Chapter 12
Fruit Fly Optimization-Based Adversarial Modeling for Securing Wireless Sensor Networks (WSN)

Priyanka Ahlawat
National Institute of Technology, Kurukshetra, India

Mukul Goyal
National Institute of Technology, Kurukshetra, India

Rishabh Sethi
National Institute of Technology, Kurukshetra, India

Nitish Gupta
National Institute of Technology, Kurukshetra, India

ABSTRACT

Node capture attack is one of the crucial attacks in wireless sensor networks (WSN) that seizes the node physically and withdraws the confidential data from the node's memory. The chapter exploits the adversarial behavior during a node capture to build an attack model. The authors also propose a fruit fly optimization algorithm (FFOA) that is a multi-objective optimization algorithm that consists of a number of objectives for capturing a node in the network: maximum node contribution, maximum key contributions are some examples of the same. The aim is to demolish the maximum part of the network while minimizing the cost and maximizing attacking efficiency. Due to the multi-objective function, the authors attain a maximum fraction of compromised traffic, lower attacking rounds, and lower energy cost as contrasted with other node capture attack algorithms. They have developed an algorithm, which is an enhanced version of FFOA and has even better efficiency than FFOA.

DOI: 10.4018/978-1-7998-7789-9.ch012

INTRODUCTION

Node capture attack is a comprehensive attack in which the intruder physically captures the sensor node by extracting keys and confidential data. With technological advances in the field of wireless sensor technology, various operations such as catastrophic and defense monitoring can be painlessly and quickly deployed to wireless sensor networks (WSN)(Lin, C,2016) . The scattered nodes communicate wirelessly to a central gateway, which connects to the wired world where users can collect, process, analyze, and present the measured physical data. Though WSNs have their advantages as the nodes are autonomous, they still need to be addressed. Some of the most common and important challenges are coverage, scalability, QoS, and security. Amidst the challenges listed, security is a major issue to be addressed in WSNs. Sensor networks is extremely vulnerable to node capture attacks. WSN is a group of a huge number of low price, low control, and self-organizing specialized sensor nodes (Lin, C,2015). It is very much vulnerable to different physical attacks due to limited resource capacity and screened to the external atmosphere for circulating network data. The node capture attack is one of the major attacks in WSN in which the attacker physically captures the node and can remove the secret information from the node's memory or misuse the confidential data (Lin.2013). With technological advances in wireless sensor technology, various operations such as the health and defense monitoring can be quickly deployed to WSN. We focus on developing a multi-objective function using which we can compromise the network efficiently and quickly, unlike random attack (RA), maximum key attack (MKA), maximum link attack (MLA). WSN is a wireless network comprising a large number of self-operative and self-sufficient nodes, which comprises low cost, less control, and self-organizing qualities(Lin.2013). This type of network uses sensors for catastrophic and defense monitoring of physical and environmental situations. When such self-governing nodes are used with routers and gateways, it creates a wireless sensor network system. This technology has its applications in various fields, including military, medical, defense, environmental, and many more.There are various issues to be addressed in WSNs. Some of them are scalability, quality of service, size, security, and many more (Tague, P,2008). Out of all these, security is the biggest challenge. Due to tight resource capacity and its exposure to the outer environment, it is prone to various kinds of physical attacks. Broadly, attacks can be of two types: active attacks, including routing attacks, eavesdropping, and passive attacks, which include all attacks against privacy. The performance is measure with other methods, and thus gives the improved resilience in order capturing node, hash computations decreased, compromise probability for proxy nodes also reduced with a revoked link (Ahlawat,2018) . The result matrix is examined with old strategies in order of the number attacking rounds, capturing cost and traffic compromised.. The performance validated by number of path compromise, path length, and route ratio (Ahlawat,2018). With this analysis of keys and linear automated theory, develop a model that effectively describes the behaviour of that network with attack. Optimal control theory method design a response for the network, which provide a network with secure stability(Bonaci,2010).Node capture attacks are one of the most major attacks in WSN. Node Capture Attack is a kind of attack in which the intruder can access the entire network and perform any operation on the network. The attacker captures the sensor node by gaining access to cryptographic keys and secret information like key pre-distribution model(Shukla,2015). Earlier, node capture attacks were having limitations like a lack of attacking methods and low attack efficiency. There are different types of node capture attacks. The next stage of the internet's development i.e. the internet of things which makes the internet a physical network requires the objects to communicate with minimal human interference. This type of network made of mobile sensor nodes communicating with each other and working