We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

186,000
International authors and editors

200M
Downloads

154
Countries delivered to

Our authors are among the

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS

BOOK CITATION INDEX

INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Anomaly-Based Intrusion Detection System

Veeramreddy Jyothsna and Koneti Munivara Prasad

Abstract

Anomaly-based network intrusion detection plays a vital role in protecting networks against malicious activities. In recent years, data mining techniques have gained importance in addressing security issues in network. Intrusion detection systems (IDS) aim to identify intrusions with a low false alarm rate and a high detection rate. Although classification-based data mining techniques are popular, they are not effective to detect unknown attacks. Unsupervised learning methods have been given a closer look for network IDS, which are insignificant to detect dynamic intrusion activities. The recent contributions in literature focus on machine learning techniques to build anomaly-based intrusion detection systems, which extract the knowledge from training phase. Though existing intrusion detection techniques address the latest types of attacks like DoS, Probe, U2R, and R2L, reducing false alarm rate is a challenging issue. Most network IDS depend on the deployed environment. Hence, developing a system which is independent of the deployed environment with fast and appropriate feature selection method is a challenging issue. The exponential growth of zero-day attacks emphasizing the need of security mechanisms which can accurately detect previously unknown attacks is another challenging task. In this work, an attempt is made to develop generic meta-heuristic scale for both known and unknown attacks with a high detection rate and low false alarm rate by adopting efficient feature optimization techniques.

Keywords: intrusion detection, data mining, classification based, DoS, Probe, U2R, R2L, false alarm rate, zero-day attacks

1. Introduction

1.1 Internet security

Today, the world has numerous inventions and technological developments with proliferation of the Internet. Advances in business forced the organizations and governments worldwide to invent and use sophisticated and modern networks. These networks mix a variety of security aspects such as encryption, data integrity, authentication, and technologies like distributed storage systems, voice over Internet protocol (VoIP), wireless access, and web services.

Enterprises are more available to these systems. For instance, numerous business associations enable access to their administration on the system through intranet and web to their partners; endeavors empower clients to connect with the systems by means of web-based business exchanges that enable representatives to get to

data by methods for virtual private systems. This usage makes it more vulnerable to attacks and intrusions. A security threat comes not only from the external intruders but also from internal user in the form of abuse and misuse. A firewall simply blocks the network but cannot protect against intrusion attempts. In contrast, intrusion detection system (IDS) can monitor the abnormal activities on the network.

1.2 Intrusion detection systems (IDS)

Intrusion detection systems play a vital role in research and development with an increase in attacks on computers and networks [1]. Intrusion detection systems monitor the events occurring in a computer system or networks for analyzing the patterns of intrusions. IDS examine a host or network to spot the potential intrusions. Host-based systems explore the system calls and process identifiers mainly related to the operating system data. On the other hand, network-based systems analyze network-related events like traffic volume, IP address, service ports, and protocol used. Intrusion detection systems will

i.   analyze and monitor the system and user activities;

ii. assess the integrity of critical system and data files; and

iii. provide statistical analysis of activity patterns.

1.3 Taxonomy of intrusion detection systems

The intrusion detection systems are broadly classified as

i. misuse detection systems and

ii. anomaly-based detection systems.

1.3.1 Misuse detection systems

A misuse detection system is also called as signature-based detection that uses recognized patterns [2]. These patterns describe suspect, collection of sequences of activities or operations that can be possibly be harmful and stored in database. It uses well-defined patterns of the attack that exploits the weaknesses in system. The time taken to match with the patterns stored in the database is minimal. A key benefit of these systems is that the patterns or signatures can easily develop and understand the network behavior if familiar. It is more efficient to handle the attacks whose patterns are already maintained in the database.

The major restriction of these signature-based approaches is that they can only detect the intrusions whose attack patterns are already stored in the database. For every attack, its signature is to be created. Attacks whose patterns are not present in the database cannot be detected. Such technique can be easily deceived as they are dependent on a specific set of expressions and string matching. In addition, the signature works well only against fixed behavioral patterns; they fail to handle the attacks with human interference or attacks with inherent self-modifying behavioral characteristics.

These detection systems are also ineffective in cases where client works on new technology platforms such as no operation (NoP) generators, encoding, and decoding payloads. The efficiency of the signature-based systems decreases due to the need of creating dynamic signatures for different variations. With growing

volume of signatures, the performance of the engine also might lose the momentum. Because of this, intrusion detection frameworks are conducted on multiprocessors and Gigabit cards. IDS developers develop new signatures before the attackers develop solutions, in order to prevent any new kind of attacks on the system.

1.3.2 Anomaly-based detection systems

Network behavior is the major parameter on which the anomaly detection systems rely upon. If the network behavior is within the predefined behavior, then the network transaction is accepted or else it triggers the alert in the anomaly detection system [3]. Acceptable network performance can be either predetermined or learned through specifications or conditions defined by the network administrator.

