ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ZIGBEE OPNET Modeller: An Efficient Performance Analyzer for Wireless Sensor Networks

Sanchari Saha
Assistant Professor, CSE Department, MVJ College of engineering, Bangalore, India
saha.sanchari85@gmail.com

Abstract

A sensor network is a special type of network. The unique characteristics of Wireless Sensor Networks separate them from the legacy communication networks. Most of the WSN's routing protocols are easy and straightforward & because of this reason they are vulnerable to attacks. The Distributed Denial of Service attack is considered particularly as it targets the energy efficient protocols that are unique to wireless sensor networks. So we start by considering such characteristics of the network and giving their impact on the security of the network. The Zigbee model provided in OPNET 16 is suitable for modelling WSNs. The main objective of this paper is to evaluate the impact of DDoS attacks on the performances of Wireless Sensor Networks by using the OPNET modeller. The effects of DDoS attacks on the performance of WSNs are considered to critically analyse these issues. The result presented in this paper can be of great help for optimization studies in Wireless Sensor Network environments under DDoS attacks.

Keywords: DDoS attack, Zigbee nodes, OPNET, Wireless Sensor Network, MAC protocol.

Introduction

Confidentiality of data can simply be explained as prevention of the untrusted third party from accessing the secure data. Data integrity ensures that replay attacks are prevented and the data is not modified and availability ensures that legitimate users can access services, data and network resources when requested. With the recent advances in modern communication systems, wireless networks are expected to provide communication with confidentiality, data integrity, and availability of service to the user. As wireless sensor networks continue to grow due to the fact that they are potentially low cost and effective, the need for effective security mechanisms also grow.

The WSN characteristics include, power they can store, node failures, their ability to cope, node mobility, heterogeneity and scalability of nodes and ability to cope under harsh environmental conditions. These basic characteristics of a WSN make them vulnerable to Denial of Service attacks. Difficulties encountered to secure the wireless medium are the main disadvantage for all wireless devices. The network can be jammed, unauthentic data can be transmitted and/or: traffic can be overheard by any adversary in the radio range. Physical tampering of sensors and their destruction in case they are deployed in unsecured areas is also possible. Because of the vulnerable structure of WSNs and the nature of DoS attacks it may be difficult to distinguish between an attack and a network failure.
We present a survey of attacks on WSN, discuss about the various DoS attacks, and the impact of DoS on the performance of the system. The simulation results show that the impact of DoS attacks on performance of WSN can be more severe, if carried out on coordinator or router, instead of just targeting the end devices. By preventing a single device from sending traffic or by preventing the communication between the network, DoS attacks target availability of services to the users [1]. Nodes of wireless sensors can be considered as small computers, very basic in terms of interfaces and the components involved. They usually consist of a limited processing capability and memory, sensors, a radio transceiver as a communication device and a limited power source such as a battery.

WSN Working Principle

Wireless sensor networks consist of clusters of devices using sensor technologies deployed in a specific area. They communicate data wirelessly to a central system. Sensor networks continuously monitor the physical, chemical processes or magnetic properties, using the existing communications infrastructure.

A software layer for processing and data management allows building industrial, government or

ISSN: 2277-9655
Impact Factor: 1.852

military applications. Wireless sensor networks based on emerging technologies such as wireless communication technologies, information technology, semiconductors, MEMS, microsystems technology and embedded micro-sensors. Wireless sensor networks have the potential to revolutionize telecommunications in a way similar to what we call the Internet of things by offering a wide range of different applications some of which remain to be discovered. Sensor networks have a huge potential for applications in various fields, including:

Environment and health: ocean temperature, collecting information on patients' conditions.

Management of critical industrial areas: monitoring of oil containers, checking the concentration of chemicals and gases.

Warehouse management and supply chain monitoring and historical states of the goods with the conditions of critical conservation.

Military applications: surveillance and recognition

A wireless sensor network consists of many tiny sensor nodes, each equipped with a radio transceiver, a microprocessor and a number of sensors. These nodes are capable of independently forming a network through which sensor readings can be propagated. Each node has an autonomous processing capacity, data can be processed as they pass through the network.
Given the limitations of the equipment and the physical environment and levels of high demands with which the nodes must operate, algorithms and protocols must be designed to provide strong and efficient energy consumption. The design of the physical layer and communication technologies and the information coding still represent significant challenges for this new technology.

