International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

DDOS Attack Detection and Handling Mechanism In WSN

Amit Dogra, Taqdir

Abstract: ***Wireless sensor network(WSN) uses in many distinct applications including real time event detection. Sensor nodes(SN) have limited energy associated with them that is required to be conserved. Once all the energy of the sensors is drained, then network dies. In addition sensor nodes are exposed to everyone hence SN is susceptible to attacks. Distributed denial of service attack is one of the common attacks caused by malicious attacker causing congestion and decay in lifetime of the network. DDOS attack floods network with the bogus requests. This causes the legitimate request to be avoided by the server due to lack of resources. Detection and prevention of such attacks thus becomes critical. This paper provides study of techniques used to detect DDOS attack along with suggest modification for improving classification accuracy in the detection techniques. in addition this paper also highlight other metrics such as mean time to failure and mean time between failure for improving the detection process.***

Keywords: ***Wireless sensor network, distributed denial of service attack, Mean time between failure, mean time to failure***

I. INTRODUCTION

Wireless sensor network[1] is becoming need of the hour since it is accessible to everyone and uses wireless medium to communicate. This communication needs the sensors to obtain routing information of the neighbouring nodes. The transmission of information from source to destination is dependent upon the topology. The topological advancement leads to efficient transfer of data causing least energy to be consumed. The basic topologies including bus, star and ring topologies are expanded to include energy efficient procedures for communication. [2], [3]Clustering is one of the strategies to minimise energy consumption during transmission in WSN. As the strategies are researched over for reducing energy consumption and increasing lifetime of the network, WSN becomes exposed to malicious users. [4]Malicious users causing the congestion over the network leading to request denial and hence lifetime of the network degrades. [5], [6]The request denial leads to attacks and most common of them is DDOS(Distributed denial of service attack). [7]

Manuscript published on 30 September 2019
* Correspondence Author
Amit Dogra*, Assistant Professor, Department of Computer Science and Engineering at SoET, BGSB University Rajouri (J&K).
Dr. Taqdir, Assistant Professor, Department of Computer Science and Engineering, Guru Nanak Dev University, R/C Gurdaspur.

This attack causes repeated requests to be generated and network bandwidth to be consumed unnecessarily. This paper provides the in-depth into the distributed denial of service attack along with comparative study of techniques used to rectify the problem caused by DDOS attack. The modifications required to improve the techniques is listed in tabular structure and hence is beneficial for future enhancement. Rest of the paper is organised as under:

- Section 2 gives the brief introduction and side effects of DDOS attack
- Section 3 gives the DDOS detection techniques along with comparative analysis of each
- Section 4 gives the research gap
- Section 5 gives the conclusion and
- Section 6 gives the references of the literature used in this survey

II. DDOS ATTACK: OCCURRENCE AND SIDE EFFECT

[8]Distributed denial of service attack causes congestion within the network and hence service denial occurs. The node possessing the resources receives undue requests that block the services and hence starvation is the result. [9], [10]This attack is kind of active attack that distorts the routing process. This attack may be due to presence of node failure un-intentionally or due to malicious attack. In active attack, content to be delivered to the destination is altered and hence this attack is more profound and dangerous as compared to passive attack. Passive attacks do not alter the contents to be delivered and are easy to detect. Rest of this paper discusses only active attack denial of service. The attack of this sort can occur at distinct layers of network.

- Physical layer: This layer can be hampered by sniffing attack that may or may not harm the physical environment required to transmit the data.
- Data Link Layer: Passive as well as active sniffing along with ARP spoofing causes network to deny requests.
- Network layer: Sniffing and denial of service attacks that allow the traffic to pass through it and then attack the route to block it.
- Transport layer: Denial of service hold impact at this layer. In other words this attack is king at this layer. Information about the machines working within the network is disclosed using such attacks at this layer. Services both online as well as offline will be affected through this attack.

- Session and Presentation layers: These layers are not practically tested and hence no attack is yet discovered at these layers.
- Application Layer: This layer is exposed to both active as well as passive attacks. Distributed denial of service is common at this layer.

