A Minor Project Synopsis

on

Detection and Mitigation of Sinkhole & DoS Attack in IoT Network

Submitted to Manipal University Jaipur

towards the partial fulfillment for the award of the degree of

Bachelor of Technology

In Information Technology

By

Prashant Tyagi

209302265

D

Suyash Srivastava

209302151

D

Under the Guidance of

Dr. Lokesh Sharma

Department of Information Technology

School of Information Technology

Manipal University Jaipur

2022-2023

Synopsis

1. Introduction

In a sinkhole attack, the attacker deliberately creates a "sinkhole" in the network to draw and intercept traffic meant for other nodes in the system. As many Internets of Things (IoT) devices have constrained processing capabilities and may not have built-in security methods to identify and defend against these types of attacks, sinkhole attacks can have major repercussions in the IoT environment.

A Denial of Service (DoS) attack is an attempt to make a system unavailable to the intended user(s), such as preventing access to a website. A successful DoS attack consumes all available network or system resources, usually resulting in a slowdown or server crash.

In recent years, there has been an increase in interest in the study of attacks in the IoT due to the proliferation of connected devices and the potential of cyberattacks. The study of attacks in the IoT is a significant step in ensuring the security and dependability of these systems and safeguarding sensitive data and individual user information that may be sent across these networks.

2. Motivation

Due to the increasing significance of the Internet of Things (IoT), ensuring the security of both the connected devices and their networks has become a critical concern in various industries. Attacks (like Sinkhole or DoS) pose a severe threat to the stability and security of IoT networks and must be comprehensively understood to minimize their impact. Therefore, studying the attack in IoT aims to increase awareness of its potential harm, develop innovative techniques for detecting and thwarting such attacks, and ultimately enhance the stability and security of IoT networks.

3. Project Objectives

- Identification of Sink Hole Attack on IoT networks
- Implementation of the Sink Hole Attack
- Analysis of the Implementation
- Mitigation Techniques

4. Methodology/ Planning of work:

The following methodology can be used to perform research on Sinkhole & DoS attacks on the Internet of Things (IoT) using NetSim:

1. Literature Review: Start by completing a thorough analysis of the literature on sinkhole and DoS attacks in the IoT as well as the instruments and methods employed to identify and lessen these attacks.
2. Setting Up a Simulation Environment: Use the NetSim tool to set up a simulation environment. This will enable you to build a virtual IoT network with multiple device kinds and communication protocols that resembles a real-world IoT network.
3. Attack Scenario Design: Create an attack scenario that represents a sinkhole assault and DoS assault on the IoT network. The characteristics of IoT devices, communication protocols, and network structure should all be considered in this scenario.
4. Data Analysis: Examine the information obtained from the simulation and make inferences regarding the efficiency of current defenses in spotting and thwarting attacks in IoT environments.

5. Facilities required for proposed work:

NetSim Standard 13.0.x64
Visual Studio Code
Wireshark

Bibliography/References

https://www.tetcos.com/netsim-documentation.html
https://www.tetcos.com/downloads/v13.1/IOT-WSN.pdf