Asian Journal of Information Technology 11 (5): 153-159, 2012
ISSN: 1682-3915

Network Intrusion Prediction Using Associative Classification Method

[1]Mohd Zakree Ahmad Nazri, [2]Nor Emizan Abdul Majid,
[1]Azuraliza Abu Bakar and [1]Hafiz Mohd Sarim
[1]Center for Artificial Intelligence Technology, Faculty of Technology and Information Science,
Universiti Kebangsaan Malaysia, 46300 Bangi, Selangor, Malaysia
[2]IT Application Management, Export-Import Bank of Malaysia Berhad, Level 13A,
EXIM Bank, Jalan Sultan Ismail, 50250 Kuala Lumpur, Malaysia

Abstract: The increasing rates of intrusion in the network systems has placed many organizations and various institutions in a very vulnerable position of having to face risks which could involve great financial or other losses. A large number of computers have been hacked over the years because some business organizations and other concerns had not taken the essential precautionary measures to protect their networks from cyber-attacks. Since, the frequency of the attacks on the network systems have dramatically increased in number and in the level of destruction over the past years, the Intrusion Detection System has become an important component to ensure the safety for such network systems. This study uses the associative classification algorithm to predict oncoming network intrusions. In order to protect network systems an algorithm is used to detect a variety of relationships and association rules of interest in the flow of traffic incidents. For this research, an attempted network thread data was obtained from a finance company in Malaysia, comprising more than 38,000 records and 20 attributes. The association rule mining is used to discover the sequence of the incidents that enables the model to predict the forth coming incidents in the network systems which in this case are considered as intrusions.

Key words: Network intrusion, sequential incidents, association rule mining, organizations, Malaysia

INTRODUCTION

A large number of Network Intrusion Detection Systems have been developed over the years to prevent network intrusions but however with the latest broadband technology, this problem is yet to be resolved. An Intrusion Detection System (IDS) conducts several important tasks which include observing and analysing users and the systems' activities, auditing the system configurations and limitations, performing statistical analyses on abnormal activities and evaluating the system reliability and the critical files. The IDS should be able to provide reports on the attack in real time and be able to distinguish a legal user from an intruder.

According to Puketza *et al.* (1996) a Security Management Model contains four components, i.e., Prevention, Detection, Investigation and Post-Mortem. To date, the detection component seems to be more important than the investigation and post-mortem components. This has been realized with the emerging softwares such as BRO and SNORT. However, the prevention component may play a vital role in predicting the following attack after a series of network intrusions have been detected. Even though cyber-attacks and hacking are now common phenomena there are however not many researchers who research on finding solutions on network intrusion or on the potential threat prediction.

Although, various networks of IDS are now available in the market, a systems administrator however will still have difficulties in identifying a real intruder that attacks a network system as the system may sometimes set off an inaccurate or a false early warning and therefore a study on achieving accurate warning is still needed. An early warning can be seen as an input that helps a systems administrator to carry out some remedial research and to monitor the network system in order to ensure that it is secure. In this way the level of system availability can be improved. Recently, research in predictive modelling that developed a model for intrusion detection based on data mining techniques has attracted the attention of organizations to safe guard their network systems so that they are secure. Generally, data mining is a process of

Corresponding Author: Mohd Zakree Ahmad Nazri, Center for Artificial Intelligence Technology, Faculty of Technology and Information Science, Universiti Kebangsaan Malaysia, 46300 Bangi, Selangor, Malaysia

discovering important patterns via knowledge from a large amount of data. These patterns can be used to detect or predict forth coming incidents.

Data mining contains several important tasks such as prediction, classification, association rule mining, deviation detection and trend analysis. The classification task has been widely used for network intrusion detection by using several common methods such as Neural Networking and the Support Vector Machine. Another important task in data mining is the Association Rule Mining (ARM) which establishes the important relationship in data based on frequency patterns. ARM is a superset of classification where a larger amount of rules can be generated compared to the classification method. It can be unsupervised since no class label is predetermined in the data. With its special mechanism of finding frequent patterns, it can be also used for network intrusion detection. Several research works have been conducted in using the ARM for network intrusion detection. In using the ARM, traffic flow data recorded by the Intrusion Prevention System (IPS) is mined to discover the relevant and useful rules. These rules are translated as important knowledge for further decisions. However, these researches focus on discovering rules that can classify the threats but not on predicting the incoming incidents.

