Journal of Autonomous Intelligence (2024) Volume 7 Issue 2
doi: 10.32629/jai.v7i2.1183

ORIGINAL RESEARCH ARTICLE

Self-adaptive credit-based framework for blockchain-based IoT (BIoT)

Ritu Baniwal[1], Sunita Rani[2,*], Rashi Rastogi[3], Priyanka[4], Anju Jain[5], Shashikant Madia[6]

[1] *Department of Computer Science, Jyotiba Phule Govt College Radaur, Yamunanagar, Haryana 135001, India*
[2] *Department of CSE & IT, BPS Mahila Vishwavidyalaya, Khanpur Kalan, Sonipat, Haryana 131305, India*
[3] *Sir Chottu Ram Institute of Engineering & Technology, Ch. Charan Singh University, Meerut 250001, India*
[4] *Department of Computer Science, MNS Govt. College, Bhiwani, Haryana 127001, India*
[5] *Department of Computer Science, Government College Hansi Hisar, Haryana 125033, India*
[6] *Department of Computer Science, Rajiv Gandhi Govt. College for Women, Bhiwani, Haryana 127001, India*
*** Corresponding author:** Sunita Rani, Sunita.bpsmv@bpswomenuniversity.ac.in

ABSTRACT

The Internet of Things (IoT) connects and improves crucial global technologies like sensor nodes. The Internet is evolving from a human-centric network to one that enables inanimate things to wirelessly communicate with one another. The lifespan of an IoT network may be affected by the energy requirements of its routing protocol. Data is transmitted through the internet, and it may compromise the security of the data. An attacker can access the data and modify the data in order to break the security of the network. Although various solutions are available, such as cryptography and steganography-based approaches, none provide secure data transmission in large-scale networks with low energy consumption. Blockchain technology plays a vital role in the prevention of network malware. In this paper, an attempt has been made to propose a credit-based mechanism for secure data transmission in an efficient manner with low energy consumption. In order to achieve optimal results, the proposed framework uses blockchain for data security and credit distribution to avoid delays. The proposed framework has been simulated using the Contiki Cooja (CC) simulator. The efficiency of the proposed framework is measured by comparing its performance with state-of-the-art techniques.

Keywords: blockchain; IoT; routing; attack; credit and security

ARTICLE INFO

Received: 29August 2023
Accepted: 20 September 2023
Available online: 12 December 2023

1. Introduction

IoT is a global network of individually identifiable physical items (e.g., gadgets, machines, appliances) embedded with electronics, software, and sensors. Without any human interaction, IoT devices may share data via the web[1]. The information generated, analyzed, and choices made by the IoT are all related to the linked items. The full promise of IoT-based applications has not yet been realized, however, because of security issues arising from the sensitive nature of the data handled by such apps[2]. Unfortunately, blockchains have a high computational requirement that is challenging to achieve in a scenario where there are little available resources for the IoT. It is expected that IoT devices would be needed to participate in a blockchain consensus process in the future[3], despite the fact that they are now unable to do so. One approach to do this is by hardware acceleration of the most computationally costly section of the protocol, which is often a large number of iterations through the cryptography-based approaches and hash function[4].

Each participant in a blockchain network stores their own copy of each transaction[5]. All financial dealings are open to public view, making it easy to spot any alterations. Imagine a city where available parking spots are updated in real time online. When sensors find a vacant parking spot, they notify the master database. The authenticity of the sensor readings has been compromised. By removing the middleman, a blockchain network of linked devices can guarantee that unaltered, real-time data from sensors reaches all nodes in the network. The blockchain also makes it possible for IoT gadgets to independently exchange data and make choices[6]. In addition to digital currency, the Ethereum Blockchain may be used as a platform for the creation of decentralized apps through the deployment of executable scripts known as smart contracts. The Ethereum Virtual computer (EVM) is a virtual computer used to execute such programs; it provides a layer of abstraction between the program and the underlying hardware[7].

Security issues including single point of failure, trust, and privacy are raised by the current trend toward centralized IoT systems. The blockchain's use of cryptography allows for reliability to be maintained without the requirement for a trusted third party. Recent interest in BIoT applications has been driven by the technology's promise to enhance privacy and security[8].

Data from the smart home's heterogeneous IoT devices, which might be of varying sizes and types, are communicated to the smart home gateway in a gateway-style BIoT architecture. The suggested design calls for a smart home gateway that can precisely regulate the IoT and process data as instructed by the user. However, there are restrictions on the suggested network design due to the increased computational complexity introduced by blockchain transactions[9]. Different BIoT devices and organization applications are depicted in **Figure 1**. BIoT architecture, which aims to address computational complexity challenges. The suggested architecture relies on the Ethereum Blockchain since it is the only solution now available that can serve the general public. The Ethereum Blockchain also facilitates cryptocurrency payment via the Ether token, in addition to blockchain programmability[10].

