ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)

Available Online at www.ijetcr.org

Volume 13; Issue 01; 2025; Page No. 01-12

RPL Routing Sybil Attack Countermeasures in Internet of Things under Static and Dynamic Environment: A Review

Deepak Upadhyay[1*] and Hiteishi Diwanji[2]

[1] *Assistant Professor, Department of Cyber Security, Gujarat Technological University, Gujarat, India.*
E-mail: ap_deepak@gtu.edu.in
[2]*Professor, Department of Information Technology, L.D Engineering College, Gujarat, India.*
E-mail: hiteishi.diwanji@gmail.com

Conflicts of interest: Nil

Corresponding author: Deepak Upadhyay

Abstract

Internet of Things a massive revolution in industry is led by business leaders and researchers looking future of the world in this technology. The new technology has inherent vulnerabilities which become critical with another challenges of resource constraints. Traditional protocols are not suitable to be used and therefore routing protocol as RPL serves the routing need of the IPv6 networks. To review the issues in routing at network layer , this paper covers the necessity of the routing protocol with different types of attacks considering the severity of sybil attack in static and dynamic environment with a range of countermeasure techniques, assessment of routing techniques, deep learning techniques, cryptography and trust-based algorithms for detection by implementing machine learning techniques, deep learning techniques, cryptography and trust based algorithms for detection and mitigation against sybil attack. It also covers the challenges, performance metrics, datasets, implementation details with the analytical evaluation of the results and further scope of research in sybil attack.

1. INTRODUCTION

The internet of Things (IoT) allows systems, objects, and devices to communicate with each other. IoT includes a network of sensors, actuators, smart devices, and software programs that gather and share data. IoT system management faces challenges in connectivity, data flow, security, and interoperability. Lossy networks and constrained devices, IoT devices typically have constrained electrical, memory and CPU speed [1]. Security is what it stands for one of the primary important problems with the Internet of Things (IoT), particularly with regard to core routing threats network where information loss can have disastrous consequences. RPL is built to function effectively on such limited-resource machines. IoT networks could also have lossy communication lines, where connectivity issues and packet loss are frequent because of things like interference and environmental conditions. The primary goal of this study is to evaluate the security measures put out in the present literature to defend LLNs from sybil attacks. In order to do so, this review begins by going over the various defenses against the sybil attack under RPL and attack's behaviour under mobility.

1.1. Scope of Network Layer for attacks on IOT network

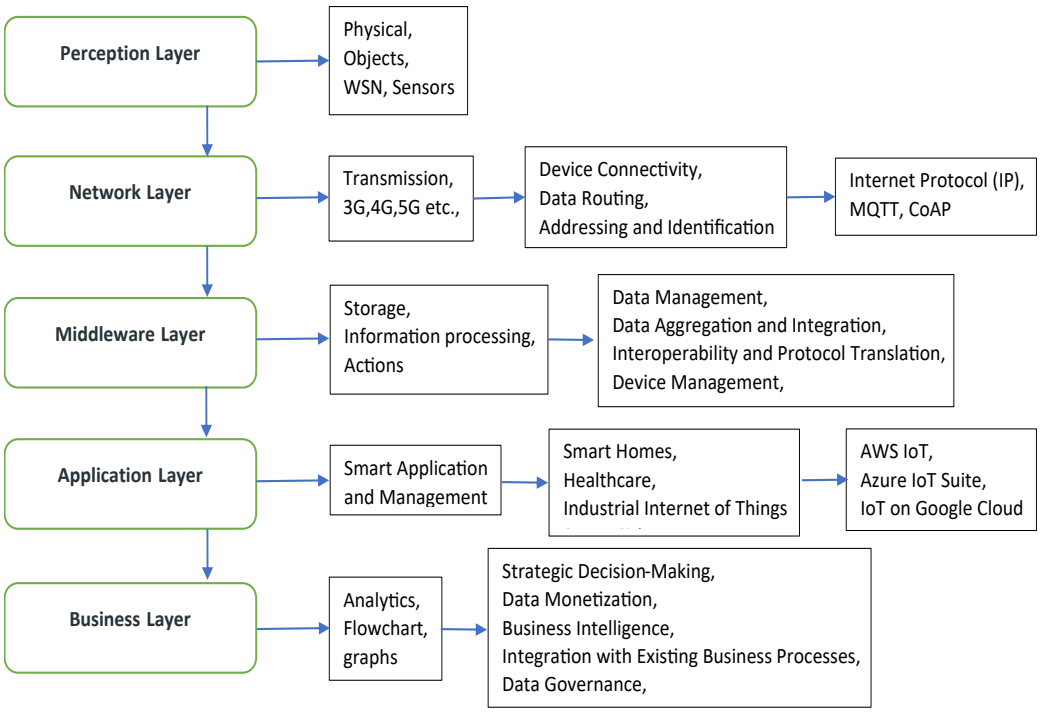

Fig 1: Internet of Things -Architecture

A layered architectural approach is commonly used to address these challenges in IoT systems [2].

