accuracy and detection rate compared to other wrapper based and filter based methods.

In [19] a hybrid approach integrating evolutionary algorithm with neural networks has been proposed. The authors have come up with two hybrids - gravitational search and gravitational search along with particle swarm optimization to train artificial neural networks. They have shown that these hybrid approaches have out run traditional IDS.

In [20] an entropy based feature selection method has been used with layered classifier based on fuzzy rules generated by a layered fuzzy control language. It was found that the layered classifier improved performance and reduced classification time.

In [21] a novel two tier classifier employing naïve bayes classifier and KNN classifier as component has been proposed. Linear Discriminant Analysis has been used for dimensionality reduction. On experimentation the system exhibited considerable gain in detection rate and false alarm compared to other models.

One of the major drawback seen in the existing systems with respect to the requirements of NSSA was that their overall attack detection rate was good but the accurate categorization of the detected attack type was not uniform (Table 8).

Since one of the functional requirements of an NSSA system is to initiate actions required to address a security event when it happens [3], the IDS part of it should be capable of accurately detecting the various attack categories uniformly.

Hence, we have focused in this article, in designing an IDS capable of identifying the various attack categories with high accuracy. The following section gives a brief review of CRF.

3. Conditional random fields

CRF is a conditional model that models conditional distributions over a set of random variables. They can be described as in [22] as follows:

X – Random variable over data sequence to be labeled
Y – Label sequence
G – A graph defined as, $G = (V,E)$

Let $Y = (Y_v)_{v\epsilon(V)}$ i.e. Y is indexed by the vertices of G. (X,Y) is a CRF if when conditioned on X, the random variables Y_v obey the Markov property with respect to the graph:

$p(Y_v \mid X, Y_w, w \neq v) = p(Y_v \mid X, Y_w, w \sim v)$, where $w \sim v$ means w and v are neighbors in G.

The joint distribution over the label sequence Y given X for a simple sequential (chain) modeling has the form,

$$p(y|x) \propto exp\left(\sum_{e\in E,k} \lambda_k f_k(e, y|_e, x) + \sum_{v\epsilon V,k} \mu_k g_k(v, y|_v, x)\right) \quad (1)$$

where,

x – data sequence
y – label sequence
$y|_S$ – set of components of y associated with the vertices in sub graph S

4. The proposed system

In the proposed system, we have used the linear chain CRF model (Fig. 1) to classify the connections as either normal or one of the attack categories. In Fig. 1, the observations are the connection features and the labels are “dos”, “u2r”, “r2l”, “probe” and “normal” respectively. We have used the R [26, 27] and weka [28] tools to perform our experimentations. The weka tool was used for performing feature selection and R tool was used for building and testing the classifier.

We have used KDDTrain+ data from the NSL-KDD dataset [23] for our experimentation. The NSL-KDD dataset is an improved version obtained by eliminating some of the problems in KDDcup99 dataset as identified in [24]. The KDDTraint+ data contains 125,973 records of simulated connection information labeled as either normal or a particular type of attack. The data contains records of 22 attack types along with the normal records. The attack