[7][11][12]The side effect of this attack is congestion and starvation problem. The DoS attacks and it side affect is comparatively given as under

Layer	Task	Attack	Side effects
Physical	Converting data to be transmitted in the form of bits and bytes	Sniffing, DDOS	Starvation and resource wastage. Lifetime of the network decay
Data Link	Forming frames from the bits received from physical layer	Passive and active DDOS attacks	Packet drop ratio increases and lifetime of the network decreases
Network Layer	Receiving data from data link layer and forming packets	Sniffing and denial of service attack	Congestion due to repeated requests
Transport	Using UDP and TCP to locate the route from source to the destination	Denial of service	Service denial at this layer causes unreliability and congestion
Session and presentation	Session establishment and presentation is critical so that receiver can receive the data in understandable format	No attack is disclosed as yet	-------
Application Layer	Protocols necessary for transmission is accommodated at this layer	DDOS, Sniffing and spoofing	Packet loss, lifetime decay

Table 1: Layers, attack types and side effects

DDOS attack hampers the performance of network as packet droop ratio increases along with decay in lifetime of the network. Techniques have been devised to tackle DDOS attack within WSN. Next section describes the mechanisms used to detect DDOS attack within WSN.

III. DDOS ATTACK DETECTION TECHNIQUES

[5]DDOS attack detection mechanisms suffer from issues of high energy consumption while detecting attack along with limited availability of resources. Attacks could be active or passive in nature. Active attacks alter the contents to be transmitted and hence are more dangerous as compared to passive attacks which only sniff but do not alter the contents. DDOS attack detection mechanisms along with merits and demerits of each is presented

DDOS Attack Detection mechanism	Description and Merit	Demerits	Parameter Enhanced	Future enhancement
UDP Flood attack detection[13]	Flood attack detection strategy employ identity detection mechanism to block the packets initiated from source beyond threshold.	High energy consumption due to lack of energy conservation procedures.	Bits per seconds parameters measure the magnitude of attack	Threshold mechanism can be dynamic that should depend upon the traffic flow.
Smurf DDOS Attack detection[14]	Smurf attack minimisation is achieved through bandwidth reservation mechanism to reduce attack percentage	Bandwidth conservation affects utilization of resources and reduces availability	Bits per second and hertz	Resource degradation and wastage must be tackled. This can be achieved by dividing the entire bandwidth into channels and blocking channels having malicious traffic

Syn flood DDOS attack[15]	This attack takes into consideration laid back approach of TCP connection and can be prevented using blockage based strategy where malicious traffic is blocked even before reaching the site	Estimation before the attack is challenging task	Bits per seconds	Filtering strategy to pre-process the traffic could be used to reduce execution time for attack detection
Ping of attack detection strategy[16]	In this attack multiple malicious pings are transmitted to the server to block the services provided by the server. Memory buffer overflow is the problem that is handled efficiently by putting constraint on the memory utilization through the request by the single client.	Legitimate packets could be denied for the resources	Bits per second and Hertz	Blocking contents to be stored within memory must be accompanied with compaction to increase the access rate.
Slowloris detection and prevention[17]	This attack attacks the specific server and makes some specific service down while other ports are unaffected. This attack is detected and avoided by eliminating more than one connection from the client side.	In case client attacks by the use of virtual public network, then this type of attack cannot be detected	Bits per second	Premption in the resource allocation could solve the problem of slowloris
Http flood detection[18]	This type of attack causes the maximum resources to be allotted to the client in response to the Http request but is tackled to apply check on the resource allocation process causing limited resource to be allotted the client	Critical resource could be avoided for allocation and hence resource consumption reduces considerably	Bits per second	Proportionate allocation mechanism with threshold could increase the resource utilization.

Table 2: DDOS attack detection and future enhancements

The most crucial and difficult attack to detect and resolve is Http flood detection. Proportionate allocation with threshold on upper limit on resource that could be allotted to clients could resolve the problem and enhance the performance of the WSN in terms of packet drop ratio and lifetime of the network.

IV. RESEARCH GAP

DDOS attack is a result of exposure of sensor nodes to malicious and unauthorised users. The limited work has been done towards the detection and prevention of Http flood attack. The http flood attack causes large number of resources to be allotted in response to the few requests from the clients. Placing check on the allocation process reduced the problem but also reduces the resource consumption.
To tackle the issue proportionate allocation with check on the number of resources to be allotted to the client could be suggested for future enhancement of the existing strategy.

V. CONCLUSION

This paper presents the comprehensive analysis of the DDOS attack and mitigation strategy. The tackling of attacks is researched over and is discussed through Table 2 in section 3. The flooding is common base from where DDOS attack is initiated and its profound affect is seen in the network and transport layers. The most common method to mitigate this attack is to use threshold on the number of resources to be allotted. This mechanism lowers the chances of DDOS attack but also reduces the availability and resource consumption.
In order to rectify the issue, proportionate allocation with check on the resource allocation is propose in the future endeavours.

