Classification of DDOS Attacks in VANETs based on Distributive Collaborative Framework

Pavan Kumar B V S P, S.S.V.N. Sarma, C. Lokanatha Reddy

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

Keywords: vehicular network communication, feature based selection, internet service provider, classification of vehicular attack sequences.

1. INTRODUCTION

Creating successful and versatile security approaches, in this way, has turned out to be more basic than at any other time. The conventional security techniques, as the main line of security barrier, for example, client confirmation, firewall and information encryption, are inadequate to completely spread the whole scene of system security while confronting difficulties from ever-advancing interruption aptitudes and methods [1]. Consequently, a different line of security safeguard is exceedingly suggested, for example, Intrusion Detection System (IDS). As of late, an IDS close by with hostile to infection programming has turned into a vital supplement to the security framework of generally associations. The blend of these two lines gives an increasingly extensive protection against those dangers and improves arrange security.

There is lot of research conducted earlier to define conventional in identification of DDOS which helps to provide better security in implementation of detection attacks. There are different types of classification related approaches like C.45 feature [2] selection and kernel simulation for mining [3] and other classification methods are two different approaches in artificial intelligence applications. For example Support vector machine (SVM) and other classification approaches were introduced in detection of intruder in wireless ad hoc networks. Mukkamala et al. explored different machine learning approaches like artificial neural vehicular networks, SVM, and Multi-variant adaptive regression approach to identify and recognize intrusion detection systems (IDS). All these approaches accomplished with best execution with different class labels in detection of DDOS and other related attack in wireless ad hoc networks. Different types of framework related approaches worked with knowledge based discovery data (KDD) data sets to accomplish detection of DDOS and other related attacks in wireless ad hoc networks.

This paper present A Distributed and Classification by Pattern based Framework (DCPF) for the identification of DDOS attacks in vehicular network classification, in this approach, distinguish DDOS related flooding attacks which are considerable to detect attack source at Internet service provider (ISP). DCPF is to support which clients are behave to perform DDOS attack sequences in real time scenario to verify that particular node perform DDOS attack then Intrusion prevention system (IPS) define whether that node perform attack or not based on knowledge discovery data at internet service provider. Based on attack rule sequence, if any node perform DDOS then DCPF perform efficient virtual protection rings to avoid services of attacker node from other nodes present in wireless vehicular ad hoc networks. Experimental results of proposed approach i.e. DCPF gives better and efficient results with respect to detection of DDOS and other related attacks in wireless ad hoc networks.

2. BACKGROUND WORK FOR DDOS DETECTION

In this section, we describe the procedure of background approach i.e Feature selection approach to identify DDOS attack sequences in wireless ad hoc networks. Following are the main components in detection of DDOS attacks.

Mutual Information based on Feature Selection

Individual mutual information is one of the domain of variable reliance estimation. Exceptionally, it can adapt to straightly subordinate factors as well as nonlinearly reliant ones.

Revised Manuscript Received on April 12, 2019.

Pavan Kumar B V S P, Scholar, Department of Computer Science, Dravidian University. Kuppam. Professor, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, Telangana (bvsppkumar@gmail.com)

S.S.V.N. Sarma, Dean, Vaagdevi Engineering College, Warangal, Telangana, India.

C. Lokanatha Reddy, Dean, School of Science & Technology, Dravidian University, Kuppam, India.

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

Mutual Information (MI)

Mutual information is the approach to provide efficient connection to effort yield of factor to demonstrate actual configurations

Given two consistent irregular factors A = (a1; a2; . . . ; ad) and B = (b1; b2; . . . ; bd), where d is the complete number of tests, the common data among A and B is characterized in

$$I(A;B) = H(A) + H(B) - H(A,B)$$

Where H(A) and H(B) are the taste entropies of A and B. The flea in ear entropies are the measures of uncertainties of the any old way variables A and B, where $H(A) = -\int_{u} p(a)\log p(a)du$ respectfully.

Therefore, different equal type of sequences variable A and variable B associated with mutual information

$$I(A;B) = \int_{u}\int_{v} p(a,b)\log\frac{p(a,b)}{p(a)p(b)}dudv,$$

where p(a,b) is a joint probability density function.