Literature reivew: Intrusion detection is a process of monitoring and analysing incidents that occur in computer systems in order to detect any security problems (Bace, 2000). The intrusion detection techniques can be defined as a system that identifies and handles an intruder in the computer or network system. In the past 10 years, intrusion detection and security technology such as criptography, verification and rewalls have become very important in safe guarding the networks (Allen *et al*., 2000). However, as more technology is introduced attacks on the computer systems have also become more sofisticated and the attention on newer technology on intrusion detection has arisen (Lippmann *et al*., 2000). Traditionally, the intrusion detection can be classified into two approaches, i.e., the Misuse Detection and the Anomaly Detection (Mounji, 1997). The Misuse Detection tries to detect the well known attack patterns or it clearly identifies attacks. The disadvantage of using this approach however is that it only the identifies attacks that have the sign or character trace that can be detected. On the other hand, the anomaly detection utilizes the user or the systems behavior and the significant deviation from the model as the potential threat. The normal user or systems behavior are known as the user or the system profile.

Recently, the data mining approach has provided several effective ways in detecting intrusions as reported in Bahrololum and Khaleghi (2008) and Betanzos *et al*. (2007). Data mining is a technology that discovers knowledge from the huge amounts of data. The application of data mining techniques can provide a full dicovery network traffic flow data to identify the characteristics and behavior of the traffic that flows in the network system. With its predictive capability, data mining has the potential in preventing any intrusion in the network systems. Generally, data mining consists of several important tasks such as classification, prediction, Association Rule Mining (ARM), sequential rule mining, deviation detection and trend analysis. Many research works solving network intrusion detection problems focus on classsification and the deviation detection task Adetunmbi *et al*. (2008) and Chebrolu *et al*. (2005). Recently, several researchers such as Ezeife *et al*. (2007), Wang *et al*. (2009) and Tsai (2009) have studied the association rule mining tasks for network intrusion detection.

ARM aims to find the relationship and regularities in the item sets of a database. The most commonly used algorithm for ARM is the Apriori Algorithm. Treinen and Thurimella (2006) introduced a framework of ARM in intrusion detection for large scale infrastructures. The study has managed to reduce false positive alarms and has also sped up the generation of new rules. Another research by Ezeife *et al*. (2007) introduces the SensorWebIDS Software which is based on the ARM algorithm. It contains three main components:

- Detection network to extract the parameter from the real-time network traffic flow
- Log mining to extract the parameter from the webpage log files
- The audit engine to analyse all parameter requested by the webpage for intrusion detection

It employs a combination of the anomaly detection and the misuse detection approaches. Their experiment produced a higher webpage intrusion detection rate compared to the existing IDS tool, SNORT.

Associative classification is a data mining approach of using the association rule mining to construct a classification model. This approach is commonly employed when there is a large amount of data and a lot of information that is needed to be in domains such as medical, marketing, banking and science in supplying useful and quality information. There are several techniques in the associative classification as discussed in Thabtah (2007) such as the classification based on

Predictive Association Rules (CPAR) Classification based on Multiple Association Rules (CMAR), Multi Class Classification based on Association Rules (MCAR) and Multi Label Associative Classification (MMAC). The main functions of these algorithms employ different rule discovery, rule ranking, rule pruning, rule prediction and rule evaluation methods.

Literature reviews highlight the use of data mining specifically association rule mining techniques for network intrusion detection. The aim of this study is to employ the ARM based concept of Associative Classification (AC). To date, not many discussions on the prediction of incoming incidents in the network intrusion detection problem has been found. Instead of having techniques that are able to perform detection, it is more important to have a predictive model that can help the network administrator to take remedial action straight away on incoming network intrusion. This is important since sometimes the detection may be too late for the administrator to decide on an immediate solution.

