IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

Performance Based Evaluation of Botnet, Black hole, Wormhole Attack in MANET

M. Lalli[1*], G. Karuthammal[2]

[1,2]School of Computer Science and Engineering, Bharathidasan University, Tiruchirappalli, India

[*]*Corresponding Author:* lalli_gss@yahoo.co.in , *mobile.:9445285069*

Available online at: www.ijcseonline.org

Accepted: 14/Aug/2018, Published: 31/Aug/2018

***Abstract*—** Denial-Of-Service (DOS) is one of the foremost dangerous attacks. It's a sort of meter attack. This framework is to judge the network's performance under these attacks with numerous network parameters. IAFV is used to browse the characteristics of the network supported time delay output and packet delivery quantitative relation. The objective of the planned technique is to check the performance metrics underneath completely different attacks. Varied relevant parameters as well as output time delay and packet delivery quantitative relation square measure evaluated. The planned technique deploys exclusive nodes known as DPS nodes employed in the network to watch the behavior of the nodes endlessly. Once the DPS hub distinguishes a hub with relate strange conduct it will report that hub as a wormhole hub to the system by communicating a message. Every single open message will be surrendered by the system from the wormhole hub. A bundle drop assault or dark opening assault might be a style of dissent of-benefit assault inside which a switch that estimated to transfer parcels rather disposes of them. This ordinarily occurs from a switch changing into traded off from assortment of different causes. The planned strategies measures are enforced using NS2 machine and also the results are mentioned.

***Keywords*—** Botnet, DDoS, Wormhole, IFAV, Attacks.

I. INTRODUCTION

MOBILE ADHOC NETWORKS

A portable unforeseen system (MANET), also called remote specially appointed system or impromptu remote system is a persistently self-designing, foundation less system of cell phones associated remotely. Every gadget in a MANET will move uninhibitedly and freely toward any path and will change it to connect with different gadgets often. Each device must forward traffic unrelated to its own use and must be a router. The essential test in building a MANET is preparing every gadget to persistently keep up the data required for legitimate course traffic.Such systems may work without anyone else's input or might be associated with the web. They may contain one or various and distinctive handsets between hubs.This results in a highly dynamic, autonomous topology. MANETs are a sort of remote specially appointed system (WANET) that as a rule has a routable systems administration condition over a connection layer impromptu system.MANETs consist of a peer-to-peer, self-forming and self-healing network. Distinctive conventions are assessed in light of measures, for example, the bundle drop rate, the overhead presented by the directing convention, end-to-end parcel delays, arrange throughput and adaptability.Versatile specially appointed systems can be utilized as a part of numerous applications. They are: sensors for condition, vehicular specially appointed correspondences, street security, wellbeing, home, shared informing, fiasco safeguard tasks, protection, weapons and robots.MANETS can be utilized for encouraging the accumulation of sensor information for information digging for an assortment of utilizations, for example, air contamination checking and distinctive kinds of models can be utilized for such applications. It ought to be noticed that a key normal for such applications is that close-by sensor hubs checking an ecological component commonly enroll comparable qualities. This sort of information excess because of the spatial connection between's sensor perceptions rouses the systems for in-arrange information collection and mining. By estimating the spatial connection between's information inspected by various sensors, a wide class of particular calculations can be produced to grow more proficient spatial information mining calculations and also more effective directing systems.

In MANETs, each node works as a router and can communicate with other nodes directly or indirectly with the help of its neighbors. MANETs can be deployed in disaster areas to collect critical information, in battlefield to communicate among soldiers and in hazardous areas in the form of sensor networks. Due to the lack of a central point of

control, it is more likely that malicious nodes join the network and launch various types of attacks. An attack can be launched by a single node or multiple nodes in a cooperative manner. The attacker node can be external or internal. The internal attackers are more dangerous and are difficult to detect than external attackers. In some attacks, multiple attackers synchronize their actions to disrupt a target network.

These types of attacks are called Collaborative Attacks (CA). Out of many such attacks, wormhole attack is one of the most severe security threats in wireless ad hoc networks. Detection and prevention of wormhole attack is a very challenging issue.