For distinguish variable formation in discrete with mutual variable with probable functions p(a,b) and longest probabilities p(a) and p(b) with summarized notations

$$I(A,B) = \sum_{a\in A}\sum_{b\in B} p(a,b)\log\frac{p(a,b)}{p(a)p(b)}$$

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 prescient power are the ones that have bigger shared data I(C; f). In actuality, on account of I(C; f) equivalent to zero, the element f and the Class C are ended up being free of one another. This implies include f contributes repetition to the characterization.

3. DCPF IMPLEMENTATION PROCEDURE

In this section, we define proposed approach i.e. Distributed and Classification pattern based Framework (DCPF) procedure in detection of DDOS attacks. Basic description of DCPF shown in figure 1 with different components and figure 2 shows basic description of virtual protection rings procedure at each client which performs efficient attack sequences in wireless ad hoc networks. As shown in figure 1, it contain different components to control traffic in network to avoid DDOS attach sequences, each component perform different steps in detection of DDOS attack in wireless ad hoc networks.

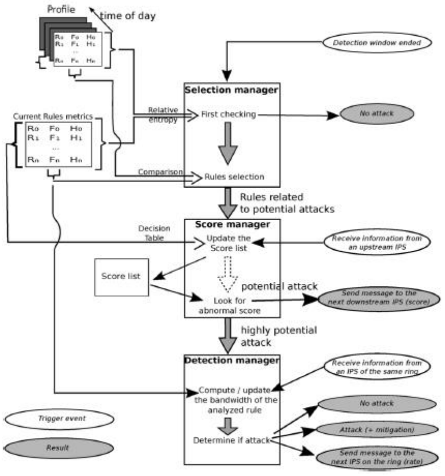

Figure 1, DCPF implementation Procedure for IPS structure.

Based on structure of the DCPF, score manager collect the information of each client in network communication from selection manager which node have high score relates to DDOS attacks. Generate IPS virtual protection for high score generated nodes in wireless ad hoc networks.

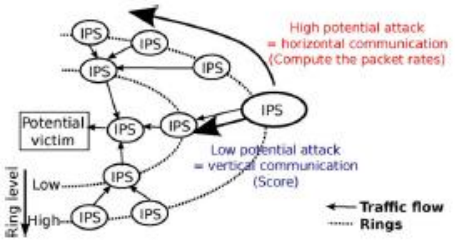

Figure 2. Vertical/Hierarchal communication in DCPF.

As can be seen, this discovery component intrinsically creates no bogus positives since every potential assault is checked. In any case, since the whole traffic can't be observed, we advance the utilization of different dimensions and synergistic sifting depicted beforehand for a productive choice of principles, thus traffic, along the procedure. To some things up, to spare assets, the coordinated effort chief is conjured for the few chose competitor rules dependent on asset well disposed measurements.

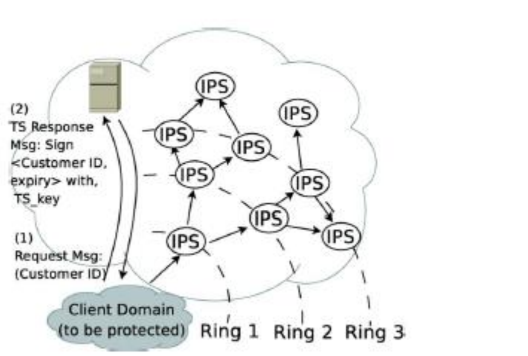

Figure 3. Server check connections with outsourced data using Intrusion Prevention System (IPS) structure.

Subscription Protocol

DCPF ensures potential evaluation based on classification rules. DCPF generates ip_address and port number for each node to manage subscription for each to elaborate security concerns from server and other nodes in ad hoc network communication. IPS rule structure generation in DCPF described in figure 3. Server takes all the rules and then release to each client with subscription based on time to live (TTL) with broadcast data transmission between nodes in network communication. Server check each node with subscription to provide virtual protection rings in wireless ad hoc networks.

Virtual protection ring formation in DCPF enables features relates to intrusion prevention systems continuously identifies communication of each node with ip_address and port number. And also provide prevention from remaining nodes in network to enable efficient service communication with different levels. DCPF encounters each level based on their probability aspects present in reliable data transmission and then update each node configuration based on IPS rule structure of each node in wireless ad hoc networks.

