Marathwada Shikshan Prasarak Mandal's
Deogiri Institute of Engineering and Management Studies, Aurangabad

Software Requirements Specification

On

Web Traffic Management System

Submitted By

Snehal Sanjay Pradhan (36172)
Aditi Ajay Deshpande (36173)

Dr. Babasaheb Ambedkar Techological University
Lonere, Raigad (M.S.)

Department of Computer Science and Engineering
Deogiri Institute of Engineering and Management Studies, Chh. Sambhajinagar
(2022- 2023)

Contents

List of Figures

1. Introduction

1.1 Purpose

A Wireless Sensor Network (WSN) comprises of sovereign sensor devices that are used to supervise physical and environmental conditions like temperature and pressure. The WSN is built of hundreds and thousands of recognizing stations called nodes, where each node consists of one or more sensors having a radio transceiver, an internal/external antenna, a microcontroller and a battery. Wireless sensor networks are the systems that are used to communicate by sensing the behavioral changes and the sensing nodes will collect the data and it will get handled. After data handling, the data will be sent to the receiver.

1.2 Document Conventions

Font Size: Heading 16

Sub-heading 14

Main Content 12

Keywords: Network Security, Wireless, Sensor, Internet, System Security, Simulator, NS2, Simulation of attacks.

1.3 Intended Audience and Reading Suggestions

The objective of this workshop is to impart knowledge on networks and to explore an open simulation environment for computer networking projects and research. The targeted audiences are UG and PG students.The next intended audience is research oriented people and attack protectors.

1.4 Project Scope

Advantages:-

1. Ns2 simulation is cheaper sometimes.

2. Sometimes it finds bugs (in design) in an advanced manner.

3. Generality: over analytic/numerical techniques, it gives more generality.

4. Detail: At an arbitrary level, system details also can be simulated.

Objectives:-

1. Performance.

2. Direct Measurement.

3. Reactive.

4. The behavior/characteristics are affected when the user/system is disturbed.

5. The simulation can be done only on completed running systems.

1.5 References

1. https://networksimulationtools.com/ns2-simulation/

2.https://www.researchgate.net/publication/225252300_The_Replication_Attack_in_Wireless_Sensor_Networks_Analysis_and_Defenses

2. Overall Description

2.1 Product Perspective

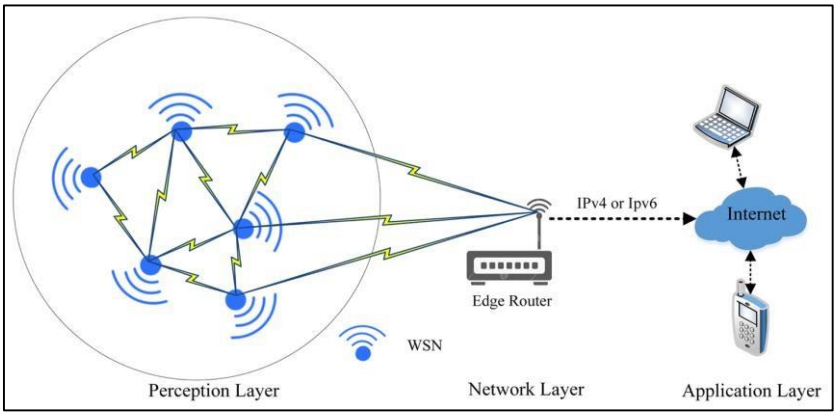

Figure 1 Architecture of WSN

Constructing a wireless sensor network (WSN) has become important in all places. The sensor nodes collect the data and direct it to the center station for processing and then it is directed to the user via a wireless medium. A WSN has copious applications in many fields. They are employed in many places.

2.2 Product Features

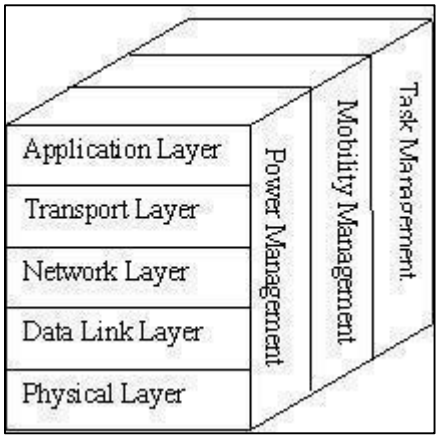

Figure 2 Layered Architecture

Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System. Base Station in a WSN System is connected through the Internet to share data.

