IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 10-16

Analyzing and Tracing of Various Packet Dropping Attacks Using Containing Order Rough Set

V. A. Afsal Basha, N. Syed Siraj Ahmed
P.G. Department of Computer Science, Islamiah College(Autonomous), Vaniyamabadi, Tamil Nadu, India
Department of Computer Science and Engineering, G P Engineering College, Tirupattur, Tamil Nadu, India

Abstract: *Intrusion detection systems (IDS) aim at determining attacks against information systems in general. It is difficult to provide secure information systems and maintain them in a secure state for their entire lifetime. Maintenance of such information system is technically difficult as well as economically costly. With the invention of new vulnerabilities to information system new techniques for determining these vulnerabilities have been implemented. Today containing order rough set (CORS) has appeared as a useful mathematical tool for dealing with uncertain data. The main theme of this paper is the analysis and evaluation of packet dropping attack data set through the applications of containing order rough set (CORS) and other concerned notations, formalizes method of data analysis of various packet dropping attacks and rule generation.*
Keywords: *IDS; CORS; Data Analysis; Vulnerabilities; Criteria*

I. Introduction

Now-a-days Internet is the best tool for distributed computing which involves dispersion of data geographically. Therefore, it is challenging for human being to retrieve information from the huge amount of data available geographically at different places servers in the world for testing of different types of attacks in the system. Hence, it is very difficult to extract expert knowledge from the universe of system dataset. The problem of imperfect knowledge has been tackled for a long time by philosophers, logicians, and mathematicians. Recently it brings attention for computer scientists, particularly in the area of knowledge mining and artificial intelligence. There are many approaches to the problem of how to understand and manipulate imperfect knowledge. The fundamental one is the crisp set. However, it has been extended in many directions as far as modeling of real life situations are concerned. The earliest and most successful one is being the notion of fuzzy sets by L. A. Zadeh [1] that captures impreciseness information. On the other hand rough sets of Z. Pawlak [2] is another attempt that capture indiscernibility among objects to model imperfect knowledge [3][4][5]. There were many other advanced methods such as rough set with similarity, fuzzy rough set, rough set on fuzzy approximation spaces, rough set intuitionistic fuzzy approximation spaces, dynamic rough set, covering based rough set were discussed by different authors to extract knowledge from the huge amount of data [6][7][8]. Universe can be considered as a large collection of objects. Each object is associated with some information with it. In order to find knowledge about the universe we need to extract some information about these objects. We need sufficient amount of information to uniquely identify the objects which is not possible in case of all objects. Therefore, we require classification of these objects into similarity classes to characterize these objects in order to extract knowledge about the universe. Rough set is an approach to extract knowledge and association between data and values of data in recent years.

However, it generates too many rules that create many difficulties in taking decision for human being. Hence it is challenging for human being to extract expert knowledge. However, many researchers has analyzed medical data by using data mining, fuzzy sets, and formal concept analysis for finding decision rules, and redundancies[7][8].

In this paper, we use two concepts such as packet dropping attack and containing order rough set to explore the relationship among the attributes. In containing order rough set we use rough set to analyze the data using rules of dominance relation whereas in intrusion detection we use formal concept analysis to explore better knowledge and most important characteristics affecting the decision making. The remainder of the paper is organized as follows: Section 2 presents the basics of intrusion detection and various attacks in wireless networks. Section 3 presents the basics of rough set. Section 4 provides data analysis using containing order rough set. The dominance relation rule formation is given in Sections 5. In Section 6, analyzing and tracing of packet dropping attacks is presented. This is further followed by a conclusion in Section 7.

II. Intrusion Detection and Various Attacks in Wireless Networks

Intrusion detection is the process of intelligently monitoring the events occurring in a computer system or network and analyzing them for signs of violations of the security policy, Parker [9] has defined six security

issues to be considered while designing an IDS: Confidentiality, Integrity, Availability, Utility, Authenticity, and Possession of a computer or network. Intrusions are caused by attackers accessing the systems from the Internet, authorized users of the systems who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given to them. Intrusion Detection Systems (IDSs) are software or hardware products that automate this monitoring and analysis process.

