INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume3, Issue2)

Available online at www.ijariit.com

Review On Detection and Prevention Schemes for Flooding Attack in WSNS

Sukhwinder Deol
Guru Kashi University, Bathinda, Punjab
sukhideol119@gmail.com

Lovepreet Kaur
Guru Kashi University, Bathinda, Punjab
lovepreetlovely22@gmail.com

Abstract: The nodes of the wireless sensor networks are operated by limited batteries. These networks are open to various kinds of attacks. While most of these attacks focus on dropping the packets being transmitted in the network, the denial of service flooding attack consumes up the batteries of the sensor nodes leaving them dead. This nature of attack makes it too fatal as it leaves network dead. This paper presents survey about the detection and prevention schemes of the same.

Keywords: Denial of Service, Flooding Attack, Wireless Sensor Networks.

I. INTRODUCTION

A wireless sensor network is typically composed of many tiny computers called sensor nodes, often no bigger than a coin or a credit card. The primary goal of a wireless sensor network is to collect useful information by monitoring phenomena in the surrounding environment and send the information to a data collector, namely, a sink. In WSNs, each sensor node individually senses the local environment, but collaboratively achieves complex information gathering and dissemination tasks. Therefore, the objective of wireless sensor nodes is twofold: (1) obtain a description of the physical surroundings by means of sensors, and (2) wirelessly communicate this description and assist other nodes in delivering descriptions. To carry out these two functions, a wireless sensor node is typically equipped with the following components: on-chip sensor(s), transceiver, a low-frequency processor, some flash memory for storage, and power supply unit. Sensors are responsible for sensing (measuring) the physical environment. A node can have more than one sensor measuring different phenomena on-board [11]. These components are shown in the figure below.

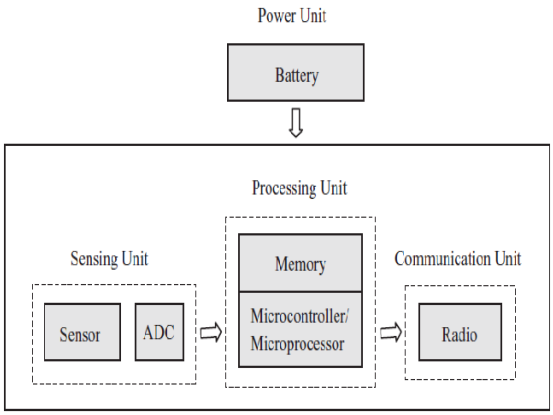

Fig: Components of a Sensor Node [11]

The number and types of sensors vary according to the application requirements. There is a wide variety of sensors available in the market. The most typical examples of sensors are temperature, humidity, light, pressure, vibration, sound, a chemical such as CO-sensor, and body sensors such as heart rate, accelerometer.

Whenever a protocol is required to maintain state at either end of a connection it becomes vulnerable to memory exhaustion through flooding [10]. It can be possible that attacker frequently requests for a new connection until all the resources are finished. A very

common form of DOS attacks involves sending a large number of common packets aimed at a single destination. The most common packets used are TCP, ICMP, and UDP. The huge traffic deluge caused by these packets leads the network to no longer be able to distinguish between legitimate and malicious traffic. Basically, all available resources such as bandwidth are used up and nothing is left for legitimate use causing the users to be denied the service of the network. This paper presents a survey of the existing schemes in Section II regarding the malicious nodes causing a denial of service- flooding attack and the schemes related to their detection and prevention.

DSR Protocol

DSR is a reactive routing protocol. It checks an ideal route just when the packet should be sent. The procedure to discover a way is quite recently executed when away is required by a node, which prompts to On-Demand Routing. The DSR protocol is made out of two principle systems that coordinate to allow revelation and support of source routes in WSN.

Route Discovery: When a source node S wishes to send a packet to the goal node D, it gets a route to D. This is called Route Discovery. Route Discovery is utilized just when Source needs to send a packet to Destination and has no data of a route to it.

Route Reply: When the node D receives the route requests messages from various nodes, it sends back RREP packets to the source node. The whole process is shown in figure 2.

Route Maintenance: The current routes are no longer usable when there is an adjustment in the network topology. In such a situation, the source S can utilize an option route to the goal D, or conjure Route Discovery. This is called Route Maintenance.

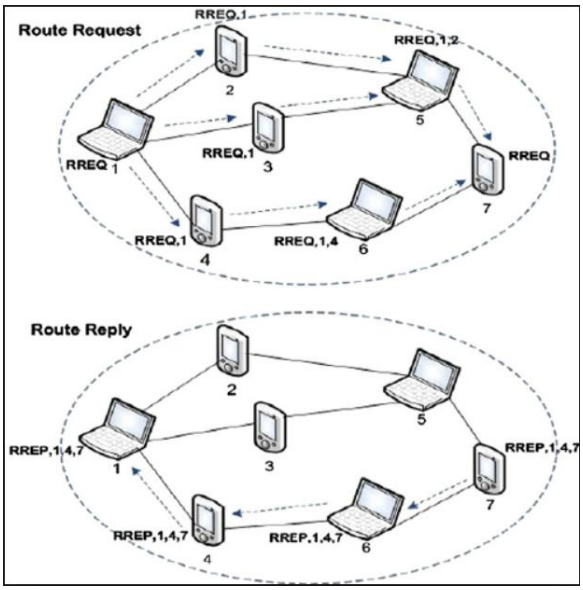

Fig: Route Discovery in DSR [12]

II. LITERATURE REVIEW

Gurbinder Singh Brar et. al., [2016] proposed PDORP protocol which is transmission-based energy aware routing protocol. The proposed protocol PDORP has the characteristics of both power efficient gathering sensor information system and DSR routing protocols. Hybridization of genetic algorithm and bacterial foraging optimization is connected to proposed routing convention to distinguish energy proficient ideal ways. The execution examination, correlation through a hybridization approach of the proposed routing convention, gives better outcome involving less piece mistake rate, less postponement, less energy utilization, and better throughput, which prompts to better QoS and drag out the lifetime of the system. Besides, the calculation model is adopted to assess and think about the execution of the both routing conventions [1].