MATERIALS AND METHODS

The methodology of this study comprises five main phases namely: problem formulation, data collection, data preparation, associative classification and testing and evaluation. Data preparation phase is critical in this study since real data and new definitions that are different from the available sources are used in this domain.

Problem formulation: The main aim of this study is to develop a data mining model from the association rule mining algorithm to predict the incoming incidents in network intrusion.

Data collection: The datasets were obtained from a financial company in Kuala Lumpur, Malaysia. The data contains information on the network traffic recorded by the company's main Intrusion Prevention System (IPS). The network traffic records are classified by the IPS automatically. Table 1 shows a sample of the original data.

Table 1: Example of original network data

Date	Time	Priority	Detection engine	Protocol	Source IP
30/12/2010	23:51:18	Medium	DMZ-DE	tcp	10.50.1.3
30/12/2010	23:51:18	High	DMZ-DE	udp	10.30.12.1
30/12/2010	23:48:17	High	DMZ-DE	udp	10.30.12.1
30/12/2010	23:42:08	Medium	DMZ-DE	tcp	10.50.1.3
30/12/2010	23:32:00	High	DMZ-DE	udp	10.30.12.1
30/12/2010	23:25:40	Medium	DMZ-DE	tcp	10.50.1.3
30/12/2010	23:24:26	Low	DMZ-DE	tcp	10.50.1.3

There were 12 attributes collected from the original network database. The attributes of the collected data are date (recorded incident date), time (recorded incident time), priority (incident priority level), detection engine, protocol (protocol used during the incident), SourceIP (incident source IP address), DestinationIP (incident's destination IP address) SRC Port/ICMP Type (port number used by the incident source)DST Port/ICMP Type (port number used by the incident destination), generator (message generator), message (incident's message) and classification (incident's classification).

Data preparation and enhancement: The aim of this study is to predict the next incident or the incident that is expected to occur based on the existing intrusion patterns. Therefore, the data is enhanced through data enrichment. The pattern of the next incident is identified and the new attributes are constructed. The new attributes constructed are nxt_class, nxt_msg, ntx_dst_ip dan time_int. The values for the new attributes are obtained from the next record of data values where they are recorded based on the time interval sequence. The attribute values for the time_int are obtained from the summation of the time difference between the two records. Table 2 shows the new attributes that are obtained.

Attribute reduction: Attribute reduction is the process of selecting the most relevant attribute in solving the main objective of mining. An attribute reduction can improve the efficiency of the mining process thus giving a higher accuracy model than the non-reduced attributes. In this study, 10 attributes that produced the least impact on the prediction modelling process after the data representation were identified. These attributes are date, time, detection engine, protocol, generator, dst_protocol and nxt_msg.

Table 2: Enhanced attributes with representation

Attribute	Description
Date	Recorded incident date
Time	Recorded incident time
Priority	Incident priority level
Detection engine	Trace engine
Protocol	Protocol used by the incident
Src_ip	IP address of incident source
Dst_ip	IP address of incident destination
Src_port	Port number used by the incident source
Src_protocol	Protocol number used by the source incident
Dst_port	Port number used by the incident destination
Dst_protocol	Protocal number used by the incident destination
Generator	Message generator
Msg	Incident message
Class	Incident classification
Nxt_class	Next incident classification
Nxt_msg	Next incident message
Nxt_dst_ip	IP address next incident destination
Time_int	Time interval of next incident

Table 3: Transformed data

dst_ip	dst_port	src_ip	src_port	src_protocol	Priority	msg
dip-3	dp-3	sip-4	sp-2	spro-tcp	Prior-medium	m-29
dip-2	dp-2	sip-7	sp-1	spro-udp	Prior-high	m-3
dip-3	dp-1	sip-2	sp-2	spro-tcp	Prior-medium	m-52
dip-3	dp-2	sip-4	sp-2	spro-tcp	Prior-medium	m-29
dip-2	dp-2	sip-7	sp-1	spro-udp	Prior-high	m-3
dip-3	dp-2	sip-4	sp-2	spro-tcp	Prior-medium	m-29
dip-2	dp-2	sip-7	sp-1	spro-udp	Prior-high	m-3
dip-3	dp-2	sip-4	sp-2	spro-tcp	Prior-medium	m-29
dip-2	dp-2	sip-7	sp-1	spro-udp	Prior-high	m-3

