DoS/DDoS Detection for E-Healthcare in Internet of Things

Iftikhar ul Sami
Graduate School of Science and Engineering
PAF-Karachi Institute of Economics and Technology
Karachi

Muhammad Asif
Lahore LEADS University
Lahore

Maaz Bin Ahmad
Graduate School of Science and Engineering
PAF-Karachi Institute of Economics and Technology
Karachi

Rafi Ullah
Graduate School of Science and Engineering
PAF-Karachi Institute of Economics and Technology
Karachi

***Abstract*—Internet of Things (IoT) has emerged as a new horizon in communication age. IoT has provided platform to various emerging technologies and applications for growth. E-Health services have also been integrated and greatly benefitted from IoT. Due to the increased use of computer technology, computer networks have faced serious security challenges and IoT is also facing the same security threats. As IoT has provided platform to other fields, like E-Health, these services are also prone to such threats. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on E-Health servers in IoT would endanger real-time monitoring of patients and also overall reliability of the E-Health services. In this paper, existing solutions to DoS/DDoS attacks in IoT have been reviewed and a reliable solution is presented for securing the servers against these attacks.**

***Keywords*—E-Healthcare; DDoS attack; Internet of Things**

I. INTRODUCTION

Internet of Things (IoT) integrates various fields of life ranging from Environmental Monitoring, Infrastructure Monitoring, Energy Management, Traffic Management and Healthcare Management. Today, new advancements are being observed in these fields. Basic motives behind theses advancements are to create simplicity in infrastructure and extend reliable solutions to the consumers. Fig. 1 shows the overview of IoT. Due to heterogeneous nature of these technologies, critical applications like traffic system monitoring and healthcare monitoring require special care for transferring their data in timely and secure fashion. Various Metropolitan cities in the world are now benefitting from IoT for real-time traffic monitoring and also integrating various hospitals into IoT for extending patient's health monitoring. Patients are also benefitting from these technologies as they are being continuously monitored without regularly visiting hospitals.

Presently, many hospitals are offering E-Healthcare facilities to their patients and their doctors are continuously engaged in monitoring of these patients. These hospitals are in formal agreement with these patients for extending required services. As these hospitals are geographically located at specific locations of a country, their patients also reside closer or at moderate distance from these hospitals. If these patients need physical checkups then they can easily visit these hospitals.

Fig. 1. Internet of Things.

E-Healthcare is a modernization of medical services, primarily designed to benefit E-Health consumers and health professionals. Fig. 2 shows E-healthcare scenario. Patients who are using sensors on their bodies for monitoring of health conditions are the consumers of E-Health system and doctors, nurses and allied staff who are responsible for extending medical services are the health professionals. Confidentiality of patient's data is very critical and must be secured to prove the reliability of the system. Servers in E-Health systems are very critical as live monitoring of patients is carried out with the help of these servers. If these servers become unavailable for a moment or longer, health monitoring of patients could be jeopardized. Expansion of networks has witnessed increased network vulnerabilities as well as launching of sophisticated attacks by professional hackers on critical resources. E-Health is critical and most challenging field in which availability of network is of prime importance and if the network becomes

under massive attack like DDoS, lifesaving operations of patients may be very difficult. So, there must be a mechanism to ensure reliability and to prevent/detect such kind of attacks.

The contents of this paper are arranged as: Section II is about literature review. In Section III, proposed solution is presented. Section IV is about conclusion and future work.

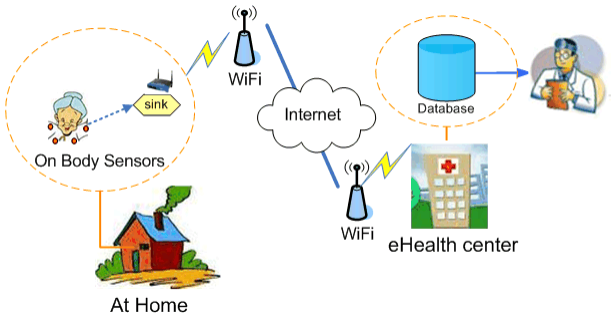

Fig. 2. E-Healthcare System.

