IJCTA, 9(27), 2016, pp. 195-201 ISSN: 0974-5572

Filtering Framework for Intrusion Detection Rule Schema in Mobile Ad Hoc Networks

Lalli M.* and Palanisamy V.**

ABSTRACT

Mobile Ad Hoc Network (MANET) has turned into an energizing and essential innovation as of latest in view of the fast expansion of wireless gadgets. MANETs are highly vulnerable against attacks because of the progressively topology changing of network, the absence of centralized point for monitoring and open medium. The different attacks against mobile hubs are Warm hole, Byzantine attack, Packet Dropping, Black hole and flooding so on. It is vital to look new architecture and networks to ensure the wireless networks and the application of mobile computing. IDS (Intrusion Detection System) devices are reasonable for distinguishing these attacks. IDS examine the network exercises by method for review information and use examples of surely understood attacks or ordinary profile to recognize potential attacks. In this paper, a framework is proposed to filtering the rule schema in the intrusion detection system of MANET. This framework is composing of three stages. The first stage is pre-processing the dataset to reduce the feature size by utilizing Genetic Algorithm. Then using that reduced dataset, a rule schema is generated using Apriori Association Rule. In the final stage, the rule schema is filtered using Artificial Neural Network. This filtered technique gives more deduction accuracy, less time consumption than the Association Rule generation.

Keywords: Intrusion Detection, MANET, Ant Colony Optimization, Apriori Algorithm, Rule Schema, Artificial Neural Network.

1. INTRODUCTION

A MANET (Mobile Ad hoc Network) is a network that comprises of mobile hubs that impart remotely and does not have a foundation. Hubs in MANET convey through either single-hop or multi-hop modes. In this way, in that environment, every hub goes about as routers and in addition a host. A noteworthy capacity in MANET is the route disclosure process [1], in which a route from a particular source to a particular destination is found with an exact finale target to exchange information packets by means of this possible route. Numerous routing protocols, for example, DSR [2] and AODV [2] have been proposed for data transmission and route detection. In the information transmission stage, every intermediate hub in the network takes an interest in sending information and control packets to different hubs. Most ad hoc routing protocols, for example, AODV and DSR are not initially intended to be secure against malicious attacks; as they depend on basic relationships of verifiable trust-your neighbor [3].

Be that as it may, and because of the expansion notoriety of the ad hoc networks, few hubs may act in the network contrarily. These hubs are called malicious hubs, and may perform attacks in the system to endanger the network resources. Because of the dynamic way of the MANETs topology and the nonappearance of framework, MANETs are more helpless against the attacks [4]. This dynamic structure of hubs may aggravate the trust relationship among hubs. The absence of essential issues makes the detection procedures of attacks are troublesome and it is difficult to screen the traffic in a dynamic and vast scaled network [5]. Every one of these attributes of MANETs permits the attackers to effortlessly focus on the network and savatage its assets by jamming and distributing the communication between legitimate hubs. Malicious hubs can perform ill-disposed attacks that can

* Department of CS, Bharathidasan University, Trichy, *Email: Lalli_bdu@yahoo.co.in*

** Department of CS & Engg., Alagappa Universtiy, Karaikudi, *Email: vpazhanisamy@yahoo.co.in*

harm the fundamental parts of security, for example, confidentiality, privacy and security [6]. Security is more basic in a few applications, for example, military, law implementation, and salvage missions. Subsequently, security in MANETs has pulled in further consideration.

