Journal of Network and Computer Applications 62 (2016) 9–17

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

A multi-level intrusion detection method for abnormal network behaviors

Soo-Yeon Ji [a,*], Bong-Keun Jeong [b], Seonho Choi [a], Dong Hyun Jeong [c,**]

[a] Department of Computer Science, Bowie State University, 14000 Jericho Park Road, Bowie, MD 20715, USA
[b] Department of Computer Information Systems, Metropolitan State University of Denver, 1201 5th Street, Denver, CO 80204, USA
[c] Department of Computer Science and Information Technology, University of the District of Columbia, 4200 Connecticut Avenue NW, Washington, DC 20008, USA

ARTICLE INFO

Article history:
Received 30 August 2015
Received in revised form
5 December 2015
Accepted 18 December 2015
Available online 30 December 2015

Keywords:
Network traffic analysis
Discrete wavelet transform
Visual analytics
Support vector machine

ABSTRACT

Abnormal network traffic analysis has become an increasingly important research topic to protect computing infrastructures from intruders. Yet, it is challenging to accurately discover threats due to the high volume of network traffic. To have better knowledge about network intrusions, this paper focuses on designing a multi-level network detection method. Mainly, it is composed of three steps as (1) understanding hidden underlying patterns from network traffic data by creating reliable rules to identify network abnormality, (2) generating a predictive model to determine exact attack categories, and (3) integrating a visual analytics tool to conduct an interactive visual analysis and validate the identified intrusions with transparent reasons.

To verify our approach, a broadly known intrusion dataset (i.e. NSL-KDD) is used. We found that the generated rules maintain a high performance rate and provide clear explanations. The proposed predictive model resulted about 96% of accuracy in detecting exact attack categories. With the interactive visual analysis, a significant difference among the attack categories was discovered by visually representing attacks in separated clusters. Overall, our multi-level detection method is well-suited for identifying hidden underlying patterns and attack categories by revealing the relationship among the features of network traffic data.

1. Introduction

Due to the advancement of Internet technologies, applications, and protocols, network traffic analysis has become more difficult since it deals with extreme amount of network traffic data. Because of the network complexity, network traffic analysis to detect unauthorized network intruders is also considered as one of the increasingly important research topics in network security.

To address the issue of protecting computing infrastructures by detecting network intruders, numerous intrusion detection (ID) techniques have been proposed. A traditionally known ID system discovers threats by analyzing traffic data at the network layer. The intrusion detection system (called host-based IDS) identifies threats on computer hosts by monitoring computer system logs, system calls, network events, and files (Das and Sarkar, 2014). To detect any abnormal behaviors, it monitors network packets to find possible attack signatures and compare them to known attack patterns. Although the host-based IDS is designed to prevent intruders by changing computer system security policies, it cannot monitor network traffic effectively because it only detects intrusions based on the analysis of information such as logs or packets (Bace, 1999). The system may detect threats based on known attack signatures, but new attacks cannot be discovered (Rubin et al., 2004).

Most analysis approaches are designed to detect intrusions by conducting misuse detection and anomaly detection. The misuse detection searches for events (i.e. known attacks) that are matched to predefined signatures (Kumar and Spafford, 1994). The anomaly detection identifies abnormal behaviors on hosts or networks based on the assumption that each attack shows different behaviors compared to normal activity. Therefore, it is possible to identify any abnormal attacks without having specific knowledge. Due to this advantage, the anomaly detection is used for designing various applications in other areas such as credit cards fraud

* Principal Corresponding author.
** Corresponding author.
E-mail addresses: sji@bowiestate.edu (S.-Y. Ji), bjeong@msudenver.edu (B.-K. Jeong), schoi@bowiestate.edu (S. Choi), djeong@udc.edu (D.H. Jeong).

http://dx.doi.org/10.1016/j.jnca.2015.12.004
1084-8045/

detection (Kou et al., 2004), fault detection in safety critical systems (Worden and Dulieu-Barton, 2004), and any domains that aim to detect abnormal activities including a medical field (Duftschmid and Miksch, 2001). However, the anomaly detection method may provide a high false alarm rate, and require extensive training sets to achieve a reliable performance result (Chandola et al., 2009; Eskin et al., 2002).

Abnormal behaviors are considered as different patterns if they do not match to a well-defined model representing normal behaviors. To discover abnormal behaviors (i.e. intrusions or attacks), understanding their trends or patterns is essential. ID can help us to minimize further damages by providing early warnings. In this paper, we extended our two previous studies by focusing on (1) generating simple and reliable rules to identify intrusions, (2) building a predictive model to determine exact attack categories by utilizing a signal processing technique (i.e. DWT) and Support Vector Machine (SVM), and (3) visually representing the input data to support an interactive visual analysis. For the visual analysis, a visual analytics tool called iPCA (Jeong et al., 2009) was used. With this tool, an interactive visual analysis was conducted to understand the intrusions and their relationships.

The rest of this paper begins with explaining related work in Section 2, our approach including a description of the data (i.e. NSL-KDD) and methods in Section 3. Study results are provided in Section 4. Lastly, Section 5 presents implications of this study and avenue for future research.

2. Related work

Researchers have applied various algorithms or theories such as statistics, machine learning, data mining, information theory, and spectral theory to extract patterns from attacks and design better anomaly detection techniques. Machine Learning (ML) is one of the broadly used algorithms in anomaly detection. ML techniques develop classifiers to determine possible attacks. Markou and Singh (2003a,b) proposed a detection technique with utilizing neural networks and statistical approaches. Rule-based anomaly detection techniques are introduced to capture rules that can identify network behaviors using Fuzzy (Chadha and Jain, 2015; Amini et al., 2015) or decision trees (Lee et al., 2008; Kruegel and Toth, 2003; Stein et al., 2005; Jain and Abouzakhar, 2013). Also, clustering technique (Lin et al., 2015) and SVM (Kuang et al., 2015; Wang et al., 2015; Aslahi-Shahri et al., 2015; Sani and Ghasemi, 2015) are used by numerous researchers to detect abnormal network behaviors. For instance, Xiang et al. (2008) introduced a multiple-level hybrid classifiers combining tree classifiers and Bayesian clustering to detect network anomaly. Kuang et al. (2015) presented a hybrid classifier by integrating SVM and principal component analysis. Golmah (2014) proposed an hybrid intrusion detection method integrating both C5.0 and SVM.