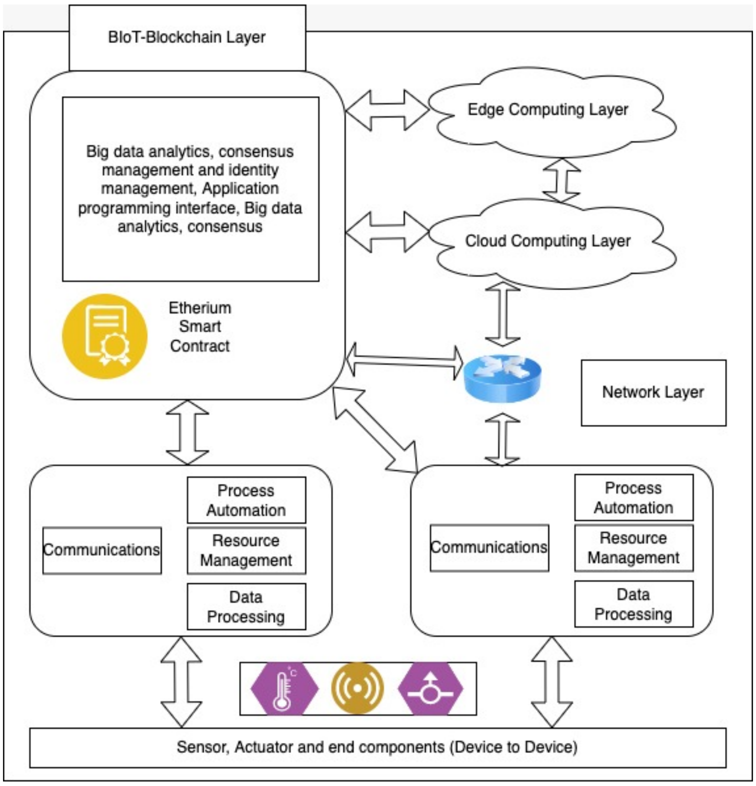


Figure 1. BIoT architecture.

Numerous devices capable of communication, computation, and data storage make up the IoT's physical layer. Modules for identity management, consensus, and P2P communication are all examples of typical services that may be found in the IoT blockchain service layer.

In addition, the distributed ledger is replicated on every BIoT device, so that any changes made to the IoT network are reflected in the network within minutes, if not seconds. Blockchain's big data analytics module can effectively store and analyse this data online, which is especially useful since IoT devices generate enormous amounts of data that cannot be managed with conventional techniques.

Multiple transactions are recorded in structured ledges, necessitating further data analysis. Smart contracts are another essential element of blockchain technology since they allow for autonomous choices to be made based on predefined parameters. An intelligent agreement is a piece of blockchain-based software that takes action based on the fulfillment or validation of predetermined conditions. The management of consensus is also an integral part of the coupling of blockchain and BIoT. The network's integrity relies on the central server's diligence in monitoring all of the nodes. It is possible for BIoT apps to use the API to connect to blockchain services. BIoT applications and data visualization processes make it possible for decision-makers to make informed judgments using data collected from actual BIoT devices at the application layer.

With the cloud computing layer in place, the company may greatly increase its storage capacity without investing in more on-premises servers. Information may be gathered from various sources and mediums, and it can be accessed from anywhere at any time[11].

The major contribution of this paper is:

- To examine the role of BIoT in secure data transmission for large-scale networks.
- To provide a credit-based framework for secure and fast data transmission in the IoT
- To provide a mathematical analysis of the proposed framework.
- To provide simulation results obtained from Cooja Simulator and compare the results with state-of-the-art techniques with performance metrics such as energy consumption and transaction cost.

The paper is divided into five sections. In section 1, an introduction to BIoT has been presented, along with the basic architecture of BIoT. Moreover, the contribution of the paper has been presented in this section. Section 2 discusses the review of the literature on different existing techniques based on BIoT that are used for secure, efficient data transmission. In section 3, the proposed framework has been discussed in depth with mathematical analysis. Section 4 provides simulation results that cover the tool used, simulation parameters, and performance metrics. At last, in section 5, the conclusion of the paper has been presented.

2. Related work

In order to construct goal-driven IoT systems that may autonomously Self-adapt to security threats in their surroundings (ASSERT), Alkhabbas et al.[12] suggest a distributed architectural Approach. ASSERT makes use of methods and concepts including agents, feedback loops, and blockchain to keep systems safe and increase confidence in their adaptations.

To reduce power consumption, Ahmed et al.[13] presented framework that use a cluster-level data aggregation technique. With blockchain embedded into a cloud server, the edge may be validated by the blockchain to guarantee the security of the services provided to IoT devices in real time. Finally, they simulated the system to determine its performance and compared it to that of more standard energy-efficient methods.

A safe and trustworthy algorithm driven by blockchain technology was presented by Sodhro et al.[14]. The suggested technique introduces a chain of blocks that uses less power, fewer cores, and somewhat more communication and computation bits to handle keys in a random fashion.

