Intrusion Detection Framework for Cyber Crimes using Bayesian Network

Chaminda Alocious, Nasser Abouzakhar, Hannan Xiao, Bruce Christianson
University of Hertfordshire, Hatfield, UK
c.alocious@herts.ac.uk
n.abouzakhar@herts.ac.uk
h.xiao@herts.ac.uk
b.christianson@herts.ac.uk

Abstract: Computer Network Security has become a critical and important issue due to ever increasing cyber-crimes. Cybercrimes are spanning from simple piracy crimes to information theft in international terrorism. Defence security agencies and other militarily related organizations are highly concerned about the confidentiality and access control of the stored data. Therefore, it is really important to investigate on Intrusion Detection System (IDS) to detect and prevent cybercrimes to protect these systems. This research proposes a novel distributed IDS to detect and prevent attacks such as denial service, probes, user to root and remote to user attacks. In this work, we propose an IDS based on Bayesian network classification modelling technique. Bayesian networks are popular for adaptive learning, modelling diversity network traffic data for meaningful classification details. The proposed model has an anomaly based IDS with an adaptive learning process. Therefore, Bayesian networks have been applied to build a robust and accurate IDS. The proposed IDS has been evaluated against the KDD DAPRA dataset which was designed for network IDS evaluation. The research methodology consists of four different Bayesian networks as classification models, where each of these classifier models are interconnected and communicated to predict on incoming network traffic data. Each designed Bayesian network model is capable of detecting a major category of attack such as denial of service (DoS). However, all four Bayesian networks work together to pass the information of the classification model to calibrate the IDS system. The proposed IDS shows the ability of detecting novel attacks by continuing learning with different datasets. The testing dataset constructed by sampling the original KDD dataset to contain balance number of attacks and normal connections. The experiments show that the proposed system is effective in detecting attacks in the test dataset and is highly accurate in detecting all major attacks recorded in DARPA dataset. The proposed IDS consists with a promising approach for anomaly based intrusion detection in distributed systems. Furthermore, the practical implementation of the proposed IDS system can be utilized to train and detect attacks in live network traffic.

Keywords: Cybercrimes, Bayesian Network, Intrusion Detection System, DARPRA, Adaptive Learning

1. Introduction

Network and system security provides ability to computer systems to merge and work together in a more secured and trusted environment. Modern day's people used to do their online shopping, learning and bank transactions. These data transferred between different parties must not be revealed to the unauthorized third parties. Therefore, providing integrity, confidentiality and availability of the information carried through the networks is a fundamental responsibility of network security. Therefore, cybercrime protection and network security is becoming increasingly more valuable. Nowadays, networks are built with large, complex systems based upon technologies that designed without security in mind. Simultaneously, these systems are under the experiments of cryptanalysis. Cryptanalysis has made significant inroads towards vulnerable computer system and which most of them have successfully exploited. We are living in an era of nuclear wars and unstable political environment which implies that highly dangerous systems must be highly secured. The implication of cybercrimes has increased ability of unauthorized access to the systems using modern cryptanalysis automated tools. These tools have been made an attacker's job much easier and accurate.

Distributed Denial of Service (DDoS) attacks has become a severe threat to Internet security. DDoS attacks carried out to make system inaccessible by flooding the server's network and end user systems with fake generated traffic. This will stop legitimate users gain access to the system resources. Moreover, problems in network security come in the form of hostile/unwanted trespass either by users or software compromise to unauthorized login, unauthorized elevation of privilege and deployment of viruses. There are three forms of intruders identified in the field of network security; masquerade which is an outsider typical action would be unauthorized access by penetrates system or access controls to exploit a legitimate user's account. The second type of intruder is misfeasor (generally an insider), which is a legitimate user that access data programs resources for which either she/he is unauthorized to access or alternatively to misuse that he/she is authorized to access. Clandestine user (insider or outsider) typically obtains administrator privilege control to avoid auditing access controls or to suppress audit collection. This research considers detecting these types of attacks with an anomaly based IDS (Khor at el, 2009). This research proposes an approach to build a distributed Intrusion Detection System (IDS) with the machine learning technique called Bayesian network (BN). A Bayesian network is an accurate and robust technique to build classification models to classify the normal and abnormal behaviors in network traffic data. This research has investigated towards the artificial intelligence and machine learning technique to construct anomaly based IDS with an adaptive learning process. Bayesian network provides the adaptive nature to the IDS, Bayesian networks are useful tool for determining suspicious activity or security threats in computer systems (Abouzakhar et al, 2010).

2. Research Background

Most of the modern computer systems are distributed systems, such systems are more vulnerable to malicious activities rather a centralized system. The distributed nature of the system allows attackers to use more resources for the attack than centralized systems, also it is difficult to prevent or detect such attacks due to the complexity of the system (Debar,2000). In the context of network security intrusions defined as any malicious activities that could compromise the system integrity, confidentiality, or availability (Debar et al, 2000). Detecting threats using machine learning techniques are more important and one of the most reliable technique is “Bayesian network” (BN) based anomaly based detection. This will eliminate the problem of changing attack signature over the time. A Bayesian network is recognized as a tool for modelling decision equations in graphically, continuing uncertainty. The IDS model proposed by in (Abouzakhar et al, 2011) was able to build an adaptive IDS model using Bayesian networks. In this paper (Abouzakhar et al, 2011) a BN is used to build automatic intrusion detection system based on anomaly detection. In this research (Abouzakhar et al, 2011) authors presenting an adaptive probabilistic approach for intrusion detection using Bayesian network in distributed systems. In this research, Bayesian learning approach for detecting cybercrime is based on detecting signature based threats in a large distributed system dataset. In (Abouzakhar et al, 2011) the developed Bayesian consists with a learning model that corresponds to the adaptive knowledge also includes the dynamic organization of the learning detector and parent variable discovery.