2.3 User Classes and Characteristics

Network simulation (NS) is one of the types of simulation, which is used to simulate the networks such as in MANETs, VANETs, etc. It provides simulation for routing and multicast protocols for both wired and wireless networks. NS is licensed for use under version 2 of the GNU (General Public License) and is popularly known as NS2. It is an object-oriented, discrete event-driven simulator written in C++ and Otcl/Tcl.

2.4 Operating Environment

Processor: Intel i3 Core

RAM: 4GB and above

Hard Disk: 256 GB and above

PC: HP

Operating System: Windows, Kali Linux

Virtual Machine: VMware Workstation

Distribution: Ubuntu

Development Tool: NS2

2.5 Design and Implementation Constraints

The Simulation of the attacks is being done by using NS2 Simulator. It is an open source free simulator available online. It stands good for simulation of TCP, UDP and many other routing protocols. It works on an object oriented language called Tool Command language (OTcl). With the help of OTcl language, different network topologies and the routing protocols can be explained. The language is very easy to use and is platform independent. The code can be written for creation of the nodes, showing the data transfer and introducing the attacks and the simulation can be shown by running the simulator. The simulator consists of a wide variety of applications, protocols like TCP, UDP and many other network parameters.

2.6 Assumptions and Dependencies

Assumptions #1: Endpoint Security Is Enough

It’s a common assumption that if the network entry points made by individual devices—employee laptops, warehouse processing terminals—are secure, then nothing else needs to be done. Familiarity with common endpoint security such as anti-virus scanners and anti-spyware programs breeds a false sense of security. Simply because individual devices are secure does not mean the overall network is safe from cyber threats.

It's not enough to have endpoint security. Adding network security monitoring means accounting for portable devices, which might not be covered by an organization's endpoint security policy. Further, it means monitoring unusual traffic patterns of insider threats. Insiders will be familiar enough with company machines to bypass endpoint security—but with network security monitoring, their behavior on the organization's system will still be supervised.

Assumption#2: A Firewall Is Enough

In the past, an organization's firewall was regarded as the heart of its network security. Firewalls filter and block various types of traffic, allowing or disallowing it based on selected characteristics such as what ports are being used. While firewalls are still important security tools, the problem is that the threat landscape has advanced beyond the simple blocking capabilities of a firewall. Cyber attacks can come through browsers or email, for example, and an IT team can't prevent email breaches with a firewall. They need advanced network security monitoring. While firewalls don't have visibility into the content and context of network traffic, advanced security monitoring technology, such as SOCVue, can closely examine the details. With log management, SIEM, and other capabilities, the managed security service SOCVue can watch network traffic for unusual and possibly threatening patterns, unlike a firewall, which follows a blind set of simple, direct rules.

Dependencies:

Cyber dependencies exist when computer systems depend upon other computer systems. Dependencies exist between multiple types of computer systems and include both information and services. Dependencies upon services range from information processing and storage to system configuration and security controls. Computers also depend upon networks to transmit data and upon specialized storage devices to store data storage devices might require their own specialized communication networks.

3. System Features

3.1 System Feature 1

3.1.1 Description and Priority

Denial of Service (DoS) is a cyber-attack on an individual Computer or Website with the intent to deny services to intended users. Their purpose is to disrupt an organization's network operations by denying access to its users. Denial of service is typically accomplished by flooding the targeted machine or resource with surplus requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

3.1.2 Stimulus/Response Sequences

Denial of service Attack involves saturating the performance of the target node with lots of unwanted communication requests which will create fake traffic. These kinds of attacks overload the server. Here, DOS attack is implemented by using UDP protocol and CBR application.

Once its buffer size is full, the target node can be seen dropping the packets coming from the malicious node as well as the source. Node 41 is the source and node 50 is the destination. The packets from the source node are sent to the destination node via the target node 58. After sometime node 48 acts as a malicious node and starts sending huge number of packets to the target node. Since the target node buffer size is limited, it cannot handle all the packets and at time 23 sec will drop the packets coming from the malicious node 48 as well as the source node 41.This will lead to the loss of data and will degrade the service of the network.