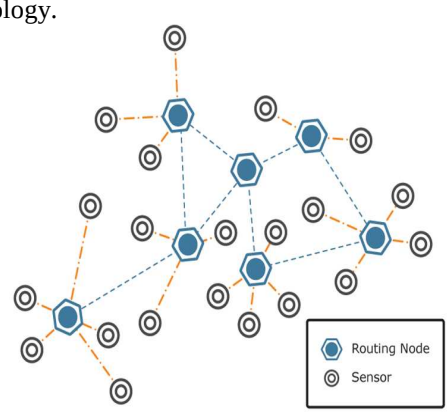

Figure 1. Simple WSN architecture

Impact of DDoS Attacks on WSN

In the era of fast-growing cyber-activism, DDoS attacks are the preferred weapon of mass disruption, rendering legacy DDoS attack solutions obsolete. While the common practice of organizations is to rely on DDoS attack detection from their service provider, the recent wave of attacks in 2011-2012 demonstrates that attackers bypass the service provider and target business websites directly.

Companies that depend on 'one-size-fits-all' in-the-cloud managed security, or on-premise security solutions alone, cannot withstand these sophisticated assaults. To effectively stop DDoS attacks, a secure network architecture that combines in-the-cloud DDoS attack detection as well as on-premise DDoS defense is necessary.

In wireless sensor networks, the wireless nature of the communication media, accompanied by the limited energy resources of sensor nodes, differentiates distributed denial of service attack modeling and detection in them. The adversary class monitors the flow of traffic in the network and labels the more active nodes, in terms of transmitting and receiving data packets, as critical nodes, which need to be targeted as part of the distributed denial of service attack. We refer to all such critical nodes as target or victim nodes. The distributed denial of service attack is launched by the adversarial nodes toward these critical sensor nodes from multiple ends of the network. The purpose of such attacks is to deplete the limited energy resources.

If the sensor network encounters DDoS attacks, the attack gradually reduces the functionality as well as the overall performance of the wireless sensor network. Projected use of sensor networks in sensitive and critical applications makes the prospect of DDoS attacks even more alarming. The 3 basic mode of attack are:

I. Consumption of limited or scares resources (network bandwidth, memory).
II. Alteration or destruction of configuration information.
III. Physical destruction of network components.

The devices which can partially or entirely disrupt a nodes signal by increasing the power spectral density are jammers. Parameters such as signal strength, location and type of jammer have great influence on the performance of the network. Another physical layer attacks include node tampering. It is not very easy to completely prevent destruction of nodes; however camouflaging and redundant nodes can mitigate this threat.

Routing disruptions can lean to DoS attacks in multihop sensor networks. They include spoofing, replaying etc. Antireplay and authentication of link layer can prevent such attacks effectively. Hello messages are broadcasted by some nodes to announce themselves to

ISSN: 2277-9655
Impact Factor: 1.852

their neighbours. So a node receiving such a message assumes that it is within the sender's radio range. However, sometimes a laptop class attacker broadcasting routing information with higher transmission power could convince other nodes in the network that the attacker is its neighbour. Protocols depending on localized information exchange between neighbouring nodes for flow control are affected by Hello flood attack. Denial of sleep attack causes the transmitter to remain awake for long intervals where it was not supposed to. The radio receiver consumes a lot of energy on a mote and an attack will drain as much energy so as to bring down the wireless network. Packet authentication can prevent this attack. Continuously resetting the sleep timers, link layer authentication and anti-replay support can protect from denial of sleep attack.

DDoS attacks in Wireless Sensor Networks can be represented in OPNET. The main aim of the paper is intended for the modelling of DDoS attacks in WSN and the simulation.

The OPNET ZIGBEE Model

The Zigbee model provided in OPNET 16 is suitable for modelling wireless sensor networks. Zigbee model suite in OPNET includes a discrete event simulation model, which allows the users to analyse the performance in Zigbee WPANs. This includes a model of IEEE 802.15.4 MAC protocol. The designed system consists of three types of wireless sensor Zigbee nodes, a coordinator, a router and an end device (sensing node). The simulation model implements MAC and physical layers as defined in IEEE standards. Due to the accuracy and its sophisticated graphical user interface, the OPNET modeller has been chosen for simulation. The Zigbee model consists of following components:

Zigbee coordinator: It forms the root of the network tree and might bridge the other networks. Most capable among the three type of Zigbee devices. There is only one Zigbee coordinator in each network as it is the device that started the network originally. It can store information about the network, including acting as the trust centre and repository for security keys.

Zigbee Router: It is a simple router that passes on the data from other devices. It keeps a routing table and controls allocation/de-allocation of local address for its allocated Zigbee end devices.