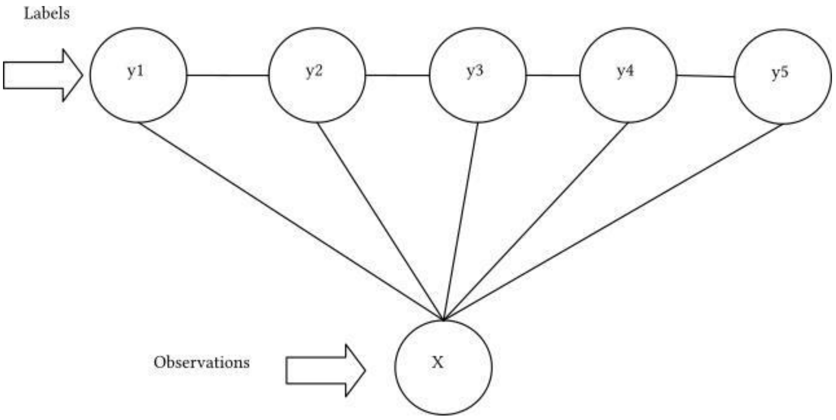

Figure.1 Graphical representation of linear chain CRF

Table 1. Features in the NSL-KDD dataset

Sr. No	Feature Name
1	Duration
2	Protocol_type
3	Service
4	Flag
5	Src_bytes
6	Dst_bytes
7	Land
8	Wrong_fragment
9	Urgent
10	Hot
11	Num_failed_logins
12	Logged_in
13	Num_compromised
14	Root_shell
15	Su_attempted
16	Num_root
17	Num_file_creations
18	Num_shells
19	Num_access_files
20	Num_outbound_cmds
21	Is_host_login
22	Is_guest_login
23	Count
24	Srv_count
25	Serror_rate
26	Srv_serror_rate
27	Rerror_rate
28	Srv_rerror_rate
29	Same_srv_rate
30	Diff_srv_rate
31	Srv_diff_host_rate
32	Dst_host_count
33	Dst_host_srv_count
34	Dst_host_same_srv_rate
35	Dst_host_diff_srv_rate
36	Dst_host_same_src_port_rate
37	Dst_host_srv_diff_host_rate
38	Dst_host_serror_rate
39	Dst_host_srv_serror_rate
40	Dst_host_rerror_rate
41	Dst_host_srv_rerror_rate

types can be grouped into one of the following four main attack categories:

· DOS: denial-of-service, e.g. syn flood;

· R2L: unauthorized access from a remote machine, e.g. guessing password;

· U2R: unauthorized access to local superuser (root) privileges, e.g., various ``buffer overflow" attacks;

· Probing: surveillance and other probing, e.g., port scanning.

Each record in the dataset contains the 41 features listed in Table 1 along with the label.

To build and test our proposed system, we have taken a sample of 12654 records (approx. 10%) of the KDDTrain+ data with the attack/normal data distribution as in Table 2.

Since, the R tools CRF implementation works only with numerical input, all the nominal features in the dataset was converted to numeric type by replacing their nominal values with their respective levels. Once all the features were converted to numeric types, they were then normalized. The normalized dataset was then used to train and test our proposed system.

The complexity of CRF is proportional to the length of the observation sequence (i.e. number of features) and the number of labels used [8]. Since the number of labels used in the intrusion detection problem is fixed i.e. 5, the problem complexity varies significantly with the length of the observation sequence.

In order to reduce the operational complexity, and increase the performance and accuracy of the proposed system we have employed feature selection to reduce the length of the observation sequence. We have used OneR algorithm [25] to select the most appropriate features for classifying the connections as attack or normal. OneR is basically a single level decision tree that chooses a

Table 2. Characteristics of the sample KDDTrain+ dataset used for the experimentation

Dos	Normal	Probe	R2l	U2r
4596	6735	1168	103	52

Table 3. Ranking of the Features of the KDDTrain+ dataset

Rank	Feature
1	src_bytes
2	service
3	diff_srv_rate
4	flag
5	hot
6	same_srv_rate
7	dst_host_diff_srv_rate
8	srv_serror_rate
9	dst_host_srv_serror_rate
10	serror_rate
11	dst_host_same_srv_rate
12	dst_host_serror_rate
13	root_shell
14	dst_host_srv_count
15	dst_host_srv_diff_host_rate
16	duration
17	count
18	num_file_creations
19	num_compromised
20	dst_host_srv_rerror_rate
21	is_guest_login
22	dst_bytes
23	dst_host_same_src_port_rate
24	protocol_type
25	rerror_rate
26	dst_host_count
27	srv_rerror_rate
28	num_root
29	num_shells
30	dst_host_rerror_rate
31	wrong_fragment
32	urgent
33	num_access_files
34	su_attempted
35	logged_in
36	num_failed_logins
37	srv_count
38	X1
39	srv_diff_host_rate

Table 4. Detection details of the different attack categories of the proposed system

Attacks	Dos	U2r	R2l	Probe	Normal
Dos	4505	0	0	0	91
U2r	0	48	2	0	2
R2l	0	0	99	0	4
Probe	15	0	0	1128	25
Normal	59	3	3	30	6640

Table 5. Classification statistics of the proposed system

Total Records	12654
Correctly Classified	12420
Wrongly Classified	234
Accuracy	98.15

Table 6. Precision, Recall and F-measure of the proposed system

Attacks	Precision	Recall	F-measure
Dos	98.38	98.02	98.20
U2r	94.11	92.30	93.20
R2l	95.19	96.11	95.65
Probe	97.40	96.57	96.99
Normal	98.19	98.58	98.39

single feature that optimally discriminates between the classes.

