BLOCKCHAIN-ENABLED TRUST FOR SECURE AND EFFICIENT WIRELESS SENSOR IOTS

BODASINGI SOWJANYA
Assistant professor,
Centurion University of Technology and Management
sowjanyabodasingi@gmail.com

ABSTRACT

The paper proposes a solution to the challenges faced by Wireless Sensor Internet of Things (WSIoTs), such as unreliable data communication, high energy consumption, security issues, and cost efficiency. To address these issues, a blockchain-based trust model is suggested. The Dijkstra algorithm is employed to develop an efficient routing protocol that prevents void holes and facilitates communication between network nodes and a sink node. Transparency is ensured by recording all node transactions in an immutable blockchain. The Proof of Authority (PoA) consensus algorithm is used to validate and add transactions to the blockchain. Additionally, the interplanetary file system is utilized for reliable and cost-effective storage. Simulation results demonstrate a 13% improvement in performance with PoA compared to the proof of work consensus algorithm. The proposed routing protocol and trust model are validated based on gas consumption, throughput, nodes' status, and energy consumption.

KEYWORDS: Trust model, IoT, Blockchain

1] INTRODUCTION:

Wireless Sensor Internet of Things (WSIoTs) involves the deployment of Ordinary Sensor Nodes (OSNs) in the environment for monitoring purposes. These OSNs collect data and send it to main servers for aggregation. Sink Nodes (SNs) act as relay nodes, facilitating communication between OSNs and the main server. WSIoTs find applications in various fields like smart cities, medicine, and military. Challenges faced by WSIoTs include limited data storage capacity, routing and security issues, void holes, and low throughput. To ensure reliable and efficient data delivery, the design of routing protocols plays a crucial role. However, existing protocols face limitations such as low Packet Acceptance Ratio (PAR), short battery life, noise, and void holes, which impact network reliability.

2] LITERATURE SURVEY:

2.1] W. She, Q. Liu ***et al***

The Internet of Things (IoT) has gained popularity for its efficiency and real-time collaboration. However, security concerns in wireless sensor networks supporting the IoT are increasing. To address the limitations of existing malicious node detection methods, a blockchain trust model (BTM) is proposed. The BTM offers a comprehensive framework and constructs a blockchain data structure for detecting malicious nodes. It employs blockchain smart contracts and the WSNs' quadrilateral measurement localization method to detect malicious nodes in 3D space, with voting consensus results recorded in the distributed blockchain. Simulation results validate the model's ability to effectively detect malicious nodes in WSNs while ensuring traceability in the detection process.

2.2] B. Jia, T. Zhou ***et al***

Crowd sensing involves engaging mobile device users in tasks like data collection and cloud computing. For cloud platforms, crowd sensing enables collaboration on large-scale awareness tasks and provides users' information for the platform. Various incentive mechanisms have been proposed to enhance crowd sensing effectiveness, including monetary rewards, gamification, social relations, and virtual credits. However, privacy protection-based incentives are rare. This paper introduces a blockchain-based location privacy protection incentive mechanism in crowd sensing networks, combining privacy protection and virtual credits. The network structure comprises intelligence crowd sensing networks, a confusion mechanism, and blockchain. Experimental results conducted in a campus environment demonstrate the effective impact of the proposed incentive mechanism on stimulating user participation.

3] PROBLEM DEFINTION:

This IOT runs on battery power and this battery has to utilized efficiently to increase network life time and avoid IOT death (will get dead or unavailable upon battery exhausted). This IOT not only has battery constrained, it also suffered from data security and trust issue. For Trust always IOT depend on third party centralized server which require money charges and if this centralized server down then trust model get shutdown.

