International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://ijemr.vandanapublications.com https://doi.org/10.31033/ijemr.13.3.26

Novel Approach for Trust and Mobility for Secure Routing in IoT

Shwetha N[1], Raghu J[2], Manu B[3], Shreyas B S[4], Harshavardhan G R[5] and Rakshith Patel[6]
[1]Department of ECE, Dr. AIT Bangalore, INDIA
[2]Department of ECE, NIE, Mysore, INDIA
[3]Department of ECE, Dr. AIT Bangalore, INDIA
[4]Department of ECE, Dr. AIT Bangalore, INDIA
[5]Department of ECE, Dr. AIT Bangalore, INDIA
[6]Department of ECE, Dr. AIT Bangalore, INDIA

[1]Corresponding Author: shwethaec48@gmail.com

Received: 28-05-2023 Revised: 14-06-2023 Accepted: 29-06-2023

ABSTRACT

The Internet of things (IoT) can be used in our daily life. Home area network (HAN) is one of the applications of loT. The Smart Grid is an intelligent power network featured by its two-way flows of electricity and information. The integrated communication infrastructure allows Smart Grid systems to manage the operation of all connected components to provide reliable and sustainable electricity supplies. The Home Area Network is a dedicated network connecting devices in the home, as well as electrical vehicles. The HAN market is now emerging within the smart grid sector to serve home with different solutions. However, at the same time, due to the dependence on information technology and the deep integration of electrical components and computing information in cyber space, the system might become increasingly vulnerable to cyber- attacks. Cyber-attacks have led to numerous incidents and have been concerned by both power system operators and users. They can undermine or even completely disrupt the control system of the power grid. This paper presents an approach to modelling and validating the secure HAN network. Here a novel Trust-Based Iterative Energy-Efficient Routing Protocol (TBIEERP) is suggested with a data encryption scheme for secured data transmission in HAN. The SHA-Secure Hashing algorithm for encryption and decryption of data is employed. Finally, to detect the intrusion a deep auto encoder was used for attack detection and to protect HAN against cyber-attacks. The whole experimentation was carried out under Ubuntu & NS2 environment. Thus, the techniques proposed produce the most promising outcome over attack detection. The proposed method obtained better detection accuracy compared to the existing methods.

Keywords-- Smart Grid (SG), Home Area Networks (HAN), Trust-based - Iterative Energy-Efficient Routing Protocol (TBIEERP), SHA Algorithm

I. INTRODUCTION

The rapid proliferation of Internet of Things (IoT) devices has revolutionized various domains, ranging from smart homes to industrial automation. However, the widespread adoption of IoTalso raises significant concerns about security and privacy. Secure routing is a fundamental aspect of IoT networks that ensures the confidentiality, integrity, and availability of data during transmission.

Traditional routing protocols often fail to address the unique challenges posed by IoT environments, such as dynamic network topologies, resource constraints, andthe diverse nature of IoT devices.

Existing routing protocols for IoT often neglect the trustworthiness and mobility characteristics of the network, leaving vulnerabilities and potential security breaches. Trust-based routing protocols aim to enhance security by considering the reputation and behavior of nodes within the network. By establishing trust levels, nodes can make informed routing decisions, avoiding compromised or malicious nodes. On the other hand, mobility-based routing protocols leverage the movement patterns and location information of IoT devices to optimize routing paths, mitigate congestion, and enhance overall network performance.

In this paper, we propose a novel protocol that combines trust and mobility metrics for secure routing in IoT. Our protocol addresses the limitations of traditional routing approaches by integrating trustworthiness and mobility awareness into the routing decision process. By incorporating trust metrics, nodes can dynamically adapt their routingchoices based on the historical behavior and reputation of neighboring nodes. Additionally, mobility metrics enable nodes to select paths that consider the movement patterns and proximity of devices, enhancing route stability and reducing packetloss. The results of our study demonstrate significant improvements in terms of security, reliability, and energy efficiency compared to traditional routing protocols. Our trust and mobility-based protocol shows promising potential in mitigating security risks, ensuring reliable communication, and optimizing resource utilization in IoT networks. By integrating trust

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.26

and mobility metrics into the routing decision process, we contribute to the advancement of secure routing solutions tailored for IoT environments.

