International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209705 Volume 8, Issue 4, July – August (2021)

RESEARCH ARTICLE

Wormhole Detection Using Encrypted Node IDs and Hop Counts in the Event Report of Statistical En-Route Filtering

Ga-Hyeon An
Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea.
angachi576@skku.edu

Tae-Ho Cho
Department of Computer Science and Engineering, Sungkyunkwan University, Suwon, Republic of Korea.
thcho@skku.edu

Received: 01 July 2021 / Revised: 05 August 2021 / Accepted: 13 August 2021 / Published: 28 August 2021

Abstract – Wireless Sensor Network (WSN), there are low capacity, low cost, tiny sensor nodes, and sinks. Sensor nodes detect an event occurring in its surroundings and send data about the event to the sink. Sensor nodes have a limited transmission range and computational power. Since the wireless sensor network operates with limited resources than the ad hoc network, it is difficult to apply the defense method as it is, so research on a new defense method is needed. In a WSN, sensor nodes manage, monitor, and collect data for a specific environmental and physical application, and the collected data is transmitted to and used by a base station. Base stations are connected via the Internet and share data with users. Since the sensor node is composed of low power and low capacity, it is mainly used in an unattended environment, so it is easily exposed to various attacks and can be damaged. This type of network makes it difficult to detect wormhole attacks when they occur along with other attacks like false report injection attacks and Sybil attacks. Therefore, to prevent this, in this study, the hop count and the encrypted node ID are added in the report generation process of the statistical en-route filtering technique to detect wormhole attacks even when a wormhole attack occurs along with a false report injection attack to improve security.

Index Terms – Wormhole Attack, Statistical En-Route Filtering, Wireless Sensor Network, Hop Counts, Encrypted Node IDs.

1. INTRODUCTION

As shown in Figure 1, the WSN is consists of low-capacity, low-cost, intelligent, and tiny sensor nodes and sink [1]. Sensor nodes detect event data occurring around it and send a message to the sink. The WSN is mainly used in unmanned environments and has applications in the military, traffic, fire, health, GPS location, and more [2].

In WSN, sensor nodes are used to collect data by using wireless communication to monitor specific environments and physical applications with limited transmission range and limited computational power using small sensor nodes. Also, many applications deploy and use sensor nodes in an unattended environment, so the lifespan of the node can be determined by the battery life, so it uses low energy [3]. As such, the sensor node uses low power, low cost, and low capacity, and is deployed in an open environment such as an unattended environment, so it can be subjected to various attacks by attackers [4, 5]. Also, the types of attacks that occur at the OSI layer are different. Table 1 shows each attack occurring at the OSI layer [6].

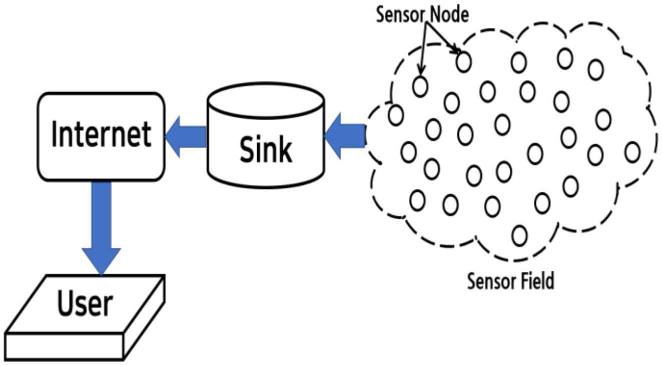

Figure 1 Wireless Sensor Network

Layers	Attacks
Physical Layer	Replay attack, Interference
Data Link Layer	Collision, Exhaustion, Denial of sleep
Network Layer	Selective forwarding attack, Sinkholes, Sybil attacks, Node replication attacks, Wormholes, Flooding, Hello flooding attack,