2. RELATED WORKS

M. Sulaiman khan, Maybin Muyeba and Frans Coenen [7] portrayed weighted association rule mining from fuzzy information in their paper. In their paper [8], they proposed association standard digging for weighted quality not as a matter of course binary value. The quality ought to be continuous or discrete worth to be exhibited in the database. Murtagh, and Farid, in their paper on Weighted Association Rule Mining Using Weighted Support and Significance Framework tended to the issues of finding huge binary connections in exchange datasets in a weighted setting [9]. The concentrated on those critical connections including things with huge weights as opposed to being overflowed in the combinatornal blast of inconsequential connections. In 2001, Li, F proposed a methodology for association standard digging for weighted association rules [10]. Wang and Fan [11] proposed non-iterative enhanced Apriori algorithm to find IDS alarms. They utilized crossing point of two unmistakable columns of (DARPA 99 dataset to recognize reoccurring designs. On the off chance that same example is rehashed in numerous crossing point operations, and then it is considered as fascinating example and utilized as Intrusion caution. Zhang yanyan and Yao Yuan [12] exhibited pattern based association principle detection algorithm for IDS standard era. Amid first pass they partitioned training database in a manner that every partition of database can be totally replicated into a principle memory of handling gadget. At that point Large Item sets for every allotment are distinguished autonomously. The union of these extensive item sets is then utilized as applicant huge item sets for complete dataset. Amid second pass, expansive item sets for complete database are recognized. This algorithm can't be effectively changed over into incremental association rule detection algorithm and time unpredictability of it is high. In 2009 Flora S. Tsai [13] depicted system intrusion Detection framework utilizing association rule mining as a part of his paper. This technique served to created fascinating standards from the KDD information set. The intrusion detection dataset KDD99 contains assortment of information beginning from twofold, discrete and nonstop information. Along these lines, it is exceptionally hard to create rules for a specific attack utilizing same methodology. To discover the association rules MingYang Su et al [14] proposed incremental fuzzy association rules mining algorithm for Network Intrusion Detection System. They utilized connection rundown of connection rundown to store all conceivable hopeful item sets and their bolster number in primary memory. This data is overhauled intermittently utilizing system activity information gathered. Upgraded data is then utilized by incremental algorithm to recognize expansive and fascinating item sets, which are utilized as principles for NIDS. The significant downside of this algorithm is gigantic principle memory necessity to sore all hopeful item sets of each size.

3. RULE SCHEMA FILTERING FRAMEWORK FOR THE INTRUSION DETECTION SYSTEM IN MANET

In the mobile ad hoc networks, the intrusion is major issues for routing the packets to the destination. Using the proposed framework, a set of rule is generated by utilizing KDD CUP 99 dataset for classifying the node as intruded and non intruded one.

3.1. Pre-Processing

Accuracy of the classifier depends on the selection of optimum feature subset. Feature selection method mainly used for selecting subset of features from the original data set. There are two feature selection methods that are already proposed namely filter and wrapper methods. Filter method was mainly based on general characteristics of data features without involving machine language. These features are ranked based on certain criteria, where features with highest rank values are selected as optimal. The main advantages of filter method are low computational cost without involving any machine language algorithm for future selection. Frequently used filter method is information