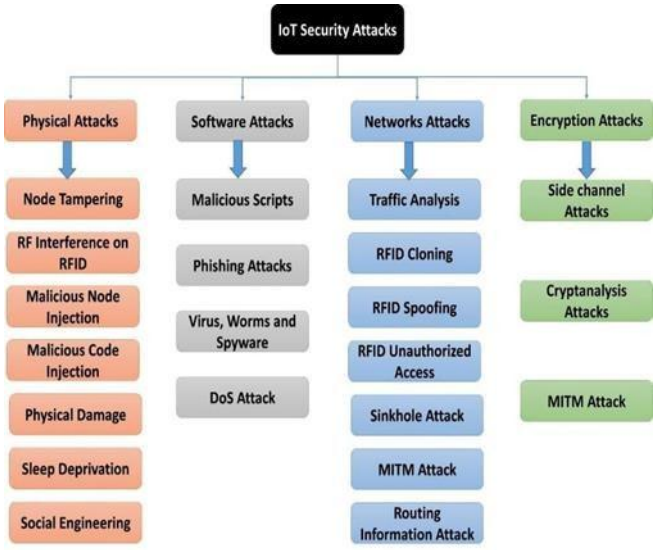
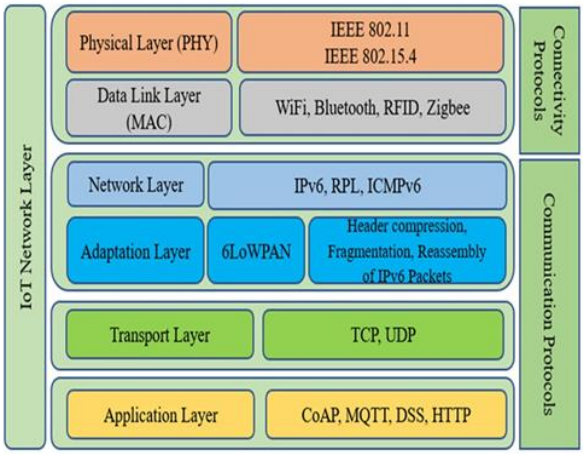


Figure 1: Security in IoT Network Layer & 6Lowpan Overveiw



IoT network layer comprises of the layered protocol stack, as shown in Fig.6LoWPAN is standardized by IETF for IPv6 adaptation layer, that comprises of cross-layer and data link layer protocol, enabling IP connectivity over LLNs. Since the requirement of frame size for low power sensor nodes is around 127 bytes, so 6LoWPAN arranges the IPv6 packets to meet the requirement. Since there is no authentication in 6LoWPAN, malicious nodes can send duplicate and overlapping fragments. Hence, it is challenging to discriminate between legitimate and malicious nodes due to the reassembly of packets. A powerful feature of 6LoWPAN is that while originally conceived to support IEEE 802.15 low-power wireless networks in the 2.4-GHz band. In the case of 6LoWPAN networks, the distance is 10 –200 m, this means that many 6LoWPAN nodes have to be distributed to cover a small area (i.e. high node density).

II. BACKGROUND

The Internet of Things (IoT) is a rapidly evolving paradigm that connects numerous devices and objects, enabling them to communicate and share data. With the proliferation of IoT devices in various domains such as smart homes, healthcare, transportation, and industrial automation, ensuring secure and reliable communication has become a critical concern. Secure routing is a fundamental aspect of IoT systems, as it enables the efficient and trustworthy delivery of data packets between IoT devices. However, the unique characteristics of IoT, including resource constraints, dynamic network topologies, and the presence of potentially untrusted nodes, pose significant challenges to achieving secure routing. Existing routing protocols in IoT often face vulnerabilities such as node compromise, malicious attacks, and privacy breaches. Traditional security mechanisms alone may not be sufficient to address these challenges effectively. Therefore, there is a need for innovative approaches that incorporate trust and mobility aspects to enhance the security and reliability of routing in IoT. Trust-based routing protocols utilize trust metrics and reputation systems to assess the reliability and trustworthiness of nodes in the network. By considering trust values during the route selection process, these protocols aim to mitigate the impact of compromised or malicious nodes on data transmission. Mobility-based routing protocols take into account the dynamic nature of IoT networks, where devices can move or change their network associations. These protocols adapt the routing paths based on the mobility patterns of nodes to optimize the delivery of data packets and improve the overall network performance. By combining trust and mobility aspects, a novel protocol can leverage trustworthiness evaluations and mobility patterns to establish secure and efficient routes in IoT networks.