The crucial stage of behavior determination is regarding the ability of detection system engine toward multiple protocols at each level. The IDS engine must be able to understand the process of protocols and its goal. Despite the fact that the protocol analysis is very expensive in terms of computation, the benefits like increasing rule set assist in lesser levels of false-positive alarms.

Defining the rule sets is one of the key drawbacks of anomaly-based detection. The efficiency of the system depends on the effective implementation and testing of rule sets on all the protocols. In addition, a variety of protocols that are used by different vendors impact the rule defining the process.

In addition to the aforesaid, custom protocols also add complexity to the process of rule defining. For accurate detection, the administration should clearly understand the acceptable network behavior. However, with strong incorporation of rules and protocol, the anomaly detection procedure would likely to perform more efficiently.

However, if the malicious behavior falls under the accepted behavior, in such conditions it might get unnoticed. The major benefit of the anomaly-based detection system is about the scope for detection of novel attacks. This type of intrusion detection approach could also be feasible, even if the lack of signature patterns matches and also works in the condition that is beyond regular patterns of traffic.

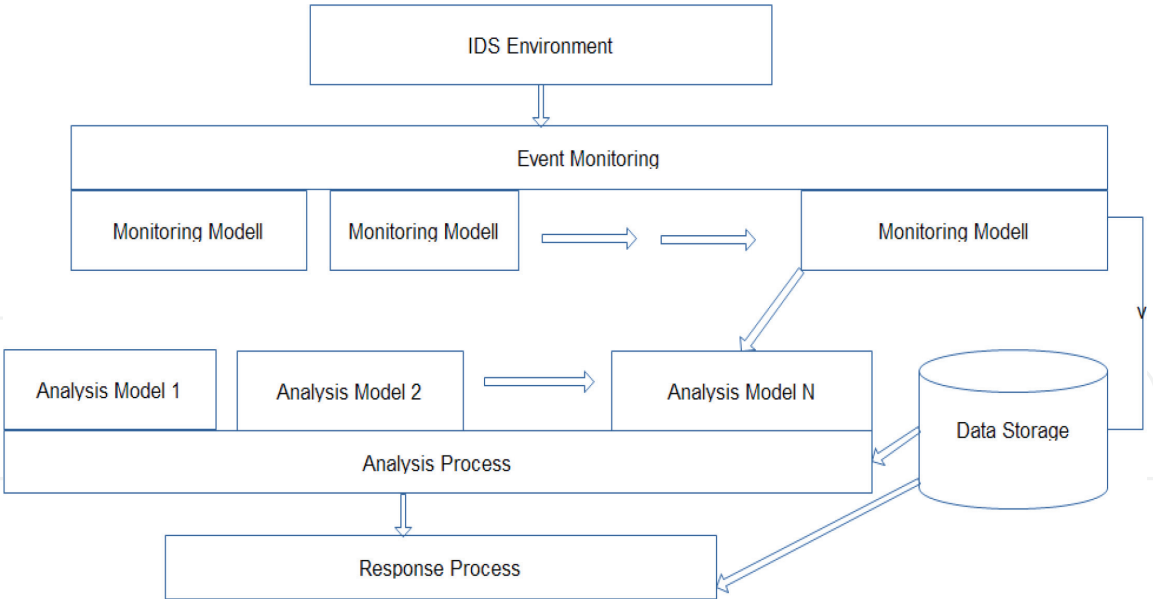## 2. Network intrusion detection systems framework

In **Figure 1**, common intrusion detection framework (CIDF) integrated with Internet Engineering Tasks Force (IETF) and Intrusion Detection Working Group (IDWG) has successfully achieved efficient performance in representing the framework. This group defines a basic IDS structural design based on four functional modules.

Event modules (E-Modules) are defined as a combination of sensing elements and are engaged in continuous monitoring of the end system. In addition, these modules are also involved in processing the information events to the bottom three modules for further analysis.

Analysis modules (A-Modules) analyze the events and detect probable aggressive behavior, in order to ensure that some kind of alarm generated in essential conditions.

Data storage modules (D-modules) store the data from the E-Modules for further processing by the other modules.

Response modules (R-Modules) are used to provide the response to the transactions based on the information obtained from the analysis module.