Raksha et. al., [2015] proposed a solution to prevent WSN from DDOS attack using dynamic source routing (DSR). For detection and prevention of attack energy of concerned nodes has been used. Various outside attacks are possible on wireless sensor networks (WSN). Many attacks such as denial of service, black hole, sinkhole etc. may affect the network performance. Distributed denials of service (DDOS) attacks attacked by a set of malicious entities towards a node or set of nodes [2].

Isha et.al., [2013] proposed some of the security goals for WSN. To do any action in WSN, the aim is to ensure the best possible use of sensor assets so that the network can perform a good function. Instead, a Denial of Service (DoS) attack aims to lower the efficient use of network resources and create problems in the essential services in the network. This attack could be considered as one of the major threats in WSN [3].

Vishal et. al., [2011] investigate the security attacks that apply to WSN. It also introduces Trust Management issue that is important to security. WSN is a technology that is used in various applications both for mass public and military. It uses sensing technology, processing power, and wireless communication which makes it lucrative for being exploited in abundance future. By including wireless communication technology also include various types of security threats [4].

Hakem et. al., [2012] author presents Connection Score scheme to overcome the DDoS attacks occurred at the application layer of TCP model. When an attack occurs, any connection is scored which is based on history and statistical analysis is done. From those connections the resources are retaken which take lower scores and considered as an adversary or malicious attacks [5].
Hao Chen et. al., [2013] proposes real-time PSD converter based on FGPA to prevent shrew ddos attacks which are low rate TCP targeted attacks. The system uses component-reusable auto-correlation (AC) algorithm and adapted 2N-point real-valued Discrete Fourier Transform (DFT) algorithm [6].
Muhammad Amir et.al., [2008] analyze various methods to prevent DDoS attacks based on traffic anomaly parameters, neural networks, entropy variations, application layer DDoS defense and device level defense. The paper also discussed some traditional methods such as traceback and packet filtering techniques [7].
Monowar H. Bhuyan et. al., [2015] explains various information metrics which describes characteristics of network traffic data for the detection of both low-rate and high-rate DDoS attacks. These matrices include Shannon entropy, Generalized entropy, Renyi's entropy, Hartley entropy and Kullback leibler divergence. To check the effectiveness of each metric different technique such as MIT Lincoln Laboratory, CAIDA and TUIDS ddos datasets are used [8].
Wei et. al., [2014] author proposed a new method to detect ddos attacks at application layer who considers detection of AL-DDoS attack in high traffic. The method involves a Real-time Frequency Vector (RFV) and attacks can be recognized by investigating the entropy of application layer -DDoS attacks and flash crowds [9].

CONCLUSION

This paper presents the survey about the most serious threat to the wireless sensor networks which aims at exploiting the batteries of the nodes by forwarding more and more number of packets. The authors have also used the genetic optimization procedure to calculate trust values to detect such attacks. These trust values are calculated according to the energy consumed by the nodes in forwarding the packets in the network.
In future, we would like to further optimize the detection process by modifying the procedure to calculate the trust values to increase the security of the network.

REFERENCES

1. **Gurbinder Singh Brar, Shalli Rani, Vinay Chopra, Rahul Malhotra**, "Energy Efficient Direction-Based PDORP Routing Protocol for WSN" in IEEE 2016.
2. **Raksha Upadhyay, Uma Rathore Bhatt, and Narendra Tripathi,** "DDOS Attack Aware DSR Routing Protocol in WSN" in ELSEVIER 2016.
3. **Isha, Arun Malik, Gaurav Raj**, "DOS Attacks on TCP/IP Layers in WSN" in International Journal of Computer Networks and Communications Security July 2013.
4. **Vishal Rathod, Mrudang Mehta**, " Security in Wireless Sensor Network: A survey" in Ganpat university journal of engineering & technology, 2011.
5. **Hakem Beitollahi and Geert Deconinck**, "Tackling Application-layer DDoS Attacks", The 3rd International Conference on Ambient Systems, Networks and Technologies 2012.
6. **Hao Chen, Thomas Gaska, Yu Chen and Douglas H. Summerville,** "An optimized reconfigurable power spectral density converter for real-time shrew DDoS attacks detection", Computers and Electrical Engineering 2013.
7. **Muhammad Aamir and Mustafa Ali Zaidi**, "DDoS Attack and Defense: Review of Some Traditional and Current Techniques", SZABIST, Karachi, Pakistan 2008.
8. **Monowar H. Bhuyan, D.K. Bhattacharyya, and J.K. Kalita,** "An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection", Pattern Recognition Letters 2015.
9. **Wei Zhoua, Weijia Jia b, Sheng Wenc, Yang Xiang c and Wanlei Zhouc**, "Detection and defense of application layer DDoS attacks in backbone web traffic" in IEEE 2014.
10. **EL Caballero**, "Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem", 2006.
11. **Praveena Chaturvedi, "**Introduction to Wireless Sensor Networks**"** in International Journal of Advanced Research in Computer Science and Software Engineering, October 2012.
12. **Mehdi Sookhak, Adnan Akhunzada, "**Securing DSR against wormhole attacks in multi rate ad hoc networks", Journal of Network and Computer Applications, March 2013.

