JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

Distributed Denial of Service Attack Detection Techniques for Mobile Ad Hoc Networks

A. Chaudhary[1]*, G. Shrimal[2], R. Rautela[3]

[1]Information Technology Department, Manipal University Jaipur, Jaipur, India
[2,3]Computer Science & Engineering Department, JaganNath University Jaipur, Jaipur, India

[*]*Corresponding Author: alka.chaudhary0207@gmail.com*

Available online at: www.ijcseonline.org

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

Abstract Nowadays, Mobile ad hoc networks are very attractive in terms of its flexibility because there is no need of predefined infrastructure for communication such as wired network. This flexibility makes mobile ad hoc network more vulnerable to threats. Threats compromise with the attributes of security so reason being threats can be decreased the survivability or performance of the mobile ad hoc networks. Several types of attacks in MANETs have been reviewed in the literature, the most popular attack is Distributed Denial of Services Attack (DDoS) because the aim of DDoS is to restrict the MANETs to provide the normal services to their intended users by consuming bandwidth or overload the resources. This paper focuses on the several detection techniques of DDoS attack and proposed a new technique based on genetic algorithm for the detection of DDoS attack on MANETs.

Keywords— Mobile Ad hoc Networks (MANETs), DDoS, Intrusion Detection System (IDS), Detection Techniques.

I. INTRODUCTION

There are some groups such as IETF (Internet Engineering Task Force), those who work together for enhancing the functionality of mobile ad hoc networks. IETF constituted the mobile ad hoc network working group in 1997 [1]. The aim of this working group is to develop standard routing protocol for MANETs and they developed reactive and proactive routing protocols for MANETs. There is another working group which established by IETF known as Ad Hoc Networks Autoconfiguration [2], the aim of this group is to consider the issues in addressing model for ad hoc networks. Basically wireless networking used IEEE 802.11 architecture which is described in [3]. The infrastructure based networks use the Basic Service Set (BSS) for communication between all the stations in the network with the help of access point (AP) but infrastructure less networks or ad hoc networks use the IEEE 802.11 independent base service set (IBSS).

In IBSS, there is no requirement of access points and nodes communicate in a distributed peer to peer fashion. Unlike conventional networks, mobile ad hoc network do not have any pre-existing infrastructure or administrative point. MANETs facilitate mobile nodes can freely communicate to each other without the need of predefined infrastructure. This effectiveness and flexibility makes these types of networks attractive for many applications such as military operations, rescue operations, neighbourhood area networks, education applications and virtual conferences. During the communication under routing protocols, mobile nodes cooperate to each other for sending data packets from source to destination that's why MANETs support the multihop communication between the nodes or two nodes can communicate or send data packets directly to each other when they come within the radio range to each others. The dynamic nature of MANETs make it more vulnerable than the conventional networks because it support the some attacks of wired networks such as denial of service, eavesdropping and spoofing [4].

Some features of MANETs such as communication via wireless links, resource constraints (bandwidth and battery power), cooperativeness between the nodes and dynamic topology make it more susceptible to attacks. For the security of MANETs, we must be able to identify these attacks and take appropriate action to against them. There are five attributes of security to protect any network such as confidentiality, Authentication, Integrity, Non- repudiation, Availability [5].

Intrusion prevention based techniques such as authentication and encryption are no longer feasible for ad hoc networks so that Intrusion detection system (IDS) is known as the second line of defense for mobile ad hoc networks. When any set of actions make an effort to compromise with the security properties such as confidentiality, integrity, availability of resources and repudiation then these actions are called intrusions and detection of such intrusions are known as intrusion detection system [5]. Intrusion detection system continuously monitors the behavior of the system for detecting any suspicious activity. If it is presented in the system than IDS initiate a proper alarm (e.g. email the Systems Administrator, start an automatic retaliation, etc.)[6].

Other sections of this paper are organized as follows: In section II, explains the proposed detection techniques for DDoS attack in literature. In section III, describes our proposed method for detection of DDoS attack which is based on genetic algorithm and finally, In Section IV, concludes the paper.

II. PROPOSED DDOS DETECTION TECHNIQUES IN MANETS

Since, DDoS attack is very prominent attack in MANETs so that due to this reason many authors have been presented many DDoS detection techniques for MANETs. In this section, we are going to describe each technique which has been proposed in Literature.

A. Yassir et al. [7] proposed a new scheme of DDOS using Intrusion Detection System in wireless mobile ad hoc network. Most important objective is observing the result of DDOS packet drop. They developed safe IDS to find this kind of attack and also block it. In this paper they elaborated about various types of DDOS attack and how to protect from them. There are different types of attacks of DDOS attack such as SYN flood, Ping of Death, Reflected Attack, Degradation of Service Attacks, Multi-Vector Attacks, Flooding Attack, HTTP Flood. They suggested that application DDoS attack operates by sending small amount of packet which overload. Intrusion Detection Algorithm detects the attack and eliminates the attacker nodes from the network. By using this it overcome the requirement of main control authority which is not practical in ADHOC network due to their self-organizing nature and protects the network. This paper uses IDS which uses the anomaly IDS in which IDS takes values, packet reception rate (PRR) and inter arrival time (IAT).It also includes a comparative study of all the different parameters that are used by different authors on MANET.

B. Ping et al.[8] discussed about A New Routing Attack in mobile ad hoc networks. In this paper, they presented a new attack, the Ad Hoc Flooding Attack, which results in denial of service when used against all previously on on-demand ad hoc networks routing protocols. To defend routing protocols against the Ad Hoc Flooding attack, they developed a generic secure component, called Flooding Attack Prevention (FAP), which can be applied to AODV routing protocol to allow that protocol to resist the rushing attack. The results of their implementation show that FAP can prevent the Ad Hoc Flooding attack efficiently. They had made a comparison between SYN Flooding Attack and Ad Hoc Flooding Attack. They had used metrics to evaluate the performance of Flooding Attack Prevention (FAP).

C. S.A.Arunmozhi et al. [9] discussed about DDoS Attack and Defense Scheme in Wireless Ad hoc Networks. In this paper, they explained about the DDoS attacks and proposed a defense scheme to improve the performance of the ad hoc networks. Their proposed defense mechanism uses the medium access control (MAC) layer information to detect the attackers. Once the attackers are identified, all the packets from those nodes will be blocked. The network resources are made available to the legitimate users. They had performed the simulation with Network Simulator and we proved that our proposed system improves the network performance. In this paper, they had proposed a new defence mechanism which consists of a flow monitoring table (FMT) at each node. By simulation results, they have shown that the proposed scheme achieves higher bandwidth received and packet delivery ratio with reduced packet drop for legitimate users.

D. V.V. Timcenko et al. [10] presented An Approach for DDoS Attack Prevention in Mobile ad hoc Networks. In this paper they had proposed a prevention mechanism for distributed denial of service (DDoS) attacks in mobile ad hoc networks environment. The presented approach relies on the investigation of widespread bandwidth attacks, with focus on Distributed Denial of Service (DDoS) attacks, which are extremely dangerous, hard to detect and challenging to prevent. The presented Intrusion prevention systems (IPS) model is based on the analysis of the forensic analysis report generated by IDS incorporated into the network security monitoring system. In this paper the focus is on efficient use of the IDS report and its application for the preventive and responsive activities in MANET security provisioning. The Flexible MANET Prevention Algorithm (FMPA) has been proposed and explained its interoperability with the used IDS solution.

E. Tariq et al. [11] suggested Detection and Defense Mechanism against DDoS in MANET. In this article they had used Reply Request (RREQ) with a thresh hold time mechanism to deal with the threat of DDoS. They had used calculations and their analysis to detect the threat and the malicious node and with the help of reply request with thresh hold time. They have proposed a detection technique and detected the malicious data source node as well. In this research they have evaluated the robustness of existing routing protocols against the malicious attacks and assess the quality and impact of security improvements and have proposed a reliable solution to handle DDoS attacks in MANETS. The proposed approach is based on reply request with threshold time in MANETs sent to 1Hop node in a particular sequence to detect the malicious behaviour and based on its reply time taken to complete the reply-request loop its IP address can be added or removed from the routing table of the nodes of the network in order to keep the network safe from this attack.

F. Qiang et al. [12] have proposed Modeling of Distributed Denial of Service Attacks in Wireless Networks. In this paper, different types of DDoS attacks launched in wireless networks are modeled and the parameter requirements to launch such DDoS attacks and analysed. Their models can be applied to obtain estimates of the connection and bandwidth resources required to provide high performance wireless Internet access and ensure a certain low packet loss probability even under DDoS attacks. The corresponding defense strategies are proposed and discussed. Servers protected by such strategies can still deliver regular service to their legitimate mobile clients. The feasibility of launching DDoS attacks in wireless ad hoc networks is also discussed.

G. Abdullah et al. [13] have presented a new scheme of detecting distributed denial of service (ddos) attack using ttl constraint in mobile adhoc networks (manet). The proposed approach offers DDoS detection and control technique based on TTL (time to live) key field and can detect any malicious or suspicious node that can harm network resources and decline network performance. The mechanism uses additional packet field named TTL (Time To Live) before the data packet is assigned TTL (Time To Live) for the nodes. This TTL assigned to node is decremented by the malicious node. Their mechanism had checked this TTL of the node and the data packet and in case it is abnormal then the node is declared as malicious or compromised node.

H. Prajeet et al. [14] suggested A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network. Their main aim was seeing the effect of DDoS in routing load, packet drop rate, end to end delay, i.e. maximizing due to attack on network. And with these parameters and many more also we build secure IDS to detect this kind of attack and block it. In this paper they discussed some attacks on MANET and DDOS also and provided the security against the DDOS attack. In their proposal they used AODV routing protocol in all normal module attack module and IDS (intrusion detection system) for prevention through attack. In this paper they simulated the three different condition results normal time, Attack time and IDS module time through NS-2 simulator. The results demonstrated that the presence of a DDOS increases the packet loss in the network considerably. The proposed mechanism protects the network through a self-organized, fully distributed and localized procedure.

I. Karthikeyan et al. [15] presented An Integrated Defense Approach for Distributed Denial of Service Attacks In Mobile Ad-Hoc Network. This paper has discussed various the attack mechanisms and problems due to DDoS attack, also how MANET can be affected by these attacks. In addition to this, a novel approach is proposed to defense against DDoS attacks in Mobile Ad-hoc Networks. This paper also described various countermeasures that should be taken to prevent the net-work from DDoS attack. An ISP level integrated approach is proposed to defense against DDoS attacks and the simulation results shows that the proposed defense method is much better than existing techniques in terms of Packet Delivery Ratio (PDR) which becomes double and the Number of Collisions reduced to half with respect to different number of attackers in Mobile Ad-hoc Networks.

J. Neeraj et al. [16] discussed Attack Prevention Methods For DDOS Attacks In MANETS. In this study, the current security issues in MANET are investigated. Particularly, the researchers have examined different DDoS attacks and some detection methods like profile-based detection specification-based detection as well as existing solutions to protect MANET protocols. Different DDoS attacks such as flooding, wormhole, modification, impersonation, fabrication, modification, selfish or lack of cooperation attacks and some detection methods like profile-based detection and specification-based detection are examined. The existing solutions such as local filtering, changing IPs, creating client bottlenecks and global solutions are improving the security of the entire internet, using globally coordinated filters and tracing the source IP address to protect MANET protocols were described.

K. Mieso et al. [17] proposed Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme. In this paper, they proposed a reputation-based incentive mechanism for detecting and preventing DoS attacks. DoS attacks committed by selfish and malicious nodes were investigated. Their scheme motivated nodes to cooperate and exclude them from the network only if they fail to do so. They evaluated the performance of their scheme using the packet delivery ratio, the routing and communication overhead and misbehaving node detection in a discrete event-simulation environment. The results indicated that a reputation-based incentive mechanism can significantly reduce the effect of DoS attacks and improve performance in MANETs. In this paper, they considered a DoS attack caused by a selfish node that drops packet and a wormhole attack caused by a malicious node. They proposed a reputation-based incentive mechanism for encouraging nodes to cooperate both in resource utilization and preventing DoS attacks.

L. Mukesh et al. [18] proposed detection and prevention of ddos attack in manet's using disable ip broadcast technique. in this paper, a technique was proposed that can prevent a specific kind of DDoS attack i.e. flood attack which disable IP Broadcast. The proposed scheme is distributed in nature it has the capability to prevent Distributed DoS (DDoS) attack. The performance of the proposed scheme in a series of simulations shows that the proposed scheme provides a better solution than existing schemes. In this paper, they compared two DDoS based attacks and propose a technique to prevent Flooding based DDoS attack. They discussed the Implementation and detection of DDOS attack mechanisms in MANET. They described the prevention technique for flooding based DDOS attack and next section presents the experimental setup to measure network performance. They presented various results which show that proposed Disable IP Broadcast Prevention technique is better than existing scheme.

M. Deepak et al. [19] presented a new approach of Detection Mechanism for Distributed Denial of Service (DDoS) Attack in Mobile Ad-hoc Networks. In this paper, various kinds of attacks are presented which are attacked on ad-hoc network and advised approach to detect DDoS attack. To provide a solution for identified problem, a mechanism is proposed to prevent data packet loss occurs during the determining the value of TTL value of nodes and detection of malicious attack in the network. The mechanism proposed which use additional packet named as TTL (time-to-live) before of data packet to determine the value of TTL of nodes. The TTL value of node is decremented by malicious one. Each node has route table which contain path for every node. Node checks the value of TTL of nodes if it is abnormal then node is declared as malicious or compromised by DDoS. Proposed mechanism offers detection and control of DDoS attacks over reputation and score based MANET.

N. Ranjana et al. [20] discussed Distributed Denial of Service Attack Detection, Prevention and Secure Communication in MANET. This paper proposes a DDoS attack detection and prevention scheme. The proposed algorithm detects the possibilities of DDoS attacks in the network and prevents the network, provide security. The objectives are to detect distributed denial of service attack in MANET, to provide prevention of MANET from distributed denial of service attack. MANET network using AODV under distributed denial of service malicious attack with secure routing and data transmission is proposed in this paper. The experimental outcome represented DDoS prevention and detection scheme with improved performance in the network. The proposed scheme is well appropriate for mobile network security.

O. VALENTINA et al. [21] presented an Application of Forensic Analysis for Intrusion Detection against DDoS Attacks in Mobile Ad Hoc Networks. This paper addresses a specific approach to resolving the problem of intrusion detection against distributed denial of service (DDoS) attacks in mobile ad hoc networks (MANET). They provided a comprehensive overview of recent advances in network forensics in MANET environment. They proposed a model of IDS that uses network forensics to detect DDoS attacks in MANET. The forensic analysis relies on inspecting simultaneous malicious activities of a group of attackers. They proposed a flexible IDS model and the associated forensic analysis algorithm based on log file inspection. The performance analysis encompasses 100-nodes network with Manhattan Grid (MG) mobility model, and different numbers of malicious nodes. The study has been carried out by the network simulator ns-2 and its associated tools for mobility scenario generation, network animation and trace files analysis. This paper focuses to IDS against DDoS attacks and, particularly, to application of network forensics in MANET IDS. The objective of this work is to point out the importance of forensic analysis in regular security system cycle, and propose a network forensic based IDS model, considering primarily the detection of DDoS attacks in MANET environment.

P. Adnan et al. [22] suggested an Adaptive Intrusion Detection & Prevention of Denial of Service attacks in MANETs. In this paper they focus on preventing denial-of-service (DoS) attacks. They showed the unsuitability of tools such as control chart, used in statistical process control (SPC), to detect DoS and propose an anomaly-based intrusion detection system that uses a combination of chi-square test & control chart to first detect intrusion and then identify an intruder. When the intruder is isolated from the network they show reduced overhead and increased throughput. Simulation results show that AIDP performs well at an affordable processing overhead over the range of scenarios tested. They then proposed an adaptive intrusion detection & prevention mechanism AIDP. It employs ABID which first use chi-square test to check the overall behaviour of the network and indicate intrusion, and then uses control chart to identify intruding nodes. Simulation results show that AIDP successfully detects identifies & isolates the intruding nodes attempting to cause DoS attacks. AIDP exhibits a high success rate and very low false alarm rate with an affordable processing overhead on the network over a range of scenarios tested.

Q. Aikaterini Mitrokotsa et al. [23] proposed an Intrusion Detection of Packet Dropping Attacks in Mobile Ad Hoc Networks. The focus of this paper is on anomaly detection techniques in order to exploit their main advantage of being able to detect unknown attacks. First, they briefly described intrusion detection systems and suggested a distributed schema applicable to mobile ad hoc networks. This anomaly detection mechanism is based on a neural network and is evaluated for packet dropping attacks using features selected from the MAC layer. The performance of the proposed architecture is evaluated under different traffic conditions and mobility patterns. In this paper, they proposed a completely distributed intrusion detection approach that is better suited for the vulnerable characteristics of wireless ad hoc networks. The intrusion detection approach is performed using neural networks. Neural networks have the great advantage of tolerance towards imprecise data. They exploit this important feature of neural networks and introduce an intrusion detection approach based on Emergent Self-Organizing Maps. In this paper, they propose a completely distributed IDS for mobile ad hoc networks using eSOM. By exploiting the visualization of network traffic our approach detects selective packet dropping attack by classifying malicious and normal behaviour. The proposed approach uses the MAC layer feature set as audit data. They examined how eSOM performs in classifying normal and abnormal behaviour in mobile ad hoc networks and exploited the advantage of visualizing network traffic that is achieved through eSOM. The proposed intrusion detection approach is also able to identify the source of the packet dropping attack.

R. Meghna et al. [24] suggested A Novel Solution to Handle DDOS Attack in MANET. This paper discusses various the attack mechanisms and problems due to DDoS attack, also how MANET can be affected by these attacks. In addition to this, a novel solution is proposed to handle DDoS attacks in mobile ad hoc networks (MANETs). This paper gives the effectiveness of DDoS attacks on such statistical-based filtering in a general context where the attackers are smart. They first give an optimal policy for the filter when the statistical behaviours of both the attackers and the filter are static. Next, this paper considers cases where both the attacker and the filter can dynamically change their behaviour, possibly depending on the perceived behaviour of the other party. This paper gives information about DDoS attack models and proposed taxonomies to characterize the DDoS attacks, the software attacking tools used, and the possible countermeasures those are available. Thus, this paper describes that DDoS attacks make a networked system or service unavailable to legitimate users and proposes a simple-to integrate DDoS victim based defense method, Packet Funneling, whose main aim is to mitigate the effect of attack on the victim.

S. Sadhu et al. [25] presented a Secure Intrusion Detection System against DDOS Attack in Wireless Mobile Ad-Hoc Network. In this paper, we mainly aiming on seeing the effect of DDoS in routing load, packet drop rate, end to end delay. With use of these parameters and many more also we build secure IDS to detect this kind of raid and block it. The proposed mechanism eliminates the need for a centralized trusted authority which is not practical in ADHOC network due to their self-organizing nature. The results demonstrate that the presence of a DDOS increases the packet loss in the network considerably. The proposed mechanism protects the network through a self-organized, fully distributed and localized procedure. The proposed mechanism can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks. They believed that this is an acceptable performance, given that the attack prevented has a much larger impact on the performance of the protocol. DDoS attacks are also a problem on Cloud computing enviourments [26].

III. GENETIC ALGORITHM BASED DETECTION TECHNIQUE OF DDoS ATTACK

In a DDoS attack an attacker holds multiple source hosts to forward attack traffic to one or more victims simultaneously so that a new computational technique have proposed using Genetic Algorithm. The proposed method performs the classification task and extracts required knowledge for detection of DDoS attack using Genetic Algorithm.

Basically, Genetic Algorithm (GA) is a search method based on concept of natural selection and population genetics. GA uses in science, engineering and business problems. GA employs three operators i.e. selection, crossover and mutation. The selection operator indicates the fittest individuals of the current population to employ as parents of the next generation. Cross over operator integrates the second half of the first record with the first half of the second record. Mutation operator freely made changes in the bits from ‘0’ to ‘1’ and vice versa.

Generally, the implementation of IDS consists of three phases such as data pre-processing, features extraction and classifier. We used genetic algorithm (GA) for the detection of DDoS attack.

In this work, data pre-processing, feature selection and classifying the attacks using genetic algorithm will be implemented for DDoS attacks. In this research, we will follow the below steps and figure – shows the flowchart of proposed work:

- Collection of DDoS attack data though Qualnet simulator 6.1 in respect of AODV routing protocol.

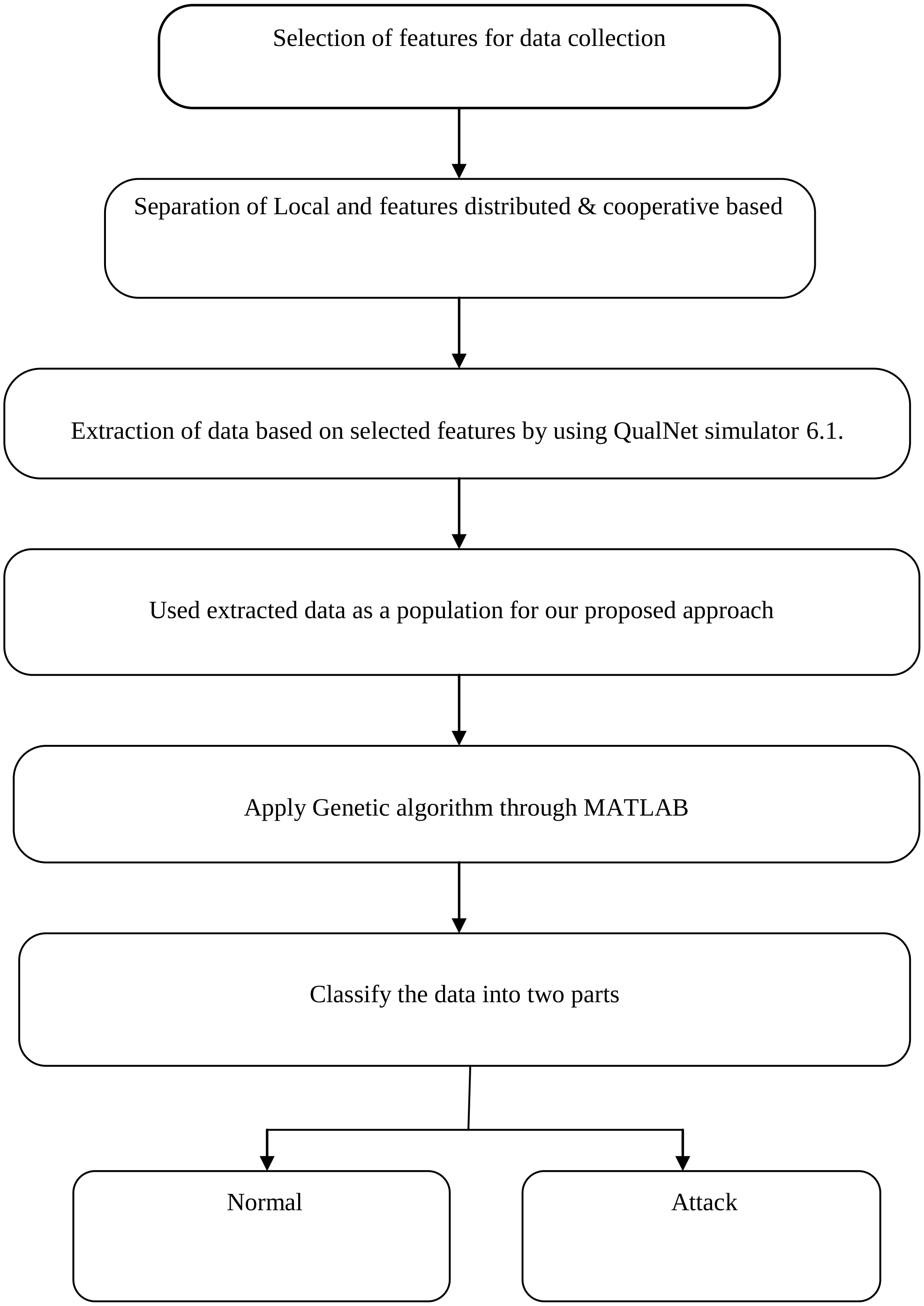
Selection of features for data collection
Separation of Local and features distributed & cooperative based
Extraction of data based on selected features by using QualNet simulator 6.1.
Used extracted data as a population for our proposed approach
Apply Genetic algorithm through MATLAB
Classify the data into two parts
Normal
Attack

Figure 1. Work flow for developing our proposed GA based IDS

Apply Genetic Algorithm for selection of optimal features of DDoS attack and classifying the normal and DDoS attack data in MANETs.