To generate a reliable ID system model, feature selection and extraction are considered as critical tasks for saving computational cost as well as for discovering data patterns. The feature selection is used to select a subset of most meaningful features from the original feature. The feature extraction is necessary for converting input data to reduce dimensions. There are various techniques that can be used for the feature extraction and selection such as Genetic Algorithm (GA) (Aslahi-Shahri et al., 2015), entropy of network features (Agarwal and Mittal, 2012), Partial Least Square (PLS) (Gan et al., 2013), Kernel Principal Component Analysis (KPCA) (Kuang et al., 2015), and cuttlefish optimization algorithm (Eesa et al., 2015). When applying the feature extraction, there is an important consideration whether the characteristics of original input data are transmitted to extracted new feature sets. However, it is important to note that the generated new feature set may not maintain the same or similar patterns compared to the original input data (Yang et al., 2011). Sanei et al. (2015) addressed the potential capability of discovering important features from input data by utilizing signal processing techniques. In our previous studies (Ji et al., 2014a,b), we emphasized the importance of detecting network abnormal behaviors. More specifically, in the study (Ji et al., 2014a), two-level ID method was introduced using a publicly available internet traffic data to show its capability in classifying abnormal network traffic. Fractal dimension (FD) was applied to identify the specific attack. Our previous works focused on generating rules to detect network anomalous activities and finding the self-similarity among the attacks. While the generated rules clearly differentiated normal and abnormal behaviors, there was a limitation of providing a detailed information (i.e. reasons) about the detected abnormal behaviors. To address this limitation, the categorical variables are converted to dummy variables. In addition, a visual analytics approach is integrated to identify transparent reasons about detected abnormal activities.

3. Approach

3.1. Data description

In this study, a publicly available intrusion detection dataset (called NSL-KDD dataset NSL-KDD, 2014; Tavallaee et al., 2009) is used. NSL-KDD dataset is the refined version of the KDD cup'99 dataset that redundant data records are removed (Tavallaee et al., 2009; NSL-KDD, 2014). The NSL-KDD dataset includes training set (125,973 records) and testing set (22,544 records). It contains 41 attributes (three nominal, six binary, and thirty-two numeric attributes), and includes normal activity and twenty-four attacks. These attacks are grouped into four major categories. Table 1 represents the four major attacks and intrusion categories. In this study, the training and testing data were combined to make a new input data. A total of 148,517 records were used as an input data.

DoS attack indicates any attempts to disable network access from remote machines (or computing resources). R2L represents that a remote user gains an access to local user accounts by sending packets to a computing machine over the network. Probe indicates that network is scanned to gather information to find known vulnerabilities. U2R denotes that an attacker accesses normal users' accounts by exploring the system as a root-user.

3.2. Methods

In this section, a brief explanation about our proposed multi-level network intrusion detection approach is provided. As shown in Fig. 1, the approach consists of three steps: (1) generating rules to detect outcome (normal/abnormal), (2) building an abnormal network behavior model to detect exact attack categories (i.e. DoS, Probe, R2L), and (3) conducting an interactive visual analysis to provide transparent reasons. First, the input data is divided into two subsets: categorical (i.e. nominal) data and numerical data. The nominal variables are used to generate rules. To determine exact attack categories, an extraction of significant DWT features from the numerical variables is performed. Furthermore, an interactive visual analysis is conducted to find the relationship between the raw and the DWT features and to present transparent reasons about the results.

3.2.1. Detection of abnormal behavior

Pre-Processing: As mentioned above, the NSL-KDD data set contains three nominal variables that include protocol type, service, and flag. However, each nominal variables contains many distinctive attribute values. Protocol type includes three attributes

(i.e. TCP, UDP, and ICMP), service includes 70 attribute values (i.e. SMTP, HTTP, POP3, SSH, WHOIS, and among others), and flag contains 11 attributes (i.e. SF, S2, S1, S3, REJ, RSTR, and among others). Since the nominal variables contain numerous amount of attribute values, it is difficult to extract transparent information regarding network abnormality. To resolve this issue, a binary coding scheme (Shyu et al., 2005) via the use of indicator variables is applied to the three nominal variables. Binary coding uses 1 ("one") to indicate the occurrence of a category of interest and 0 ("zero") to represents its non-occurrence (Neter et al., 1996). For example, if the attribute value of protocol type is "TCP", it is converted to 1, and otherwise 0.

When labeling all attacks as "abnormal", total of 77,054 normal and 71,463 abnormal data are formed. To generate a rule-based method to identify abnormal behaviors, nominal and binary variables are used. By reforming the nominal variables, total of 90 features including binary variables (i.e. yes/no) are generated. Since the binary coding to the nominal variables causes an increase of data dimensions, important features are selected. For this selection, a statistical validation using SAS is performed. Then, each normal and abnormal data are randomly divided into 10 different subsets to apply ten-fold cross-validation.

Rule generation with CART: To design a rule-based model, Classification and Regression Tree (CART) (Breiman et al., 1984) is used. CART applies the concept of information theory to create a decision tree that captures complex patterns of input data. It is broadly used due to its efficiency in dealing with multiple data types and missing values. CART expression forms explicit and transparent grammatical rules (Loh and Vanichsetakul, 1988; Fu, 2004). Thus, it is much simpler to understand data patterns than other models. In addition, it uses an exhaustive search of all variables and split values to find optimal splits for each node by measuring the degree of impurity for each outcome of the feature. To find the most important features for identifying network traffic abnormal behaviors, a statistical test (i.e. ANOVA) is performed. Then, trees are generated from each training set using the selected significant features. Due to the difficulty of extracting rules from the generated trees, a software application (called *TreeParser*) is designed to extract rules from the trees by navigating all branches of the generated trees. With the extracted rules, the performance of each rule is measured with a distinctive testing dataset.

Table 1
Four attack categories in the NSL-KDD dataset.

Four categories	Intrusion types
DoS	Back, land, neptune, pod, smurf, teardrop, mailbomb, processtable
R2L	ftp_write, imap, guess_passwd, multihop, phf, spy, warezclient, warezmaster sendmail, snmpgetattack, snmpguess, worm, xlock, xsnoop, named
U2R	buffer_overflow, loadmodule, perl, spy, rootkit,ps, xterm, sqlattack,mscan
Probe	ipsweep, nmap, portsweep, satan, saint

3.2.2. Classification of exact attack categories

When incoming network traffic events are considered as "abnormal behaviors" or "attacks", it is important to specify their exact attack categories. Providing the exact information is critical for system administrators so that relevant actions can be taken to protect computing infrastructures. In this study, three attack categories (i.e. DoS, Probe, R2L) are considered due to insufficient amount of U2R data.