4] PROPOSED APPROACH:

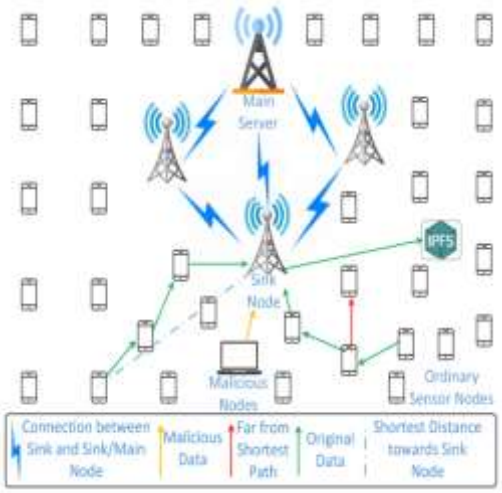
To overcome from above issue author employing Block chain distributed technology to maintain TRUST model. As Block chain stores data in multiple nodes (distributed storage) and if one node down then trust model get executed from other working nodes and runs

on virtual nodes so no 3rd party monitoring or money payment required. To reduce energy consumption author avoiding VOID (void means nodes has no nearest neighbor for routing so no data will transfer) routing issue using Dijkstra algorithm which calculates all routes between source and SINK node and then remove all paths which has VOID or no nearest neighbor issue and then select only that path which is nearest and less energy consumption.

Storing huge IOT data in Blockchain will take more money so author employing IPFS (inter-planary file system) for data storage. IPFS will store IOT data and then return hash code of saved data and this hash code will stored in Blockchain. While reading data we can collect all hash codes from Blockchain and then by issuing hash code to IPFS we can collect IOT data back.

Each IOT will sense data and then report to Sink Node which will check IOT id and if valid IOT ID data received then only data will be reported to Blockchain. While reading data Main Server will check weather given Hash code is valid or not and if valid then only it will read data from Blockchain and send to IOT back. While storing data Blockchain associate each data with unique hash code and then store data and hash code in blocks and before storing any new block it will perform verification of all blocks and if data not change then same hash code will be generate and verification will be successful and if data changes then result into mismatch hash code and attack will be detected. So by using Blockchain we can avoid internal attack (data steal or change by internal working employees). External attack means hackers will hack IOT and then change its packet data.

5] ARCHITECTURE:



6] PROPOSED METHODOLOGY:

Contribution of propose paper

1) A routing protocol using Dijkstra algorithm is proposed to find the shortest path from OSNs (normal node) tothe SN (sink node)
2) The void holes are avoided during route findingprocedure
3) the malicious activities in the network are avoided by aBlockchain based trust model

4) PoA consensus mechanism is used to minimize the computational overhead, caused due to Proof ofWork (PoW)
5) A distributed storage platform, known as InterplanetaryFile System (IPFS), is used to provide a cost effectivedata storage solution for WSIoTs.

Create IOT Simulation: using this we are creating some IOT sensors as simulation

Calculate Sink Nodes: using this we will calculate sink nodes which are closer to Main Server so it can send data to Main server.

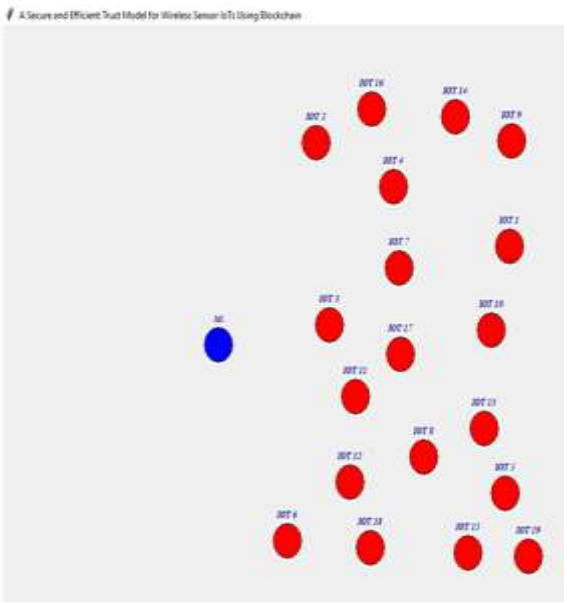
Route using Shortest Path: using this we can select source node and then it will sense some random data and then it will calculate paths using Dijkstra algorithm and then select best path without VOID and send to sink node. Sink node will send to server and server will store data in IPFS and then hash code returned from IPFS will get stored in Blockchain.