Figure 1.
Common intrusion detection framework architecture.
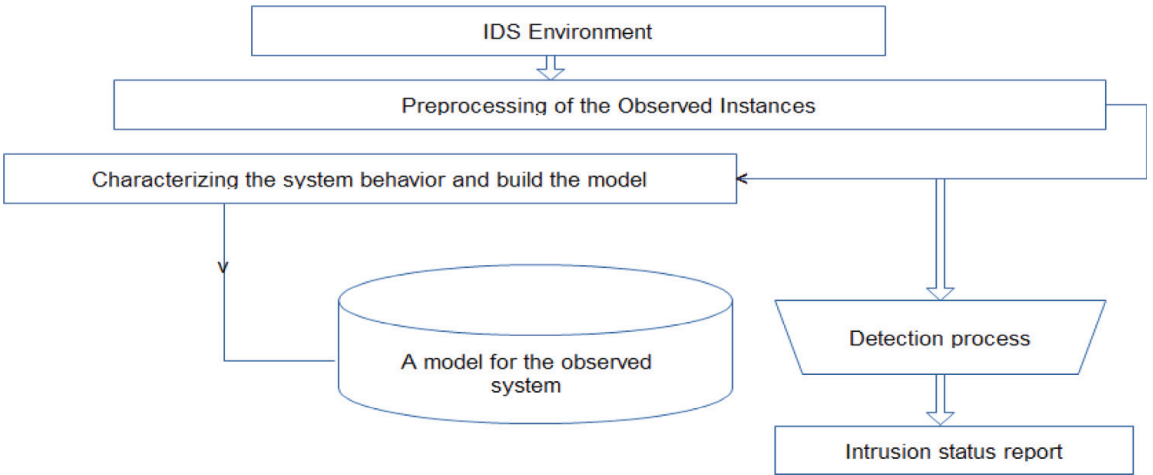
Figure 2.
Common anomaly-based network IDS.

Figure 2 represent the Common anomaly-based network IDS. The functional stages normally adopted in the anomaly-based network intrusion detection systems (ANIDS) are as follows:

Formation of attributes: In this stage, preprocessing of the attributes is done based on the target system.

Observation stage: A model that is built on the basis of behavioral features of the specified system where observations of intrusions can be carried out either through automatically or by manual detection procedure.

Functional stage: It is also called as detection stage. If the characterizing system model is available, it will match with the observed traffic.

3. Anomaly-based intrusion detection techniques

Figure 3 represents the taxonomy of anomaly-based intrusion detection techniques. They are statistical based, cognitive based or knowledge based, machine learning or soft
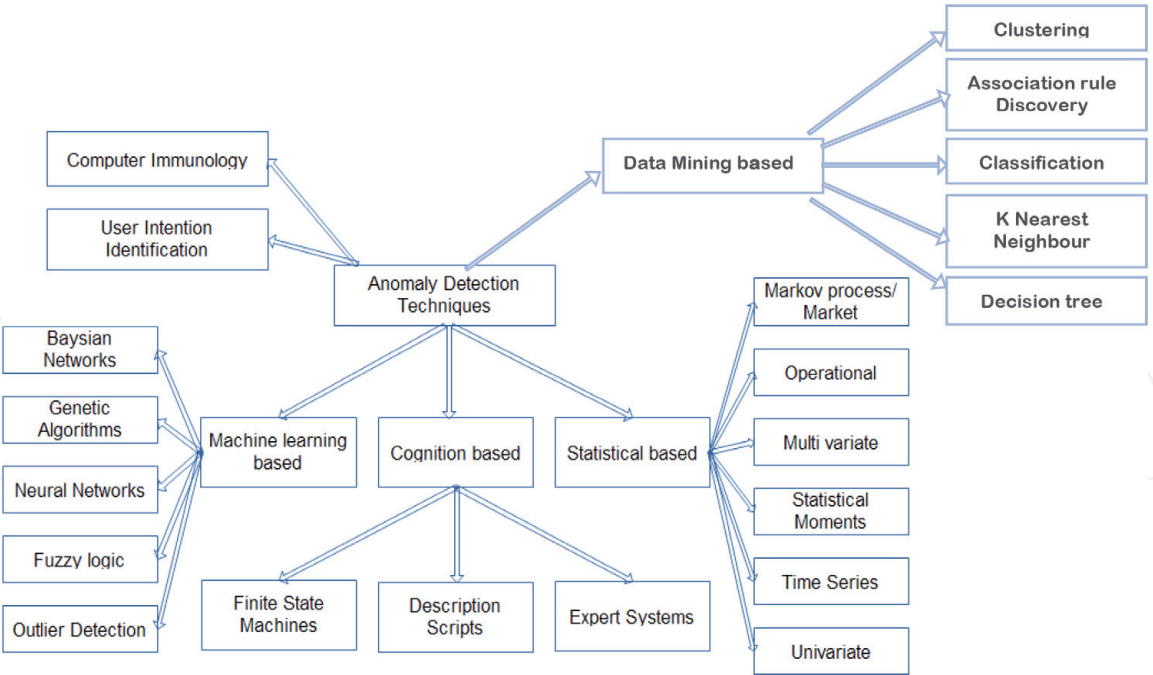
Figure 3.
Classification of anomaly-based intrusion detection techniques.

computing based, data mining based, user intention identification, and computer immunology.

3.1 Statistical-based techniques

Statistical-based techniques use statistical properties such as mean and variance on normal transaction to build the normal profile [4]. The statistical tests are employed to determine whether the observed transaction deviates from the normal profile. The IDS assigns a score to the transactions whose profile deviates from the normal. If the score reaches the threshold, alarm is raised. The threshold value is set based on count of events that occur over a period of time.

Statistical-based techniques are further classified into operational model or threshold metric, time series model, Markov process model or Marker model, parametric approaches, statistical moments or mean and standard deviation model, multivariate model, and nonparametric approaches.

