International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 3 Issue 3, March 2014

Estimating the Exposure of Network Mechanisms to High-Tech DDoS Attacks

[1]S.Vasanthi, [2]R.Ravi, [3]Dr. Beulah Shekhar
[1]PG Scholar, Department of Network Engineering, Francis Xavier Engineering College, Tirunelveli.
[2]Professor& Head, Department of Computer Science and Engineering, Francis Xavier Engineering College,Tirunelveli, Tamil Nadu State, India.
[3]Associate Professor, Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu State, India.

Abstract- **The DDoS Attack are launched by malicious nodes, whose only motive is to degrade the performance of other users. To secure and improve the performance. The proposed scheme of anomaly detection to sense the cruel node in the system. In this proposal the training data of received signal strength are rationalized occasionally. The training data includes the convey of control packets in the system. The packet contains the information about the neighbor nodes in the system. The cruel node can be recognized with the help of the received signal strength of the training data and the information is sent to the base station concerning the occurrence of a cruel node in the system. The training data also includes the ridge expanse in the system. We use RSSI algorithm. There are several nodes are created, in that one node acts as base station. The communication and data transmission between the base station and other neighbor nodes are done by using topology discovery, In general DDoS attacks refers to many distributed attacks. The base station receiver many nodes and it analyzes the signal strength of each node by using RSSI, with the help of RSSI indication of the signal strength the base station will list the node which has low signal strength as malicious node and detect it for future use.**

Index Terms—: **Received Signal Strength Indicator (RSSI), Distributed Denial of Service (DDoS), Topology Discovery.**

I.INTRODUCTION

An essential variety of a DDoS attack is effortless, high-bandwidth DDoS attacks. The aim is an extraordinarily huge amount achieved by sending anything knowledge without the use of network resources on the server, the received connection, i.e., bandwidth consumption, and how much traffic it sends simple brute force , flooding becomes a raw socket or zombies , each with a regular user requests follow the using a military transport .The complicated low-bandwidth DDoS goal of their ability to attack by unwanted traffic case affected by the weakness of the system design . It attacks the body's complexity and accepting is needed , a low-bandwidth DDoS attacks, a higher frequency of attacks compared to the three most important compensation : less traffic consumes 1) little price , 2) tiny trace Surprisingly , it is difficult to diagnose , and the work-flow control mechanism protected Settings injury 3) capacity , we focus on advanced low- bandwidth attacks . The complex attack and Quality (RoQ) attacks Reduction: The mainly regular definition is described, including two new huge species of all different attack types.

The initial part of the occupation is a original metric to estimate the blow of difficult attacks, an denial is individual have the preparation. The advance of nasty users to distribute most presentation and complicated scheme of estimate to compensation base for the metric to recommend the utilize of a definite quantity of scheme property. The DDoS attacks metric provides the capability to know the flexibility the systems in the case that a number of steps to get the same problem makes a collection of the mainly flexible. Open and Closed Hash: The next part is a field of metric. The blow feature are testing is used to metric provides the results of weakness, An network algorithms normally used the hash data organization, which is an approximation . The essential discovery are easily testing method will have an effect on designs , The two mainly general types of hash hard to complicated attacks that vary from each other in their collision .

The another part are various sorting algorithms are used in computer networks, Then the collision is an check. The first come first served (FCFS) is instruct to address a extremely straightforward. while the attack are under this structure , " we have to stay like each one else ," so it can instruct to demonstrate that they have no categorize of their use of space and they are still on regular the similar amount of resources then users are the common reason are important injured . This approach are immediately basic nasty users submits the big jobs . In fact the level of exposure the system can be infinite. finally the another one is an open or closed hash computer system , or in the case of an attack ,Therfore the attack are still behind the end of normal users still shows the act as suffers . The results show that a data structure whose amortized complication , still if an attacker manages to O (1) , such as open hash .they are combined with the organization of the array is susceptible to malicious attacks . even though the data structure itself is resistant to essential strikes as waiting in line at the request processing time can increase considerably increase the diversity . As far as we are aware , The first point is to power of the performance . We are using this model preceding it by a row of hash table data structure is a practical and common case analysis of this exhibition ,They are still the accurate size of the die such a way that the " harm " hash mechanism , therefore the attack are ended after the regular users are comparing the force of open and closed hash full denial of service will suffer .