1.2. Comparison of different Routing protocol for Network layer in IoT:

By enforcing the ranking constraint that a node's parent must have a lower rank than its children, RPL uses the trickling algorithm to limit broadcast

1.3 Routing attacks on RPL topology and network traffic

Table 1: Network Protocol Comparison table [3]

Routing Protocol	CORPL	CARP	RPL	P2P-RPL	LOADng
Working Method	Extension of RPL	Communication at Underwater.	DODAG	Finds the optimal path for every combination of source and destination.	A lightweight variation of AODV and Energy-aware metrics
Server Technology Support	Yes	No	Yes	NA	NA
Storage Management	Not Supported	Supported	Supported	High memory usage	Low Memory Usage
Type of Traffic	MP2P, P2P & P2MP	MP2P, P2P & P2MP	MP2P, P2P & P2MP	P2P	P2P
IPv6 Support	Yes	Yes	Yes	Yes	Yes
Energy Efficient	Yes	Yes	No	Yes	No
Security	Yes	No	No	No	No

Table 2: Different types of RPL attacks at the Network Layer

Attack Type	Paper Reference	Metrics	Simulator	Research Gap
Sinkhole Attack	[6]	End to End Delivery	Cooja	Metrics related to energy consumption, delay and overhead.
Black Hole Attack	[7]	Transmission power and Route Request (RReqs)	OMNET++	Large network with multiple malicious sybil nodes.
Sybil Attack	[8]	Throughput, average delivery delay and detection rate	Cooja	For time-sensitive IoT applications, increased latency is unsuitable; instead, a test bed is needed to evaluate the suggested technique.
Wormhole Attack	[9]	ADR, Ratio of packet loss and energy consumption.	Cooja	SLF-RPL will be expanded to include the additional attacks.
Selective Forwarding Attack	[10]	Rate of detection and false alarm rate.	Cooja	Advanced proposed attacks with very limited energy consumption.
Rank manipulation	[11]	PDR, Delay, Energy Consumption	Cooja	Causing loops to start if a malicious node announces a rank value that is comparable to that of its chosen parent.

In this paper, authors classified the RPL routing attacks into three categories related to traffic, resources and topology. [4][5]
Some of the critical attacks with their functionality and parameters are in table 2.

The paper is presented with the: Section 2 presents an overview of sybil attack on RPL. Section 3 Literature review for countermeasures for sybil Attacks in RPL. Section 4 Challenges and opportunities in utilizing machine learning for detection of sybil attack in RPL. Section 5 Future Directions & Emerging Trends. Section 6 concludes the study with part as Conclusion and Future work.

2. Overview of Sybil Attack in RPL

The increase in Internet of Things (IoT) device proliferation has revolutionized several domains, from production and home automation to healthcare and transportation. IoT networks provide uniform communication and data sharing across many connected devices, enhancing efficiency and convenience. However, these networks distributed, and dynamic structure also poses substantial security difficulties. The Sybil assault is one of the most serious dangers to IoT networks [12].

Attacks using Sybil can interfere with device-to-device communication, jeopardize data security, change network protocols, and trick reputation and trust systems. This thorough review study intends to give a detailed analysis of Sybil assaults in IoT networks, investigating its traits, consequences, detection methods, and defence mechanisms. This study aims to promote IoT security by bringing together current research, noting gaps, and emphasizingpotential techniques. It also aims to help academics and practitioners build strong defences against Sybil assaults. [13]

2.1 Literature Review

A few of the related paper are in [14] author proposed a unique fog-enabled GINI Index-Based Trust Mechanism architecture that lowers energy consumption, decreases isolation delay, and improves the rate of Sybil attack detection. GITM detects and isolates a greater quantity of malicious network nodes than other methods in an

equivalent amount of time. The suggested GITM architecture results in a 4.48% rise in the Sybil attack detection rate, a 21% decrease in energy usage, and a 26.30% (concerning time) reduction in isolation latency. Moreover, the total latency is only 0.30 percent involvement in their situation, and there are 28% fewer control messages.

In [15] author proposes a mechanism based on PUF and Bloom filter for sybil attack detection. The mechanism minimizes memory cost as well as detection latency.

In [16] author countermeasure sybil attack with a new collaborative and centralized approach as Random Password Generation. It consists of comparison methodology having detection and prevention algorithms based on the RPG.