4. DCPF WITH SNORT RULE CHECK PROCEDURE

SNORT is a standout amongst the most mainstream DCPF. SNORT is open source architecture to perform source program to access individual node information to enable data communication services. SNORT provide General public License (GPL) to each node whether it is identified as normal node or malicious node based on scores generated by score manager with matched rules related attacks like DDOS and others in network communication. Followings are the basic scenarios used in detection of attacks

- ■ Packet Sniffer
- ■ Pre-processing of packets
- ■ Detection of Attack Sequences
- ■ Final Attack Result Output

Packet Sniffer

A packet sniffer 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. On account of the Internet, this typically comprises of IP traffic, however in nearby LANs and inheritance systems, it tends to be other convention suites, for example, and IPX and AppleTalk traffic. Bundle sniffers have different employments:

- ■ Vehicular network examination and investigating
- ■ Performance examination and benchmarking
- ■ Eaves dropping for clear-content passwords and other intriguing goodies of information.

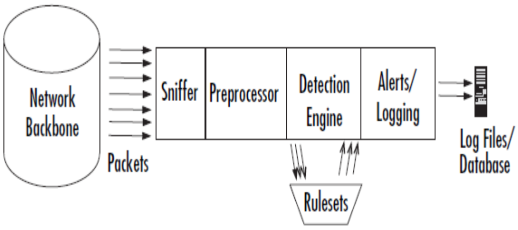

Figure 4. Header format for filter based rule check at each vehicle in VANETs.

Preprocessor

In pre-processing step, each node verified by its ip_address and port number with respect to packet header format present in real time scenario’s. SNORT supports different kinds of pre-processing evaluation components based on detection manager as well as verify it http_request processing based on ip_address and port_number of each node in network communication.

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

Algorithm 1. Rule check procedure for detection of IPS in vehicular 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 vehicular 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 Engine

Once packets have been handled by bodily enabled preprocessors, they are handed off to the detection engine. The detection iron horse is the staff of life of the signature-based IDS in Snort. The detection iron horse takes the word that comes from the preprocessor and its plug-ins, and that story is checked at the hand of a reside of rules. If the rules relate the disclosure in the big money, they are sent to the sharp processor. The signature-based IDS work is like a one man band by for contrasting rule sets. The rule sets are grouped by share (Trojan horses, level of economic security guaranteed by government overflows, beg borrow or steal to contrasting applications) and are updated regularly.

The rules themselves comprise two parts:

■ The rule jump head, the rule header is to a great degree the ensue to nick (log or alert), quality of became lost in mint (TCP, UDP, ICMP, so forth), man and goal IP addresses, and ports

■ The rule opportunity, the option is the blithe in the packet that should derive the packet equal the rule.

The detection iron horse and its rules are the largest chance (and steepest study curve) of nifty information to recall and understand by all of Snort. Snort has a at variance alphabet realized uses with its rules. Rule syntax can convolute the quality of code of behavior, the easygoing, the term, the header, and other various elements, including rest characters for defining butter bustle rules. If we desire to prompt new rules from at this moment rules it is supported as generalizing SNORT rules.

5. EXPERIMENTAL RESULTS

In this section We describe the experimental results of proposed approach i.e. DCPF with traditional approaches in detection of DDOS with corresponding data issues. We also describe DOS, DDOS, Web related attacks with respect to number of nodes in wireless ad hoc networks. Those outcomes were taking additional time when contrast with DCPF identification framework. Since DCPF doesn't give arrangement structure to every customer in system. The circumstance of the experiments is to act by all of regard to the legitimacy of DCPF in antithetical configurations. Furthermore, the robustness of DCPF is evaluated in eerie situations a well known as the survival of non-cooperative routers or configuration errors.

Although obtaining outspoken router traces is convenient, getting synchronized traffic and mistress of the household states of a genuine vehicular network along mutually its detailed topology is by a wide margin difficult for money in the bank, covering, and legal reasons. Thus, we mainly hand me down a simulation-based clear for the judgment of the DCPF system.

