Int. J. Advanced Networking and Applications
Volume: 10 Issue: 04 Pages: 3905-3910 (2019) ISSN: 0975-0290

Flow-based Attack Detection and Defense Scheme against DDoS Attacks in Cluster based Ad Hoc Networks

Deepa
Research Scholar, Dept. of RIC, I.K. Gujral Punjab Technical University, Kapurthala, Punjab, INDIA
Email: deepa.nehra@gmail.com
Dr. Kanwalvir Singh Dhindsa
Professor, Dept. of CSE, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, INDIA
Email: kdhindsa@gmail.com
Dr. Bharat Bhushan
Associate Prof., Dept. of Computer Application, Guru Nanak Khalsa College, Yamuna Nagar, Haryana, INDIA
Email: bharat_dhiman@hotmail.com

ABSTRACT

DDoS attacks in MANETs needs to be handled as early as possible so as to avoid them to reach the victim node. DDoS attacks are difficult to detect due to their features like varying attack intensity, large amount of packets etc. so it becomes necessary to distinguish and filter attack traffic in source or intermediate clusters. Here the cluster heads will uses flow based monitoring schemes to identify the suspicious behaviours of incoming traffic in each clusters. Cluster head constructs flows from the incoming traffic and computes normalized entropy for specific time windows. The normalized entropy is compared against threshold entropy to identify the presence of suspicious flows. Later packet rate of suspicious flow is calculated and compared against packet rate entropy to identify the suspicious flows. Later the suspicious flow information is shared with neighbouring cluster heads to further confirm the presence of DDoS attack or not. If DDoS attack is confirmed the packets related to suspicious flows will be discarded. The efficiency and accuracy of proposed attack detection algorithm is evaluated using some performance metrics.

Keywords – **Clustering, Distributed denial of service (DDoS) attacks, Defense, Flow, MANETs**

Date of Submission: Dec 25, 2018 Date of Acceptance: Jan 10, 2019

I. INTRODUCTION

A MANET is the network of infrastructure less, self-configuring devices connected to each other wirelessly [1]. Every node in mobile ad hoc networks can move freely and independently into any direction. Mobile nodes can also change their connections to other devices very frequently. MANETs are also prone to many kinds of attacks but DDoS attack is one of the serious threats that affect their normal operations. The purpose of DDoS attack is to stop the genuine nodes of MANETs from accessing the normal services of other nodes [2, 3]. An attacker can perform a DDoS attack by flooding a huge quantity of malicious packets to the target node by the use of a huge number of intermediate compromised nodes. The attacker sends a lot of unwanted traffic that eats the available network bandwidth or the computing power available with the victim node, so that data requests from legitimate nodes will be rejected. So there is need of an efficient defense mechanism that can accurately distinguish between attack and legitimate traffic and prevents it to reach the victim.

The work proposed here is an attack detection algorithm that differentiates among attack and legitimate packets form the incoming flow. It can be implemented by the cluster heads as they are solely responsible for the routing of entire packets received from its member nodes (one hope away from cluster head). The traffic received by the cluster heads contains a mix of legitimate and attack packets originated from its different member nodes. Initially flows (for each fixed value of time window) are constructed from the incoming traffic and then their normalized entropy is calculated. Normalized entropy is then compared against a predefined threshold value to identify the presence of abnormal activity. If abnormal activity is found then flows are further investigated to identify the flow responsible for creating abnormal behaviour. This can be done by calculating and comparing the packet rate of each flow against a predefined threshold value. After the successful identification of suspected flow, it is further confirmed whether it was DDoS attack or not. Cluster head shares suspected flow information with the neighbouring cluster heads to compute the packet rate for the flow heading towards the identified destination. If suspected flow is confirmed to be the part of DDoS attack then cluster head will discard all the packets related it.

II. RELATED WORK

The MANETs research is a very vast field containing its architecture, security, and routing mechanism. There exist many research papers in the literature that discusses about the DDoS attacks and defense mechanism in MANETs.