Mao et al.[15] provided a thorough overview of strategies for communicating and computing that minimize energy consumption in Industrial internet of things(IIoT) systems. In addition, classify the works already out there, study, debate, and compare the works to investigate their advantages and disadvantages.

The blockchain-based problem was examined at extent by Fernando and Saravannan[16], who offered solutions that included improving the blockchain's consensus mechanism and employing renewable energy sources to reduce the network's carbon footprint. Blockchain technology has to explore less energy-intensive alternatives to improve its ethical and industrial compliance and increase its flexibility across all industries.

For effective communication in industrial NIB applications, Sodhro et al.[17] present an ML-driven mobility management approach. Similarly, Zahid et al.[18] provide a state-of-the-art architecture for smart and connected healthcare that concurrently improves energy economy, battery life, and dependability.

For edge computing enabled IoT, Wang et al.[19] presented a framework that uses a security label, comprising the task's security level (SL) and its completion criteria, is intergraded into the block header to limit the ability of task receivers. In addition, BSDA protects against privacy leaks by segmenting critical tasks and task recipients.

Zhang et al.[20] presented an enhanced efficient-aware method (EEA) based on self-adaptive power regulation to reduce energy demand and increase the battery's useful life and improve its dependability. Finally, propose a layered, DL-driven design for IoMT. A fourth proposal makes use of wireless channel characteristics and body postures to simulate the energy consumption of IoMT.

In order to increase the scalability and decentralization of the prosumer grouping mechanism in the context of peer-to-peer energy trading, Ali et al.[21] propose a framework, an adaptive model that makes use of blockchain technology. Prosumer groups may be formed and transaction data can be stored using smart contracts.

In order to establish the amount of support and the attained satisfaction for IoT multimedia services, Singh and Lee[22] undertake a research of numerous self-adaptive security techniques for IoT multimedia and analyze them based on crucial, security criteria.

To counteract the risks to data privacy and security posed by IoT networks, Satamraju and Malarkodi[23] created a framework, a novel paradigm that combines the two technologies. Integrating authentication of devices, permission and access control, and data management are all tasks that benefit greatly from the usage of smart contracts.

Rasolroveicy[24]studied the latest findings in the field of Blockchain and IoT research, as well as self-adaptive systems and the documentation of various Blockchain platforms.

Wu et al.[25] build an optimistic scenario on top of blockchain technology and propose an analytical approach to the problem of energy usage balance optimization across several mobile devices and tasks. The corresponding ratio of approximation is studied. There have been various simulation experiments that evaluate the overall energy demand optimization approach vs the random technique.

Blockchain-based framework of an initial investigation by Yuan and Wang[26]. They discuss the connection between B2 ITS and PtMS, keeping in mind that blockchain is one of the protected and trustworthy architectures for constructing the recently established parallel transportation management systems (PtMS).

Articles proposing IoT security solutions are surveyed by Banerjee et al.[27]. The authors note many things, including the dearth of readily accessible IoT datasets for use by academics and industry professionals.

A more accurate evaluation of HD is possible with the use of an IoT platform developed by Subahi et al.[28], which employs a baysean mechanism. Vital indicators, such as electrocardiogram (ECG) and blood pressure, are recorded and sent to a computer while the patient wears the wristwatch and pulse sensor gadget.

Javaid and Sikdar[29] propose a blockchain architecture based on a block checkpoint mechanism and a dynamic proof-of-work consensus. The checkpoint establishes a distinct way to produce the next block hash in the blockchain.

Rana et al.[30] examines the current developments of various BIoT architectures, paying special attention to the technology, applications, difficulties, and possibilities that have arisen in this field. The Chinese remainder theorem (CRT) based approach is suggested and compared to the secure hash algorithm (SHA-256) for use in encrypting and generating keys for elliptical curve cryptography (ECC).

3. Proposed framework

This section has introduced the proposed framework for ensuring the safety of IoT data transmissions. This framework involves assigning and exchanging credits to nodes based on their past history of data exchange within the network. These credits represent value within the IoT and can be used to reward nodes.

In the first phase of proposed framework, all nodes are set up to be equally weighted contributors to the network so that routing may begin. At this stage, nodes receive the resources and TTL values they will use during the routing process. After the network has been set up, messages are sent between nodes using sender nodes and forwarded using relay nodes. Initiating the routing procedure also stimuli the agent node. An agent is a relay node that keeps track of how many bundle requests have been sent. It also keeps a database of each node’s trustworthiness. Our suggested approach uses a round-robin distribution method in which messages are sent from one agent node to another. Here, the agent gathers up all of the requests at once and then sends out the requests as a group to each of the other nodes. Nodes calculate the trustworthiness of the following node based on the messages they’ve forwarded to it. When nodes relay messages, this trust value is also modified. The **Figure 2** illustrates how the proposed approach works, which begins with the deployment of nodes at random to start the routing process through the COAP routing protocol. In addition, a node designated as an agent is made active and tasked with determining the trustworthiness of each node in the network. If the source node’s packet id (S_packet) matches the destination node’s packet id (D_packet), then the node is trusted; otherwise, it is labelled as malicious.

