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: 6.017

IJCSMC, Vol. 6, Issue. 6, June 2017, pg.351 – 353

DDOS Attack in WSN: A Survey

Syed Faizan[1], Zahid Mushtaq[2], Irfan Rashid[3]

[1]Department of CSE, SSM College of Engg and Tech, Baramulla, India

[2]Department of CSE, SSM College of Engg and Tech, Baramulla, India

[3]Department of CSE, SSM College of Engg and Tech, Baramulla, India

[1] Syedfaizaan81@gmail.com; [2] Er.zahid00@gmail.com; [3] Samirfan@gmail.com

ABSTRACT—Wireless Sensor Networks (WSNs) is collection of large number of sensor nodes which are of limited capabilities, to collect sensitive information. With the advancement of this technology, one of the major concerns these days is of security. There are so many attacks possible on WSN, in Distributed-Denial of Service (DDOS) attacks, malicious nodes adapts many attacks such as flooding attack, black hole attack and warm hole attack, to halt the overall functioning of network. The risks are even more when we talk about military and industrial applications. Furthermore in WSN there are so many constrains like limited battery power, low capabilities of nodes etc. To present a security model that will consider these constraints and provide security is a major challenge these days. There are many mechanisms which are proposed by researchers to detect or defend from this DDOS attack. In this paper we will review these approaches on basis of various parameters.

Keywords --- Wireless Sensor Networks (WSNs), Sensor nodes, Security, DDOS attack.

I. Introduction

Wireless Sensor Networks (WSNs) consists of small sensor nodes communicated through radio links. They are used in many applications like (agriculture, health, home, industrial, and military) for monitoring and data collection purpose. Its main advantage is that it is easy to deploy in harsh environments, where infrastructure is difficult to deploy.

In many applications (like military, medical and industrial) security is very crucial requirement. Due to so many limitations in WSNs, the traditional security methods cannot be directly implemented. There limitations include limited battery power, power to communicate and compute. Furthermore the area for deployment of WSNs may be public locations, where intruder can physically take over sensor nodes and take all information. Moreover due to energy failures some nodes may die, or new nodes can join the network and the channel used for communication is very insecure. Hence more efficient security approaches are required which consider all these constraints .

Rest of the paper is organized as, Section II includes WSNs Architecture, Section III defines Attacks in WSNs. Section IV, gives the related work. Finally the section V gives the conclusion.

II. WSNs Architecture

Wireless Sensor Network (WSN) mainly contains one or few Base Station (BS) or Sink and hundreds or thousands of sensor nodes. Sensors have limited capacity whereas base stations are having more capabilities and are used to communicate with other networks. Sensor nodes are deployed at random, and responsible for data collection, whereas base stations are responsible for data aggregation and management of the network. BS sends aggregated data through internet to the user(Fig 1).

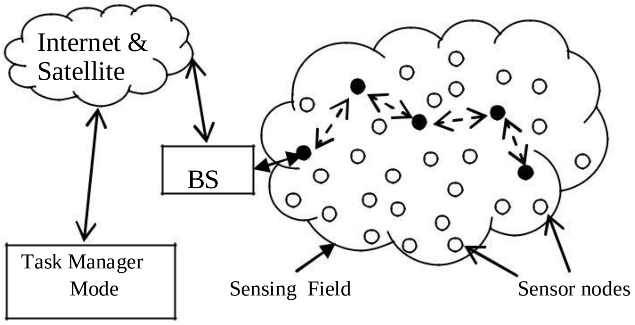

Fig.1. WSN Architecture

III. ATTACKS IN WSNS

WSN is susceptible to so many attacks, because of broadcasting nature of network. The main security services of network are: Integrity, Authentication, Confidentiality, Availability, Access Control etc.

- Integrity: This service ensures that whatever is sent is same as whatever is received, i.e is not being modified.
- Authentication: It ensures that the sender is same what it claims to be.
- Confidentiality: It ensures that the contents of message are understandable to only intended entities.
- Availability: This service ensures that services should be available to authorized members.
- Access Control: Access should be given only to authorized nodes.

In addition to these services efficiency and scalability are also the requirements. WSNs are vulnerable to so many security threats called Attacks.

A. Passive Attacks

In Passive Attacks intruder will listen to the channel or monitor the traffic but will not disrupt the communication between sender and receiver. Hence Passive attacks are hard to detect. It can further classify into:

1. Data Disclosure: In this attack intruder may harm to the privacy of information i.e. disclosure of information to unauthorized users.

2. Traffic Analysis: If actual information is in non readable form, then attacker may analyze the traffic and try to find other aspects such as, type of information, frequency of messages transferred etc.