The paper presented in (Howard et al, 2009) has discussed two practical real time applications of Bayesian network for distributed system intrusion detection. Voice-over-IP (VoIP) System and E-commerce system were tested based on their Bayesian network model. The specialty of this effort is Bayesian network was manually created by the expert knowledge and based on attack graph. The Bayesian networks were based on attack graphs that include several multi-step attacks for software vulnerability (Howard et al, 2009). The model explains in this research contains an attack graph, Bayesian algorithm, Inference algorithm and a controller. Bayesian network feature selection has been evaluated by the research effort in (Khor et al, 2009). There are many features selection algorithms that can use in building Bayesian network. This research proposes two feature selecting algorithms, which are used to filter important features from original dataset that can use to build the Bayesian network. Built classifier models evaluated based on three types of a Bayesian network. Firstly, naive Bayes classifiers (NBC) which involves no learning process. Secondly, the Learned Bayesian Network classifiers which uses a learning algorithm to learn the Bayesian structure. Finally, the Expert-elicited Bayesian Network normally utilizes a standard network intrusion dataset [3] to train the structure. The data set contains 4 different types of instances that fall into the category of most known attacks. Denial of service, Probing, Remote to Local (R2L) and User to Root (U2R) are the four main categories of attacks that appear in the dataset (Khor et al, 2009).

Research work presented in (Tang et al, 2009) has addressed the situational awareness, the adaptive detecting ability in the context of Insider cyber threat. Tthis approach using Dynamic Bayesian Network (DBN) as the concept of adapting the changes of the threats. In (Tang et al, 2009) authors claiming that most of traditional IDS or Intrusion prevention systems fail to address the dynamic inference capability and dynamic nature of the threats. In (Tang et al, 2009) authors proposed improved algorithm based on a DBN to recognize the dynamic behavior in the transition relationship of the Hidden Markov Model (HMM). DBN used to detect the user’s session behavior dynamically and must capture these changing situations and capture the future actions based on historic data. The framework in (Tang et al, 2009) established behavior representation by two types of variables called randomly observable state variables and random hidden state variables. This representation (DBN) typically a classification model is transformed into an HMM with the application of inference algorithm. DBN to HMM transformation benefit all three stages of classification model construction, learning and inference. Grid computing is the future of distributed computer systems and grid computer systems uses proxy for credentials authentication and authorization. These credentials will be attacked even they have very short lifetime, but system proposed in (Kunz et al, 2011) presenting a Bayesian network based classifier on this grid computing infrastructure. This Bayesian classifier will detect abuse grid credentials and legitimacy user alteration. Grid computer infrastructure slightly changed to add a Bayesian network classifier that detecting abused grid credentials details. This paper (Kunz et al, 2011) proposed an improved middleware security in the grid infrastructure that increases the grid security up to 99.5%. In this case, Bayesian classifier train data that's collected upon proxy credentials audit records that has labelled as legitimate or abuse. Bayesian classifiers build on the knowledge of both Grid path graph and the credentials graph interconnected or overlay two graphs to correlate the information in both graphs (Kunz et al, 2011).

The paper in (Frigault, 2008) has proposed a DBN approach to detect vulnerabilities in the computer system and address the issue of the changing nature of the threat by the time. When more technical details of the vulnerability published exploitability of the thread become more sophisticated. Mainly, the research (Frigault, 2008) has focused on building a DBN based IDS. The proposed DBN uses for detecting and change the model based on the evolving nature of the threat. DBN can be derived from the attack graphs and attack graphs update with updating constantly changing security environment. The model uses standard CVSS scores which ensure the model can lead to actionable knowledge (Frigault ,2008). This type of IDS endures the nature of the system and attack environment changes. Alma Cemerlic, Li Yang, Joseph M. Kizza in (Cemerlic, 2011) has presented a method with adaptive network intrusion detection with Bayesian network as the model construction technique, Bayesian training done through a mixed dataset containing real-world data and also DARPA dataset traffic. Most of research that focuses on anomaly detection using a statistically based approach, but as in (Cemerlic, 2011) authors mentioned that statistic is not based on a model of adaptive intelligent learning. Bayesian network solves the problem of adaptive learning from the past data. This proposed model that using K2 training algorithm as the Bayesian network learning algorithm and the junction tree as an inference algorithm.