Feature extraction and selection: Since signal processing technique has a capability of discovering hidden patterns from input data, discrete wavelet transform (DWT) is used. DWT is a promising technique for time-frequency analysis by decomposing the input data until pre-determined level. By decomposing the input data, further detailed information (e.g. any pattern changes) can be represented. It is beneficial to understand non-stationary data such as network traffic since DWT has an ability to detect any changes from the data. Due to the benefit, Wavelet Transform (WT) is commonly used to analyze data in other domains such as medicine, health, and stock. While researchers (Callegari et al., 2008; Gao et al., 2006; Tan et al., 2012; Dainotti et al., 2006) utilized WT techniques in the context of intrusion detection, they only used WT for reconstructing the data or determining a threshold for detecting intrusions. The threshold was used to make a decision to determine abnormality in their studies. However, in our study, we used DWT to extract new features representing hidden but significant patterns.

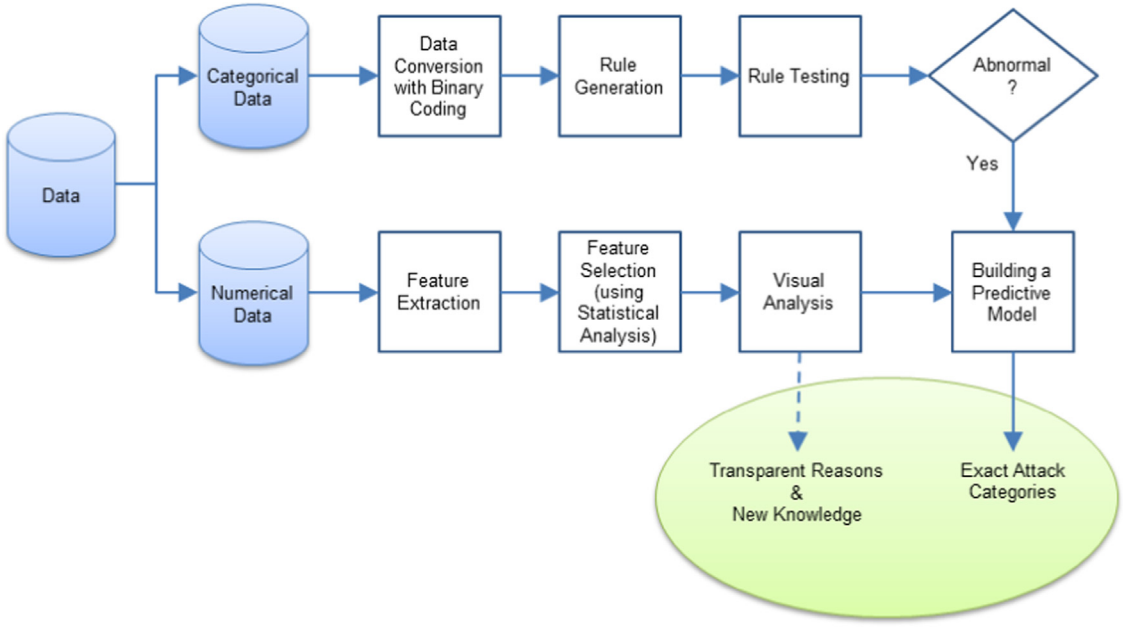

Fig. 1. A schematic diagram of the proposed approach.

The selection of specific mother wavelet is often considered as a difficult task since results can vary depending on what mother wavelet is applied. For this study, a broadly used Daubechies' wavelet family (specifically, a db2) is utilized. A three-level decomposition is applied to the data with an overlapping sliding window (size of 100 data points) to examine rapid changes within the data. By applying DWT, three features (i.e. standard deviation of absolute values, root mean square, and energy) are calculated. The features are

$$\sigma_k = \sqrt{\left[\left(\frac{1}{N}\Sigma_{i=1}^{N}(|d_i^k| - \mu)^2\right)\right]},$$
$$m_k = \sqrt{((1/N \quad \Sigma_{i=1}^{N}(d_i^k)^2)},$$
$$e_k = \Sigma_{i=1}^{N}(|d_i^k|)^2$$

where $\mu = 1/N\Sigma_{i=1}^{N} d_i^k$, N is the size of each coefficient, d_i represents wavelet coefficients, and k indicates a decomposition level (our study uses $k=3$).

Detection of exact attacks: Once the features are extracted, the significance of each feature is tested. Only significant features are selected to generate a classifier (i.e. learning model) that can be used to detect exact attack categories using ML algorithms. Three ML algorithms such as SVM, Neural Network (NN), and Naïve Bayes are compared. Naïve Bayes and NN are commonly used to classify data consisting of two groups (e.g. normal/abnormal). The main idea of SVM, a statistical learning theory, is finding a hyperplane that can separate the input data precisely. That is, SVM finds the optimal hyperplane by minimizing the mis-classification error. Naïve Bayes, a simplified Bayesian probability model based on Bayes theorem, calculated prior and conditional probabilities to generate a learning model. This learning model may cause an error because of the impacts of bias and variance, and training data noise. NN is an information processing model that is inspired by the biological nervous systems. It is composed of a large number of highly interconnected neurons. It has limitations including falling into a local solution instead of global one and having a slow convergence. In general, SVM (Vapnik, 1998) is simple, fast in operation, and has good robustness than Bayes and Neural Network. Therefore, it is widely used in different domains such as bioinformatics (Idicula-Thomas et al., 2006), data mining, pattern recognition (Shawe-Taylor and Cristianini, 2004), and text categorization (Joachims, 1998). In this study, SVM is used to generate a classifier. Also, a performance comparison with NN and Naïve Bayes is conducted.

3.2.3. Visual analysis

A visual analytics approach is utilized to perform an interactive visual analysis on the network traffic data. Visual analytics has been known as a new research area that focuses on performing analytical reasoning with interactive visual interfaces (Thomas and Cook, 2006). In this study, an extended version of a visual analytics tool called iPCA (Jeong et al., 2009) is used to conduct an interactive factor analysis. iPCA is designed to represent the results of Principal Component Analysis (PCA) using multiple coordinated views and a rich set of user interactions to support interactive analysis of multivariate datasets. The network traffic data are projected onto two user-selected principal components. A parallel coordinates visualization is used to show the data in the original data dimensions. In the parallel coordinates visualization, horizontal lines represent features of the data and each line indicates an individual network traffic data. Within iPCA, the user is allowed to select data in one view and immediately see the corresponding data highlighted in the other view which helps the user to understand the relationship between the two. To enhance the capability of interactive visual analysis within each view, several user interactions (i.e. highlighting, brushing, and filtering of data items or dimensions) are supported. A detailed explanation of conducted visual analysis with iPCA is included in Sections 4.2.2 and 4.2.3.

4. Results

This section presents the generated rules to identify network abnormality, the performance of detecting exact attack categories, and the visual analysis to examine the relationship among the DWT features and its correlation analysis.