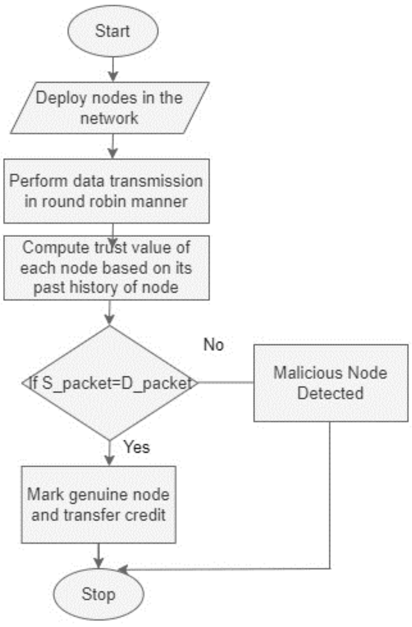

Start
Deploy nodes in the network
Perform data transmission in round robin manner
Compute trust value of each node based on its past history of node
If S_packet=D_packet
No
Malicious Node Detected
Yes
Mark genuine node and transfer credit
Stop

Figure 2. Proposed framework.

Mathematical model

This section provides mathematical analysis of above-mentioned algorithm. Here trust value (tv) of each node (N) is calculated. The trust value is fetched on the basis of initialization of total number of packets at sender side (S_packet) in perspective of delivery of total number of packets at receiver side(R_packet) as depicted in Equation (1).

$$tv = \frac{Transmitted}{Received} - Initialized \tag{1}$$

In this case, as shown in Equation (2), the estimated number of initialised packets (E_initialized) is a function of both the Preparation stage (T_preparation) and the used time (T_used). The sum of the Preparation and used times reveals the sum of messages that were started and maintained throughout the communication.

$$E_{initialized\_p} = T_{\mathrm{preparation}} \times T_{used} \tag{2}$$

The likelihood of a message being delivered successfully Using Equation (3), we can determine P(D). Specifically, think about the scenario where S is the event that a message is distributed and T is the occurrence that node is not malicious. To conclude, we employ Bayes' Theorem to

$$P(D) = \frac{P(T)P(S/T)}{P(T/S)} \tag{3}$$

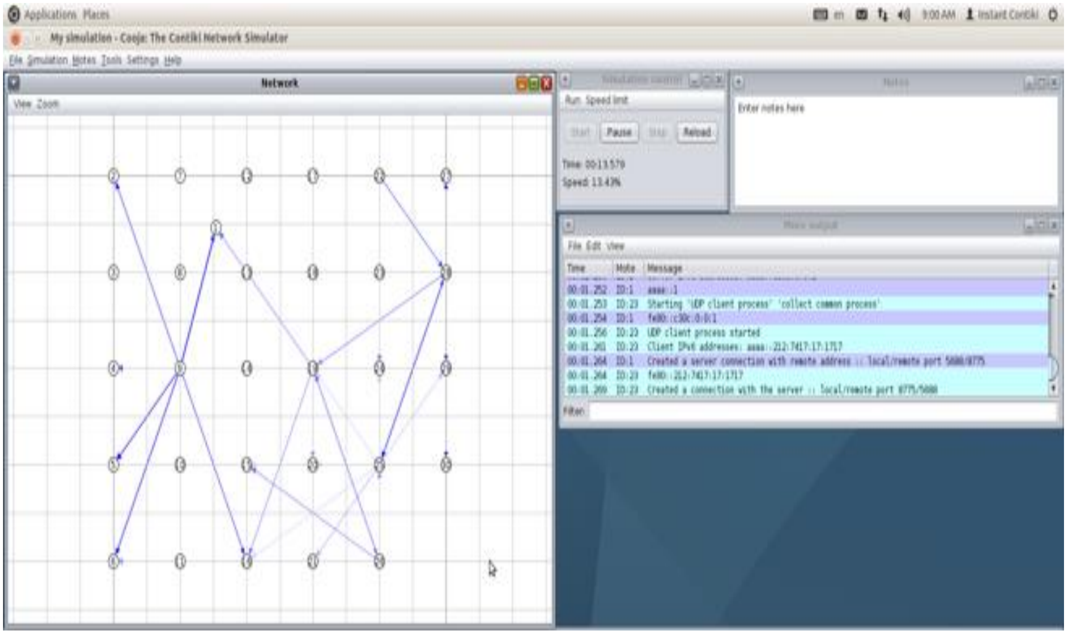
$P(S/T)$ = Checking with local tv to see how much a node is malicious. Here, we'll assume the node is not malicious by giving $P(T/S)$ as 1. The computed tv value is then written to the node's buffer storage. Agent node performs tv verification to ensure the node can be trusted.