II.PREVIOUS WORK

This indicates that the Open Hash is advanced. The act of together is not distant from that of the “perfect scheme” then each inclusion requires accurately one recollection access to use. However, the further users are nasty, the Open Hash system is extreme and further capable for the entire choice of parameters. In the Post attack Operation difficulty metric the variation between the performances of the two types of Hash is still more important. When the further users are cruel, the Open Hash system is extreme and is well-organized for the entire variety of the parameters and stays. The perpendicular axis is depicting in log scale, specifically, the gap among the utilization of usual and cruel users is extremely huge in mutual models. The easy advance of relying on difficulty based regulations of operations in charge to observe the act of needs of a system. The attack strength measures and estimates the quantity of act deprivation inflicted by an attacker according to his resources. Clearly, strength can be global to compute any complicated attack.

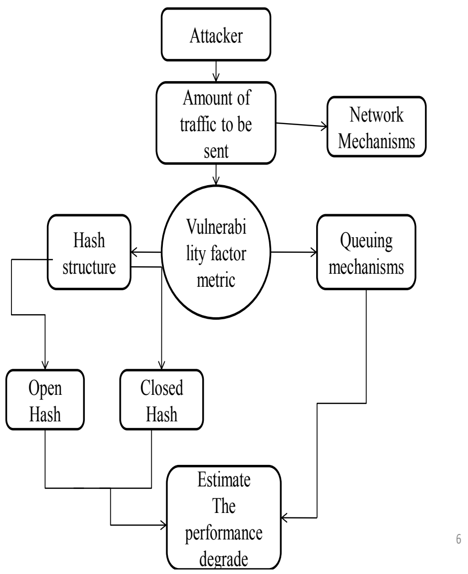

Fig 1: System Overview

From the figure, the attacker sends the amount of traffic to the network mechanism. Server are used to measure the vulnerability factor metric. It follows two techniques; Queuing mechanisms and Hash structure. The queuing mechanism serves in FCFS order,i.e. it Responds to the client, which is first in priority. Hash structure contains two methods, they are Open hash technique and Closed hash technique. When compared to the open hash the closed hash technique is more vulnerable. At last, we estimate the performance degradation.

III.PROPOSED SCHEME

The proposed scheme of anomaly detection to sense the cruel node in the system. In this proposal the training data of received signal strength are rationalized occasionally. The training data includes the convey of control packets in the system. The packet contains the information about the neighbor nodes in the system. The cruel node can be recognized with the help of the received signal strength of the training data and the information is sent to the base station concerning the occurrence of a cruel node in the system. The training data also includes the ridge expanse in the system. The scrutiny with training data is used to safe our system from any kind of attack in the network.RSSI algorithm is used in wireless environment. to secure and improve the performance level we use RSSI algorithm.RSSI is the relative received signal strength.RSSI is an indication of the power level being received by the antenna.therfore the higher the RSSI number, the stronger the signal. The end user will likely observe the RSSI value when measuring the signal strength.

