DDOS Attack Detection on Wireless Sensor Network using DSR Algorithm with Cryptography

Amandeep Kaur
Student
SBS STC, Ferozepur

Daljeet Kaur
Associate Professor
SBS STC, Ferozepur

Gagandeep
Assistant Professor
SBS STC, Ferozepur

ABSTRACT

Nowadays, distributed denial of service (DDoS) attacks creates one amongst the foremost serious security threats to the web. DDoS attacks may result in a very nice harm to the network service. The DDoS attackers typically utilize an outsized variety of puppet machines to launch attacks against one or additional targets, which might exhaust the resources of the victim facet. that produces the victim loses the potential to serve legitimate customers and forestall legitimate users from accessing info or services. Since DDoS attacks will greatly degrade the performance of the network and square measure troublesome to find, they need become one amongst the foremost serious security challenges to this intrusion detection system (IDS). within the existing analysis work the various varieties of issues, such perspective in terms of police work DoS attacks is to look at downside the matter as that of a classification problem on network state (and not on individual packets or alternative units) by modeling traditional and attack traffic and classifying this state of the network nearly as good or unhealthy, thereby police work attacks after they happen. Another is that the Transmission failures or point misses might lead to disturbances to the method, degradation of the management performance. of these square measure resolved with the assistance of a DDoS attack detection and DSR algorithmic rule with Cryptography on Wireless device network and therefore the WSN with bachelor's degree, CH and calculate the various parameters like Residual Energy, Throughput, Packet delivery quantitative relation, Delay and packet ratio etc. All the work is enforced in NS2 and obtaining the utmost results.

Keywords

DDoS, BS, CH, WSN, Attacks etc.

1. INTRODUCTION

In this sense, DoS, particularly DDoS, not solely threatens the net, however additionally threatens the civil security, as a result of its rife usage in cyber-crimes. therefore to know well the characteristics of DDoS issues and investigate corresponding defense mechanisms have vital contributions not just for domain and business, however additionally for the social insurance and emergency management agencies, since they'll use such data to reinforce their skills of risk assessments and facilitate the stakeholders to form acceptable selections once facing DDoS threats. Since DDoS issues will create large injury and have the massive impact on legitimate net usage and civil security, within the last decade, a lot of and a lot of researchers from the domain, business and additionally government organizations devoted themselves into this analysis space. although several solutions were projected to unravel the DDoS downside and a few sorts of the attacks area unit so countered, DDoS attacks still be a main threat within the net. in keeping with the report from Arbor Networks [3] the dimensions of the DDoS attacks evolved plenty that it absolutely was determined a big increase in the prevalence of attack rates within the ten Bbps Vary. The frequency of DDoS attacks, although isn't as high as the year 2000 to the year 2004, remains removed from extinction. Fig. 1 and Fig. 2 show the dimensions and frequency severally.

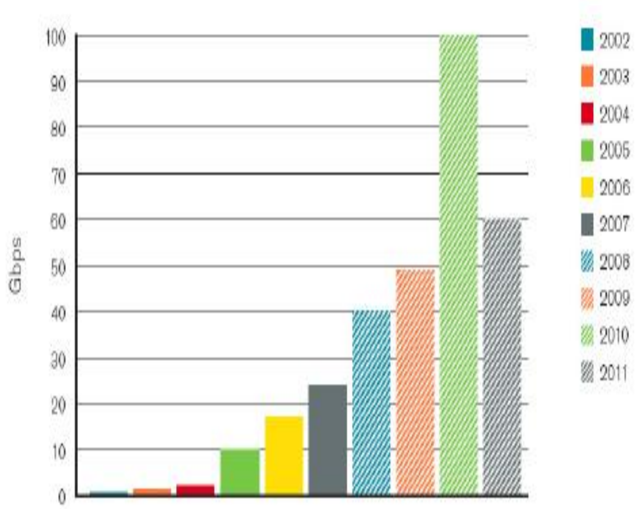


Fig.1: The largest bandwidth attacks reported from 114 service providers. Source: Arbor Networks [1]

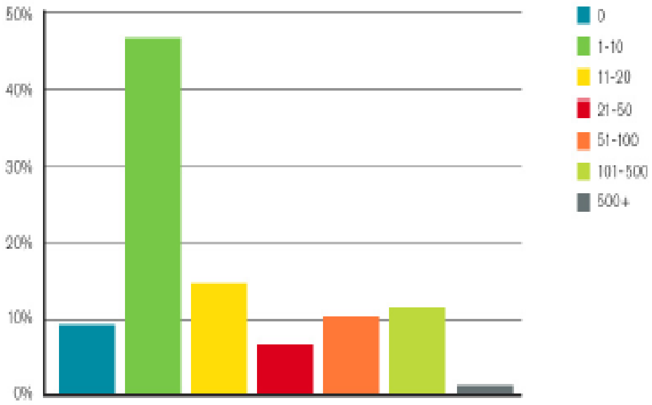


Fig. 2: Average number of DDoS attacks per month during October 2010 to September 2011, based on the reports from 114 service providers throughout the world. They can see that there are around 45% of the respondents encountered DDoS attacks 1-10 times per month. More than 10% of the respondents encountered DDoS attacks 101-500 times per month. Source: Arbor Networks [1]

2. BANDWIDTH AND RESOURCES ATTACKS

The DDoS attacks can even be divided as information measure attacks and resources attacks in terms of the target of DDoS attacks. For the information measure attack, there are sometimes 2 sorts of DDoS attacks, namely, denial of edge service and denial of network service attacks [5], that are shown in the Fig. 3 and Fig. 4. For the previous sort, the attackers sometimes attempt to saturate the ingress information measure of the victim aspect. The reflector attack belongs to the previous sort, which may render traditional users ineffectual to receive responses from the server on time. throughout a resource attack, the wrongdoer principally tries to send an outsized range of virtual connections so as to exhaust hardware and memory resources of the victim. Since the resource of the host is prescribed, an outsized range of broken connections can end in the incapacity of the server to reply to legitimate users.

