Technique for Mitigation of DDoS attack

Davinder Kaur[#1]

[1]davinderkaur940@ymail.com

***Abstract*— The spatially distributed measurement nodes interface with sensors to monitor assets or their environment. In this research work the DDoS prevention protocol in Cloud is implemented on the basis of ACO optimization scheme. ACO is used to provide a reciprocal path for every link in case of its failure. In this method mutation operator, is used and the new mutation rate is generated by the self-adaptive approach The proposed approach helps to reduce the load and drops in the network, so using the proposed methodology the QOS parameters such as packet delivery ratio, throughput, overheads, average end-to-end delay, average energy consumption are quite improved as shown in the result section. The improvement of 16% is shown between the existing and proposed approach in above defined features.**

***Keywords*— Cloud, VM, VM Placement**

I. INTRODUCTION

A wireless sensing element network could be an assortment of huge variety of sensing element nodes and a minimum of one base station. The sensing element node is associate autonomous little device that consists of in the main four units that are sensing, processing, communication and power provide. These sensors are accustomed collect the knowledge from the setting and pass it on to base station. A base station provides an association to the wired world wherever the collected knowledge is processed, analyzed and conferred to helpful applications. Therefore by embedding process and communication inside the physical world, Wireless sensing element Network (WSN) will be used as a tool to bridge real and virtual setting. Before an attacker is able to attempt any kind of wireless mischief, one of the first activities would be for him to identify the various wireless targets in range. Probing and network discovery type attacks described in this section are amongst the first activities engaged by any attacker. There are primarily 2 main types of probing, active and passive probing. Active probing involves the attacker actively sending probe requests with no SSID configured (very much like a normal wireless client would do) in order to solicit a probe response with SSID information and other information from any access points in range. Active probing cannot detect for access points that are cloaked (configured not to respond to probe requests with no SSID set) or out of range of the attacker's wireless transmission range.

II. DDOS ATTACK

Denial of Quality (DoS) attack is a new style of Distributed Denial of Service (DDoS) attack. DDoS, short for Distributed Denial of Service, is a type of DoS attack where multiple compromised systems -- which are usually infected with a Trojan -- are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack. In a DDoS attack, the incoming traffic flooding the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin. On the other hand in DoS attacks are a new breed of attacks that target adaptation mechanisms employed in current computing systems and networks.The traditional intent and impact of DoS attacks is to prevent or impair the legitimate use of computer or network resources. Regardless of the diligence, effort, and resources spent securing against intrusion, Internet connected systems face a consistent and real threat from DoS attacks because of two fundamental characteristics of the Internet.

The Internet is comprised of limited and consumable resources.The infrastructure of interconnected systems and networks comprising theInternet is entirely composed of limited resources. Bandwidth, processing power, and storage capacities are all common targets for DoS attacks designed to consume enough of a target's available resources to cause some level of service disruption. An abundance of well-engineered resources may raise the bar on the degree an attack must reach to be effective, but today's attack methods and tools place even the most abundant resources in range for disruption.

Internet security is highly interdependent. DoS attacks are commonly launched from one or more points on the Internet that are external to the victim's own system or network. In many cases, the launch point consists of one or more systems that have been subverted by an intruder via a security-related compromise rather than from the intruder's own system or systems. As such, intrusion defence notonly helps to protect Internet assets and the mission they support, but it also helps prevent the use of assets to attack other Internet-connected networks and systems. Likewise, regardless of how well defended yourassets may be, your susceptibility to many types of attacks, particularly DoS attacks, depends on the state of security on the rest of the global Internet.