Such a protocol has the potential to enhance routing security, mitigate attacks, and ensure reliable data transmission in diverse IoT applications.

III. PROBLEM STATEMENT

In Internet of Things, there are numerous objects and the environment is very dynamic and heterogeneous too. The ultimate objective of any trust management system in social Internet of Things should be increasing

the level of cooperation among objects to reach common goals. In the absence of trust, objects may not cooperate and network performance drops. Owners of objects/things are humans that are usually selfish by nature due to their objects' limited resources or social ties. Individual selfishness refers to the behavior that makes an object unwilling to provide service to another object in order to conserve its resources.

IV. EXISTING SYSTEM

The conventional security practices are inadequate to address the specific security needs of IoT. Because of its simple deployment and incorporation into the IoT network, the trust-based approach is a feasible alternative to provide RPL security.

V. PROPOSE SYSTEM

Proposed System aims to develop a trust-based routing protocol for IoT applications and improve security in RPL at the IoT network layer against DOS and tamper proof attacks.

VI. OBJECTIVE

The objectives of the Trust and Mobility Based protocol for Secure routing in the Internet of Things (IoT) project can include:

1. Develop a Trust and Mobility-Based Protocol for Secure Routing in Internet of Things (IoT) networks.
2. Enhance the security and reliability of data transmission within IoT networks by incorporating trust metrics and considering node mobility patterns.
3. Mitigate the risks associated withcompromised or malicious nodes in IoTrouting.
4. Create a resilient routing framework using SHA Algorithm that adapts to the dynamic nature of IoT environments while maintaininghigh levels of security.

VII. LITERATURE REVIEW

A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust- based Approaches by Syeda M. Muzammal, Student Member, IEEE, Raja Kumar Murugesan, Member, IEEE, NZ. Jhanjhi, Member IEEE Internet of Things (IoT) is a network of 'things', connected via Internet, to collect and exchange data. The scalability and heterogeneity of IoT offer limited protection and is prone to diverse attacks, including WSN-inherited attacks. Moreover, IPv6 Routing Protocol for Low Power and Lossy Networks (RPL), a de facto routing protocol for IoT networks, also suffers from certain vulnerabilities based on its features and functionalities.

Tamperproof IoT with Blockchain by Guangsheng Yu∗, Ren Ping Liu∗, J. Andrew Zhang∗, Y. Jay Guo∗ We investigate the tamper-resistant property of Blockchain and its effectiveness for IoT systems. In particular, we implemented an IoT testbed, and built a Blockchain into the testbed. A number of tamper-resistance experiments were conducted and analyzed to corroborate the process of block validation in Blockchain. Our analysis and experimental results demonstrate the tamper-resistant capability of Blockchain in securing trust in IoT systems.

Cooperative and feedback based authentic routing protocol for energy efficient IoT systems by A. Gayathri, A. Jerwin Prabu, +4 authors Yinan Qi Computer Science Concurrency and Computation: Practice and Experience 2022:- This proposed CFTEERP uses the nearest secure node costs to increase the network lifetime without selecting the nearest nodes for routing the data, and provides 90% of PDR and a minimal energy consumption rate of 25% lesser than the existing systems against different malicious attacks.

Fragmentation Attacks and Countermeasures on 6LoWPAN Internet of Things Networks: Survey and Simulation by Sarah Alyami, Randa Alharbi, Farag Azzedin Sensors (Basel, Switzerland}2022:- A survey of fragmentation attacks and available countermeasures is provided, one of the most harmful fragmentation attacks that may cause DoS, is studied and simulated in detail and a countermeasure for this attack is implemented based on a reputation-scoring scheme. A security flaw is investigated by carrying out an attack against the rank value of the RPL protocol in an IoT environment.

Simulation of trust-based attacks in Internet of Things by Vera Suryani1,2,* Selo Sulistyo2,*, and Widyawan Widyawan2: In this paper, we simulated trust-based attacks in IoT environment by giving the fake reputation values of an object. For this purpose, we utilized ConTrust model, a trust-based security model. Matlab was used to simulate the attacks, and the simulation result showed that ConTrust model was outperformed on mitigating a trust-based attack. The attack was detected and resolved correctly.