The wormhole assault is conceivable regardless of whether the assailant has not traded off any hosts and all the correspondence gives genuineness and secrecy.. It is a serious threat for routing protocols such as Ad hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR). Generally, this attack is launched by two or more malicious nodes having a private channel called tunnel between them. A malicious node at one end of the tunnel captures the control packet and sends it to the other malicious node through the tunnel; the second malicious node rebroadcasts the packet locally. The route through the tunnel is selected based on having better metrics (e.g. less time or less number of hops as compared to the other routes) for communication between the source and the destination. If the time interval is longer than normal, the packet is dropped. During the past few years, several authors have proposed solutions to overcome the problem of wormhole attack. Most of the solutions are based on time interval between sending and receiving packets.

The rest of the paper is organized as follows:

Section 2 explains the related work for the proposed system. Section 3 is the proposed method of how the attacks are detected. Section 4 discusses the performance of the ad hoc network under various attacks. Section 5 is the concluding remarks.

II. RELATED WORK

Parmar et al, proposed and implemented a wormhole detection and prevention mechanism to detect and prevent the wormhole attacks. In our technique, no special hardware is required. All we have done is calculated the Round Trip Time (RTT) of every route to calculate threshold RTT. According to simulation results of various parameters like Average end to end delay, Packet delivery fraction and Average throughput it is proved that proposed mechanism performs better than wormhole affected AOMDV[1].

Arathy et al., proposed two algorithms for the detection of single and collaborative black hole attacks. The proposed D-MBH calculation utilizes a phony RREQ with nonexistent target address and processes a limit for DSN and makes a rundown of dark gap hubs. Utilizing the limit, rundown of dark opening hubs and next jump data separated from RREP, the proposed D-CBH calculation makes a rundown of community oriented dark gap hubs. We have broke down the proposed calculations with the current DRI, constancy and trust based plans and found that the directing overhead and computational overhead has been extensively diminished [2].

Tariq et al., proposed an efficient for step technique that confirms that this attack can be detected and defended with least efforts and resource consumption. The technique will boost the reliability by presciently initiating a cooperative scheme that involves neighboring nodes of malicious node. Suspect and detection decision are done with the help of consensus algorithm that is based on thresh hold cryptography. The proposed mechanism is efficient and effective with controlled overhead and great detection rate [3].

Rajesh et al., proposes a strategy which is known as NHBADI, which utilizes Honeypot procedure to recognize and separate Black Hole assaults. Unlike existing techniques, the proposed Honeypot technique enhances the security of the MANET by reducing the network overhead. To measure the effectiveness of the proposed system, NS-2 simulator is used. The proposed method recognizes malevolent Black Hole hubs as well as disengages the powerless Black Hole hubs from the system. The proposed NHBADI scheme reduces network overhead, normalized routing load and packet drop ratio [4].

Aaditya et al., analyzes the effect of many attacks under CBR traffic in different scenarios for DSR MANET routing protocol. In view of examinations and information investigation of reproduction comes about, it is presumed that without the nearness of any steering assault DSR perform well in gently stacked systems. In any case, the nearness of black hole, gray hole, and surging assault at the season of directing impacts on by and large execution of DSR convention by diminishing parcel conveyance proportion and normal throughput yet by expanding normal end to end delay [5].

III. METHODOLOGY

Presented a unique model for the DDoS class of assaults, where the botnet imitates ordinary movement by constantly taking in acceptable examples from the earth. Devised an inference algorithm that is shown to provide a consistent (i.e., converging to the true solution as time elapses) estimate of the botnet possibly hidden in the network. The validity of the proposed inferential strategy on a test bed environment was verified. Tests results shows that for several scenarios of implementation, the proposed botnet identification algorithm needs an observation time in the order of less than one minute to identify correctly almost all bots, without affecting the normal users' activity. Implemented a hybrid algorithm for botnet identification to analyze the network performance at the time of attack. Utilized IAFV time arrangement to

portray the state change highlights of system stream. Detecting the DDoS attack is equivalent to classifying the IAFV time series virtually. Large number of relevant parameters including throughput, time delay and packet delivery ratio are used to test the proposed algorithm.