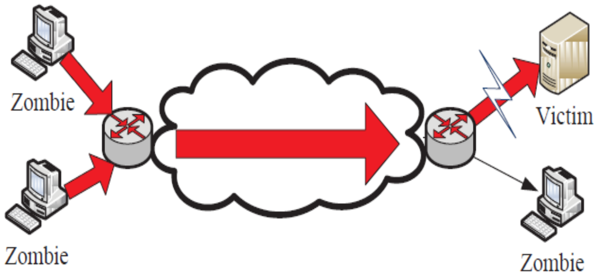


Fig.3: Denial of edge service

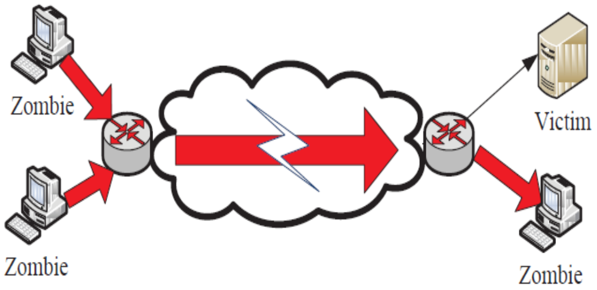


Fig. 4: Denial of network service

3. WHY DDOS ATTACKS EXIST?

The prevalence of DDoS attacks these days is especially as a result of the look goal of the web [6]. within the history, the look goal of net chiefly targeted on practicality instead of security and therefore the network tries to supply easy, quick and low-cost communications. Those sophisticated functionalities are appointed to finish hosts. underneath such best efforts principle, the network itself was designed with delivery potency while not considering security problems. it's not possible for the today's net to manage the behavior of end-hosts. The attackers invariably attempt to notice enough vulnerable hosts and deploy them into their BotNet. The attacks are launched as a result of several reasons like annoying, extortion, or attempting to disable opponent's network operations. However, the web itself has no plan regarding the attacks and it'll invariably strive its best to forward malicious packets to the destinations. what is more, it solely takes a bit value for attackers to cause giant scale damages? that's why DDoS attacks become the foremost fashionable attack suggests that for the attackers. Current DoS attacks are sometimes extended to the distributed version of DoS. There are 2 main reasons for that. Firstly, the targets are usually extremely provisioned servers, and one machine sometimes cannot overwhelm such a server. By using an outsized range of zombie machines, the wrongdoer will simply take down a strong server. Secondly, by victimization several compromised machines, it's laborious for the defense theme to trace back the supply of attacks.[7]

4. DDOS DETECTION

Systems accustomed sight DDoS attacks are thought-about as a kind of Network Intrusion Detection Systems (NIDS). The latter use 2 distinct approaches to sight malicious activities: signature-based detection and anomaly-based detection [2]. Signature-based sighting is employed to detect well-known security threats (e.g., a deadly disease or distorted packets) searching for specific patterns (signatures) to look in individual packets. On the opposite hand, anomaly-based NID is employed to sight potential security threats supported abnormal behaviors over a collection of packets. thanks to the character of flooding-based DDoS attacks, wherever each malicious packet could seem legitimate if analyzed on an individual basis however wherever the traffic behavior might suffer abrupt variations (e.g. abrupt will increase of traffic volume), anomaly-based sighting is often accustomed detect flooding-based DDoS attacks. within the recent decade, several anomaly-based detection ways were planned to spot DDoS attacks from network traffic. Basically, these detection ways may be classified into 2 categories: off-line DDoS mining and online DDoS detection. Off-line DDoS mining sometimes attempts to realize attacks by analyzing the most characteristics of feature distributions of the network traffic with some systematic ways, like PCA (Principal element Analysis)) [4, 5] and dominate states analysis [5]. the fundamental plan of PCA is to implant the four-dimensional information into lower dimensional mathematical space within which traditional instances and therefore the anomalies seem considerably totally different. the fundamental plan of the dominant state's analysis is to explore the interaction or dependence among the size of {the information the info the information} by the distinctive set of values (dominate states) to represent or approximate the initial data in their likelihood distribution. Anomalies may be known since their dominant states deviate considerably from the conventional ones. once the network anomalies are known, information cluster ways, like k-means cluster [6], are applied to cluster differing kinds of anomalies along for more identification, correlating anomalies to attacks. to realize correct analysis results, the process procedures of off-line ways are dead on the entire information trace, and these ways sometimes involve pricey computations, e.g PCA involves matrix computations for computing principal parts of the info. therefore the off-line DDoS mining ways will hardly be utilized in online detection, thanks to time and area complexities. However, the analysis results from the off-line anomaly mining will facilitate build the baseline profile for the important time detection. Considering the massive scale of the DDoS attacks, detection over the huge volume of traffic (e.g. multi-10Gbps) is basically difficult [7]. Computation over huge information streams is being studied within the rising field of knowledge streaming, aiming at ways for process huge amounts of knowledge in an exceedingly time period fashion, specified every tuple within the information stream is merely processed once. information streaming computation has been adopted in applications like money markets and mobile phones or MasterCard fraud detection applications [8]. Recently, information streaming has additionally been planned for DDoS detection at high-speed network links, wherever streams of packets are processed by continuous queries to search out abnormal DDoS-related traffic patterns in real time. information streaming queries are cited as continuous as they're perpetually "standing" over the streaming tuples and unendingly manufacturing output results. Most data-streaming primarily based DDoS detection ways specialize in mistreatment are economical and time-efficient algorithmic rule to stay track of the significant hitters, e.g. a supply causation scores of packets to several destinations, within the monitored traffic. One explicit algorithmic rule used is sketch algorithmic rule [9]. The sketch may be a probabilistic outline technique which may sustain giant streaming datasets. It keeps the outline updates mistreatment projection on random vectors to realize area potency with secure probabilistic reconstruction accuracy. However, sketch primarily based solutions don't support continuous observation with the window since the random vectors used for maintaining the sketches are reset once some anomalies are detected or some predefined amount expires. so sketch-based resolution might miss the anomalies spanning consecutive periods. Considering the kinds of DDoS attacks that are within the focus of the previous add DDoS detection, SYN flooding is that the most typical one, since such attacks sometimes cause an imbalance between the quantity of SYN packets and therefore the SYN/ACK or FIN packets [10]. However, observation such imbalance to sight SYN flooding might need the monitor to be deployed at the sting routers, thanks to the routing imbalance. thus solutions which may sight DDoS attacks at the first stage, i.e. at the backbone links, are desired. However, observation high-speed traffic in backbone links is difficult [11]. To sight information measure flooding attacks, change-point detection [11] and ripple analysis [8] were planned. Change-point detection maintains a moving average of every flow and compares the present rate against the moving average; if the dynamic quantitative relation exceeds the edge, then the flow is known as suspicious. ripple detection maps the series of the flow rates into a spectral domain. Since the attack flows and therefore the legitimate flows have distinguishable frequency parts, the presence of attack flows may be detected[12]. However, most of the change-point primarily based and wavelet-based detections solely specialize in police investigation the abrupt changes of the traffic rate, so that they could also be depleted for police investigation association requests flooding, like SYN flooding, since the traffic rate might not increase most in such attacks.[11]