The proposed architecture contains two phases 1. Training phase 2. Testing phase. In training phase, Data pre-processing, feature selection and classifying the attacks using genetic algorithm and DDoS patterns were identified. Second stage is testing stage, the captured traffic is evaluated as in training stage, pattern identified, matched with database and decision to be taken. New patterns were identified by analyzing the behavior of the traffic, if it was against the legitimate traffic, the pattern was captured and updated in the database. The design and their implementation of Genetic based IDS have following phases such as, Pre-processing, Feature Selection, and Classifier. Figure 1 shows the steps of our proposed work.

IV. CONCLUSION AND FUTURE WORK

Achievement of trustable security in MANETs is most complex issue due to its dynamic characteristics in these days. Only prevention based techniques such as cryptography and authentication are no longer sufficient for its nature. MANETs works as an open medium for attackers because anyone can join and move the network at any time due to the communication via wireless link. The security mechanism of wired networks cannot be directly applied on MANETs because of its dynamic nature.

In this paper, our main concentration on security of MANETs from DDoS attack. There are many techniques which have been proposed in literature for MANETs. We have analyzed the working style of some above discussed proposed DDoS detection techniques and reached on decision that still we do not have any promising solution for this dynamic environment from DDoS attack so that we have proposed a genetic algorithm based solution for MANETs which may show the good results for the detection of DDoS. We will publish the implementation results using genetic algorithm in future.

REFERENCES

[1] IETF Mobile Ad-Hoc Networks Working Group (MANET), IETF web-site www.ietf.org/dyn/wg/charter/manet-charter.html

[2] IETF Ad-Hoc Networks Autoconfigurations (autoconf) Working Group, IETF website http://datatracker.ietf.org/wg/autoconf/charter/

[3] IEEE Std 802.11-2007, “IEEE standard for information technology-Telecommunication and information exchange between systems-Local and metropolitan area network-Specific requirement, Part 11 Wireless LAN medium access control and physical layer specifications”, June 2007.

[4] Chaudhary, Alka, V. N. Tiwari, and Anil Kumar. "A new intrusion detection system based on soft computing techniques using neuro-fuzzy classifier for packet dropping attack in manets", International Journal of Network Security 18, no. 3, 514-522, 2016.

[5] Chaudhary, A., V. N. Tiwari, and A. Kumar. "Analysis of fuzzy logic based intrusion detection systems in mobile ad hoc networks", BVICA M's International Journal of Information Technology 6.1, 2014.

[6] Chaudhary, Alka. "Neuro-fuzzy based intrusion detection systems for network security", Journal of Global Research in Computer Science 5.1, pp. 1-2, 2014.

[7] Farooqui, Yassir, Vanita Mane, and Puja Padiya. "DDOS using Intrusion Detection System in Wireless Mobile Ad hoc Network”.

[8] Yi, Ping, et al. "A new routing attack in mobile ad hoc networks", International Journal of Information Technology 11.2, pp. 83-94,2005.

[9] Arunmozhi, S. A., and Y. Venkataramani. "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks", arXiv preprint arXiv: pp.1106.1287,2011.

[11] Ahamad, Tariq, and Abdullah Aljumah. "Detection and defense mechanism against DDoS in MANET", Indian Journal of Science and Technology 8.33, 2015.

[10] Timcenko, V. V. "An approach for DDoS attack prevention in mobile ad hoc networks", Elektronika Ir Elektrotechnika 20, no. 6 pp.150-153, 2014.

[12] Huang, Qiang, Hisashi Kobayashi, and Bede Liu. "Modeling of distributed denial of service attacks in wireless networks", Communications, Computers and signal Processing, 2003. PACRIM. 2003 IEEE Pacific Rim Conference on. Vol. 1. IEEE, 2003.

