Available Online at http://www.journalajst.com

ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ISSN: 0976-3376

Asian Journal of Science and Technology
Vol. 14, Issue, 08, pp. 12618-12621, August, 2023

RESEARCH ARTICLE

SOLVING DECREASED RANK IN RPL ATTACK: THE ETHEREUM BLOCKCHAIN APPROACH

***Joshua Teddy Ibibo and Mwrwan Abubakar**

Blockpass ID Lab, School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK

ARTICLE INFO

Article History:
Received 19th May14, 2023
Received in revised form
10th June, 2023
Accepted 21st July, 2023
Published online 24th August, 2023

Keywords:
IoT, RPL, Blockchain,
Smart Contract, Attacks.

ABSTRACT

The routing protocol of nodes in RPL networks will now use a safe blockchain-based authentication system, according to this study. The Ethereum blockchain and smart contracts are used in the suggested approach to address the security issues, notably Decreased Rank At-tack in RPL network topology. The background of RPL, IoT-LLNs, and blockchain technology is covered in the study, along with the suggested methodology and its application. The study also assesses the performance of the suggested remedy and contrasts it with current approaches.

Citation: ***Joshua Teddy Ibibo and Mwrwan Abubakar.*** **2023.** "Solving decreased rank in rpl attack: the ethereum blockchain approach", *Asian Journal of Science and Technology*, 14, (08), 12618-12621.

INTRODUCTION

The increasing expansion of IoT devices has generated questions regarding the security of low-power and lossy networks and incorporation into a variety of domains [1]. Routing Protocol for Low-Power and Lossy Networks is a popular protocol for IoT-LLNs (RPL). Many internal cyberattacks are possible against RPL networks [2], which can exhaust the energy of sensor nodes that are already underpowered. Routing attacks against RPL also cause the IoT-LLNs to operate poorly, which can have deadly repercussions for essential applications running on the RPL network. In order to address the security issues in the topology of RPL networks, this research proposes a safe blockchain-based authentication mecha-nism for nodes' routing protocols [3]. To this purpose, a number of researchers have put forth different iterations of RPL that use blockchain technology as a means of authentication to prevent routing attacks or to enhance the routing performance of RPL in IoT-LLNs [3–8]. However, the blockchain technology has been researched and examined by the authors of [9] as a potential technique for safeguarding the IoT ecosystem. They provided many case studies demonstrating how IoT and blockchain may be used in tandem for things like access control, anonymity, and secure electronic transactions. They primarily examined the difficulties associated with connecting blockchain with IoT and made recommendations for future directions to address these difficulties, however they were unable to put the method for preventing internal RPL attacks into practise.

The following are the clear and original contributions of this publication:

- a cutting-edge, powerful architecture based on the blockchain that uses smart contracts to authenticate nodes and prevent malicious nodes from initiating routing attacks in IoT-LLN scenarios.
- The proposed solution successfully integrated Ethereum blockchain and smart contracts into the RPL network to provide a decentralized authentication and authorization mechanism.
- Our system demonstrated increased security and resilience against internal routing attacks compared to traditional RPL networks.
- The implementation of blockchain technology in the RPL network provided enhanced transparency and traceability, improving network management and auditability.
- We identified several blockchain features that can help enhance the defense mechanism at different layers of routing security in RPL networks.

The remaining parts of the research are arranged as follows. We give some background terms for RPL, blockchain, and the ongoing development in the com-puting work in Section 2. Section 3 of this paper's talks about the methodology that may be made safe against RPL attacks using current blockchain research. while in Section 4. We consider the implementation of the proposed method, and also the goal and main objective of the research, and Finally, in Section 6 we concluded with future study in the domain.

Related Background and Computing Work

Background: This section introduces the RPL prologue and gives a brief explanation of its operation. Also, we provide a brief introduction to blockchain technology.