5. RELATED WORK

Akash Mittal et.al.[2011] have studied Internet is the primary medium for communication which is used by number of users across the Network. At the same time, its commercial nature is causing increase vulnerability to enhance cyber crimes and there has been an enormous increase in the number of DDOS (distributed denial of service attack) attacks on the internet over the past decade. In this paper basically summarizing different techniques of DDoS and its countermeasures by different methods such as Bloom Filter, Trace Back method, Independent Component Analysis and TCP Flow Analysis.[1]

Divya Kuriakose et.al.[2013] have studied Network is collection of nodes that interconnect with each other for exchange the Information. This information is required for that node is kept confidentially. There are many security attacks in network. One of the major threats to internet service is DDoS (Distributed denial of services) attack. DDoS attack is a malicious attempt to suspending or interrupting services to target node. Various schemes are developed defence against to this attack. Main idea of this paper is present basis of DDoS attack. Types of DDoS attack, components of DDoS attack, need for Distributed defense system, comparative study of different defense mechanism.[2]

Saurabh Ratnaparkhi et.al.[2013] have studied DoS/DDoS attacks are a strong, comparatively new type of Internet attacks, they have basis some Biggest web sites on the world -- owned by the mainly famous E-Commerce companies such as Yahoo, eBay, Amazon -- became unreachable to customers, partners, and users; the financial losses are very huge. While former security threats could be faced by a tight security policy and active measures like using recalls, vendor patches etc. these DDoS are novel in such way that there is no totally pleasing protection yet. In this paper they classify diverse Forms of attacks and give an indication over the most common DDoS tools. The goal of this paper to is present the idea behind various protecting technique against the DDOS attack.[3]

Darshan Lal Meena1 et.al.[2014] have studied Distributed denial-of-service (DDoS) is a rapidly growing problem. The multitude and variety of both the attacks and the defense approaches is overwhelming. This paper is a survey on the problem of denial-of-service (DoS) and Distributed Denial of Service (DDoS) attacks and proposed ways to deal with it. they describe the nature of the problem and look for its root causes, further presenting brief insights and suggested approaches for defending against DDoS. They point out both the positive and negative sides of each potential solution. Future work identifies and justifies open research issues. This provides better understanding of the problem and enables a security administrator to effectively equip his arsenal with proper prevention mechanisms for fighting against DDoS threat.[4]

Shenam Chugh et.al.[2015] have studied a review on the problem of denial-of-service (DoS) attacks and proposed ways to deal with it. Broadcast authentication is an important application in sensor networks.Public Key Cryptography (PKC) is desirable for this application,but due to the resource constraints on sensor nodes, these operations are expensive, which means sensor networks using PKC are susceptible to Denial of Service (DoS) attacks: attackers keep broadcasting bogus messages, which will incur extra costs, thus exhaust the energy of the honest nodes. In addition, the long time to verify each message using PKC increases the response time of the nodes; it is impractical for the nodes to validate each incoming message before forwarding it. They describe the nature of the problem and look for its root causes,further presenting brief insights and suggested approaches for defending against DoS.[5]

Raksha Upadhyay et.al.[2015] have studied Open nature of wireless sensor networks (WSN) makes it vulnerable to outside attacks. Many security threats like denial of service, black hole, sinkhole etc. may affect the network performance. Distributed denials of service (DDOS) attacks are defined as attacks that are launched by a set of malicious entities towards a node or set of nodes. In this work They propose a solution to prevent WSN from DDOS attack using dynamic source routing (DSR). Energy of concerned nodes has been used for detection and prevention of attack. Qualnet 5.2 simulator is used for implementation of the proposed solution.[6]

6. PROBLEM FORMULATION

In the analysis work huge processing on wireless detector network totally different issues are sweet-faced that are given below:

- a vital such perspective in terms of detective work DoS attacks is to look at downside the matter as that of a classification problem on network state (and not on individual packets or different units) by modeling traditional and attack traffic and classifying this state of the network pretty much as good or dangerous, thereby detective work attacks once they happen. There is a resource overloading downside because of DDoS attacks.
- Another downside is that the down security downside because of attacks.
- Transmission failures or point misses might end in disturbances to the method, degradation of the general management performance.