B. Active Attacks

In these attacks, an attacker can modify the information or disrupt the commutations between the sender and the receiver. These attacks are more dangerous than passive attacks. Denial of Service is one type of Active attack. In this paper we will further focus on DOS attack.

1. Denial of Service (DOS): Denial of Service Attack (implemented by attacker by targeting the scheme of routing) occurs due to the failure of nodes unintentionally and also due to malicious action. In DoS attack, the resources available at the victim node are exhausted by receiving unnecessary packets which are not meant or entitled for that node. DoS attack is not only for adversary nodes but also for those events which dismisses the capability of network to provide services. In Wireless Sensor Network (WSN), various types of DoS attacks occur at each layer like jamming and tampering at physical layer, exhaustion, collision and unfairness at link layer, black holes, misdirection etc at network layer. At transport layer, DoS attacks occur due to de-synchronization and malicious flooding. So, to overcome all these DoS attacks a mechanism is included which contain pushback, authentication, network resources and identification of traffic.

IV. CONCLUSION

Wireless Sensor Network is sensitive to so many security threats. DoS attacks are much easier to launch in WSN. In this paper we defined various security services, attacks possible in ad-hoc WSN. The main focus is to study various types of DoS attacks, and techniques to prevent from these attacks. Many security techniques are invented in WSN, but it is still vulnerable to so many DoS attacks. Most techniques suffer from false alarms and high consumption of energy. As in WSN less consumption of battery power is very crucial, in order to enhance network lifetime. In future we improve the techniques which will have low false alarm problem and less energy consumption.

ACKNOWLEDGEMENT

Words are not just enough to express our gratitude but we take this opportunity to express our profound sense of gratitude and respect to all those who helped us throughout the duration of this paper. First of all we are very thankful to our **HOD Yasmeen Bhat** for her regular support and guidance. We are also very thankful to Allah for providing us such a great opportunity. We feel privileged to offer our sincere thanks and deep sense of gratitude to our college for expressing confidence in us by letting us work on a paper of this magnitude and providing support, help & encouragement in implementing this paper.

REFERENCES

[1] Kumari, J.; Prachi, "A comprehensive survey of routing protocols in wireless sensor networks," in Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on, vol., no., pp.325-330, 11-13 March 2015

[2] Yun Zhou; Yuguang Fang; Yanchao Zhang, "Securing wireless sensor networks: a survey," in Communications Surveys & Tutorials, IEEE, vol.10, no.3, pp.6-28, Third Quarter 2008 doi: 10.1109/COMST.2008.4625802

[3] Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks," SenSys '03: Proc. 1st

[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, August 2002.

[5] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299-302, year 2003.

[6] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", International conference on Advanced Computing Technologies, Page1043-1045, year 2006,

[7] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26 – 36.

[8] Wang, B-T. and Schulzrinne, H., "An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 – 904.

[9] Raymond, David R.; Midkiff, S.F., "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," in Pervasive Computing, IEEE , vol.7, no.1, pp.74-81, Jan.-March 2008 doi: 10.1109/MPRV.2008.6

[10] Perrig, A., Szewczyk, R., Wen, V., Culler,D., Tygar, J.D.: SPINS: Security protocols for sensor networks. Wireless Networks,pp. 521–534, 2002.

[11] Eschenauer, Laurent, and Virgil D. Gligor. "A key-management scheme for distributed sensor networks." In Proceedings of the 9th ACM conference on Computer and communications security, pp. 41-47. ACM, 2002

[12] Ferreira, Adrian, Marcos Vilaça, Leonardo Oliveira, Eduardo Habib, Hao Wong, and Antonio Loureiro. "On the security of cluster-based communication protocols for wireless sensor networks." Networking-ICN 2005, pp. 449-458. Springer, 2005.

[13] Oliveira, Leonardo B., Hao C. Wong,Marshall Bern, Ricardo Dahab, and Antonio AF Loureiro. "SecLEACH-A random key distribution solution for securing clustered sensor networks." In Network Computing and Applications 2006. NCA 2006. Fifth IEEE International Symposium on, pp. 145-154. IEEE, 2006.

[14] Abuhelaleh, M. A., T. M. Mismar, and A. A. Abuzneid. "Armor-LEACH-energy efficient, secure wireless network communication" In computer communication and networks, 2008 ICCCN'08, Proceedings of 17th International Conference on, pp. 1-7.

[15] Song, F. and Zhao, B. 2008. Trust-Based LEACH Protocol for Wireless Sensor Networks. In Proceedings of the 2008 Second International conference on Future Generation Communication and Networking - Volume 01 (December 13 -15,2008) FGCN, IEEE Computer society Washington.DC,202-207,IEEE,2008.