There are two main types of Intrusion Detection System (IDS): Signature Based IDS (SBIDS) and Anomaly Based IDS (ABIDS) [9].

In SBIDS, also known as misuse detection, signatures of known attacks are stored and the events are matched against the stored signatures. It will signal an intrusion if a match is found.

ABIDS has attracted many academic researchers due to its potential for addressing novel attacks. Novelty detection is the identification of new or unknown data that a machine learning system is not aware of during training [9].

Initially, Ahmed and Acharjya (2015) introduce the concept to detect denial of service attacks in wireless network using dominance based rough set [10].

Similarly, Ahmed and Acharjya (2015) discuss about different jamming attacks that may be employed against a wireless network. Additionally, to cope with the problem of jamming, they propose a detection strategy using dominance based rough set. This technique is employed over physical and data link layer parameters [11].

Later in 2016 Ahmed portrays an evaluation of intrusion detection data set through an applications of containing order rough set and rule generation [12].

Ahmed et al., (2017) also propose a model for identification of phishing attacks and chief attributes that make an object phishing object using rough set and formal concept analysis [13].

Likewise, Acharjya and Ahmed (2017) explain variety of attacks and their symptoms in wireless sensor network. They analyzes wireless sensor network using trusting based protection techniques which includes some classical techniques such as fuzzy, bayesian, game theory etc., and some modern techniques such as clustering, bio-inspired computing, key establishment based techniques etc., to provide maximum protection for each node without an attack [14].

III. Rough Set

Rough set theory is a new mathematical tool for handling the **v**ague and uncertainty proposed by the Poland scholar Z. Pawlak in 1982 [1][14]. It is regarded as extremely vital significance for the artificial intelligence and cognitive science, which provides a theoretical framework for the machine learning, data mining, knowledge acquisition, pattern recognition and approximate reasoning and other areas of information processing. Whereas it can't discover inconsistent problems concerned with criteria (attribute containing preference order). Thus inconsistency that original rough set method unnecessarily detects may lose important information. Further more, original rough set method can't produce rules containing preference order, namely, can't achieve more meaningful and general rules. Thus in this paper we take the advantage of common attributes (attributes not containing preference order information) and criteria to describe the object together. We call such containing preference order rough set methodology as CORS. In CORS, given a set of objects, there is a criterion at lest among condition attributes, and all objects are divided into ordered decision classes by decision attribute (decision attribute is also a criteria). In addition, criteria in condition attributes are correlated semantically with ordered decision attribute. The CORS method can detect inconsistency from dominance principle and realize approximating decision classes by means of dominance relation

Definition 1: Let T= (U, A, V, f) is an information table, if U denotes a finite and nonempty set of object x , called universe; A denotes a finite and nonempty set of attributes; $V= \cup V_a$, V_a denotes value domain of attribute $a \in A$; $f=\{f_a: a \in A\}$ denotes a map from U to V, where $f_a: U \rightarrow V_a$ if x is an object, $f_a(x)$ is value of x on attribute a, shortly x_a or a(x).

Definition 2: Let T be a decision table, C is condition attributes set, D is decision attributes set, if T=(U, A, V, f) is an information table, and $A=C \cup D$, $C \neq \Phi$, $D \neq \Phi$, $C \cap D=\Phi$.

Definition 3: In decision table T=(U, A, V, f),if for some an attribute $a \in C$, there exists preference order in its value domain and it correlates semantically with some other criterion, such attribute is criterion. If there is a criterion at least in C and D respectively, and all criteria in C correlate semantically with criteria in D, this decision table is called ordered decision table.

