Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 5, May 2019, pg.155 – 163

Comparative Analysis of Detection of DDOS Attack in WSN

Ankur Sharma[1]; Anurag Rana[2]; Gourav Tandon[3]
Associate Professor, Assistant Professor, M.Tech Scholar
Department of Computer Science and Engineering
Arni University Kathgarh, (Indora)-176401 Kangra, Himachal Pradesh

Abstract: In network there are different kinds of attack that impact its presentation and it might hazard security amid the transmission. The security is the serious issue in network transmission that may hurt by these attacks. In this paper the investigation of DDOS attack in network must be finished. The attack that impact network by creating malevolent characters or IP addresses is DDOS attack. The one attack the personality of the network client and makes misinterpretation among different hubs that are in network. It manufactured the personalities of clients that chance the security. In this paper the different procedure that are uses to recognize DDOS attack in network are considered. Likewise different strategies are thought about based on parameter that is used in every strategy.
Keywords: Intrusion, Network, Malicious, Nodes, DDOS attack

1. Introduction

Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc. The sensor nodes have extreme resource limitations, unreliable communication medium and that too in unattended environments. This makes it very difficult for the implementation of the existing security approaches to WSNs due to the complexity of the existing algorithms.

1.1 ATTACKS IN WSN

Due to the unique characteristics of underlying networking protocols, sensor networks are vulnerable to security threats. Attacks can occur at any layer such as physical, link, network, transport, and application etc. Most of these routing protocols are not designed to have security mechanisms and it makes it even easier for an attacker to break the security for example, attacks at the physical layer of the network include jamming of radio signal, tampering with physical devices etc. In the following section we discuss in detail the layer wise attacks in WSNs

A. Physical layer attacks

- **Jamming** – It is caused due to interference with the radio frequencies of the network's devices which is an attack on the availability of the sensor network. It is different from normal radio propagation in the way that it is unwanted and disruptive, thus resulting in denial-of-service conditions.
- **Tampering** – It is also called node capturing in which a node is compromised, it is easy to perform and is pretty harmful. Tampering is physically modifying and destroying sensors nodes.

B. Link layer attacks

- **Collision** – It is caused in link layer that handles neighbor-to-neighbor communication along with channel arbitration. Entire packet can be disrupted if an adversary is able to generate collisions of even part of a transmission, CRC mismatch and possibly require retransmission can be caused by a single bit error.
- **Exhaustion** – Exhaustion of a network's battery power can be induced by an interrogation attack. A compromised node could repeatedly send thus consuming the battery power more than required

C. Network layer attacks

- **Hello flood attack** – It is caused when an attacker with high transmission power can send or replay hello packets which are used for neighbour discovery. In this way, attacker creates an illusion of being a neighbor to other nodes and underlying routing protocol can be disrupted which facilitate further types of attacks.
- **Wormhole attack** – It is caused due to formation of a low-latency link that is formed so that packets can travel from one to the other end faster than normally via a multi-hop route. The wormhole attack is a threat against the routing protocol and is challenging to

detect and prevent. In this type of attack, an adversary can convince the distant nodes that are only one or two hops away through the wormhole causing confusion in the network routing mechanisms.

- **DDOS attack-** Distributed denial of service attack is caused due to high congestion and denial of services to the users. The traffic is jammed in this cased and hence users may not get the resources they require. The performance degrades in terms of cost and energy consumption.
- **Sybil attack –** It is caused when an attacker uses a malicious device to create a large number of entities in order to gain influence in the network traffic. The ID of these malicious nodes can be the result due to fake network additions or duplication of existing legitimate identities. The sybil attack usually targets fault tolerant schemes including distributed storage, topology maintenance, and multi-hop routing.
- **Sinkhole attack –** It is caused when an attacker prevents the base station of the network from obtaining complete and accurate sensing data, thus resulting in a serious threat to higher-layer applications. By Sinkhole attack, attacker can attract nearly all the traffic from a specific area. Sinkhole attacks work in the way by making malicious node look especially attractive to other surrounding nodes with respect to routing protocols underling routing algorithm.

A DDOS attack is a Multiple Identity Attack utilizing multiple distributed attack sources. Typically, the attackers use a large number of controlled bots distributed in different locations to launch a large number of Multiple Identity Attack attacks against a single target or multiple targets. With the rapid development of network technology in recent years, the attack traffic scale caused by Multiple Identity Attack attacks has been increasing, with the targets including not only business servers, but also internet infrastructures such as firewalls, routers and DNS system as well as network bandwidth, the attack influence sphere has also become broader.