VIII. ATTACKS IN IOT CONSIDERED

Trust-based Attack: Attacks may occur among objects in IoT, especially those relating to trust. The types

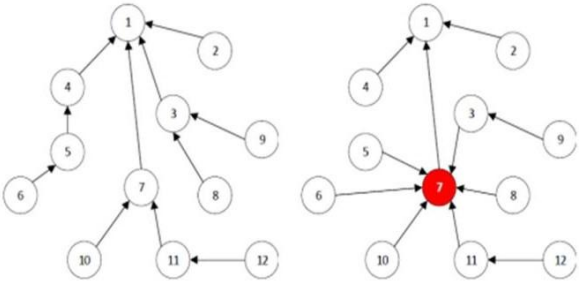
e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.26

of attacks on fake trust scores include:

- Good-mouthing attacks: gives a false trustvalue of an object, that is exaggerated value
- Bad-mouthing attacks: gives a false trustvalue of an object, that is to vilify an object

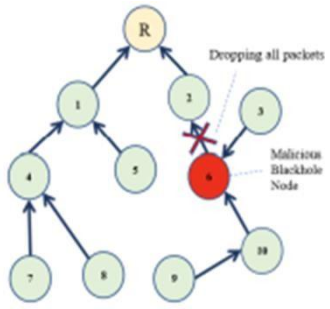
Tampering Attack: The intruder modifies the nodes or damages the node's services and takes complete control over the captured node. The physical devices are damaged in this attack, so that the resources will be deficient . The attack is prevented by changing the key frequently, and proper key management schemes are implemented. *Tamper proofing* is one method of preventing this attacks.

Rank Attack: An attack on the property of Rank has a major effect on RPL's overall function and routing topology. There is no function in RPL to control the node's behaviour, thus allowing chances for the occurrence of Rank attacks. Rank attacks can be divided into three categories:Worst-Parent, Increased Rank, and Decreased Rank attack. This project focuses on defence against Decreased Rank attacks indicated in Figure.



Packet Drop Attack: The security attacks in WSN in which the Packet Drop attack has two distinct characteristics. The malicious node act as a black holewhen the packets pass through these Packet Drop,then the attacker can manipulate the data.

A Packet Drop Attack can be avoided by monitoring the network, changing packet routing, or using authentication mechanisms.

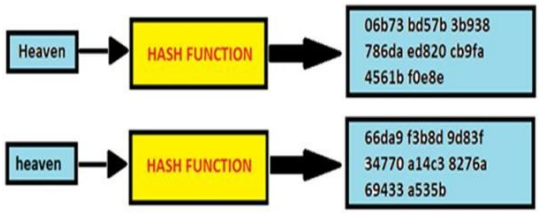


IX. METHODOLOG

The proposed Trust and Mobility-Based Protocol for Secure Routing in IoT addresses the security challenges and vulnerabilities present in existing routing protocols by incorporating trust metrics and considering node mobility patterns. This sectionprovides an overview of the underlying principles,algorithms, and mechanisms used in the protocol and explains how they address the identified security challenges.

SHA Algorithm

SHA stands for secure hashing algorithm. SHA is used for hashing data and certificates. A hashing algorithm shortens the input data into a smaller form that cannot be understood by using bitwise operations,modular additions, and compression functions. SHA works in such a way even if a single character of the message changed, then it will generate a different hash. For example, hashing of two similar, but different messages i.e., Heaven and heaven is different. However, there is only a difference of a capital and small letter.



Software Requirements

- Operating System : UBUNTU 20.04 LTS
- Tool: NS-2.33
- Language : TCL and AWK
- Programming language : Java

Table 1. Simulation specifications setting [19]

Specifications	Values
Simulator	NS 2.35
Area (m^2)	(200 x 200)m
Count of nodes	100
Simulation Time	60 s
Routing Protocols	Existing and TBIEERP (Proposed)
Node energy	2 Joules
Starting energy	0.5 Joules
Size of the packet	1024 bits
En_{elec}	50 nJ/bit
Portability design	Random waypoint
Portability speed	(10-50) m/s

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.26

X. ANALYSIS

To evaluate the performance of the Trust and Mobility Based Protocol for Secure Routing in IoT, a series of experiments/simulations/case studies were conducted. The results obtained from these evaluations are presented in this section, along with an analysis of the protocol's performance in terms of various security metrics. A comparison of the results with existing routing protocols or benchmarks is also provided.