**Corresponding author: Joshua Teddy Ibibo*
Blockpass ID Lab, School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK

RPL Terminologies RPL is an effective and efficient channel access system for distance-vector resources. In data networks, a distance-vector routing system determines the optimum path for data packets depending on distance [10]. RPL (DAGs) is built on the topological idea of directed acyclic graphs. The DAG dis-plays the default connections for the Low Power and Lossy Network (LLN) nodes as a tree. A DAG structure is more complex than a normal tree since a node can connect to several parent nodes whereas conventional trees can only have one parent. RPL restructure network nodes into Destination-Oriented DAGs (DODAGs), whose roots are the Internet's default gateways or sinks that are of-ten visited [4, 5]. The creation of the DODAG root comes first in the procedure. The root serves as a gateway, sending DIO messages including information such as rank, RPL instance ID, version number, and DODAG ID to connect with its neighbours. Based on the messages they receive, these DIO messages are multi-cast downstream, and the neighbouring nodes choose whether or not to join the root node. Nodes decide their rank and select the parent according to that rank in order to join the DODAG root. DAO messages have an upward route if they are sent to the root node. From all of the nodes, the parent with the lowest rank is picked. By delivering the DIS message, every new Node can join the DODAG. To protect IoT-LLNs against RPL attacks, a security strategy must be used to address the many flaws related to various stages of the routing process. In RPL, the routing procedure consists of three basic steps: DODAG advertisement level, Node joining the network level, and DODAG maintenance level [6]. The parent (root) Node propagates the LLN configuration data at the DODAG advertising level, which comprises MOP, version number, beginning rank, objective function, and DODAG Preference number. While a node is in the Node Joining the Net-work stage, many nodes, including a parent node or root node, may respond to a node's request for DODAG configuration information. After obtaining several replies, the requesting node must take the following actions: Initially, the en-quiring node chooses as its preferred parent the answering node with the lowest rank. The objective function of the configuration information and the rankings of the several responding nodes are then used to establish its rank. In order to complete route registration [7, 8], the node sends an advertising object to the sink node after delivering it to the parent node of its choice; The node may now publicise its presence to allow other nodes to join the LLN through it after submitting a membership request to the LLN. The network architecture of the DODAG maintenance level, the parent (root), and every other node in the LLN eventually update their views of the network by exchanging routing information at predetermined intervals controlled by a trickle timer.

Smart Contract According to our study, smart contracts should be utilised to send warning signals in the event of routing attacks, complete with bogus rank and version number details. Smart contracts, also known as "digital contracts," are software applications that provide a set of guidelines or protocols that are accepted by all peer-participating nodes. Smart contracts automatically confirm and uphold the terms of a contract or agreement without involving a third party in the process. Smart contracts, which protect data, are implemented on the Ethereum platform [7, 11]. A smart contract's conclusion for a particular transaction is also always known to participating nodes. On a proposed method offered by blockchain, smart contracts will be implemented. Blockchain Blockchain is a decentralised, public, and secure transaction ledger technology that is easily adaptable to complex network conditions. The failure of some nodes has no impact on the consistency of the system's operation. Dis-tributed authentication across nodes prevents hostile nodes from invading the network. Even a few compromised nodes won't be able to change the ledger. The "genesis block," which serves as the basis of the blockchain, is the first block and has no parents. As a result, the blockchain's three primary functions are block production, validation, and transaction [12, 9]. Every transaction that is started is verified and released. Blockchains can be classified as private, public, or consortium-based. Public blockchains are open for anybody to join without a licence, and miners update the blockchain with new transactions when the consensus procedure has been completed. Read rights on a private blockchain are openly accessible to all users, but write permissions are managed by a sin-gle central authority. In the consortium blockchain, which is semi-private, most access rights are controlled by a single organisation. Private blockchains offer anonymity, low latency, and little energy consumption, making them more suit-able for IoT. The fundamental benefit of Smart Contract construction provided by blockchain technology has greatly facilitated its broad adoption.