The main advantages of statistical-based techniques are as follows:

i. They do not require any prior knowledge about the signatures of the attacks. So, they can detect zero-day attacks.

ii. As the system is not depended on any of the signatures, updating is not required. Hence it is easy to maintain.

iii. The intrusion activities that were occurred over extended period of time can be identified accurately and are good at detecting DoS attacks.

The disadvantages of statistical-based techniques are as follows:

i. They need accurate statistical distributions.

ii. The learning process of statistical-based techniques takes days or weeks to become accurate and effective.

3.2 Cognitive-based or knowledge-based techniques

Knowledge-based techniques are used to extract the knowledge from the specific attacks and system vulnerabilities. This knowledge can be further used to identify the intrusions or attacks happening in the network or system. They generate alarm as soon as an attack is detected. They can be used for both misuse and anomaly-based detection [5].

The knowledge-based techniques are broadly classified as state transition analysis, expert systems, and signature analysis.

The knowledge-based techniques possess good accuracy and very low false alarm rates. The knowledge gathered makes security analyst easier to take preventive or corrective action.

The knowledge-based techniques are maintaining the knowledge of each attack based on the careful and detailed analysis performed; it is a time-consuming task. A prior knowledge to update the each attack is a difficult task.

3.3 Data mining-based techniques

The knowledge-based IDS can detect the attacks whose patterns are known, but it is difficult to detect the inside attacks. One of the solutions is data mining techniques. The core idea is to extract the useful patterns and also the previously ignored patterns from the dataset [6].

The data mining-based techniques are further classified into clustering, association rule discovery, classification, K-nearest neighbor, and decision tree methods.

The key advantages of data mining-based techniques are as follows:

  i. They can handle high dimensional data.

  ii. As the precomputed models are designed in the training phase, comparing each instance at the testing phase can be done in faster way.

  iii. They can generate the patterns in unsupervised mode.

The key disadvantages of data mining-based techniques are as follows:

  i. These methods identify abnormalities as a by-product of clustering and as are not optimized for anomaly detection.

  ii. They require high storage and are slow in classifying due to high dimensionality.

3.4 Machine learning or soft computing-based techniques

Machine learning can be characterized as the capacity of a program or potentially a framework to learn and improve their performance on a specific task or group of tasks over a time [7]. Machine learning strategies emphasize on building a framework that enhances its execution based on previous results, that is, it can change their execution strategy based on recently acquired data.

Machine learning-based techniques are broadly classified as Bayesian approaches, support vector machines, neural networks, fuzzy logic, and genetic algorithms. Their key advantage is flexibility, adaptability, and capture of interdependencies. The disadvantage is high algorithmic complexity and long training times.

3.5 User intention identification

Intrusion detection system can be built based on the features that categorize the user or the system usage, to distinguish the abnormal activities from normal activities. During the early investigation of anomaly detection, the main emphasis was on profiling system or user behavior from monitored system log or accounting log data. The log data or system log may contain UNIX shell commands, system calls, key strokes, audit events, and network packages used.

3.6 Computer immunology

Computer immunology is a field of science that includes high-throughput genomic and bioinformatics approaches to immunology. The main objective is to convert immunological data into computational problems, solve these problems using statistical and computational approaches, and then convert the results into immunologically meaningful interpretations.

4. NSL-KDD dataset

The NSL-KDD [8] dataset is a refined version of its predecessor KDD99 dataset. NSL-KDD dataset comprises close to 4,900,000 unique connection vectors, where every connection vector consists of 41 features of which 34 are continuous features and 07 are discrete features. Each vector is labeled as either normal or attack. There are four major categories of attacks labeled in NSL-KDD: denial of service attack, probing attack, users-to-root attack, and remote-to-local attack.

   i. *Denial of service attack (DoS):* Denial of service is an attack category, which exhausts the victim's assets, thereby making it unable to handle legitimate requests. Examples of DoS attacks are "teardrop," "neptune," "ping of death (pod)," "mail bomb," "back," "smurf," and "land."

   ii. *Probing attack* (*PROBE*)*:* Objective of surveillance and other probing attacks is to gain information about the remote victim. Examples of probing attacks are "nmap," "satan," "ipsweep," and "portsweep."

   iii. *Users-to-root attack* (*U2R*)*:* The attacker enters into the local system by using the authorized credentials of the victim user and tries to exploit the vulnerabilities to gain the administrator privileges. Examples of U2R attacks are "load module," "buffer overflow," "rootkit," and "perl."

   iv. *Remote-to-local attack* (*R2L*)*:* The attackers access the targeted system or network from the remote machine and try to gain the local access of the victim machine. Examples of R2L attacks are "phf," "warezmaster," "warezclient," "spy," "imap," "ftp write," "multihop," and "guess passwd."