4. Results

The proposed framework has been simulated with Cooja simulator. The Cooja is based on C programming and it is open-source platform for simulation. **Figure 3** depicts the simulation scenario of proposed framework. The Sky motes nodes are varied from 10 to 30 in the interval of 10 for performing simulation. Furthermore, the **Table 1** depicts the parameters used for simulation in Cooja simulator. The nodes communicate using Constrained Application Protocol (COAP). It is a designed for use with constrained devices with low power and low-power, lossy networks like those found in the IoT applications. COAP is intended to provide a lightweight and efficient way for these devices to communicate with each other.

Table 1. Simulation parameters.

Simulation parameters	Values
Range	50 m
OS	Contiki 2.7
Simulation duration	60 minutes
Routing	COAP
Node	Sky mote
Topology	Linear

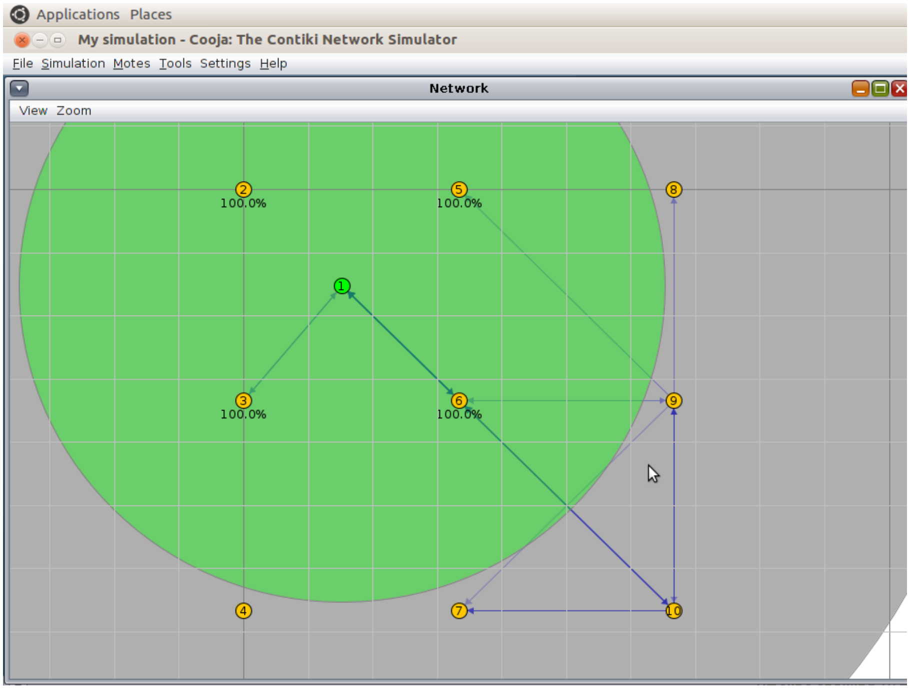


Time: 00:13.579
Speed: 13.43%

```
Time       Mote   Message
00:01.252  ID:1   aaaa::1
00:01.253  ID:23  Starting 'UDP client process' 'collect common process'
00:01.254  ID:1   fe80::c30c:0:0:1
00:01.256  ID:23  UDP client process started
00:01.261  ID:23  Client IPv6 addresses: aaaa::212:7417:17:1717
00:01.264  ID:1   Created a server connection with remote address :: local/remote port 5688/8775
00:01.264  ID:23  fe80::212:7417:17:1717
00:01.269  ID:23  Created a connection with the server :: local/remote port 8775/5688
```

Figure 3. Deployment of nodes.

Figure 4 depicts the simulation scenario of the proposed framework when the number of nodes is 10. Whereas **Figures 5** and **6** show the simulation of 20 and 30 nodes, here the blue line shows the actual message transmission, whereas the green circle shows the range of nodes.



Applications Places
My simulation - Cooja: The Contiki Network Simulator
File Simulation Motes Tools Settings Help
Network
View Zoom
1
2
100.0%
3
100.0%
4
5
100.0%
6
100.0%
7
8
9
10

Figure 4. Data transmission during 10 nodes scenarios.

