Abstract

The development of the internet of things (IoT) has been growing, such as wireless sensor networks (JSN). The use of JSN in daily life has helped a lot in various fields. JSN has interconnected nodes with limited memory, resources, and computation. Because of these limitations, messages or data on these nodes are in danger of being tampered with or known by attackers. In its development, JSN has several methods to secure the message or data. For example, broadcast authentication schemes and puzzle schemes using session keys [1]. In this paper, we propose a modification of broadcast authentication scheme by adding confidentiality aspects to messages and session keys. The session key is secured with a modified hill cipher encryption. The test results from the hill cipher implementation show that the time required for encryption with Backward Keychain is 98.697% lower than encryption with ECDH.

Keywords: IoT, WSN, *broadcast authentication*, *hill cipher*.