3. Intrusion Detection and Machine Learning

In this section machine learning based ID systems has been discussed in detail with the diversity of methods and modern trends of artificial intelligence and data mining techniques. ID systems were developed to detect and prevent malicious activities and provide strong security for the security critical computer systems. Modern research community investigating towards the intelligent based IDS systems that can detect intrusions with smart behaviors. ID systems are performing the detection of internal and external attackers, one of the major tasks of intrusion detection identifies the unusual patterns in user activities; provide early alarms and taking action against attacks. IDS can be divided into two major categories. Host based intrusion detection systems (HIDS) and Network based intrusion detection (NIDS). HIDS consider the data of local audit records such as windows audit files or process information, but NIDS system analyzes the network traffic data which is a recorded "tcpdump" file from a network. Signature based detection also called as rule based detection determines the user behavior with a comparison of some rules defined related to legitimize the user's behavior. Statistical anomaly Detection is another method used in IDS systems for detecting by data collection carried out for legitimate user over a period of time. Then these learned structures (profiles) can be used to determine unauthorized users' behaviors with the highest level of confidentiality (Mukhopadhyay et al, 2011).

3.1 Signature-based Intrusion Detection

Signature based IDS consists with a database of known signatures of known attacks, these attacks are predefined based on the attack analysis. Most of the signature based system has a low false positive rate, which is really accurate in terms of detecting known attacks by comparing incoming network data with signature database. Modern cyber-attacks are growing rapidly and change its formation regularly. Due to this reason signature based IDS systems are difficult to maintain the demand.

3.1.1 Genetic Algorithms

A genetic algorithm is a computational model, the basic concepts behind genetic algorithm is an evaluation and natural selection. This means only fittest will be survived in the process of natural selection. Genetic algorithms creating set of rules for network data with the following sample structure (Pr-owl). The below connection structure will be searched in the incoming network traffic to find out the attack connections.

If { The connection has following information: source IP address 124.12.5.18;

Destination IP address: 130.18.206.55; Destination port number: 21; Connection time: 10.1 seconds}

Then {Stop the connection}

3.2 Anomaly-based Intrusion Detection

This is the most common and useful IDS method used in network security. This type of methods creates profiles for the normal behavior of the network connections. This normal profiles learned IDS can be used to distinguish the incoming connections as normal or anomaly. Anomaly based ID system's major strength is reliable detection of unknown attacks. However, same time it gives so many false alarms, which eventually cause flooding out the network. The proposed IDS belongs to an anomaly based category. Machine learning techniques for Intrusion detection has become a crucial research area due to its high importance. Machine Learning based IDS systems are still in the early stages, however these methods getting popular. Researches consider the artificial intelligent (AI) techniques and data mining approaches to build more robust, accurate IDS (Kandeeban et al, 2011). In (Mukhopadhyay at al, 2011) explains most of the modern intrusion detection techniques.

3.2.1 Artificial Neural Networks

Artificial Neural Networks can be train with the network traffic data, then use these neural networks to recognize the patterns in network data. These neural patterns can be used to verify and distinguish between intrusion and normal connections. An artificial neural network consists with set of treatments to transform inputs to a set of searching outputs, through a set of simple processing units or nodes and connections between them (Sans Institute, 2011).. The neural network based intrusion detection uses two types of training algorithms called supervised learning and unsupervised learning. Supervised learning state is learning the desired output for a given input. Multilevel perception (MLP), this is the most commonly used supervised learning algorithms (Sans Institute, 2011). Unsupervised neural network learning algorithm (ex: self organized maps) learns without specifying the desired output (Sans Institute, 2011).

3.2.2 Bayesian Network

Bayesian networks apply to many domains such as medical diagnosis, machine learning, speech recognition, signal processing, Bioinformatics, natural language processing and cellular networks (Pr-owl, 2011). Bayesian Networks are very attractive machine learning technique that represents the domain knowledge and domain information in an elegant mathematical structure with simplified visual representation. Bayesian networks are graphically represented models that show a probabilistic relationship between a set of variables under the domain of uncertainty. The Bayesian network structure is represented in a directed acyclic graph and conditional probability tables (CPTs). The CPT table represents the probability of a random variable where, given the occurrence of its parent nodes. However, can we apply the same conceptual strategy to network security with Bayesian network. The computer security and thread models are changing with the time, adaptive Bayesian network is a strategic solution for network intrusion detection.

4. Proposed IDS Model

The proposed IDS has three major functionalities which implemented using WEKA Java API for machine learning. Firstly, the IDS consists with a dataset pre-processing technique such as, attribute selection, attribute filtering, and instance filtering. Secondly, the IDS consists with a Bayesian network classification model, which is the key component in the system, which does the classification of the network data. Thirdly, Inference analyzer which has designed as the prediction module for incoming testing network traffic. These modules named as data preprocessing, Bayesian network structure learning and inference algorithm module to classify the incoming new data respectively.

4.1 Proposed IDS Conceptual Model

The proposed IDS is not merely to detect only denial of service attacks, IDS also capable of detecting other types of attacks which has appeared in testing dataset. This case, those attack types were “probes”, “user to root” and “remote to user” attacks. The major component of the system is the Bayesian network classification model which has four different Bayesian network models, which coordinates together to provide accurate detection results. This will guarantee that very less number of attacks will by-pass the IDS, beacuse each network is a specialist model to detect the special kind of attack type. The main novelty of the proposed IDS is in the form of ability to adapt based on the input dataset. The proposed IDS is capable to work by adding more and more Bayesian network models based on different attacks. Two other major components are data distributor and Inference analyzer.

Pre-processing: Pre-processing is responsible for data preparation for the Bayesian network model learning process. This module uses attribute selection, attribute filtering and instances filtering for preparing the input dataset.