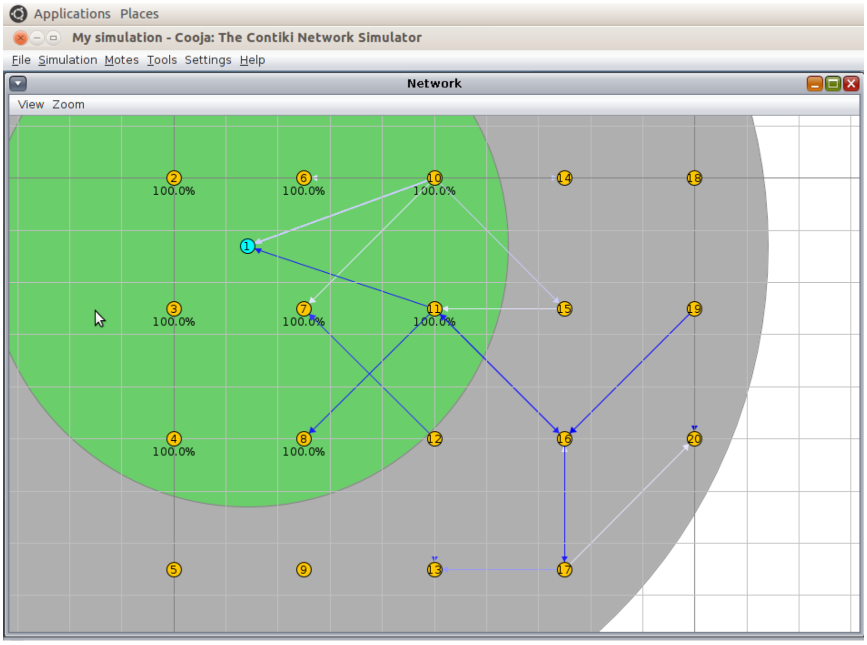

Applications Places
My simulation - Cooja: The Contiki Network Simulator
File Simulation Motes Tools Settings Help
Network
View Zoom
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
100.0%

Figure 5. Data transmission during 20 nodes scenarios.

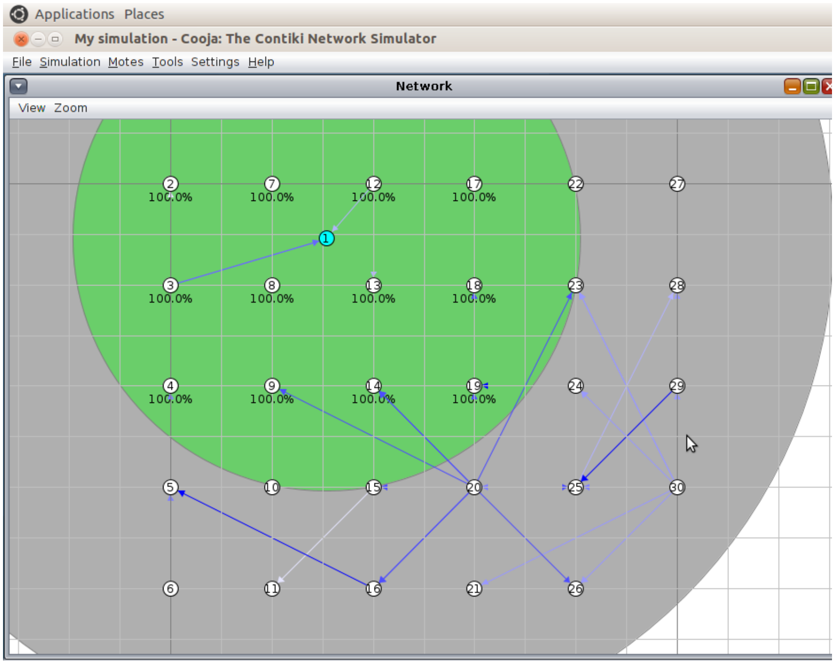

Applications Places
My simulation - Cooja: The Contiki Network Simulator
File Simulation Motes Tools Settings Help
Network
View Zoom
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
100.0%

Figure 6. Data transmission during 30 nodes scenario.

Figure 7 depicts the energy consumption comparison of the proposed credit-based framework with the existing ECC-CRT approach. The purpose of the improvements implemented in this study is to improve the total efficiency of the system and make it last longer. Battery life is a key consideration for IoT nodes due to their dependence on constant power to function. Here, focus on the real energy consumption of the IoT and the millijoule scale that models the estimation approach for the energy consumption rate. In the proposed credit-based framework, the energy consumption rate is low compared to the existing approach because the proposed framework distributes credits in order to achieve a low message drop rate. As messages are successfully delivered to the destination node without any interruption by malware, the rate of energy consumption decreases. Furthermore, a packet delivery ratio (PDR) comparison is depicted in **Figure 8**. The PDR is used to measure the performance of a network in terms of successful delivery of messages from the perspective of the total number of messages it receives. In the proposed framework, the rate of PDR is high compared to the existing approach.