4.1. Abnormal behavior detection

As described in Section 3.2.1, total of 77,054 normal and 71,463 abnormal data are used. After converting the nominal input variables to binary scheme indicators, total of 90 variables including six binary variables are generated. A statistical analysis (i.e. ANOVA) is performed to determine statistically significant features. As a result, 22 features (e.g. ICMP, HTTP, SMTP, domain_u, SF, private, S2, S1, IRC, REJ, land_0, login_Yes, POP3, FTP, FTP_data, x11, Host_login_Yes,urp_i, Telnet, IMAP4, Guest_login_Yes, Gopher) are found to be statistically significant ($p < .05$). Then, the 22 significant features are used to generate decision trees. Ten trees are created and tested with distinctive test datasets. Table 2 represents the samples of extracted rules maintaining the testing accuracy of 85% or above.

We found that “SF”, one of the attribute values in “flag”, is an important attribute to identify network abnormality. Also, the generated rules are complicated to present the “Abnormal” behavior. When considering the “SF” feature (indicating normal establishment and termination), if the “SF” feature is “NO”, there is a higher chance that network activities are determined as abnormal behaviors. However, it is important to verify the result by

Table 2
Samples of the extracted rules that are used to identify abnormal network traffic behaviors.

Rules	Testing accuracy
If(SF='NO' & http='NO' & login_Yes='YES' & IRC='NO' & S1='NO' & smtp='NO' & X11='NO') then Abnormal	5521/5542=99.62%
If (SF='YES' & ICMP='YES' & urp_i='NO') then Abnormal	840/929=90.41%
If(SF='YES' & ICMP='NO' & private='NO' & pop_3='YES') then (Abnormal)	324/342=94.73%
If (SF='YES' & ICMP='NO' & private='NO' & ftp='NO' & pop_3='NO' & telnet='YES' & login_No='NO') then Abnormal	506/507=99.80%
if(SF='NO' & http='YES' & REJ='YES') then Normal	304/326 =93.25%
If (SF='YES' & ICMP='NO' & private='NO' & pop_3='NO' & telnet='NO' & ftp='NO' & ftp_data='YES') then Normal	560/633=88.46%
If(SF='YES' & ICMP='NO' & private='NO' & pop_3='NO' & telnet='NO' & ftp='NO' & ftp_data='NO' & imap4='NO' & tcp='NO') then Normal	1271/ 1297=97.99%
If(SF='NO' & http='YES' & REJ='YES') then Normal	308/333=92.49%
If(SF='YES' & ICMP='NO' & private='NO' & pop_3='YES') then Abnormal	324/342=94.73%
If (SF='YES' & ICMP='NO' & Pop_3='NO' & telnet='NO' & ftp='NO' & ftp_data='NO' & imap4='NO' & tcp='YES' & login='NO') then Normal	4799/4913=97.67%
If (SF='YES' & ICMP='NO' & ftp='NO' & pop_3='NO' & telnet='NO' & ftp_data='NO' & gopher='NO' & login='NO') then Normal	5744/6085=94.4%

checking other features. Due to this reason, the size of the rule can be longer and complex than when the "SF" feature is "Yes".

4.2. Exact attack category detection

To detect the exact attack category, thirty-two numerical variables in abnormal data (i.e. total of 71,344) are used. A total number of 54,275 data for the DoS attack, 14,077 for the Probe attack, and 2992 for the R2L attack are used. Since two numerical variables (i.e. urgent and num_outbound_cmds) have all zero values, they are removed from the analysis. As explained in Section 3.2.2, DWT is applied to extract features. With the DWT, total of 2841 (2167 for DoS, 559 for Probe, and 115 for R2L) datasets with 144 features are generated. A statistical test is applied to find a statistical significance of each feature. As a result, 77 out of 144 features were determined as statistically significant ($p < 0.05$) features.

4.2.1. Feature comparison

A feature comparison between the raw and the DWT features is performed by measuring the average of the features. Since the raw and the DWT features have different scales, a normalization between 0 and 1 is applied. As shown in Fig. 2, we found that the DWT features clearly separate the attack categories while the raw features maintain similar patterns. For the raw features, we noticed that the five features (i.e. r1, r4, r7, r8, and r14) are almost identical between the two attack categories (Probe and R2L). Although the DoS attack shows a distinctive pattern among the three attacks at the features (see the features of r5, r6, r10, r11, r12, and r13), the raw features may not be useful for differentiating the three exact attacks.

4.2.2. Visual comparison of the features

To project the raw and the DWT features, PCA computation is performed to identify principal components. PCA requires a high computational power to compute eigenvectors and eigenvalues, thus an approximation method based on SVD called Online SVD (Brand, 2006) is used to perform the PCA computation and maintain real-time user interactions when interacting with large scale datasets. Fig. 3 represents PCA projections with two principal components on (A) the raw features and (B) the DWT features. From the projection of the raw feature (Fig. 3(A)), it is difficult to identify a clear separation among the three attack categories. The DoS attacks are appeared mostly in three regions, the Probe attacks occupies two regions, and the R2L attacks are spread out all over the Projection space. This indicates that identifying the difference among the three attacks is extremely difficult due to the fact that they maintain similar patterns. However, there was a clear separation among the attacks in the projection of the DWT features (see Fig. 3(B)). The DoS attack is forming two clusters that are completed separated from other attacks. Since there is a similarity between Probe and R2L even in the DWT features, an additional analysis is conducted to determine common features appeared in both categories.

4.2.3. Dimension contribution analysis

iPCA supports the change of dimension contributions by moving slider bars where each feature provides the ability to analyze the data non-linearly. The dimension contribution analysis is performed to identify dominant features that make several attacks to become appeared within other clusters. As shown in Fig. 4, when dimension contribution analysis is performed by changing the contribution of the five features (d37, d38, d68, d72, and d75) from 100% to 0%, a clear separation of pattern is emerged. Interestingly, we identified a couple of possible outliers. Fig. 4 (A) indicates that a R2L attack is appeared within a DoS cluster. Fig. 4(B) represents that a DoS attack positioned in a R2L cluster. These outliers might be strongly related to the five features. To investigate the cause of the items being appeared in other attack clusters, it is important to conduct an outlier analysis. Since understanding outliers is not a primary concern of this study, we leave it as a future work.

To investigate the relationship among the features, Pearson-correlation analysis is conducted. Fig. 5 represents the correlations of the (A) raw and (B) DWT feature datasets. In Fig. 5, the diagonal displays the name of dimension as a text string. The lower triangulation shows the coefficient value between two dimensions with a color indicating positive (red), neutral (white), and negative (blue) correlations. The upper triangulation contains cells of scatter plots where all data items are projected onto the two intersecting dimensions. As we discussed above, there was no clear separation among the attacks using the raw features (see Fig. 3(A)). This might be because a half of the features maintain neutral correlations (Fig. 5(A)). However, positive and negative correlations are easily discovered in the DWT features (Fig. 5(B)). When looking at the scatterplots having highly positive correlation coefficients ($\gamma = 0.99$) in Fig. 5(C) and (D), we identified that they maintain different distributions. Although the scatterplot in Fig. 5 (C) shows vertically or horizontally increasing patterns (i.e. skew correlation), the scatterplot in Fig. 5(D) presents a directly proportional pattern by showing a linear relationship between the two features. In addition, the scatterplot (Fig. 5(D)) displays that the attack categories are appeared by forming different patterns as the R2L attacks are mostly appeared in the lower bottom corner, the DoS attacks are forming two visible clusters, and the Probe attacks are spread out in the middle and lower regions.