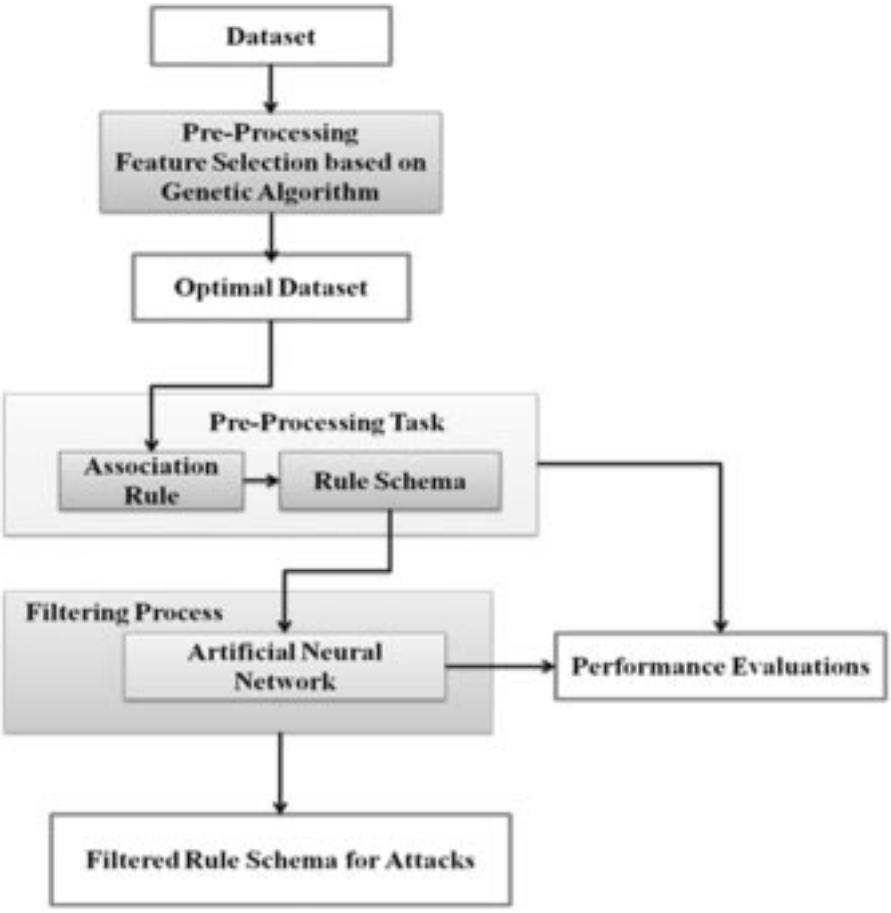

Figure 1: Proposed framework for filtering Attacks Rule Schema in MANET

gain method. Wrapper method is mainly used for feature subset selection from the data set based on objective function and analysis of the performance of feature subset.

Brief Steps about Genetic Algorithm that chose features from dataset is accessible as algorithm below

Step 1: Initialize a populace of Pre-handled information.

Step 2: Calculate target task for every individual.

Step 3: Selection of individual result.

Step 4: Perform mating of pair of individuals.

Step 5: Perform change operation.

Step 6: Calculate target function for recently made population.

Step 7: If it fulfills stop the operation.

Step 8: Otherwise repeat step 3.

Step 9: Return the best components from KDD 99 dataset that reflects the properties of DoS.

3.2. Rule Generation utilizing Association Rule Mining

Association Rule Mining is a two-stage process [15]:

1. Identify all common itemsets utilizing Apriori algorithm.

2. Make solid association rules from the common itemsets

For rule generation, precursor part is produced by utilizing apriori algorithm and for resulting; classification strategy is utilized in which the entire KDD dataset is distributed into two classes, that is ordinary and attack class on the basis of marks gave in the dataset. The accompanying algorithm is utilized for finding the regular itemsets from the dataset that is Apriori algorithm:

Algorithm: Apriori Algorithm for finding continual itemset

Information: Normalize dataset, minimum support (minsupp) = 0.2

Step 1: Initialize k (number of itemset) = 1

Step 2: Find regular itemset Lk from Ck of all applicant itemsets

Step 3: Scan D and include each itemset Ck,

Step 4: If count is greater than minimum support, then it is continuous

Step 5: Form Ck + 1 from Lk; k = k + 1

Step 6: Join Lk-1 itemset with itself to get the new contestant itemsets,

Step 7: If found a non-continuous subset then expel that subset.

Step 8: Store incessant itemset in the rule pool

Step 9: Repeat step 2 to step 9 until Ck is empty

Output: Frequent itemsets.

3.3. Rule Generation Algorithm

After finding the incessant item set, confidence vale, support and rules have to be created for every attack types. The accompanying algorithm is general for any kind of information set. Here F contains the largest common item set. Min_supp defines the client defines sustain and Min_conf defines the client defines certainty. RULE contains the desired rules created from the data set. The algorithm is as follows:

Algorithm

Step 1: Take the biggest incessant item set F with Min_Supp and Min_Conf esteem.

Step 2: Generate every single conceivable subset of F and store it in SUB.

Step 3: Count SUPP and CONF esteem for every components of SUB.

Step 4: If (SUPP > = Min_Supp & & CONF > = Min_Conf) then

a. Choose the specific components of SUB and store in RULE

b. Generate different principles and store in RULE

Step 5: Else reject the specific component of SUB and go to step 3.

Step 6: Return RULE.

Step 7: End

3.4. Proposed Rule Schema Filtration Method by Artificial Neural Network

The Artificial Neural Networks are created from an enormous quantity of basics through the input devoted into a sort of magnitudes superior than in computational requisites of traditional architectures [16]. These elements are

named as artificial neuron and these are interrelated into cluster by a statistical form for data processing found on the top of the association in approach to computation. The neural systems create their neuron receptive to accumulate the items. And also, it is capable for using deformation open-minded piling up of a huge quantity of cases exemplified by elevated facet vectors.

There are various kinds of neural network methods have been accomplished for document classification tasks. Some of the researchers use the single-layer perception, which restrains merely a key in layer and the productivity layer in consequence of its unfussiness of executing [17]. However, inputs are supplied openly in the direction of the productivity via a sequence of weights. Thus it can be measured as the modest type of feed-forward network. The multi-layer observation that is further purified, which contains of an input in layer, single or additional obscured layers, and the productivity (output) layer within its configuration, moreover it is broadly executed meant for categorization responsibilities.