7. ALGORITHM

Step 1: Scenario setup, Node setup, Routing protocol setup, Source and destination setup setting initial trust value, threshold value setup.

Step 2: Apply flooding process in a mobile ad hoc network to check condition of the links, link scanner infers all links statuses on the basis of data collection from a prior probe flooding process.

Step 3: After that step is to count no of nodes.

Step 4: Check any node mismatch in network If hop count exceeded then System is invalid

Go to End

Else If any node is dropping data or mismatched in hop count then DoS attack and link failure detected inside the network then report to the system

Else

Source can transmit data, Marked system is valid end if

Step 5: Generation of the encrypted security key in which node initialization time is taken as a secure key. After getting the secure key the node is marked as an authenticated node.

Step 6: Calculation of confidence value. The confidence value is derived by using node *threshold value * trust value. This confidence trust value is use to authenticate nodes.

Step 7: Check whether a node has secure key then authentication successful for data transmission and node is marked as the secure node.

Step 8: Test data packet distribution ratio If data packet distribution ratio drops to the given threshold then Starting source node arbitrarily pick the supportive address of any one node neighbor to malicious node Send request toward the node If anyone node reply from other path except neighbor node then take the reverse locating program and direct check data packets Check messages to detect DoS malicious node Data source node give list of DoS attack malicious node

Set alarm packet

Go to End

Else

Go to End

End if

Step9: After that is to find route for secure data transmission. The shortest path is discovered across the node.

Step 10: Select a node to destination If selected node is found in route list then Selected node is marked as secure node and route detection is successful. Route is confirmed for data transmission

Else

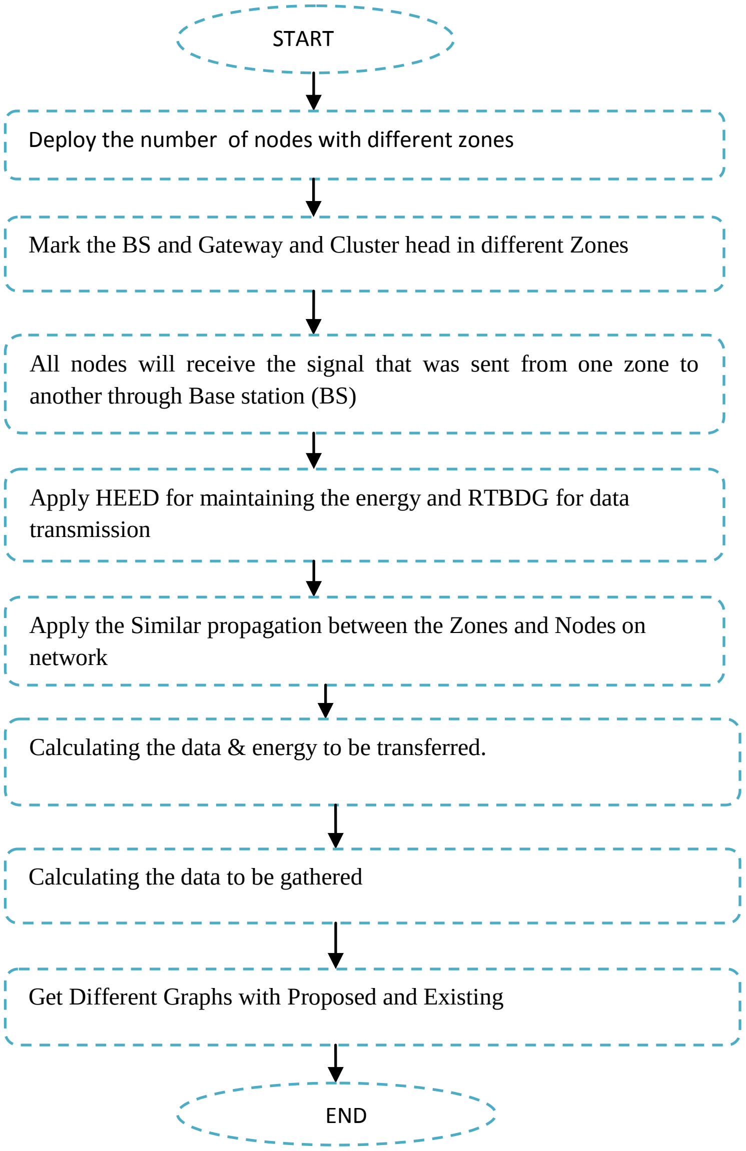
Select another new node, check authentication

End if

Step 11: During data transmission any link may fail so backup node selection method is always used by system for backup node setup.

Step 12: After successful data transmission the route record is maintained by system for future use.