Volume: 10 Issue: 04 Pages: 3905-3910 (2019) ISSN: 0975-0290

Some of them along with their advantages and limitations are discussed here.

Wei et al. [4] presented a defense technique which contains together the attack detection and mitigation schemes. The detection based technique in this scheme observes the signals at the medium access control layer and a mitigation technique based on ECN (Explicit Congestion Notification) marking is discussed. Only drawback of this method is that monitoring of packets sent by the source nodes is not discussed. Hence it becomes difficult to identify the attacking nodes. It further results in the growth of false negatives and false positives. Ping et al. [5] suggested an improved DoS and defense mechanism for MANETs. A fresh kind of DoS attack, named ad hoc flooding attack, may causes a DoS when it is to be used against on-demand routing protocols (e.g. AODV and DSR) in MANETs. Rizwan et al. [6] has presented a new architecture for the identification and response against DDoS attacks in MANETs. The architecture contains various modules like Reputation System, Monitor, Path Manager and Trust Co-operation system. The main benefit of this scheme is that it increases functionality and performance of MANETs by the prevention, identification, and mitigation of DDoS attacks.

Arunmozhi and Venkataramani [7] suggested a defense system in which each device maintains a flow monitoring table. The main benefit in this method is that it increases network efficiency, packet delivery ratio, and bandwidth. It further also reduces the ratio of legitimate packet drops. Jin et al. [8] suggested a new zone sampling based traceback algorithm that can be used to traceback DoS attackers in MANET. The idea behind this technique is to divide the network into different zones. Every zone places its own ID to the every packet that passes through it. Whenever a mobile node wants to forward a received packet to every other node, firstly it will require placing its own ID on the packet and then forwards it to every other node with probability (P). By looking into the zone ID, it becomes easy to know whether a node is suffered with a denial of service attack or not. Later the target node can examine these packets to traceback the complete path used by the attacker [9]. Singh et al. [10] suggested a thresholds and entropy based DDoS attack detection scheme that detects the presence of DDoS attack on the edge routers of stub networks. The detection mechanism was implemented in the form of agents that monitors the incoming traffic with the help of detection algorithms. The detection successfully detects DDoS attacks with fewer false positives and false negatives.

III. FLOW BASED DDOS ATTACK DETECTION

The concept of entropy is identified by Shannon in 1948 [11]. Entropy is an information theoretic concept that can be used to measure the uncertainty of a random variable or randomness in flows [12]. The value of entropy lies between 0 and 1. The feature of entropy can be used for the monitoring of network. If the network changes from normal to suspicious mode (e.q. the case of DDoS attack) the value of entropy will get decreased. This phenomenon can be applied to various filed of IP packets like sender node address, receiver node address, receiver port, sender port, total no of packets etc. The proposed attack detection mechanism is also based on Shannon entropy and threshold values to identify the presence of attack from the incoming flows. The concept of shannon entropy is used to calculate the entropy of cluster head. The values of normalized entropy and packet can be calculated as:

Normalized entropy: The normalized entropy for a specific time window (Δt) of the cluster head node can be calculated as:

$$NeCH = \frac{\sum_{1}^{n}(-P(xi)\times Log_2 P(xi))}{Log_2 N} \quad \text{.....(1)}$$

Where P(xi) – Probability of packets belonging to flow(xi)
N – Total number of flows

Packet rate: The value of packet rate at a particular time can be calculated as:

$$Pr = \frac{Total\ packets\ belonging\ to\ flow\ (xi)}{N} \quad \text{.....(2)}$$

Where N = Total number of flows

The purpose of proposed attack detection algorithm is to distinguish between attack and legitimate traffic during the DDoS attacks by the cluster head. The different threshold values (Te = 0.90 and Tpr = 100) used in the detection algorithm are calculated offline on sample traffic in the presence and absence of attacks. Some assumptions like threshold values, clustered based MANETs are taken for the proposed algorithm.

