DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5009

ISSN No. 0976-5697

Volume 8, No. 9,November-December 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

DDOS ATTACK ON WIRELESS SENSOR NETWORK: A REVIEW

Priya Pandey
Scholar
Department of CSE
AIST, Sagar (MP), India

Maneela Jain
Assistant Professor
Department of CSE
AIST, Sagar (MP), India

Rajneesh Pachouri
Assistant Professor
Department of CSE
AIST, Sagar (MP), India

***Abstract*:** Controlling the denial of service attacks in the wireless sensor networks are becoming more difficult, and now it seems like a Halloween in network where the ghostly creatures are moving fearless. On the other way, this also obstruct the understanding of DDoS phenomenon. The diverse variety of such attacks makes a view that the world of these attacks is very vast and its difficult to explore and resist that. For preventing these attacks, it is necessary to understand the problems and faults in our networks and see the current solution sp*ace.*

Keywords: DDOS, WSM IoS LEACH, AIS

I. INTRODUCTION

Wireless sensor network have main focus on military application. These networks are also motivated by consumer and industrial applications. These applicationsare in health sector, industrial process and automation security. In sensor network, some conditions, data is fused and data is returned back. These data is sinking to one or multiple nodes depending upon the surrounding of sensor [1].The selection of route takes place in multi hop pattern. The transmit sinks communicates to the user. These act as task manger nodes through satellite or internet. Sensors are inserted randomly in the sensor field [2].

The sensor network is made with four basic units: a processing unit, sensor units, transceiver and GPS system. Other than these units, mobilizer and power unit are also used. Analog to digital converters and sensor are employed in sensing units [4].In beginning the signals are passed to ADC and then they transferred to processing units. The processing unit is a storage unit which used performs various task in in sensor network with other sensor node. To regulate the communication transceiver are used. Apart from these power unit is an important component of sensor node to limit the power. When a sensor is mobile, mobilizer is used which are application dependent. However, locationfinding system is common component in sensor nodes for getting accurate knowledge of sensed data by the use of sensing routing technique.

The main problem in the wireless sensor network is optimization of energy. The data transfer from base station to nodes gives more energy. To optimized this energy a new protocol is required.

The main advantages of wireless sensor network are to provide dense sense of nodes. These nodes are used to circumvent large amount of traffic back to the base station. This is explain with an example, a system have average humidity and temperature of a geographical region. These values are calculated by combined senosered value. This calculated value is secured.

This paper is design as a sequence stated below. The overall previous work is described in Section II. Section III describes the performance metrics. Finally, Section IV describes the conclusion of paper.

II. PREVIOUS RESEARCHERS

Yan, Qiao, F. Richard Yu, Qingxiang Gong2016 [3] as in present scenario due to the vital properties of cloud computing DDoS attacks are increasing rapidly. As noe the cloud computing is developed over the years and in latest advancement in software defines networking (SDN). The software defined networkings clouds are become a new approach to fight with DDoS attacks successfully. But the point of consideration is also that SDN and DDoS are conflicting to each other.

SamanTaghavi, James Joshi 2013 [1] This paper told that the DDos attacks are efforts t interrupt the legal user authentication to the services. Attackers are generally got access over the various systems and by knowing their security faults they made up an attack force (i.e., Botnets). As soon attackers create army then they performed a huge scale attack on multiple targets.

Pelechrinis, Konstantinos, MariosIliofotou 2011as information sharing is acommon feature wireless network. it also permits wireless Denial of service attacks. By the recent researches we get to know that WDoS attacks are can be easily operated by using off the shelf components.

Shamshirband, Shahaboddin 2014 [9] As the DDos service attacks have very dispersed nature due to this is get more difficult to detect such attacks by the use of conventional attack detecting methods in wireless sensor networks (WSNs). In this present paper a new method is commence which is game based fuzzy Q learning.

Yu, Yanli, Keqiu Li, Wanlei Zhou, and Ping Li2012 [8] As the security of wireless sensor network is always an issue of trust so its necessary to stop such attacks to revive trust schemes. In their research they compute various types of attacks and their preventions techniques.

Modares, Hero, Rosli Salleh2011 [10] For receiving the information from an insecure environment we generally approach to wireless sensor networks (WSN). In WSN security protocols they think that all the attackers can get complete access by the way of direct physical access.