***Zigbee End device*:** Contains just enough functionality to communicate with the parent nodes. It cannot route data from other devices. This allows the node to be asleep for a longer period of time and hence long battery life.

When the simulation scenario of the study is considered, the objectives are:

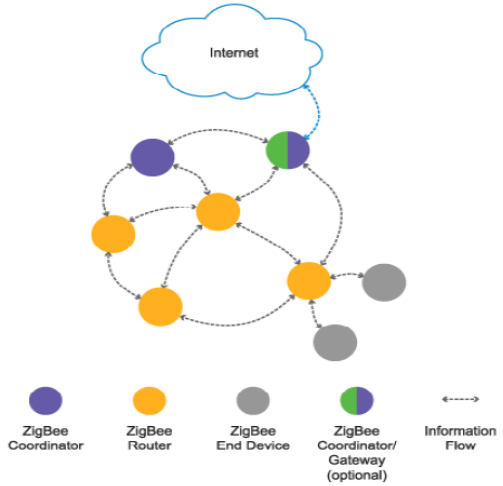

Figure 2. A simple Zigbee network

The simulation model considered here has a tree topology where the communication takes place between the nodes coordinator, a router and the end device. Each of the operating devices has a unique address. The traffic source generates the application data. This data can be generated either by the Personal Area Network coordinator or by the end device.

Each Zigbee node is powered with two AA batteries which should be sufficient for long interval of uninterrupted operation. Traffic by the attacker has been created using the traffic centre in OPNET modeller. Different data rates and different types of data's are employed to represent a DoS attack. Various traffic parameters can be set as according to the requirement.

Every simulation scenario is considered to represent a typical attack and observe the consequences. The simulation time is set to 10 hours for every run to make sure that the simulation reaches to steady state and average value converges.

WSN Performance Evaluation

In order to evaluate the performance of the Wireless sensor networks, and to analyse the impact of the DoS attack, we need to measure the performance metrics of the network. The WSN is modelled by using Zigbee nodes in OPNET for analysis in details. Scenarios of DoS attack on the zigbee router, zigbee coordinator, and zigbee end device have been modelled with suitable parameters. Simulation results have been illustrated for performance measures such as throughput, and traffic sent in the nodes. The results are compared for various cases of DoS attacks and normal scenario. Our standard scenario for all the experiments contains the following parameters:

ISSN: 2277-9655
Impact Factor: 1.852

I. At first 10 Zigbee end device have been considered depending on the conditions set to obtain the desired results.
II. One Zigbee router is used as a router gateway, to connect the Zigbee coordinator and the end devices.
III. A Zigbee coordinator forms the root of the network tree and bridge with the other networks. It stores information about the network, including the acting trust centre and repository for security keys.
IV. The traffic in the network can be set as per the requirements. Destination of the traffic is set to end device, via router. Packet size and inter arrival times are varied accordingly.

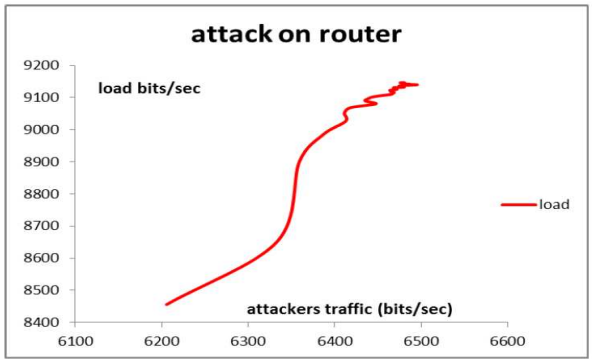

Figure 3. Average Load vs. Average Traffic of attacker during attack on router.

In figure 3, the impact of the load on the network due to attacker's traffic is shown, while there is an attack on the router. The Denial of Service attack on the router, affects the performance of the overall network severely. The attack mainly degrades the performance due to the over load of traffic, as shown in the figure 4.

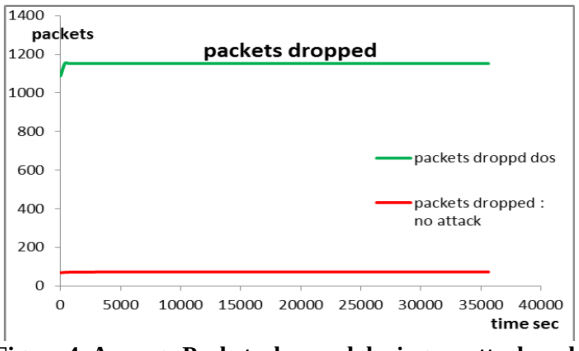

Figure 4. Average Packets dropped during no attack and DoS attack on router.