Definition 4: Let x and y be an a-indiscernible object, if values x_a and y_a about attribute $a \in A$ satisfy $x_a =_a y_a$, where T=(U, A, V, f) is a decision table. Call $IND(B_n)$ as an indiscernibility relation on U, if every attribute in $B_n \subseteq A$ is common attribute, where $IND(B_n)=\{(x, y) \in U^2, \forall a \in B_n, x_a =_a y_a\}$. Say that x and y are B_n-indiscernible, if $(x, y) \in IND(B_n)$, denoted as $x\ I_{Bn}\ y$.

Definition 5: An object y dominates x with respect to criteria a, if $x_a \preceq_a y_a$, where x_a and y_a are values with respect to a, a∈A is a criterion, T=(U, A, V, f) is a decision table. $DOM(B_o)$ is a dominance relation on U, if $DOM(Bo)=\{<x, y>\in U^2, \forall\ a\in B_o, x_a \preceq_a y_a\}$, where $B_o \subseteq A$ is a criteria set. Call y dominating x with respect to B_o, if $<x,y> \in DOM(B_o)$, denoted as $y\ D_{Bo}\ x$. Further, $DOM(B)=\{<x,y>\in U^2, <x, y> \in DOM(B_o) \wedge (x,y) \in IND(B_n)\}$is a total dominance relation on U, if $B_o \subseteq A$ is a criteria set, $B_n \subseteq A$ is a common attributes set, $B=B_o \cup B_n$ is a join set of criteria and common attributes. And say that y totally dominates x with respect to B, if $<x, y> \in DOM(B)$, denoted $y\ D_B\ x$. Dominance relation is directional , if $<x, y> \in DOM(B_o)$, y is subjective and x is passive.

Definition 6: If $x \in U$ is passive, we define a set of objects $y \in U$ dominating x with respect to attribute set R, called R-dominating x set, $D_R^+(x) =\{y \in U : y\ D_P\ x \wedge x\ I_Q\ y\}$, where $R \subseteq C$ is attributes set, $P \subseteq R$ is criteria set, then Q =R - P is common attributes set. Similarly, define a set of objects $y \in U$ dominated by x with respect to attributes set R, called R-dominated set by x, $D_R^-(x)=\{y \in U : x\ D_P\ y \wedge x\ I_Q\ y\}$

Further the decision attributes set D divides all objects in U into finite decision classes, denoted $CL=\{Cl_t, t \in T\}$, $T=\{1,2,\ldots,n\}$,and that $x \in U$ only belongs to a decision class $Cl_t \in CL$. Further suppose that these decision classes satisfy total order relation. Let r<s, objects in Cl_r are all inferior to ones in Cl_s

Definition 7 Let D={d}, then d divides objects in U into finite classes $CL=\{Cl_t, t \in T\}$, $T=\{1,2,\ldots,n\}$. The upward union and downward union of every $Cl_t \in CL$ are defined respectively:

$Cl_t^{\geq} = U\ Cl_s$ where $t \leq s$, $t=1,2,\ldots,n$

$Cl_t^{\leq} = U\ Cl_s$ where $s \leq t$, $t=1,2,\ldots,n$

Actually, if a criterion has total order relation, it has upward and downward union also. To distinguish from upward and downward union of decision attribute, we call that of criterion in condition attributes as ordered upward union and ordered downward union.

IV. Data Analysis

CORS unite dominance and indiscernibility relation to make them both approximating knowledge together. Here, knowledge granules approximated are decision classes, upward or downward unions, i.e. Cl_t, $Cl_t^{\geq}$ and $Cl_t^{\leq}$. Granules approximating knowledge are $D_P^+(x)$, $D_p^-(x)$, where $P \subseteq C$, $t \in \{1,2,\ldots,n\}$. Classification patterns deduced are Cl_t, $Cl_t^{\geq}$ and $Cl_t^{\leq}$ and functions expressed by $D_P^+(x)$ and $D_p^-(x)$

Inconsistency in CORS can be found from dominance relation through examining whether objects dominance principle: If object x and object y are indiscernible in common attributes, but their criterion don't satisfy dominance principle with ordered decision class, they are inconsistent.