The Artificial neural systems are able to acquire contributions y_k turned up in the course of pre-synaptic associations, Synaptic efficiency is reproduction of using the real weights wg_k and the reply through neuron in a non linear purpose f of its subjective inputs. The productivity of neuron i for prototype q is P_{qi} where

$$P_{qi}(net_i = \frac{1}{1+e^{-i\alpha net_i}}$$

$$net_i = Wg_{bias} * bias + \sum_j P_{qj} Wg_{ij}$$

Neural system for text categorization can fabricate positive outcomes in multifaceted servers and apposite for both separate and constant data. When the training is comparatively sluggish then there is fast in the testing and examining the results are complicated intended for customers to understand the cultured systems (contrasting with Decision tree), Empirical Risk Minimization (ERM) composes ANN endeavor towards the reduce the working out of mistakes, could guide to over fitting. In this paper, multi-layered feed forward network architecture is used with one hidden layer and this architecture is trained by using Multi-Layer Perceptron Back Propagation learning is employed.

4. SIMULATION RESULT AND DISCUSSIONS

4.1. Performance Metrics

Detection of attacks/intrusion can be measured [11] by following metrics:

True Positive (TP): Corresponds to the quantity of recognized attacks and it is actually as attack.

False Positive (FP): Corresponds to the quantity of distinguished attacks however it is actually normal. really typical.

False Negative (FN): Corresponds to the quantity of distinguished ordinary occurrences but it is really as attack, in other words these attacks are the objective of intrusion detection systems.

Detection Rate: Detection rate alludes to the percentage of identified attack among all input test data, and is characterized as follows:

[illegible] [illegible] * 100

False Negative Rate: False negative rate alludes to the rate of attack data which is wrongly perceived as should be expected, and is characterized as follows:

[illegible] [illegible] [illegible]

False Positive Rate: False positive rate alludes to the rate of ordinary information which is wrongly perceived as an attack, and is characterized as follows:

The proposed technique for intrusion detection of hub in the MANET is completed with KDD 99 Cup database in order to contrast results with association rule mining. The preparation dataset contains 400 attack associations arbitrarily chose from KDD 99 Cup database, where four sorts of attacks (Dos, Probe, U2R and R2L) are incorporated. A sum of 6 characteristics which are chosen in the progression pre-handling is incorporated into every association; initial 6 properties that is term, convention sort, administration, banner, source bytes and destination bytes separately. With the number of inhabitants in 250 eras 2323 principles are extricated. Every tenet is removed on the off chance that it happens often with a measurably critical level in the database. Consequently, every rule is removed from the entire database by considering all the association data. For this examinations, 500 marked associations (hubs properties are considered).

Table 1
Confusion Matrix for Association Rule Schema Generation

	Normal	*Attack/Intrusion*	*Total*
Normal	65	35	100
Attack/Intrusion	45	355	400
Total	110	390	500

Table 2
Performance Comparison of Association Rule Schema and Crisp Data mining technique

	Crisp Data Mining (%)	*Association Rule Schema(%)*
Detection Rate (DR)	98.6	97.3
False Positive Rate (FPR)	0.66	2
False Negative Rate (FNR)	5.2	3

Using Neural Network, After 250 generations, 1758 rules related to the normal connections are extracted from Association Rule Schema.

Table 3
Confusion Matrix for proposed Filtering Rule Schema Generation

	Normal	*Attack/Intrusion*	*Total*
Normal	98	2	100
Attack/Intrusion	12	388	400
Total	110	390	500

Table 4
Performance Comparison of Proposed Filtering Rule Schema and Association Rule Schema

	Proposed Filtering Rule Schema (%)	*Association Rule Schema(%)*
Detection Rate (DR)	99.2	97.3
False Positive Rate (FPR)	0.82	1
False Negative Rate (FNR)	6.0	3.2

From the table 1, 2, 3 and table 4, it is concluded that the proposed filtering rule schema generates the accurate rules for detection of attacks using KDD CUP 99 dataset. And Association Rules also performs good but not better than filtering rule schema generation by utilizing Artificial Neural Network.

