273. END TO END INTRUSION DETECTION SYSTEM IN WIRELESS SENSOR NETWORK

C.Abirami[1],Mrs. P. SARANYA M.E[2]
Department Of Computer Science And Engineering
Shreenivasa Engineering College
[1]abi.rajev04@gmail.com, [2]saranyapalanisamycse@gmail.com

Wireless Sensor Networking is one of the most promising technologies that have applications ranging from health care to tactical military. Although Wireless Sensor Networks (WSNs) have appealing features (e.g., low installation cost, unattended network operation), due to the lack of a physical line of defense (i.e., there are no gateways or switches to monitor the information flow), the security of such networks is a big concern, especially for the applications where confidentiality has prime importance. Therefore, in order to operate WSNs in a secure way, any kind of intrusions should be detected before attackers can harm the network (i.e., sensor nodes) and/or information destination (i.e., data sink or base station). A survey of the state-of-the-art in Intrusion Detection Systems (IDSs) that are proposed for WSNs is presented. Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) are the methods used for the encryption. In this encryption, conversion of file containing text is done using AES algorithm and key will be encrypted using ECC algorithm. Result will be text (cipher) which is decrypted on the receiver's side. AES and ECC algorithm implemented together to perform hybrid cryptography Techniques.

ISBN 978-81-904760-6-5