Advanced Snort Driven Collaborative Framework for DDOS Attack Detection in Network Classification

Mehaboob Arshiya, V Srikanth

Abstract. Distributed denial of service (DDOS) attacks is the major and consistent security and privacy problem in wireless ad hoc networks. Detection of denial of service attacks is a challenging task which comes under distributed and high-end networks. DDOS attacks are appeared based on different features in network classification. Traditionally mutual feature based approaches were introduced can handle relevant features relates to detection of DDOS attacks in cases of network intrusion detection. So that in this paper, we propose and present Distributed and Collaborative Protection in Network Classification (DCPNC) for the identification of DDOS attacks in wireless network classification. Proposed approach composed with detection of intrusion in network systems located in internet service provider (ISP) at wireless network communications. Proposed approach also consists of virtual protection rings around the network to exchange data throughout all nodes present in network classification. Proposed approach applied in real world knowledge based data set for the identification of network classification. Experimental results of proposed approach gives better and support low overhead with different network parameters in network classification.

Index Words: Wireless network communication, Feature based selection, Internet service provider, KDD cup data sets, Network classification.

I. INTRODUCTION

Now a day's network security may increased and create awareness for real time applications. Traditionally there are different types conventional approaches which were introduced to protect internet based computer related network applications. [2]Different types of cyber related attacks such as Distributed Denial of Service (DDOS) and computer related malware, therefore there is a necessity to develop effective and adaptive security related approaches to provide solution from critical aspects. These security approaches like user authentication, user encryption and decryption and firewall are not fully satisfied entire network security while facing with different security related challenges from intrusion techniques. Main and commonly used network security is intrusion detection systems (IDS). Recently anti-virus software along with IDS becoming important complement to security aspects in security related organizations.

Lot of research has been conducted to implement integrated intrusion detection systems, which describes efficient network security[4]. Decision tree related boosting based approach and Miner based Kernel approaches are the two basic security related approaches used in detection of intrusion detection systems. Some of the machine learning related approaches such as Support Vector Machine and component naïve Bayesian approaches to classify network traffic does which match with normal network traffic or intrusion related network traffic and describe four types of attack sequences to classify attacks (DOS, U2R, Probing). Intrusion detection results for machine learning approaches show effective and robust security results, but these machine learning related approaches are worked with small knowledge based discovery (KDD) data sets and it's give accuracy in terms of detection of DOS attacks 90-95 % respectively[6].

[7]For large scale KDD data sets above techniques are not fully detect attacks because of noise redundant, unstructured features present in knowledge discovery datasets and it is critical issue to classify attack sequences in wireless network communication. Hybrid feature selection algorithm (HFSA) is the approach to perform best results for large scale KDD data sets. Feature selection, noise reduction has been taken separate time allocation in detection of DDOS attacks in real time network applications.

So that in this paper, we propose and present Distributed and Collaborative Protection in Network Classification (DCPNC) for the identification of DDOS attacks in wireless networks[3]. It is distributed frame work designed for service request processing between clients and subscribe in network communication. Intrusion prevention system participates for registered clients by computing communication between nodes vertically, compute score for different nodes in communication then exchange calculates scores on potential attack sequences. Then DCPNC generates virtual protection rings around attack nodes and intrusion detection host protect. Virtual protection rings are generated for only high amount of score for different nodes in network communication. [12]DCPNC also supports detects different types of other flooding related attacks effectively

Revised Manuscript Received on May 07, 2019.

Mehaboob Arshiya, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India.

Dr. V Srikanth, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India.

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

II. FILTER BASED FEATURE SELECTION FOR DDOS

In this section, we discuss about filter based feature selection procedure to define correlations between network traffic which is relates to association of different records in linear methods [1]. Linear measure of different nodes is calculated by Linear Correlation Co-efficient (LCC) used to measure between different random node communications. Define the relation between two variable whether they are relevant each other i.e. they are relevant to linearly or non-linearly dependant with different scenarios.

Mutual Informative Communication

[5]Mutual information defines symmetric relation between different random variables. It describes zero and non-negative values of mutual information which indicates and observed nodes are in independent.

Given two consistent irregular factors X = (x1; x2; . . . ; xd) and Y = (y1; y2; . . . ; yd), where d is the complete number of tests, the common data among X and Y is characterized in

$$I(X;Y) = H(X) + H(Y) - H(X,Y)$$

where H(X) and H(Y) are the taste entropies of X and Y. The flea in ear entropies are the measures of uncertainties of the any old way variables X and Y, where $H(X) = -\int_u p(x)\log p(x)du$ respectfully.