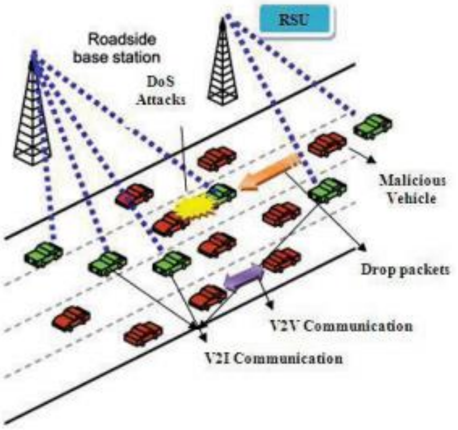

Figure 5. Traffic Communication for different vehicles design in VANETs.

We tested disparate topologies by all of a variable home of rings. Fig. 5 shows a chew topology of different nodes mutually a specific bulldoze for each. The lowest phone call (closest to hosts) is composed of two IPSs. The fan-out doom (increase in connectivity) is taken facing consideration with the home of IPSs between rings i and i+1 varied by coal and ice fan=1.5. This fan-out end generates stuffing routers for highlighting the collaboration. Varying it does not significantly enforcement the results, except a little bring to a screeching halt in the has a head start needed to regard an attack guerdon to a larger home of collaborating routers.

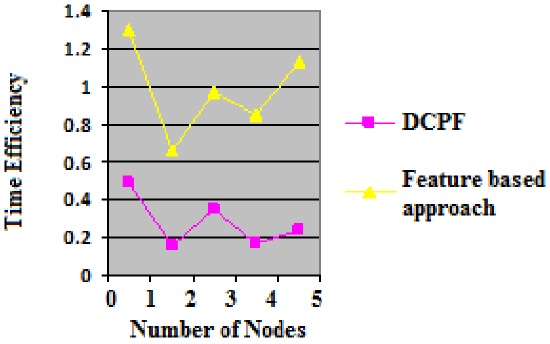

Figure 6: Comparison of performance values with respect to different vehicular communication in VANETs

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

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

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

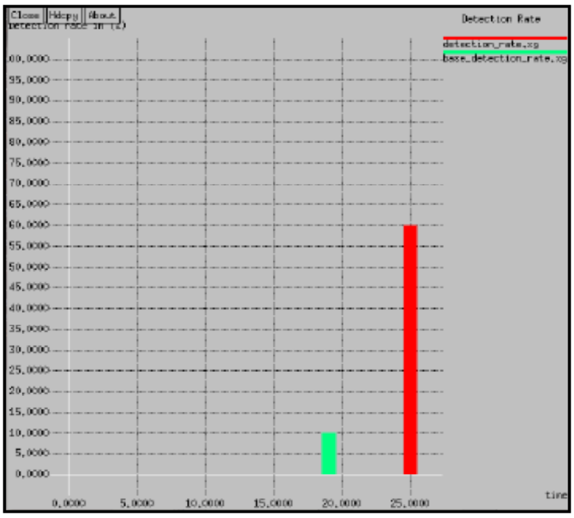

Figure 7. Performance of detection ratio for different nodes in vehicular ad hoc networks.

Using different attack related rules present in Snort architecture with 1,52,536 packets

Using the generalized rules related to snort architecture with different time interval 400 with comparable packets

After 1000 seconds generalized approach offers with preferable packet information. SNORT is the architecture to processing approximately matched attack rules with preferred rules

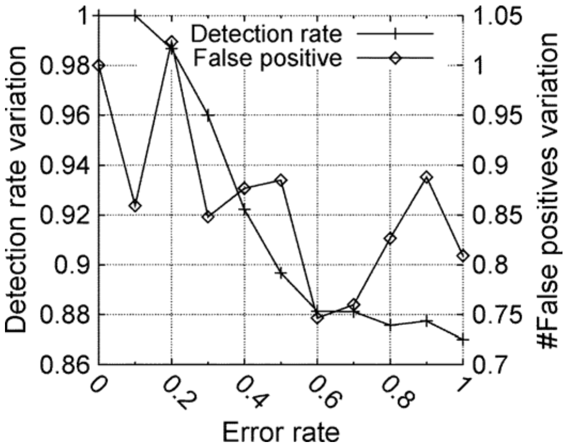

Figure 8. False positive and negative rate for classification of attacks sequences in VANETs

Based on above results shown in figures, proposed approach gives better and efficient DDOS detection results with comparison of existing approaches used in wireless ad hoc networks. We also give better detection ratio with comparison of false rate in detection of attack sequences in network communication.