Shamshirband, Shahaboddin 2014 [11] was described denial service attack. The author was described traditional detection system in the wireless sensor network. In this, author was proposed hybrid clustering method. The applied method was compare with existing K – Mean, K-MICA technique with accuracy & clustering quality. The accuracy & clustering was 87 % and 0.99 repectively.

Arunmozhi, S. A., and Y 2011 [12] were discussed about DDos attack. A protactive defense system was adopted to defense the medium access control. The frequency of receiver RTS/CTS packet is calculated from the status value of MAC layer.

Nanda, Rohan, and P. Venkata Krishna2011 [13] due to recent advancements in network protocols, WSN is approached as a rising sector. WSN s are adopted by security and military forces worldwide. Further is also used in hospitals and industries.

Jan, Mian, Priyadarsi Nanda2016 [14] Wireless sensor networks (WSNs) consist of resource-starving miniature sensor nodes deployed in a remote and hostile environment. These networks operate on small batteries for days, months, and even years depending on the requirements of monitored applications.

Ahmed, and Salman 2010 [15] As from recent decade there is much advancement in wireless network sector but as it grows is also increase the growth of number of attacks over these wireless networks. A huge work is done for securing the wireless network like now a days w ae using wireless sensor networks. By taken in account the environment of such network the chances of distributed attacks DoS cannot be ignored.

P. Venkata Krishna2011 [16]the interconnection of network is connected with the everyday elements. The attacks on the security protocols are of various types, but here we are protecting IoT networks from attacks. The main aim of Dos attacks is to make the information inaccessible to the user, and when numerous DOS attacks are present in same network this is called as DDoS.

Shamshirband, Shahaboddin2014 [17]was introduced a bio-inspired method. The integrated bio inspired method based on cooperative fuzzy artificial immune system is used to data transmitted from infected source.

Kumar, P. Arun Raj2013 [18] attacking the systems and networking resources to resist the user from accessing the information, this is done form the last decades and it still threatening us. As to detect he attacks we use various algorithms from that NFBoost algorithm is the st accurate which gives result upto 99.2% detection with minimum failure rate. As the costing is also very minimal for the NFBoost as compard with the traditional algorithms.

Baig, Zubair A 2011 [19] was introduced a new method to protect the network. As the attacks are distributed so to detect these attacks we use pattern recognition methods in a more precise manner. The accuracy & packet ratio was performance parameter. The accuracy and packet ratio was 91.5 % and 5.6 respectively.

Li, Shancang, LidaXu, Xinheng Wang2012 [20]presented a cloud computing technology. The scheme is based on enterprise information system. The optimization technique was used to improve the accuracy of the system.

Ho, Jun-Won, Matthew Wright, 2012 [21] After the execution the nodes are fixed to their positions in wireless networks. In this author was introduced subset of the different nodes. They were provided a platform to transfer energy from one node to another node. The energy computation and cost of false positive is minimum. The malicious node was detected with the analysis & simulation of the wireless sensor networks

Hamdi, Mohamed, and Noureddine 2007 [22]was introduce a wavelet transform method to increase accuracy of the transfer of energy. The monitoring points was pick out from the various sensor network and their stability was checked. Om the basis of that point decomposition was done.

Delgado-Mohatar, Oscar2011 [23] The sensor networks which are opted now a days are the ad hoc networks which consisted of sensors and have very limited computational capiblities.

The author was discussed about key management and authentication protocols. The cryptography technique was applied to secure the network. The applied protocols are compared with existing SPINS and BROSK protocols. The energy computation was reduce up to 67 %

III. PERFORMANCE PARAMETER

The following quantitative metrics are to be used to evaluate the performance of DDoS attacks and their prevention techniques under different combinations in the fixed mobile wsn network.

1. Throughput:

Throughput is a dimensional parameter which tells about the fraction of channel capacity that is desired for the successful communication that choose a receive location before the execution that is does our data packs are successfully transmitted or not. The receiver for this is define as an ration among number of bits receiver between the time interval of first and end bits received.

2. No. of Collisions:

One of the most important parameter is collision. Collision is occurring when dual bits are transferred in the identical time intervals. When collision occur, some packets are lost. To avoid this situation, all the packets are transmitted in a sequence in a particular time slot.