Step 13: End


START
Deploy the number of nodes with different zones
Mark the BS and Gateway and Cluster head in different Zones
All nodes will receive the signal that was sent from one zone to another through Base station (BS)
Apply HEED for maintaining the energy and RTBDG for data transmission
Apply the Similar propagation between the Zones and Nodes on network
Calculating the data & energy to be transferred.
Calculating the data to be gathered
Get Different Graphs with Proposed and Existing
END

8. RESULT & DISCUSSION

This includes the different snap shots for solving the above problems with different objectives. These snap shots are given below:

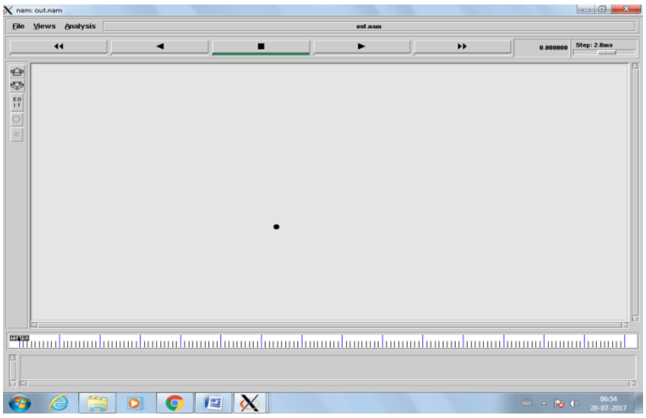
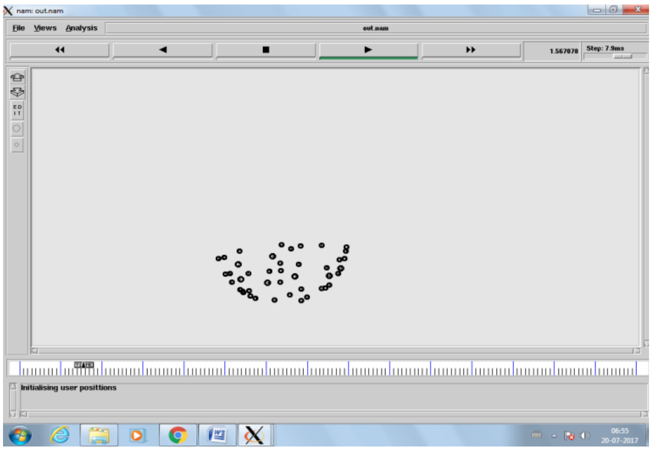


Fig. 5: Initial window for processing the work

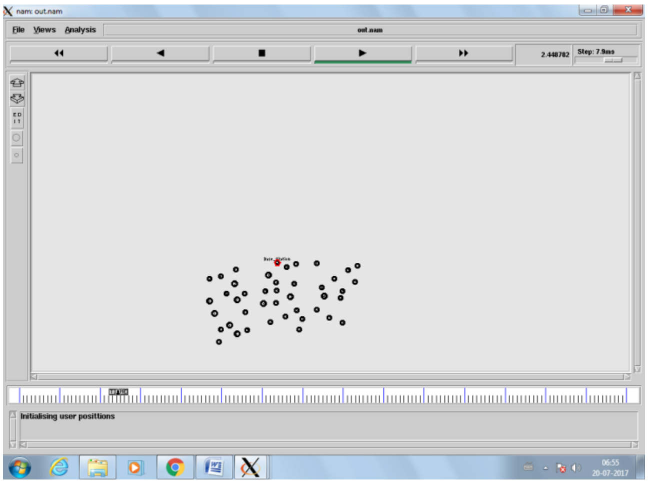
Fig. 5 is the initial window of the work. It includes the number of nodes that are processed on a network.



Initialising user positions

Fig. 6: Nodes deployments on Network

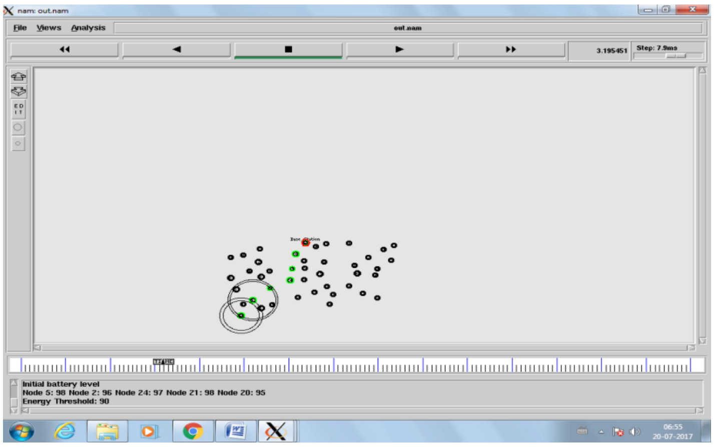
Fig. 6 is the deployments of the nodes on a network. It also displays the number of nodes with different numbers.



Initialising user positions

Fig. 7: BS station with Red color on Network

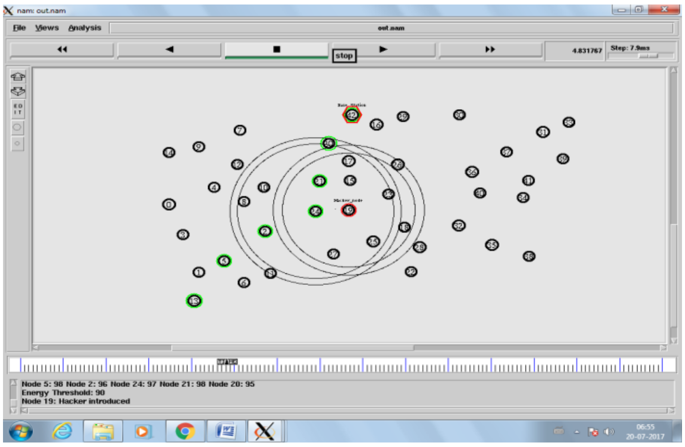
Fig. 7 displays the different nodes on the network. In this network diagram, the Base station is marked with red color.