5. Issues and challenges in anomaly-based intrusion detection systems

Although many methods and systems have been developed by the research community, there are still a number of open research issues and challenges. Some of the research issues and challenges of AIDS are as follows:

i. A network anomaly-based IDS should reduce the false alarm rate. But, totally mitigating the false alarm is not possible. Developing an intrusion detection system independent of the environment is another challenge task for the network anomaly-based intrusion detection system development community [9–13].

ii. Developing a general methodology or a set of parameters that can be used to evaluate the intrusion detection system is another challenging task [12, 13].

iii. When new patterns are identified in ANIDS, updating the database without compromise of performance is another challenging task [9, 13].

iv. Another task to be addressed is to reduce the computational complexities of data preprocessing in the training phase and also in the deployment phase [9, 10].

v. Developing a suitable method for selecting the attributes for each category of attack is another important task [9–11].

vi. Identifying a best classifier from a group of classifiers that is nonassociated and unbiased to build an effective ensemble approach for anomaly detection is another challenge [9–11].

6. Feature optimization using canonical correlation analysis

The preprocessed set of network transactions are partitioned based on its labeling ("normal" transactions as one set, "DoS" transactions as the other set and similar other range of sets). Unique values of each feature value set $f_i v(NTS)$ in the resultant normal transactions set (NTS) and its percentage of coverage are:

$$f_i v = \left\{ f_i(v_1, c_1), f_i(v_2, c_2), f_i(v_3, c_3), f_i(v_4, c_4), \ldots\ldots\ldots\ldots f_i(v_j, c_j) \right\} \qquad (1)$$

The procedure for feature optimization for each attack A_k is as follows:

i. Consider the transactions set $ts(A_k)$ denoting attack type A_k (as an example considers DoS as an attack).

ii. For every feature $f_i(A_k)$, consider all the values as a set $f_i v(A_k)$. An empty set $\overline{f_i v}$ of size $|f_i v(A_k)|$ is created and fills it based on its coverage as $|f_i v(A_k)| \cong |\overline{f_i v}|$, in which $|f_i v(A_k)|$ denotes the size of the feature values set of $f_i(A_k)$.

iii. The process is used to generate the feature values vector $\overline{f_i v}$ of the NTS, such that $\overline{f_i v}$ is compatible to the "$f_i v(A_k)$" toward size and that also represents the coverage ratio of the values in $f_i v(NTS)$.

iv. The process is applied for all feature values set in network transactions of attack A_k.

v. Find the canonical correlation between $f_i v(A_k)$ and $\overline{f_i v}$. If the resultant canonical correlation is less than the threshold or zero, then the feature

$f_i(A_k)$ can be considered as optimal toward assessing the scale of intrusion scope.

It is imperative from the implementation of the above procedure that optimal features of a specific attack A_k can be identified. Further, the optimal features are ordered using the canonical correlation values. The values with lower than threshold are considered as optional set of features. Reducing the features leads to lesser computational complexities to the minimal level. The optimal features shall be used for further assessing the impact scale intrusion of type A_k.

7. Feature association impact scale (FAIS)

The approach for measuring the proposed feature association support *(fas)* metric considers the network transaction of the training dataset. The feature categorical values used in the network transactions are in the form of two independent sets. These values are used to develop a duplex graph between them.

7.1 Assumptions

Let $\{f1, f2, f3, \ldots\ldots fn \forall f_i = \{f_i v_1, f_i v_2, \ldots\ldots\ldots, f_i v_m\}\}$ be the set of categorical features values used for forming the set of network transactions T. Here T is a set of network transaction records of the given training set such as:

$$T = \{t_1, t_2, t_3, \ldots\ldots t_n \forall t_i = \{val(f_1), val(f_2), \ldots val(f_i), val(f_{i+1}), \ldots\ldots val(f_n)\}\}$$
(2)

Categorical values of the set of features related to every network transaction shall be considered as transaction value set *tvs* and all transaction value sets are treated as "*STVS*."

In the description above in Eq. 2, $val(f_i)$ can be expressed as $val(f_i) \in \{f_i v_1, f_i v_2, \ldots\ldots, f_i v_m\}$. The term "feature" refers to the current categorical value of the feature. The two features "$val(f_i)$" and "$val(f_j)$," "$val(f_i)$" are connected with "$val(f_j)$" if and only if $\left(val(f_i), val(f_j)\right) \in tvs_k$.

7.2 Algorithm for FAIS technique

Step 1: The edge weight between the features $val(f_1)$ and $val(f_2)$ is estimated as:

$$w(val(f_1) \leftrightarrow val(f_2)) = \frac{ctvs}{|STVS|}$$
(3)

Step 2: The edge weight between transaction value sets and its corresponding set of feature categorical values can be measured as:

$$E = \{(tvs_i, val_j) : val_j \in tvs_i, tvs_i \in STVS, val_j \in v\}$$
(4)

Step 3: Further assuming the transaction value sets of the given duplex graph as pivots and the feature categorical values as pure prerogatives, the pivot and prerogative values are measured.

Step 3.1: Consider matrix u, which denotes pivot initial value as 1.

Step 3.2: Transpose the matrix A as A'.
Step 3.3: Calculate prerogative weights by multiplying A' with u.
Step 3.4: Calculate original pivot weights using matrix multiplication between A and V.