Computing Work

This section examines the pertinent works of the present plans: For rank attacks, the [13] suggests the Secure RPL Routing Protocol (SRPL-RP). Although it doesn't stop node communication routes when attacks authen-ticate, it primarily identifies, mitigates, and isolates attacks in RPL networks. Nevertheless, analytical findings revealed that the SRPL-RP significantly im-proves with a Packet Delivery Ratio (PDR) of 98.48%, a control message value of 991 packets/second, and an average energy usage of 1231.75joules, which blockchain technology was not depoloyed. The only information provided in this paper [14] is a brief summary of RPL, a suggested taxonomy of all recently published studies regarding rank assaults, various mitigation techniques, and the harm done to network parameters. As a conclusion, a discussion with some other recent studies about security against rank attack has been offered, along with a comparison between a number of assaults using the Friedman test ap-proach. However the author failed in the implement any method in mitigating the rank attack. In this article, the author [15] proposes a tiered model of IoT routing security to assess the flaws in each step of the routing process. More-over, they investigate ways to use blockchain's built-in characteristics to improve IoT-LLN routing security. In order to do this, we offer a blockchain-based frame-work with a smart contract for effectively identifying the sensor nodes involved in the alteration of LLN configuration information. However, we do not utilise blockchain to authenticate the rpl nodes in the rpl network architecture. To fight against rank cyberattacks on the RPL protocol, Dvir et al. created VeRA [16]. This system stops the attack node from changing its rank and uses the hash chain technique [17] to achieve it, however it is not used in the Contiki context. Publicly distributed blockchains' basic networking principles, as well as any potential security holes and system weaknesses, are thoroughly examined by the authors [18]. A study of the many blockchain integration strategies for the Internet of Things is provided by the authors [19]. The technique used in this work [20] controls how quickly rank values increase or decrease and uses one-way hashed functions like the secure hash algorithm 1 to prevent rank changes (SHA1). Regrettably, when hashing methods are utilised, this strategy raises operational expenses. As this technique needs the central authority to send a message verifying the receipt of the data packet, it is vulnerable if a rogue node mounts the data to gain rewards. The authors of [21] have investigated and assessed blockchain as a potential method for safeguarding the IoT ecosystem. In this author [22] summarises earlier research on the thorough decentralisation of IoT via blockchains, in addition to analysing specific blockchain-based IoT solutions and the challenges they provide. Problem Statement and Research Gaps The protection against routing attacks in LLNs is a critical barrier in implementing IoT in various domains. Existing security mechanisms for RPL networks are insufficient and vulnerable to several internal cyberattacks. The research gap lies in addressing internal attacks, specifically Decreased Rank Attack, in RPL networks. This project aims to propose a secure blockchain-based IoT framework to build a robust security mechanism against Decreased Rank Attack in RPL networks.

METHODOLOGY

The proposed solution employs the Ethereum blockchain and smart contracts to create a secure environment for nodes in an RPL network topology. Access control decisions and other important policies are implemented using smart con-tracts. The blockchain layer serves as an

additional layer of security in the net-work topology, authenticating communication links between the routing layer and the sensors layer. The implementation process includes network simulations using the Cooja simulator and the deployment of an Ethereum private blockchain network. The smart contract receives transactions from all nodes, extracts the sender node's address, matches it with the node ID, and sends events to all nodes in the topology to update their routing tables. The nodes update their tables based on the events sent from the smart contract.