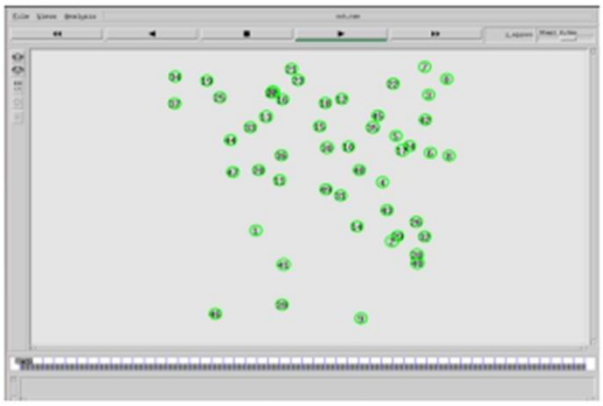


Figure 1

XI. RESULTS

Present the results obtained from the experiments/simulations/case studies, showcasing the performance of the Trust and Mobility-Based Protocol. For example: - Trust Metric: Provide the trust values assigned to nodes in the network based on the trust-based approach used in the protocol. Demonstrate how the protocol effectively identifies trustworthy nodes for data forwarding, reducing the risk of compromised or malicious nodes.

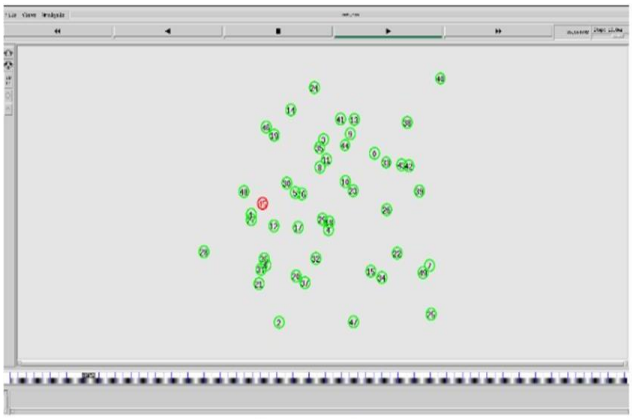


Figure 2

PDR(Packet Delivery Ratio): The packet delivery ratio (PDR) is a crucial metric used to evaluate the performance of routing protocols in wireless networks, including the proposed Trust and Mobility-Based Protocol for Secure Routing in the Internet of Things (IoT).

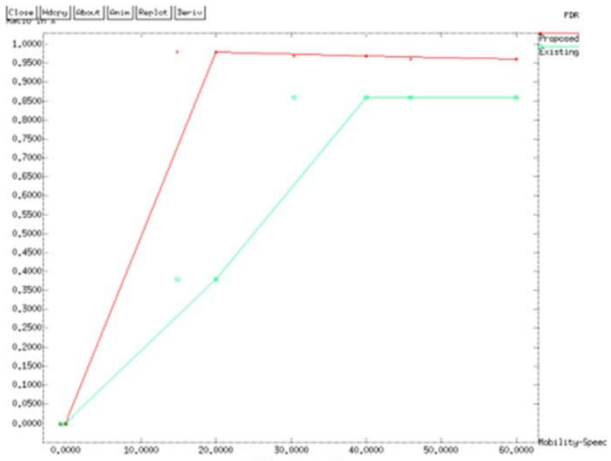


Figure 5

Throughput: Analyzing the throughput provides insights into the protocol's ability to handle and process data effectively. The throughput graph depicts the relationship between data transmission rate and time, illustrating how efficiently the protocol can deliver data packets within the network.