Step 4: Calculate the feature categorical value *fas* of $f_i v_j$ as:

$$fas(f_i v_j) = \frac{\sum_{k=1}^{|STVS|} \{u(tvs_k) : (f_i v_j \rightarrow tvs_k) \neq 0\}}{\sum_{k=1}^{|STVS|} u(tvs_k)} \tag{5}$$

Step 5: the Feature Association Impact Scale *fais* for every transaction value set tvs_i is estimated as:

$$fais(tvs_i) = 1 - \frac{\sum_{j=1}^{m} \{fas(\{val_j \exists val_j \in V\}) : (val_j \subset tvs_i)\}}{|tvs_i|} \tag{6}$$

Step 6: The Feature Association Impact Scale threshold *faist* can be measured as:

$$faist = \frac{\sum_{i=1}^{|STVS|} fais(tvs_i)}{|STVS|} \tag{7}$$

Step 7: Calculate the standard deviation as:

$$sdv_{faist} = \sqrt{\frac{\left(\sum_{i=1}^{|STVS|} fais(tvs_i) - faist^2\right)}{(|STVS| - 1)}} \tag{8}$$

Step 8: The Feature Association Impact Scale range can be explored as Step 8.1 and Step 8.2:

Step 8.1: Calculate lower threshold of *faist* as $faist_l = faist - sdv_{faist}$.
Step 8.2: Calculate higher threshold of *faist* as $faist_h = faist + sdv_{faist}$.

8. Analysis of experimental results

The total number of records chosen for the test is 25% of the actual dataset, that is, 34,361. The combination of test records chosen is from various categories such as Probe, DoS, U2R, R2L, and Normal. The difference between CC average and standard deviation of CC is called as lower bound of CC threshold. The sum of CC average and standard deviation of CC is called as upper bound of CC threshold.

The records that identified to be normal are 19.8% of the total test data records, with observations of 4.7% of it as "false negatives" and 15.1% of it as "true negatives." The cumulative number of records that are detected as "intruded transactions" is 80.2%, with 75.3% of them being "truly intruded transactions" of test data records and the "false positive" percentage of 4.9% of test data records.

As per the results obtained, the proposed model is found to be accurate up to 90.4%. The experiments are conducted on the same dataset using "anomaly-based network intrusion detection through assessing Feature Association Impact Scale (FAIS)" [14]. The results depict that the proposed model is also scalable and

effective for detecting the scope of intrusion from a network transaction. Despite the fact that the FAIS model proposed shows 88% accuracy, the major limitation is process complexity in training the system. Such process complexities of designing the scale using FAIS are due to the number of features selected for assessing the scale. The issue of selecting the optimal features for training the Intrusion Detection System using Association Impact Scale is significantly addressed in the FCAAIS [15] model.

Table 1 indicates the comparison of performance metrics such as precision, recall/sensitivity, specificity, accuracy, and F-measure of FCAAIS over FAIS. **Figure 4** indicates that the accuracy of FCAAIS with optimal features is 91%, whereas the FAIS accuracy with all features is 88%. The precision of the FCAAIS model with optimal features and FAIS with all features is 92%. The other performance metrics such as sensitivity, specificity, and F-measure is calculated on FCAAIS over FAIS. The sensitivity, specificity, and F-measure are 96, 49, and 95%, respectively, for FCAAIS, whereas sensitivity, specificity, and F-measure are 95, 46, and 91%, respectively, for FAIS.

		FCAAIS	FAIS
	Total number of records tested	34,361	34,361
TP (true positive)	The number of transactions identified as normal, which are actually normal	29,379	27,889
FP (false positive)	The number of transactions identified as normal, which are actually intruded	1968	2752
TN (true negative)	The number of transactions identified as intruded, which are actually intruded	1901	2375
FN (false negative)	The number of transactions identified as intruded, which are actually normal	1113	1345
Precision	TP/(TP + FP)	0.937218873	0.910185699
Recall/sensitivity	TP/(TP + FN)	0.963498623	0.953991927
Specificity	TN/(FP + TN)	0.491341432	0.46323386
Accuracy	(TP + TN)/(TP + TN + FP + FN)	0.910334391	0.880765985
F-measure	2 × (PRECISION × RECALL)/ (PRECISION + RECALL)	0.951646837	0.91131588

Table 1.
Comparison of performance metrics of FCAAIS and FAIS.
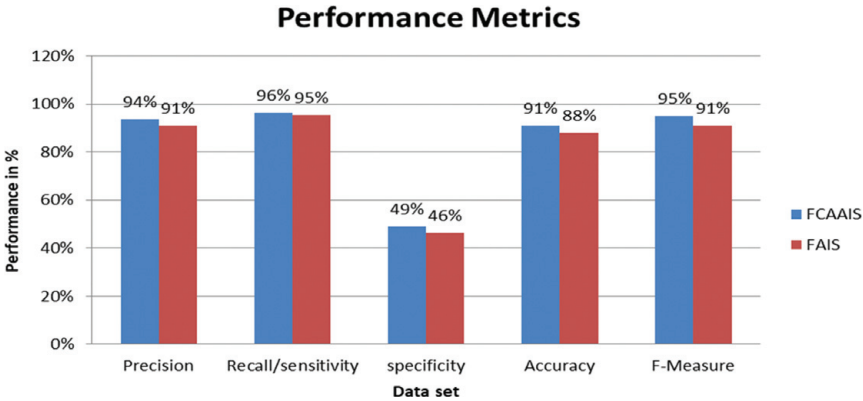
Figure 4.
The performance metrics observed for FCAAIS over FAIS.