In [17] author propose the PITrust approach to detect the sybil attack and used received signal strength indicator (RSSI) as key parameter for improving detection and PDR in relation to other schemes. The approach is based on the trust path routing as physical identification of the device.

In [18] author proposes channel base machine learning approach for detecting' malicious attacks like sybil attack. This approach is light weighted for industrial wireless devices achieving 84% authentication accuracy without manual labelling, based on simulations and tests in actual settings. Future work aims to improve label of offline training sample through improved channel difference threshold approach strengthens channel characteristics for better identification and investigate CSI-based physical layer authentication for detecting advanced persistent threat (APT) assaults using long-term CSI information collecting.

In [19] The author suggests a dependable GAN-C methodology for attack detection events that combines two stages of GAN and SVM techniques. The performance of GAN-C was enhanced with the inclusion of SVM classifiers, and the author employed Dataset, which was obtained from the Cooja simulator. In subsequent work, the author will need to design a cross-application solution for an attack detection model based on active learning in order to leverage heterogeneous data in real time.

In [20] author considered the vulnerable IoT healthcare system attacks at network layer like sybil, wormhole, grey hole etc. The sybil attack as the most severe attack. Author proposes the use of the various cryptography and encryption algorithm with performance metrics against Sybil attacks.

In [21] author propose the scheme related to controlling the access for the IOT network ELECTRON. Here, the device social trust is calculated to protect the sybil attack. The implementation has been done by using NS3 simulator with performance comparison with SA2CI System

2.2 Overview of mobility for sybil attack in RPL

The detection of sybil attack becomes severe when the nodes are changing the position in the DODAG. The DODAG graph has a root node and a new node at joining of graph requires to choose a parent with the computation of rank. There are various issues such as shadowing, path loss, disappearance due to which the node gets disconnected from the graph or network. [22].

2.2.1 Literature Review for dynamic sybil attack in IOT

In [23] author proposed a lightweight mathematical edge computing-based algorithm. The results are based on the count of edge nodes and if nodes are more than four then it has TPR greater than 94% and FPR less than 14%. If edge nodes are equal to four then it achieves TPR more than 92% and FPR less than 16%.

In [24] author presents a novel method for identifying rogue Sybil nodes in a network called physical layer security (PLS) by exploit of Doppler Shift due to mobility of these nodes in the network. This doppler shift method is considered

as a novel detection against sybil node under mobility. The performance parameter for the solution is TPR and FPR.

In [25] author introduced a novel framework under mobility using multi-mobile agent which is energy efficient. The MMTM-RPL uses fog layer features to mitigate internal threats in WSNs that are based on IoT. Due to dynamic environment of mobile agents, 25% to 30% message overhead and energy is minimised and improves network lifetime along with the detection rate by 10% or more.

In [26] author shows challenges for the RPL due to mobile nodes in the network. The author's solution falls into one of the following categories: related to Power, Energy, Position and Timer.

In [27] author proposed SecRPL-MS with the performance which is evaluated using the sail fish algorithm, and Quantum Inspired Neural Network (QINN) with Network Simulator 3.

In [28] author implement MobiRPL on cooja simulator, which consist of four in mobility scenarios: Adaptive timeout and probing, Proactive neighbour discovery, objective function is based on RSSI and hop distance, and the last is identifying mobile and fixed nodes. Operational and performance data for MobiRPL and RPL are shown on the monitor using log messages.

In [29] author has examined several RPL protocols related to mobility like Mobility Enhanced RPL, EMA-RPL, Extended Kalman filter (KP-RPL). The performance metrics are, handover delay, signalling cost, energy consumption and route stability of various algorithms.

3. Literature review for countermeasure for sybil Attacks in RPL:

The identification of Sybil attack in IoT networks has drawn substantial attention to machine learning approaches. These approaches have used different algorithms and data analysis to find trends and anomalies that point to Sybil behaviour. Machine learning techniques offer several advantages when it comes to identifying Sybil attacks. Here are some typical ways that machine learning is used to identify Sybil attacks [30] [31]

Some countermeasures other than AI with metrics are based on Information of neighbouring nodes, Signal Strength, time difference of arrival, based on key pre-distribution and testing of radio resource, testing based on angle of arrival [32-36].

In [37] author introduced early-stage detection based on deep learning DNN model on IRAD dataset.

3.1 Artificial Intelligence Components and metrics for detection of sybil attack

3.1.1 Behavioral Analysis

Based on past data, machine learning algorithms may be trained to find behavioral patterns connected to Sybil nodes. An algorithm using K-mean clustering is proposed to visualize the deployment location selection procedure of an attacker and it achieves 48.7% coverage with the use of K-mean clustering technique. This figure can be further improved using other efficient clustering techniques.[52][23][38].