In the below figure, the architecture for botnet attack is explained. The nodes will form a network. Then, single hop and multi hop communication is done to confirm data communication among nodes. The nodes will send RREQ and RREP to other nodes in the network. But, the botnet nodes will send request only to the server. The server will monitor this to a specified time. After some time, the server will intimate the remaining nodes about the botnet nodes. The novel nodes will communicate among themselves without communicating the botnet nodes.

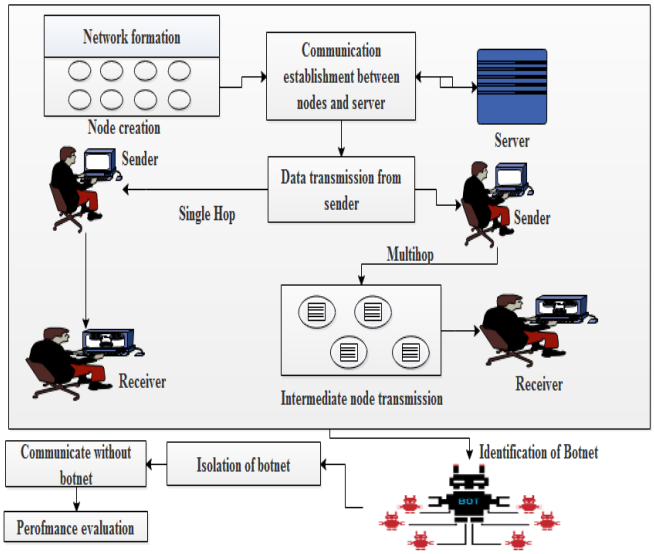

Figure 1: Botnet Attack Architecture diagram

Definition of IP Address Feature Value and Algorithm

The assault streams of DDoS have a few highlights like the sudden movement change, stream dissymmetry, conveyed source IP addresses and thought target IP addresses, and so on. In this paper, we propose the concept of IAFV (IP Address Feature Value) to reflect the four features of DDoS attack flow.

The network flow F in the certain time span T is given in the form of < (t1, S1, D1), (t2, S2, D2)… (tn, Sn, Dn)>. For the ith packet p, ti is the time, Si is the source IP address and Di is the destination IP address. Classify all the packets by source IP and destination IP, which mean all packets in a certain class share the same source IP address and destination IP address. A class which is consisted of packets with a source IP Ai and a destination IP Aj is noted as SD (Ai, Aj). Carry out the following rules to the above mentioned classes: If there are two different destination IP address Aj, Ak, which makes class SD(Ai, Aj) and class SD(Ai, Ak) both nonempty, then remove all the class with a source IP address of Ai. If there is only one class SD (Ai, Aj) containing the packets with a destination IP address Aj, then remove all the classes with a destination IP address Aj. Assume that the remaining classes are SDS1, SDS2… SDSl, classify these classes by destination IP address, that is all the packets with the same destination IP address will be in the same class. The class made up of packets of the same destination IP address Aj is noted as SDD (Aj), these classes is SDD1, SDD2… SDDm, the IAFV (IP Address Features Value) is defined as:

$$IAFV_F = \left(\sum_{i=1}^{m} SIP(SDDi) - m\right) \quad \_1$$

in which SIP(SDDi) is the number of different source IP addresses in the class SDDi. In order to analyze the state features of the network flow F more efficiently and exclude the disturbance of a normal flow, the definition of IAFV classify the packets of F by source IP address and destination IP address. A DDoS attack is usually composed of several attack sources rather than a single one with the true source IP address, so the class with packets from the same source IP address Ai to different destinations belongs to a normal flow, thus the classes with a source IP address Ai can be removed. After that, if there is a destination address Ak makes Ai and Aj in SD(Ai, Ak) and SD(Aj, Ak) the same, then the destination IP address Ak is not visited by multiple sources, which implies a normal flow, thus the class with packets going to the destination Ak can be removed. The above mentioned two steps can reflect the asymmetry of a DDoS attack flow as well as a decrease in the disturbance of the normal flow. DDoS attack is a kind of attack that sends useless packets to the attack target from many different sources in the hope of exhausting the resources of the target. This act can produce lots of new source IP addresses in a short time, which will lead to an abnormal increase of SIP(SDDi) for some classes of F, that is, the number of different sources to different destination will increase abnormally, causes the flow to be in a quite different state in a short time. The definition of IAFV sums up the different source IP addresses of each SDDi of F in a certain period, then subtract the number of different destination IP addresses m, and divide m at last. So IAFV can reflect the characteristics of a DDoS attack including the burst in the traffic volume, asymmetry of the flow, distributed source IP addresses and a concentrated destination IP address.

The procedure of IAFV method is given below:

Input: an initial network flow data F, a sample interval Δt, a stopping criterion C, an arrival time of an IP Packet T, a source IP address S, a destination IP address D, an IP address class set SD, SDS and SDD, an IP address features IAFV.

Output: IAFV time series which characterize the essential change features of F.

1. Initialization-related variables;
2. **while** (criterion C is not satisfied){
3. Read the T, S and D of an IP packet from F;

4. **if** (T is not over the sample interval Δt){
5. flag= New_SD(S, D,SD);
// Judge whether (S, D) is a new element of SD
6. Add_SD (flag, S, D, SD);
// add a new element (S, D) to SD
}
7. **if** (the arrival time of IP Packet exceeds the sample interval Δt){
8. remove_SD (SD);
// remove all (S, D) with same S and different D from SD.
9. Add_SDS (SD, SDS);
//add all (S, D) of SD with different S and same D to SDS.
10. classify_SDS (SDS, SDD);
// classify SDS by D and then add all (S, D) of SDS to SDD.
11. m=Size (SDD);
//count the number of the elements in SDD.
12. $IAFV_F$ = ($\sum_i^!$
//calculate IAFV of SDD
13. **return** IAFV;
}
}

Detection Method Based on IAFV

To raise the detection rate, decrease the false alarm rate, and enhance the adaptability of detection method, we propose a simple but robust scheme to detect DDoS attacks by extracting IAFV time series from normal flow and DDoS attack flow respectively, and use the SVM (Support Vector Machine) classifier to detect DDoS attacks. By sampling the network flow data F with sampling interval Δt, and calculating the IAFV of every sample, we can get the IAFV time series sample set A after sampling N times, A(N,Δt)={IAFVi,i=1,2,…,N}, N is the length of the time series. Subsequent to Using IAFV time arrangement to portray the state change highlights of system stream, distinguishing DDoS assault is equal to ordering IAFV time arrangement for all intents and purposes. SVM classifier can get the optimal solution base on the existing information under the condition that the sample size tends to be infinite or be limited. It can establish a mapping of a non-linear separable data sample in higher dimensional characteristic space by selecting the non-linear mapping function (kernel function), construct the optimal hyper plane, and transform a non-linear separable data sample into a linear separable data sample in the higher dimensional characteristic space. Furthermore, it can solve the problem of higher dimension, and its computational complexity is independent of the data sample dimension. Therefore we use the SVM classifier, which can be established by learning from the IAFV time series of the normal flow samples and DDoS attack flow samples, to classify the IAFV time series gotten by sampling network flows with sample interval ΔT, and identify DDoS attack. The SVM classifier is

$$\eta = \sum_{i=1}^{M} \beta i Yi K(\emptyset i, \emptyset) + b$$

_2

in which 'η' is the classification result for sample to be tested, 'βi' is the Lagrange multipliers, Yi is the type of classification, *Yi∈{-1,1}*, *K(ϕ□i,ϕ)* is the kernel function, b is the deviation factor, ϕi is the classification raining data sample, *i=1,2,…,M*,*ϕ*□is
the sample to be tested.