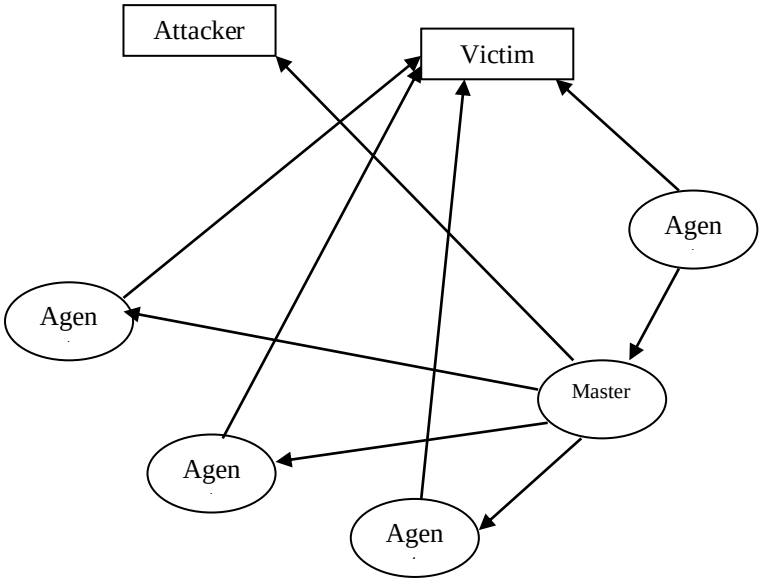

Fig 1: DdoS attack Components

In the attack network architecture of the reflector model, the reflector layer creates a major difference from the basic DdoS attack architecture. In the request messages, the agents change the source address field in the IP header to the victim's address and thus replace the real agents' addresses. Then, the reflectors will in turn generate response messages to the victim. As a result, the flooding traffic that finally reaches the victim computer or the victim network is not from a few hundred agents, but from a million reflectors. An exceedingly diffused reflector based DdoS attack raises the bar for tracing out the real attacker by hiding the attacker behind a large number of reflectors.

III. RELATED STUDY

Shital Patil and Sangita Chaudhari [1] proposed an immune system for the DoS attack on WSN which will improve the accuracy rate of attack prevention, reduce the false alarm rate and able to recognize different Dos attack. Parmar Amish and V.B.Vaghela [2] surveyed techniques dealing with wormhole attack in WSN and a method is proposed for detection and prevention of wormhole attack. AOMDV (Ad hoc On demand Multipath Distance Vector) routing protocol is incorporated into these method which is based on RTT (Round Trip Time) mechanism and other characteristics of wormhole attack.

Poonam Rolla et al. [3] reviewed on DDoS detection and prevention techniques on WSN as WSN become wide spread, security becomes a cardinal affair. One of the terrible threats is Distributed Denial of Service (DdoS) that not only affects the network bandwidth but also affects the performance of the network. A focused on the challenges related to the security of Wireless Sensor Network and began with the concept of WSN. N. Krishna Murthy and R. Selvam [4] investigated the security related issues and challenges in wireless sensor networks as WSN consists of hundreds or thousands of low cost, low power and self organizing nodes which are highly distributed. Security is an important issue nowadays in almost every network. Amit Rathee et al. [5] highlighted WSN, its architecture, challenges, applications and classification of various protocols concerning it. It also classifies various security protocols to make WSN a secure network. Wireless Sensor Network (WSN) is the current research field in computer science & has growing use in day to day life. Poonam Rolla and Manpreet Kaur [6] review on DdoS attacks and their prevention techniques in WSN was performed. DdoS (Distributed denial of service) attack floods unnecessary packets in the sensor network. A new scheme early detection of DdoS attack in WSN has been introduced for the detection of DdoS attack. It will detect the attack on early stages so that data loss can be prevented and more energy can be reserved after the prevention of attacks. Performance of this scheme has been seen on the basis of throughput, packet delivery ratio, no. of packets flooded and remaining energy of the network. Kanchan Kaushal and Varsha Sahni [7] described the security goals and DdoS attack in WSNs. Most of the schemes are available for the detection of DdoS attacks in WSNs. But these schemes prevent the attack after the attack has been completely launched which leads to data loss and consumes resources of sensor nodes which are very limited. Karthikeyan Thyagarajan and Arunkumar Thangavelu [8] discussed various the attack mechanisms and problems due to DdoS attack, also how MANET can be affected by these attacks is presented. In addition to this, a novel approach is proposed to defense against DdoS attacks in Mobile Ad-hoc Networks. DoS attacker, which is on the basic of hierarchical topology structure in wireless mesh networks. Through performance analysis in theory and simulations experiment, the scheme would improve the flexibility and accuracy of DoS attack detection, and would obviously improve its security in wireless mesh networks. Liangyu Luan et al. [9].

IV. METHODOLOGY

Step 1: First of all the nodes will be deployed in network over a specified area.

Step 2: After deployment process the traffic is introduced in the network when nodes generate traffic in network.

Step 3: Now the attack is simulated in the network in form of DDOS attack which will be responsible for denial of services. DDOS attack generates bogus packets in the network so that the resources can be occupied and services may not be delivered.

Step 4: Implement DDOS detection technique i.e. Co-FAIS. This technique introduced fuzzy logics in detection of DDOS attack.

Step 5: In the last step the results and generated and validated by comparing it with Co-FAIS technique.

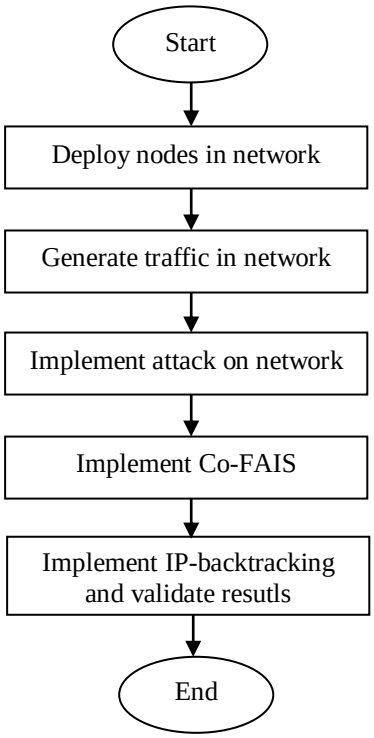

Fig 2: Flow chart

V. RESULTS AND DISCUSSION

In current section with the help of comparative study, we can draw all the pros and cons of the above defined scheduling schemes. In this scenario a comparison is made between hybrid routing schemes by taking 0 to 20 subscriber stations which is shown below.

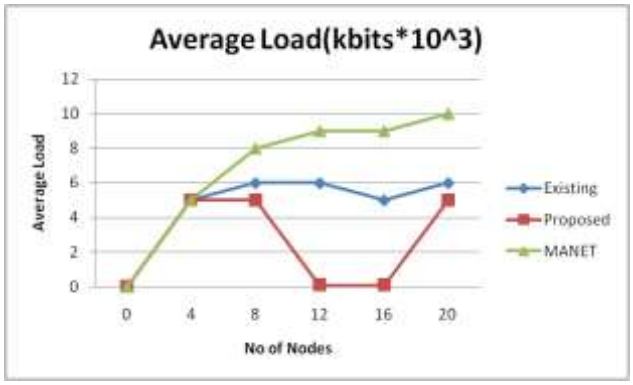

Fig 2: Average load

Load: The load in two DoS mitigation protocols in various nodes. From the above graph it is shown that the load in proposed approach is less than that of existing approach.

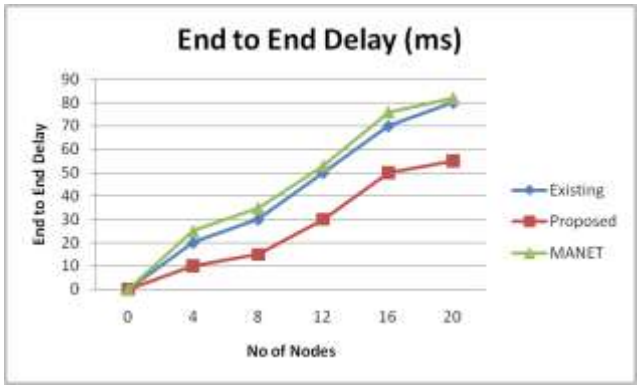

Fig 3: Delay

Delay: Delay in proposed and existing protocol in various nodes. From the graph it can easily depicted that the delay in proposed protocol is less than that of existing protocol.

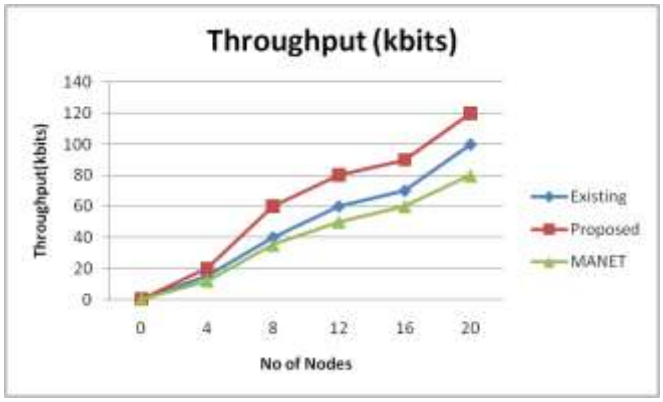

Fig 4: Throughput

Throughput: Throughput in existing and proposed in various nodes. From the graph it can easily depicted that the throughput in proposed protocol is more than that of existing protocol. Throughput in case of proposed case is approx 110 packets and in existing case it is approx 100 packets.

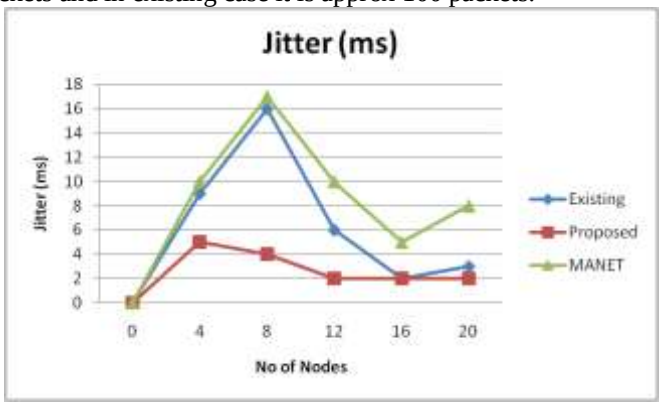

Fig 5.4: Jitter

Jitter: Jitter in proposed and existing protocol in various nodes. From the graph it can easily depicted that the jitter in proposed protocol is less than that of existing protocol. Jitter in case of proposed case is approx 3.5 sec and in existing case it is approx 7 sec.

VI. CONCLUSION

In this thesis, a generalized model for detection has been created by studying the existing models and algorithms on DoS attacks.Internet security is vital to facilitate e-commercetransactions, and there has been continued research effort to provision network traffic monitoring at high speeds. The hardware capabilities achieved by some other approaches like the deep packet inspection [14,15], at relatively low speeds show that our proposed approach can be realizable. That the fast memory, i.e., SRAM, is exorbitantly costly, and the cheap memory, i.e., DRAM, is too slow to work at the high speed line rates, are the two critical considerations in provisioning high speed monitoring. In this section, we briefly discuss some of the recent techniques proposed in the literature that can facilitate realization of the proposed detection system architecture.

VII. REFERENCES

[1]. Shital Patil, Sangita Chaudhari, "DoS attack prevention technique in Wireless Sensor Networks", 7th International Conference on Communication, Computing and Virtualization, Volume: 79, 2016, pp: 715-721

[2]. Parmar Amish, V.B.Vaghela, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol", 7th International Conference on Communication, Computing and Virtualization, Volume: 79, 2016, pp: 700-707

[3]. Poonam Rolla, Manpreet Kaur, Jabarweer Singh, "Review of Prevention Techniques for Denial of Service Attack in Wireless Sensor Network", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 6, Issue 6, June 2016, pp: 281-282

[4]. N. Krishna Murthy, R. Selvam, "Security Issues in Wireless Sensor Network", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 6, Issue 3, March 2016, pp: 233-237

[5]. Amit Rathee, Randeep Singh, Abhishilpa Nandini, "Wireless Sensor Network- Challenges and Possibilities", International Journal of Computer Applications, ISSN: 0975 8887, Volume 140, No.2, April 2016, pp: 1-15

[6]. Poonam Rolla, Manpreet Kaur, "Review Of Prevention Techniques For Denial Of Service (DOS) Attacks In Wireless Sensor Network", International Journal Of Scientific & Technology Research, ISSN 2277-8616, Volume 5, Issue 07, July 2016, pp: 52-54

[7]. Kanchan Kaushal, Varsha Sahni, "Early Detection of DDoS Attack in WSN", International Journal of Computer Applications, ISSN: 0975–8887, Volume: 134, No. 13, January 2016, pp: 14-18

[8]. Karthikeyan Thyagarajan, Arunkumar Thangavelu, "An Integrated Defense Approach for Distributed Denial of Service Attacks In Mobile Ad-Hoc Network", International Journal of Applied Engineering Research, ISSN: 0973-4562, Volume: 11, No. 7, 2016, pp 4898-4910

[9]. Liangyu Luan, Yingfang Fu, Peng Xiao, "An effective Denial of Service Attack Detection Method in Wireless Mesh Networks", International Conference on Medical Physics and Biomedical Engineering, Volume: 33, 2012, pp: 354-360