The 41 features describing the connection were ranked using the OneR algorithm (Table 3). The optimal subset of features was identified by iteratively picking features from the rank list, building a classification model using a subset of the original dataset and testing its accuracy (Fig. 2). In our experimentation it was found that the first 24 features in the feature rank list (Table 3) resulted in optimal classification of the connections.

The selected features of the dataset were then used as the observation sequence and the CRF was trained. We have used 10-fold cross validation to train and test the dataset.

5. Results and discussion

The confusion matrix of our experimentation is shown in Table 4. The overall accuracy of our proposed system is shown in Table 5. The precision, recall and f-measure obtained by our proposed system for each of the connection types are shown in Table 6. It can be seen from the results obtained that the proposed system is capable of detecting the different attack categories individually with good accuracy (>92%) as well as exhibits good overall attack detection accuracy (98.15%).

Tables 7 and 8 and Fig. 3 show the performance comparison of the proposed system with some of the state of the art IDS in the literature. It can be seen from the comparisons that the proposed system exhibits superior performance in terms of both individual attack category detection as well as overall attack detection.

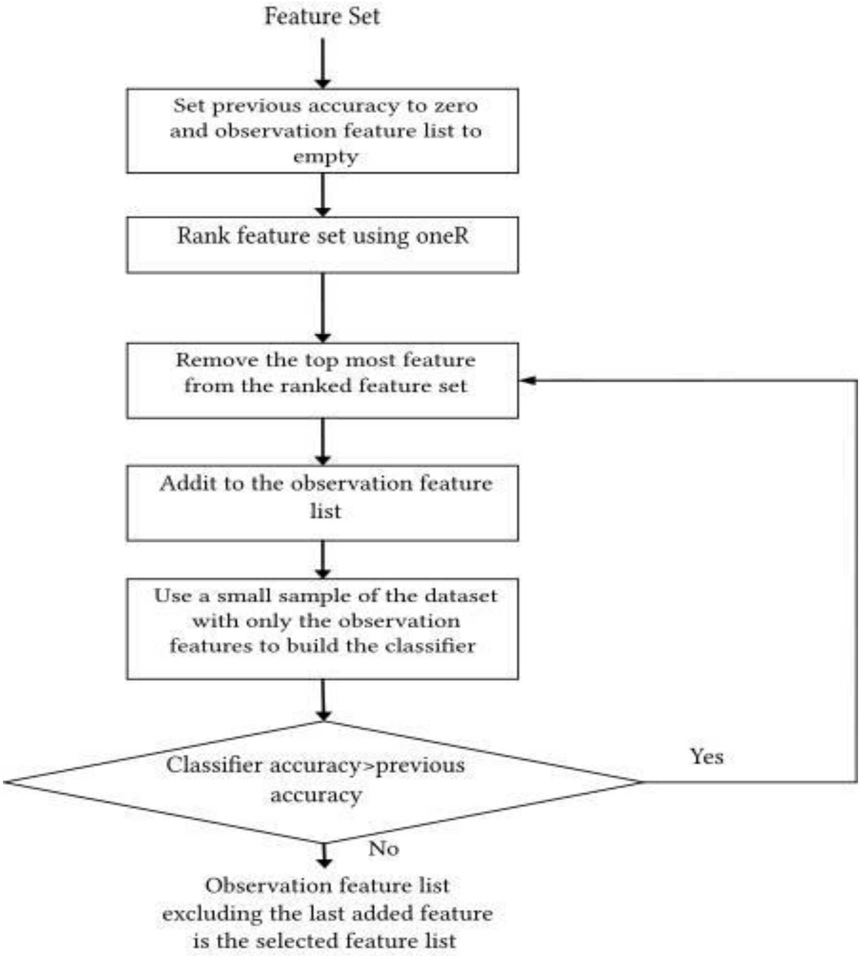
Feature Set
Set previous accuracy to zero and observation feature list to empty
Rank feature set using oneR
Remove the top most feature from the ranked feature set
Addit to the observation feature list
Use a small sample of the dataset with only the observation features to build the classifier
Classifier accuracy>previous accuracy
Yes
No
Observation feature list excluding the last added feature is the selected feature list