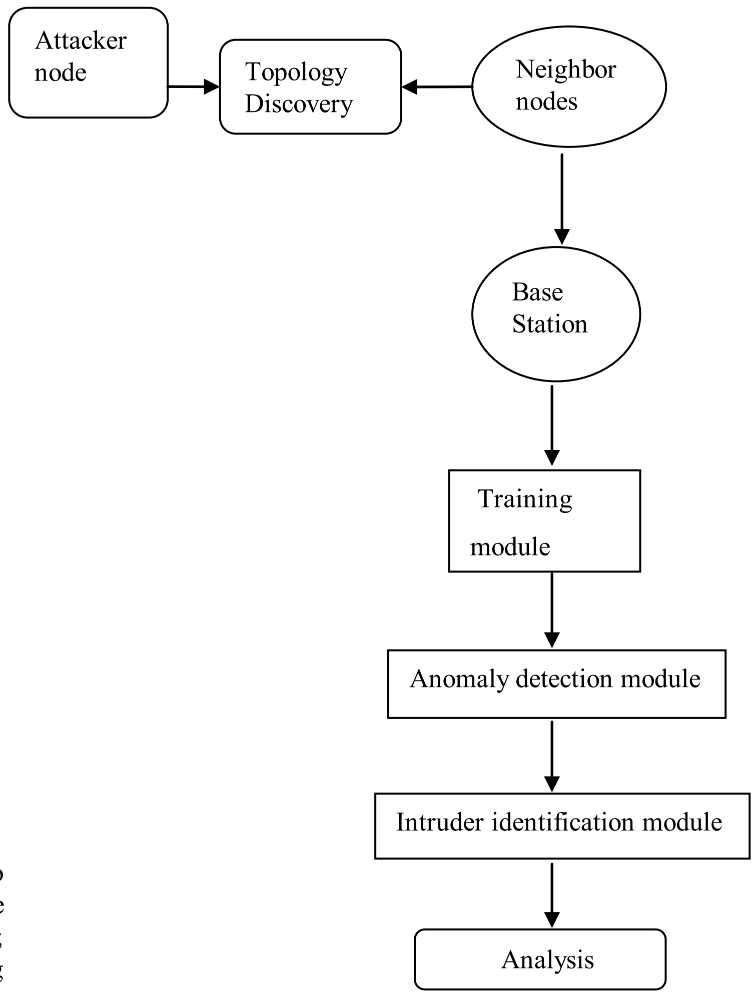

Fig 2: Proposed overview

RSSI Algorithm:

RSSI algorithm are used to create several nodes, in that one node acts as base station. The communication and data transmission between the base station and other neighbor nodes are done by using topology discovery, In general DDoS attacks refers to many distributed attacks. The base station receiver many nodes and it analyzes the signal strength of each node by using RSSI, with the help of RSSI indication of the signal strength the base station will list the node which has low signal strength as malicious node and detect it for future use.

Modules:

1) *Training module:*

In this module we get the training data by running the simulation without any attackers. The numbers of RREQ, RREP, RERR packets that are send or received by a particular node in the network are recorded in the files for every 5msec. These training data are used for the comparison of the number of control packets that are send or received in the network under attackers. If the existing of control packet in the network is more then we can find that network is under attack.

2) *Anomaly detection*:

The principle component analysis is the method used to explores the correlations between each feature. The comparisons is done by analyzing the number of control packets which is transmitted or received in the network at the normal state and the network with the attackers.

3) *Intruder identification module:*

In this module the detected attacker's ids are informed to all the nodes in the network in order to avoid the hacking of data from the nodes in the network.All nodes in the network send the data to base station, then the base station analyses the received signal strength of all nodes in the network then the stronger received signal strength is identified as malicious node.

4) *Analysis:*

In this module the attacks are analyzed using the graphs. If the analyzed data is not in the normal form then we discard that data otherwise we store the data in the training files.

IV.RESULT ANALYSIS

The simulation results were conducted with the help of the Network Simulator. The network is running on a laptop with intel3 core, Processor CPU and memory 3-GB RAM. The intention is to provide simulation results and make it easier to compare the results. In NS 2, the nominal configuration has 65 nodes in a flat space. Throughput arises from 0.00 to 80.00kb/s.In order to measure and compare the performance of proposed scheme, consider the following two parameters. Packet delivery ratio (PDR)**:** Packet Delivery Ratio defines the ratio between the number of packets received by the target node and the number of packets sent by the source initiator node. The comparison graph has been plotted between the malicious nodes and Packet Delivery Ratio. In the existing system the packet drop ratio increases due to the presence of several malicious nodes ,but in the proposed system the malicious nodes are detected by using RSSI algorithm.