Residual Energy Graph: using this we will plot energy consumption between existing and propose as all existing techniques were considering VOID path so it will have no neighbours so will consume more energy and will have less residual battery

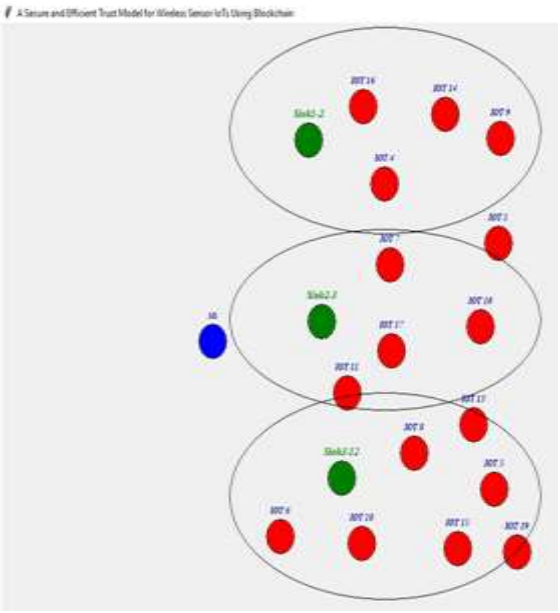
Extension Memory Graph: in propose paper author storing all data in IPFS so it will take lots of server memory and to avoid this issue as extension we are compressing all IOT data to reduce size which will consume less server memory and application runs faster and then we are plotting memory consumption graph between propose and with extension compression technique

Search Main Server: using this module we can select any node and then send request to Main server to read back IOT sense data. Main server will evaluate IOT and its hash codes to identify weather request is coming for valid IOT data.

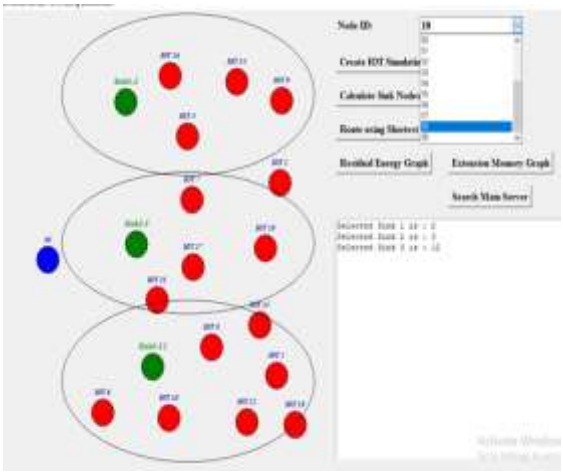
7] RESULTS:



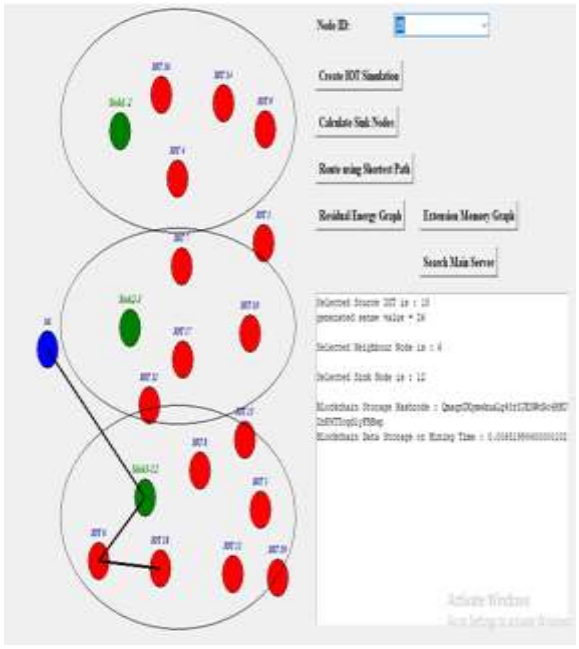
In above screen Creating IOT Simulation, all red colour circles are normal IOT and blue colour is the Main Server