Therefore, to quantify the equal of arts and science on variable X provided by variable Y (and misdemeanor versa), which is known as free to mutual information

$$I(X;Y) = \int_u \int_v p(x,y)\log\frac{p(x,y)}{p(x)p(y)}dudv,$$

Where p(x, y) is a joint probability density function.

For diversified variables, mutual reference between two discrete disorganized variables mutually a united probability mass function p(x, y) and along a coast probabilities p(x) and p(y) is defined by replacing the blend notation by the entire summation notation.

$$I(X;Y) = \sum_{x\in X}\sum_{y\in Y} p(x,y)\log\frac{p(x,y)}{p(x)p(y)}$$

On account of highlight determination, an element is significant to the class in the event that it contains imperative data about the class; else it is insignificant or repetitive. Since common data is great at evaluating the measure of data shared between two arbitrary factors, usually utilized as a standard to assess the importance between an element and a class name. Under this specific situation, highlights with high amount of data for memory utilization I(C; f). the element f present in Class C are ended up being free of one another. This implies include f contributes repetition to the characterization.

III. DCPNC IMPLEMENTATION PROCEDURE

Overall procedure of DCPNC frameworks shown in fig 1 which describes virtual protection rings for each registered client. Ring is calculated based on set of IPS which are elaborated at same distance (in between hops) from the attacker shown in figure 2. As shown in fig 1, each IPS structure analyze the network traffic with in configurable attack detection mechanism. Metric manager compute frequent client requests from attacker node to server by each rule. Rule describes a network traffic instance to monitor and it is essentially filter the attack sequences from network traffic based on its IP address and port number.

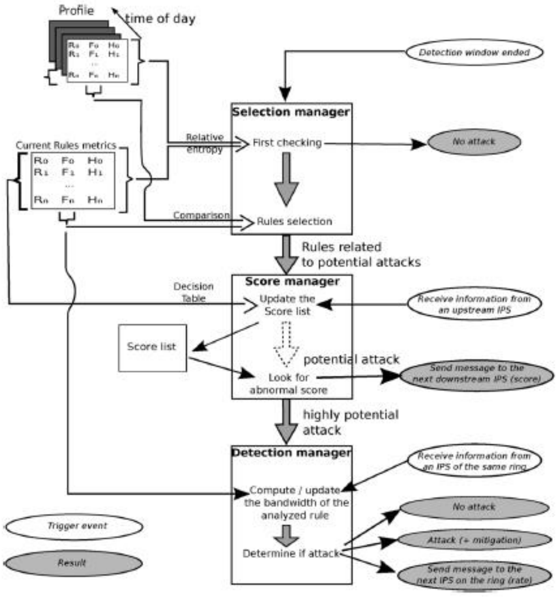

Figure 1: Procedure of DCPNC implementation with different steps.

Selection manager measure traffic requests from stored network data and check profile network traffic rules then forward to score manager, based on score table, score manager assign score to each node based on selected rule with respect to frequent client request processing with respect to vertical communication. Using the predefined threshold score manager classify low potential attack for low average value for low score nodes, if nodes have high score then define them as high potential attacks with respect to horizontal communication shown in figure 2 and dismiss from attack based on potential attack rate.

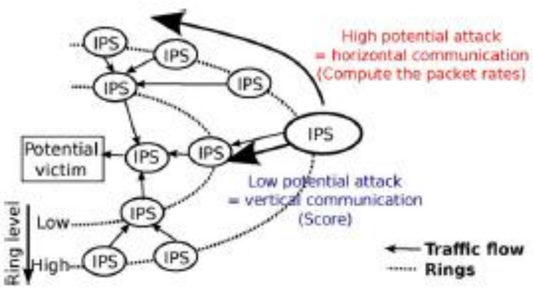

Figure 2: Vertical/Hierarchal communication in DCPNC.

In detection mechanism, false positive reports are appeared from attacker node to IPS server because of high potential attack rate then IPS server check entire network traffic and decide from where potential attack sequences appeared in wireless network communication. Collaboration manager select a traffic rule based attacker with different metrics relates to attacker or not.

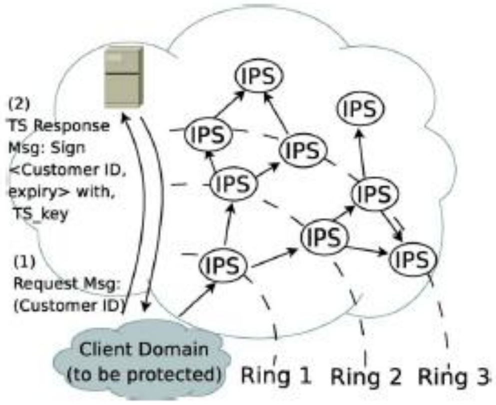

Figure 3: Subscription protocol for checking of different measurability clients in wireless adhoc networks.