Initial battery level
Node 5: 98 Node 2: 96 Node 24: 97 Node 21: 98 Node 20: 95
Energy Threshold: 90

Fig. 8: Initial battery level and data transmission

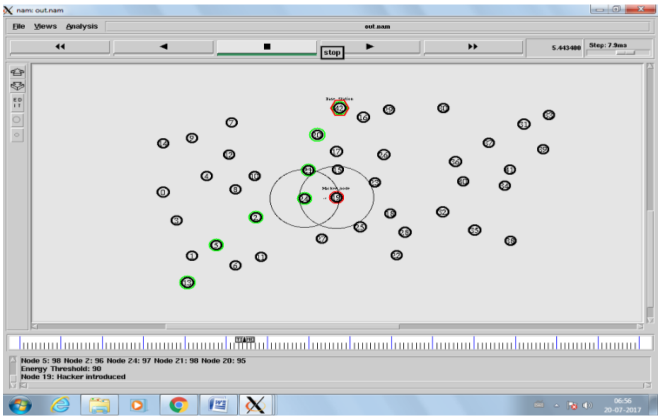
Fig. 8 is the initial battery level and data transmission with different colors. Here in this Fig., the red color is the base station and the green color is the nodes. In which data is transmitted.



Node 5: 98 Node 2: 96 Node 24: 97 Node 21: 98 Node 20: 95
Energy Threshold: 90
Node 19: Hacker introduced

Fig. 9: Attacked Node on Network due to DDoS attack

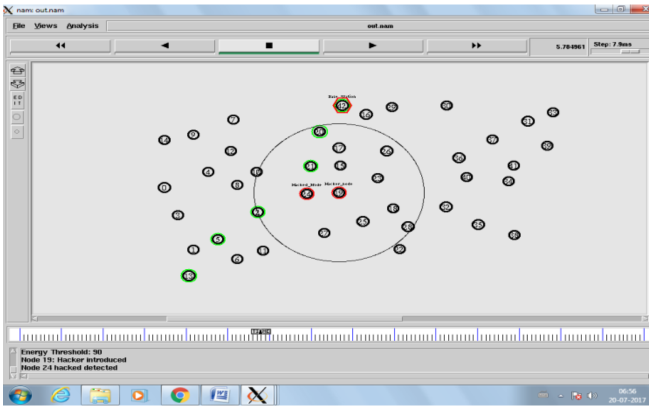
Fig. 9 is the attacked node on the network due to a DDoS attack. In this Fig., the red color node is attacked node and it is marked with attached node.



Node 5: 98 Node 2: 96 Node 24: 97 Node 21: 98 Node 20: 95
Energy Threshold: 90
Node 19: Hacker introduced

Fig. 10: Attacked node and other node data transmission

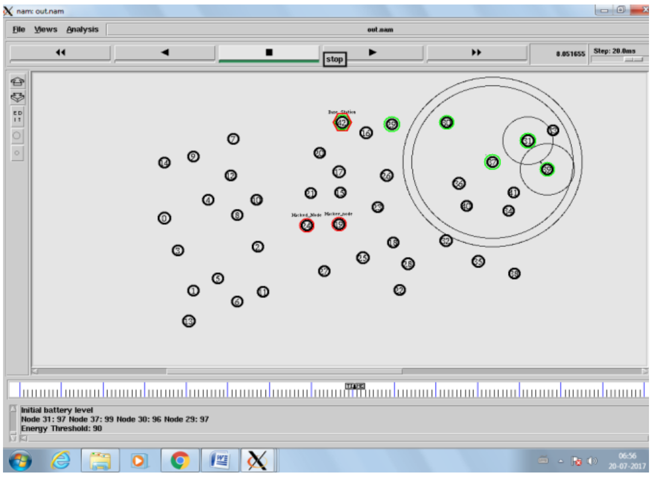
Fig. 10 is the attacked node and other node data transmission. In this diagram green and red node displayed. Green node is the active node and red is the BS and hacked node.



```
Energy Threshold: 90
Node 19: Hacker introduced
Node 24 hacked detected
```

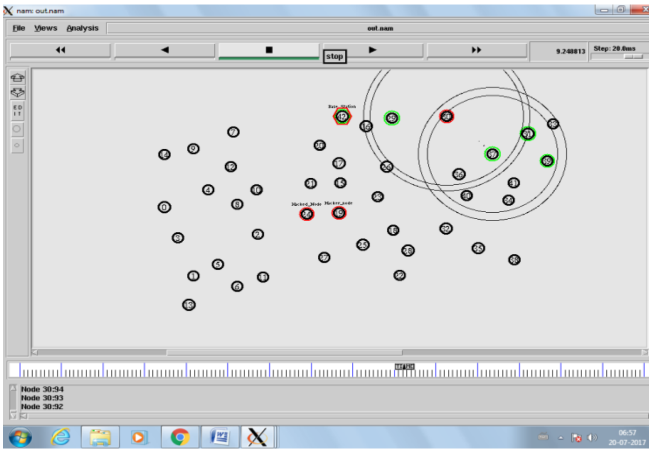
Fig. 11: 2- Attacked node and other node data transmission

Fig. 11 is the Two attacked node and other node data transmission. In this diagram green and red node displayed. Green node is the active node and red is the BS and Two hacked node.



```
Initial battery level
Node 31: 97 Node 37: 99 Node 30: 96 Node 29: 97
Energy Threshold: 90
```

Fig. 12: Node data transmission with signal broadcasting



```
Node 30:94
Node 30:93
Node 30:92
```

Fig. 13: 3- Attacked node and other node data transmission

Fig. 13 is the three attacked node and other node data transmission. In this diagram green and red node displayed. Green node is the active node and red is the BS and three hacked node.