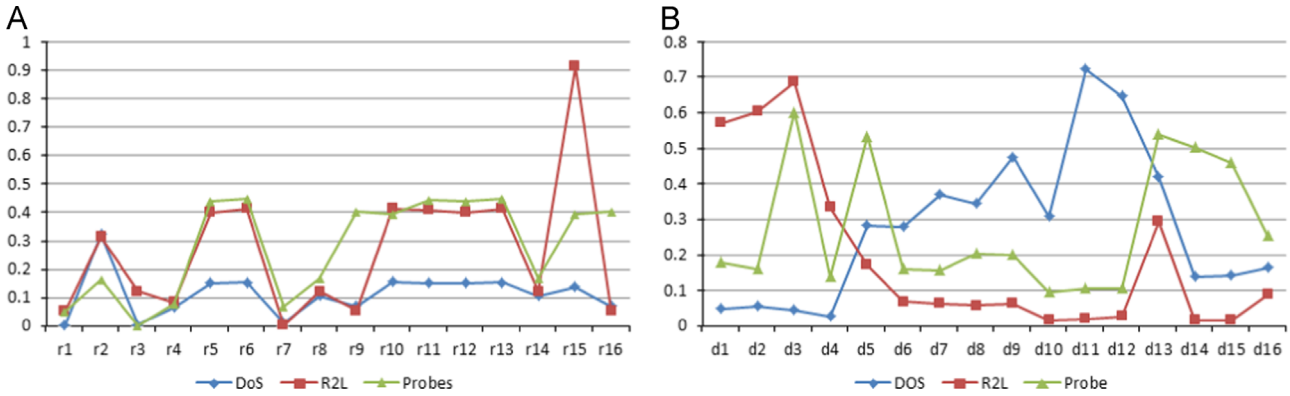

Fig. 2. A comparison between the raw features (A) and the DWT features (B). *x*-axis indicates the DWT and raw features, and *y*-axis presents the average value of each feature.

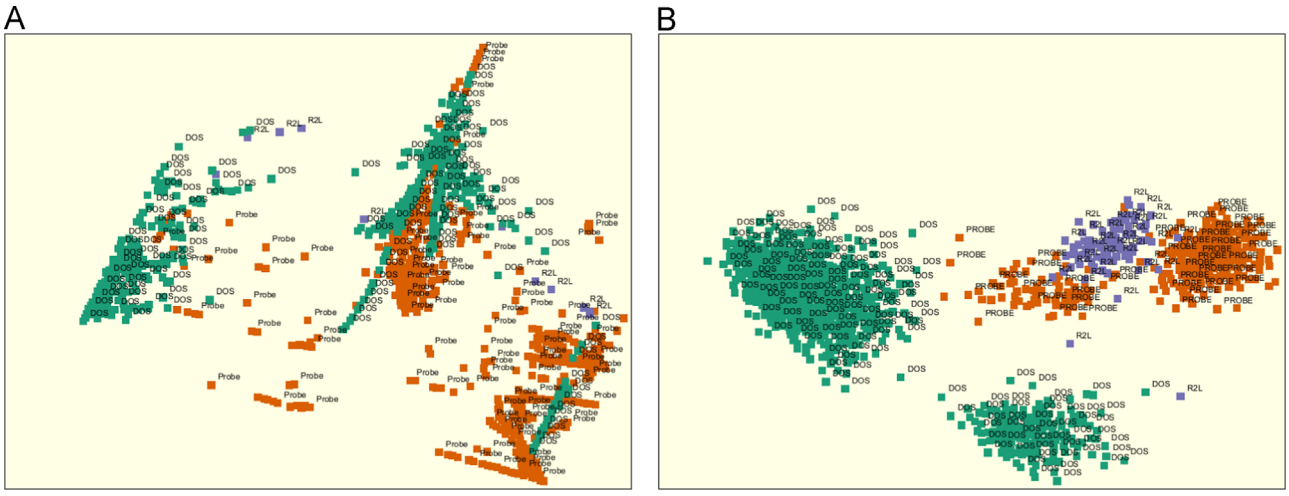

Fig. 3. PCA projections of (A) the raw feature and (B) the DWT feature datasets. The data are mapped with different color attributes as DoS (green), Probe (orange), and R2L (purple). (For interpretation of the references to color in this figure caption, the reader is referred to the web version of this paper.)