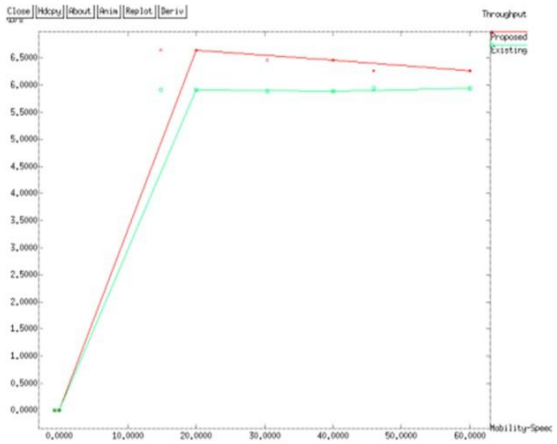
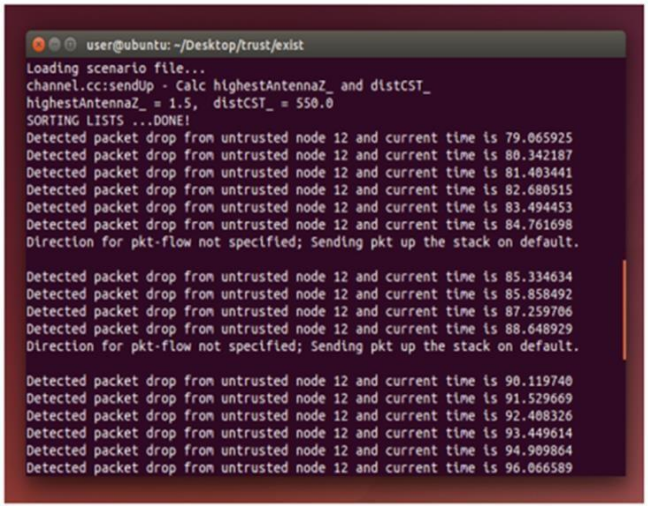


Figure 6

Number of Packet Loss: The number of packet loss is a critical metric that measures the quantity of packets that fail to reach their intended destination within a network.Packet loss can occur due to various reasons such as network congestion, node failures, or transmission errors. Analyzing the number of packet loss

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.26

provides valuable insights into the reliability and efficiency of the Trust and Mobility-Based Protocol.



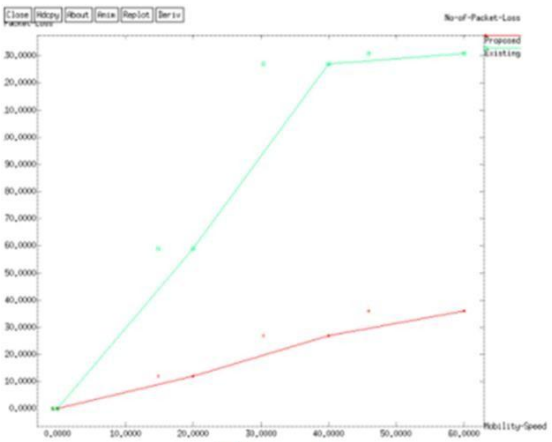


Figure 7

Energy: Energy efficiency is crucial in IoT networks as many IoT devices operate on limited power sources, such as batteries, and optimizing energy consumption can prolong device lifespan and reduce maintenance requirements. Analyzing energy consumption provides insights into its efficiency in utilizing energy resources within the network.

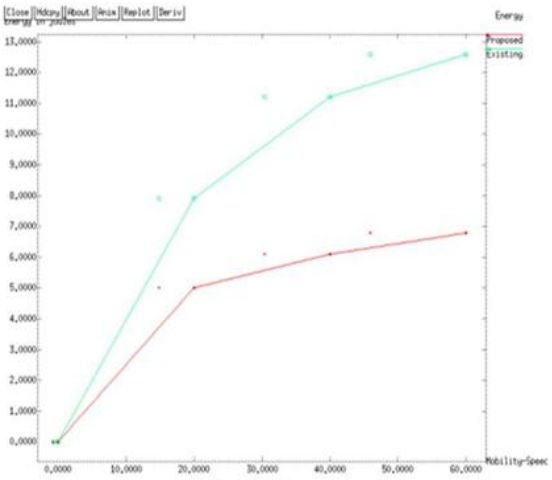


Figure 8

Delay & Overhead: Delay, also known as latency, is an important performance metric that measures the time it takes for a packet to travel from the source to the destination within a network