[2]WSN provides a wide range of computing resources from servers and storage to enterprise applications. WSN is a hosting environment that is immediate, flexible, scalable, secure and available. The computing resources from cloud can be easily and quickly accessed and released after use with very less management effort. The concept of WSN can be used in mobile

applications running on SMDs to boost up their performance. With the integration and support of WSN into the complex mobile applications, the term Mobile WSN (MCC) arises.

This paper presents the comparative study of distance based mechanism for detecting DDOS attack within WSN. Various distances that exists within WSN includes:

- Manhattan distance
- Minkowski Distance
- Cosine distance
- Hamming distance

1.2 Clustering mechanisms using distances

The distances considered above can be used to form the clustering. the clustering can be used to determine the closest neighbours in order to determine any abnormality within the transmitted bits, The various clustering mechanisms that could be employed for the abnormality detection is listed as under

- **Partitioning Method**

Assume we are given a database of "n" articles and the dividing technique develops "k" segment of information. Each parcel will speak to a bunch and $k \leq n$. It implies that it will characterize the information into k gatherings, which fulfil the accompanying prerequisites –

.Each gathering contains no less than one protest.

.Each protest must have a place with precisely one gathering[3].

- **Hierarchical Method**

This strategy makes a various levelled deterioration of the given arrangement of information articles. We can order various levelled techniques on the premise of how the progressive disintegration is shaped. There are two methodologies here –

- **Agglomerative Approach**

This approach is otherwise called the base up approach. In this, we begin with each question framing a different gathering. It continues blending the items or gatherings that are near each other. It continues doing as such until the majority of the gatherings are merged into resultant or until the end condition holds.

- **Top down Approach**

This approach is otherwise called the top-down approach. In this, we begin with the greater part of the articles in a similar group. In the persistent cycle, a bunch is part up into littler groups. It is down until each protest in one bunch or the end condition holds. This technique is unbending, i.e., once a consolidating or part is done, it can never be fixed[4].

- **Density-Based Method**

This strategy depends on the idea of thickness. The fundamental thought is to keep developing the given bunch the length of the thickness in the area surpasses some edge, i.e., for every information point inside a given group, the sweep of a given group needs to contain no less than a base number of focuses[5].

- **Grid-Based Method**

In this, the items together shape a framework. The question space is quantized into limited number of cells that shape a framework structure. Advantages:

i. The significant preferred standpoint of this strategy is quick preparing time.

ii. It is reliant just on the quantity of cells in each measurement in the quantized space[6]

2. Literature Survey

(Y.Chen.2016) proposed a generalized attack detection model that utilizes the spatial correlation of received signal strength inherited from wireless nodes. The suggested work provide a theoretical analysis of our approach. We then derive the test statistics for detection of identity-based attacks by using the K-means algorithm. The proposed attack detector is robust when handling the situations of attackers that use different transmission power levels to attack the detection scheme. We further describe how we integrated our attack detector into a real-time indoor localization system, which can also localize the positions of the attackers.

(Analysis n.d.) In the suggested paper the accuracy of range based algorithm is analyzed. The range based algorithm is range or distance dependent. If the distance is high than the accuracy of the algorithm will start to decay. The distance should be less in case of the range based algorithm. The concept of cooperative localization will be used in this case.

(Bachrach and Taylor n.d.) Localization in sensor network is considered in this case. Localization will depend upon the distance. If the distance is high than the localization is difficult to be performed otherwise localization is relatively easy to be performed. In order to solve the problems of the range based algorithm range free algorithm is used. The range based algorithm cannot be operational if the distance between the nodes become high. The range free algorithm does not consider the distance and hence perform better in case of high distance between the sensor nodes.

(Kumar et al. 2011) in the suggested technique range free algorithm is considered. In this case the course information is derived on the basis of range free algorithm. The range free algorithm is independent of the distance. Also the cost associated with the algorithm is low.

(Pathan, Lee, and Hong 2006) The concept of the security is considered in this case. The WSN when comes in contact with the number of different types of users the security of the WSN is sacrificed. The various security issues and there rectifications are considered in this case. The malicious nodes are handled in this case.

(Stoleru, He, and Stankovic 2007) in the suggested technique range free algorithm is considered. In this case the course information is derived on the basis of range free algorithm. The range free algorithm is independent of the distance. Also the cost associated with the algorithm is low.

(Walters and Liang 2007) The concept of the security is considered in this case. The WSN when comes in contact with the number of different types of users the security of the WSN is sacrificed. The various security issues and there rectifications are considered in this case. The malicious nodes are handled in this case.

