IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 26 May 2023, accepted 7 June 2023, date of publication 15 June 2023, date of current version 27 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3286536

RESEARCH ARTICLE

GITM: A GINI Index-Based Trust Mechanism to Mitigate and Isolate Sybil Attack in RPL-Enabled Smart Grid Advanced Metering Infrastructures

MUHAMMAD HASSAN[1], NOSHINA TARIQ[1], AMJAD ALSIRHANI[2], ABDULLAH ALOMARI[3], (Member, IEEE), FARRUKH ASLAM KHAN[4], (Senior Member, IEEE), MOHAMMED MUJIB ALSHAHRANI[5], MUHAMMAD ASHRAF[1], AND MAMOONA HUMAYUN[6]

[1]Department of Avionics Engineering, Air University, Islamabad 44000, Pakistan
[2]Department of Computer Science, College of Computer and Information Sciences, Jouf University, Sakaka, Al Jouf 72388, Saudi Arabia
[3]Department of Computer Science, Al-Baha University, Al Baha 65779, Saudi Arabia
[4]Center of Excellence in Information Assurance, King Saud University, Riyadh 11653, Saudi Arabia
[5]College of Computing and Information Technology, University of Bisha, Bisha 61361, Saudi Arabia
[6]Department of Information Systems, College of Computer and Information Sciences, Jouf University, Sakaka, Al Jouf 72388, Saudi Arabia

Corresponding authors: Mamoona Humayun (mahumayun@ju.edu.sa) and Noshina Tariq (noshina.tariq@mail.au.edu.pk)

This work was supported by the Deputyship for Research and Innovation, Ministry of Education, Saudi Arabia, under Project 223202.

ABSTRACT The smart grid relies on Advanced Metering Infrastructure (AMI) to function. Because of the significant packet loss and slow transmission rate of the wireless connection between smart meters in AMI, these infrastructures are considered Low-power and Lossy Networks (LLNs). The routing protocol in an AMI network is crucial for ensuring the availability and timeliness of data transfer. IPv6 Routing Protocol for Low-power and lossy networks (RPL) is an excellent routing option for the AMI communication configuration. However, it is highly at risk against many external and internal attacks, and its effectiveness may be severely diminished by Sybil assault. Different trust-based techniques have been suggested to mitigate internal attacks. However, existing trust systems have high energy consumption issues, which cause a reduction in the performance of LLNs due to complex calculations at the node level. Therefore, this paper presents a novel fog-enabled GINI index-based trust mechanism (GITM) to mitigate Sybil attacks using the forwarding behavior of legitimate member nodes. Regarding identifying and isolating Sybil assaults, our approach outperforms the state-of-the-art methods. GITM detects and isolates a more significant number of malicious network nodes compared to other techniques within a similar time frame. By using the proposed GITM framework, the Sybil attack detection rate increases by 4.48%, energy consumption reduces by 21%, and isolation latency reduces by 26.30% (concerning time). Furthermore, the end-to-end delay is merely 0.30% more in our case, and the number of control messages decreases by 28%.

INDEX TERMS Smart grid, GINI index, advanced metering infrastructure, LLN, RPL, Sybil attack, trust.

I. INTRODUCTION

Smart Grid (SG) infrastructures are believed to be the next generation of traditional electricity grids. These infrastructures often include several innovations that boost efficiency and stability to ensure an uninterrupted power supply to households and businesses. It is a revolutionary innovation with advanced computing environments interconnected through the Internet [1]. In addition, technologies such as 5G and 6G empower the upcoming age of remote correspondence frameworks with modern security methods [2]. Smart meter communication networks are often built using wireless technology. They are generally installed as Low power and Lossy Networks (LLNs) [3]. LLNs are a group of associations in which the inter-connected devices are largely resource-limited (i.e., with memory, power, and computing

The associate editor coordinating the review of this manuscript and approving it for publication was Neetesh Saxena.

capabilities) and are categorized by low information, high error rates, and volatility in correspondence joins [4]. Power consumption information is gathered from consumers using massive smart meters in an Advanced Metering Infrastructure (AMI).

Unfortunately, attackers have colossal freedom to hack SG devices and use them harmfully. These devices' security is an area that is being investigated and has pulled scientists to eliminate their weaknesses. Many organizations and associations are engaged in advancing and planning a secure SG network. Numerous protocols and cryptographic methods portray RPL-based Networks' security issues; they neglect to deal with internal attacks in such networks due to their resource-constrained nature [5]. Developing robust routing methods to cope with aggressive inferring Sybil assaults is crucial for continuous and dependable data transfer in AMI networks. However, it is widely acknowledged that RPL is susceptible to many attacks, such as Sybil, rank, and sinkhole [6], [7], [8]. This issue has raised a need for a trust-based component to secure the routing and correspondence of resource-compelled SG infrastructures.