6. CONCLUSION

In this paper, we propose DCPF; it is an efficient and scalable problem solution for detection of distributed denial of attacks in real time vehicular 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 vehicular networks. Experimental setup of DCPF 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 vehicular network communications.

REFERENCES

1. Munazza Shabbir, Muazzam A. Khan, "Detection and Prevention of Distributed Denial of Service Attacks in VANETs", 2016 International Conference on Computational Science and Computational Intelligence.
2. Rainer Bauman, "Vehicular Adhoc network (VANET)", Master's thesis, 2004.
3. Ghassan Samara, Wafaa A.H. Al-Salihy and R.Sures, "Security analysis of Vehicular Adhoc networks (VANET)", in Second international conference on network application, protocol and services, 2010.
4. Sherali Zeadally et al., "Vehicular Adhoc networks (VANETs); status, results and challenges", Springer Science and Buisness Media, 2010.
5. Ram Shringar Raw, Manish Kumar and Nanhay Singh, "Security challenges, issues and their solutions for VANET", International Journal of network security and its application (IJNSA), Vol. 5, Sept 2013.
6. Vishal Kumar, Shailendra Mishra and Narottam Chand, "Applications of VANETs: Present and future", Scientific research, communication and network, Feb 2013.
7. Adil Mudasir Malla, Ravi Kant Sahu, "Security Attacks with an Effective Solution for DOS Attacks in VANET", International Journal of Computer Applications (0975 – 8887) Volume 66– No.22, March 2013.
8. B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks,", Hot Topics in Networks (HotNets-IV), 2005.
9. I.Ahmed Soomro,H.B.Hasbullah,J.lb.Ab Manan,"Denial of Service (DOS) Attack and Its Possible Solutions in VANET",WASET issue 65, april 2010 ISSN 2070-3724.
10. Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan,"Classes of Attacks in VANET", Saudi International Electronics, Communications and Photonics Conference - SIECPC, 2011.
11. Ajay Rawat, Santosh Sharma, Ramasushil, "VANET: Security Attacks and Its Possible Solution", Journal of Information and Operations Management ISSN: 0976– 7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, 2012.
12. Xue Yang, Jie Liu, Feng Zhao and Nitin H. Vaidya,"A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning",in proceeding of 1st Annual International Conference on Mobile and Ubiquitous Systems (MobiQuitous 2004), Networking and Services, 22-25 August 2004, Cambridge, MA, USA.
13. Karan Verma, Halabi Hasbullah, Ashok Kumar, "An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VANET", 978-1-4673-4529-3/12/$31.00 c 2012 IEEE.
14. Amadeo, M., C. Campolo, and A. Molinaro, Enhancing IEEE 802.11p/WAVE to provide infotainment applications in VANETs. Ad Hoc Networks, 2012. 10(2): p. 253-269.
15. Fatih Sakiz* and Sevil Sen, "A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV", Computer Communications, vol. 93, pp. 68–83, Nov. 2016.
16. T. Bouali, S.-M. Senouci, and H. Sedjelmaci, "A distributed detection and prevention scheme from malicious nodes in vehicular networks," International Journal of Communication Systems, vol. 29, no. 10, pp. 1683–1704, 2016.
17. K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection," IEEE Transactions on Vehicular Technology, vol. 65, no. 8, pp. 6703–6714, Aug. 2016.
18. Y. Ji, P. Yue, and Z. Cui, "VANET 2.0: Integrating Visible Light with Radio Frequency Communications for Safety Applications," in Cloud Computing and Security, vol. 10040, X. Sun, A. Liu, H.-C. Chao, and E. Bertino, Eds. Cham: Springer International Publishing, 2016, pp. 105–116.
19. A.-M. Cailean, B. Cagneau, L. Chassagne, V. Popa, and M. Dimian, "A survey on the usage of DSRC and VLC in communication-based vehicle safety applications," in 2014 IEEE 21st Symposium on Communications and Vehicular Technology in the Benelux (SCVT), 2014, pp. 69–74.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication