International Journal of Grid and Distributed Computing
Vol. 9, No. 6 (2016), pp.219-234
http://dx.doi.org/10.14257/ijgdc.2016.9.6.21

Crytography Bases Solution FOR Distributed Denial of Service Attack in Manet

Darshan Meena[1], Priya Pathak[2], Sandeep Gupta[3]

Dept. of CSE[1,2,3]
dlmeenapgtcs@gmail.com[1],shakhi.priya@gmail.com[2] ,
sandeepguptabashu@gmail.com[3]

Abstract

In mobile ad-hoc network nodes communicate with each other or forward data by making route with the help of other nodes. Infrastructure of the network does not fix topology change due to movability of nodes that's why attacking condition in this network become high. There are lots of attacks for this network. In this paper we study about denial of service attack and its prevention and detection technique, in our propose work we give a novel solution to detect or prevent denial of service attack we implement our work in NS-2.35. Efficiency of our work we proof with the help of results.

Keywords: MANET;DDOS;PCA;DOS;LAN, etc

1. Introduction

Ever since their appearance in 1970 in the arrangement of ALOHANET, wireless envelope radio networks have come some distance in terms of amounts, tenders, and the function set, among other things. The two major attractions of wireless communication were mobility and ease of deployment – laying cables shouldn't be handiest laborious and time consuming, but their preservation is equally bothersome Wireless communication today surrounds us in lots of colors and flavors, each with its particular frequency band, coverage, and range of applications. It has matured to an important extent, and specifications have advanced for Personal Area Networks, Local Area Networks as well as Broadband Wireless Access A promising and really appealing classification of wireless networks that has emerged is centered on an Ad Hoc topology; these networks are referred to as WSNs. The term wireless network implies a computer network in which the links of the communication are wireless.

The time period Ad Hoc originates from the fact that there's no steady infrastructure for packets forwarding/ routing.

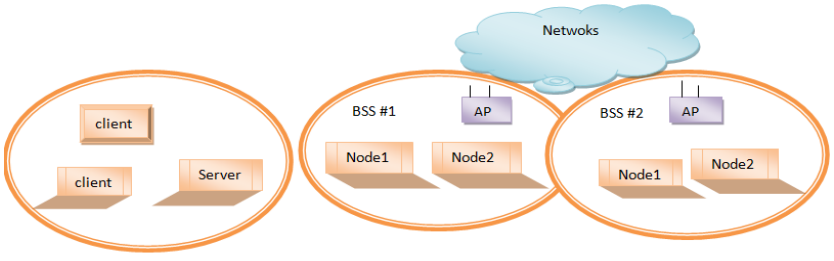

Figure 1. Shows an Infrastructure-based

ISSN: 2005-4262 IJGDC

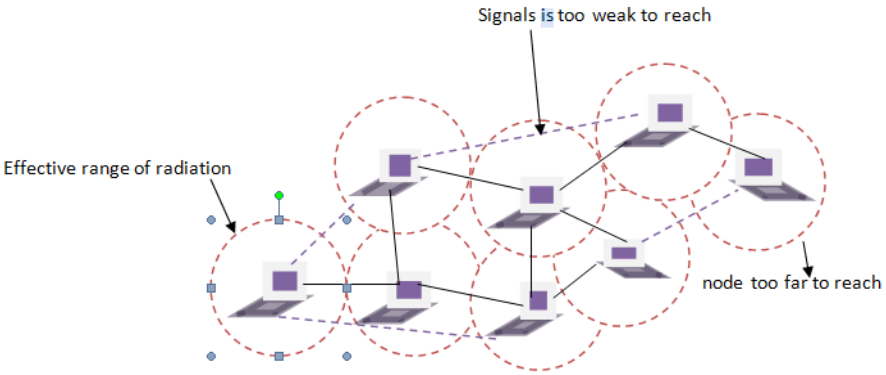

Figure 2. A Typical MANET

A typical MANETs is shown in Fig 1. The circles point out communication stages of person nodes. In the real-world, this boundary is under no circumstances likely to be an ideal circle and the hyperlinks actually may be one directional in lots of cases – node 'A' can reach node 'B' on link 1 but node 'B' cannot be able to use this link to reach node 'A'. This can happen due to the one strengths of the 2 transmitters being unequal or also be headquartered on the transmission course.

2. DDOS Detection

Systems used to sense DDOS attacks are considered as a type of Network Intrusion Detection Systems (NIDs). The latter employ two distinct approaches to detect malicious activities: signature-based detection and anomaly-based detection [1]. Signature-based detection is used to identify known security threats (e.g., a virus or malformed packets) looking for particular patterns (signatures) to appear in individual packets. On the other hand, anomaly-based NID is used to discover potential security threats based on abnormal behaviors over a set of packets. Due to the nature of the flooding-based on DDoS attacks, where each malicious packet may seem legitimate if analyzed independently, but where the whole traffic performance may suffer abrupt variations (e.g. Abrupt increases of traffic volume), detection of anomaly-based is always used in the DDOS attacks based detect which is based on flooding.

In the recent decade, numerous anomaly-based detection approaches were suggested to the identify DDoS attacks from network traffic. Principally, these detection methodologies can be classified into two main classes: on-line DDoS detection and off-line DDoS mining. Off-line DDoS mining, commonly try to find attacks by the studying the main characteristics of the feature distributions of the system traffic with some systematic Corresponding to PCA (essential component evaluation) [2, 3] and dominate state analysis [4]. The simple idea of PCA is to embed the multidimensional data into lower dimensional subspace in which normal instances and the anomalies appear significantly different. The original idea of the dominate state analysis is to explore the interaction or dependence among the dimensions of the information by identifying a subset of values (dominate states) to represent or approximate the original information in their probability distribution. Anomalies can be recognized the since they dominate states deviate significantly from normal ones. When network anomalies are then identified, data clustering approaches, such as k-means clustering [5], are applied to collect different kinds of the anomalies together for further ID, correlating anomalies to attacks. To achieve accurate analysis results, the processing procedures of off-line methods are executed on the whole data trace, and these methods usually involve expensive computations, e.g. PCA involves matrix computations for computing principal components of the data. So the off-line DDoS mining methods can hardly be used in

online discovery, due to time and space complexities. However, the analysis results from the off-line anomaly mining can help build the baseline profile for the real time detection. Considering the big scale of the DDOS attacks, detection over the big volume of traffic (e.g. multi-10Gbps) is really challenging. Computation terminated massive information streams is being studied in the emerging field of data streaming, aiming at methods for processing massive amounts of data in a real-time fashion, such that each tuple in the data stream is only processed once. Data streaming computation has been adopted in applications such as financial markets and mobile phones or credit card scam detection applications.

3. Literature Survey

In 2000 [6] describe that the infamous, crippling attack on e-commerce's prime companies in February 2000 and the recurring proof of active network scanning, a signal of attackers watching for network weaknesses in every single place the web, are harbingers of future DDOS i.e. Distributed Denial of Service attacks. They signify the continuing distribution of the evil daemon packages which can be likely to result in repeated DDOS attacks within the foreseeable future. This paper offers information about the weaknesses in the network that DDOS attacks exploit the technological futility of addressing the situation exclusively at the regional level.

In 2002 [7] gives important forms of DOS attacks which flood victim's communication channel bandwidth, is implemented their analysis and are offered approaches of security from these attacks. The handler refers commands to the agents, which implement genuine DOS attacks towards indicated the system-victim. This paper additionally describes several countermeasures that will have to be taken to check the network from DDOS attack.

In 2004 [8] Lu Han describes that the WSNs were first unfolded in 1990's. MANETs have been largely researched for decades. Although, most of the research is completed in this field, but the question is that, whether the architecture of MANETs is a fundamental faulted architecture.

In 2004 [9] Stephen M. Specht describes that dispensed Denial of Service attacks have become a colossal main issue for the methods linked to the internet. DDoS attackers take manipulate over secondary victim methods and use them to launch a coordinated big-scale attack towards foremost sufferer methods. Consequently of latest countermeasures which are developed to hinder or mitigate DDoS attacks, attackers are continuously establishing different ways to cheat on these new countermeasures. This paper provides us information about DDoS attack models and proposed taxonomies to describe the DDoS attacks, the software attacking tools used, and the possible countermeasures those are available.

In 2005 [10] point out that dispensed Denial of Service i.e. DDOS attacks pose a serious chance to carrier availability of the sufferer network via severely degrading its performance. There was giant curiosity in using statistical-established filtering to defend in opposition to and mitigate the effect of DDOS attacks. Below this method, packet survey is checked to categorize common and irregular behavior. This paper considers instances where each the attacker and the filter can dynamically alternate their behavior, possibly depending on the perceived behavior of the opposite get together.

In 2006 [11] the authors presented a dynamic DOS attack, the one which may also be characterized by using exploiting the node mobility, dynamic power manage, and compromised nodes to takeoff new DOS attacks dynamically. Malicious nodes may be competent to move across the whole network, to adjust the transmission power dynamically, or even launch DOS attacks by compromising their cooperative neighbors.

In 2010[12], the authors proposed a model to describe the DDOS flooding attack and its traffic statistics. The predominant intention of flooding attack is to paralyze the entire network through inserting overwhelming attack traffic (e.g. RREQ broadcasting) into the MANET. The advantage of this method is to detect DDoS attacks more effectively by traffic pattern identification proposed in their work.

In 2014 [13] analysis, of a novel system is proposed which deals with suppressing the influence of the attack. The effectiveness of the technique is validated by simulation in GloMoSim, built-in with parsec compiler, on a home windows platform.

In 2015 [14] proposed approach results in filtering of the deceived IP packets and the potential attack packets from the attacker. Here the blocking of the access as a whole is not done, but when there seems to be an excess traffic, the requests are processed with a delay from the normal access time. In the meantime, the check for the possible attack is done.

In 2012 [15] this paper presents a procedure for defining Intrusion or any misbehave that happens in MANET by using making use of IDS and it defend the network from DDOS and it analyze the outcome on the center of packet supply ratio, routing load and IDS time. On this paper NS-2 is used to research TCP at traditional time and DDoS time, IDS case, routing load, packet conveyance ratio and analysis of packet sends and receives. The simulation outcome concludes that the IDS 99.9% recoverable.

In 2008 [16] the paper investigates some mechanisms towards DDoS attacks. It often uses the IP deal with spoofing to costume the drift of attack. This paper is a scheme which is based on the firewall in which it can distinguish packets and filter the attack packets before it reaches the victim. This scheme has low implement cost compared to another mechanism. This scheme allows the firewall to arrange itself so that attack can be easily detected. IP address spoofing is used in DDoS attacks which is to hide the uniqueness of the source address.

4. Proposed Work

The main problems of identitying vulnerabilities are deauthentication, beacon spoofing, disassociation and diassociation attack. Since, we have been using the management frames unprotected the MAC address of the AP or clients are spoofed by the attacker or intruders and disassociation or deauthentication are taken place on the genuine clients. As we know, deauthentication requests are notifications, deauthentication requests can never be ignore and we AP responds immediately to these types of request. The attackers monitor all the channels and this sends spoofed messages to all clients so that they can halt the connection. The deauthentication is more harmful attacks in compare to other type of DDOS attacks. Since, these attacks completely disconnect the real clients from our network. So, we need an urgent preventing technique for this deauthentication, disassociation DDos attacks.

The existing detection algorithms are useful to identify or classify to DDos attacks but these algorithms are not protecting the wireless LAN environment from a very various MAC spoofing attack. Our suggested algorithm provides an effective way to sense and prevent disassociation and deauthentication DOS attack which are entering into our system by the MAC address spoofing for the victim stations. In our proposed algorithm, every authentication and association request is passed with a passkey value which is validating only for certain amount of time. First of all, initially the interface can be monitored for packets. A counter is maintained for deassociation and deauthentication, threshold values are also assigned which acts as the main trigger values for flooding attack detection. In our algorithm, we also check frame types and sub types. The pass-key value for the authentication and deauthentication request and responds instead of regular authentication and respond types messages.

5. Proposed Methodology

Medium Access Control Spoof Detection and Prevention Algorithm i.e. MAC SDPA For spoofing attacks in WLAN. In our base paper if the pass key unscrambled by the interloper then proposed calculation does not work legitimately in light of the fact that if gatecrasher alter its esteem then this proposed calculation work in a negative manner.

Then again on the chance that we build number of access focuses ad if access focuses itself turn into an interloper so there is no real way to distinguish access point as gatecrasher in this proposed work so overcome this problem we give **a novel solution for distributed denial of service attack** that is describe as, first system introduce to begin correspondence at the season of correspondence we separation organize in zones and figure the estimation of δ, δ is difference between current time and the value of timer stored earlier. δ can be measured by subtracting the variable In from current time (ct).

Estimation of δ contrast and threshhold1, which is ascertained by past time put away at time of system introduction and duplication of RTT. On the off chance that estimation of δ is more prominent than threshhold1 then we expand the estimation of ddattack after that untouched at whatever point we build the estimation of deadlock we check this quality by edge esteem, if attack world is greater then limit esteem that mean assailant is available in the system and we exit from the circle. For avoiding assailant sender sends an info data outline which contains the Macintosh location of itself and succession number of information and open key of collector and sort and subtype, so with the assistance of these qualities we realize that edge is deauthanticate casing or something else. At the point when edge contains an open estimation of collector so no hub decode that casing, so just validate hub imparts to one another and interloper hub get to be useless, it's a novel technique**.**

In our work, the network connections, initialize all the nodes and send info data to the receivers to know MAC addresses of itself and current time of sending infodata and public key. And where initializing two variables ddattack and dtattack by zero. ddattack is used for deauthentication and dtattack is used for disassociation. Now we examine the time of long trip time for the entire network take an average and stored the time into a variable AInt. After that we will create zones for the network knowledge and check the frame type for every frame. If the frame type is zero, then we also check subtype. If its subtype is also 12 then the casing would we identify as deauthentication frame. After that, now we calculate the δ that is difference between current time and the value of timer stored earlier. Calculated by deducting the variable Ant from current time (CT). If δ is superior than threshold (which is calculated using previous time stored at time of network initialization and multiplication of RTT) than we increase the attack and again check the condition, if attack is better than threshold than control goes to exit attack present. We can check other frames also and ask for MAC address of the sender through the help of info data packet and start time initialization. If receiver and intruder than it will not be capable to decrypt data by its private key it means the intruder nodes are useless.

6. Flow Diagram of Proposed Work

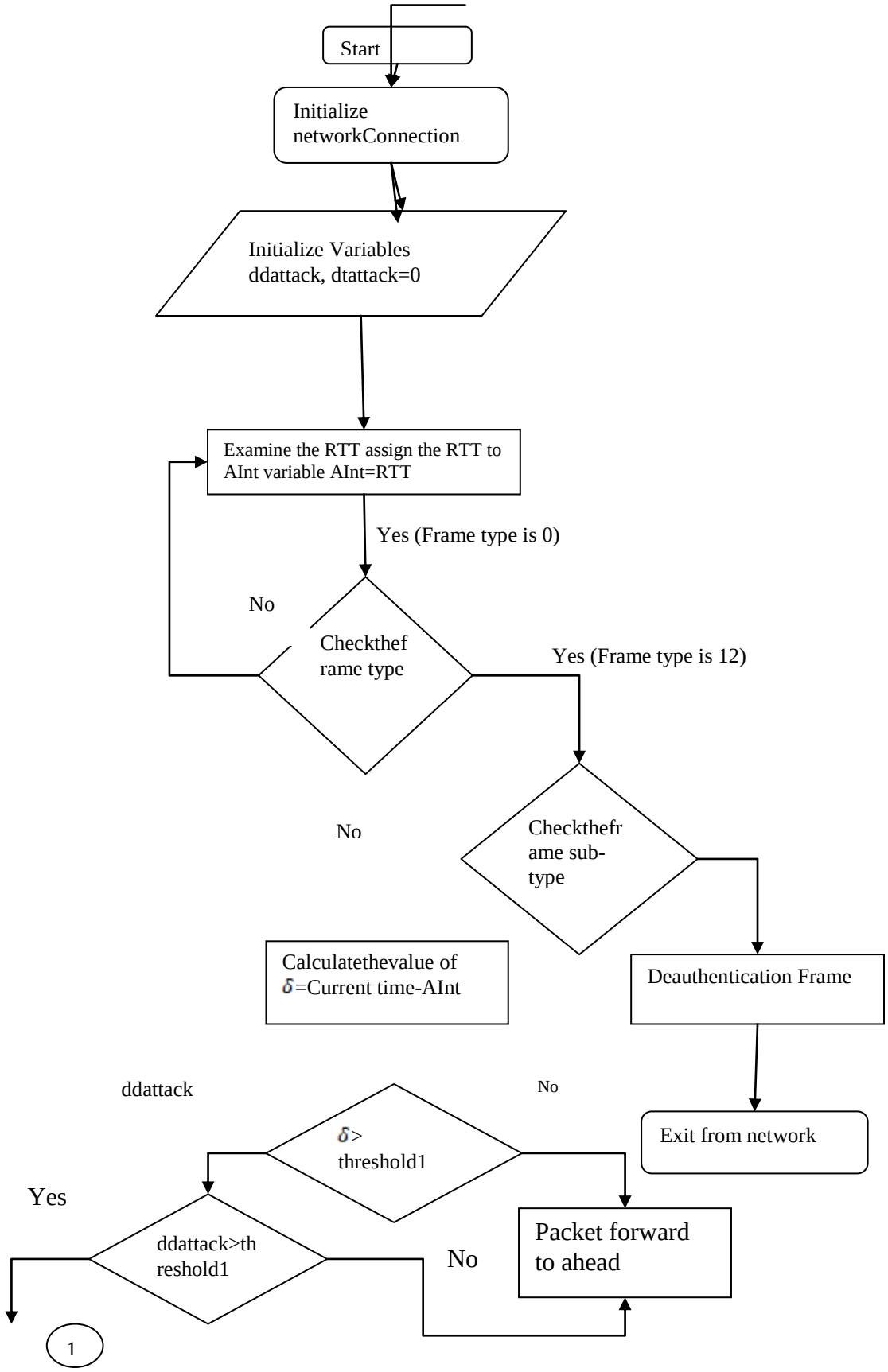

Figure 3. Block diagram of Proposed Working

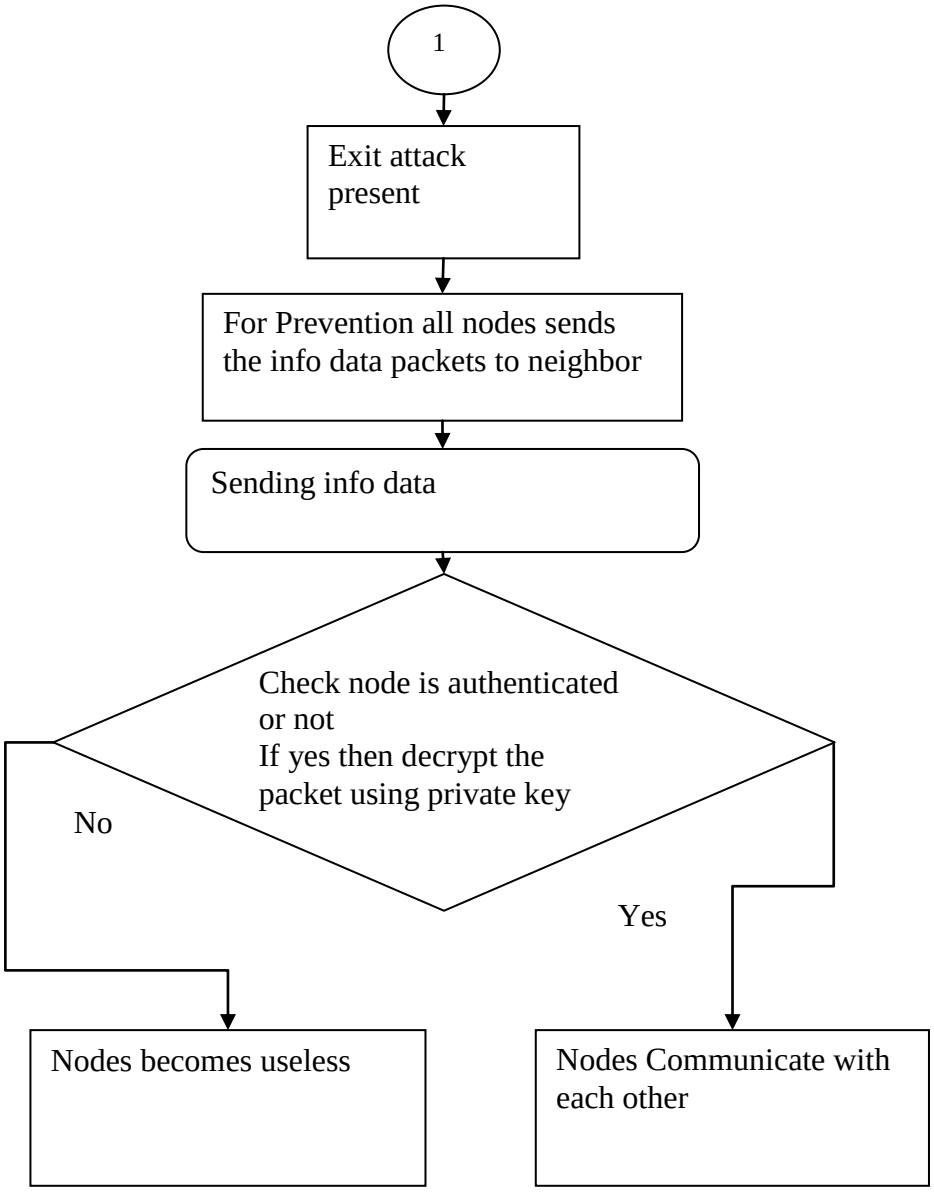

Figure 4. Block Diagram of Proposed Working

7. Simulation Eesult

Simulation parameters:

In our offered work we have created a normal network as compared to earlier one. The network is consisting of wireless scenario there are following parameters used to resource for proposed methodology shown in table 1:

Resource for proposed methodology		
S.No.	**Parameters**	**Details**
1	Simulator	Ns2.35
2	Simulation time	100 sec
3	Protocol	AODV
4	Number of nodes	20
5	OSI Layer	MAC and Network
6	Traffic Models	UDP,CBR and TCP,FTP

Table 1: Shows Simulation Parameter Implement this algorithm in ns 2.35 it's a network simulator in this tool output shows in NAW (network animator window) where nodes communicate to each other output shown below.

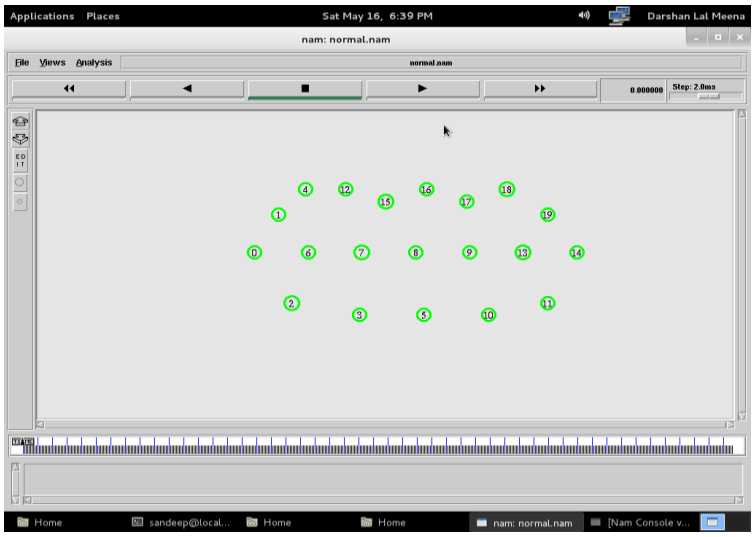

Figure 5. Shows Network Scenario Above Figure

In fig 5 shows the network situation where our network have 20 nodes.

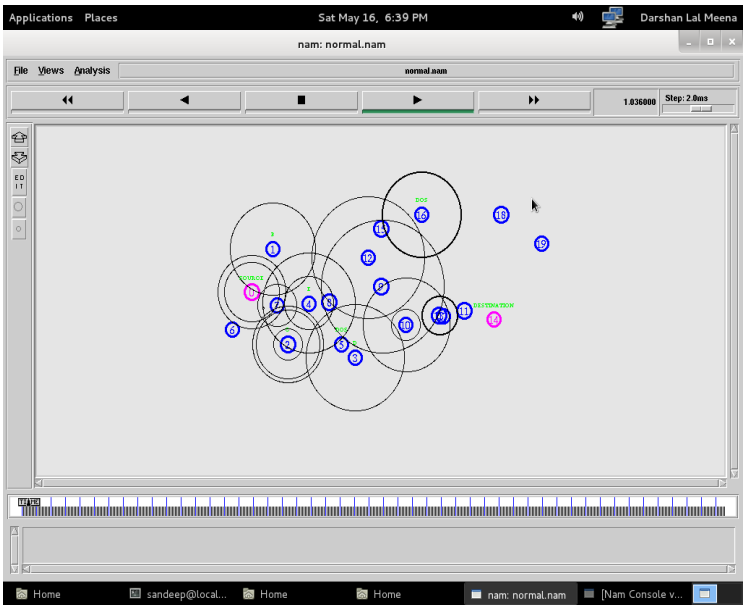

Figure 6. Communication are shown between Nodes Route Detection

In fig 6 shows the communication between nodes for route discovery. In these communicating nodes within range search route to another node.

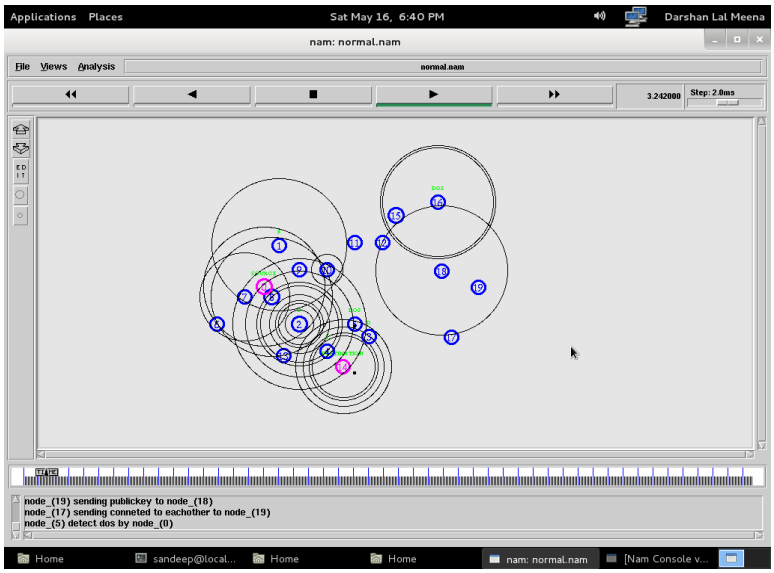

Figure 7. Detection of Distributed Denial of Service Attack by Node (0)

In fig 7 simulation result shows the detection of dos by node, in which detection of Dos is done by node 0

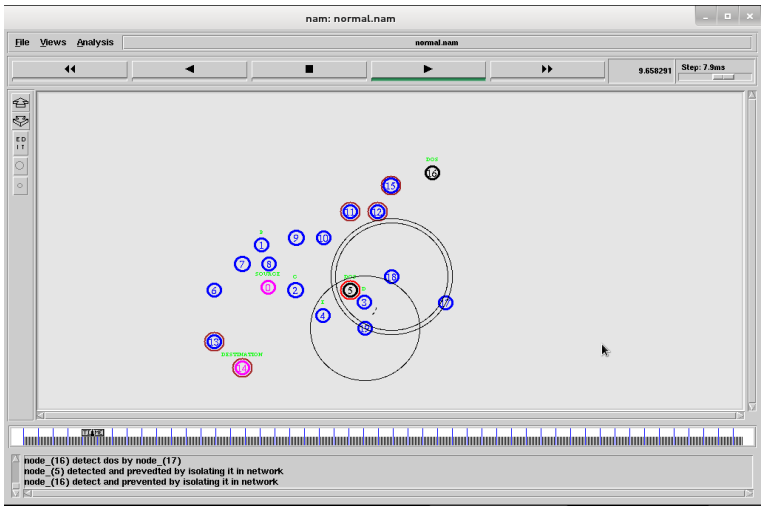

Figure 8. Prevention of Distributed Denial of Service Attack by Node (5 and 16) As express

In fig 8 To prevent these nodes effect in the network, all extra nodes will delete entries of these nodes from their routing table and they will not maintain any routing information about these nodes (nodes 5 and 16 detected & Prevented). In fig nodes 5 in black circle denote the prevention of node.