Anomaly Based Intrusion Detection and Prevention System

Proposed a Detection and Prevention System (DPS) to identify and square malevolent hubs in MANETs. Exceptional hubs called DPS hubs are sent in the system, which consistently screen the conduct of different hubs. At the point when a DPS hub finds a hub with a suspicious conduct, it announces that suspicious hub as a wormhole hub by communicating a message. All information and control messages are disposed of by the system from a hub that has been announced as wormhole. The quantity of DPS hubs relies on two variables: arrange region and transmission extend. To accomplish best outcomes, DPS hubs ought to be sent such that they cover the entire system region and speak with each other specifically. At whatever point a DPS hub gets a RREQ, course ask for checking begins. As every dp hub keeps record of its neighbours in the Analysis Table, at whatever point it gets a RREQ from a hub, it first checks whether the hub that is communicating the RREQ is as of now incorporated into its Analysis Table. In the event that it isn't found in the Analysis Table then another passage is made in which the status is set to dynamic, RREQ check is set to 1.

The Suspicious esteem is set to 0 and Wormhole affirmed fields are set to No. The Suspicious esteem count process checks every one of the hubs in the Analysis Table whose status is dynamic. On the off chance that there is a hub that has RREQ check not as much as Minimum Request Count then its Suspicious esteem is augmented by one. On the off chance that the suspicious esteem is equivalent to Minimum Threat Value and the Wormhole Threat field is No, at that point the DPS hub will communicate a danger message, which incorporates the ID of the vindictive hub. In the wake of sending the Threat message, the Wormhole Threat field of the noxious hub is set to Yes. At that point the procedure will proceed for different hubs. In the event that the suspicious estimation of a hub winds up equivalent to Maximum Threat Value and its Wormhole Confirmed field is No, at that point the DPS hub will communicate a Block message, which contains the ID of the malevolent hub. Subsequent to sending the Block message, the Wormhole Confirmed field is set to Yes. To decrease the false positive rate, if there is a hub that has Suspicious Value more than zero yet indicates typical conduct i.e. the RREQ advances are more than the Minimum

Request Count, at that point its Suspicious Value is decremented by one. This condition lessens the odds of genuine hubs being announced as wormhole hubs because of separation from the system. Toward the finish of the Suspicious Value estimation process, the status of the considerable number of hubs in the table is set to dormant and the RREQ Count is set to zero.

Black Hole Detection Algorithm

Actions by Source Node (SN)

Step 1: Source Node (SN) sends a Request to Restricted IP (RRIP) to the Back Bone Node(BBN).

Step 2: On getting the Restricted IP (RIP), from the BBN it sends the RREQ for the Destination and for the RIP at the same time.

Step 3: Awaits for RREP.

Actions by Intermediate Node/Destination Node

Step 1: On receiving the RREQ it first makes an entry in its Routing table for the node that forwarded the RREQ.

Step 2: If it is the Destination node or if it has a fresh enough route to the Destination node, it replies to the RREQ with an RREP.

Step 3: If it is nether the neither destination nor does it have a fresh enough route to the Destination, then it forwards the RREQ to its neighbours.

Step 4: On receiving an RREP, it again makes a note of the node that sent the RREQ in its routing table & then forwards the RREP in the reverse direction.

Table 1. Simulation Parameters

P1	Simulating Time	20ms
P2	Number of Nodes	30
P3	Area Size	300 * 300
P4	Packet Size	50
P5	Node Placement	Random
P6	Maximum no of malicious nodes	5
P7	Types of Attack	Black hole, Worm hole and Botnet Attack
P8	Movement Model	Static
P9	Radio propagation model	Two Ray Ground
P10	MAC Type	802.11
P11	X and Y Axes	967, 596

P1,P2,P3,P4,P5,P6,P7,P8,P9,P10,P11 various parameters

Step5: On receiving a request to enter into the promiscuous mode, it starts listening in the network for all the packets destined to that particular IP address & monitors its neighbours, for the movement of the dummy data packet.