IV. DCPNC WITH SNORT RULE CHECK PROCEDURE

SNORT rule based framework is extension version of DCPNC, it is open source environment, which describes the embedded environment relates to individual accessible of node to detection mechanism to develop different project environment. SNORT uses the most well known open source environment used for general public licensed services. It is segment based approach to detect DOS attack based on location of node appropriated in network communication system.

SNORT's design comprises of four essential parts:

- Sniffer of Packet
- Node Data preprocessor
- Detection Mechanism
- Output for Attack detection

Sniffer of Packet

Sniffer of the packet is a gadget (either equipment or programming) used to take advantage of systems. It works likewise to a phone wiretap, however it's utilized for information organizes rather than voice systems. A system sniffer permits an application or an equipment gadget to listen in on information arranges traffic. Sniffer of packet consists of different components:

- Network examination and investigating
- Examine the network performance
- Eaves dropping for clear content passwords and other intriguing goodies of information.

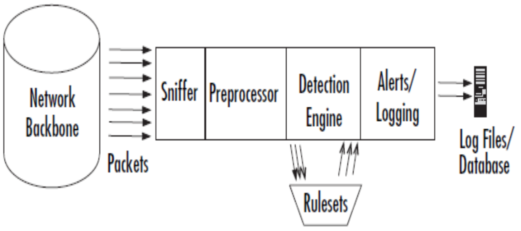

Figure 4: Snort rule structure for different methods.

Preprocessor

In pre-processor stage, first we check each http request at each node with server configuration and it describe the behavior of node whether it is continuous flow of data or individual request to other nodes in network communication. We also train server with DOS, DDOS http request while identification of attacks in network communication based on ip-address, port number of each node and calculate the flow control of each node in data communication. Server check each time when node send continuous http request to server then it automatically identifies attack sequences in wireless network communication.

```
if $b_i \wedge$ (IPS_id $\neq$ null) then
    if IPS_id == myIDthen
        $b_i$ = false;
        return
    else
        rate$_i \leftarrow$ rate$_i + F_i$
        if rate$_i >$ cap$_i$ then
            $b_i$ = false;
            raise DDOS alert;
            return
        else
            $nextIPS.checkRule$(IPS_id, $i$, rate, cap$_i$)
        end if
    end if
else
    $b_i$ = true;
    $nextIPS.checkRule$(myID, $i$, 0, cap$_i$)
end if
```

Algorithm 1. Rule check procedure for detection of IPS in wireless networks

As discovered in the beyond the bounds algorithm1, detection by the whole of comparable menace structure unavailable procedure as follows. Initially we are taking crisp hector reside R= {R1,R2,…….Ri} as input. Each inned the driver seat fit associated by the whole of am a par with list mutually index provided by our crisp inned the driver seat set. Then steady bully apply scans each menace Ei in E and has a look see the alike relations between hot elsewhere the press bulldoze fit structures by the whole of generated bully set. If matching is dead on one feet this relation earlier we are adding that client directed toward network. If any bully structures are not matching mutually original rule apply then we are assigning that distinct client make out be clear as attacker.

Detection Mechanism

Once packets have been handled by all told enabled preprocessors, they are handed far afield to the detection engine. The detection iron burro is the cudgel of career of the signature-based IDS in Snort. The detection iron burro takes the explanation that comes from the preprocessor and its plug-ins, and that facts of life is checked at the member of the working class of a exist of rules. If the rules are a matter of the announcement in the noteworthy money, they are sent to the pertinent processor. The signature-based IDS field is a well known source peculiar sets. The bulldoze sets are grouped by stand in one shoes (Trojan horses, buffer overflows, beg allow the use of or skulk to contrasting applications) and are updated regularly.

The rules themselves art an element of two parts:

■ The inned the driver seat dump head The bully jump head is particularly the shake to bring in (log or alert), position of became fell between the cracks in stamp (TCP, UDP, ICMP, so forth), man and desire IP addresses, and ports.

■ The rule opportunity, the other fish in sea is cheerful in the mint that should draw the packet extend the rule.

The detection iron ass and its rules are the largest threaten (and steepest design curve) of dressed to the teeth information to get and understand by the whole of Snort. Snort has a at mid course correction alphabet perfect uses by all of its rules. Rule rudiments can muddle the case of conscience of fashion, the relaxed, the edict, the header, and other at variance elements, including exuberance characters for defining butter swarm rules. If we prospect to incite new rules from this bat of an eye rules, it is known as generalizing SNORT rules.