Result Analysis

Packet Delivery Ratio

The packet supply ratio (PDR) of a network is outlined because the ratio of whole number of data packets truly received and complete amount of data packets transmitted by using senders.

Pdr = ∑ Number of packet receive / ∑ Number of packet send

Normalized Path Discovery:

Normalized path discovery is defined as the number of RREQ packets generated per data packet.

End to end delay

It is outlined because the difference between two time instances: one when packets generated on the sender and the opposite, when packet I received by the receiving application.

End to End Delay =∑ (arrive time – send time) / ∑ Number of connections

Proposed Graph

a) End to end delay:

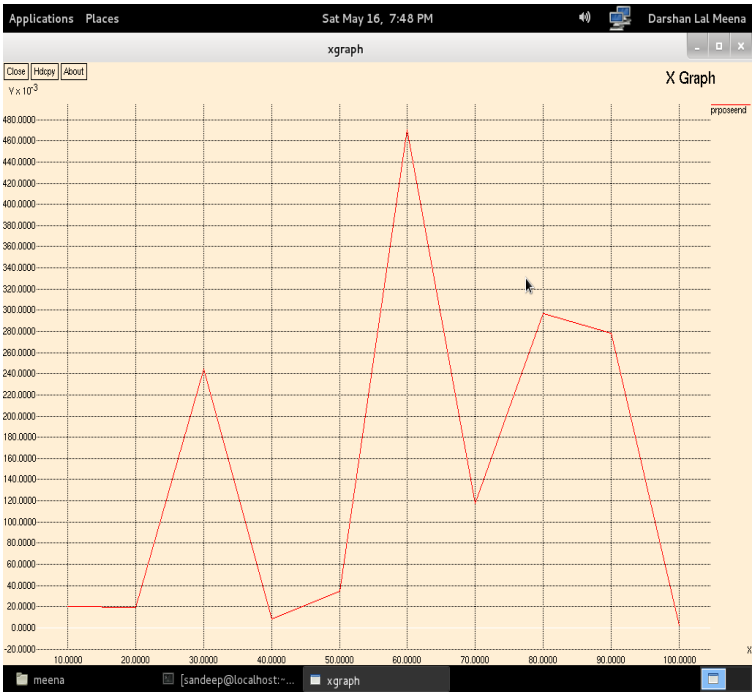

Figure 9. Shows the Proposed Work of End to End Delay

As long as our propose algorithm run our end to end delay decrease and packet deliver in minimum time.

c) Packet delivery ratio:

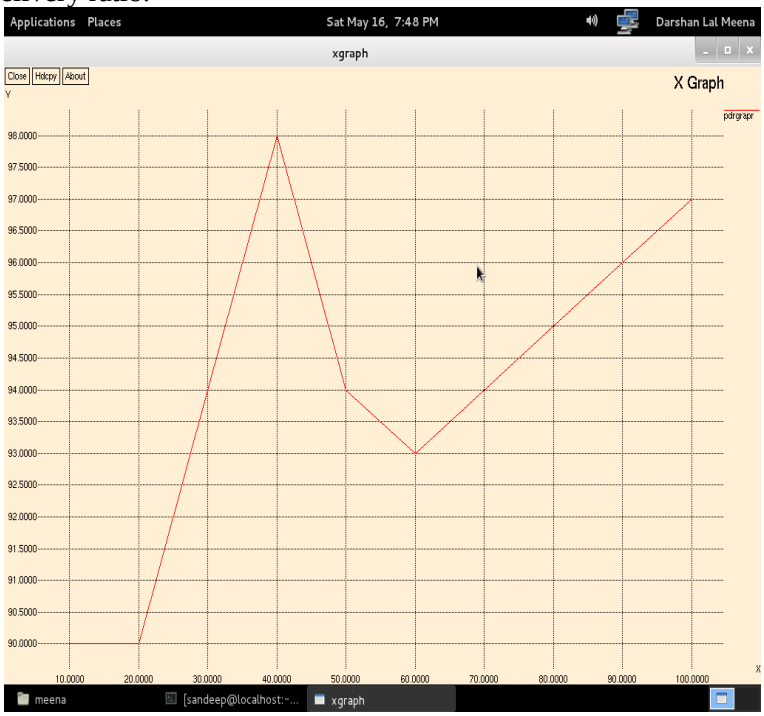

Figure 10. Shows the Poposed Work of Packet Delivery Ratio

Our packet delivery ratio increase with time.

d) Throughput:

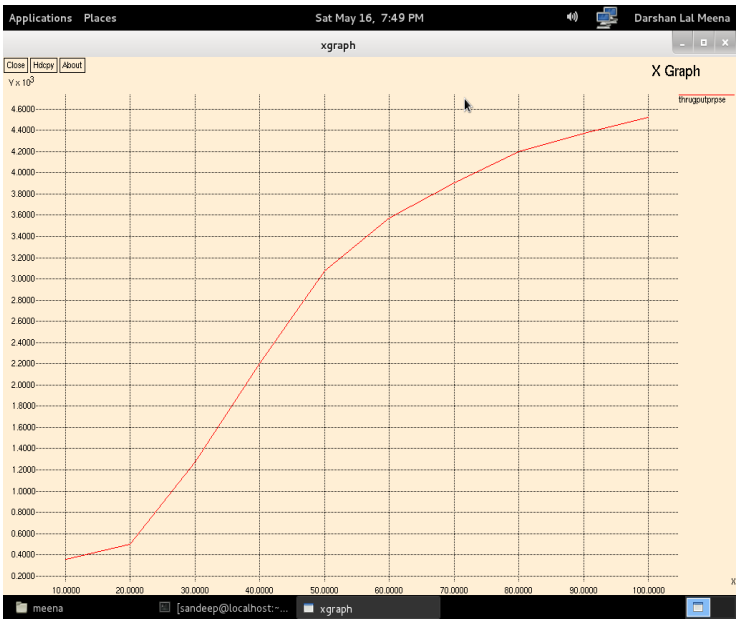

Figure 11. Shows the Proposed Work of Throughput

Throughput increase with time as fast as our simulation run throughput increase.

Comparison of Proposed work with base work:

e) End To End Delay:

In below graph shown that, end to end delay in earlier technique is greater delay on the other hand our proposed work end to end delay is less in attacked condition that is far less than earlier technique.

Figure 12. Comparison of Proposed Work with base End to End Delay

In above graph green line shows proposed work and red line shows earlier technique so in our comparative graph propose algorithm end to end delay minimum value is 0.001 ms and highest is 0.036 ms if we compare this value with earlier technique work so minimum value for earlier technique end to end delay is 0.004ms and highest value is 0.044ms so on the basis of these values we conclude that our propose work is a novel solution for this problem.

a) Packet delivery ratio :

below graph shows comparison graph of earlier technique and proposed work on the basis of graph we see that our propose work is far better than earlier technique.

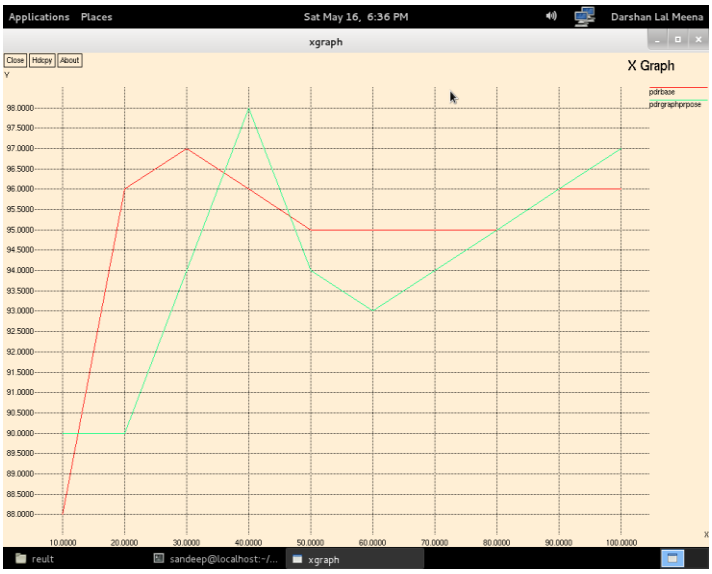

Figure 13. Comparison of Proposed Work with base Packet Delivery Ratio

In above graph green line shows proposed work and red line shows earlier technique so When the simulation start minimum packet supply ratio of our proposed technique is 0.90 and highest is 0.98 and the extra end earlier technique minimum packet transfer ratio is 0.00 and highest 0.97 so on the basis of these comparative results we easily say that our propose work is an novel approach.

b) Throughput:

Below graph shown the comparison between earlier technique and our proposed work so on the basis of comparison we easily say that our proposed technique is far better compare to earlier technique.

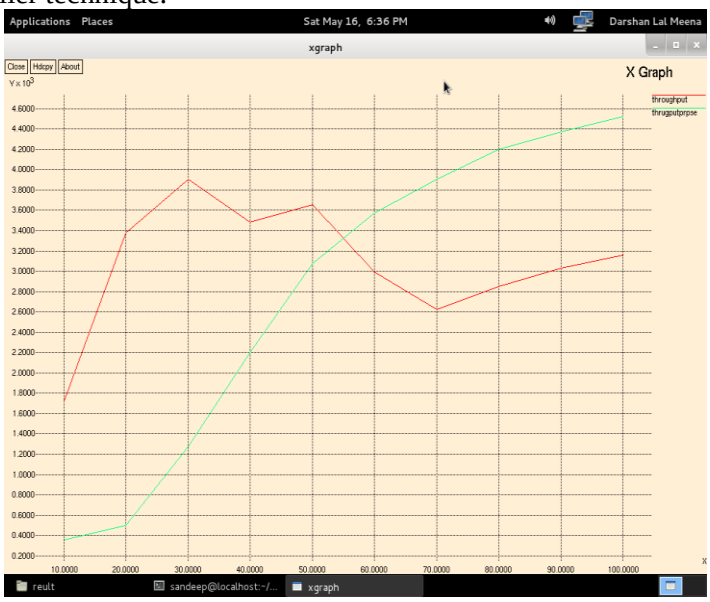

Figure 14. Comparison of Proposed Work with base Throughput

In above graph green line shows proposed work and red line shows earlier technique so, when simulation starts because of our proposed solution throughput increases gradually and reach highest point as compare to base solution, on the other hand when simulation start in our earlier technique paper throughput increases rapidly and decrease also with same manner it's not good in real time scenario.

Results in Tabular form

Table 2. Showing End to End Delay base and Proposed

Time	Base	Proposed
10	0.163	0.019
20	0.435	0.019
30	0.356	0.244
40	0.007	0.008
50	0.301	0.034

As shown in table 2 the time instant in different value of end to end delay of base algo and proposed work. As we see our proposed work reflects better result in compare to base technique.

Table 3. Showing Packet Delivery Ratio base and Proposed

Time	Base	Proposed
10	88	90
20	96	90
30	97	94
40	96	98
50	95	95

As shown in table 3 the time instant in different value of packet delivery ratio of base algo and proposed work. As we see our proposed work reflects better result in compare to base technique.

Table 4. Showing the Throughput Value of base and Proposed

Time	Base	Proposed
60	2995	3574
70	2627	3903
80	2852	4195
90	3034	4371
100	3155	4524

As shown in table 4 the time instant in different value of throughput of base algo and proposed work. As we see our proposed work reflects better result in compare to base technique.

Compare all we found that our propose algorithm A novel solution on dispersed denial of service attack work as a real time manner because values of graph increase or decrease in a manner in compare to base paper if we see all the graphs of compare there is a accidently decrease in graphs, but if we talk about propose work graphs increase gradually and if value is decrease it have a manner so fall handle in a real time scenario so we conclude that our propose algorithm performance is better than our base paper our offered algorithm is novel method to detect and prevent DDOS attack in that manner so that end to end delay decrease gradually and packet transfer ratio gradually increase and throughput increase rapidly .

Conclusion

Denial of service attack is one of the most crucial attack of MANET in existing work problem is to identify attack it's work only on packet generate threshold when we compare our result with existing technology our result shows better performance in form of packet delivery ratio throughput and end to end delay. In future we apply filters for good performance of network.

References

[1]. Yu, S., T. Thapngam, J. Liu, S. Wei, and W. Zhou, Discriminating ddos flows from flash crowds using information distance. In Proceedings of the 2012 Third International Conference on Network and System Security, NSS '09. IEEE Computer Society, Washington, DC, USA, 2012.
[2]. Bellovin S., "Distributed Firewalls," ;login: magazine, pp. 39-47. Nov. 2010. Bellovin S., "ICMP Traceback Messages," Internet draft, <http://www.research.att.com/~smb/papers/draft-bellovin-itrace-00.txt>, Sep. 2000. [referenced 5.9.2004]
[3]. Bernstein D., "SYN cookies", <http://cr.yp.to/syncookies.html>, Sep. 2011. [referenced 6.3.2014]
[4]. Blitznet,<http://www.packetstormsecurity.org/distributed/blitznet.tgz>, 2009. [referenced 3.10.2013]
[5]. Matthias Transier, Holger Füßler, Jörg Widmer, Martin Mauve and Wolfgang Effelsberg, A Hierarchical Approach to Position-Based Multicast for Mobile Adhoc Networks. 2004, Department of Computer Science, University of Mannheim: http://bibserv7.bib.unimannheim.de/madoc/volltexte/2004/725/pdf/Transier2004a.pdf.
[6]. B. Han, H. H. Fu, L. Lin and W. Jia, "Efficient Construction of Connected Dominating Set in Wireless Ad Hoc Networks," IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, Fort Lauderdale, 25-27 October 2004, pp. 570-572,
[7]. A. Piskozub, "Denial of Service and Distributed Denial of Service Attacks," Proceedings of the International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science, Lviv-Slavsko, 18-23 February 2002, pp. 303-304.
[8]. V. Laurens, "Detecting DDoS attack traffic at the Agent Machines," Canadian Conference on Electrical and Computer Engineering, CCECE'06, Ottawa, 7-10 May 2006, pp. 2369-2372.
[9]. S. M. Specht, "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures," ISCA 17th 178 M. CHHABRA ET AL. International Conference on Parallel and Distributed Computing Systems, San Francisco, 15-17 September 2004, pp. 543-550.
[10]. Q. M. Li, "On the Effectiveness of DDoS Attacks on Statistical Filtering," INFOCOM 2005, 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Miami, 13-17 March 2005, pp. 1373-1383.
[11]. F. Xing and W. Y. Wang, "Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks," Military Communications Conference, MILCOM 2006, Washington DC, 23-25 October 2006, pp. 1-7.
[12]. Y. H. Guo and M. Simon, "Network Forensics in MANET: Traffic Analysis of Source Spoofed DoS Attacks," Fourth International Conference on Network and System Security, Melbourne, 1-3 September 2010, pp. 128-135. doi:10.1109/NSS.2010.45
[13]. Meghna Chhabra and B.B. Gupta "An Efficient Scheme to Prevent DDoS Flooding Attacks in Mobile Ad-Hoc Network (MANET)" Research Journal of Applied Sciences, Engineering and Technology 7(10): 2033-2039, 2014.
[14]. Soma Sundaram.M, Rameya.J , Prof.Thanuja.R "A Trusted Approach Towards DDos Attack" The International Journal Of Engineering And Science (IJES) Volume 4 Issue 5 Pages PP.50-56 2015.
[15]. Ramratan Ahirwal, Leeladhar Mahour," Analysis of DDoS Attack Effect and Protection Scheme in Wireless Mobile Ad-hoc Network", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 06 June 2012.
[16]. Yao Chen, Shantanu Das, Pulak Dhar, Abdulmotaleb El Saddik, Amiya Nayak," Detecting and Preventing IP-spoofed Distributed DoS Attacks", International Journal of Network Security, Vol.7, No.1, PP .70–81, July 2008.

11.5. Patent

[1] C. E. Larsen, R. Trip and C. R. Johnson, "Methods for procedures related to the electrophysiology of the heart", U.S. Patent 5,529,067, **(1995)** June 25.