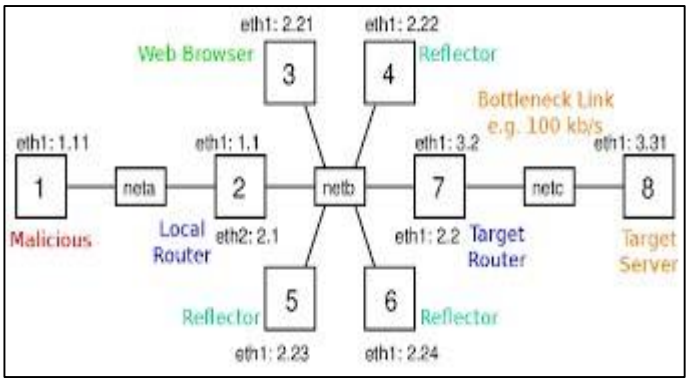

Figure 3 Dos Attack

3.1.3 Functional Requirements

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

3.2 System Feature 2

3.2.1 Description and Priority

Sybil attack is one of the most harmful and dangerous attack in WSN. It is the attack in which a node acts as a malicious node and claims multiple identities. When there are many systems connected in a network, a single system which is insecure will act as a malicious system and claims multiple identities. This can lead to many problems like false communication and loss of data. This sort of an attack must be recognized and must be prevented so that the system can be made secure. Maintaining the identities of the system is necessary. There are many authorities that help in maintaining the identity by using certification softwares.

3.2.2 Stimulus/Response Sequences

The simulation of the Sybil attack is done by using the NS2 Simulator. The attack can be seen by dropping of the packets of the intermediate node. This attack is one of the well-known attack in WSN. The attacker nodes may obtain the legitimates IP Address or Mac Address in order to Steal and make its own. Then the attacker node can do plenty of things with new stolen identity. Node 43 acts as source whereas node 44 is the destination node. The source node start sending packets to the destination node through the shortest path that is decided by the routing protocol. The intermediate node 15 acts as a malicious node and at time 30 sec, it starts dropping the packets coming from the node.

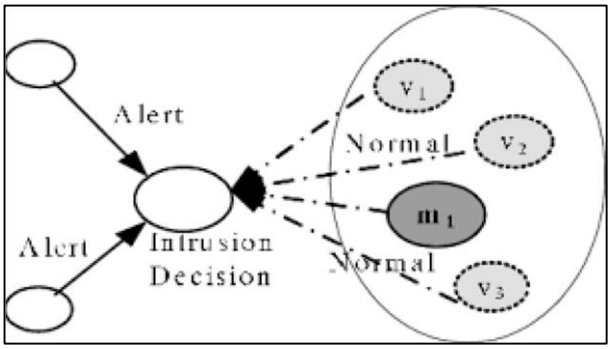

Figure 4 Sybil Attack

3.2.3 Functional Requirements

Sybil Attack is a type of attack seen in peer-to-peer networks in which a node in the network operates multiple identities actively at the same time and undermines the authority/power in reputation systems. The main aim of this attack is to gain the majority of influence in the network to carry out illegal(with respect to rules and laws set in the network) actions in the system.

3.3 System Feature 3

3.3.1 Description and Priority

The black hole attack is one of the well-known security threats in wireless mobile ad hoc networks. The intruders utilize the loophole to carry out their malicious behaviors because the route discovery process is necessary and inevitable. Many researchers have conducted different detection techniques to propose different types of detection schemes.

3.3.2 Stimulus/Response Sequences

In black hole attack, a malicious node uses its routing protocol in order to publicize itself for having the shortest route to the destination node. This aggressive node publicizes its availability of fresh routes regardless of checking its routing table. In this attack, attacker node always has the accessibility in replying to the route request so adapt the data packet and drop it (Biswas & Ali, 2007). In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from any actual node; therefore a malicious and faked route will create. When this route set up, now it's depending to the node whether to drop the packets or forward them to an unknown address.