Data transformation: Data transformation is a process of representing, normalising, discretising or rescaling of the data to specific representation that is required by the mining algorithm. In this study all the data except the time_int are transformed to the itemset as data. This process is compulsory since the apriori-like algorithm is used where counting the frequency of the itemset and the rule generation are the main processes. Table 3 shows the sample data after the transformation process. Appendix A shows the detailed data transformation.

Class attribute determination: The main aim of this study is to predict the incoming intrusion that will occur in the network. Three attributes are involved in the creation of the class in the expected incident which is represented as: nxt_class, nxt_dst_ip and time_int. These attributes are combined to form a new class attribute nxt_class. It is transformed as shown in Eq. 1:

$$\text{New nxt\_class} = \text{nxt\_class(nc)-nxt\_dst\_ip-time\_int} \quad (1)$$

For example nc-3-2-5 denotes the original nxt_class = 3 with nxt_dst_ip = 2 and time_int = 5.

Associative classification: Associative classification rule mining originated from the association rule mining algorithm. The basic concept of association rule mining is to find the frequency patterns from the transaction database (Agrawal and Srikant, 1994). Basically, the associative rules are obtained through post mining steps that include removing the redundancy in the association rules, the summarization and the generalization of the association rules, clustering the association rules and creating the associative classifier (Thabtah, 2007).

The patterns are selected if they meet certain minimum support and confidence. To date, there is no fixed formula to determine the value of the minimum support and confidence. The frequency patterns will indicate the occurrence of items at the exact time of transaction. Several experiments were conducted to obtain the appropriate threshold values for this study. The initial support threshold is set from 10-50% with the same confidence value of 90%. The number of rules and the threshold values were recorded. Here the samples of the associative rules with the confidence of 0.98 generated by the associative classification procedure are:

Associative classification rules:

src_ip = sip-7 6487 ⟹ nxt_class = nc-2-3-5
dst_port = dp-2 6565 ⟹ nxt_class = nc-2-3-5
priority = prior-high 7052 ⟹ nxt_class = nc-2-3-5
dst_ip = dip-2 6617 ⟹ nxt_class = nc-2-3-5
dst_ip = dip-2 priority = prior-high 6441 ⟹ nxt_class = nc-2-3-5
src_protocol = spro-tcp 7810 ⟹ nxt_class = nc-2-3-5
src_port = sp-2 7804 ⟹ nxt_class = nc-2-3-5
src_port = sp-2 src_protocol = spro-tcp 7784⟹ nxt_class = nc-2-3-5

Determining minimum support and confidence values: In order to obtain the appropriate threshold value for the min_sup and min_conf, several series of experiments with various parameter settings were conducted. According to Agrawal and Srikant (1994), the high minimum threshold will cause lesser rules to be generated. Thus, the loss of knowledge may occur. In this research the best min_sup range from 10-50% were identified whereas the best min_conf values range from 50-90%. The average number of rules generated for each threshold is shown in Table 4.

Generation of strong rules: In order to obtain a good classification result, the selection of strong rules is critical. There are various techniques to determine the strong rules. In this study, the method proposed by Borgelt (2003) was adopted where the difference between the confidence of the rules generated and the predetermined minimum confidence values are calculated. Rules that give the larger confidence values compared to other rules will be selected as strong rules. For example for two rules P1 and P2 where confidence values are 0.97 and 0.95, respectively with the minimum confidence 0.8, P1 is stronger than P2 since the difference of P1 is 0.17 and P2 is 0.15. However, the threshold of strong rules needs to be determined.