3.1.2 Feature Engineering

The identification of Sybil attacks in IoT requires the use of feature engineering. The author suggests utilizing the physical layer properties of the radio signals released by the UAVs as detected by two ground nodes to develop an intelligent Sybil attack detection method for FANETs-based IoFT. The experiment was conducted using two radio signal characteristics: the received signal strength differential (RSSD) and the time difference of arrival (TDoA). Models for detecting Sybil attacks get more accurate and effective with the use of feature engineering. [53][39][40]

3.1.3 Anomaly Detection

To analyze the generated data and anticipate unexpected or abnormal occurrences, artificial intelligence and machine learning may be very helpful in enabling the prompt setup of efficient reactions against these unexpected events. Data from a sensor network may be analyzed using a machine learning-based method to find abnormalities associated with sensor failures or unusual occurrences like fires, gas leaks, and infiltration attempts. [54][41][42]

4. Challenges and opportunities in utilizing machine learning for detection of sybil attack in RPL.

Here the author studies the comparison of different challenges and opportunities in utilizing machine learning for detection.

4.1.1 Load Imbalance

The challenge of data imbalance in the context of the RPL (Routing Protocol for Low-Power Wireless Networks) can be addressed by using various techniques to balance the traffic load over the network. A new metric in the RPL objective function to address the load imbalance issue, which is a significant weakness in the protocol, especially when dealing with non-uniform distribution in large-scale LPWNs [55][43].

4.1.2 Adversarial Attacks

Adversarial attacks, including Sybil attacks, pose significant challenges to the security and performance of the RPL in IoT systems. Sybil attacks happen when a hacker uses several false identities to maliciously influence a network by taking advantage of security holes in the

system. [56][12][44]. Sybil attacks can be especially harmful in the context of RPL as they can corrupt any reputation-based system and alter the routing topology [57][45].

4.1.3 Scalability

In RPL-based IoT networks, scalability poses a serious obstacle to the detection and mitigation of Sybil attacks. To counteract Sybil attack, for example, a cooperative and lightweight Trust-enabled Hybrid RPL protocol has been developed. [57][46]. This protocol includes a mathematical security study and a Sybil threat model. Using trust mechanisms, THC-RPL is another tactic that defends against external and internal attacks, including Sybil attacks. [12][47]

Using historical data, these techniques can provide insights into Sybil behavior and assist in the identification of likely Sybil nodes. For example, a machine learning-based technique has been presented for identifying Sybil attacks in Internet of Things networks. It utilizes several factors, including the number of neighbors, the average RSSI value, and the hop count to the sink.[23][48]

Furthermore, using machine learning techniques could need a lot of processing power, which could be difficult in IoT networks with limited resources. Therefore, further research is needed to develop machine learning- or deep learning-based Sybil attack detection systems that are both scalable and effective for Internet of Things networks.

4.2 Overview of different detection and prevention mechanism for sybil attack

Reputation-Based Approaches: In order to detect Sybil threats in Internet of Things networks, reputation-based techniques have been proposed. To detect Sybil assaults, these methods rely on the reputation of nodes. For instance, a distributed trust model is used in a reputation-based Sybil attack detection technique that has been developed to identify Sybil attacks in Internet of Things networks.[23]

Statistical Analysis Techniques: In RPL-based IoT networks, statistical analysis techniques have been suggested as a way to identify Sybil assaults. One way to recognize and stop Sybil attacks in RPL networks is to use a countermeasure based on the Gini index. [14][49]

Graph-Based Methodologies: By recognizing features of the refined graph structure, preprocessing techniques are used by graph-based Sybil detection approaches to enhance the graph and identify Sybil nodes. From the intended distributed systems, they then extract social structures. [58][50]

Machine Learning Techniques: In RPL-based IoT networks, machine learning approaches have been suggested to identify Sybil assaults. These techniques may help identify Sybil attacks more accurately and strengthen IoT network security. [57][51] Using machine learning algorithms to analyze the activity of authentic nodes and identify abnormalities that could point to a Sybil attack is one strategy.[59] Using machine learning methods to identify Sybil assaults in RPL-based IoT networks is an additional strategy. Machine learning methods are used in a lightweight Sybil attack detection scheme that leverages the physical unclonable function and Bloom filter to identify Sybil assaults in IoT networks. [15]