Step6: In case, it finds out that the dummy data packet loss is exceptionally more than the normal data packet at any particular node, it informs back the IP of this IN.

IV. RESULTS AND DISCUSSION

4.1 Performance metrics

(i) Packet Loss: The total number of data packets lost legitimately or through malicious action without any notification.

Packet Loss = No of Loss Packets / No of Received Packets _3

(ii) Packet Delivery Ratio (PDR): The ratio of total number of data packets delivered to the total number of data packets sent.

PDR = Received Packets by the Destination / Generate Packets by the Source _4

(iii) Energy Consumption (EC): The average energy consumed by each node during the given simulation time and expressed in Joules (J).

EC = Current Energy Value – Initial Energy Value _5

(iv) Throughput: The amount of data packets within a specified amount of time.

Throughput=The Amount of Data Moved Successfully from Source to Destination / Unit Time Period _6

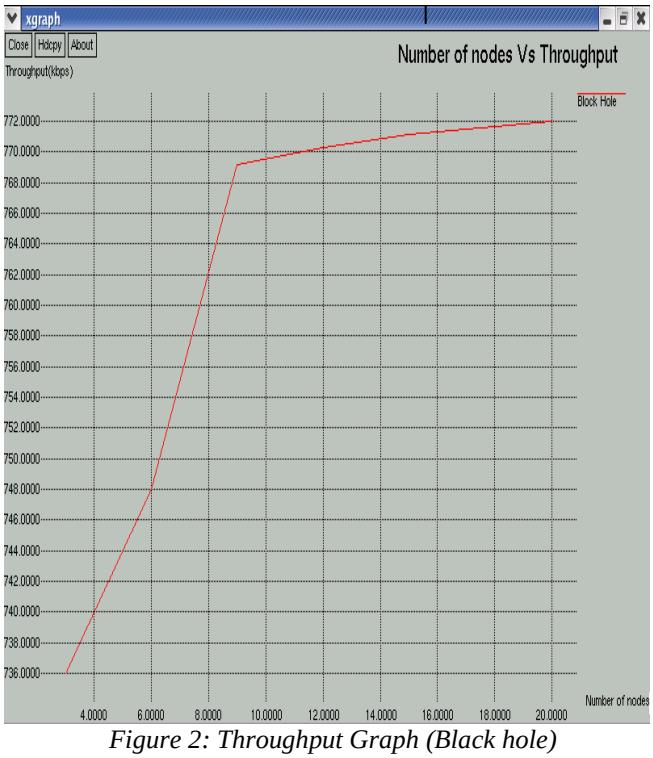

Figure 2: Throughput Graph (Black hole)

The figure 2 shows that the throughput of an ad hoc network when subjected to black hole attack. The X and Y axes are number of nodes and throughput respectively.

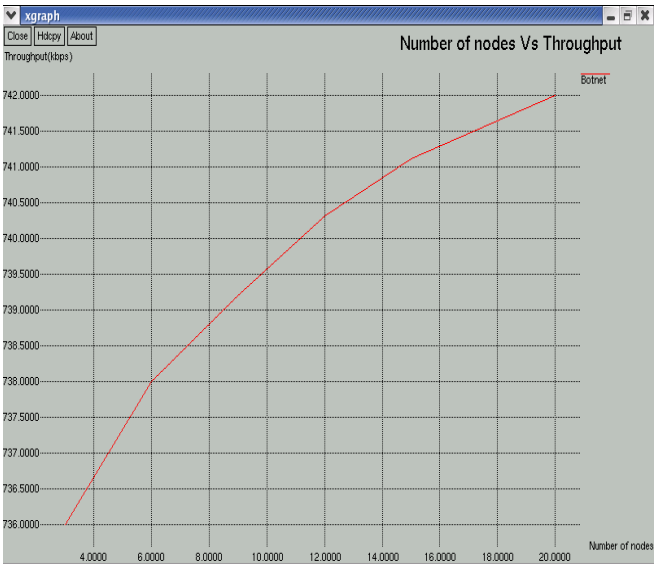

Figure 3: Throughput Graph (Botnet)

The figure 3 shows that the throughput of an ad hoc network when subjected to botnet attack. The X and Y axes are number of nodes and throughput respectively.