Bayesian network structure learning (Building Bayesian Models): This is the key module of the proposed IDS, proposed architecture contains four Bayesian networks to detect four different attack types. Data distributor is used to feed relevant data (network traffic) to relevant Bayesian network model for training. These models are adaptable to detect new attacks since proposed IDS support adding new Bayesian networks or modifying of existing network with attack's features.

Inference Analyser: Once all the Bayesian network models are built (trained on network traffic) and those networks are ready for predicting attacks in incoming network traffic. Test data divided by inferential analyses to each Bayesian network to classify in the attacks. Inference Analyser classify each record of the input data to normal connection or to a relevant attack. The proposed IDS model has been demonstrated below in detail.

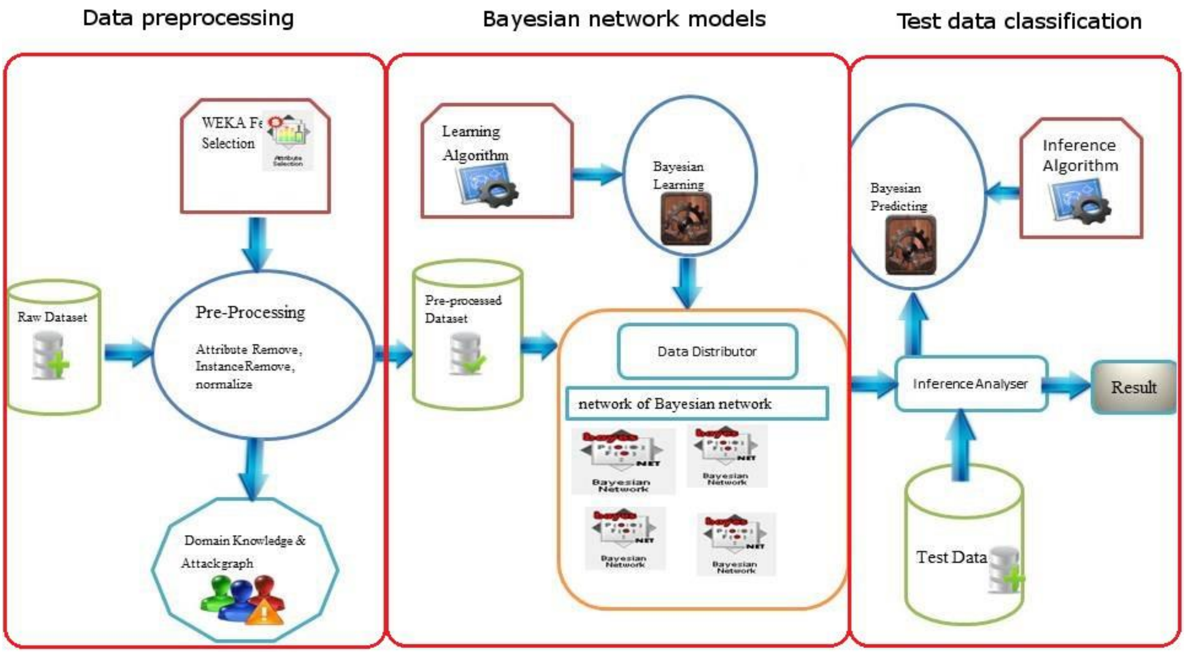


Figure 1: Proposed IDS model using Bayesian Network

4.2 Feature extraction & Data Pre-processing

Data pre-processing is required in order to remove unwanted attributes from the original dataset and construct a dataset which can be used to build a Bayesian network. The feature selection specifically achieved by analyzing, packet information, in this section dataset feature will be analyzed based on the attacks nature and additional domain knowledge. However, since vast numbers of cyber-attacks recorded in KDD dataset, it is better to build a Bayesian network by focussing on each attack type. Identified attack types are DDOS, R2L, U2R and Probes. Data pre-processing including extracting features from original dataset. WEKA attribute filtering has been used with other pre-processing techniques such as attribute selection, attribute discreatize and filling missing instances.

Table 1: Attribute selected for each attack type

Dataset	Attributes
DDoS	This attack type has carefully studied and attributes related to this has been selected. Ex : Protocol type, service, server related attributes (server error rate), file creation, guest login, destination host error rate, destination server error rate and same service rate. (Bayesian network displays the full set of attributes).
Probes	Service, Protocol type, flag ,serror_rate , rerror_rate, same_srv_rate,diff _srv_rate , dst_host_diff_srv_rate, dst_host_srv_diff_host_rate, dst_host_srvserror_rate, dst_host_error_rate, dst_host_srv_rerror_rate

User to Root	Duration, Protocol type, service, src bytes, num compromised, hot, root_shell, dst_host_count ,dst_host_srv count ,dst_host_same_src_port rate, num_failed_logins
Remote to User	duration ,protocol_type ,service ,src_bytes, urgent ,hot ,num_failed_logins lnum_compromised, lroot_shell, is_host_login , dst_host_same_src_port_rate dst_host_rerror_rate ,dst_host_srv_rerror_rate

4.3 Data Distributer

This module's major function is to distribute the training data among the separate Bayesian networks , where each category is designed to train a special kind of attacks. Data distributor is generating four separate "arff" data files that can be used to train the each different network. Input dataset has 41 attributes which must be distributed to each sub dataset based on the configuration setup by attributes removal algorithm.