Table 4 Matrix for different countermeasure approach with parametric evaluation

	Reputation-Based Approaches				Statistical Analysis Methods				Graph-Based Approaches				Machine Learning Techniques				
Performance Metrics	DA	FPR	FNR	CC	DA	FPR	FNR	CC	DA	FPR		FNR	CC	DA	FPR	FNR	CC
	✓					✓						✓					✓
Evaluation Criteria	SE	E	SC	R	SE	E	SC	R	SE	E	SC	R	SE		E	SC	R
	✓					✓					✓						✓
Weakness	CA	FP	DN	LTD	CA	FP	DN	LTD	CA	FP	DN	LTD	CA	FP		DN	LTD
	✓					✓					✓						✓
Traded-off	CC	A	CR		CC	A	CR		CC	A	CR		CC	A		CR	
	✓					✓			✓							✓	
Open Challenge	SC	RC	DNT	PP	SC	RC	DNT	PP	SC	RC	DNT	PP	SC	RC		DNT	PP
	✓					✓					✓						✓

Abbreviation for Table:

- Performance Metrics: False Negative Rate (FNR),, Detection Accuracy (DA), Computational Complexity (CC) and False Positive Rate (FPR).
- Evaluation Criteria: Security (SE), Efficiency (E), Scalability (SC), Robustness(R).
- Weakness: Collusion Attacks (CA), False Positive (FP), Dynamic Networks (DN), Labelled Training Data (LTD).
- Trade-off: Computational Complexity (CC), Accuracy (A), Computing Resources (CR).
- Open Challenge: Scalability (SC), Resource Constraints (RC), Dynamic Network Topology (DNT), and Privacy Protection (PP).

5. Future Directions & Emerging Trends

Investigate integrating several detection techniques to increase detection accuracy and robustness against Sybil attack, such as combining statistical analysis, graph-based methods, and machine learning. Emphasize privacy-preserving methods that shield the private data of trustworthy nodes while successfully locating Sybil nodes.

Artificial Intelligence and Machine Learning: anomaly detection algorithms and Deep learning are two examples of cutting-edge approaches that might be used to detect Sybil attack [1][57].

Blockchain Technology: Researchers have proposed various defenses against Sybil attacks, including lightweight trust-enabled routing protocols, blockchain-based trust mechanisms, and distributed blockchain-based authentication and trust validation.

The use of blockchain technology in these mechanisms is seen as a promising approach to

prevent internal attacks such as Sybil attacks in IoT networks [57] [60].

Collaboration in Detection: Collaboration in the detection of Sybil attacks in IoT networks can be achieved through various techniques, such as: Collaborative edge computing-based distributed and lightweight Sybil attack detection techniques that circumvent RSSI and seek to identify Sybil threats in mobile IoT environments [23]. Blockchain-based trust mechanisms and lightweight trust-enabled routing protocols, which use blockchain technology to detect and mitigate the consequences of Sybil attacks in IoT networks. [49]

6. Conclusion and Future work

This study investigates the problem of Sybil assaults in Internet of Things networks, emphasizing their consequences, ways to identify them, and countermeasures. Online social networks and decentralized systems are particularly vulnerable to Sybil attacks, which fabricate identities to deceive networks. The study explores various detection methods, countermeasures, and Sybil-resistant systems. It also discusses mobility issues and the importance of scalability, resource limitations, network topology, privacy protection, and adversarial attacks. The paper highlights future research in emerging trends like machine learning, blockchain technology, collaborative detection, and edge computing. By putting effective detection and prevention mechanisms in place, the study seeks to safeguard IoT deployments' reliability and integrity against malevolent actors. A comprehensive analysis of recent works focused on RPL routing attacks was conducted to provide a concise synopsis of the attacks and their corresponding defenses. Additionally, every approach under study was thoroughly investigated in a methodical manner to categorize and correlate the attacks with the RPL. Future work, Deep learning approaches can be explored for detection of sybil attack in response to critical applications.

Acknowledgement:

Funding organizations from the governmental, private, or non-profit sectors did not provide any special grants for this study.

Conflict of Interest:

The author confirms that they have no conflicts of interest to disclose for this work.

Author's contribution statement:

Deepak Upadhyay: Data Collection, Paper collection, manuscript preparation, conceptualization and analysis of collected papers.

Hiteshi Diwanji: Supervision and guidance for manuscript, key points for methods and techniques in draft paper.

References

1. Albishari, M., Li, M., Zhang, R., & Almosharea, E. (2023). Deep learning-based early-stage detection (DL-ESD) for routing attacks in Internet of Things networks. Journal of Supercomputing, 79(3), 2626–2653.
2. Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., & Jin, Y. (2018a). Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. Journal of Hardware and Systems Security, 2(2), 97–110.
3. Anna, T.., Panagiotis S,& Thomas, D. (2018). Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends Network Protocols. Wireless Communications and Mobile Computing Volume 2018, Article ID 5349894.
4. Sana R Tarek A, & Faouzi, Z. (2022) IoT Routing Attacks Detection Using Machine Learning Algorithms. Wireless Personal Communications (2023) 128:1839–1857.
5. Mali, S. D., & Govinda, K. (2021). A study on network routing attacks in IoT. Materials