Table 4: Average number of rules generated for each class with various minimum support and confidence values

Minimum support with 90% minimum confidence	No. rules	Minimum confidence with 10% minimum support (%)	No. rules
10	486	50	631
20	344	60	572
30	243	70	529
40	134	80	493
50	38	90	486

Table 5: Strong rules with minimum confidence 70%

Classification rules	Class
dst_ip = dip-4, dst_port = dp-2, src_ip = sip-5, src_port = sp-2, src_protocol = spro-tcp, class = c-4 ⟹ nxt_class = nc-1-2-5	NC-1
dst_ip = dip-2, src_port = sp-1, src_protocol = spro-udp, priority = prior-high, class = c-11 ⟹ nxt_class = nc-2-3-5	NC-2
dst_ip = dip-3, src_port = sp-2, src_protocol = spro-tcp, priority = prior-medium ⟹ nxt_class = nc-3-3-5	NC-3
dst_ip = dip-2, src_ip = sip-3, src_protocol = spro-tcp, priority = prior-high ⟹ nxt_class = nc-4-3-5	NC-4
dst_port = dp-1, src_port = sp-2, src_protocol = spro-tcp, class = c-6 ⟹ nxt_class = nc-5-3-5	NC-5
dst_ip = dip-4, src_ip = sip-8, src_port = sp-2, src_protocol = spro-tcp ⟹ nxt_class = nc-6-4-5	NC-6
dst_port = dp-1, src_port = sp-2, src_protocol = spro-tcp, priority = prior-medium ⟹ nxt_class = nc-7-2-5	NC-7
dst_ip = dip-4, dst_port = dp-2, src_protocol = spro-tcp, priority = prior-low ⟹ nxt_class = nc-8-4-5	NC-8
dst_ip = dip-4, dst_port = dp-1, src_ip = sip-8, src_port = sp-2, src_protocol = spro-tcp, priority = prior-medium ⟹ nxt_class = nc-9-10-5	NC-9
dst_port = dp-1, src_port = sp-2, src_protocol = spro-tcp, priority = prior-medium ⟹ nxt_class = nc-10-2-5	NC-10
src_ip = sip-2, src_port = sp-2, src_protocol = spro-tcp, priority = prior-medium, class = c-2 ⟹ nxt_class = nc-11-2-5	NC-11
dst_port = dp-1, src_port = sp-2, src_protocol = spro-tcp, priority = prior-medium ⟹ nxt_class = nc-12-2-5	NC-12
dst_port = dp-1, src_port = sp-2, src_protocol = spro-tcp, priority = prior-medium ⟹ nxt_class = nc-13-3-5	NC-13

RESULTS AND DISCUSSION

The development of the Incident Prediction Model based on ARM uses the WEKA Software for classification based association. The attribute nxt_class is used as a class attribute in order to predict the incident that is expected to occur. The interesting and strong rules are generated from the association rules and clustered into a set of classification rules. A total of 39 strong rules are extracted from the original rules with an average of 3 rules from each class. Table 5 shows the examples of strong rules extracted and that represent classes NC-1 to NC-13.

A simple voting method is employed for the classification of the new dataset. In this study six records from each category are tested with 39 rules. Table 6 shows the classification test results obtained where out of 79 data 71 are classified correctly while 7 data are classified as uncertain. This is defined as uncertain data since the data is classified into two or more different classes with equal frequency. Thus, both classes are acceptable and both indicate that two potential incidents may occur.

Incident Prediction Model: The uncertain rules are improvised to obtain a set of uncertain rules that are potentially to be used for incident prediction purposes. The rules undergo the process of clustering where some redundant rules are eliminated and some are merged to form a single rule. Table 7 shows the samples of the uncertain classification rules obtained with the variants of the incident categories as the consequence. Based on the rules, the clustered rules can assist the network systems administrator in investigating the incident and be able to take remedial action to protect the network. The reduced number of rules will aid the network administrator in making a prediction of the next incident. Then part of the rules are placed in the sub category that predicts the information of the type of incident that will occur, the target IP destination and the expected time interval of the incident.

