EAI Endorsed Transactions
on Mobile Communications and Applications
Research Article EAI.EU

E-HMAC: An Efficient Secure Homomorphic MAC Scheme for NC-Enabled WSNs

Haythem Hayouni*

SupCom, University of Carthage, Tunisia

Abstract

The main goal of Network Coding (NC) is to find an optimal transmission of data in a network. NC presents an advantage for wireless sensor networks (WSNs) in term of network lifetime. However, the Network Coding-enabled WSNs are affected by various attacks, such as pollution attacks. Many HMAC schemes have been proposed in the literature to secure packets against pollution attacks. In 2015, Esfahani et al. proposed a dual-homomorphic MAC scheme based to the construction of two different MACs to ensure the integrity of coded packets. Their solution has many weaknesses in terms of security against tag pollution attacks. In this paper, we improve their scheme by proposing a novel HMAC scheme for NC enabled WSNs, called E-HMAC, based on multi-linear space to check the integrity of coded packets. The simulation results demonstrate the ability of our proposed scheme to secure the coded packets with a low key storage overhead and communication overhead, compared to Esfahani et al.'s scheme.

Keywords: Network Coding, Wireless sensor networks, Homomorphic MAC, linear mapping, pollution attacks

Received on 06 May 2021, accepted on 26 September 2021, published on 29 September 2021

doi: 10.4108/_____

1. Introduction

WSNs [1] consist of a set of devices having limited computing resources. This type of network has attracted much attention in recent years, not only in academia but also in industry, for the study and development of a number of potential applications. However, the resource constraint is the most important feature of this network. Network Coding (NC) find an optimal transmission of data in a network. Network Coding can also improve network resiliency against attacks. Wireless Sensor Networks (WSNs) can benefit from the benefits of NC.

1.1 Motivations

In many applications of Network Coding-enabled WSNs, data can be threatened by external events that should not occur during normal network operation. Among these attacks, we find pollution attacks [2]. There are two types of pollution attacks: data pollution attack and tag pollution attack. In data pollution attack, the mission of an adversary is to insert fake data and to realize the verification of other innocent sensors which causes. In tag pollution attack, the objective of adversary is to get correct data packets be beaked as false and be isolated by intermediate sinks or nodes, which discard the correct packets. If a data pollution attack is not detected at the forwarders nodes, the base station cannot be able to verify if the received message is correct or not, and cannot check the source messages correctly. In WSN, as long as the polluted packets propagates via recording, a small number of these packets can affect the security of large number of downstream nodes. There are several cryptographic methods [3] providing the security and integrity of transmitted data such as Homomorphic MAC [4][5]. In 2015, Esfahani et al. proposed a dual homomorphic MAC scheme based the generation of two different MACs to ensure the integrity of

*Email: *haythem.hayouni@supcom.tn*