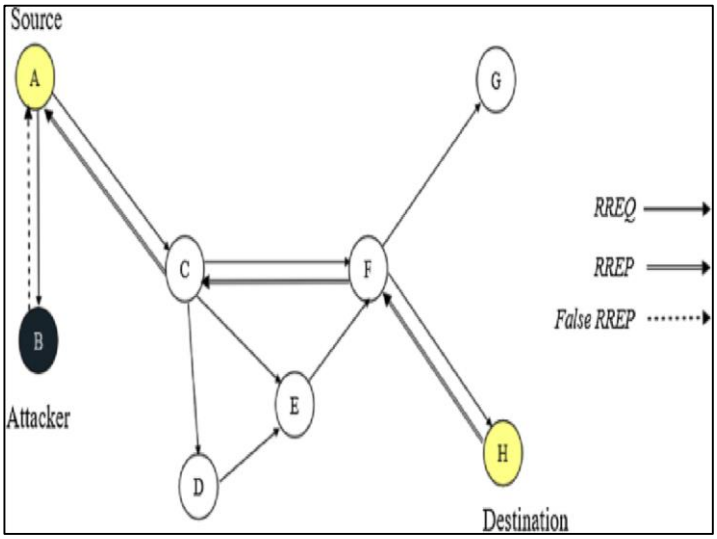

Figure 5 Blackhole Attack

3.3.3 Functional Requirements

The Blackhole attack works by blocking network traffic from a host or container. It drops Internet Protocol (IP) packets at the transport layer by using traffic policing features built into the Linux Kernel and the Windows Filtering Platform for Windows hosts.

3.4 System Feature 4

3.4.1 Description and Priority

Wormhole attack is a severe and popular attack in VANETs and other ad-hoc networks. This attack involves two or more than two malicious nodes and the data packet from one end of the malicious node is tunneled to the other spiteful/malicious node at the other point, and these data packets are broadcasted. In the wireless network, this malicious node even listens to the packets not intended for them and then tunnels them to the other end of the tunnel. A wormhole attack is capable of conducting a DOS attack, disrupting the routing of the network. Wormhole attack can easily disrupt the multicasting and broadcasting routing

3.4.2 Stimulus/Response Sequences

The idea behind this attack is to forward the data from one compromised node to another malicious node at the other end of the network through a tunnel. As a result the other nodes in the WSN can be tricked into believing that they are closer to other nodes than they really are which can cause problems in the routing algorithm.Also the compromised nodes may temper with the data packets.

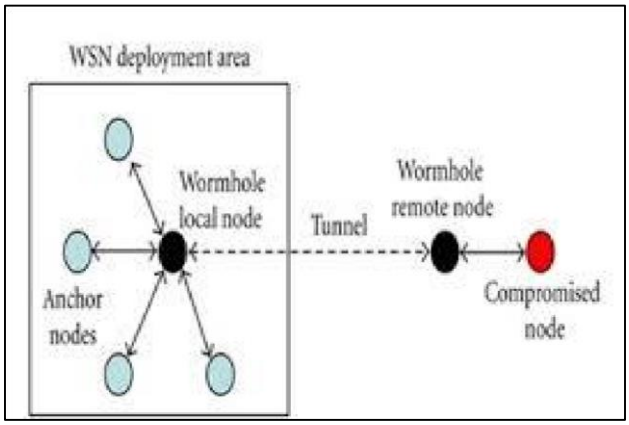

Figure 6 Wormhole Attack

3.4.3 Functional Requirements

A wormhole receives a message at its “origin end” and transmits it at its “destination end.” Note that the designation of wormhole ends as origin and destination is dependent on the context. We also assume a wormhole is passive (i.e., it does not send a message without receiving an inbound message) and static (i.e., it does not change its location).

4. External Interface Requirements

4.1 Hardware Interfaces

Processor	Intel i3 and above
RAM	4GB and above
Hard Disk	256GB and above
PC	HP

4.2 Software Interfaces

Operating System	Windows, Linux
Virtual Machine	VMware Workstation
Distribution	Kali Linux
Development Tool	NS2

4.3 Communications Interfaces

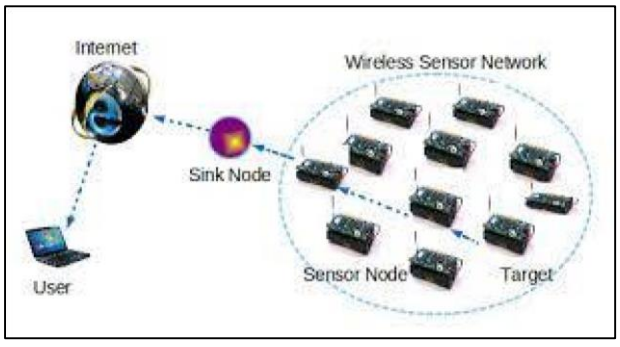

Figure 7 Communication interface of WSN

Constructing a wireless sensor network (WSN) has become important in all places. The sensor nodes collect the data and direct it to the center station for processing and then it is directed to the user via a wireless medium. A WSN has copious applications in many fields.