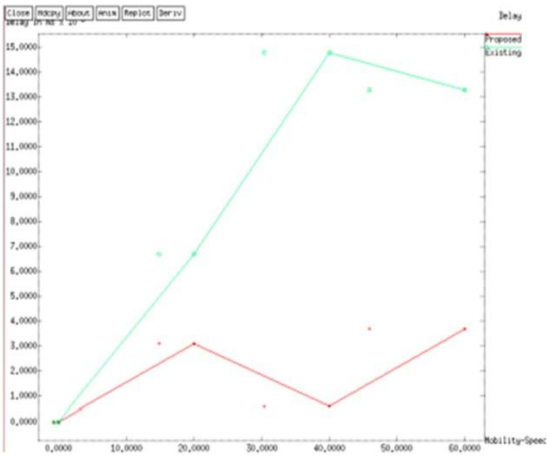
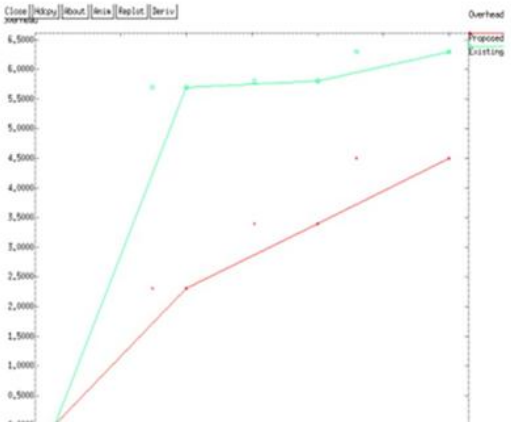


Figure 9

Overhead in the context of network protocols, refers to the additional data or computational resources required to support the functioning of the protocol.

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.26



Advantages

- Interpret the results to showcase the effectiveness of the proposed protocol in addressing the security challenges in IoT routing.
- Discuss how the protocol's integration of trustmetrics and mobility patterns contributes to enhanced security, reliability, and resilience.
- Highlight the advantages of the protocol in terms of trustworthiness of nodes, optimized routing paths, secure data transmission, and adaptability to dynamic IoT environments.

Limitations

- The scalability of the protocol for large-scale IoT deployments and its ability to handle resource-constrained environments.
- Acknowledge any constraints in terms of computational complexity or communication overhead.
- Additionally, consider any potential vulnerabilities or limitations of the trust or mobility based mechanisms employed and discuss strategies for mitigating these challenges.

XII. CONCLUSION

In conclusion, this Major project has proposed a Trust and Mobility-Based Protocol for Secure Routing in Internet of Things (IoT) networks. The protocol combines trust metrics and mobility patterns to address the security challenges associated with compromised or malicious nodes in IoT routing. The main contributions and findings of this research can be summarized as follows: Novelty and Significance: The proposed protocol introduces a novel approach to enhance routing security in IoT networks by integrating trust metrics and considering node mobility patterns. By utilizing trust-based routing and mobility aware mechanisms, the protocol improves the selection of trustworthy nodes, optimizes routing paths, and enhances the resilience of IoT networks.

Future Research Directions

Identify potential areas for future research based on the limitations or challenges identified. Discuss how further researchcan address scalability concerns, optimize computational efficiency, or enhance the adaptability of the protocol. Explore possibilities for integrating additional security mechanisms or improving trust and mobility modeling to further enhance routing security in IoT networks.

REFERENCES

[1] M. Maduranga and Y. Weerasinghe, “Survey on Communication Technologies for Home Area Network (HAN) in Smart Grids”, International Journal of Advanced Scientific Research and Management, Vol. 2, Issue 9, 2017.

[2] E. Kabalci and Y. Kabalci, “Introduction to smart grid architecture”, Smart Grids and Their Communication Systems, pp. 3-45,2019.

[3] F. B. Saghezchi, G. Mantas, J. Ribeiro, M. A. Rawi, S. Mumtaz, and J. Rodriguez, “Towards a secure network architecture for smart grids in 5G era”, In: Proc. of 2017 13th International Wireless Communications and Mobile Computing Conference, 2017, pp. 121-126.

[4] K. Deepa and M. S. Khurana, “Optimization of Routing in Smart Grids Using Intelligent Techniques”, In: Proc. of 3rd International Conference on Internet of Things and Connected Technologies, pp. 26-27, 2018.

[5] B. Chatfield and R. J. Haddad, “RSSI-based spoofing detection in smart grid IEEE 802.11

[6] Home area networks”, In: Proc. of 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference, pp. 1-5, 2017.