Figure 4, clearly shows that in a span of 10 hours, the number of packets dropped in DoS attack is nearly 1200 packets as compared to merely a 100 packets during the period with no attacks. This is a significant gap to evaluate the performance of the network in both the cases. The reason for the significant difference in loss of packets is the faulty traffic of the attacker which reduces the performance drastically and overloads the network. As the attacker overloads the network the legitimate users are not able to use the resources available.

In figure 5, the impact of load on the network due to traffic introduced by attacker is shown. This time the attack is on the coordinator. Due to the Denial of Service attack on the coordinator, there is a deep impact which degrades the performance significantly due to the over load of traffic, as shown in the graph. The load in case of attack on coordinator is higher i.e. (27500 bits/sec) compared to the load in case of an attack on router i.e. (9100 bits/sec) and attack on end device. Hence, the simulation results show that the impact of DoS attacks on performance of WSN can be more severe, if carried out on coordinator, instead of just targeting the router or end devices. In case of no attack, as shown in figure 8, the load on the network is much lower compared to all the other case of attacks.

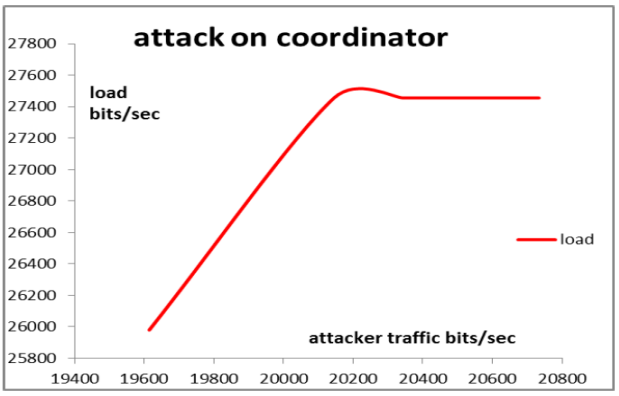

Figure 5. Average Load vs. Average Traffic of attacker during attack on coordinator.

Conclusion

The scenarios considered are mainly taken from the literature. The simulation results show that the impact of Denial of Service attacks on performance of WSN can become quite significant. In case there is an attack on the coordinator, node the performance degradation is more severe. This is mainly because the other nodes cannot access to relevant information used for routing which is available in the coordinator node. A simulation study of a Wireless Sensor Network has analysed the effects of various kind of attacks. The scenarios considered are no attack, attack on coordinator, attack on router and attack on the end devices.

ISSN: 2277-9655
Impact Factor: 1.852

The simulation tool OPNET 16.0 is used effectively for detailed analysis. The effects of the DoS attack targeting the router node is also quite significant, but routing related computations can be conducted in coordinator node in case the gateway node is overwhelmed. In case of attacks on end devices the overall network is not affected as severely as the ones mentioned above.

It is desirable to further extend these studies in order to analyse the effects of DoS on energy related policies. Such a study would be essential since energy consumption is very critical for WSNs.

References

[1] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks, *IEEE Communications Magazine*, 40(8):102–114, August2002.

[2] Healy.M, Newe.T, Lewis.E, „Security for Wireless Sensor Networks: A Review", IEEE Sensor Application Symposium, New Orleans, LA, USA-Feb 17-19, 2009.

[3] Raymond, D.R, Midkiff, S.F, „Denial of Service in Wireless Networks: Attacks and Defences, IEEE CS: Security and Privacy, 2008,pg 74-81.

[4] Yahaya.F.H, Yussoff.Y.M, Rahman.R.Ab, Abidin.N.H,"Performance Analysis of Wireless Sensor Network", 5th International Colloquium on Signal Processing & its Applications (CSPA), 2009.

[5] Vlajic.N, Stevanovic.D, Spanogiannopoulos.G, „Strategies for improving performance of IEEE 802.15.4/Zigbee WSNs with path constrained mobile sinks", Computer Communication Journals, 2010.

[6] OPNET Technologies, www.opnet.com

[7] ZigBee Specification v1.0: ZigBee Specification (2005), San Ramon,CA, USA: ZigBee Alliance http://www.zigbee.org/en/spec_download/download_request.asp

[8] Rui Silva, Serafim Nunes "Security Issues on ZigBee" (2005), http://rtcm.inescn.pt/fileadmin/rtcm/WorkShop_22_Jul_05/s2_Security Issues_on_ZigBee.pdf. accessed: 5 January 2009.