5. Other Non-functional Requirements

Requirements (NFRs) are system qualities that guide the design of the solution and Nonfunctional often serve as constraints across the relevant backlogs. As opposed to functional requirements, which specify how a system responds to specific inputs, nonfunctional requirements are used to specify various system qualities and attributes, such as:

1. Performance: fast system and it should respond to requests
2. Scalability: system can handle an increase in users or workload
3. Security: system should protect against malicious attacks and unauthorized access.
4. Usability: Using NS2 it is easy to detect the system attacks.
5. Maintainability: System is easy to maintain the malicious attacks.

5.1 Performance Requirements

The performance is dependent on the design of a network since the protocol, routing, topology, energy model, etc, have significant influence on the running of a simulator. It also depends on the internal design of the simulator such as its architecture, data structure, and algorithm. To quantify these issues, we employ some criteria to reflect the performance and efficiency of a simulated network, and use the simulation results to evaluate the simulator. Criteria employed in our evaluation include:

1. General information including simulation time and size of generated trace files.
2. Data transmission latency.
3. Number of transmission hops.
4. Amount of data packets transmitted.
5. Amount of dropped data.
6. Effectiveness of the network.
7. Utility of the network.

5.2 Security Requirements

Network security is a broad topic with a multilayered approach. It can be addressed at the data link layer, network layer and application layer. The issues concerned are: packet intrusion and encryption, IP packets and routing tables with their update version, and host-level bugs occurred at data link layer, network layer and application, respectively.

The TCP/IP protocols are being used globally irrespective of the nature of the organization whether it belongs to the general category of organizations or security specific sensitive organizations. The news -:"information about hacking of some website or portal by some undesired people is very common nowadays. This shows that TCP/IP protocols are susceptible to intercept. This generated a need to ensure all round security for the network in an organization. The task of network administrator had to widen to inc1ude the overall security of the network. He has to ensure that all parts of this network are adequately protected and adequate measures of security have been implemented within a TCP/IP network. He should be aware of an effective security policy. He should also be able to pinpoint the main areas of risk that the network may face. Basically, these main areas of risk vary from network to network depending upon the organization functioning. There are, therefore, various securityrelated aspects which have direct implications for network administrators along with the means to monitor the implemented measures of security effectively to tackle the problem of breach of security if it happens.

Basic Requirements of Network Security: The main objective of the network is to share information among its users situated locally or remotely. Therefore, it is possible that undesired users can hack the network and can prove to be harmful for the health of the network or user. There are few basic points which must be followed by network administrators to provide the network an adequate security other than network-specific security as in case of e-commerce, etc. These are given below:

1. Networks are designed to share information. Therefore, the network must be clearly configured to identify the shareable information and non-shareable information.

2. The network should also clear with whom the shareable information could be shared.

3. With the increase of system security, the price for its management will also increase accordingly, therefore a compromising level between security and prices should be established as per the requirement of the network security system policy. This will largely depend upon the level of security needed to apply in the network, overall security requirements and the effective implementation of chosen level of security.

4. Division of the responsibilities concerning the network security must be clearly defined between users and system administrators.

5. The requirements for security must be detailed within a network security policy of the organization that indicates the valuable data and their associated cost to the business. After defining the detailed network security policy and identifying the clear cut responsibilities in the organization, the system administrator should be made then responsible for ensuring that the security policy is effectively applied to the company environment, including the existing networking infrastructure.

5.3 Software Quality Attributes

Following are the software quality attributes:

Sr.no	Quality Attributes	Description
1	Performance	Fast system and it should respond to requests.
2	Scalability	System can handle an increase in users or workload.
3	Security	System should protect against malicious attacks.
4	Usability	Using NS2 it is easy to detect the system attacks.
5	Maintainability	System is easy to maintain against malicious attacks.