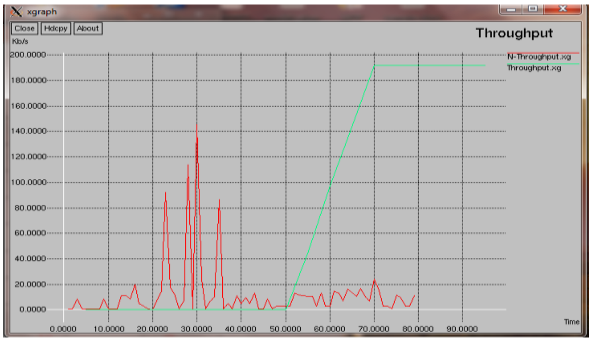

Fig 3:Throughput Analysis

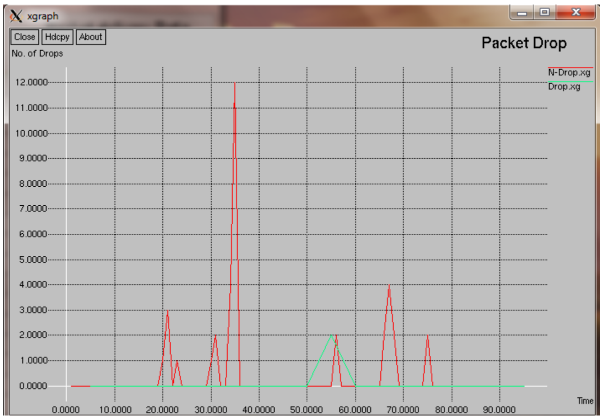

Fig 4: Performance Analysis on Packet Drop

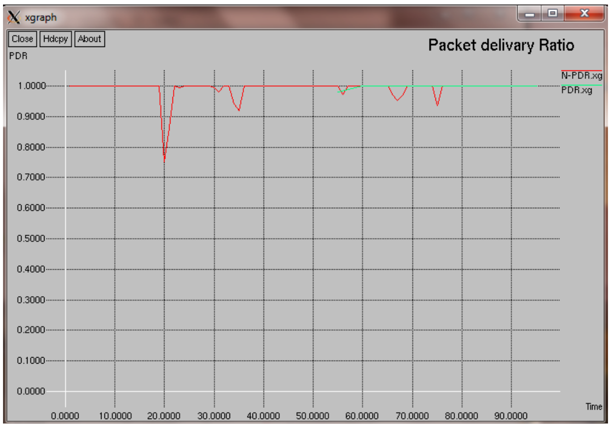

Fig 5: Performance Analysis on Packet Delivery Ratio

V.CONCLUSION

The existing system indicates that the Open Hash is advanced and extreme and further capable for the entire choice of parameters. In the Post attack Operation difficulty metric the variation between the performances of the two types of Hash is still more important. When the further users are cruel, the Open Hash system is extreme and is well-organized for the entire variety of the parameters and stays. The perpendicular axis is depicting in log scale, specifically, the gap among the utilization of usual and cruel users is extremely huge in mutual models. The easy advance of relying on difficulty based regulations of operations in charge to observe the act of needs of a system. The attack strength measures and estimates the quantity of act deprivation inflicted by an attacker according to his resources. Clearly, strength can be global to compute any complicated attack. The proposed scheme of anomaly detection to sense the cruel node in the system. In this proposal the training data of received signal strength are rationalized occasionally. The training data includes the convey of control packets in the system. The packet contains the information about the neighbor nodes in the system. The cruel node can be recognized with the help of the received signal strength of the training data and the information is sent to the base station concerning the occurrence of a cruel node in the system. The training data also includes the ridge expanse in the system. The scrutiny with training data is used to safe our system from any kind of attack in the network.RSSI algorithm is used in wireless environment. to secure and improve the performance level we use RSSI algorithm.RSSI is the relative received signal strength.RSSI is an indication of the power level being received by the antenna.therfore the higher the RSSI number, the stronger the signal. The end user will likely observe the RSSI value when measuring the signal strength. For more performance the RSSI algorithm is used to detect the malicious nodes.