4.4 Bayesian Network Classifiers Construction

Bayesian network classifiers are built based on the training data provided by data distributor. Bayesian network classifiers building process includes structure learning, parameter learning, and building probability distribution tables for each node in the network. There are two major learning processes for Bayesian network structure learning. The structured learning, also known as casual discovery which is the process that Bayesian network used to learn the structure and parameters with the provided input data. The causal discovery aims to learn the structure and learn the parameters. The proposed IDS is using various algorithms such as K2, Hill climbing and tabusearch. The probability distribution learning achieved with algorithms such as Bayesnet estimator, BMA estimator and multinomial estimator. Once structure learning is complete then parameter learning completes the CPT tables for each feature in the BN.

4.4.1 Bayesian Network Design for DDOS Attacks

The following network design diagram is for detecting distributed denial service attacks. Bayesian network design needs to consider the attributes, search algorithm and estimation algorithms. The "Hillclimber" search algorithm with five parents used as the search algorithm for this network with simple estimator as an estimation algorithm with threshold value "0.5". Finally, After studying the attack graphs and also with the domain expert knowledge and analysis using tools following set of features were selected to construct the DDOS Bayesian network.

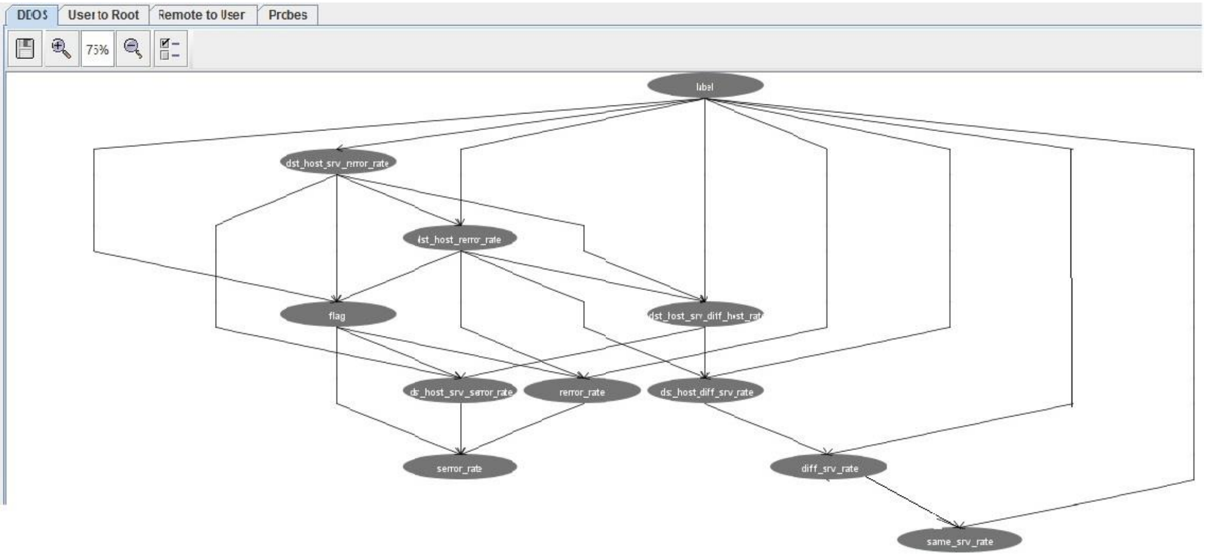


Figure 2: Proposed Bayesian Network for DDOS

The same procedure will be followed to create the Bayesian networks for other attacks types. The proposed IDS allows to integrate new Bayesian network models to the IDS based on the expert knowledge on the modern attacks. In this scenario we have designed three other Bayesian networks for attack types. Such as probing attacks , user to root attacks and remote to user attacks.