Table 6: Classification accuracy

Test results	Correctly classified	Uncertainly classified
No. of test data	71.00	7.00
Accuracy (%)	89.87	8.86

Table 7: Uncertain classification rules

ID	Rules
P1	dst_ip in (dip-2, dip-3, dip-4), dst_port in (dp-1, dp-2), src_ip in (sip-2, sip-5, sip-7), src_port in (sp-1, sp-2), src_protocol in (spro-tcp, scp-udp), priority in (prior-high, prior-medium), class in (c-2, c-4, c-6, c-11) THEN nxt_class = nc-2-3-5 OR nxt_class = 3-1-5 OR nxt_class = nc-1-2-5 OR nxt_class = nc-2-1-5 OR nxt_class = 9-3-5
P2	dst_ip = dip-3, dst_port = dp-1, src_ip = sip-2, src_port = sp-2, src_protocol = spro-tcp, priority = prior-medium, class = c-2 THEN nxt_class = nc-3-3-20 OR nxt_class = nc-4-1-5 OR nxt_class = nc-5-2-20 OR nxt_class = nc-7-2-20
P3	dst_ip in (dip-2, dip-3), dst_port = dp-2, src_ip = sip-3, src_port = sp-2, src_protocol = spro-tcp, priority = prior-medium, class = c-7 THEN nxt_class = nc-4-3-5
P4	dst_ip in (dip-3, dip-4) dst_port in (dp-1, dp-2) src_ip in (sip-2, sip-5) src_port = sp-2 src_protocol = spro-tcp priority = prior-medium class in (c-2, c-4, c-6) THEN nxt_class = nc-4-4-5 OR nxt_class = nc-11-4-5
P5	dst_ip in (dip-2, dip-3) dst_port in (dp-1, dp-2) src_ip in (sip-2, sip-7) src_port in (sp-1, sp-2) src_protocol in (spro-tcp, spro_udp) priority in (prior-medium, prior-high) class in (c-2, c-11) THEN nxt_class = nc-5-2-5 OR nxt_class = nc-5-3-5 OR nxt_class = nc-9-1-5
P6	dst_ip = dip-3 dst_port = dp-1 src_ip = sip-2 src_port = sp-2 src_protocol = spro-tcp priority = prior-medium class in (c-2, c-6) THEN nxt_class = nc-6-2-5 OR nxt_class = nc-6-3-5 OR nxt_class = nc-7-2-5

From the final set of rules obtained, it is indicated that almost all incidents at the targeted IP address (dst_ip) use the lower and middle levels of port numbers (dst_port dan src_port) which involves the large interval between 1024-49151 that can be manipulated by either an internal or an external intruder. These rules are presented to the networks administrator of the company for verification.

Expert verification: Thirty nine rules were presented to two network experts (network administrators who have 5-10 years' experience in network management). The experts verified that the rules are very important and useful and allows them to use them for intrusion prediction and remedial action. The datasets used are the traffic flow and the incident records kept in the log file of the IPS device. The IPS device monitors the traffic flow in a local network system. Therefore, most of the recorded data is identical or repeated data. Basically, the external address intrusion has attracted more attention of the systems administrator in looking for prevention but nevertheless, the internal IP attack is also needed to be considered seriously.

For each rule, a network systems administrator is given the potential incoming incident that may occur in a situation. The rules will support the decision on the incident that it is predicted to occur. The administrator can focus only on the suggestion in the rules as this will save time in taking remedial action/s such as policy updates on firewall or any other network devices. The present rules generated can still be merged but however to reduce the focus of the systems administrator, the rules are retained. The larger rules merge the longer and the length of the consequences of the rules will therefore cause difficulties in decision making. The larger amount of data may provide more useful knowledge through the generation of interesting and strong rules.

CONCLUSION

The generation of associative classification rules limits the vast rules generated by the association rule mining. With the advantages of the apriori algorithm that generates rules based on the frequency of the item set, the intrusion detection problem can be potentially solved in terms of incident prediction. In other words, instead of having the rules that support a decision these rules can be used for prediction. The prediction of the next incident is very useful to the network systems administration since detection maybe too late for remedial action. In this study, the novel results obtained are based on the new term the uncertain classified rules. These rules are improvised in order to produce more interesting rules. Later, these rules can be embedded in the decision support system thus they can be used in the prediction task.