II. Literature Review

Authors of [1] have classified DDoS attacks in two categories as flooding and logical (software) attacks. In flooding attacks, they have highlighted SYN flooding, ICMP attack, UDP flooding and in logical attack they have identified ping of death, teardrop attack, and land attack. They have suggested preventing DDoS attacks at edge routers by installing up-to-date patches and by applying filtering at these edge routers. Firewalls can be efficiently utilized by denying protocols, IP addresses and ports to counter the DDoS attacks. They have also highlighted DDoS detection techniques such that signature based detection and anomaly based detection. In this paper, they have suggested countermeasures like using load balancer, Fault tolerance and Quality of Service techniques to counter the threat. Authors of [2] have presented a survey in which they have highlighted various types of DoS/DDoS attacks on network in which they identified UDP flood, ICMP/PING flood/, SYN flood, ping of death. They have also identified the scenarios in which DoS attack can be launched such as Jamming, kill command attack and de-synchronization attacks. In this paper they didn't present any method to prevent Dos/DDoS attack on the network. Authors of [3] have discussed various attacks like Jamming and it can be avoided by using cryptographic techniques (Attribute based and fuzzy attribute based). They have suggested spread spectrum, priority message and cycle duty to counter the jamming and eavesdropping attacks. Collision attack on network can be avoided by applying error correcting codes. Hello flooding attack is used to create confusion in the network. Authors of [4] have identified various defense methods against DDoS like filtering the attack packets, single/multi-source attacks and application of IDS systems. They have suggested adaptive defense mechanism that can adaptively adjust itself according to the attack severity. In adaptive approach they have focused on the value of traffic rate at specific time which obviously is very high at the time of attack. Authors of [5] have analyzed attack pattern on application layer based on entropy of HTTP GET request per source IP address by applying support vector machine classifier. Authors of [6] have proposed a detection scheme based on Information theory in which they have used user browsing behavior. On the basis of entropy, suspicious requests are identified. They have suggested rate limiter to downgrade services to malicious users. Authors of [7] have explored the scope of DDoS flooding attack in various situations and explored various countermeasures according to the situation in which one of the countermeasure is packet dropping, based on the level of congestion.

Authors of [8] have analyzed security measures incollaborative environment and identified various tools and surveys the existing traceback mechanisms to identify the real attacker. Authors of [9] have suggested network architecture and algorithms for countering DDoS attack on IoT server. They introduced a router throttle technique by proposing-leaky bucket rate at server that is under stress. In their proposed solution, they used level-k max-min fairness technique for allocating server capacity amoung routers.

In above referenced papers, researchers have tried different techniques to counter the attacks as there is no specific solution for diverse network situations. With the passage of time, nature and severity of attack is also changing which also needs state of the art techniques to cope with this problem. Some researchers have also tried machine learning approaches to learn the different models for detection of attack which reflects that the use of conventional network analysis techniques alone are not sufficient and it requires various other integrated efforts for securing network resources against these attacks. The basic scenario of DDoS attack is presented in the Fig. 3.

III. Proposed Methodoogy

In our proposed solution we have taken few assumptions such that Server has some normal buffer utilization i.e. 70% or 75% under normal operations. But when its utilization increases from normal range to maximum, it is suspected that server is under DoS attack. Under such situations, an adaptive measures like selective packet dropping methodology to be taken by server to escape from this attack.

In the proposed solution, we have used packet buffer utilization rate of a server and the TTL value of arriving packet and matched both values with pre-determined values for analyzing attack pattern.

As we know that when packet is in the path, its mutable fields are changing at various routers and its TTL value is also decremented at each router. So it is heuristics that packet having less Time To Live value is coming from far distance in the network which indicates that such packets are coming from geographically far distance. These packets might be generated by bots or by some subnets using various DoS attack techniques. Following algorithm have been suggested to check the DoS attack

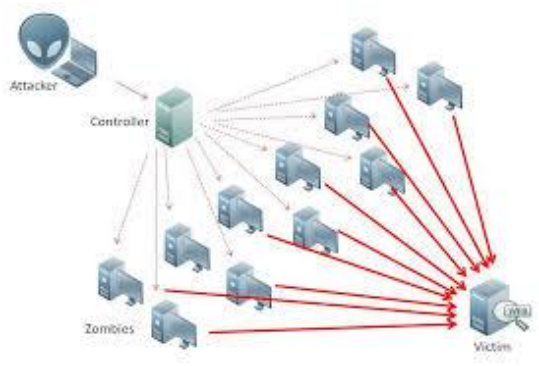

Fig. 3. DDoS Attack.