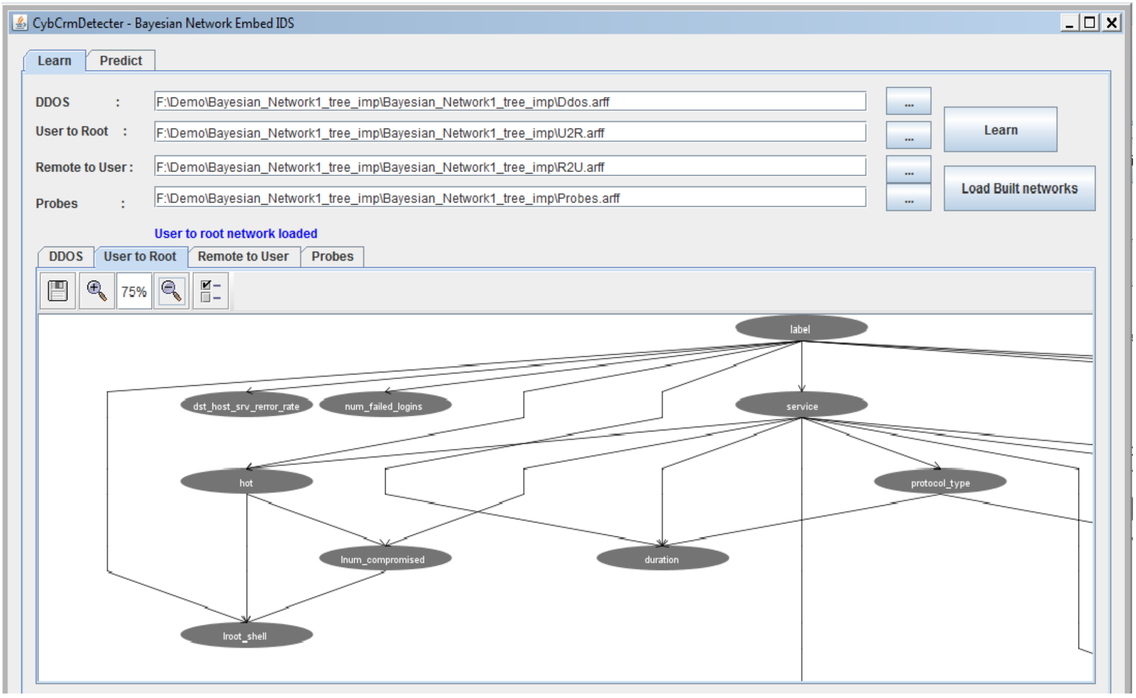
4.4.2 Inference Analyser

The inference analyzers perform the classification of new incoming data with the every relevant Bayesian network model created. Inferential analysis determines which network gives the best result for particular inference effort. Attributes distribution in inferential analyses takes the new connection data and distribute the relevant attributes to the Bayesian network for inference. Once all the virtual datasets created its feed into the inference algorithm which can be used to do the classification of each dataset.

5. Experiments and Results

- Bayesian Network Learning / Training Process

The proposed IDS has been implemented using the Java WEKA library for data mining and machine learning. The implementation consists with four major module's data pre-processing, data distributor, Bayesian structure learning and Bayesian inference analysis. The proposed IDS system prototype was developed as below diagram. Developed system learned with HillClimber algorithm and generate four Bayesian networks and then use those networks to predict on a given test data file.



CybCrmDetecter - Bayesian Network Embed IDS

DDOS : F:\Demo\Bayesian_Network1_tree_imp\Bayesian_Network1_tree_imp\Ddos.arff

User to Root : F:\Demo\Bayesian_Network1_tree_imp\Bayesian_Network1_tree_imp\U2R.arff

Remote to User : F:\Demo\Bayesian_Network1_tree_imp\Bayesian_Network1_tree_imp\R2U.arff

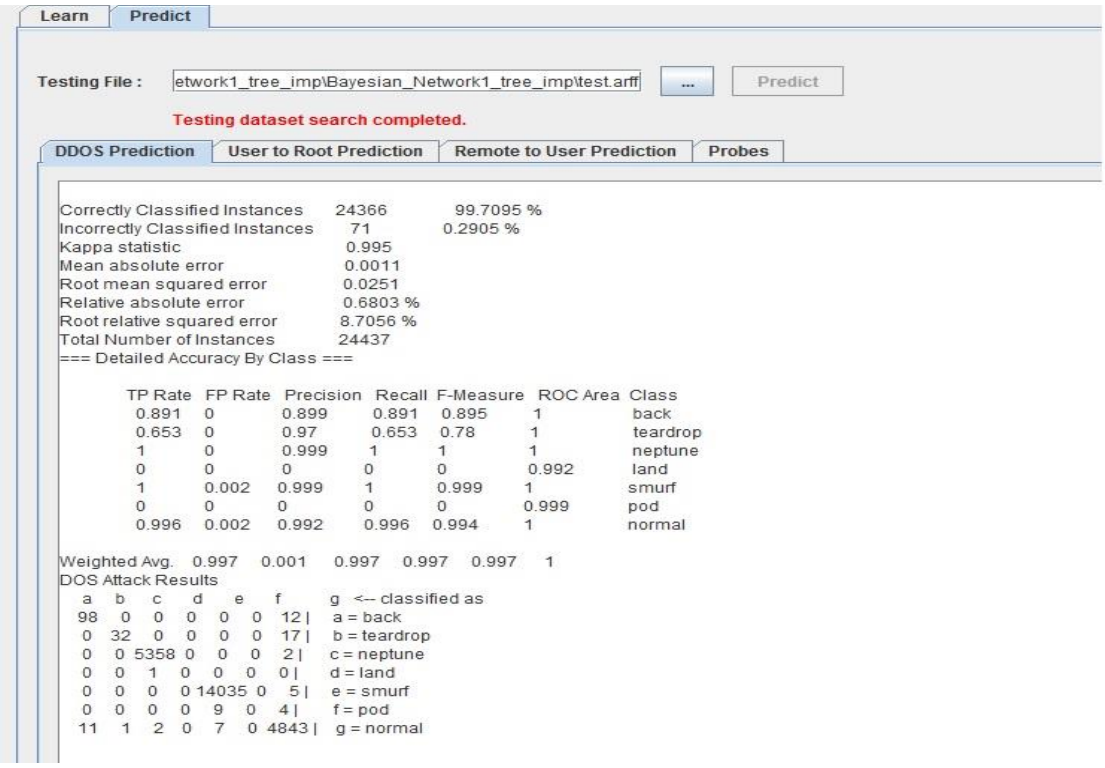
Probes : F:\Demo\Bayesian_Network1_tree_imp\Bayesian_Network1_tree_imp\Probes.arff

User to root network loaded

Figure 3: Proposed IDS Learning Stage Screen

- Bayesian Network Predicting process

Prediction on new test data file and writing the result to the user is displayed as following diagram.