For $P \subseteq C$, objects determinately belonging to $Cl_t^{\geq}$ and $Cl_t^{\leq}$ constitute their P-lower approximation $P_*(Cl_t^{\geq})$ and $P^*(Cl_t^{\leq})$ respectively. CORS theory admits, x definitely belongs to $Cl_t^{\geq}$ when every element in P-dominating x set all belongs to $Cl_t^{\geq}$; the unions of P-dominating x set of x in $Cl_t^{\geq}$ form all elements possibly belonging to $Cl_t^{\geq}$, i.e.

$P_*(Cl_t^{\geq}) = \{ x \in U : D_P^+(x) \subseteq Cl_t^{\geq}\}$

$P^*(Cl_t^{\geq}) = U\ D_P^+(x)$, $x \in Cl_t^{\geq}$, $t = 1,2,\ldots,n$

Similarly, we can define lower, upper approximation $P_*(Cl_t^{\leq})$ and $P^*(Cl_t^{\leq})$ of $Cl_t^{\leq}$:

$P_*(Cl_t^{\leq}) = \{ x \in U : D_P^-(x) \subseteq Cl_t^{\leq}\}$

$P^*(Cl_t^{\leq}) = U\ D_P^-(x)$, $x \in Cl_t^{\leq}$, $t = 1,2,\ldots,n$

Boundary region of $Cl_t^{\leq}$ and $Cl_t^{\geq}$ can be denoted by $B_{np}(Cl_t^{\leq})$ and $B_{np}(Cl_t^{\geq})$ respectively and is defined as

$B_{np}(Cl_t^{\geq}) = P^*(Cl_t^{\geq}) - P_*(Cl_t^{\geq})$

$B_{np}(Cl_t^{\leq}) = P^*(Cl_t^{\leq}) - P_*(Cl_t^{\leq})$

The classification accuracy of approximation is defined as

$\alpha_p(Cl_t^{\geq}) = |P_*(Cl_t^{\geq})|/|P^*(Cl_t^{\geq})|$, $t=2,3,\ldots n$ (1)

$\alpha_p(Cl_t^{\leq}) = |P_*(Cl_t^{\leq})|/|P^*(Cl_t^{\leq})|$, $t=1,2,\ldots n-1$ (2)

The quality of approximation of classification is defined as

$\gamma_p(Cl) = |(U - (U\ B_{np}(Cl_t^{\leq})))| / |U|$, $t \in T$ (3)

$\gamma_p(Cl) = |(U\ P_*(Cl_{t1}^{\leq})) U (U\ P_*(Cl_{t2}^{\geq})) / |U|$ (4)

Where $t1= 1,2,\ldots,n-1$, $t2= 2,3,\ldots..,n$, $T = 1,2,\ldots\ldots,n$

V. Dominance Relation Rule Formation

From the point of view of knowledge discovery, rough approximations of upward and downward union based on dominance principle, are capable of deducing more generalized description for objects in data table. P-lower approximations of unions represent determinate knowledge provided by criteria and common attributes in $P \subseteq C$. We can deduce such rules as "if …, then …" according to lower approximation of upward and

downward union,. Here we illustrate a question, classical RS can discover inconsistency rooted indiscernibility relation, CORS is helpful for finding inconsistency from dominance principle. Simply, there appears inconsistency when of two objects at least one criterion in condition criteria don't satisfy dominance principle with decision attribute, while values are indiscernible in common attributes and other criterion satisfy dominance principle. Once such inconsistency exists in logic, we try to eliminate it. The simplest method is to delete inconsistent objects in order to keep consistency of data and which method to adopt, is not included here.