Today: Proceedings. https://doi.org/10.1016/j.matpr.2021.07.092
6. Al-chikh Omar, A. A. R., Soudan, B., & Ala' Altaweel. (2023). A comprehensive survey on detection of sinkhole attack in routing over low power and Lossy network for internet of things. Internet of Things, 22, 100750.
7. Elsayed, Jurcut, A. D., Azer, M. A. A., Karimi, R., Abdelhamid, A., Said Elsayed, M., Jurcut, A. D., & Azer, M. A. (2023). Citation: Abdelhamid, A A Lightweight Anomaly Detection System for Black Hole Attack.
8. Khan, M. A., Rais, R. N. bin, & Khalid, O. (2023). Collaborative Detection and Prevention of Sybil Attacks against RPL-Based Internet of Things. Computers, Materials and Continua, 77(1), 827–843.
9. Javed, S., Sajid, A., Kiren, T., Khan, I. U., Dewi, C., Cauteruccio, F., & Christanto, H. J. (2023). A Subjective Logical Framework-Based Trust Model for Wormhole Attack Detection and Mitigation in Low-Power and Lossy (RPL) IoT-Networks.
10. Jiang, J., & Liu, Y. (2022). Secure IoT Routing: Selective Forwarding Attacks and Trust-based Defenses in RPL Network.
11. Rouissat, Mehdi, Belkheir, Mohammed, Belkhira, Hichem S. A., Mokaddem, Allel and Ziani, Djamila. "Implementing and evaluating a new Silent Rank Attack in RPL-Contiki based IoT networks" Journal of Electrical Engineering, vol.74, no.6, 2023, pp.454-462.
12. C. Pu, "Sybil attack in RPL-based internet of things: Analysis and defenses," IEEE Internet of Things Journal, vol. 7, no. 6, pp. 4937–4949, 2020.
13. Bang, A. O., & Rao, U. P. (2021). A novel decentralized security architecture against sybil attack in RPL-based IoT networks: a focus on smart home use case. Journal of Supercomputing, 77(12), 13703–13738.
14. Hassan, M., Tariq, N., Alsirhani, A., Alomari, A., Khan, F. A., Alshahrani, M. M., Ashraf, M., & Humayun, M. (2023). GITM: A GINI Index-Based Trust Mechanism to Mitigate and Isolate Sybil Attack in RPL-Enabled Smart Grid Advanced Metering Infrastructures. IEEE Access, 11, 62697–62720.
15. Pu, C., & Choo, K. K. R. (2022). Lightweight Sybil Attack Detection in IoT based on Bloom Filter and Physical Unclonable Function. Computers & Security, 113, 102541.
16. Khan, M. A., Rais, R. N. bin, & Khalid, O. (2023). Collaborative Detection and Prevention of Sybil Attacks against RPL-Based Internet of Things. Computers, Materials and Continua, 77(1), 827–843.
17. J. D. Kim, M. Ko and J. M. Chung, "Physical identification-based trust path routing against Sybil attacks on RPL in IoT networks," IEEE Wireless Communications Letters, vol. 11, no. 5, pp. 1102–1106, 2022.
18. Chen, S., Member, S., Pang, Z., Member, S., Wen, H., Yu, K., Zhang, T., Lu, Y., Wen, H., & Zhang, T. (2021). Automated Labeling and Learning for Physical Layer Authentication Against Clone Node and Sybil Attacks in Industrial Wireless Edge Networks. IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, 17(3).
19. Sharmistha Nayak, Nurzaman Ahmed, and Sudip Misra. 2021. Deep Learning-Based Reliable Routing Attack Detection Mechanism for Industrial Internet of Things. Ad Hoc Netw. 123, C (Dec 2021).
20. Sai, A., Thuluva, S., Sorakaya Somanathan, M., Somula, R., Sennan, S., & Burgos, D. (n.d.). Secure and efficient transmission of data based on Caesar Cipher Algorithm for Sybil attack in IoT.
21. de Oliveira GHC, de Souza Batista A, Nogueira M, dos Santos AL. An access control for IoT based on network community perception and social trust against Sybil attacks. Int J Network Mgmt. 2022; 32(1):e2181.
22. Cobârzan, C., Montavont, J., & Noel, T. (n.d.). LNCS 8965 - Integrating Mobility in RPL.

