Chapter 8
Firewall in Underwater Wireless Sensor Networks

Manni Kumar
Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

Osho Gupta
Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

Shikha Rani
National Institute of Technology, Kurukshetra, India

ABSTRACT

In this technological arena, a firewall is a major tool for network security system to predetermine its basic rules so that it can control and monitor incoming and outgoing network traffic. The firewall generally restricts the faulty and unusual data entering the system. It can be categorized as host-based firewalls and network-based firewalls. There are various applications of firewall and how these firewalls can help the underwater wireless sensor network (UWSN) in protecting the sensor nodes where a huge amount of sensitive data is communicated among different countries. Firewall mainly aims to secure the network from different attacking devices and the attackers in a very efficient way. Firewall creates a barrier in which only the authorized data can be passed through after continuously checking by the firewall policies. To protect a local system and network of system from threats which are generally network based firewall is the most effective way. The design of the firewall is required to be accurate as it acts as a filter at higher protocol layer and some levels of IP-packets.

INTRODUCTION

It has been observed a steady evolution in the information system of corporate sector, government agencies or any private organizations. Some of the developments that came to see are to support directed connected terminals in which there is a main data processing system which have its own central mainframe. Use of LAN's helps to interconnect PC's in an organization and also all the terminal units

DOI: 10.4018/978-1-7998-3640-7.ch008

(Alves et al., 2012). Network premises which consists of interconnected LAN's, PC's, servers, and the connected mainframe unit. Wide Area Network (WAN) consists of wide networks that are interconnected to each other. Every employee working in an organization need internet services to fulfil their task and if it is not provided by the company they can get a dial-up connection from the Internet Service Provider (ISP). Internet gives every facility that is required by the users but the main problem is data security on the internet (Barbeau et al., 2014; Goyal et al., 2016; 2017). There is huge amount of data present on the internet the internet service providers must ensure for the proper use of that data. Similarly in case of Underwater Wireless Sensor Network (UWSN) as network providers are increasing day by day, they don't have enough space to install their devices and communication lines so for that a unique concept of communication have been introduced that is UWSN. In UWSN a network is installed deep under the sea water to provide communication facility to different people among different countries. In this chapter we will discuss about firewalls and how firewalls can help to protect UWSN from various attacks (Chouiten et al., 2012; Goyal et al., 2018).

Generally firewalls works on the rule defined in them when a data enter in the system it checks the data with its defined table, if the data is secure which meets the requirements policy of the firewall it allows the data to enter. Every firewall has its default policy and every default policy has three actions (reject, accept and drop).Suppose when there is no rule defined to the server about the SSH connection the firewall will follow the default policy. Only the default policy allows the system to establish a connection to the server, if it is set to allow the other users can easily establish a connection to the server line therefore always set default policy as drop which is a great exercise (Dee et al., 1995; Goyal et al., 2019a).

The mentioned authors also discuss about various filtering techniques or types that can be implemented to protect data entering the sensor nodes and also how each firewall types have their own features of protecting the data. The main area to discuss is to protect UWSN from various kinds of external unusual activities or noisy data present in the data stream, this can only be secure with the help of the various firewalls which help to protect the noisy data to enter or pass through the nodes making a good way to transfer data in a decent way (Goyal et al., 2019b; Feldstein et al., 2008). This firewall also helps to protect against various attacks that can be enforced or performed in UWSN. Some of the attacks like attaching viruses or malware with the data packet, hijacking the sessions and get fully access to the nodes in which data is transmitted can be discontinued with the help of the firewall. So firewall plays a vital role to protect the network. Sometimes the attacker tries to overload the traffic by adding more number of data packets to a particular path that leads to slow down of the network. In this case firewall helps to discard the unwanted data packets from the path making it easy for the actual data packets to pass easily. The necessity of firewall is increasing as it provides the single point protection where inspecting and security of data can be imposed. It also helps to provide the log details about each and every event occurring within the nodes and that log contains information about what type and how much traffic is there and can only be accessible to administrator. Thus this is an important point as the firewall serves the same purpose as armed guard.

THE REQUIREMENTS OF THE FIREWALL

The giant cyber security professionalism of NCSA studied that only 4 percent of Americans have a proper knowledge of firewalls and rest around 90 percent they are completely unaware of the firewall. Sometimes without having the enough knowledge about firewall they set there firewall to off or sometimes