Testing File : etwork1_tree_imp\Bayesian_Network1_tree_imp\test.arff

Testing dataset search completed.

```
Correctly Classified Instances      24366         99.7095 %
Incorrectly Classified Instances       71         0.2905 %
Kappa statistic                       0.995
Mean absolute error                   0.0011
Root mean squared error               0.0251
Relative absolute error               0.6803 %
Root relative squared error           8.7056 %
Total Number of Instances             24437
=== Detailed Accuracy By Class ===

          TP Rate  FP Rate  Precision  Recall  F-Measure  ROC Area  Class
           0.891    0        0.899      0.891   0.895      1          back
           0.653    0        0.97       0.653   0.78       1          teardrop
           1        0        0.999      1       1          1          neptune
           0        0        0          0       0         0.992       land
           1        0.002    0.999      1       0.999      1          smurf
           0        0        0          0       0         0.999       pod
           0.996    0.002    0.992      0.996   0.994      1          normal

Weighted Avg.   0.997    0.001    0.997    0.997    0.997    1
DOS Attack Results
   a    b    c     d     e     f      g   <-- classified as
  98    0    0     0     0     0    12 |   a = back
   0   32    0     0     0     0    17 |   b = teardrop
   0    0 5358     0     0     0     2 |   c = neptune
   0    0    1     0     0     0     0 |   d = land
   0    0    0     0 14035     0     5 |   e = smurf
   0    0    0     0     9     0     4 |   f = pod
  11    1    2     0     7     0  4843 |   g = normal
```

Figure 5: Proposed IDS predicting screen

Experiment of the research has obtained valuable result for detecting DDoS attacks. Experimental setup for the research presented with detail using WEKA Knowledge flow. IDS has evaluated with its true positive, false positive rates with some other parameters such as precision and recall.

5.1 Experimental Setup

In the experiment each Bayesian network trains with relevant attack category instances from the input datasets and build all BN at training stage. Generated BN models are used to classify using one large testing datasets. Normalization of training datasets and testing dataset is done through the WEKA dataset unsupervised learning. Experiment setup can be modelled using the WEKA experimental designing tool as follows.

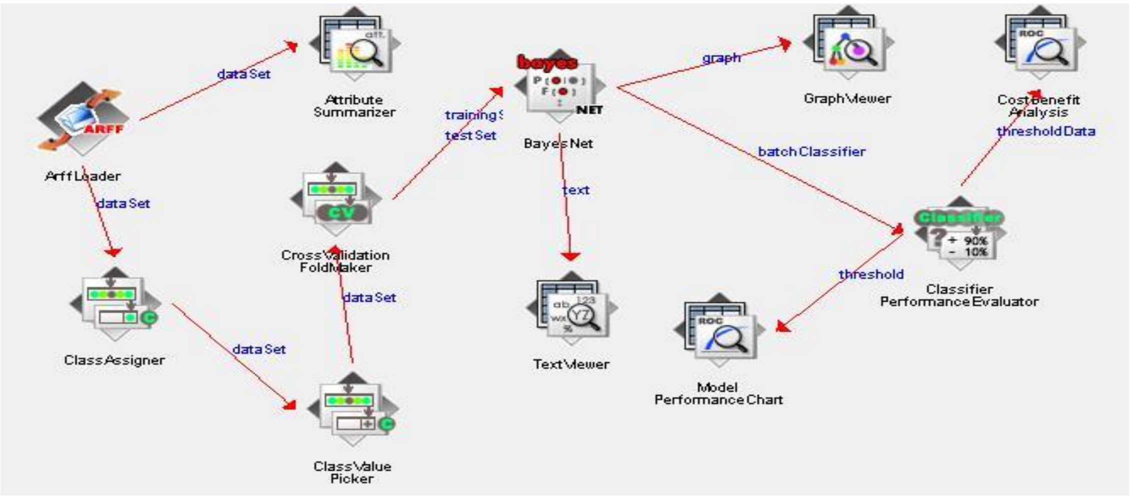


Figure 6：Model Experimental Setup

5.2 Result Evaluation

Experimental data was captured with each attack and their true positive, false positive, precision, recall and F-Measure. Experiment data (training and testing) only based on DARPRA dataset which is quite different than the real world connection data. Therefore IDS accuracy is recorded as high it can be reduced if the experiment's data was real time.
True Positive: This is the rate of correctly classified records out of all records in the give testing dataset.
False Positive: This is the ratio of number of incorrectly classified normal connections.

5.2.1 Performance Evaluation of DDOS Attacks

DDOS attacks are most common and devastating attacks for security critical systems. Experiments carried out to evaluate the proposed systems DDOS attack detection ability. An experiment carried out with 10 folds cross validation, evaluation methods for the following dataset configuration for each attack. The result has categorized as dataset configuration, detail, accuracy by each attack and confusion matrix.