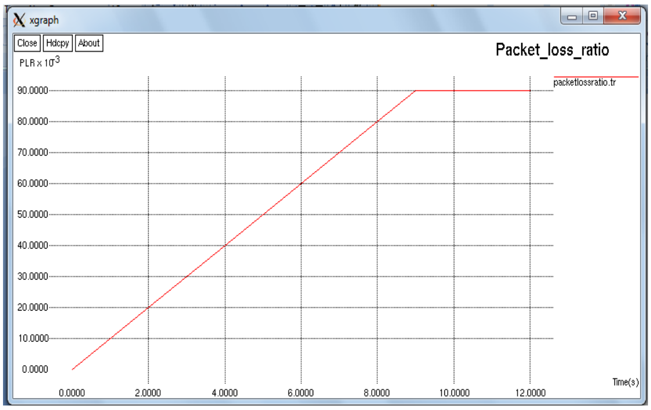


Fig. 14: Packet _loss ratio vs. Time

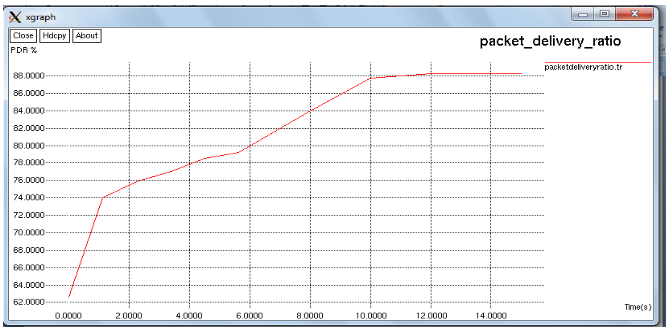


Fig. 15: Packet Delivery ratio vs. Time

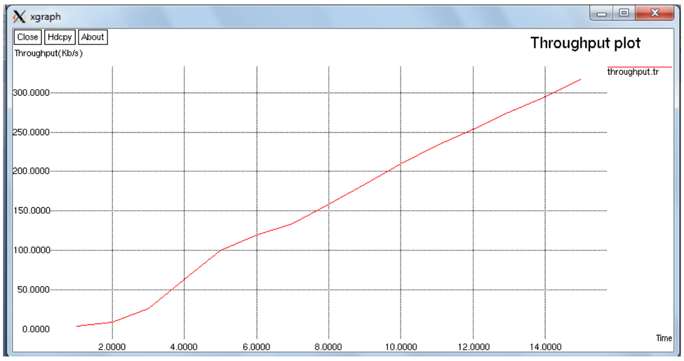


Fig. 16: Throughput vs. Time

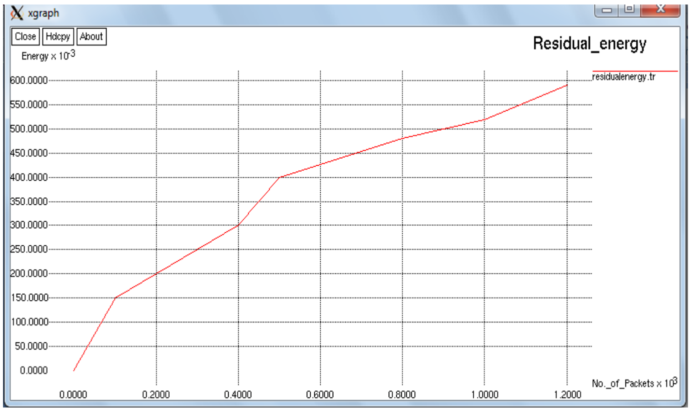


Fig. 17: Residual energy vs. No. of Packet

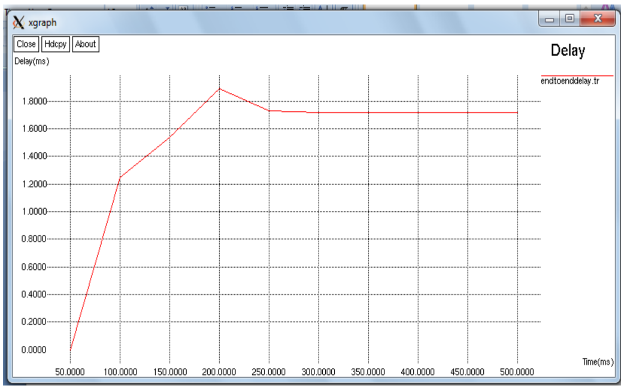


Fig. 18: Delay Vs. Time

9. CONCLUSION &FUTURE WORK

Distributed Denial of Service (DDoS) attack now becomes a great challenge for the various ISP's (Internet Service Providers) as well as researchers who are working in the field of network security in the world. To handle this great challenge a lot of research and work have been done and based on that a lot of recommended models and mechanisms are there. Complete elimination of denial of service threats is infeasible given the current Internet infrastructure. The Internet, being an open environment with no limits set in stone on the number of users, is inherently vulnerable to attacks of the denial of service type. There is no way to predict the parameters of the largest possible flood. In the phone network, the infrastructure is set and it is known what the provisions should be in order to reduce the risks to acceptable levels. Such a provision is hardly imaginable on the Internet, as it is. Discussed approaches and strategies could be combined to offer various levels of mitigation of attacks and disincentive for the attackers, but complete set of tools for defense is currently not available both in the academic and industrial communities. We covered an overview of the DDoS problem, available. Defense challenges and principles, and a classification of available DDoS prevention mechanisms. This provides a better understanding of the problem and enables a security administrator to effectively equip his arsenal with proper prevention mechanisms for fighting against the DDoS threat. The main problem is that there are still many insecure machines over the Internet that can be compromised to launch a large-scale coordinated DDoS attack. One promising direction is to develop a comprehensive solution that encompasses several defense activities to trap a variety of DDoS attack. In this, we are getting 88% packet delivery and other parameters.