In CORS, we consider two kinds of determinate rules as follows:

1. Determine $D_{\leq}$ - rules : For those objects contained in $R_*(Cl_t^{\leq})$, if for $\forall q \in Q$ $x_q =_q r_q \wedge$ for $\forall p \in P$ $x_p \leq_p r_p$, then $x \in Cl_t^{\leq}$, t = 1,2,…,n-1.
2. Determine $D_{\geq}$ - rules : For those objects contained in $R_*(Cl_t^{\geq})$, if for $\forall q \in Q$ $x_q =_q r_q \wedge$ for $\forall p \in P$ $x_p \geq_p r_p$, then $x \in Cl_t^{\geq}$, t = 2,3,….,n.

Where $\forall r \in R=PUQ$, Q is a common attributes set, P is criteria set.

Based on the above determinate rules the following four principles are generated as follows:

Principle 5.1 If there is some an equivalence class in indiscernibility relation led by some a common attributes set Q of condition attributes set, which is contained in some a decision class (including upward or downward union), generate corresponding rules.

Principle 5.2 If there is some an equivalence class or ordered union led by some a criteria set P of condition attributes set, which is contained in some a decision class (including upward or downward union), generate corresponding rules.

Principle 5.3 If there is some an intersect of some an equivalence class led by some attribute(s) and an equivalence class or ordered union led by some a criterion in condition attributes set, which is contained in some a decision class (including upward or downward union), generate corresponding rules.

Principle 5.4 If there exists some an equivalence class or an ordered union or an intersect of them, which has formed rules based on above three principles, it won't take part in following the same directional rules generation.

VI. Analyzing and Tracing of Packet Dropping Attacks

The containing order rough set approach has been efficiently applied for analyzing and evaluating packet dropping attack in mobile ad-hoc wireless network data set. Here we have taken such application by using the following data from paper [18].

U	X_1	X_2	X_3	Y
N_1	VL	3	N	BN
N_2	A	10	A	WH
N_3	A	11	A	WH
N_4	L	1	A	GH
N_5	A	10	N	WH
N_6	L	7	N	BN
N_7	VL	5	N	BN
N_8	L	8	A	GH
N_9	H	6	A	BH
N_{10}	VL	4	N	GH
N_{11}	H	2	N	BH
N_{12}	L	9	A	GH

Table 1: Packet dropping attack data set

The above table contains 12 nodes in a mobile ad-hoc network information with 3 conditional attributes $C=\{X_1, X_2, X_3\}$ and a decision attribute Y. U is a Node identification number in a server; X_1 is a packet dropping rate status (H : High, A : Average, L : Low, VL : Very Low); X_2 is a number of neighbor nodes for the current node; X_3 is a type of signal received (N : Normal, A : Abnormal); Y is a type of attack (BH : Black Hole, WH : Worm Hole, GH : Gray Hole, BN : Benign Node), Where X_1 is a criteria, X_2 and X_3 are common attributes and Y is a decision attribute.

Classes based on these selected attributes are then computed (inductively learned) using the appropriate, formatted audit data. Here we have shown that classes can be introduced using dominance relation among conditional attributes used in a packet dropping attack models since they can decide whether an observed node activity is "black hole" or "worm hole" or "gray hole" or "benign node". The aforementioned table gives evidences of packet dropping attack data set in a mobile ad-hoc wireless network and its various types of attack status.

The equivalence classes achieved according to common attributes set $\{X_2\}$, $\{X_3\}$ and $\{X_2, X_3\}$ are $\{\{N_1\}, \{N_2, N_5\}, \{N_3\}, \{N_4\}, \{N_6\}, \{N_7\}, \{N_8\}, \{ N_1S9\}, \{N_{10}\}, \{N_{11}\},\{N_{12}\}\}$, $\{\{N_1, N_5, N_6, N_7, N_{10}, N_{11}\},$