[13] Aljumah, Abdullah. "detecting distributed denial of service (ddos) attack using ttl constraint in mobile adhoc networks (manet)", Science International 27.6,2015.

[14] Sharma, Prajeet, Niresh Sharma, and Rajdeep Singh. "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network", International Journal of Computer Applications 41.21 2012.

[15] Thyagarajan, Karthikeyan, and Arunkumar Thangavelu. "An Integrated Defense Approach for Distributed Denial of Service Attacks In Mobile Ad-Hoc Network", International Journal of Applied Engineering Research 11.7, pp. 4898-4910,2016.

[16] Sharma, Neeraj, B. L. Raina, Prabha Rani, Yogesh Chaba, and Yudhvir Singh. "Attack Prevention Method Methods for DDOS Attack in MANET", Asian Journal Of Computer Science And Information Technology1 1, pp.18-21, 2010.

[17] Denko, Mieso K. "Detection and prevention of Denial of Service (DoS) attacks in mobile ad hoc networks using reputation-based incentive scheme", Journal of Systemics, Cybernetics and Informatics 3.4, pp. 1-9, 2005.

[18] Kumar, Mukesh, and Naresh Kumar. "DETECTION AND PREVENTION OF DDOS ATTACK IN MANET'S USING DISABLE IP BROADCAST TECHNIQUE", International Journal of Application or Innovation in Engineering & Management 2.7, pp. 29-36, 2013.

[19] Vishwakarma, Deepak, and D. S. Rao. "Detection Mechanism for Distributed Denial of Service (DDoS) Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications 102.9, pp. 23-26, 2014.

[20] Kumari, Ranjana, and Achint Chugh. "Distributed Denial of Service Attack Detection, Prevention and Secure Communication in MANET",

[21] Timcenko, V. A. L. E. N. T. I. N. A., and Mirjana Stojanovic. "Application of forensic analysis for intrusion detection against DDoS attacks in mobile ad hoc networks", Proceedings of the 1st WSEAS Int. Conf. on Information Technology and Computer Networks (ITCN'12), Vienna. 2012.

[22] Nadeem, Adnan, and Michael Howarth. "Adaptive intrusion detection & prevention of denial of service attacks in MANETs", Proceedings of the 2009 international conference on wireless communications and mobile computing: Connecting the world wirelessly. ACM, 2009.

[23] Mitrokotsa, Aikaterini, Rosa Mavropodi, and Christos Douligeris. "Intrusion detection of packet dropping attacks in mobile ad hoc networks," Proceedings of the International Conference on Intelligent Systems And Computing: Theory And Applications. 2006.

[24] Chhabra, Meghna, Brij Gupta, and Ammar Almomani. "A novel solution to handle DDOS attack in MANET", Journal of Information Security 4.03, 2013.

[25] Sharma, Prajeet, Niresh Sharma, and Rajdeep Singh. "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network", International Journal of Computer Applications 41.21 2012.

[26] Patidar, V., & Kumbhkar, M., "Analysis of Cloud Computing Security Issues in Software as a Service", International Journal of Scientific Research in Computer Science and Engineering, 2(3), pp. 1-5, 2014.

Authors Profile

Alka Chaudhary received her M.C.A. degree from Institute of Technology and Science (ITS), Mohan Nagar, Ghaziabad in 2010. Currently, she is pursuing M.Tech in Computer Science from Jagannath University Jaipur, Rajasthan. She has published 21 research papers in International Journals and Conferences. Her research interests include Information Security, Mobile Ad Hoc Networks, Neural network, Fuzzy Logic, Intrusion Detection/Prevention, and Network Security.

Gajendra Shrimal is B.E., M.Tech in the field of Computer Science and Engineering. He is currently working as an Assistant Professor in Computer Engineering Department at JaganNath University, Jaipur. His area of interest includes Pattern Recognition & Image Processing. Artificial Intelligence, Randomize Algorithms, and Nature Inspired Computing.

Ria Rautela is a B.Tech student. She is doing B.Tech from Manipal University Jaipur. Her research interests include Network Security, Algorithms.