According to the results, the accuracy of FCAAIS (selected feature set using canonical correlation) minimized the process complexity of designing the scale using FAIS (**Figure 5** and **Table 2**).

The observed time complexity is adaptable, as the completion time is not directly related to the ratio of features count, which is due to the higher CC threshold as shown in **Figure 6**. Hence it is obvious to conclude that the applying canonical correlation toward optimized attribute selection is significant improvement to the FAIS model (shown in **Figure 6**).

It is observed that applying canonical correlation toward optimized attribute selection results in 3% improvement in the accuracy of FAIS [14]. **Table 3** indicates precision, recall, and F-measure values calculated under divergent canonical correlation threshold values (**Figure 7**).
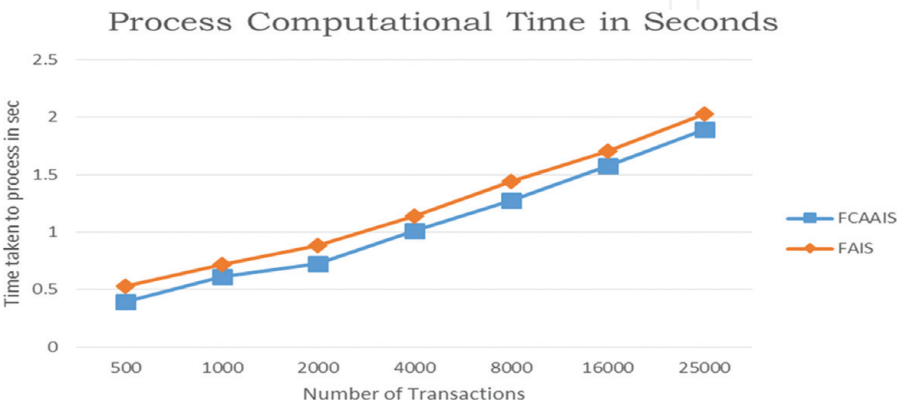

Figure 5.
The process computational time observed for FCAAIS over FAIS.

Number of transactions	FCAAIS (s)	FAIS (s)
500	0.397	0.527
1000	0.611	0.714
2000	0.723	0.882
4000	1.012	1.139
8000	1.275	1.439
16,000	1.578	1.703
25,000	1.891	2.031

Table 2.
Process computational time of FCAAIS and FAIS.
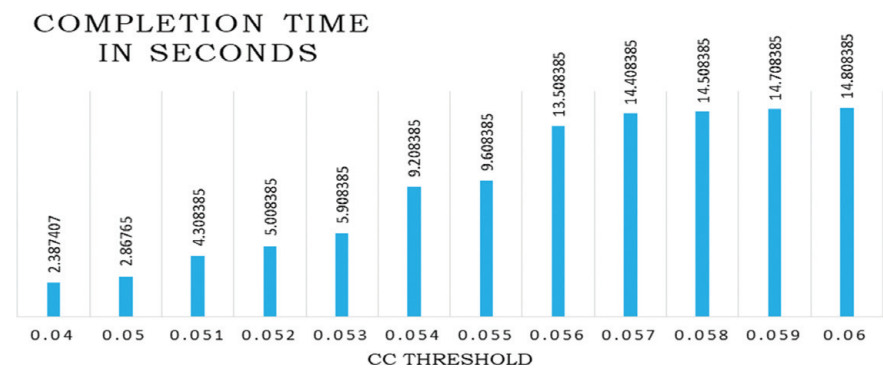
Figure 6.
The FCAAIS consumption of time under divergent canonical correlation thresholds.

	Precision	F-measure	Recall
Less than the upper bound of CC threshold	0.989	0.987998988	0.987
Less than the lower bound of CC threshold	0.98	0.984974619	0.99
Less than the CC threshold	0.985	0.985	0.985