$\{N_2, N_3, N_4, N_8, N_9, N_{12}\}\}$ and $\{\{N_1\}, \{N_2\}, \{N_3\}, \{N_4\}, \{N_5\}, \{N_6\}, \{N_7\}, \{N_8\}, \{N_9\}, \{N_{10}\}, \{N_{11}\}, \{N_{12}\}\}$. The ordered classes got by criterion X_1 are $\{\{N_1, N_7, N_{10}\} \leq \{N_4, N_6, N_8, N_{12}\} \leq \{N_2, N_3, N_5\} \leq \{N_9, N_{11}\}\}$, corresponding ordered downward unions are $\{\{N_1, N_7, N_{10}\}, \{N_1, N_4, N_6, N_7, N_8, N_{10}, N_{12}\}, \{N_1, N_2, N_3, N_4, N_5, N_6, N_7, N_8, N_{10}, N_{12}\}, \{N_1, N_2, N_3, N_4, N_5, N_6, N_7, N_8, N_9, N_{10}, N_{11}, N_{12}\}\}$ and satisfy $\{N_1, N_7, N_{10}\} \leq \{N_1, N_4, N_6, N_7, N_8, N_{10}, N_{12}\} \leq \{N_1, N_2, N_3, N_4, N_5, N_6, N_7, N_8, N_{10}, N_{12}\} \leq \{N_1, N_2, N_3, N_4, N_5, N_6, N_7, N_8, N_9, N_{10}, N_{11}, N_{12}\}$; corresponding ordered upward unions are $\{N_1, N_2, N_3, N_4, N_5, N_6, N_7, N_8, N_9, N_{10}, N_{11}, N_{12}\} \leq \{N_2, N_3, N_4, N_5, N_6, N_8, N_9, N_{11}, N_{12}\} \leq \{N_2, N_3, N_5, N_9, N_{11}\} \leq \{N_9, N_{11}\}$. It's easy to see that objects N_6 and N_{10} are inconsistent because they are indiscernible in common attributes $\{X_2, X_3\}$ and don't satisfy the dominance principle between criterion $\{X_1\}$ and decision attribute $\{Y\}$. For this reason we eliminate objects N_6 and N_{10} from data Table 1 in following study.

All objects are divided into four ordered classes $Cl_1 = \{N_1, N_6, N_7\}$, $Cl_2 = \{N_4, N_8, N_{10}, N_{12}\}$, $Cl_3 = \{N_2, N_3 N_5\}$, $Cl_4 = \{N_9, N_{11}\}$ by ordered decision attribute, where Cl_4 is worsted than Cl_3, Cl_3 is worsted than Cl_2, Cl_2 is worsted than Cl_1. So $Cl_1^{\leq} = \{N_1, N_6, N_7\}$, $Cl_2^{\leq} = \{N_1, N_4, N_6, N_7, N_8, N_{10}, N_{12}\}$, $Cl_3^{\leq} = \{N_1, N_2, N_3, N_4, N_5, N_6, N_7, N_8, N_{10}, N_{12}\}$, $Cl_4^{\geq} = \{N_9, N_{11}\}$, $Cl_3^{\geq} = \{N_2, N_3, N_5, N_9, N_{11}\}$, $Cl_2^{\geq} = \{N_2, N_3, N_4, N_5, N_8, N_9, N_{10}, N_{11}, N_{12}\}$.

Initially, we implement "$D_{\leq}$ - rules" and rule (1) is obtained based on principle 4.1:

U	X_1	X_2	X_3	Y
N_1	VL	3	N	BN
N_7	VL	5	N	BN

Table 2: if X_2= (3,5) ^ X_3=N then Y ≤ GH

Rule (2) is obtained by principle 4.2:

U	X_1	X_2	X_3	Y
N_1	VL	3	N	BN
N_7	VL	5	N	BN

Table 3: if X_1 ≤ VL then Y ≤ BN

Further rule (4) and (5) are generated using table 4 and 5.

