A Decentralized Secure Framework For Mitigating RPL Attacks in Smart Environment

Jaspreet Kaur
Student of Computer Science & Engineering
Indian Institute of Technology
Jodhpur , India
kaur.3@iitj.ac.in

Abstract

The Routing Protocol for Low-Power and Lossy Networks (RPL) is the existing routing protocol for Internet of Things (IoT). RPL is a lightweight, Distance Vector protocol which offers security against various forms of routing attacks. There are various attacks which is possible in the RPL network, it may be from externally or internally. But we have to protect this network from both. These attacks are occur due to problem of unauthenticated or unencrypted control frames, centralized root controller, compromised or unauthenticated devices and many more ways. There are various solutions present in the literature but every solution has its pros and cons. There is no appropriate system framework till now which completely solves these all issues. So, we present a decentralized secure framework in the smart environment to mitigate these attacks more efficiently and effectively. In this paper, we provide the theoretical analysis of this approach which provide better protection from these attacks than any other method.

Introduction

In todays world, IoT is technical revolutionary area in mobile and wireless communication field which deploy Low power and Lossy Networks. These networks are typically composed of many heterogeneous embedded devices with limited power, memory, and processing resources. Now, IoT is applicable in many areas such as smart home, health care, environmental monitoring, smart city and smart grid etc.

RPL is distance based protocol used for routing in IoT network. A RPL protocol creates a Destination Oriented Directed Acyclic Graph (DODAG) which consists of paths from the sender nodes to the sink node. During routing, every node maintains its rank relative to its position in the DODAG tree, and every DODAG is maintained by control information . The control frames are used by DODAG are DODAG Information Object (DIO),Destination Advertisement Object (DAO) and DODAG Information Solicitation (DIS) for transmitting the DODAG information. Route path selection is a key factor for RPL that use the Various metrics such as hop count, energy minimization and latency to compute the best route path.

Motivation

There are various attacks possible in RPL network either from externally or internally which significantly impact the network resources, topology and its performance. The attacks are increased or decreased rank attack, version number modification, flooding, sinkhole attack, blackhole attack, sniffing, identity attack and many more. There are various firewalls, Intrusion detection systems and many more solutions are available for prevention of these attacks.But these attacks are still possible due to the problem of unauthenticated or unencrypted control frames(such as rank attacks, version number attacks), centralized root controller(single point of failure), compromised or unauthenticated devices and many more ways. These attacks become more stronger when combine to other attacks. So, we need a approach or framework which completely remove these attacks.

