SESCAS: A System for Mitigating Forwarding Misbehaviour in Wireless Sensor Networks

Premkumar. M, Sundararajan. TVP, Bhuvaneswari. A, Bhuvaneshwari. M, Deepika. S

Abstract: ***Remote Sensor arrange is the most standard administrations utilized in business and modern applications because of its specialized advancement in the processing, communication and low-control utilization of installed PC equipment. Due to open sent nature, the attackers effectively attack the node, so there is an absence of security. To avoid this, Selective sending approach is actualized. This paper aims to establish a simple countermeasure Scalable and Energy efficient Single Check Point based Acknowledgement Scheme; SESCAS is to detect and isolate the misbehaviour node in a wireless sensor network based on time out and retransmission. We carry out extensive simulation experiments to evaluate and compare performance with the extensive CHEMAS, CAM and CAD. The result of the simulation shows that the proposed mechanism can diminish the false recognition rate, collision of packets, energy utilization rate, propagation delay; we likewise enhance the packet delivery ratio and identification rate.***

Index Terms: ***Check point detection, Forward misbehaviour, Software Cluster based Management, Wireless sensor network.***

I. INTRODUCTION

A wireless sensor network (WSN) is a network which consists of many low powered devices that are spatially deployed to supervise the environmental conditions in hostile areas. These gadgets, or nodes, when combined with routers and a gateway, give rise to a typical WSN system. These distributed nodes will communicate wirelessly to a central gateway. It provides a link between the wired world and them to collect, process, evaluate, and present the data. To extend distance and improve the reliability in a WSN, the routers can be used to gain an additional communication link between end nodes and the gateway. Currently, the WSNs are ready to be deployed at an accelerated pace. This new technology is exciting with unlimited potential for numerous application areas including environmental monitoring, medical applications, transportation, crisis management, homeland defence, entertainment and smart spaces.

Since, nodes of WSNs are exposed to different environmental factors during deployment stage and are often left unprotected during communication, this make them vulnerable to attacks. When sensor network are deployed in hostile environments security becomes more important as they are prone to different types of malicious attacks [16] & [22].The attacker easily attacks the nodes and retrieves the data or even change the data due to its open nature. Most of the networks routing protocol are not suitable for security purpose. WSNs are easily attacked by the popularly-known denial of service attack (DoS) [15] that mainly target the availability of services by interrupting network routing protocols or interfering with currently running communications. Selective forwarding attack means disruption in packet transmission due to the unfortunate invitation of one or more malicious nodes in the communication path. In selective forwarding attack, dropping of packets takes place due to the malicious node in the network. This malicious node does not allows the forwarding of the packet to the sink [14]. This type of selective forwarding attack drops the packet from the nodes in a random manner. In black hole attack [1] & [11], whereby an infected node drops any incoming packet without letting the communication parties have knowledge about it (blindly), is a problem that needs greater attention to address forwarding misbehaviour issues aroused due to such nodes.

In order to provide security for sensor network, various types of key management techniques are applied. Due to this attack, adversaries cannot forward the certain messages and simply drop them. This leaves the attacker to stick to an option to use a malevolent device to create a huge number of entities in order to gain influence in the network traffic. The ID of these malevolent nodes can be the result of forged network additions or duplication of existing legitimate identities. The attack especially Sybil targets fault tolerant schemes including distributed storage, topology maintenance, and multi-hop routing and it leads to data loss.

II. RELATED WORKS

In this paper, the selective forwarding misbehaviour is overcome [3], [11-13] & [21], which means the malicious node in the network, deny the forwarding packets and selectively drop the packets and lack of security in the network. This mainly affects the forwarding packet transmission efficiency. To overcome this, in the network, the neighbouring node will intimate the previous node regarding failure and then it decides to change the path. Then the packet follows the alternate path which means shortest path. The remaining packet is forwarded to the destination as it is. This leads to reduction in the fake recognition rate and improve packet transport efficiency.

Revised Manuscript Received on July 05, 2019.
Premkumar. M, Department of ECE, SSM Institute of Engineering and Technology, Dindigul, India.
Sundararajan. TVP, Department of ECE, Sri Shakthi institute of Engineering and Technology, Coimbatore, India.
Bhuvaneswari. A, Department of ECE, SSM Institute of Engineering and Technology, Dindigul, India.
Deepika. S, Department of ECE, SSM Institute of Engineering and Technology, Dindigul, India.
Bhuvaneshwari. M, Department of ECE, SSM Institute of Engineering and Technology, Dindigul, India.