U	X_1	X_2	X_3	Y
N_1	VL	3	N	BN
N_2	A	10	A	WH
N_3	A	11	A	WH
N_4	L	1	A	GH
N_5	A	10	N	WH
N_7	VL	5	N	BN
N_8	L	8	A	GH
N_{12}	L	9	A	GH

Table 4: if X_1 ≤ A ^ X_2= (1, 3, 5, 8, 9, 10, 11) then Y ≤ WH

U	X_1	X_2	X_3	Y
N_1	VL	3	N	BN
N_5	A	10	N	WH
N_7	VL	5	N	BN

Table 5: if X_1≤ A ^ X_3 = N then Y ≤ WH

We continue deducing "$D_{\geq}$ - rules" and rule (5) is obtained by principle 4.1:

U	X_1	X_2	X_3	Y
N_2	A	10	A	WH
N_3	A	11	A	WH
N_4	L	1	A	GH
N_8	L	8	A	GH
N_9	H	6	A	BH
N_{12}	L	9	A	GH

Table 6: if X_2= (1, 6, 8, 9, 10, 11) ^ X_3 = A then Y ≥ GH

Rule (6) is obtained by principle 4.2:

U	X_1	X_2	X_3	Y

N_9	H	6	A	BH
N_{11}	H	2	N	BH

Table 7: if $X_1 \geq H$ then $Y \geq BH$

Similarly the rule (7) and (8) are generated using table 8 and 9.

U	X_1	X_2	X_3	Y
N_2	A	10	A	WH
N_3	A	11	A	WH
N_5	A	10	N	WH
N_9	H	6	A	BH
N_{11}	H	2	N	BH

Table 8: if $X_1 \geq A \wedge X_2 = (2, 6, 10, 11)$ then $Y \geq WH$

U	X_1	X_2	X_3	Y
N_2	A	10	A	WH
N_3	A	11	A	WH
N_9	H	6	A	BH

Table 9: if $X_1 \geq A \wedge X_3 = A$ then $Y \geq WH$

The lower approximation, upper approximation and boundary region of Clt is shown in the below table:

Cl_i	$P_*(Cl_i)$	$P^*(Cl_i)$	$Bn_P(Cl_i)$
$Cl_1^{\leq} = \{N_1, N_7\}$	$\{N_1, N_7\}$	$\{N_1, N_4, N_7, N_8, N_{12}\}$	$\{N_4, N_8, N_{12}\}$
$Cl_2^{\leq} = \{N_1, N_4, N_7, N_8, N_{12}\}$	$\{N_1, N_4, N_7, N_8, N_{12}\}$	$\{N_1, N_2, N_3, N_4, N_5, N_7, N_8, N_{12}\}$	$\{N_2, N_3, N_5\}$
$Cl_2^{\geq} = \{N_2, N_3, N_4, N_5, N_8, N_9, N_{11}, N_{12}\}$	$\{N_2, N_3, N_5, N_9, N_{11}\}$	$\{N_2, N_3, N_4, N_5, N_8, N_9, N_{11}, N_{12}\}$	$\{N_4, N_8, N_{12}\}$
$Cl_3^{\leq} = \{N_1, N_2, N_3, N_4, N_5, N_7, N_8, N_{12}\}$	$\{N_1, N_2, N_3, N_4, N_5, N_7, N_8, N_{12}\}$	$\{N_1, N_2, N_3, N_4, N_5, N_7, N_8, N_{12}\}$	ϕ
$Cl_3^{\geq} = \{N_2, N_3, N_5, N_9, N_{11}\}$	$\{N_9, N_{11}\}$	$\{N_2, N_3, N_5, N_9, N_{11}\}$	$\{N_2, N_3, N_5\}$
$Cl_4^{\geq} = \{N_9, N_{11}\}$	$\{N_9, N_{11}\}$	$\{N_9, N_{11}\}$	ϕ

Table 10: Lower and Upper Approximation of Cl_t

From the above tables (2 to 9), we can see that principle 4.4 enable us to avoid redundant and insignificant work. For example in rule (2), know ledge granule $\{N_1, N_7\}$ satisfies principle 4.2.

Through deduction of above rules, we can easily see that these rules have covered all objects except objects N_6 and N_{10} are simplified in a certain extent.

