Abstract

There are currently more objects connected to the Internet than people in the world. This gap will continue to grow, as more objects gain the ability to directly interface with the Internet. Providing security in IoT is challenging as the devices are resource constrained, the communication links are lossy, and the devices use a set of novel IoT technologies such as RPL and 6LoWPAN. Due to this it is easy to attack in IoT network. The proposed system is a novel intrusion detection system for the IoT, which is capable of detecting Wormhole attack and attacker. The proposed methods use the location information of node and neighbor information to identify the Wormhole attack and received signal strength to identify attacker nodes. Design of such system will help in securing the IoT network and may prevent such attacks. This method is very energy efficient and only takes fixed number of UDP packets for attack detection, hence it is beneficial for resource constrained environment.

References

- IETF, RPL. "Routing Over Low Power and Lossy Networks."
- Wallgren, Linus, Shahid Raza, and Thiemo Voigt. "Routing Attacks and
- Yifeng Zhou, Lamont L, Li Li, "Wormhole attack detection based on distance verification and the Use of hypothesis testing for wireless ad hoc networks", Military Communications Conference, MILCOM IEEE, 2009.

Index Terms
Computer Science
Networks
Keywords

Intrusion Detection  Internet of Things  RPL  Wormhole  Packet Relay  Encapsulation

RSSI