(Yang 2014) The ubiquitous nature of WSN applications and their access to confidential information, either sensed directly or gained from their environments, makes them attractive targets for unscrupulous individuals to subvert, in an attempt to gain access to the WSNs and/or disrupt the interactions of users with both the networks and subsequently with their environment. Consequently, providing effective security is crucial for the successful adoption and operation of WSNs. We cannot deploy such a critical technology without first addressing the security and privacy challenges to ensure that it does not compromise those whom it is meant to benefit. This chapter provides a general review and categorization of the fundamental security primitives required to establish secure WSNs. The ZigBee security service is introduced as an example. The

chapter then discusses Denial of Service (DoS) attacks and defences, focusing on the threat of a DoS attack on a WSN. A framework for increasing the resistance of WSNs to remote DoS threats is introduced, implemented, and evaluated using a WSN based home automation as a case study.

(Yu, Prasanna, and Krishnamachari 2006) Localization in sensor network is considered in this case. Localization will depend upon the distance. If the distance is high than the localization is difficult to be performed otherwise localization is relatively easy to be performed. In order to solve the problems of the range based algorithm range free algorithm is used. The range based algorithm cannot be operational if the distance between the nodes become high. The range free algorithm does not consider the distance and hence perform better in case of high distance between the sensor nodes.

(Zheng and Dehghani 2012) in the suggested technique range free algorithm is considered. In this case the course information is derived on the basis of range free algorithm. The range free algorithm is independent of the distance. Also the cost associated with the algorithm is low.

3. Conclusion

This paper shows that DDOS attacks can altogether by a wide margin increasingly horrendous the execution of network and security risk by disintegrating diverse networking shows. So the examination of varied DDOS attack revelation frameworks has been appeared foreseen on the changed parameters show the information amassing, watching, and affirmation strategies are performed at heaps of network territories. In this paper we inspect the unique systems used for intrusion acknowledgment in WSN. The overall examination of various methods will bring about distinctive the better and expansive security segment to stay WSN. By using range based algorithm in our paper we shield our data from DDOS attack.

References

[1] Advisor, Dissertation and Dissertation Committee. 2007. “Communication Security in Wireless Sensor.”

[2] Almuzaini, Khalid K. 2010. “Range-Based Localization in Wireless Networks Using Density-Based Outlier Detection.” *Wireless Sensor Network* 02(11):807–14.

[3] Analysis, A. Lower Bound. n.d. “Accuracy of Range-Based Cooperative Localization in Wireless Sensor Networks :” 1–11.

[4] Anwar, Raja Waseem et al. 2014. "Security Issues and Attacks in Wireless Sensor Network." *World Applied Sciences Journal* 30(10):1224–27.

[5] Avila-Vazquez, Daniela et al. 2014. "Geospatial Recommender System for the Location of Health Services." Pp. 1–4 in *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE. Retrieved January 13, 2016 (http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6877023).

[6] Bachrach, Jonathan and Christopher Taylor. n.d. "Localization in Sensor Networks."

[7] Badshah, Gran, Siau-chuin Liew, Jasni Mohamad Zain, Syifak Izhar Hisham, and Amatul Zehra. 2015. "Importance of Watermark Lossless Compression in Digital Medical Image Watermarking." 4(3):75–79.

[8] Boudhir, Anouar Abdelhakim and Ben Ahmed Mohamed. 2010. "New Technique of Wireless Sensor Networks Localization Based on Energy Consumption." *International Journal of Computer Application* 9(12):25–28.

[9] C. Wu, Z. Yang, Y. Liu, and W. Xi. 2013. "WILL: Wireless Indoor Localization without Site Survey." *IEEE Transactions on Parallel and Distributed Systems* 24(4):839–48. Retrieved January 12, 2016 (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6216368).

[10] Chandrasekhar, Vijay R. and Winston K. G. Seah. n.d. "Range-Free Area Localization Scheme for Wireless Sensor Networks." Corke, Peter et al. 2010. "Environmental Wireless Sensor Networks." *Proceedings of the IEEE* 98(11):1903–17.

[11] He, Tian, Chengdu Huang, Brian M. Blum, John A. Stankovic, and Tarek Abdelzaher. 2003. "Range-Free Localization Schemes for Large Scale Sensor Networks 1."Kalita, Hemanta Kumar and Avijit Kar. 2009. "W S N S a." 1(1):1–10.