Volume: 10 Issue: 04 Pages: 3905-3910 (2019) ISSN: 0975-0290

Algorithm: 1 (Proposed attack detection algorithm)

Parameters Initializations

Step 1: Assign value to various parameters like sampling time (t), time window (Δt) and various thresholds (Ten, Tpr)

Characterization of Incoming Flows

Step 2: Collect incoming traffic after every Δt on cluster head (CH)

Step 3: Construct flows from the incoming traffic for every Δt second

$F_1,F_2,F_3….F_n$	$F_1,F_2,F_3….F_n$	……	$F_1,F_2,F_3….F_n$
Δt_1	Δt_2	…….	Δt_n

Step 4: For each flow, compute normalized entropy (using eq 1) at cluster head

Identification of suspicious flow

Step 5: Compare normalized entropy (N_eCH) with threshold (Ten)

Step 6: If (N_eCH < Ten), Then treat the flows as suspected flow,
Else if (N_eCH >=Ten) then treat the flows as Legitimate flow

Step 7: For each suspected flow, calculate packet rate (Pr) (using eq 2)

Step 8: If packet rate (Pr) < Tpr then consider the flow as legitimate flow
Else consider the flow as suspected flow.

Confirmation of DDoS attack

Step 9: Identify cluster and destination information from the suspected flow (C,D)

Step 10: Pass cluster and destination information (C, D) and ask neighbouring cluster head to compute packet rate for all the flows heading towards destination D.

Step 11: At neighbouring cluster head, for each flow (i), check if destination=D,
then compute packet rate Pr(i),
Else neglect the packet.

Step 12: Send Pr(i) to the asking cluster head

Step 13: For each value of Pr(i), compare the value of Pr(i) against Tpr,
If Pr(i) < Tpr then consider the flow as legitimate flow,
Else consider the flow as attack flow (DDoS attack)

Attack Traffic Filtering

Step 14: Mark destination D as under DDoS attack and share this information with neighbouring cluster heads

Step 15: Drop all the packets related to the attack flow

The monitoring of incoming traffic is done by the cluster heads by implementing above mentioned algorithm 1 in each cluster. The main purpose cluster heads is to detect the presence of DDoS attack as early as possible so that it can be avoided to reach the victim. The cluster heads of neighbouring clusters will participate in the detection of DDoS attack and will collaboratively fight against DDoS attack in distributed manner.

IV. EXPERIMENTATION

To evaluate the efficiency of proposed attack detection technique, a testbed containing some attack and legitimate nodes in clustered form is constructed using OMNeT++ ver. 4.6 [13] simulation tool. OMNET++ is a widely accepted simulation tool for conducting research in MANET. The simulation is conducted by taking 1000m x 1000m area with a total of 150 numbers of nodes. The transmission range used for mobile nodes can vary from 50m to 250m. The group model of nodes mobility is used to perform the simulation. Table 1 below depicts the various simulation parameters to be used in the testbed.

Table 1: Parameters

Parameter	Value
Total devices	150
Area of simulation (m2)	1000 * 1000
Mobility model	Group Mobility
Routing protocol	AODV
Packet Size	64 bytes
Number of nodes	100
Legitimate nodes	60
Attack nodes	90
Traffic type	CBR (constant bit rate)
Queue	Drop tail (50)
Transmission range	50m to 250m
Time window	2 Sec
Simulation time	20 Sec

The attack started at time t=8th seconds and remains active till t= 16th second. The whole simulation will last for 20 seconds. Legitimate nodes randomly send packet at the normal rate (10-15 pkts/sec) during the start of simulation

Volume: 10 Issue: 04 Pages: 3905-3910 (2019) ISSN: 0975-0290

(i.e. 0 to 1 seconds) whereas the attack nodes are configured to send traffic at a higher rate (100-110 pkts/sec) during the attack duration (8th to 16th second). The results of the simulation are collected in the form scalar and vector values which can be later analysed with data of interest.