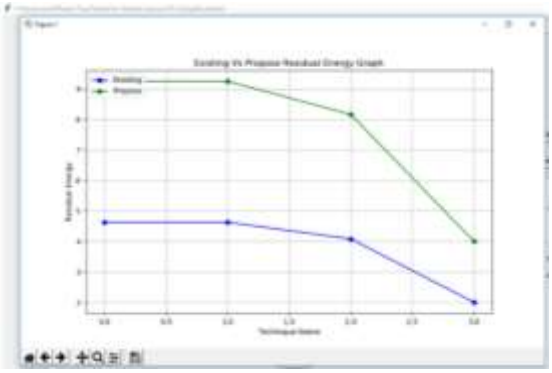
In above screen Calculating Sink Node, all green colour circles are selected Sink Node and big circle represents all nodes inside it are neighbours to one and other and now select any source IOT from the above drop down box



Route using Shortest Path, In above screen I am selecting 18 as the source node

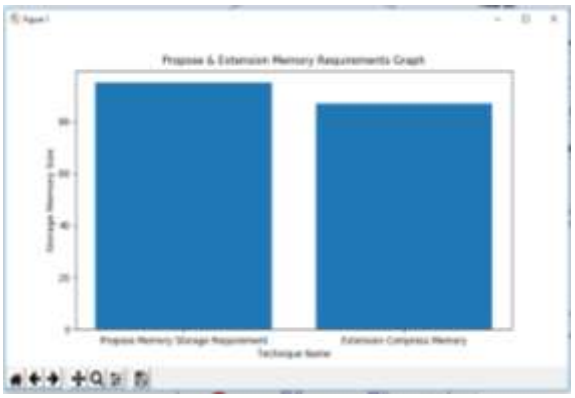


In above screen source 18 sending to nearest neighbour IOT 6 which is sending to nearest SINK 3 and sink sending to main server and this path you can see with black lines. Sending data to sink and main server and each random sensing data will store in IPFS and Blockchain



In above graph x-axis represents number of packets sent and y-axis represents available energy and in above graph green line represents

propose algorithm available energy and blue line represents available energy using extension technique. So by using propose work network can have high available energy and its lifetime will be more



In above graph x-axis represents propose and extension work and y-axis represents Memory requirements size and with propose technique we need more memory for storage and with extension compress storage we need less memory so memory can saved with extension technique.

IOT ID	Sense Data	Blockchain Hashcode	Sense Date & Time
18	generated sense value = 26	QmaupUXynwkuaLg48eYJESWtRo4fBfUZnK9TTogd1yFBBwg	2023/01/11-13 36:57
18	generated sense value = 25	QmcYpbHVhvE653L1wuuUfFbuzDmErba2gsVTHqQcY3UB2	2023/01/11-13 38:30

In above screen in first column we can see IOT ID and then its sense data and then hash code stored in Blockchain and then we can see IOT sensing data date and time.

8] CONCLUSION:

A routing protocol is introduced, which finds the shortest path using the Euclidean distance formula and the Dijkstra algorithm. Additionally, the proposed algorithm avoids the void holes, which results in less battery usage of the network nodes and ultimately helps the network in the long run. Moreover, the security is maintained by the proposed blockchain based trust model. Therefore, the nodes in the network can communicate securely.

9] REFERENCES:

[1] N. Javaid, A. Sher, H. Nasir, and N. Guizani, ‘‘Intelligence in IoT-based 5G networks: Opportunities and challenges,’’ IEEE Commun. Mag., vol. 56, no. 10, pp. 94–100, Oct. 2018.

[2] N. Javaid, ‘‘Integration of context awareness in internet of agricultural things,’’ ICT Exp., to be published, doi: 10.1016/j.icte.2021.09.004.

[3] K.-V. Nguyen, C.-H. Nguyen, P. Le Nguyen, T. Van Do, and I. Chlamtac, ‘‘Energy-efficient routing in the proximity of a complicated hole in wireless sensor networks,’’ Wireless Netw., vol. 27, no. 4, pp. 3073–3089, May 2021.

[4] M. Selvi, S. V. N. Santhosh Kumar, S. Ganapathy, A. Ayyanar, H. Khanna Nehemiah, and A. Kannan, ‘‘An energy efficient clustered gravitational and fuzzy based routing algorithm in WSNs,’’ Wireless Pers. Commun., vol. 116, no. 1, pp. 61–90, Jan. 2021.