[12] Kaur, Amanjot and Jaspreet Kaur. 2012. "Comparision of Dct and Dwt of Image Compression Techniques." 1(4):49–52.

[13] Kumar, Ashok, Narottam Chand, Vinod Kumar, and Vinay Kumar. 2011. "Range Free Localization Schemes for Wireless Sensor Networks." *International journal of Computer Networks & Communications* 3(6):115–29. Retrieved (http://www.airccse.org/journal/cnc/1111cnc07.pdf).

[13] La, Vinh Hoa and Ana Cavalli. 2014. "S Ecurity Attacks and Solutions in V Ehicular a D Hoc N Etworks : A S Urvey." 4(2):1–20.

[14] Muhammad, Syed, Safdar Hussain, and Muhammad Yousaf. 2015. "Neighbor Node Trust Based Intrusion Detection System for WSN." *Procedia - Procedia Computer Science* 63:183–88. Retrieved (http://dx.doi.org/10.1016/j.procs.2015.08.331).

[15] Pal, Santar and S. C. Sharma. 2015. "Range Free Localization Techniques in Wireless Sensor Networks : A Review." *Procedia - Procedia Computer Science* 57(i):7–16. Retrieved (http://dx.doi.org/10.1016/j.procs.2015.07.357).

[16] Pathan, a. S. K., Hyung-Woo Lee Hyung-Woo Lee, and Choong Seon Hong Choong Seon Hong. 2006. "Security in Wireless Sensor Networks: Issues and Challenges." *2006 8th International Conference Advanced Communication Technology* 2:6 pp. – 1048. Retrieved (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1625756).

[17] Patil, Kishore J., Manojkumar Z. Chopda, and Raghunath T. Mahajan. 2011. "Lipase Biodiversity." *Indian Journal of Science and Technology* 4(8):971–82. Retrieved (http://www.indjst.org).

[18] Purushothaman, Deepanchakaravarthi and Sunitha Abburu. 2012. "An Approach for Data Storage Security in Cloud Computing." 9(1):100–105.

[19] Ruj, Sushmita, Marcos Antonio Cavenaghi, Zhen Huang, Amiya Nayak, and Ivan Stojmenovic. 2011. "On Data-Centric Misbehavior Detection in VANETs." *2011 IEEE Vehicular Technology Conference VTC Fall* 35(2):1–5. Retrieved (http://arxiv.org/abs/1103.2404).

[20] Science, Computer and Management Studies. 2014. "Securing User Data on Cloud Using Fog Computing and Decoy Technique." 7782:104–10.

[21] Si, Weisheng and Selvadurai Selvakennedy. 2008. "A Position-Based Deployment and Routing Approach for Directional Wireless Mesh Networks." *2008 Proceedings of 17th International Conference on Computer Communications and Networks* 1–8. Retrieved (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4674234).

[22] Stoleru, Radu, Tian He, and John A. Stankovic. 2007. "Range-Free Localization." *Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks* 3–31.

[23] Walters, Jp and Zhengqiang Liang. 2007. "Wireless Sensor Network Security: A Survey." *Security in distributed, ...* 1–50. Retrieved (http://books.google.com/books?hl=en&lr=&id=KhxxsN3vJuYC&oi=fnd&pg=PA367&dq=Wireless+Sensor+Network+Security+:+A+Survey&ots=R4RpHtOLGz&sig=Z_PWgD18TATEHDJK6qLCzP4CsTk).

[24] Wang, C., Q. Wang, K. Ren, and W. J. Lou. 2009. "Ensuring Data Storage Security in Cloud Computing." *Iwqos: 2009 Ieee 17th International Workshop on Quality of Service* 37–45\n302. Retrieved (<Go to ISI>://000274551300005).

[25] Yang, Shuang-Hua. 2014. "WSN Security." 187–215. Retrieved (http://link.springer.com/chapter/10.1007/978-1-4471-5505-8_9).

[26] Yu, Yang, Viktor Prasanna, and Bhaskar Krishnamachari. 2006. "Energy Minimization for Real-Time Data Gathering in Wireless Sensor Networks." *IEEE Transactions on Wireless Communications* 5(10):3087–96.

[27] Zheng, Jun and Asghar Dehghani. 2012. "Range-Free Localization in Wireless Sensor Networks with Neural Network Ensembles." *Journal of Sensor and Actuator Networks* 1(3):254–71. Retrieved (http://www.mdpi.com/2224-2708/1/3/254/).

[28] Zhong, Ziguo. 2009. "Achieving Range-Free Localization Beyond Connectivity." *Sensys* 281–94.