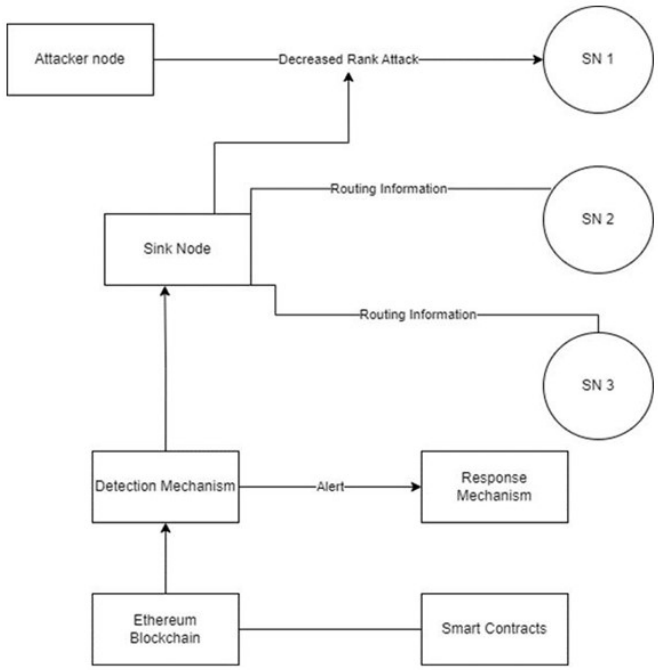

Fig. 1. Diagram of attack simulations

Implementation stage

The implementation stage of this project involves the following steps:

Setup the simulation environment:

- Install and configure the Contiki-NG operating system for IoT devices.
- Set up the Cooja simulator for simulating the IoT network with RPL routing protocol.
- Design the IoT network topology with Sink Node and Sensor Nodes, includ-ing the Attacker Node.

Develop the Ethereum-based blockchain infrastructure:

- Create a network of private Ethereum network.
- Use the Solidity programming language to implement smart contracts as the detection and reactional mechanisms.
- Install the Ethereum blockchain with the smart contracts.

Integrate the blockchain with IoT network:

- Create a communication interface between the Ethereum blockchain and IoT devices (Sink Nodes and Sensor Nodes).
- Include the features required to communicate with IoT device-generated smart contracts.
- Update the firmware on IoT devices to add the blockchain interaction and authentication capabilities.

Develop algorithms to monitor and analyze the routing data within the IoT network.

- Integrate these algorithms with the smart contracts to detect possible attacks and trigger appropriate responses.

Implement the Response Mechanism:

- Develop algorithms to respond to detected attacks, such as isolating the attacker node or adjusting the routing protocol parameters.
- Integrate these algorithms with the smart contracts to automate the response to any detected attacks.

Goal for this project: This project's main goal is to suggest and put into practice a safe blockchain-based authentication mechanism for the RPL (Routing Protocol for Low-Power and Lossy Networks) nodes' routing protocol. By addressing internal security problems and difficulties like the Decreased Rank Attack, the initiative seeks to increase the security of RPL networks.

Conclusion and Future Study: In this project, we proposed a secure blockchain-based authentication system for the routing protocol of nodes in RPL networks. The primary aim was to improve the security and resilience of IoT devices in RPL networks against in-ternal routing attacks, such as Decreased Rank Attack. The main findings and contributions of this project are as follows:

The proposed solution successfully integrated Ethereum blockchain and smart contracts into the RPL network to provide a decentralized authentication and authorization mechanism.

- Our system demonstrated increased security and resilience against internal routing attacks compared to traditional RPL networks.
- The implementation of blockchain technology in the RPL network provided enhanced transparency and traceability, improving network management and auditability.
- We identified several blockchain features that can help enhance the defense mechanism at different layers of routing security in RPL networks.