Figure. 2 The steps in the automatic feature selection process

Table 7. Accuracy of the various IDSs

Methods	Accuracy
Proposed System	98.15
chi-square multiclass SVM [11]	98
Fuzziness semi-supervised IDS [12]	84.12
FCAAIS [13]	90.4
LFCL [20]	99.16
LA-IDS [17]	98.9
Hybrid SVM and ELM [14]	95.75
MI-BGSA [18]	88.36
GSPSO-ANN [19]	98.13
Naıve Bayes and CF-KNN [21]	94.56
modified OPF [15]	91.74
Layered CRF [8]	90
ML-DR [9]	98.44

6. Conclusion

In today’s world with the widespread usage of social media, online transactions and business, security of data on a network has become an area of deep concern. NSSA systems have wide a role to play in this context, in detecting attacks on a network and taking remedial measures. In order for a NSSA system to perform effectively, the IDS in the system should be capable of detecting various types of attack with high accuracy. To this end, we have proposed an IDS using CRF based classifier. To improve the operational efficiency of the classifier we have also proposed a feature selection method using oneR algorithm. From the experimentation of the proposed system, it has been shown that the system is capable of detecting various attacks with high accuracy. The high performance of the system is due to the capability of CRF utilizing the overlapping relationships between remote features. In future, the system can be tested upon various other datasets to check its efficacy and also steps can be taken to device a still better feature selection method for reducing still the number of features required for optimal operation of the classifier.

Table 8. Performance comparison of the various IDSs

Methods	Accuracy					
	Overall	**dos**	**u2r**	**r2l**	**probe**	**normal**
Proposed System	98.15	98.02	92.30	96.11	96.57	98.58
chi-square multiclass SVM [11]	98	99.9	73.9	98.7	99.2	99.6
Fuzziness semi-supervised IDS [12]	84.12	---	---	---	---	---
FCAAIS [13]	90.4	---	---	---	---	---
LFCL [20]	99.16	99.08	---	100	97.39	---
LA-IDS [17]	98.9	---	---	---	---	---
Hybrid SVM and ELM [14]	95.75	99.54	21.93	31.39	87.22	98.13
MI-BGSA [18]	88.36	---	---	---	---	---
GSPSO-ANN [19]	98.13	---	---	---	---	---
Naıve Bayes and CF-KNN [21]	94.56	84.68	67.16	34.81	79.76	94.56
Modified OPF [15]	91.74	96.89	77.98	81.13	85.92	98.55
Layered CRF [8]	90	97.4	86.33	29.62	98.62	---
Gower kNN [10]	---	99.89	70.64	95.96	99.60	99.96
ML-DR [9]	98.44	95.99	79.77	78.66	94.97	95.74