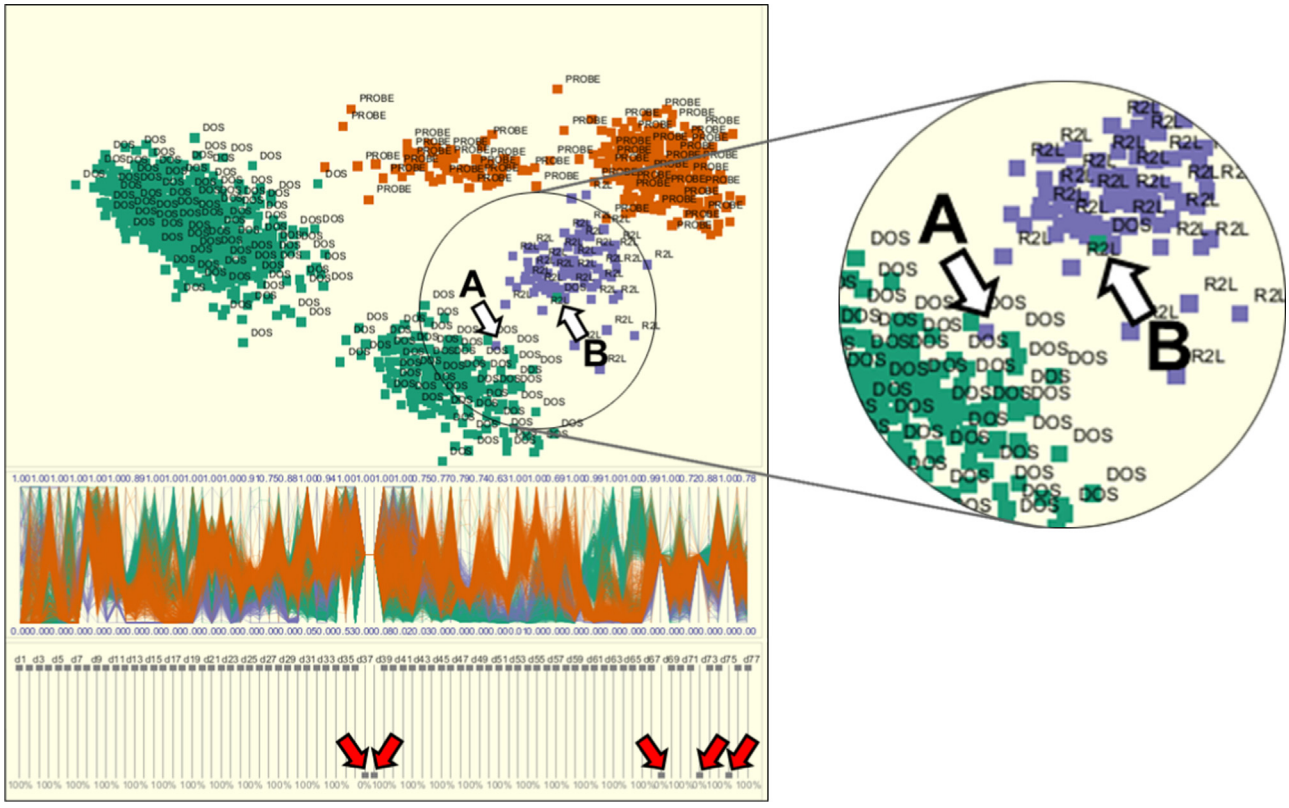

Fig. 4. Dimension contribution is applied in the five DWT features (d37, d38, d68, d72, and d75) from 100% to 0% using the slider bars to make a clear separation between Probe and R2L (see the red arrows). 0% indicates that the selected variable is not used to going to contribute to the final PCA. (For interpretation of the references to color in this figure caption, the reader is referred to the web version of this paper.)

4.2.4. *Classification comparison*

A classification is performed to determine exact attack categories with a ten-fold cross-validation (CV). The performance of three ML techniques (i.e. SVM, Naïve Byes, and NN) is compared and presented in Table 3. The average accuracy to detect exact attack categories with SVM, Naïve Bayes, and NN were 95.5471%, 89.024%, and 96.67%, respectively. We found that NN shows a slightly higher accuracy than SVM. But, when measuring the standard error of the mean (SEM), there was a variation difference as SVM (0.285), Naïve Bayes (2.02), and NN (0.683). In addition, when generating a learning model with SVM and NN, it took 0.157 s and 13.04 s, accordingly.

5. Discussion and conclusion

This study presents a multi-level network abnormality detection method by utilizing reliable rules to detect abnormal behavior, generating a predictive model to detect the exact attacks (i.e. DoS, R2L, and Probe) using the DWT features, and applying a visualization analytic tool to provide further detailed understanding and analysis for users.

Although DWT was often used by researchers to detect network abnormal behaviors, it was simply used to determine a threshold or to reconstruct data by removing noise. Unlike other studies, this study emphasizes the importance of using DWT to extract

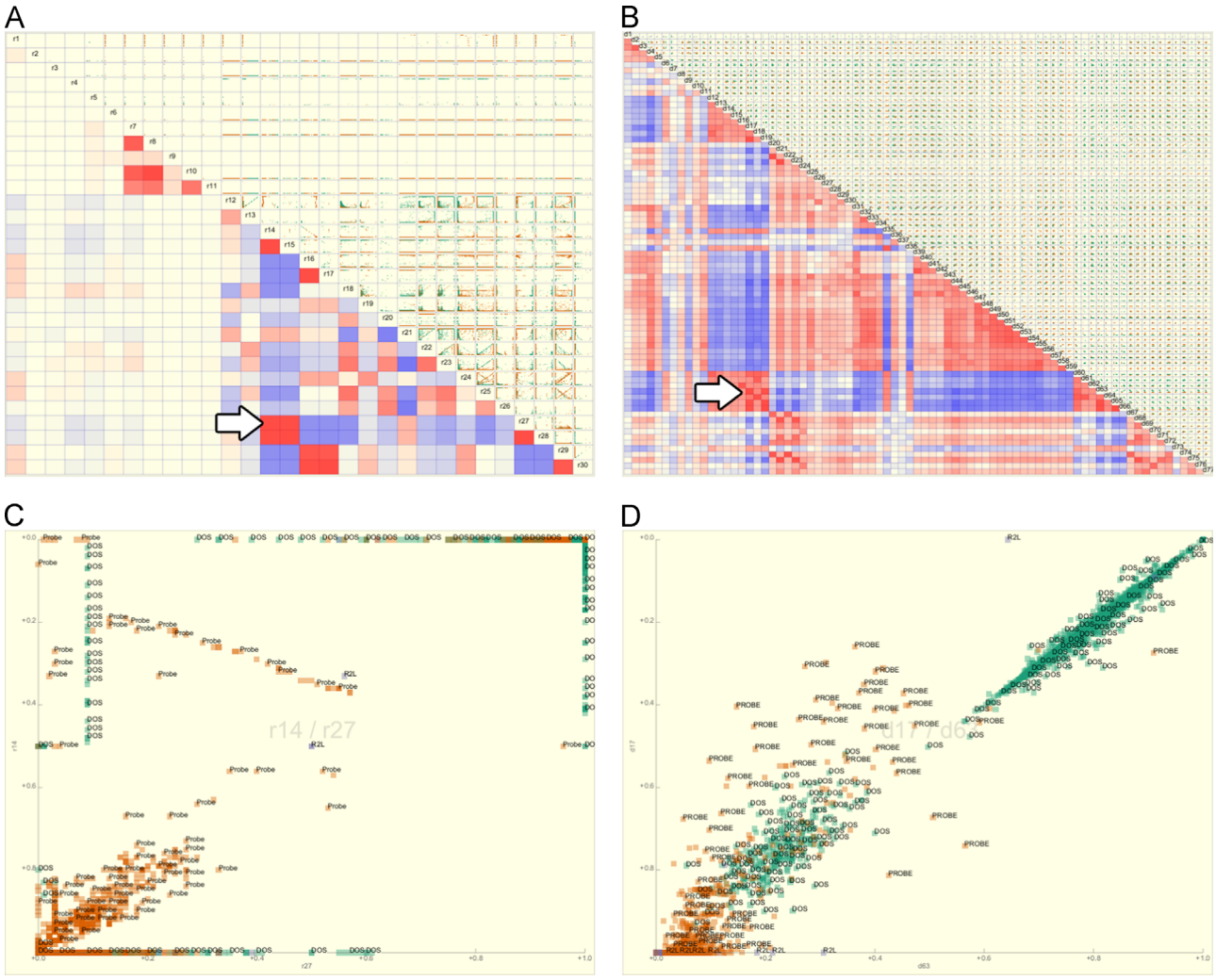

Fig. 5. Correlation views of the (A) raw feature and (B) DWT feature datasets. Each color indicates positive (red), neutral (white), and negative (blue) correlations. The arrows in (A and B) indicate the scatterplots having positive correlation coefficients (γ=0.99). Their scatterplots are presented in (C and D). (For interpretation of the references to color in this figure caption, the reader is referred to the web version of this paper.)