IV. CONCLUSION

It can be concluded that a distributed framework can get better results by operating among with multiple defense subsystem. We introduce trace back methods for preventing from undesired traffic by eliminating flooding base DDOS attacks. This work mainly illustrate that the detection algo should detect the DDOS attacks at the beginning with high performance. Two main necessities for competent traceback are to swiftly and precisely find possible attackers and other is to filter attack packets so that a host can resume the normal ability to legitimate clients. Most of the continuing IP traceback methods focus on pursuing the locale of attacker's after the attack. This work, we implemented an efficient methodology for discovering possible attackers who retain the DDOS-based attack.

V. REFERENCES:

[1] Zargar, SamanTaghavi, et.al "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." IEEE communications surveys & tutorials, Vol 15, issue 4, pp 2046-2069, 2013.

[2] Pelechrinis et.al "Denial of service attacks in wireless networks: The case of jammers." IEEE Communications Surveys & Tutorial, Vol 13, issue2, pp 245-257, 2011.

[3] Yan, Qiao et.al "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey." IEEE Communications Surveys & Tutorials, vol 18, issue 1, pp 602-622, 2016.

[4] Yu, Yanl et.al "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures " Journal of Network and computer Applications issue 35, vol 3 2012, pp 867-880, 2012.

[5] Modares, Hero et.al "Overview of security issues in wireless sensor networks." In Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 3rdInternational Conference on, pp. 308-311. IEEE, 2011.

[6] Shamshirband et.al "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks." Engineering Applications of Artificial Intelligence, Vol 32. pp 228-241, 2014.

[7] Arunmozhi, S. A., and Y. Venkataramani. "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks." Vol 5, pp 1106 -1287, 2011.

[8] Nanda, Rohan et.al "Mitigating denial of service attacks in hierarchical wireless sensor networks." Network securityvol 10, pp 14-18, 2011.

[9] Jan, Mian et.al "PAWN: a payload-based mutual authentication scheme for wireless sensor networks." Concurrency and Computation: Practice and Experience, 2016.

[10] ELBeltag et.al "Fluoxetine improves the memory deficits caused by the chemotherapy agent 5-fluorouracil." Behavioural brain research, vol 208, issue 1, pp 112-117, 2010.

[11] Misra, Sudip, P. Venkata Krishna, HarshitAgarwal, AntrikshSaxena, and Mohammad S. Obaidat. "A learning automata based solution for preventing distributed denial of service in Internet of things." 4th International Conference on Cyber, Physical and Social Computing, pp. 114-122. IEEE, 2011.

[12] Shamshirbann et.al "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks." Engineering Applications of Artificial Intelligencevol32 pp 228-241, 2014.

[13] Kumar et.al "Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems." Computer Communications Vol 36, issue. 3 pp 303-319, 2013.

[14] Baig, Zubair A. "Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks." Computer Communications,vol34, issue 3 (2011): 468-484, 2011.

[15] Li, Shancang et.al "Integration of hybrid wireless networks in cloud services oriented enterprise information systems." Enterprise Information Systems issue 6, vol 2, pp 165-187, 2012.

[16] Ho, Jun-Won et.al "Distributed detection of mobile malicious node attacks in wireless sensor networks." Ad Hoc Network,Vol 10, issue 3, pp 512-523, 2012.

[17] Hamdi et.al "Detecting Denial-of-Service attacks using the wavelet transform." Computer Communications, vol30, issue 16 (2007): 3203-3213.

[18] Delgado-Mohatar et.al "A light-weight authentication scheme for wireless sensor networks." Ad Hoc Networks , Vol 9, issue 5, pp727-735 , 2011

[19] Vasserman et.al "Vampire attacks: draining life from wireless ad hoc sensor networks." IEEE transactions on mobile computing, vol 12, issue 2 pp 318-332, 2013.

[20] Ho, Jun-Won et.al "Distributed detection of mobile malicious node attacks in wireless sensor networks." Ad Hoc Networks , vol 10, issue 3 , pp 512-523 , 2012

[21] Hamdi, Mohamed et.al "Detecting Denial-of-Service attacks using the wavelet transform." Computer Communications,vol 30 issue 16, pp 3203-3213, 2007.

[22] Delgado-Mohatar et.al "A light-weight authentication scheme for wireless sensor networks." Ad Hoc Networks vol 9, issue 5 pp 727-735 , 2011

[23] Vasserman et.al "Vampire attacks: draining life from wireless ad hoc sensor networks." IEEE transactions on mobile computing vol 12, issue 2, pp 318-332, 2013.