Proposed Framework

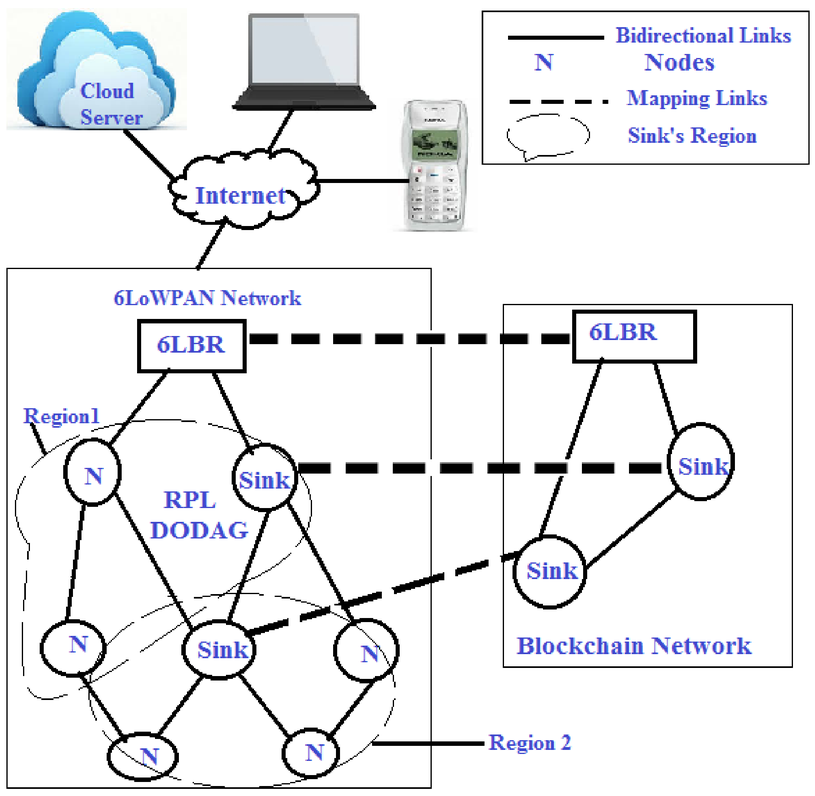

Figure 1: Proposed Framework

A RPL network is made up of heterogeneous embedded devices or sensors. In RPL network, there is only one sink node called as 6LBR(6LoWPAN Border Router as root node) which causes single point of failure. But in this work, we use multiple sink nodes which are finally designated to the 6LBR. These sink nodes are the devices which has the high memory, capability and processing power than the normal sensors nodes. These sink nodes have the capability and power as close as to the root node. In this work, we assume that sink nodes are stationary for better resource utilization when implementing blockchain (tracking of packets for correct route selection and more authentication) on these. Normal sensor nodes are stationary as well as mobile. Every sink node has covered a particular area of transmission region as shown in proposed framework.

Sensor nodes are attach to the closest sink node. This closeness is depends on the parameters such as: hop count, energy minimization and latency. At last all these devices along with sink nodes create a DODAG. In this DODAG, all control messages are encrypted for increase the privacy of messages. Now blockchain comes, which is fundamentally a decentralized, distributed, shared and immutable database ledger that stores data across a peer-to-peer network. It has chained blocks of data that have been timestamped and validated by miners. Fundamentally, the block data contains a list of all transactions(in this case all control frames) and a hash to the previous block. The blockchain has a full history of all transactions and provides a global distributed trust. In this work, DODAGs all sink nodes including 6LBR are mapped to the blockchain structure and create a secure distributed ledger for all the communication occurred in the RPL network. The number of multiple sink nodes including 6LBR are lie between 10-15% of total sensor nodes available in RPL network.

Results

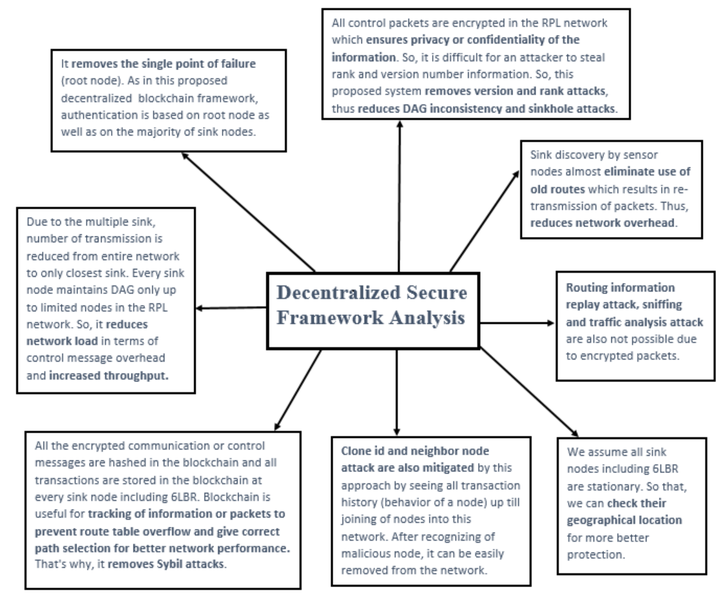

Figure 2: Theoretical Analysis of Proposed System

Conclusions

RPL network is prone to various kind of attacks as rank, version modification attack and sybil attack etc. These attacks are very dangerous for the network resources and performance . These attacks are occur due to problem of unauthenticated or unencrypted control frames, centralized root controller, compromised or unauthenticated devices and many more ways. There is no standard protection framework developed yet in the survey. So, we develop a decentralized secure framework for mitigating RPL attacks in smart environment. In this approach we use multiple sinks, encryption and blockchain mechanisms for protection to these attacks. Then, we theoretically analyzed our approach which is very effective and reliable for mitigating these attacks. It also reduces network overhead along with increases the performance and throughput of the network due to the multiple sinks. These nodes information are never compromised by the attacker due to the encryption techniques and distributed blockchain authentication.

Forthcoming Research

In the future work, Firstly we will do simulation or real time implementation of this approach using network simulator (NS3) for RPL Secure network along with Ethereum blockchain. After that we will focus on more attacks such as Zero day attacks in RPL protocol and other layers attacks in IoT stack. We also want to reduce the complexity of our approach as low as possible through new ideas such as use of ring signature instead of digital signature in blockchain. Lastly we must ensure, our approach is backward compatible to original protocol.

References

[1] Khan, Minhaj Ahmad, and Khaled Salah. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems 82 (2018): 395-411.