Table 3
Classification performance comparisons.

Test data-set	Three attack classification		
	SVM	Naïve Bayes	NN
Test 1	95.77%	91.47%	94.77%
Test 2	96.83%	91.23%	95.93%
Test 3	96.83%	95.5%	100%
Test 4	95.77%	89.77%	96.83%
Test 5	96.47%	90.47%	95.77%
Test 6	96.12%	78.2%	96.1%
Test 7	95.77%	89.1%	94.57%
Test 8	95.77%	93%	94.2%
Test 9	97.88%	76.8%	100%
Test 10	98.22%	94.7%	98.59%

significant features for detecting network abnormal behaviors. As discussed earlier, our previous study (Ji et al., 2014a) presented decision rules for detecting network abnormal behaviors with utilizing only four variables (i.e. duration, protocol type, service, and flag). The rules were statistically significant to detect intrusions. While the generated rules clearly differentiated normal and abnormal behaviors, there was a limitation of providing a detailed information about the detected abnormal behaviors since each variable includes numerous attribute values. For instance, the rule (*protocol* ≠ *HTTP*) does not provide useful information because there are about 70 attribute values indicating different network protocols. To avoid this ambiguity, the nominal variables are converted dummy variables to generate more accurate rules. So, the result can provide appropriate meaning about the detected network abnormal behaviors.

Based on the performance measure of each rule, only highly accurate rules were used for intrusion detection analysis. However, it is important to note that even the rules with less accuracy may provide a valuable information for detecting intrusions. For instance, the rule - if (SF='YES' & ICMP='NO' & private='YES') then Abnormal – has 72.16% of accuracy. Although the accuracy does not represent a high performance, we found that the rule is fitted to the majority of the data (306/424).

Among the extracted DWT features, 53.47% features are shown to be statistically significant ($p < 0.05$). Even though R2L attacks have less amount of data compared to other attacks, we identified that the true positive for the R2L with the raw feature is 59.8% and 75% for the DWT features. One of the major concerns in many previous studies for detecting intrusions is how to reduce high false positive (FP) results. In our study, the FP rate for the raw and the DWT features were 7.9% and 2.3%, respectively. The DWT features can provide a better performance if we have a larger

amount of R2L data. It is also important to note that, unlike other previous methods utilizing wavelet transform techniques, our approach includes a method of performing a mathematical calculation and a statistical validation to extract hidden underlying patterns from the input data.

In this study, we utilized a visual analytics tool to interpret the results, discover new knowledge, and find reasons efficiently. As shown in Fig. 3, there was no clear separation of the raw features among DOS, Probe, and R2L. However, when using the DWT features, we identified a clear separation among the attack categories. Most importantly, the "R2L" attack was not identifiable with the raw features. When analyzing the DWT features further, we identified that there was a similarity between Probe and R2L. The dimension contribution analysis was performed with iPCA to identify specific features that make them difficult to separate. The dimension analysis with iPCA is quite challenging because the user needs to maintain an awareness of this change by the contribution since the projection of data will be modified. With carefully adjusting dimension contributions to each feature, we identified a clear separation (see Fig. 4). More specifically, we identified five features as strong dimension contributors that make the Probe and R2L attacks appeared nearby in the PCA projection.

Our study has potential avenues for future research. We plan to enhance our approach by identifying possible outliers and understand their patterns as well as effectiveness for determining the abnormality precisely. In addition, we are going to test our proposed approach with different network intrusion datasets. In this study, we only focused on utilizing supervised learning algorithms. To determine the effectiveness of our approach of extracting and utilizing DWT features, we consider to compare our approach to unsupervised learning algorithms. In addition, we are going to conduct additional visual analysis to identify the cause of outliers appeared in the network traffic data. Lastly, our method can be applied to other research domains that require to detect abnormal behaviors (or activities) with providing meaningful information. Specifically, we plan to apply our proposed approach to detect abnormality in software applications.

Acknowledgements

This study is fully supported by the U.S. Army Research Office (ARO Grant no. W911NF-13-1-0143) and partially supported by the same agency (ARO Grant no. W911NF1210060).