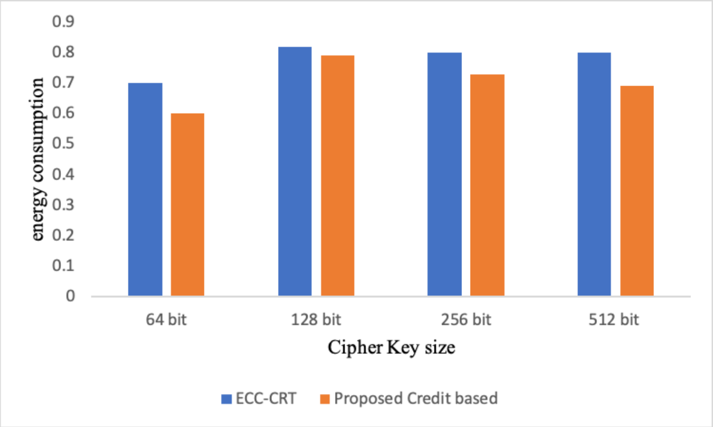


Figure 7. Power consumption comparison of proposed framework and existing approach.

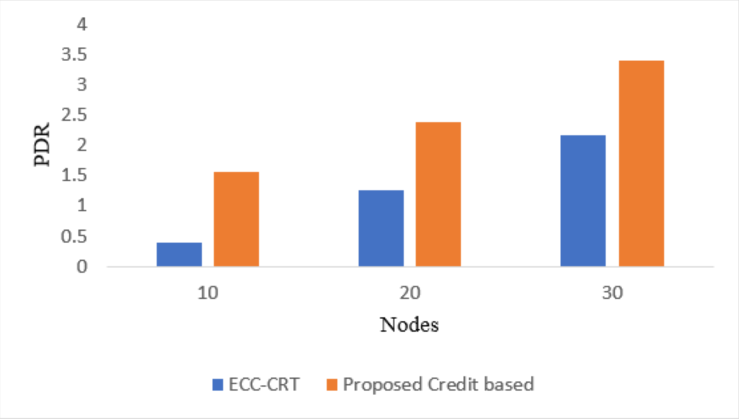


Figure 8. PDR comparison of proposed framework and existing approach.

5. Conclusion

The critical nature of most IoT resources makes them vulnerable to security breaches. To prevent network attacks, it is necessary to apply blockchain to the IoT network in order to achieve secure data transmission. This paper provides a secure framework that uses a credit-based method in which some credits or rewards are assigned to the node for the successful delivery of messages. This credit distribution method is really beneficial for fast and secure data exchange in the IoT. In the proposed framework, the malware is detected based on the past history of nodes by checking the number of messages it actually transferred in perspective of the total messages it received. The simulation of proposed framework has been performed using Cooja Simulator, and results depict that in proposed framework, the energy consumption is less and the rate of transaction cost is higher as compared to the existing technique. The healthcare and intelligent business sectors are two possible applications of our work. A potential next step for this research is to examine how well the proposed service model integrates with other IoT frameworks. The suggested method will be evaluated and refined in future work to ensure its applicability to the actual BIoT system.