10. FUTURE WORK

In the future work other types of attacks like flooding attacks such as ICMP flooding, ACK flooding and scanning activities are removed from the network.

11. REFERENCES

[1] Akash Mittal, Prof. Ajit Kumar Shrivastava, Dr. Manish Manoria "A Review of DDOS Attack and its Countermeasures in TCP Based Networks" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011.

[2] Divya Kuriakose,V.Praveena "A Survey on DDoS Attacks and Defense Approaches" International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 1, Issue 8, October 2013.

[3] Saurabh Ratnaparkhi , Anup Bhange " Protecting Against Distributed Denial of Service Attacks and its Classification: An Network Security Issue" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013

[4] Darshan Lal Meena, Dr. R. S. Jadon " Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches" International Journal of Advance Research in Computer Science and Management Studies , Volume 2, Issue 4, April 2014.

[5] Shenam Chugh, Dr. Kamal Dhanda " Denial of Service Attacks" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 8, August 2015

[6] Raksha Upadhyay, Uma Rathore Bhatt, Harendra Tripathi "DDOS Attack Aware DSR Routing Protocol in WSN" International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015.

[7] Liang Hu, Xiaoming Bi, "Research of DDoS Attack Mechanism and Its Defense Frame,"Computer Research and Development (ICCRD), 3rd International Conference, pp. 440–442, March 2011.

[8] Robert Vamosi, "Study: DDoS attacks threaten ISP infrastructure," Online at http://news.cnet.com/8301-1009_3-10093699-83.html, CNET News, Nov. 2008.

[9] Elinor Mills, "Radio Free Europe DDOS attack latest by hactivists," Online at http://news.cnet.com/8301-10784_3-9933746-7.html, CNET News, May. 2008.

[10] Christos Douligeris and Aikaterini Mitrokotsa, "DDoS Attacks And Defence mechanisms: A Classification," in Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology, (ISSPIT'03), pp. 190-193, Dec 2003.

[11] Nisha H. Bhandari, "Survey on DDoS attacks and its detection defense approach," International Journal of Science and Modern Engineering,Vol.1, Issue.3, pp.67-71, Feb 2013.

[12] S.A.Arunmozhi, Y.Venkataramani,"DDoS attack and Defense in wireless ad-hoc Network," International Journal of Network Security & Its Applications Vol.3, No.3, pp.182-187, May 2011.

[13] Monika Sachdeva, Gurvinddr Singh, Krishnan Kumar, Kuldip Singh, " A comprehensive Survey of Distributed Defense Techniques against DDoS Attack," International Journal of Computer Science and Network Security, Vol.9, No.12, pp.7-15, Dec 2009.

[14] Shibiao Lin Tzi-cker Chiueh," A Survey on Solutions to Distributed Denial of Service Attacks", Department of Computer Science Stony Brook University, pp.1-38, Sep 2006.

[15] Shuchi Juyali, Radhika Prabhakar, "A Comprehensive Study of DDOS Attacks and Defense Mechanisms," Journal of Information and Operations Management, Vol.3, Issue.1, 2012.

[16] Quan Jia, Kun Sun, Angelos Stavrou, "CapMan: Capability-based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET,"proceedings of the 20th international conference on computer communication and networks, pp 1-6, 2011.

[17] Antonio Challita, Mona El Hassan, Sabine Maalouf, Adel Zouheiry, ” A Survey of DDoS Defense Mechanisms ,“ The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[18] Anurekha, R.,K. Duraiswamy, A. Viswanathan, V.P. Arunachalam, K. Ganesh Kumar, A. Rajivkannan” Dynamic Approach to Defend Against Distributed Denial of Service Attacks Using an Adaptive Spin Lock Rate Control Mechanism,” Journal of Computer Science, pp.632-636, 2012.

[19] Puneet Zaroo,” A Survey of DDoS attacks and some DDoS defense mechanisms,” Advanced Information Assurance (CS 626), 2003.

[20] Guangsen Zhang, Manish Parashar,”Cooperative Defense against DDoS Attacks,” Journal of Research and Practice in Information Technology, pp.1-6, 2006.

[21] Wei Ren, Dit-Yan Yeung, Hai Jin, Mei Yang, ”Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks,” International Journal of Network Security, Vol.4, No.2, pp.227-234, Mar. 2007.

[22] Jelena MIrkovic, Max Robinson, Peter Reither, George Oikonomou, “Distributed Defense against DDoS Attacks,” Available: http”//www.isu.edu/~mirkovic/ publication/udel_tech_report_2005.pdf, 2005.

[23] Haining Wang Cheng Jin Kang G. Shin” Defense Against Spoofed IP Traffic Using Hop-Count Filtering,” Networking, IEEE/ACM Transactions on Networking, vol. 15, pp 1-13, 2007.

[24] A.Anna lakshmi, Dr.K.R.Valluvan “A survey of Algorithms for Defending MANETs against the DDoS Attack,” International Journal of Advanced Research in Computer Science and Software Engineering, vol.2, Issue 9, pp.155-164, Sep 2012.