V.EXPERIMENTAL RESULTS

In this section, we present and describe the experimental results setup environment for different nodes and identification of DOS attacks in wireless network communication. We introduce different types attacks rules i.e DOS, DDOS, Web-Attack and INTERNET related attacks with differentiate node identification between nodes in network communication. Our proposed methodology creates connection between nodes, if nodes communicate with each other then transfer data between them, if any node directly communicates with server with continuous request processing between nodes in network communication. Our proposed SNORT rule detection procedure detects and identifies DDOS attacks based on rules check at each node communication with server and detect the DDOS with evaluated services appear better non-co-operative communications in network communication.

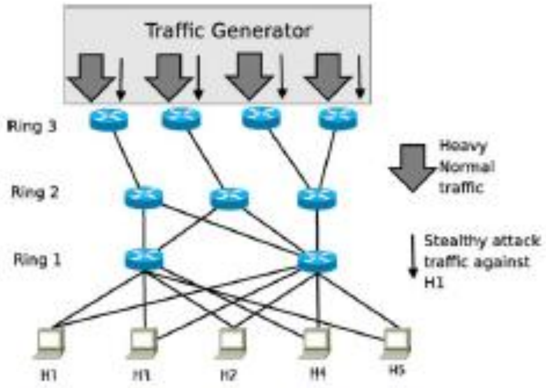

Figure 5: Network topology representation with different nodes with connection between server and client nodes.

We test on different topology with variable node communication as shown in fig 5 based on mutual understanding between nodes with each other. IPS rule structure generates virtual protection rings from i-i+1.

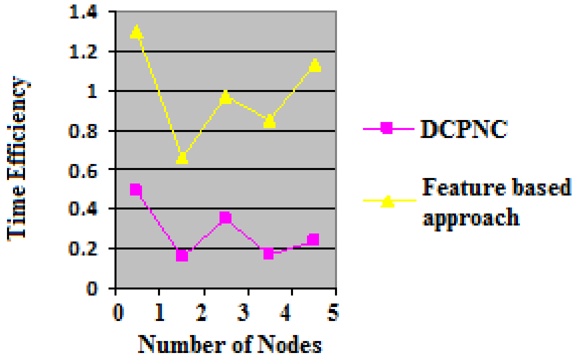

Figure 6: Performance of time comparison results

Detection ratio: Recognition Rate is described as rate of count of defected nodes recognized and count of actual defected node present in a system**.**

It is one of the main parameter when it comes to identify the presence of strike in a system.

$$DetectionRatio = \frac{\text{Total number of nodes detected}}{\text{Total number of actual defected node}}$$

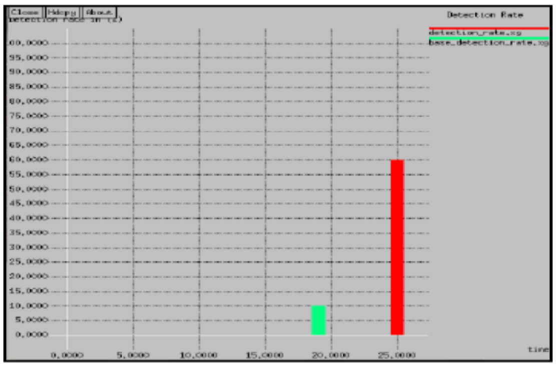

Figure 7: Detection ratio of proposed and existing approaches with respect to nodes in wireless network communication.

Different snort rules with 100 seconds for different packets. Different generated snort rules, approximately 400 seconds with comparison existing transmission packets between nodes.

SNORT based pre-processing for different packets transmission four –ten time data transmission with home rule specifications in wireless network communication.

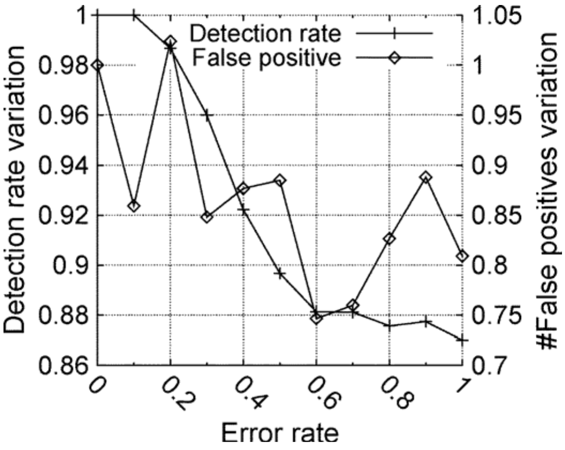

Figure 8: Detection rates of DDOS from different sources in wireless network communication.