V. PERFORMANCE ANALYSIS

The performance of various QoS parameters [14, 15] is evaluated by conducting various experiments in the absence and presence of attack detection system. The efficiency of attack detection system depends on how accurately it detects attacks during attack detection. The threshold value performs an important role in the accurate detection of DDoS attacks. The effect of effect of defense system on the performance of legitimate and attack traffic is discussed here.

5.1 Throughput

Throughput is the number of packet delivered to a destination node in a unit of time. It is used to test the efficiency of MANETs in the presence and absence of attacks. It can be evaluated by measuring the number of packets (or number of bits per seconds) successfully delivered to the specific destination. Here the throughput can be evaluated by measuring the no. of packets successfully delivered at the destination in following three cases.

1. In the absence of attack flow and detection system,
2. In the presence of attack flow but without detection system, and
3. In the presence of both attack flow and detection system.

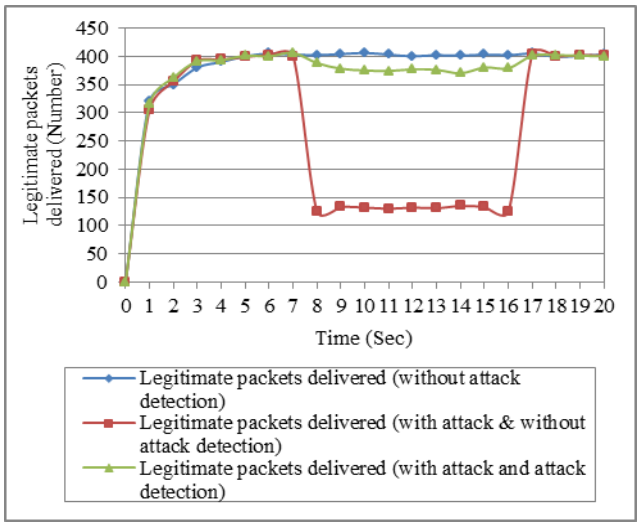

Fig.1: Throughput variants

Fig.1 above shows that the ratio of legitimate packets transported to destination under different conditions. In the absence of attack and defense mechanism, almost all the packets are delivered to the destination. When attack happens (i.e. from 8th to 16th second) and there is no defense, the legitimate packet delivered ratio will get decreased considerably. Later the test is performed in the presence of both attack and defense mechanism and found that the ratio of legitimate packets delivered will get increased as defense mechanism block attack packets and legitimate packets will get more bandwidth to reach the destination.

5.2 PDR (Packet Delivery Ratio)

PDR can be used to measure the ratio of legitimate packet received by the destination. It can be computed by dividing the total no. of legitimate packets successfully delivered at receiver with no. of packets sent from sender. The effect of defense mechanism on the value of PDR can be measured in the absence and presence of DDoS attacks. It can be measured as:

$$PDR = \frac{Total\ no.\ of\ legitimate\ packets\ delivered}{Total\ no.\ of\ packets\ sent}$$