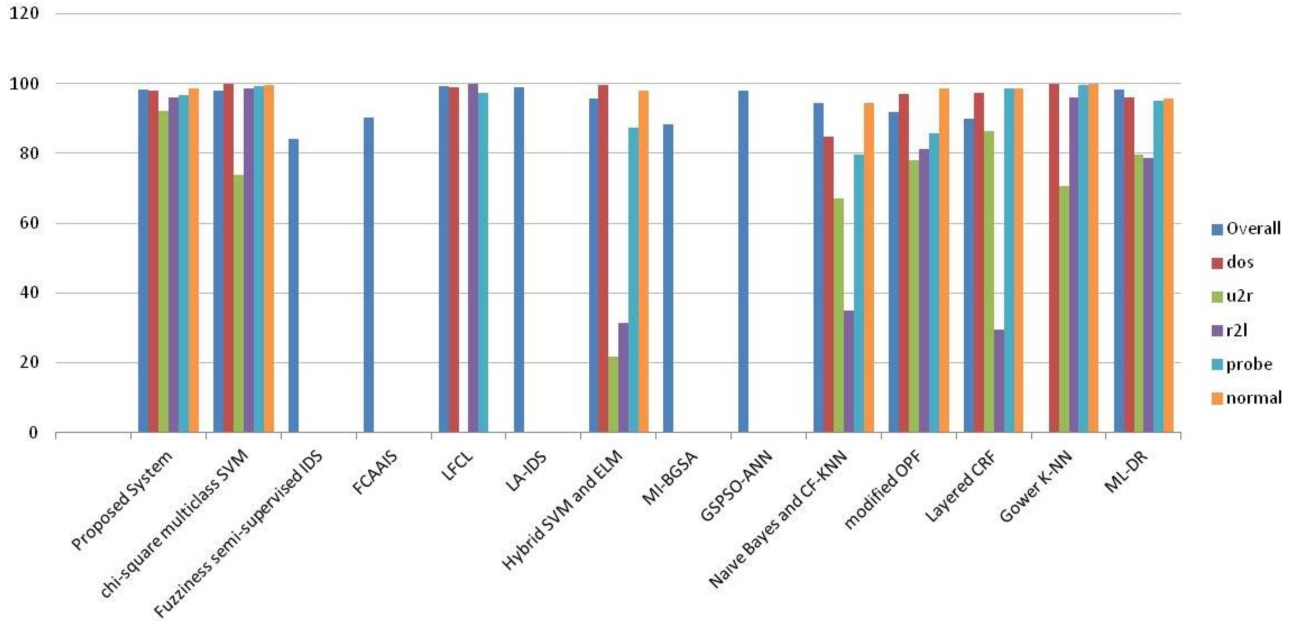

Figure.3 Performance comparison of the various IDSs

References

[1] *Team Coordination Training, Student Guide*, United States Department of Homeland Security, 2004.

[2] P. Barford, Y. Chen, A. Goyal, Z. Li, V. Paxson, and V. Yegneswaran, “Employing Honeynets For Network Situational Awareness”, In S. Jajodia et al., (eds.), *Cyber Situational Awareness, Advances in Information Security*, Vol.46, 2010.

[3] C. Onwubiko, “Functional requirements of Situational Awareness in Computer Network Security”, In: *Proc. of the IEEE International Conference on Intelligence and Security Informatics*, pp.209-213, 2009.

[4] K. Scarfone and P. Mell, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, Recommendations of the National Institute of Standards and Technology, 2007.

[5] M. Qiu , L. Zhang , Z. Ming , Z. Chen , X. Qin, and L. Yang, “Security-aware optimization for ubiquitous computing systems with SEAT

graph approach", *J. Comput. Syst. Sci*, Vol.79, No.5, pp.518–529, 2013.

[6] E. Hernndez-Pereira, J. Surez-Romero, O. Fontenla-Romero, and A. Alonso-Betanzos, "Conversion methods for symbolic features: a comparison applied to an intrusion detection problem", *Expert Syst. Appl*, Vol.36, No.7, pp.10612–10617, 2009.

[7] Q. Yan and F. Yu, "Distributed denial of service attacks in software-defined networking with cloud computing", *IEEE Commun. Mag*, Vol.53, No.4, pp.52–59, 2015.

[8] K. K. Gupta, B. Nath, and R. Kotagiri, "Layered Approach Using Conditional Random Fields for Intrusion Detection", *IEEE Transactions on Dependable and Secure Computing*, Vol.7, No.1, pp.35 – 49, 2010.

[9] B. N. Kumar, M. S. V. S. B. Raju, and B. V. Vardhan, "Enhancing the Performance of an Intrusion Detection System through MultiLinear Dimensionality Reduction and Multi-Class SVM", *International Journal of Intelligent Engineering and Systems*, Vol.11, No.1, pp. 181-190, 2018.