APPENDIX

Data transformation

Attribute	Attribute values	Representation	Attribute	Attribute values	Representation
	External IP Address	sip-1, dip-1, ndip-1		POLICY SMTP relaying denied (1:567)	m-33, nm-33
	10.50.1.x	sip-2, dip-2, ndip-2		SMTP expn root (1:660)	m-34, nm-34
Src_ip	10.30.1.x	sip-3, dip-3, ndip-3		SMTP MDaemon 6.5.1 and prior versions	m-35, nm-35
Dst_ip	10.20.1.x	sip-4, dip-4, ndip-4		MAIL overflow attempt (1:3656)	
Nxt_dst_ip	10.31.1.x	sip-5, dip-5, ndip-5		SMTP Microsoft Outlook Web Access	m-36, nm-36
	10.32.1.x	sip-6, dip-6, ndip-6		From field cross-site scripting attempt (3:13894)	
	10.30.12.x	sip-7, dip-7, ndip-7		SMTP Novell GroupWise client IMG	m-37, nm-37
	10.30.7.x-10.30.11.x	sip-8, dip-8, ndip-8		SRC buffer overflow (1:13364)	
	10.51.0.x	sip-9, dip-9, ndip-9		SMTP SEND overflow attempt (1:3655)	m-38, nm-38
	255.255.x.x	sip-10, dip-10, ndip-10		SMTP vrfy root (1:1446)	m-39, nm-39
Dst_port	0-1023	dp-1, sp-1		SMTP_COMMAND_OVERFLOW (124:1)	m-40, nm-40
Src_port	1024-49151	dp-2, sp-2		SMTP_DATA_HDR_OVERFLOW (124:2)	m-41, nm-41
	49152-65535	dp-3, sp-3		SMTP_HEADER_NAME_OVERFLOW (124:7)	m-42, nm-42
	BACKDOOR Infector.1.x (1:117)	m-1, nm-1		SMTP_RESPONSE_OVERFLOW (124:3)	m-43, nm-43
	BAD-TRAFFIC dns cache poisoning attempt (3:13667)	m-2, nm-2		SPECIFIC-THREATS netsky.q smtp propagation detection (1:9378)	m-44, nm-44
	DNS dns response for rfc1918 10/8 address detected (1:13249)	m-3, nm-3		SQL ping attempt (1:2049)	m-45, nm-45
				SQL sp_password-password change (1:683)	m-46, nm-46
	DNS dns response for rfc1918 172.16/12	m-4, nm-4		WEB-CGI calendar access (1:882)	m-47, nm-47
	DNS named version attempt (1:1616)	m-5, nm-5		WEB-CGI redirect access (1:895)	m-48, nm-48
	DNS SPOOF query response with TTL of 1 min. and no authority (1:254)	m-6, nm-6		WEB-IIS .cnf access (1:977)	m-49, nm-49
				WEB-IIS encoding access (1:1010)	m-50, nm-50
	DNS squid proxy dns PTR record response denial of service attempt (1:17484)	m-7, nm-7		WEB-IIS source code disclosure attempt (1:17648)	m-51, nm-51
				WEB-IIS view source via translate header (1:1042)	m-52, nm-52

Appendix: Continue

Attribute	Attribute values	Representation	Attribute	Attribute values	Representation
	DNS TCP inverse query (1:2922)	m-8, nm-8		WEB-MISC apache directory disclosure attempt (1:1156)	m-53, nm-53
Msg	DNS UDP inverse query (1:2921)	m-9, nm-9		A Network Trojan was Detected	c-1, nc-1
Nxt_msg	DOS Apache mod_ssl non-SSL	m-10, nm-10		Access to a Potentially Vulnerable	c-2, nc-2
	connection to SSL port denial of	m-12, nm-12		Web Application	
	service attempt (1:11263)			An Attempted Login Using a Suspicious	c-3, nc-3
	HI_CLIENT_IIS_UNICODE (119:7)	m-11, nm-11		Username was Detected	
	MS-SQL Suspicious SQL				
	ansi_padding option (1:16075)	m-12, nm-12		Attempted Administrator Privilege Gain	c-4, nc-4
	ORACLE all_constraints access (1:1680)	m-13, nm-13	Classification	Attempted Denial of Service	c-5, nc-5
	ORACLE all_source access (1:1682)	m-14, nm-14	Nxt_class	Attempted Information Leak	c-6, nc-6
	ORACLE all_tab_columns access (1:1684)	m-15, nm-15		Attempted User Privilege Gain	c-7, nc-7