Algorithm:

1. Read server buffer utilization
2. If buffer utilization > Threshold Value
   // the server is suspected to under DoS attack
3. If (packet TTLvalue < min Value)
   Discard those packets
4. else

   go to step after some specific time

We can also consider geographical locations of nodes. As we know that coordinators (Controller Body Area Network) must be predefined at some geographical locations. By using this information, we can calculate the number of routers (estimated) which may come in the path of a packet to detect DoS attack. As legitimate nodes have some predefined time to send data to a server, and attackers nodes might take longer than normal calculated time.

MTU = 1500 bytes (1460 bytes payload + 40 bytes header)

Data rate of link = d_rate

At coordinator side "A is coordinator"

Time to get data on link by node "A" = TG_A

Packet size in bits = Psize

Data rate in bits = Dr

TG_A = Psize / Dr (1)

Speed or Rate at which data is sent to server = V

Time taken by packet to reach server = T_travel

T_travel = total_dist / V

Time to get packet from link by server (Receiver) = TGs

Note that TGs = TG_A

Total time taken = Total_time

$$Total\_time = TGA + T\_travel + TGs \quad (2)$$

Using this Total_time we can detect DoS attack. By using heuristics, that our actual nodes must have some deterministic time to reach server. We will discard all other packet whose Total_time is greater than some threshold value.

Algorithm:

1. Calculate Total_time for incoming packets
2. if Total_time >= Threshold Value
   // the server is suspected under attack
   discard those packets
3. else
   accept packets

Our proposed solution is based on the assumption that all communicating nodes are present in specific geographical locations (except few, who are temporarily out from the actual zone due to some reasons) and their most likely routes are calculated on pre-commissioning trials. Total packet travel time for a packet at different hours of a day is also taken and threshold rate is calculated based on these packet travel times. Buffer utilization of a server is also calculated based on pre-commissioning trials of the system.

IV. Conclusion

In our proposed solution, we have focused on enhancing server abilities to observe attack pattern and take adaptive measures to handle DoS/DDoS attack. We have also tried not to over burden the edge/path routers for combing these attacks. In our proposed solution, legitimate packets can also be identified by their pre-calculated TTL values and attack packets can easily be identified and dropped before attack reaches its peak point. In this way normal traffic of legitimate users also possible and attack packets filtering in real time is also carried out.

V. Future Work

In our future work, we will apply machine learning approach to enhance the abilities of our system to cope with DDoS attacks. Daily log of our system will be utilized for training of our model and based on training examples, attack behavior could be timely observed and adaptive defense mechanism can be effectively utilized.

There is a problem in our proposed solution. If attacker is from same distance as our legitimate users then our algorithm will detect attack here. For such scenario we proposed multi-layer check. We set some range in which our proposed solution will use some existing methods.

References

[1] A. Srivastava, B.B. Gupta, A. Tyagi, Anupama Sharma and Anupama Mishra, "A Recent Survey on DDoS Attacks and Defense Mechanisms," *Advances in Parallel Distributed Computing*, pp. 570-580, 2001.

[2] Krushang Sonar and Hardik Upadhyay, "A Survey: DDOS Attack on Internet of Things," International Journal of Engineering Research and Development, pp.58-63. 2014.

[3] Masdari, Tahmineh Haddadi Bonab and Mohammad, "Security attacks in wireless body area networks: challenges and issues," Academie Royale Des Sciences D Outre-Mer Bulletin Des Seances, pp. 100-107, 2015.

[4] Muhai Li and Ming Li, "An Adaptive Approach for Defending against DDoS Attacks," Mathematical Problems in Engineering, 2010.

[5] Tongguang Ni, Xiaoqing Gu, Hongyuan Wang and Yu Li, "Real-Time Detection of Application-Layer DDoS Attack Using Time Series Analysis," Journal of Control Science and Engineering, 2013.

[6] S. Renuka Devi and P. Yogesh, "Detection of Application Layer DDoS Attacks using Information Theory based matrics," Computer Science and Information Technology (CS & IT), pp. 217-223, 2012.

[7] M. Young, "A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks," IEEE Communications Surveys & Tutorials, pp. 2046-2069, 2013

[8] Arun, Raj Kumar P., and S. Selvakumar. "Distributed denial-of-service (ddos) threat in collaborative environment-a survey on ddos attack tools and traceback mechanisms." In Advance Computing Conference, 2009. IACC 2009. IEEE International, pp. 1275-1280, 2009.

[9] Yau, David KY, John Lui, Feng Liang, and Yeung Yam. "Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles." IEEE/ACM Transactions on Networking (TON) 13, no. 1 (2005), pp. 29-42.