Table 2: DDOS evaluation dataset configuration

Attack name	No of Instances
Back	2203
Neptune	107201
Land	21
Smurf	280790
Pod	264
Normal	97277

Table 3: Result table of DDOS Detailed Accuracy by Class

Attack Name	TP Rate	FP Rate	Precision	Recall	F-Measure
back	0.926	0.02	0.908	0.926	0.917
teardrop	0.982	0.02	0.997	0.982	0.989
neptune	0.99	0.01	1	0.99	1
land	0.857	0.03	0.529	0.85	0.655
smurf	0.99	0.01	1	1	1
Normal	0.998	0.001	0.997	0.998	0.997

Table 4: Confusion matrix for DDOS

Classified as	a	b	c	d	e	f	g
a=back	2039	0	0	0	0	0	164
b=teardrop	0	961	0	0	0	0	18
c=nepture	1	0	107187	8	0	0	5
d=land	0	0	3	8	0	0	5
E=smurf	0	0	0	0	28076	6	23
F=pod	0	0	0	0	2	177	85
G=normal	205	3	0	8	18	5	97038

6. Conclusion

This research proposes a novel distributed IDS to detect and prevent attacks such as denial service, probes, user to root and remote to user attacks. In this work, we implement and evaluate an IDS based on Bayesian network classification modelling technique. The proposed model has an anomaly based IDS system with an adaptive learning process. The proposed IDS system has been evaluated against the KDD DAPRA dataset which was designed for network IDS evaluation. The research methodology consists of four different Bayesian networks as classification models, where each of these classifier models are interconnected and communicated to predict on incoming network traffic data. Each designed Bayesian network model is capable of detecting a major category of attack such as denial of service (DoS). Experiments and project implementation used WEKA Java API to develop the IDS model and required simulation scenarios. Experiments result shows that proposed IDS system's. The experiments show that the proposed system is effective in detecting attacks in the test dataset and is highly accurate in detecting all major attacks recorded in DARPA dataset. Furthermore, the practical implementation of the proposed IDS system can be utilized to train and detect attacks in live network traffic.

7. REFERENCES

Abouzakhar, N. , Gani A., Abuitbel, M. (2010) “Bayesian Learning Networks Approach to Cybercrime Detection”, Proceedings of the 2003 PostGraduate Networking Conference, Vol 1, UK

Kunz, C., Tahmasebi, N. , Risse, T. (2011) “Detecting Credential Abuse in the Grid using Bayesian Networks, Grid Computing (GRID)”, 2011 12th IEEE/ACM International Conference, Vol 8, Lyon

Khor, K. , Ting C., Amnuaisuk S., (2009) “From Feature Selection to Building of Bayesian Classifiers A Network Intrusion Detection Perspective””, American Journal of Applied Sciences, Malaysia

Tang, K.,Tian M., Wang, Z. (2009) Insider Cyber Threat Situational Awareness Framework using Dynamic Bayesian Networks, Computer Science & Education, 2009. ICCSE '09. 4th International Conference

Howard, G., Bagchi, S., Lebanan, G. (2009) Determining Placement of Intrusion Detectors for a Distributed Application through Bayesian Network Modeling, 11th International Symposium, Volume 5230 , pp 271-290 ,RAID 2008, Cambridge, MA, USA

Debar, M., Dacier, Wespi, A. (2000), A revised taxonomy for intrusion-detection," Annals des Telecommunications, Vol. 1,

Lincoln labotary, (2000.), "DARPA Intrusion Detection Data Sets,[online], http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html.

Jemili, .F, Zaghdoud, M. , Ahmed, M. (2007) "A Framework for an Adaptive Intrusion Detection System using Bayesian Network”, IEEE symposium, New Brunswick, NJ

Kendall, .K, (1999) A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems, Massachusetts Institute of Technology

Frigault, M., Lingyu W., (2008) "Measuring Network Security Using Bayesian Network-Based Attack Graphs," Computer Software and Applications, 2008. COMPSAC '08. 32nd Annual IEEE International , vol., no., pp.698,703

Cemerlic, A. , Yang, L. , Kizza, M. (2009) "Network Intrusion Detection Based on Bayesian Networks"

Conrady, S. , Jouffe, L. , (2011) "Introduction to Bayesian Networks Practical and Technical Perspectives"

Wee, Y. , Cheah, W. , Tan, S. (2011)" Causal Discovery and Reasoning for Intrusion Detection using Bayesian Network," International Journal of Machine Learning and Computing (IJMLC), Vol.1(2), 185-192 ISSN: 2010-3700

Korb, K., Nicholson, A. Nicholson, (2004) "Bayesian Artificial Intelligence", [online] , http://www.csse.monash.edu.au/bai/

Wang, Z. , Gombault S. , Guyet, T. (2006)"Towards fast detecting intrusions using key attributes of network traffic," Telecom Bretagne, france, Vol. 1

Kandeeban, S. , Rajesh R.. (2011) "A Mutual Construction for IDS Using GA ," International Journal of Advanced Science, Vol. 29

Mukhopadhyay, I., Chakraborty, M., Chakraborty, S. (2011) "A Comparative Study of Related Technologies of Intrusion Detection and Prevention Systems," Journal of Information Security, Vol. 29

Pr-owl, "Bayesian Netowrk”, http://www.pr-owl.org/basics/bn.phpSans Institute, (2011) "Neural Networks to Intrusion Detection," Journal of Information Security