References

Agarwal B, Mittal N. Hybrid approach for detection of anomaly network traffic using data mining techniques. Proced Technol 2012;6:996–1003.
Amini M, Rezaeenour J, Hadavandi E. Effective intrusion detection with a neural network ensemble using fuzzy clustering and stacking combination method. J Comput Secur 2015;1(4).
Aslahi-Shahri B, Rahmani R, Chizari M, Maralani A, Eslami M, Golkar M, Ebrahimi A. A hybrid method consisting of ga and svm for intrusion detection system. Neural Comput Appl 2015:1–8.
Bace R. An introduction to intrusion detection & assessment. ICSA intrusion detection systems consortium white paper; 1999. p. 1–38.
Brand M. Fast low-rank modifications of the thin singular value decomposition. Linear Algebr Appl 2006;415(1):20–30.
Breiman L, Friedman JH, Olshen RA, Stone CJ. Classification and regression trees. New York: Chapman & Hall; 1984.
Callegari C, Giordano S, Pagano M. Application of wavelet packet transform to network anomaly detection. In: Balandin S, Moltchanov D, Koucheryavy Y, editors. Next generation teletraffic and wired/wireless advanced networking. Lecture notes in computer science, vol. 5174. Berlin, Heidelberg: Springer; 2008. p. 246–57.
Chadha K, Jain S. Hybrid genetic fuzzy rule based inference engine to detect intrusion in networks. In: Intelligent distributed computing. Springer; 2015. p. 185–98.
Chandola V, Banerjee A, Kumar V. Anomaly detection: a survey. ACM computing surveys (CSUR) 2009;41(3):15.
Dainotti A, Pescape A, Ventre G. Nis04-1: wavelet-based detection of dos attacks. In: Global telecommunications conference, 2006. GLOBECOM '06. IEEE; Nov 2006. p. 1–6.
Das N, Sarkar T. Survey on host and network based intrusion detection system. Int J Adv Netw Appl 2014;6(2):2266–9.
Duftschmid G, Miksch S. Knowledge-based verification of clinical guidelines by detection of anomalies. Artif Intell Med 2001;22(1):23–41.
Eesa AS, Orman Z, Brifcani AMA. A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems. Expert Syst Appl 2015;42(5):2670–9.
Eskin E, Arnold A, Prerau M, Portnoy L, Stolfo S. A geometric framework for unsupervised anomaly detection. In: Applications of data mining in computer security. Springer; 2002. p. 77–101.
Fu CY. Combining loglinear model with classification and regression tree (cart): an application to birth data. Comput Stat Data Anal 2004;45(4):865–74.
Gan X-s, Duanmu J-s, Wang J-f, Cong W. Anomaly intrusion detection based on pls feature extraction and core vector machine. Knowl Based Syst 2013;40:1–6.
Gao J, Hu G, Yao X, Chang R. Anomaly detection of network traffic based on wavelet packet. In: Asia-Pacific conference on communications, 2006. APCC '06; August 2006. p. 1–5.
Golmah V. An efficient hybrid intrusion detection system based on c5. 0 and svm. Int J Database Theory Appl 2014;7(2):59–70.
Idicula-Thomas S, Kulkarni AJ, Kulkarni BD, Jayaraman VK, Balaji PV. A support vector machine-based method for predicting the propensity of a protein to be soluble or to form inclusion body on overexpression in Escherichia Coli. Bioinformatics 2006;22(3):278–84.
Jain R, Abouzakhar N. A comparative study of hidden Markov model and support vector machine in anomaly intrusion detection. J Internet Technol Secur Trans (JITST) 2013;2(1/2/3/4):176–84.
Jeong DH, Ziemkiewicz C, Fisher B, Ribarsky W, Chang R. iPCA: an interactive system for PCA-based visual analytics. Computer graphics forum; 2009.
Ji S-Y, Choi S, Jeong DH. Designing a two-level monitoring method to detect network abnormal behaviors. In: 2014 IEEE 15th international conference on information reuse and integration (IRI); 2014. p. 703–9.
Ji S-Y, Choi S, Jeong DH. Designing an internet traffic predictive model by applying a signal processing method. J Netw Syst Manag 2014b:1–18.
Joachims T. Text categorization with support vector machines: learning with many relevant features. In: Proceedings of the 10th European conference on machine learning. ECML '98. London, UK, UK: Springer-Verlag; 1998. p. 137–42.
Kou Y, Lu C-T, Sirwongwattana S, Huang Y-P. Survey of fraud detection techniques. In: 2004 IEEE international conference on networking, sensing and control. vol. 2. IEEE; 2004. p. 749–54.
Kruegel C, Toth T. Using decision trees to improve signature-based intrusion detection. In: Recent advances in intrusion detection, Springer; 2003. p. 173–91.
Kuang F, Zhang S, Jin Z, Xu W. A novel svm by combining kernel principal component analysis and improved chaotic particle swarm optimization for intrusion detection. Soft Comput 2015:1–13.
Kumar S, Spafford, EH. A pattern matching model for misuse intrusion detection; 1994.
Lee J-H, Lee J-H, Sohn S-G, Ryu J-H, Chung T-M. Effective value of decision tree with kdd 99 intrusion detection datasets for intrusion detection system. In: 10th international conference on advanced communication technology, 2008. ICACT 2008. vol. 2, IEEE; 2008. p. 1170–5.
Lin W-C, Ke S-W, Tsai C-F. Cann: an intrusion detection system based on combining cluster centers and nearest neighbors. Knowl Based Syst 2015;78:13–21.
Loh W-Y, Vanichsetakul N. Tree-structured classification via generalized discriminant analysis. J Am Stat Assoc 1988;83(403):715–25.
Markou M, Singh S. Novelty detection: a review part 1: statistical approaches. Signal Process 2003a;83(12):2481–97.
Markou M, Singh S. Novelty detection: a review part 2: neural network based approaches. Signal Process 2003b;83(12):2499–521.
Neter J, Kutner MH, Nachtsheim CJ, Wasserman W. Applied linear statistical models, vol. 4. Irwin, Chicago; 1996.
NSL-KDD, 2014. NSL-KDD dataset. ⟨http://nsl.cs.unb.ca/NSL-KDD/⟩, [Online; accessed 2-April-2014].
Rubin S, Jha S, Miller BP. Automatic generation and analysis of nids attacks. In: 20th annual computer security applications conference, 2004, IEEE; 2004. p. 28–38.
Sanei S, Smaragdis P, Ho AT, Nandi AK, Larsen J. Guest editorial: machine learning for signal processing. J Signal Process Syst 2015;79(2):113–6.
Sani RA, Ghasemi A. Learning a new distance metric to improve an svm-clustering based intrusion detection system. In: 2015 international symposium on artificial intelligence and signal processing (AISP), IEEE; 2015. p. 284–9.
Shawe-Taylor J, Cristianini N. Kernel methods for pattern analysis. Cambridge, UK: Cambridge University Press; 2004.
Shyu M-L, Sarinnapakorn K, Kuruppu-Appuhamilage I, Chen S-C, Chang L, Goldring T. Handling nominal features in anomaly intrusion detection problems. In: 15th international workshop on research issues in data engineering: stream data mining and applications, 2005. RIDE-SDMA 2005, IEEE; 2005. p. 55–62.
Stein G, Chen B, Wu AS, Hua KA. Decision tree classifier for network intrusion detection with ga-based feature selection. In: Proceedings of the 43rd annual southeast regional conference, vol. 2, ACM; 2005. p. 136–41.
Tan J, Chen X-s, Du M, Zhu K. A novel internet traffic identification approach using wavelet packet decomposition and neural network. J Cent South Univ 2012;19(8):2218–30.

Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A detailed analysis of the kdd cup 99 data set. In: Proceedings of the second ieee international conference on computational intelligence for security and defense applications, CISDA'09, Piscataway, NJ, USA: IEEE Press; 2009. p. 53–8.

Thomas JJ, Cook KA. A visual analytics agenda. IEEE Comput Graph Appl 2006;26 (January (1)):10–3 URL http://dx.doi.org/10.1109/MCG.2006.5.

Vapnik VN. Statistical learning theory. New York, USA: Wiley-Interscience; 1998.

Wang G, Chen S, Liu J. Anomaly-based intrusion detection using multiclass-svm with parameters optimized by pso; 2015.

Worden K, Dulieu-Barton J. An overview of intelligent fault detection in systems and structures. Struct Health Monit 2004;3(1):85–98.

Xiang C, Yong PC, Meng LS. Design of multiple-level hybrid classifier for intrusion detection system using bayesian clustering and decision trees. Pattern Recognit Lett 2008;29(7):918–24.

Yang W, Sun C, Zhang L. A multi-manifold discriminant analysis method for image feature extraction. Pattern Recognit 2011;44(8):1649–57.