Chapter 6

Malicious Node Detection Using Convolution Technique:

Authentication in Wireless Sensor Networks (WSN)

Priyanka Ahlawat
National Institute of Technology, Kurukshetra, India

Pranjil Singhal
National Institute of Technology, Kurukshetra, India

Khushi Goyal
National Institute of Technology, Kurukshetra, India

Kanak Yadav
National Institute of Technology, Kurukshetra, India

Rohit Bathla
National Institute of Technology, Kurukshetra, India

ABSTRACT

Considering the situation when the node which is entering in the network is a malicious node, it can check and record the various operations of the network which could be responsible for some serious security issues. In order to safeguard the network, the author propose an approach which is in view of the advanced encoding strategy, termed as convolution coding approach. According to the requirement of network, the initial bits are assigned, and by applying the convolution technique, the final code is generated for each and every node. Considering the fact that it is a digital method, the codes can be represented by using the binary number system. All the nodes that are a part of the network will be having their corresponding final binary code, say C. The verification of each node is carried out by matching the generated code C with the security code within a particular time period before transmitting the data. This process enables the detection of malicious or attacker node. Furthermore, to enhance the versatility and execution, the system is organized into clusters.

DOI: 10.4018/978-1-7998-7789-9.ch006

INTRODUCTION

Wireless sensor networks (WSNs) are basically described in the form of a collection of sensor hubs or nodes which are spread in a region and utilized for checking and recording various observations, perceptions and states of being of a specific domain and conditions of any particular surrounding. Because of the autonomous structures of Sensors networks, the nodes are having the permission to enter or then leave the system or formed network at any instant of time. It makes the system vulnerable and prone to attacks. The main characteristics of WSNs are their infrastructure-less nature and the ability that they can be self-configured without the need of any predefined structure or configuration. WSNs comprises of a set of a number of small senor nodes. The communication carried out in such network is wireless. Primarily, WSNs were developed for some complex military communications in certain areas where it was not feasible to establish wired networks. Nowadays wireless sensors are useful in numerous other applications, considering few as, industrial modelling, logistics, defence and security, forest fire monitoring, monitoring of poisonous gases etc. The key features of a WSN are that they are spatially distributed, infrastructure less, self organized, do not require any predefined structure. Generally, the sensor nodes are having very low storage capacity, low computational capabilities and limited supply of energy. Sensor nodes are allowed to be a part or leave the system at any given moment. This autonomous behaviour of the network which allows node mobility is solely responsible for some serious security concerns. Any malicious or attacker node can enter into the legitimate network and cause some serious damage. The secrecy and integrity of the information transferred within the network could be tampered or lost, threatening the entire sensor network.

Hence, there is a serious need of some security mechanism in order to keep the authenticity, integrity and confidentiality of the data which is being monitored, collected by sensor nodes and further transferred in the network for the purpose of its storage, processing and analysis. As these networks could be easily compromised due to its limitations, it is really critical to complete the task of detection and isolation of the malicious nodes for avoiding any chance of some further damage (Perrig A.,2002)

Till now a number of approaches are proposed and implemented in order to fulfil the objective of providing security standards to the network. One of approach among them is cryptography, which basically executes the task of securing the original data by the use of a key. Encryption could be done by two methods: symmetric cryptography and asymmetric cryptography. In the case of symmetric cryptography, we can use the same key for both of the operations .While with later cryptographic technique; we need to use unique keys for encryption and decryption. As there is a need of keys for encryption and decryption, each node in the network is to be provided with unique keys. Due to limited supply of energy and storage space in WSNs it becomes difficult to perform cryptography. Therefore, for the systems having bigger sets of sensor hubs or nodes, the process of generation of keys becomes cumbersome and more complex .Later some hybrid cryptographic techniques were also suggested such as a combination which make use of both type of cryptographic techniques and digital signature. However, the efficiency of these techniques was also not sufficient enough because the complexity used to increase with the networks having bigger sets of nodes, we are considering.

While with the implementation of this technique, we are considering to obtain a binary code word for security purpose, which need to be matched by all the nodes before accessing the information. The process of generation of code word is to be done into two steps.

Initially we the security bits are assigned according to the network requirement depending upon its size, which is directly proportional to the number of sensor nodes present in the system. After that