23. Yan, J., Jiang, T., Lin, L. et al. A novel Sybil attack detection scheme in mobile IoT based on collaborate edge computing. J Wireless Com Network 2023, 25 (2023).
24. S. Dogan-Tusha, S. Althunibat and M. Qaraqe, "Doppler Shift based Sybil Attack Detection for Mobile IoT Networks," in IEEE Internet of Things Journal.
25. Farooq, U., Asim, M., Tariq, N., Baker, T., & Awad, A. I. (2022). Multi-Mobile Agent Trust Framework for Mitigating Internal Attacks and Augmenting RPL Security. Sensors, 22(12).
26. Shah, Z., Levula, A., Khurshid, K., Ahmed, J., Ullah, I., & Singh, S. (2021). electronics Routing Protocols for Mobile Internet of Things (IoT): A Survey on Challenges and Solutions.
27. Rakesh, B., & H, P. S. (2021). Novel Authentication and Secure Trust based RPL Routing in Mobile sink supported Internet of Things. Cyber-Physical Systems.
28. Kim, H., Youn, J., Kim, H.-S., Yoon, S.-G., & Bahk, S. (2020). Demo: Mobility Enhanced RPL for General Mobility Scenarios. In 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW).
29. Yadav, R. K., & Awasthi, N. (2020). A survey on enhanced RPL: Addressing the mobility in RPL. Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020, 1189–1195.
30. Baghani, A. S., Rahimpour, S., & Khabbazian, M. (2022). The DAO Induction Attack: Analysis and Countermeasure. IEEE Internet of Things Journal, 9(7), 4875–4887.
31. Butun, I., Österberg, P., & Song, H. (2019a). Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures.
32. M. Wen, H. Li, Y.-F. Zheng, K.-F. Chen, TDOA-based Sybil attack detection scheme for wireless sensor networks. J. Shanghai Univ. (Engl. Edn.) 12(1), 66–70 (2008)
33. K.-F. Ssu, W.-T. Wang, W.-C. Chang, Detecting Sybil attacks in wireless sensor networks using neighboring information. Comput. Netw. 53(18), 3042–3056 (2009).
34. M. Demirbas, Y. Song, An RSSI-based scheme for Sybil attack detection in wireless sensor networks. In Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks (IEEE Computer Society, 2006), pp. 564–570.
35. J. Newsome, E. Shi, D. Song, A. Perrig, The Sybil attack in sensor networks: analysis and defenses. In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks (ACM, 2004), pp. 259–268.
36. Y. Zhang, K. Fan, S. Zhang, W. Mo, AOA based trust evaluation scheme for Sybil attack detection in WSN. Appl. Res. Comput. 27(5), 1847–1849 (2010)
37. Albishari, M., Li, M., Zhang, R., & Almosharea, E. (2023). Deep learning-based early-stage detection (DL-ESD) for routing attacks in Internet of Things networks. Journal of Supercomputing, 79(3), 2626–2653.
38. G. Rohini, C. Gnana Kousalya & J. Bino (2022) Intrusion Detection System with an Ensemble Learning and Feature Selection Framework for IoT Networks, IETE Journal of Research.
39. Abhishek Verma , Virender Ranga . ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things. TechRxiv. January 01, 2020.
40. P. Jaya Prakash and B. Lalitha. 2022. Optimized Ensemble Classifier Based Network Intrusion Detection System for RPL Based Internet of Things. Wirel. Pers. Commun. 125, 4 (Aug 2022), 3603–3626.
41. A. Samy, H. Yu and H. Zhang, "Fog-Based Attack Detection Framework for Internet of Things Using Deep Learning," in IEEE Access, vol. 8, pp. 74571-74585, 2020.
42. Bang, A. O., Rao, U. P., Kaliyar, P., & Conti, M. (2023). Assessment of Routing Attacks and Mitigation Techniques with RPL Control Messages: A Survey. In ACM Computing