Table 3.
Precision, recall, and F-measure values calculated under divergent canonical correlation threshold.
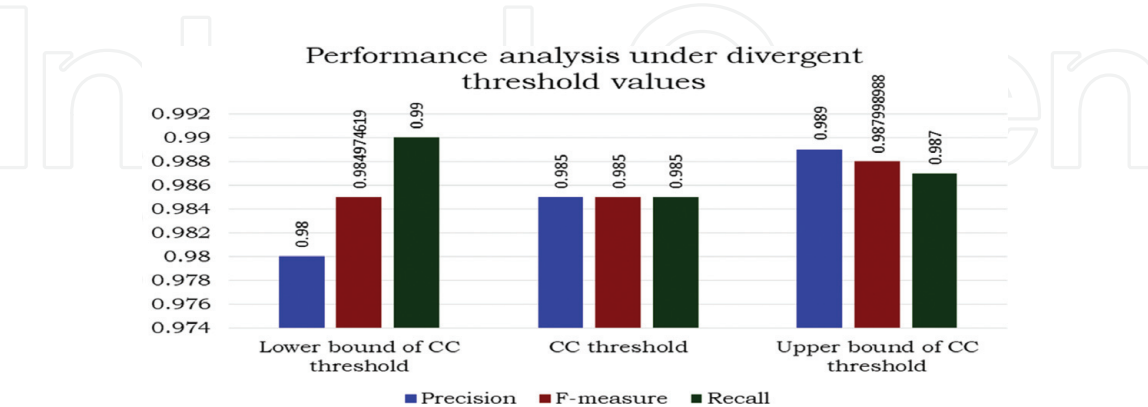
Figure 7.
Performance analysis of the prediction accuracy of FCAAIS under divergent canonical correlation threshold value.

9. Conclusion

It is desirable for anomaly-based network intrusion detection system to achieve high classification accuracy and reduce the process complexity of extracting the rules from training data. In this chapter, a canonical correlation analysis is proposed to optimize the features toward designing the scale to detect the intrusions. The selection of optimal features simplifies the process of FAIS. The experiments were conducted using a benchmark NSL-KDD dataset. The results indicate that the accuracy of FCAAIS with optimal features is 91%, whereas the FAIS accuracy with all features is 88%. The precision of the FCAAIS model with optimal features and FAIS with all features is almost close to 92%. It is observed that applying canonical correlation toward optimized attribute selection has 3% improvement in the accuracy of FAIS. The other performance metrics such as sensitivity, specificity, and F-measure is calculated on FCAAIS over FAIS. The sensitivity, specificity, and F-measure are 96, 49, and 95%, respectively, for FCAAIS, whereas they are 95, 46, and 91%, respectively, for FAIS.

Author details

Veeramreddy Jyothsna[1*] and Koneti Munivara Prasad[2]

1 Sree Vidyanikethan Engineering College, Tirupati, India

2 Chadalawada Ramanamma Engineering College, Tirupati, India

*Address all correspondence to: jyothsna1684@gmail.com

IntechOpen

References

[1] Debar H, Dacier M, Wespi A. A revised taxonomy of intrusion-detection systems. Annales des Telecommunications. 2000;**55**(7–8): 361-337

[2] Gong Y, Mabu S, Chen C, Wang Y, Hirasawa K. Intrusion detection system combining misuse detection and anomaly detection using genetic network programming. In: ICCAS-SICE. 2009

[3] Hall J, Barbeau M, Kranakis E. Anomaly-based intrusion detection using mobility profiles of public transportation users. IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. 2005

[4] Lee J, Moskovics S, Silacci L. A survey of intrusion detection analysis methods. CSE 221, University of California, San Diego, Spring 1999

[5] Prayote A. Knowledge-based anomaly detection [PhD dissertation]. School of Computer Science and Engineering, The University of New South Wales; 2007

[6] Caulkins LTCBD, Lee J, Wang M. A dynamic data mining technique for intrusion detection systems. In: Proceedings of the 43rd Annual Southeast Regional Conference (ACM-SE 43). Vol. 2. 2005. pp. 148-153

[7] Tsai C-F et al. Intrusion detection by machine learning: A review. Expert Systems with Applications. 2009; **36**(10):11994-12000

[8] Revathi S, Malathi DA. A detailed analysis on NSLKDD dataset using various machine learning techniques for intrusion detection. International Journal Engineering Research and Technology (IJERT). Dec 2013;**2**(12)

[9] Bhuyan MH, Bhattacharyya DK, Kalita JK. Network anomaly detection: Methods, systems and tools. IEEE Communications Surveys & Tutorials. 2014;**16**(1):303-336

[10] Wagh SK, Pachghare VK, Kolhe SR. Survey on intrusion detection system using machine learning techniques. International Journal of Computer Applications (0975–8887). 2013;**78**(16): 30-37

[11] Gilmore C, Haydaman J. Anomaly detection and machine learning methods for network intrusion detection: An industrially focused literature review. In: International Conference Security and Management; CSREA Press.

[12] Pedro G-T. Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security. 2009;**28**(1):18-28

[13] Patcha A, Park J-M. An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks. 2007;**51**(12): 3448-3470

[14] Veeramreddy J, Vaddella RPV. Anomaly-based network intrusion detection through assessing feature association impact scale. International Journal of Information and Computer Security. 2016;**8**(3):241-257

[15] Jyothsna V, Rama Prasad VV. FCAAIS: Anomaly based network intrusion detection through feature correlation analysis and association impact scale. ICT Express. 2016;**2**(3): 103-116