REFERENCES

1. S. Muhammad, S. Hussain, and M. Yousaf, "Neighbor Node Trust Based Intrusion Detection System for WSN," *Procedia - Procedia Comput. Sci.*, vol. 63, pp. 183–188, 2015.
2. G. S. Arumugam and T. Ponnuchamy, "EE-LEACH : development of energy-efficient LEACH Protocol for data gathering in WSN," *IEEE Access*, 2015.
3. A. Kaur and H. Kaur, "A REVIEW ON A HYBRID APPROACH USING MOBILE SINK AND FUZZY LOGIC FOR REGION BASED CLUSTERING IN WSN," *IEEE Access*, vol. 16, no. 2, pp. 7586–7590, 2017.
4. M. A. Kafi, D. Djenouri, J. Ben-othman, and N. Badache, "Congestion Control Protocols in Wireless Sensor Networks : A Survey," vol. 16, no. 3, pp. 1369–1390, 2014.
5. A. Kaur, "DDOS Attack Detection on Wireless Sensor Network using DSR Algorithm with Cryptography," *ijca*, vol. 175, no. 3, pp. 16–23, 2017.
6. K. Kaushal and V. Sahni, "Early Detection of DDoS Attack in WSN," *Int. J. Comput. Appl.*, vol. 134, no. 13, pp. 14–18, 2016.
7. M. Hyvarinen, "Detection of Distributed Denial-of-Service Attacks in Encrypted Network Traffic," *Masters Thesis Inf. Technol.*, 2016.
8. L. Barki, A. Shidling, N. Meti, D. G. Narayan, and M. M. Mulla, "Detection of distributed denial of service attacks in software defined networks," *2016 Int. Conf. Adv. Comput. Commun. Informatics*, pp. 2576–2581, 2016.
9. K. Giotis, M. Apostolaki, and V. Maglaris, "A reputation-based collaborative schema for the mitigation of distributed attacks in SDN domains," *Proc. NOMS 2016 - 2016 IEEE/IFIP Netw. Oper. Manag. Symp.*, no. Noms, pp. 495–501, 2016.
10. R. Wang, Z. Jia, and L. Ju, "An entropy-based distributed DDoS detection mechanism in software-defined networking," *Proc. - 14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2015*, vol. 1, pp. 310–317, 2015.
11. N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions," *Arab. J. Sci. Eng.*, vol. 42, no. 2, pp. 425–441, 2017.
12. D. Kim and S. An, "PKC-based dos attacks-resistant scheme in wireless sensor networks," *IEEE Sens. J.*, vol. 16, no. 8, pp. 2217–2218, 2016.
13. S. Kumarasamy and D. R. Asokan, "Distributed Denial of Serivce (DDoS) Attacks Detection Mechanism," *Int. J. Comput. Sci. Eng. Inf. Technol.*, vol. 1, no. 5, pp. 39–49, 2011.
14. Z. Yi, L. Qiang, and Z. Guofeng, "A real-time DDoS attack detection and prevention system based on per-IP traffic behavioral analysis," *Proc. - 2010 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol. ICCSIT 2010*, vol. 2, no. August, pp. 163–167, 2010.
15. Z. Mašetić, D. Kečo, N. Doğru, and K. Hajdarević, "SYN flood attack detection in cloud computing using support vector machine," *TEM J.*, vol. 6, no. 4, pp. 752–759, 2017.
16. B. Kashyap and S. K. Jena, "DDoS Attack Detection and Attacker Identification," *Int. J. Comput. Appl.*, vol. 42, no. 1, pp. 27–33, 2012.
17. V. Bukac and V. Matyas, "Analyzing traffic features of common standalone DoS attack tools," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9354, pp. 21–40, 2015.
18. S. Indraneel and V. Praveen Kumar Vuppala, "HTTP Flood attack Detection in Application Layer using Machine learning metrics and Bio inspired Bat algorithm," *Appl. Comput. Informatics*, 2017.

AUTHORS PROFILE

Dr. Taqdir, Designation: Assistant Professor Qualification:PhD(CSE,NITJalandhar),M.Tech(CSE,),B.Tech(CSE) Department: Computer Science and Engineering Email: taqdir_8@rediffmail.com

Dr. Taqdir is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Guru Nanak Dev University, R/C Gurdaspur. She holds the experience of 17 years in teaching at University level and her area of interest is Digital Image Processing and Machine Learning.

Mr. Amit Dogra Designation: Assistant Professor Qualification: M.Tech, B.E
Department: Computer Science and Engineering
Email: amitdogra004@gmail.com. Amit Dogra is currently working as an Assistant Professor in the Department of Computer Science and Engineering at SoET, BGSB University Rajouri (J&K). He holds a B.E degree in Information Technology and M.Tech degree in Networking and Internet Engineering.