ACKNOWLEDGMENT

First of all we thank the almighty for giving us the knowledge and courage to complete the research work successfully. I express our gratitude to my respected Professor and Head of CSE Dr R.Ravi M.E.,Ph.D., for following me to do research work intentially.

REFERENCES

1. Udi Ben-Porat, Student Member, IEEE, Anat Bremler-Barr, Member, IEEE, and Hanoch Levy, Member, IEEE, 'Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks' IEEE Transactions On Computers, Vol. 62, No.5, May 2013.
2. C. Labovitz, D. McPherson, and F. Jahanian, 'Infrastructure Attack Detection and Mitigation'Proc. ACM SIGCOMM Conf.Applications, Aug. 2005.
3. TCP SYN Flooding and IP Spoofing Attacks, CERT, http://www.cert.org/advisories/CA-1996-21.html, Sept. 1996.
4. S.A. Crosby and D.S. Wallach, 'Denial of Service via Algorithmic Complexity Attacks' Proc. USENIX Security Symp., Aug. 2003.
5. A. Bremler-Barr, H. Levy, and N. Halachmi, 'Aggressiveness Protective Fair Queuing for Bursty Applications' Proc. IEEE Int'l Workshop Quality of Service (IWQoS), Jun. 2006.
6. M. Guirguis, A. Bestavros, and I. Matta, 'Exploiting the Transients of Adaptation for RoQ Attacks on Internet Resources' Proc. IEEE Int'l Conf. Network Protocols (ICNP), Mar. 2004.
7. M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, 'Reduction of Quality (RoQ) Attacks on Internet End-Systems'Proc. IEEE INFOCOM, Mar. 2005.
8. A. Kuzmanovic and E.W. Knightly, 'Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants)' Proc. ACM SIGCOMM Conf. Applications, Aug. 2003.
9. M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, 'Reduction of Quality (RoQ) Attacks on Dynamic Load Balancers: Vulnerability Assessment and Design Tradeoffs' Proc. IEEE INFOCOM, May 2007.
10. Firdous kausar,Eisa al eisa and Imam bakhsh, 'Intelligent home monitoring using RSSI in Wireless Sensor Networks' International journal of computer Networks& communications(IJCNC), Vol.4,No.6,November 2012.
11. Sajid hussian* and Md shafayat rahman, ' Using received signal strength indicator to detect node replacement and replication attacks in wireless sensor networks'.
12. www.google.com

S.Vasanthi is doing M.E Network Engineering in Francis Xavier Engineering College, Tirunelveli. She completed her B.E Computer science and Engineering in V.P.M.M. Engineering College, Srivilliputhur-Virudhunagar in the year of 2012. She published many Conference Papers. She is an active member in Computer Society of India. Her areas of interest are Network Security, Wireless communication and Mobile Technology.

R. Ravi is an Editor in International Journal of Security and its Applications (South Korea). He is presently working as a Professor & Head and Research Centre Head, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. He completed his B.E in Computer Science and Engineering from Thiagarajar College of engineering, Madurai in the year 1994 and M.E in Computer Science and Engineering from Jadavpur Government research University, Kolkatta. He has 18 years of experience in teaching as Professor and Head of department in various colleges. He published 12 International Journals, 1 National Journal. His areas of interest are Virtual Private networks, Networks, Natural Language Processing and Cyber security.

Dr. Beulah Shekhar is a Coordinator for Victimology & Victim Assistance, in the Department of Criminology and Criminal Justice Sciences; she is presently working as a Associate Professor in the Department of Criminology and Criminal Justice Sciences. And her areas of interest are Crimes against Women Empowerment, Human Rights, and Police Training.