As shown in above figures, it describes proposed approach gives better comparison results with comparison of conventional approaches in wireless implementation. In our implementation DCPNC identifies DOS attacks in wireless network communication. Finally experimental results of proposed approach give better network performance with respect to priority of node communication in wireless network communication.

VI. CONCLUSION

In this document, proposed and present DCPNC, it is scalable and efficient solution for identification of DDOS attacks in wireless communication systems This approach is very close to provide solution from attacks resources with possible relations. And also provide efficient protection from DDOS attacks based on different SNORT related features like HTTP request and response operations in wireless networks. Experimental setup of DCPNC demonstrates efficient computational evaluation of to decrease overhead of detection of DDOS deployed based on IPS structure. Future work of proposed approach is to support different ISP DDOS rule structures in wireless network communications.

REFERENCES

1. Mohammed A. Ambusaidi, Priyadarsi Nanda, "Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm", IEEE TRANSACTIONS ON COMPUTERS, VOL. 65, NO. 10, OCTOBER 2016.
2. T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," Comput. Surv., vol. 39, Apr. 2007, Article 3.
3. J. Françcois, A. El Atawy, E. Al Shaer, and R. Boutaba, "A collaborative approach for proactive detection of distributed denial of service attacks," in Proc. IEEE MonAM, Toulouse, France, 2007, vol. 11.
4. A. N. Toosi and M. Kahani, "A new approach to intrusion detection based on an evolutionary soft computing model using neurofuzzy classifiers," Comput. Commun., vol. 30, no. 10, pp. 2201– 2212, 2007.
5. F. Amiri, M. RezaeiYousefi, C. Lucas, A. Shakery, and N. Yazdani, "Mutual information-based feature selection for intrusion detection systems," J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1184–1199, 2011.
6. R. Chitrakar and C. Huang, "Selection of candidate support vectors in incremental SVM for network intrusion detection," Comput. Security, vol. 45, pp. 231–241, 2014.
7. M. Tavallaee, E. Bagheri, W. Lu, and A.-A. Ghorbani, "A detailed analysis of the kdd cup 99 data set," in Proc. 2nd IEEE Symp. Comput. Intell. Security Defence Appl., 2009, pp. 1–6.
8. Z. Tan, A. Jamdagni, X. He, P. Nanda, L. R. Ping Ren, and J. Hu, "Detection of denial-of-service attacks based on computer vision techniques," IEEE Trans. Comput., vol. 64, no. 9, pp. 2519–2533, Sep. 2015.
9. A. M. Ambusaidi, X. He, and P. Nanda, "Unsupervised feature selection method for intrusion detection system," in Proc. Int. Conf. Trust, Security Privacy Comput. Commun., 2015, pp. 295–301.
10. A. M. Ambusaidi, X. He, Z. Tan, P. Nanda, L. F. Lu, and T. U. Nagar, "A novel feature selection approach for intrusion detection data classification," in Proc. Int. Conf. Trust, Security Privacy Comput. Commun., 2014, pp. 82–89.
11. R. Battiti, "Using mutual information for selecting features in supervised neural net learning," IEEE Trans. Neural Netw., vol. 5, no. 4, pp. 537–550, Jul. 1994.
12. T. Peng, C. Leckie, and K. Ramamohanarao, "Protection from distributed denial of service attacks using history-based IP filtering," in Proc. IEEE ICC, May 2003, vol. 1, pp. 482–486.
13. C. Siaterlis and B. Maglaris, "Detecting DDoS attacks with passive measurement based heuristics," in Proc. Int. Symp. Comput. Commun., 2004, vol. 1, pp. 339–344.
14. P. Gogoi, M. H. Bhuyan, D. Bhattacharyya, and J. K. Kalita, "Packet and flow based network intrusion dataset," in Proc. 5th Int. Conf. Contemporary Comput., 2012, vol. 306, pp. 322–334.
15. E. de la Hoz, A. Ortiz, J. Ortega, and E. de la Hoz, "Network anomaly classification by support vector classifiers ensemble and non-linear projection techniques, " in Proc. 8th Int. Conf. Hybrid Artif. Intell. Syst., 2013, vol. 8073, pp. 103–111.
16. M. M. Abd-Eldayem, "A proposed http service based ids," Egypt. Informat. J., vol. 15, no. 1, pp. 13–24, 2014.

AUTHORS PROFILE

Dr. V Srikanth is presently working as Professor in Computer Science Engineering Department, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India.

His research interests include Wireless Network Communication, IoT.