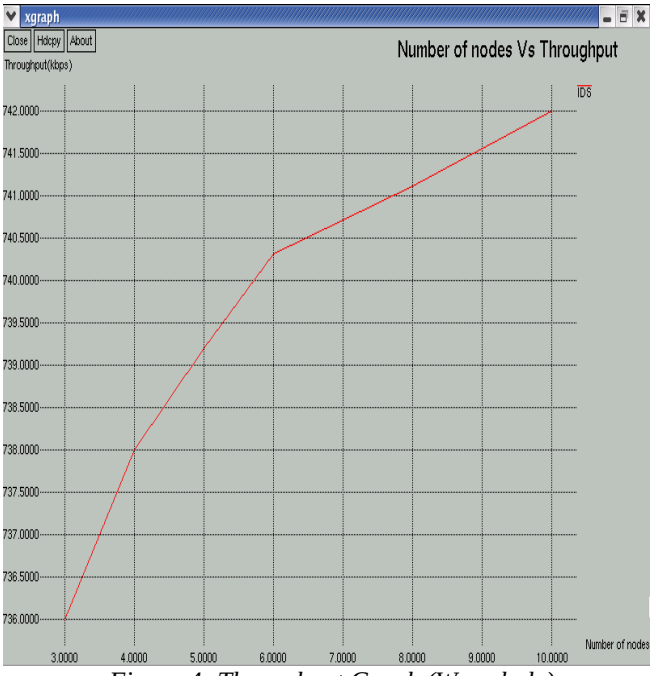

Figure 4: Throughput Graph (Wormhole)

The figure 4 shows that the throughput of an ad hoc network when subjected to wormhole attack. The X and Y axes are number of nodes and throughput respectively.