5. CONCLUSIONS

Data mining methods are capable of extracting patterns automatically and adaptively from a large amount of data. Various methods related to intrusion detection system are studied and compared. From the obtained results, it is concluded that the proposed filtering rule schema generation improves the detection accuracy and reduces the error rates than the rule schema generation by Apriori Association rule mining algorithm. Thus, this framework can be used for the detection of attacks in the Mobile Ad Hoc Network by considering the nodes which are connected to the network.

REFERENCES

[1] A. Anand, R. Rani, H. Aggarwal, "A Security Model based on Reputation and Collaboration through Route-Request in Mobile Ad Hoc Networks", *KSII Transactions on Internet and Information Systems*, **9(11)**, 4701-4719, November 2015.

[2] Hetal P. Mistry, Nital H. Mistry, "A Survey: Use of ACO on AODV & DSR Routing Protocols in MANET", *2015 International Conference on Innovations in Information, Embedded and Communication Systems*, **1(6)**, 19-20 March 2015.

[3] Y. Haripriya, K.V. Bindu Pavani, S. Lavanya and V. Madhy Viswanatham, "A Framework for Detecting Malicious Nodes in Mobile Ad Hoc Network", *Indian Journal of Science and Technology*, **8**, 151-155, January 2015.

[4] Adnan Ahmed, Kamalrulnizam Abubakar, Muhammed Ibrahim Channa, Khalid Haseeb, Abdul Waheed Khan, "A Survey on Trust based Detection and isolation of malicious nodes in ad hoc and sensor networks", *Frontiers of Computer Science*, **9(2)**, 280-296, 2015.

[5] Fatih Celik, "DEVS-M: A Discrete Event Simulation Framework for MANETS", *Journal of Computational Science*, **13**, 26-36, March 2016.

[6] M. Kaliappan, B. Paramasivan, "Enhancing Secure Routing in Mobile Ad Hoc Networks using a Dynamic Bayesian Signalling Game Model", *Computers and Electrical Engineering*, **41**, 301-313, January 2015.

[7] M. Sulaiman Khan, Maybin Muyeba, Frans Coenen, "Weighted Association Rule Mining from Binary and Fuzzy Data", *ICDM 2008*, LNAI 5077, 200–212, 2008.

[8] M. Sulaiman Khan, Maybin Muyeba, Frans Coenen, David Reid, "Mining Fuzzy Association Rules from Composite Items", *Lecture Notes in Computer Science Volume* 5433, 62-74, 2009.

[9] Tao, F., Murtagh, F., Farid, M, "Weighted Association Rule Mining Using Weighted Support and Significance Framework". *In: Proceedings of 9th ACM SIGKDD Conference on Knowledge Detection and Data Mining*, Washington DC, 661-666, 2003.

[10] Lu, S., Hu, H., Li, F, "Mining Weighted Association Rules", *Intelligent data Analysis Journal*, **5(3)**, 211 - 255, 2001.

[11] Wang Taihua, Guo Fan, "Associating IDS Alerts by an Improved Apriori Algorithm", *IEEE Third International Symposium on Intelligent Information Technology a nd Security Informatics*, 978-0-7695 -4020-7/10, 478 – 482, 2001.

[12] Zhang yanyan,Yao Yuan, "Study of Database Intrusion Detection Based on Improved Association Rule Agorithm", *IEEE* 978-1-4244-5540- 9/10, 673 – 676, 2010.

[13] Flora S. Tsai, "Network Intrusion Detection Using Association Rules". *In International Journal of Recent Trends in Engineering*, **2(2)**, November 2009.

[14] Ming-Yang Su, Kai-Chi Chang, Hua-Fu Wei, Chun-Yuen Lin, "A Real-time Network Intrusion Detection System Based on Incremental Mining Approach", *IEEE*, 1-4244-2415-3/08, 179 – 184, 2008.

[15] Helm B., "Fuzzy Association Rules: An Implementation in R" *Master's Thesis, Vienna University of Economics and Business Administration Vienna*, 2007.

[16] Camila Lorenz, Antonio Sergio Ferraudo, Lincoln Suesdek, "Artificial Neural Network applied as a Methodology of Mosquito Species Detection", *Elsevier Acta Tropica*, 165-169, 2015.

[17] Marcus Frean, "The Upstart Algorithm: A Method for Constructing and Training Feedforward Neural Networks", *Neural Computation*, Massachusetts Institute of Technology, 198-209, 1990.