34

Various Defense Countermeasures against DoS Attacks in Wireless Sensor Networks

M. Premkumar, Dr TVP. Sundararajan , Dr. K. Vinoth Kumar

Abstract— Wireless Sensor Networks (WSNs) is actually a group of much kind of sensor nodes. These sensor nodes are restricted to limited capabilities, for collecting precise information. Security is one of the today's major issues in this era of advanced technology. Due to their unique deployment places ultimately in ornery territories WSN are supposing various kinds of attacks. Self configuration, autonomous device addition, network connection and resource limitation are the dominant features of WSN that makes it highly prone to network attacks. Denial- of- Service (DoS) is one of the practically common and competitive means of attacking these computing systems. Furthermore the limitations of energy, computation and computerized information for sensors etc, the risks are at some future timetually more when we talk virtually military and scientific applications. This research paper attempts to study the DoS attacks and its main types. The study will provide valuable knowledge about the defence measures for these attacks. Based on the survey we express the best approach to designing a WSN resilient against DoS attacks.

Index Terms— Wireless Sensor Networks, DoS Attacks, Classification, Countermeasures, Security, Energy, Computation.

1 INTRODUCTION

WIRELESS Sensor Networks (WSNs) consists many number of small sensor nodes communicated through They are used for surveillance and data collection purposes in many civilian applications such as military, home, agriculture, industry and healthcare. Wherever the deployment of infrastructure is difficult, it can be deployed which is the main advantage. Due to the constraints of vitality, computation and memory capacity of sensors so on, the WSNs have also been generally implemented in numerous applications; presenting the efficient and lightweight security protocol to avoid multiple attacks in WSN, particularly for the DoS attack is a enormous challenge [1-6]. Generally, different types of sensors are used randomly in WSNs to monitor the environment situations.

A Denial of service (DoS) attack is a attack which is extremely easy to implement, however is an exceptionally ground-breaking technique to attack the internet distributed systems. This kind of attacks can unplug the whole country's internet. The DoS attack is viewed as the section of cyber war strategies [7], however it is repeatedly used for Blackmailing and extortion purposes. In both wired and wireless environments [8], this DoS attack can be introduced by flooding the packets to a specific server to render them unresponsive. With the goal that the legal users won't get any desirable service from the base station. DoS attack is an effort to render a computer or network inaccessible to its legal users, such as disrupting the host services associated with Internet. Over the past few years, DoS attack has become an intensifying issue, foremost augment in the quality services of victims.

M.Premkumar , Assistant Professor , Department of ECE , SSM Institute of Engineering and Technology , Dindigul , Tamil Nadu , India.
prem53kumar@gmail.com

Dr.TVP.Sundararajan , Professor , Department ECE , Sri Sakthi Institute of Engineering and Technology , Coimbatore , Tamil Nadu , India.
suntvp@yahoo.co.in

Dr.K.Vinoth Kumar, Associate Professor, Department of ECE, SSM Institute of Engineering and Technology , Dindigul , Tamil Nadu , India.
vinodkumaran87@gmail.com