The classification accuracy of upward approximation can be calculated according to formula (1) .

$$\alpha_p(Cl_t^{\geq}) = |P_*(Cl_t^{\geq})|/|P^*(Cl_t^{\geq})|,\ t=2,3,\ldots n \qquad (1)$$

The classification accuracy of downward approximation can be calculated according to formula (2).

$$\alpha_p(Cl_t^{\leq}) = |P_*(Cl_t^{\leq})|/|P^*(Cl_t^{\leq})|,\ t=1,2,\ldots n-1 \qquad (2)$$

The classification quality of approximation can be calculated according to formula (3) and (4), we have

$$\gamma_p(Cl) = |(U - (U\ Bn_P(Cl_t^{\leq})))| / |U| \quad t \in T \qquad (3)$$

where T=1,2,…..,n

VII. Conclusion

This paper discloses a case on organized construction of assessment on packet dropping attack in wireless network data set using containing order rough set. We also give an evidence of packet dropping attack in a wireless network and its various type of attacks. Finally we have even shown the core, the decision rules following certain observation of packet dropping attack data set by applying containing order rough set.

References

[1]. Zadeh, L. A., (1965) Fuzzy sets, Information and Control, Vol. 8, pp338-353.
[2]. Pawlak, Z., (1982) Rough Sets, International Journal of Computer and Information Sciences, Vol. 11, pp341-356.
[3]. Pawlak, Z. and Skowron, A., (2007) Rudiments of rough sets, Information Sciences, An International Journal, Elsevier, Vol. 177, No. 1, pp. 3-27.
[4]. Pawlak, Z. and Skowron, A., (2007) Rough sets and boolean reasoning, International Journal of Information Sciences, Elsevier, Vol. 177, No. 1, pp. 41-73.
[5]. Slowinski, R. and Vanderpooten, D., (2000) A generalized definition of rough approximations based on similarity, IEEE Transactions on Knowledge and Data Engineering, Vol. 12, No. 2, pp. 331-336.
[6]. Dubois, D. and Prade, H., (1990) Rough fuzzy sets and fuzzy rough sets, International Journal of General System, Vol. 17, pp. 191-209.
[7]. Li, Ya, D., and Qing, H. B., (2007) A kind of dynamic rough sets, Fourth International Conference on Fuzzy Systems and Knowledge Discovery, pp. 79-85.
[8]. Zhu, W., and Wang, F.Y., (2007) On three types of covering rough sets, IEEE Transactions on Knowledge and Data Engineering, Vol. 19, No. 8, pp. 1131-1144.
[9]. Patcha, A. and Park, J. M. (2007) An overview of anomaly detection techniques: existing solutions and latest technological trends, Journal of Computer Networks, Vol. 51, pp. 3448-3470.
[10]. Ahmed, N. S. S. and Acharjya, D. P., (2015) Detection of denial of services attack in wireless network using dominance based rough set. International Journal of advanced computer science and applications, Vol. 6, No. 12, pp. 267-278.
[11]. Ahmed, N. S. S. and Acharjya, D. P., (2015) A dominance based rough set approach for the detection of jamming attack. International Journal of Philosophies in computer science, Vol. 1, No. 2, pp. 45-66.
[12]. Ahmed, N. S. S., (2016) An application of containing order rough set for analyzing data of intrusion detection. An Interdisciplinary Journal of Scientific Research & Education, Vol. 2, No. 5, pp. 52-57.
[13]. Ahmed, N. S. S., Acharjya, D. P., & Sanyal, S. (2017) A framework for phishing attack identification using rough set and formal concept analysis. International Journal of Communication Networks and Distributed Systems, Vol. 18, No. 2, pp. 186-212.
[14]. Acharjya, D. P. & Ahmed, N. S. S. (2017) Recognizing attacks in wireless sensor network in view of internet of things. In: Acharjya, D. P. & Geetha, M. K., Internet of Things : Novel Advances and Envisioned Applications, Studies in Big Data, Vol. 25, pp. 149-172.