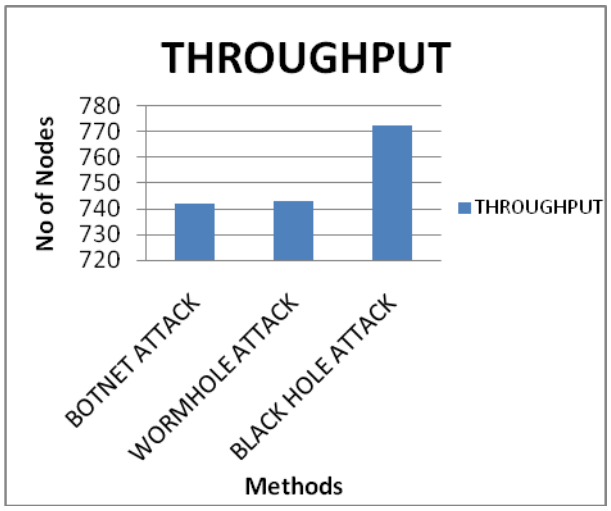

Figure 5: Throughput comparison of various attacks

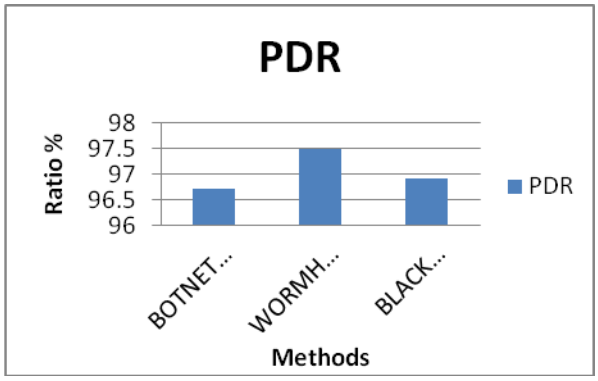

Figure 6: PDR comparison of various attacks

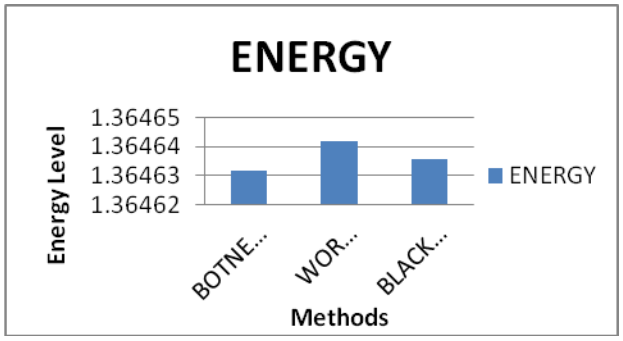

Figure 8: Delay comparison of various attacks

V. CONCLUSION

Distributed Denial of Service (DDoS) attacks launched by bots are capable to learn the application layer interaction possibilities, so as to avoid repeating one simple operation many times. The main contributions of this work are as follows: i) introduced a formal model for the class of randomized DDoS attacks with increasing emulation dictionary ii) proposed an inference algorithm aimed at identifying the botnets executing such advanced DDoS

attacks and ascertained the consistency of the algorithm, namely the property of revealing the true botnet as time elapses iii) evaluated the proposed methodologies on a testbed environment. A detection and prevention system (DPS) against wormhole attacks in Mobile Ad hoc Networks (MANETs) is presented here. The proposed DPS provides the following benefits: i) the normal nodes are not affected i.e. there is no extra processing required for the detection of malicious nodes and no extra delay is added. ii) The threat that a compromised node spreads false information of declaring a normal node as wormhole is minimized. iii) The DPS nodes do not take part in normal data transfer so their batteries live for longer durations In a dark gap directing assault, a malignant (aggressor) hub sends counterfeit steering data to alternate hubs, guaranteeing that it has an ideal course to goal and makes other great hubs course information parcels through the vindictive one. In DSDV, the aggressor can send a phony RREP (counting a phony goal grouping number that is created to be equivalent or higher than the one contained in the RREQ) to the source hub, vindictive hub guaranteeing that it has an adequately crisp course to the goal hub. This makes the source hub select a course that goes through the (malignant) aggressor, all movement will be steered through the assailant, and along these lines, aggressor hub can abuse or dispose of the activity, in MANETs.

REFERENCES

[1] Parmar Amisha ,V.B.Vaghelab,"Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol", In proceedings of the 2016 International Conference on Communication, Computing and Virtualization, India , pp: 700 – 707,2016.

[2] Arathy K Sa, Sminesh C Na,"Black Hole Attacks in MANET", A Novel Approach for Detection of Single and Collaborative, Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST 2016), pp: 264 – 271, 2016.

[3] Tariq Ahamad, "Detection and Defense Against Packet Drop Attack in MANET", International Journal of Advanced Computer Science and Applications, (IJACSA), Vol. 7, No. 2, pp: 328 – 331, 2016.

[4]. M. Rajesh Babu, G. Usha, "A Novel Honeypot Based Detection and Isolation Approach (NHBADI) To Detect and Isolate Black Hole Attacks in MANET", Wireless Personal Communications , pp: 1 – 15, Feb 2016.

[5] Aaditya Jain,"Performance Analysis of DSR Routing Protocol With and Without the Presence of Various Attacks in MANET", International Journal of Engineering Research and General Science Volume 4, Issue 1, pp: 454 – 461, 2016.

Authors Profile

M. Lallii completed her Ph.D in computer science Alagappa University,Karaikudi in the year of 2018.Currently She is working as a Assistant Professor in the Department of Computer Science Engineering and Applications,Bharathidasan University,Trichy,Tamilnadu, India, She has published research papers jointly around 20 papers at International journals and International conferences.She has 18 years of experience in teaching. Her area of interest is MANETs, information security and computer networks.

G.karuthammal is currently research scholar pursuring M.phil. in Computer Science from Bharathidasan University, Tiruchirappalli, India and done her B.Sc.in computer science and M.Sc in computer science from BharathisanUniversity. Tiruchirappalli, in the year of 2017, her area of interest is Networking.s