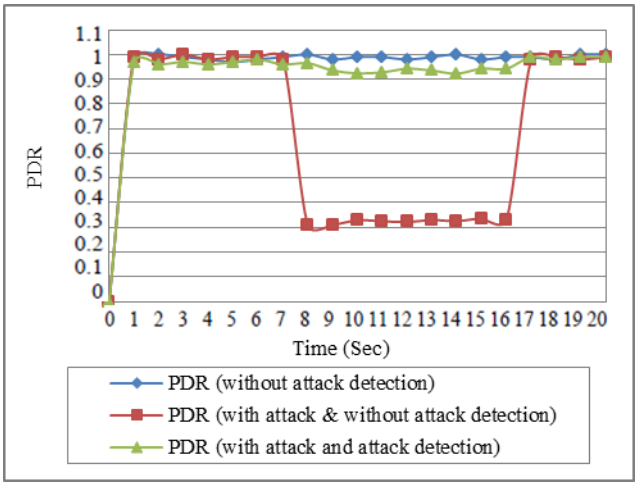

Fig 2: Variations in PDR value

Fig. 2 above shows the value of PDR in the presence and absence of defense mechanism with attack traffic. In the absence of attack the packet delivery ratio is almost 1, because packets will get full bandwidth to reach target. The value of PDR will get decreased when attack happens during (8th to 16th seconds) as their no defense mechanism but when it tested in the presence of defense mechanism, the PDR will get increased because more legitimate packets will be delivered to the destination.

5.3 End to End (EtoE) Delay

The amount of time a packet takes to travel from sender device to receiver device is known as end to end delay. When there is no attack, then the value of delay will be very low but when attack happens, it will get increased. From network point of view, its value should be minimum.

Volume: 10 Issue: 04 Pages: 3905-3910 (2019) ISSN: 0975-0290

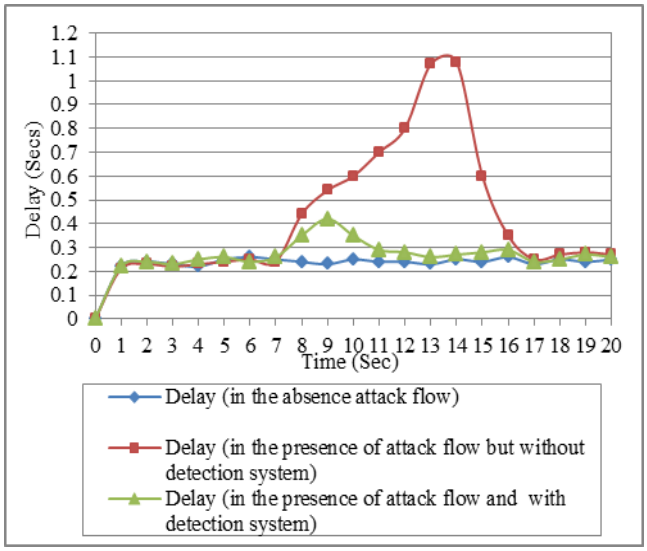

Fig.3: Variation in EtoE delay value

The variations in end to end delay under different situations are shown by Fig. 3 above. In absence of attack the value of delay remains low (i.e. nearly 0.2 sec), but it will get increased and can even touch to 1 second when attack is launched. The presence of defense algorithm will control the delay time during attack duration and keep it as minimum as possible.

VI. CONCLUSIONS

A DDoS defense system is considered good if it does accurate attack detection during traffic monitoring. The attack detection algorithm proposed here identify the presence of DDoS attack by monitoring incoming traffic by the cluster heads in cluster based MANETs. The normalized entropy of flow is computed and compared against a predefined threshold to identify the presence of suspicious behaviour. Packet rate of each flow is compared against another threshold to identify the suspicious flow. Later with the help of neighbouring cluster heads it can be confirmed whether the suspicious flow is creating dodos attack or not. The testing of proposed attack detection algorithm is done by conducting simulations using OMNeT++. The performance of genuine traffic is evaluated in the presence and absence of defense mechanism. The results of various performance metrics shows that the proposed algorithm does the job with more efficiency.

REFERENCES

[1] S. Corson and J. Macker, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, RFC 2501, 1999. Available at https://www.ietf.org/rfc/rfc2501.txt.

[2] J. Mirkovic, G. Prier, and P. Reiher, Attacking DDoS at the source, *Proc. of ICNP 2002*, Paris, France, 2002, 312-321.

[3] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govindan. Cossack: Coordinated suppression of simultaneous attacks. *Proc. DARPA Information Survivability Conference and Exposition*, Washington, DC, USA, 2003, 94-96.