Surveys (Vol. 55, Issue 2). Association for Computing Machinery.
43. Murali, S., & Jamalipour, A. (2020). A Lightweight Intrusion Detection for Sybil Attack under Mobile RPL in the Internet of Things. IEEE Internet of Things Journal, 7(1), 379–388.
44. Morales-Molina, C. D., Hernandez-Suarez, A., Sanchez-Perez, G., Toscano-Medina, L. K., Perez-Meana, H., Olivares-Mercado, J., Portillo-Portillo, J., Sanchez, V., & Garcia-Villalba, L. J. (2021). A dense neural network approach for detecting clone id attacks on the rpl protocol of the iot. Sensors, 21(9).
45. Simoglou, G., Violettas, G., Petridou, S., & Mamatas, L. (2021). Intrusion detection systems for RPL security: A comparative analysis. In Computers and Security (Vol. 104). Elsevier Ltd.
46. Violettas, G., Simoglou, G., Petridou, S., & Mamatas, L. (2021). A Softwarized Intrusion Detection System for the RPL-based Internet of Things networks. Future Generation Computer Systems, 125, 698–714.
47. Almesaeed, R., & Al-Salem, E. (2022). Sybil attack detection scheme based on channel profile and power regulations in wireless sensor networks. Wireless Networks, 28(4), 1361–1374.
48. Kaliyar, P., Jaballah, W. Ben, Conti, M., & Lal, C. (2020). LiDL: Localization with early detection of sybil and wormhole attacks in IoT Networks. Computers and Security, 94.
49. Arshad, A., Hanapi, Z. M., Subramaniam, S., & Latip, R. (2021). A survey of Sybil attack countermeasures in IoT-based wireless sensor networks. PeerJ Computer Science, 7, 1–33.
50. Almogren, A., Mohiuddin, I., Din, I. U., Almajed, H., & Guizani, N. (2021). FTM-IoMT: Fuzzy-Based Trust Management for Preventing Sybil Attacks in Internet of Medical Things. IEEE Internet of Things Journal, 8(6), 4485–4497.
51. S. Chen, Z. Pang, H. Wen, K. Yu, T. Zhang and Y. Lu, "Automated Labeling and Learning for Physical Layer Authentication Against Clone Node and Sybil Attacks in Industrial Wireless Edge Networks," in IEEE Transactions on Industrial Informatics, vol. 17, no. 3, pp. 2041-2051, March 2021.
52. A. K. Mishra, A. K. Tripathy, D. Puthal and L. T. Yang, "Analytical Model for Sybil Attack Phases in Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 379-387, Feb. 2019.
53. D. Chulerttiyawong and A. Jamalipour, "Sybil Attack Detection in Internet of Flying Things-IoFT: A Machine Learning Approach," in IEEE Internet of Things Journal, vol. 10, no. 14, pp. 12854-12866, 15 July15, 2023.
54. H. Gao, B. Qiu, R. J. D. Barroso, W. Hussain, Y. Xu and X. Wang, "TSMAE: A Novel Anomaly Detection Approach for Internet of Things Time Series Data Using Memory-Augmented Autoencoder," in IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, pp. 2978-2990, 1 Sept.-Oct. 2023.
55. Kala Venugopal , T. G. Basavaraju , A Combined Metric Objective Function for RPL Load Balancing in Internet of Things, International Journal of Internet of Things, Vol. 10 No. 1, 2022, pp. 22-31.
56. F. Medjek, D. Tandjaoui, I. Romdhani and N. Djedjig, "Performance Evaluation of RPL Protocol under Mobile Sybil Attacks," 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, Australia, 2017, pp. 1049-1055.
57. Arshad, D., Asim, M., Tariq, N., Baker, T., Tawfik, H., & Al-Jumeily OBEID, D. (2022). THC-RPL: A lightweight Trust-enabled routing in RPL-based IoT networks against Sybil attack.
58. J. Mao, X. Li, Q. Lin and Z. Guan, "Deeply understanding graph-based Sybil detection techniques via empirical analysis on graph processing," in China Communications, vol. 17, no. 10, pp. 82-96, Oct. 2020.
59. F. Medjek, D. Tandjaoui, M. R. Abdmeziem and N. Djedjig, "Analytical evaluation of the impacts of Sybil attacks against RPL under mobility," 2015 12th International Symposium

on Programming and Systems (ISPS), Algiers, Algeria, 2015, pp. 1-9.
60. Ali SE, Tariq N, Khan FA, Ashraf M, Abdul W, Saleem K. BFT-IoMT: A Blockchain-Based Trust Mechanism to Mitigate Sybil Attack Using Fuzzy Logic in the Internet of Medical Things. Sensors (Basel). 2023 Apr 25;23(9):4265.

	Deepak Upadhyay is currently working as Assistant Professor with the department of Cyber Security,Gujarat Technological University,India. He has completed his M.Tech from Guru Gobind Singh Indraprashtha University, New Delhi, India in 2013, B.Tech in Information Technology from GEC Ajmer, Rajasthan,India in 2011. He is pursuing PhD in field of Internet of Things and Cyber Security from Gujarat Technological University. He has a rich academics & research experience in various areas of Computer Engineering, IoT and Cyber Security. He has published many research articles in reputed journals.His research area is Internet of Things, Cyber Security, Machine Learning. Learning and Computer Networks. Email: ap_deepak@gtu.edu.in
	Dr. Hiteshi Diwanji is currently holds the position of Professor in the department of Information Technology at L.D Engineering Colleger, Ahmedabad, ,India. Dr. Hiteshi has contributed significantly to the academic field, publishing numerous research articles in reputable international journals and proceedings of esteemed international conferences.Her research interests encompass a broad spectrum, including Information and network security, wireless technology, Mobile ad hoc network, IOT. In addition to his research contributions, Dr. Hiteshi actively contributes to the academic community. She serves as a reviewer for various journals of international repute.