[5] N. Javaid, ‘‘NADEEM: Neighbor node approaching distinct energyefficient mates for reliable data delivery in underwater WSNs,’’ Trans. Emerg. Telecommun. Technol., p. e3805, Dec. 2019.

[6] W. Ali, I. U. Din, A. Almogren, M. Guizani, and M. Zuair, ‘‘A lightweight privacy-aware IoT-based metering scheme for smart industrial ecosystems,’’ IEEE Trans. Ind. Informat., vol. 17, no. 9, pp. 6134–6143, Sep. 2021.

[7] I. Ullah, N. U. Amin, A. Almogren, M. A. Khan, M. I. Uddin, and Q. Hua, ‘‘A lightweight and secured certificate-based proxy signcryption (CB-PS) scheme for E-prescription systems,’’ IEEE Access, vol. 8, pp. 199197–199212, 2020.

[8] S. D. Muruganathan, D. C. F. Ma, R. I. Bhasin, and A. O. Fapojuwo, ‘‘A centralized energy-efficient routing protocol for wireless sensor networks,’’ IEEE Commun. Mag., vol. 43, no. 3, pp. S8–13, Mar. 2005.

[9] P. P. Ray, B. Chowhan, N. Kumar, and A. Almogren, ‘‘BIoTHR: Electronic health record servicing scheme in IoT-blockchain ecosystem,’’ IEEE Internet Things J., vol. 8, no. 13, pp. 10857–10872, Jul. 2021.

[10] S. Namasudra, G. C. Deka, P. Johri, M. Hosseinpour, and A. H. Gandomi, ‘‘The revolution of blockchain: State-of-the-art and research challenges,’’ Arch. Comput. Methods Eng., vol. 28, no. 3, pp. 1497–1515, May 2021.

[11] A. Bhardwaj, S. B. H. Shah, A. Shankar, M. Alazab, M. Kumar, and T. R. Gadekallu, ‘‘Penetration testing framework for smart contract blockchain,’’ Peer–Peer Netw. Appl., vol. 14, no. 5, pp. 2635–2650, Sep. 2021.

[12] M. Allouche, M. Mitrea, A. Moreaux, and S.-K. Kim, ‘‘Automatic smart contract generation for internet of media things,’’ ICT Exp., vol. 7, no. 3, pp. 274–277, Sep. 2021.

[13] D. Unal, M. Hammoudeh, and M. S. Kiraz, ‘‘Policy specification and verification for

blockchain and smart contracts in 5G networks,'' ICT Exp., vol. 6, no. 1, pp. 43–47, Mar. 2020.

[14] A. Mateen, J. Tanveer, N. A. Khan, M. Rehman, and N. Javaid, ''One step forward: Towards a blockchain based trust model for WSNs,'' in Proc. 14th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput. (3PGCIC), 2019, pp. 57–69.

[15] G. Ramezan and C. Leung, ''A blockchain-based contractual routing protocol for the Internet of Things using smart contracts,'' Wireless Commun. Mobile Comput., vol. 2018, pp. 1–14, Nov. 2018. 4578 VOLUME 10

[16] W. She, Q. Liu, Z. Tian, J.-S. Chen, B. Wang, and W. Liu, ''Blockchain trust model for malicious node detection in wireless sensor networks,'' IEEE Access, vol. 7, pp. 38947–38956, 2019.

[17] B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, ''A blockchain-based location privacy protection incentive mechanism in crowd sensing networks,'' Sensors, vol. 18, no. 11, p. 3894, 2018.

[18] Z. Rahman, F. Hashim, M. F. A. Rasid, and M. Othman, ''Totally opportunistic routing algorithm (TORA) for underwater wireless sensor network,'' PLoS ONE, vol. 13, no. 6, Jun. 2018, Art. no. e0197087.

[19] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, ''Computation offloading and content caching in wireless blockchain networks with mobile edge computing,'' IEEE Trans. Veh. Technol., vol. 67, no. 11, pp. 11008–11021, Nov. 2018.

[20] Y. Xu, G. Wang, J. Yang, J. Ren, Y. Zhang, and C. Zhang, ''Towards secure network computing services for lightweight clients using blockchain,'' Wireless Commun. Mobile Comput., vol. 2018, pp. 1–12, Nov. 2018.