[10] Y. Hamid, B. Ranganathan, L. Journaux, Q. Farooq, and S. Muthukumarasamy, "An Improvised k-NN Respecting Diversity of Data for Network Intrusion Detection", *International Journal of Intelligent Engineering and Systems*, Vol.10, No.3, pp. 409-417, 2017.

[11] I. S. Thaseen, and C. A. Kumar, "Intrusion detection model using fusion of chi-square feature selection and multi class SVM", *Journal of King Saud University – Computer and Information Sciences*, Vol.29, No.4, pp.462-472, October 2017.

[12] R. A. R. Ashfaq, X. Wang, J. Z. Huang, H. Abbas, and Y. He, "Fuzziness based semi-supervised learning approach for intrusion detection system", *Information Sciences*, Vol.378, pp.484-497, 2017.

[13] V. Jyothsna and V. V. R. Prasad, "FCAAIS: Anomaly based network intrusion detection through feature correlation analysis and association impact scale", *ICT Express*, Vol.2, No.3, pp.103–116, 2016.

[14] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Multi-Level Hybrid Support Vector Machine and Extreme Learning Machine Based on Modified K-means for Intrusion Detection System", *Expert Systems with Applications*, Vol.67, pp.296-303, 2017.

[15] H. Bostani and M. Sheikhan, "Modification of Supervised OPF-based Intrusion Detection Systems using Unsupervised Learning and Social Network Concept", *Pattern Recognition*, Vol. 62, pp.56–72, 2017.

[16] G. R. Kumar, N. Mangathayaru, G. Narsimha, and G.S. Reddy, "A Self Constructing Feature Clustering Approach for Anomaly Detection in IoT", *Future Generation Computer Systems*, Vol. 74, pp.417-429, 2017.

[17] S. Jamali, and P. Jafarzadeh, "An intelligent intrusion detection system by using hierarchically structured learning automata", *Neural Comput & Applic*, Vol.28, No.5, pp.1001–1008, 2017.

[18] H. Bostani and M. Sheikhan, "Hybrid of Binary Gravitational Search Algorithm and Mutual Information for Feature Selection in Intrusion Detection Systems", *Soft Comput*, Vol.21, No.9, pp.2307–2324, 2017.

[19] T. Dash, "A Study on Intrusion Detection using Neural Networks Trained with Evolutionary Algorithms", *Soft Comput*, Vol.21, No.10, pp.2687–2700, 2017.

[20] S. Ramakrishnan and S. Devaraju, "Attack's Feature Selection-Based Network Intrusion Detection System Using Fuzzy Control Language", *International Journal of Fuzzy Systems*, Vol.19, No.2, pp.316-328, 2017.

[21] H. H. Pajouh, G. H. Dastghaibyfard, and S. Hashemi, "Two-tier network anomaly detection model: a machine learning approach", *Journal of Intelligent Information System*, Vol.48, No.1, pp.61-74, 2017.

[22] J. Lafferty, A. McCallum, and F. Pereira, "Conditional Random Fields: Probabilistic Models for Segmenting and Labeling Sequence Data", In: *Proc. of 18th Int'l Conf. Machine Learning*, pp.282-289, 2001.

[23] NSL-KDD Dataset. Retrieved from http://www.unb.ca/cic/research/datasets/nsl.html

[24] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set", In: *Proc. of the 2nd IEEE International Conference on Computational Intelligence for Security and Defense Applications*, pp.53–58, 2009.

[25] R.C. Holte, "Very simple classification rules perform well on most commonly used datasets", *Machine Learning*, Vol. 11, pp.63-91, 1993.

[26] R Core Team, *R: A language and environment for statistical computing*, R Foundation for Statistical Computing, Vienna, Austria, 2013. URL http://www.R-project.org/

[27] L. Wu, *CRF: Conditional Random Fields*, 2017. R package version 0.3-14. https://CRAN.R-project.org/package=CRF

[28] E. Frank, M. A. Hall, and I. H. Witten, *The WEKA Workbench. Online Appendix for "Data Mining: Practical Machine Learning Tools and Techniques"*, Morgan Kaufmann, Fourth Edition, 2016.