REFERENCES

Adetunmbi, A.O., S.O. Falaki, O.S. Adewale and B.K. Alese, 2008. Network intrusion detection based on rough set and knearest neighbor. Intl. J. Comput. ICT Res., 2: 60-66.

Agrawal, R. and R. Srikant, 1994. Fast algorithms for mining association rules. Proceedings of the 20th International Conference on Very Large Data Bases, September 12-15, 1994, San Francisco, USA., pp: 487-499.

Allen, J., A. Christie, W. Fithen, J. McHugh, J. Pickel and E. Stoner, 2000. State of the practice of intrusion detection technologies. Technical Report CMU/SEI-99-TR-028 ESC-99-028, Carnegie Mellon University. http://www.sei.cmu.edu/reports/99tr028.pdf.

Bace, R.G., 2000. Intrusion Detection. Sams Publishing, USA., ISBN: 1578701856, Pages: 339.

Bahrololum, M. and M. Khaleghi, 2008. Anomaly intrusion detection system using hierarchical gaussian mixture model. IJCSNS Int. J. Comput. Sci. Network Secur., 8: 264-271.

Betanzos, A.A., S.N. Marono, F.M.C. Fortes, J.A.S. Romero and B.P. Sanchez, 2007. Classification of computer intrusions using functional networks: A comparative study. Proceedings of the 15th European Symposium on Artificial Neural Networkss, April 25-27, 2007, Bruges, Belgium.

Borgelt, C., 2003. Apriori: Finding association rules/hyperedges with the apriori algorithm. http://www.kdkeys.net/apriori-finding-association-ruleshyperedges-with-the-apriori-algorithm/.

Chebrolu, S., A. Abraham, J. Thomas, 2005. Feature deduction and ensemble design of intrusion detection systems. Computers Sec., 24: 295-307.

Ezeife, C.I., J. Dong and A.K. Aggarwal, 2007. SensorWebIDS: A web mining intrusion detection. Int. J. Web Inf. Syst., 4: 97-120.

Lippmann, R.P., D.J. Fried, I. Graf, J.W. Haines and K.R. Kendall *et al*., 2000. Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation. Proceedings of the 2000 DARPA Information Survivability Conference and Exposition (DISCEX), Jan. 25-27, IEEE Computer Society Press, Los Alamitos, CA, pp: 12-26.

Mounji, A., 1997. Languages and tools for rule-based distributed intrusion detection. Ph.D. Thesis, Facult-Es Universitaires Notre-Dame De La Paix Namur, Belgium.

Puketza, N.J., K. Zhang, M. Chung, B. Mukherjee and R.A. Olsson, 1996. A methodology for testing intrusion detection systems. IEEE Trans. Software Eng., 22: 719-729.

Thabtah, F.A., 2007. A review of associative classification mining. Know. Eng. Rev., 22: 37-65.

Treinen, J.J. and R. Thurimella, 2006. A framework for the application of association rule mining in large intrusion detection infrastructures. Proceedings of the 9th international conference on Recent Advances in Intrusion Detection, September 20-22, 2006, Hamburg, Germany, pp: 1-18.

Tsai, F.S., 2009. Network intrusion detection using association rules. Int. J. Recent Trends Eng., 2: 202-204.

Wang, H., G. Zhang, H. Chen and X. Jiang, 2009. Mining association rules for intrusion detection. Proceedings of the International Conference on Frontier of Computer Science and Technology, December 17-19, 2009, Shanghai, pp: 644-648.