Author contributions

Conceptualization, RR and P; methodology, RR and P; software, RB; validation, SM; formal analysis, AJ; writing—original draft preparation, SR. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Bhushan B, Sahoo C, Sinha P, Khamparia A. Unification of Blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions. *Wireless Networks* 2021; 27(1): 55–90. doi: 10.1007/s11276-020-02445-6
2. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. *Ieee Access*2016; 4: 2292–2303. doi: 10.1109/access.2016.2566339
3. Wang X, Zha X, Ni W, et al. Survey on blockchain for Internet of Things. *Computer Communications* 2019; 136: 10–29. doi: 10.1016/j.comcom.2019.01.006
4. Haque MR, Tan SC, YusoffZ, et al. SDN architecture for UAVs and EVs using satellite: A hypothetical model and new challenges for future. In: Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC); 9–12 January 2021; Las Vegas, NV, USA. pp. 1–6.
5. Abdelmaboud A, Ahmed AIA, Abaker M, et al. Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges and future research directions. *Electronics* 2022; 11(4): 630. doi: 10.3390/electronics11040630
6. Dai HN, Zheng Z, Zhang Y. Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal*2019; 6(5): 8076–8094. doi: 10.1109/jiot.2019.2920987
7. Rana A, Chakraborty C, Sharma S, et al. Internet of medical things-based secure and energy-efficient framework for health care. *Big Data* 2022; 10(1): 18–33. doi: 10.1089/big.2021.0202
8. Harada S, Yan Z, Park YJ, et al. Data aggregation in named data networking. In: Proceedings of the TENCON 2017—2017 IEEE region 10 conference; 5–8 November 2017; Penang, Malaysia. pp. 1839–1842.
9. Rana AK, Sharma S. Enhanced energy-efficient heterogeneous routing protocols in WSNs for IoT application. *International Journal of Engineering and Advanced Technology* 2019; 9(1): 4418–4415. doi: 10.35940/ijeat.a1342.109119
10. Rao AR, Clarke D. Perspectives on emerging directions in using IoT devices in blockchain applications. *Internet of Things* 2020; 10: 100079. doi: 10.1016/j.iot.2019.100079
11. Samaniego M, Deters R. Using blockchain to push software-defined IoT components onto edge hosts. In: Proceedings of the international conference on big data and advanced wireless technologies; 10 November 2016; pp. 1–9.
12. Alkhabbas F, Alsadi M, Alawadi S, et al. Assert: A blockchain-based architectural approach for engineering secure self-adaptive IOT systems. *Sensors* 2022; 22(18): 6842. doi: 10.3390/s22186842
13. Ahmed A, Abdullah S, Bukhsh M, et al. An energy-efficient data aggregation mechanism for IoT secured by blockchain. *IEEE Access* 2022; 10: 11404–11419. doi: 10.1109/access.2022.3146295
14. Sodhro AH, Pirbhulal S, Muzammal M, Zongwei L. Towards blockchain-enabled security technique for industrial internet of things based decentralized applications. *Journal of Grid Computing* 2020; 18(4): 615–628. doi: 10.1007/s10723-020-09527-x
15. Mao W, Zhao Z, Chang Z, et al. Energy-efficient industrial internet of things: Overview and open issues. *IEEE Transactions on Industrial Informatics* 2021; 17(11): 7225–7237. doi: 10.1109/tii.2021.3067026
16. Fernando Y, Saravannan R. Blockchain technology: Energy efficiency and ethical compliance. *Journal of Governance and Integrity* 2021; 4(2): 88–95. doi: 10.15282/jgi.4.2.2021.5872
17. Sodhro AH, Zahid N, Wang L, et al. Toward ML-based energy-efficient mechanism for 6G enabled industrial network in box systems. *IEEE Transactions on Industrial Informatics* 2020; 17(10): 7185–7192. doi: 10.1109/tii.2020.3026663
18. Zahid N, Sodhro AH, Kamboh UR, et al. AI-driven adaptive reliable and sustainable approach for internet of things enabled healthcare system. *Mathematical Biosciences and Engineering* 2022; 19(4): 3953–3971. doi: 10.3934/mbe.2022182
19. Wang X, Garg S, Lin H, et al. A secure data aggregation strategy in edge computing and blockchain-empowered Internet of Things. *IEEE Internet of Things Journal* 2020; 9(16): 14237–14246. doi: 10.1109/jiot.2020.3023588
20. Zhang T, Sodhro AH, Luo Z, et al. A joint deep learning and internet of medical things driven framework for elderly patients. *IEEE Access* 2020; 8: 75822–75832. doi: 10.1109/access.2020.2989143
21. Ali FS, Bouachir O, Özkasap Ö, Aloqaily M. SynergyChain: Blockchain-assisted adaptive cyber-physical P2P energy trading. *IEEE Transactions on Industrial Informatics* 2020; 17(8): 5769–5778. doi: 10.1109/tii.2020.3046744
22. Singh I, Lee SW. Self-adaptive and secure mechanism for IoT based multimedia services: A survey. *Multimedia Tools and Applications* 2021; 81(19):26685–26720. doi: 10.1007/s11042-020-10493-5
23. Satamraju KP, Malarkodi B. Proof of concept of scalable integration of internet of things and blockchain in healthcare. *Sensors* 2020; 20(5): 1389. doi: 10.3390/s20051389
24. Rasolroveicy M. A self-adaptive blockchain framework to balance performance, security, and energy consumption in IoT applications. In: Proceedings of the 2020 IEEE International Conference on Autonomic Computing and Self-Organizing Systems Companion (ACSOS-C); 17–21 August 2020; Washington, DC, USA. pp. 243–245.
25. Wu J, Haider SA, Soni M, et al. Blockchain based energy efficient multi-tasking optimistic scenario for mobile edge computing. *PeerJ Computer Science* 2022; 8: e1118. doi: 10.7717/peerj-cs.1118

26. Yuan Y, Wang FY. Towards blockchain-based intelligent transportation systems. In: Proceedings of the 2016 IEEE 19th international conference on intelligent transportation systems (ITSC); 1–4 November 2016; Rio de Janeiro, Brazil. pp. 2663–2668.
27. Banerjee M, Lee J, Choo KKR. A blockchain future for internet of things security: A position paper. *Digital Communications and Networks* 2018; 4(3): 149–160. doi: 10.1016/j.dcan.2017.10.006
28. Subahi AF, Khalaf OI, Alotaibi Y, et al. Modified Self-Adaptive Bayesian algorithm for smart heart disease prediction in IoT system. *Sustainability* 2022; 14(21): 14208. doi: 10.3390/su142114208
29. Javaid U, Sikdar B. A checkpoint enabled scalable blockchain architecture for industrial internetof things. *IEEE Transactions on Industrial Informatics* 2020; 17(11): 7679–7687. doi: 10.1109/tii.2020.3032607
30. Rana A, Sharma S, Nisar K, et al. The rise of blockchain internet of things (biot): Secured, device-to-device architecture and simulation scenarios. *Applied Sciences* 2022; 12(15): 7694. doi: 10.3390/app12157694