REFERENCES

1. Kim, H.S., Ko, J., Culler, D.E. and Paek, J., 2017. Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): A survey. IEEE Communications Surveys Tutorials, 19(4), pp.2502-2525.
2. Mosenia, A. and Jha, N.K., 2016. A comprehensive study of security of internet-of-things. IEEE Transactions on emerging topics in computing, 5(4), pp.586-602.
3. Sahay, R., Geethakumari, G. and Mitra, B., 2020. A novel blockchain based frame-work to secure IoT-LLNs against routing attacks. Computing, 102, pp.2445-2470.
4. Sahay, R., Geethakumari, G. and Mitra, B., 2020. A novel blockchain based frame-work to secure IoT-LLNs against routing attacks. Computing, 102, pp.2445-2470.
5. Singh, J., Dhurandher, S.K., Woungang, I. and Chatzimisios, P., 2022, May. Mul-tivariate Gaussian Mixture-based Prediction Model for Opportunistic Networks. In ICC 2022-IEEE International Conference on Communications (pp. 4932-4937). IEEE.
6. Rashid, A., Masood, A. and Khan, A.U.R., 2023. Zone of trust: blockchain assisted IoT authentication to support cross-communication between bubbles of trusted IoTs. Cluster Computing, 26(1), pp.237-254.
7. Ramezan, G. and Leung, C., 2018. A blockchain-based contractual routing proto-col for the internet of things using smart contracts. Wireless Communications and Mobile Computing, 2018.
8. Mohanta, B.K., Jena, D., Ramasubbareddy, S., Daneshmand, M. and Gandomi, A.H., 2020. Addressing security and privacy issues of IoT using blockchain technol-ogy. IEEE Internet of Things Journal, 8(2), pp.881-888.

9. Makhdoom, I., Abolhasan, M., Abbas, H. and Ni, W., 2019. Blockchain's adoption in IoT: The challenges, and a way forward. Journal of Network and Computer Applications, 125, pp.251-279.
10. Kamgueu, P.O., Nataf, E. and Ndie, T.D., 2018. Survey on RPL enhancements: A focus on topology, security and mobility. Computer Communications, 120, pp.10-21.
11. Sahay, R., Geethakumari, G. and Mitra, B., 2020. A novel blockchain based frame-work to secure IoT-LLNs against routing attacks. Computing, 102, pp.2445-2470.
12. Laurence, T., 2023. Blockchain for dummies. John Wiley Sons.
13. A. Almusaylim, Z., Jhanjhi, N.Z. and Alhumam, A., 2020. Detection and mitiga-tion of RPL rank and version number attacks in the internet of things: SRPL-RP. Sensors, 20(21), p.5997.
14. Boudouaia, M.A., Ali-Pacha, A., Abouaissa, A. and Lorenz, P., 2020. Security against rank attack in RPL protocol. IEEE Network, 34(4), pp.133-139.
15. Sahay, R., Geethakumari, G. and Mitra, B., 2020. A novel blockchain based frame-work to secure IoT-LLNs against routing attacks. Computing, 102, pp.2445-2470.
16. Dvir, A. and Buttyan, L., 2011, October. VeRA-version number and rank authen-tication in RPL. In 2011 IEEE eighth international conference on mobile ad-hoc and sensor systems (pp. 709-714). IEEE.
17. Glissa, G., Rachedi, A. and Meddeb, A., 2016, December. A secure routing pro-tocol based on RPL for Internet of Things. In 2016 IEEE Global Communications Conference (GLOBECOM) (pp. 1-7). IEEE.
18. Neudecker, T. and Hartenstein, H., 2018. Network layer aspects of permissionless blockchains. IEEE Communications Surveys Tutorials, 21(1), pp.838-857.
19. Ali, M.S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F. and Rehmani, M.H., 2018. Applications of blockchains in the Internet of Things: A comprehensive survey. IEEE Communications Surveys Tutorials, 21(2), pp.1676-1717.
20. Perrey, H., Landsmann, M., Ugus, O., Schmidt, T.C. and W¨ahlisch, M., 2013. TRAIL: Topology authentication in RPL. arXiv preprint arXiv:1312.0984.
21. Makhdoom, I., Abolhasan, M., Abbas, H. and Ni, W., 2019. Blockchain's adoption in IoT: The challenges, and a way forward. Journal of Network and Computer Applications, 125, pp.251-279.
22. Yeow, K., Gani, A., Ahmad, R.W., Rodrigues, J.J. and Ko, K., 2017. Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. IEEE Access, 6, pp.1513-1524.

****