[7] D. B. Avancini, J. J. Rodrigues, S. G. Martins, R. A. Rabêlo, J. A. Muhtadi, and P. Solic, “Energy meters evolution in smart grids: A review”, Journal of Cleaner Production, Vol. 217, pp. 702-715, 2019.

[8] Z. Amjad, M. A. Shah, C. Maple, H. A. Khattak, Z. Ameer, and M. N. Asghar, “Towards energy efficient smart grids using bio-inspired scheduling techniques”, IEEE Access, Vol. 8, pp. 158947-158960, 2020.

[9] Alnasser and H. Sun, “A fuzzy logic trust model for secure routing in smart grid networks”, IEEE Access, Vol. 5, pp. 17896-17903, 2017.

[10] Xiang and J. Zheng, “A situation-aware scheme for efficient device authentication in smart grid-

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.26

enabled home area networks",Electronics, Vol. 9, p. 989, 2020.

[11] E. McCary and Y. Xiao, "Malicious device inspection home area network in smart grids", International Journal of Sensor Networks, Vol. 25, pp. 45-62, 2017.

[12] N. Shwetha, L. Niranjan, V. Chidanandan and N. Sangeetha, "Advance System for Driving Assistance Using Arduino and Proteus Design Tool," *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, Tirunelveli, India, 2021, pp. 1214-1219, doi: 10.1109/ICICV50876.2021.9388620.

[13] S. N, N. L, G. N, S. Jahagirdar, S. A. R and S. N, "Efficient Usage of water for smart irrigation system using Arduino and Proteus design tool," *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India, 2021, pp. 54-61, doi: 10.1109/ICOSEC51865.2021.9591709.

[14] N. Shwetha and M. Priyatham, "Performance Analysis of Self Adaptive Equalizers using EPLMS Algorithm," *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2020, pp. 872-876, doi: 10.1109/I-SMAC49090.2020.9243512.

[15] Shwetha, N., Niranjan, L., Chidanandan, V. & Sangeetha, N. (2021), Smart driving assistance using Arduino and proteus design tool. Expert Clouds and Applications, 647–663.

[16] R. Taseen, H. Yaseen, N. L, G. Radha, M. B. Neelagar and S. N, "An Innovative Method for Energy Intensive Routing and Transmission Network Positioning in Integrated Wireless Detector Networks," *2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC)*, Mysore, India, 2023, pp. 1-7, doi: 10.1109/ICRTEC56977.2023.10111924.

[17] Shwetha, N., Gangadhar, N., Neelagar, M.B., Shilpa, K.C. (2022). ANN-based Hybridization Approach for Detection of Cardiac Disease. In: Shakya, S., Balas, V.E., Kamolphiwong, S., Du, KL. (eds) Sentimental Analysis and Deep Learning. Advances in Intelligent Systems and Computing, vol 1408. Springer, Singapore. https://doi.org/10.1007/978-981-16-5157-1_20.

[18] Shwetha, N., Manoj Priyatham, and N. Gangadhar. "Adaptive Channel Equalization Using Seagull Optimization with Various Initialization Strategies." *J. Commun.* 17, no. 4 (2022): 302-307.

[19] Shwetha, N., Priyatham, M. (2021). Performance Analysis of Self Adaptive Equalizers Using Nature Inspired Algorithm. In: Smys, S., Balas, V.E., Kamel, K.A., Lafata, P. (eds) Inventive Computation and Information Technologies. Lecture Notes in Networks and Systems, vol 173. Springer, Singapore. https://doi.org/10.1007/978-981-33-4305-4_37.

[20] Shwetha, N., Priyatham, M. (2021). Convergence Analysis of Self-Adaptive Equalizers Using Evolutionary Programming (EP) and Least Mean Square (LMS). In: Bindhu, V., Tavares, J.M.R.S., Boulogeorgos, AA.A., Vuppalapati, C. (eds) International Conference on Communication, Computing and Electronics Systems. Lecture Notes in Electrical Engineering, vol 733. Springer, Singapore. https://doi.org/10.1007/978-981-33-4909-4_48.

[21] H. Tabassum, N. L, S. P. Atti, A. Pasha, N. Shwetha and M. B. Neelagar, "A Fiber-Wireless Monitoring System with a QoE Instrument for Smart Grid Technology," *2023 Second International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2023, pp. 404-410, doi: 10.1109/ICEARS56392.2023.10085662.