[4] W. Ren, D.Y Yeung, H. Jin, M. Yang, Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks, *International Journal of Network Security*, 4(2), 2007, 227-234.

[5] P. Yi, Z. Dai, S. Zhang, Y. Zhong, A New Routing Attack in Mobile Ad Hoc Networks, *International Journal of Information Technology*, 11(2), 2005, 83-94.

[6] R. Khan, A.K. Vatsa, Detection and Control of DDoS Attacks over Reputation and Score Based MANET, *Journal of Emerging Trends in Computing and Information Sciences*, 2(11), 2011, 646-655.

[7] S.A. Arunmozhi, Y. Venkataramani, DDoS Attack and Defense Scheme in Wireless Ad hoc Networks, *International Journal of Network Security & Its Applications*, 3(3), 2011, 182-187.

[8] X. Jin, Y. Zhang, Y. Pan, Y. Zhou, ZSBT: A novel algorithm for tracing DoS attackers in MANETs. *EURASIP Journal on Wireless Communications and Networking*, 2006, 2006:096157, 1-9.

[9] I. Kim and K. Kim, A resource-efficient IP traceback technique for mobile ad-hoc networks based on time-tagged bloom filter, *Proc. of Third International Conference on Convergence and Hybrid Information Technology*, 2008, 2, 549- 554.

[10] K. Singh, K. Dhindsa, and B. Bhushan, Threshold-Based Distributed DDoS Attack Detection Mechanism in ISP Networks, *Turkish Journal of Electrical Engineering & Computer Sciences*, 26(4), 2018, 1796-1811.

[11] C.E. Shannon, A Mathematical Theory of Communication, *Bell System Technical Journal*, 27, 1948, 379-423 & 623-656.

[12] T.M. Cover, and J.A. Thomas, *Elements of Information Theory*, Second Edition, John Wiley & Sons, 2006.

[13] A. Varga, The OMNeT++ Discrete Event Simulation System, *Proceedings of the European Simulation Multi-conference*, Prague, Czech Republic, 2001.

[14] M. G, and K. TNR, Packet Transfer Rate & Robust Throughput for Mobile Adhoc Network, Int. J. Advanced Networking and Applications, 8(6), 2017, 3242-3245.

Volume: 10 Issue: 04 Pages: 3905-3910 (2019) ISSN: 0975-0290

[15] A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq, and T. Saba, Energy Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function, IEEE Access, 5, 2017, 10369-10381.

Author Profiles:

Deepa, is doing her Ph.D. in the field of Network Security from IKG Punjab Technical University, Kapurthala (Punjab). She obtained his MCA degree from Kurukshetra University, Kurukshetra (Haryana), India. She has a teaching and research experience of more than 12 years. She has authored more than 8 papers in various international journals & the proceedings of reputed national and international conferences. Her research interests are in the fields of Computer Networks, Network Security, and Adhoc Networks.

Dr. Kanwalvir Singh Dhindsa, is working as Professor in the Department of CSE at Baba Banda Singh Bahadur Engg. College, Fatehgarh Sahib (Punjab). He obtained his Ph.D. in Computer Engg. (In the field of Mobile Computing & Information Systems) from Punjabi University Patiala. He has guided many M.Tech. students & is currently guiding 7 Ph.D. scholars. He has authored more than 90 publications in various esteemed international referred journals & proceedings of reputed national and international conferences. His research interests are in the fields of Cloud Computing, Big Data, IoT, Mobile Computing, Database & Security, and Web Engineering.

Dr. Bharat Bhushan is employed as Head and Associate Professor in the Department of Computer Science & Applications, Guru Nanak Khalsa College, Yamunanagar (Haryana). He has done Ph.D. in Computer Science & Applications from Kurukshetra University, Kurukshetra, India. He has more than 70 research papers to his credit in various referred international journals and reputed international conferences. His research interests are in the fields of Software Quality and Mobile Networks.