Compared to internal attacks, external attacks are receptive to standard security techniques such as authorization, encryption, and other cryptographic mechanisms. However, these approaches incur enormous computing, energy, and storage overheads, rendering them inapplicable for resource-constrained SG applications [6]. Therefore, for internal assaults to be dealt with, a process must be in place. Trust-based security, often known as soft security, is commonly used to prevent internal threats. Once the rogue nodes are identified, the remaining nodes use this knowledge to safeguard their communications. However, standard trust assessment algorithms need substantial memory, energy, and message overhead. Resource-constrained IoT devices' significant processing and communication overheads reduce their performance and longevity. Monitoring a variety of trust metrics enables the discovery of the incorrect node. Once a malicious or destructive node is identified, the other nodes use it to safeguard the network. However, the current trust methods use plenty of resources owing to communication messages and computation overheads, which consistently weaken the efficiency and limit the durability of sensor nodes-based SG infrastructures [9], [10].

Unluckily, present routing techniques are incapable of effectively managing such traffic patterns. As a result, RPL can solve these issues with a preemptive and efficient IPv6 network protocol. This proactive IPv6 distance routing protocol builds topologies using Destination Oriented Directed Acyclic Graph (DODAG) [11]. It can direct between lossy connections and equipment with a large Packet Error Rate (PER). Unfortunately, a solid security system is not empowered, making RPL powerless against internal and external attacks. Internal attacks, such as Sybil, are challenging to handle. Much research has been done; however, most of the existing models strain the already constrained IoT devices due to heavy node-level computations and message exchange [12]. The classic security measures, such as encryption and other cryptography procedures, are unsuitable for internal threats. These techniques pose enormous computational, energy, and storage overheads, making them inappropriate for resource-constrained IoT networks. As a result, trust-based mechanisms that offer security against internal attacks with minimal energy consumption overhead are needed. In addition, internal attacks also increase message and energy overheads due to the resending of lost packets [13], [14].

Internal assaults need efficient security mechanisms to be dealt with. When preventing internal threats, a technique known as ''soft security'' or ''trust-based security'' has become popular [15]. Other nodes utilize this information to protect their communication after it has been used to identify rogue nodes. In contrast, traditional trust assessment methods cost many resources due to memory requirements, energy consumption, and message overheads. These trust-based techniques' substantial computational and communication overheads reduce the performance and lifespan of resource-constrained Internet of Things (IoT) devices [16]. Hence, there is a significant need for trust-based systems that are small, lightweight, and energy-efficient, with minimal storage use and processor complexity. To overcome these problems, we propose a practical yet powerful trust-based security framework that fulfills the above criteria. In addition, it is an energy-efficient trust mechanism using GINI Index at the fog layer, known as GITM, for convenience. We aim to reduce memory, processing, and network congestion in LLNs while enhancing security in RPL for increased effectiveness and lifetime to counter internal threats. This paper's contributions are given below:

1) A novel dual-layered architecture is presented, tailored for RPL-based SG networks, facilitating an in-depth nodes' behavior analysis for improving the network functionality and performance under Sybil attack scenarios.
2) An Energy-Efficient GINI Index-based trust assessment framework is proposed to detect and isolate Sybil attacks, thereby enhancing the resilience of RPL-based SG networks.
3) To mitigate Sybil attacks with minimized memory, computation, and message overhead at the node level, the proposed method is designed to promote the more efficient performance of RPL-based SG networks.
4) Mathematical modeling of the Sybil threat model is performed to provide a quantitative framework for understanding potential Sybil threats and their impacts on the network, thereby formulating more effective mitigation strategies.
5) Underpinned by mathematical propositions, corollaries, and proofs, the research's theoretical aspects are solidified, thereby underscoring the proposed solution's robustness and reliability.
6) Meticulously devised scenarios are included and a mathematical case study is performed to facilitate the

validation of the proposed solution and demonstrate its practical feasibility and effectiveness.

7) A comprehensive comparison with current state-of-the-art approaches is provided, offering empirical evidence of the superior performance of the proposed solution, hence underlining its relevance and potential for practical applications.

The rest of the paper is organized into different sections; the related work is summarized in Section II. The background is provided in Section III. A helpful threat model is proposed in Section IV. The proposed GITM model is detailed in Section V. The experimentation details and results are articulated in Section VI. Finally, a fruitful discussion of the findings is provided in Section VII followed by the conclusion, which is presented in Section VIII.

II. RELATED WORK

Several trust-based approaches and the types of attacks they can counter are discussed here. A trust model was presented in [17] to regulate the rank of each node in the network. Each node in this paradigm computes its level of trust in the next node based on the path a packet took to get there. To protect against RPL routing protocol assaults, Airehrour et al. [18] presented the Sec-trust RPL method. In this method, rank and Sybil assaults are dealt with by a trust calculation across nodes considering indirect and direct packet transfers. Another work proposed in [19] provided a multi-dimensional trust model for the LLN-based IoT that is both comprehensive and dynamic. This study focuses on Sybil, blackhole, and rank attacks. Packet loss, packet forwarding indicator, mobility, and energy are metrics used to assess a node's reliability. Each child node reports its neighbor ID, own ID, energy percentage, and packet error rate to the parent node using the trust RPL model established in [9]. A trust-based method for detecting distributed denial of service attacks was proposed in [10]. The authors based their method on the frequency of sent packets as a reliability metric. The parent node keeps track of how often each child node transmits data and flags any child node whose packet frequency is much higher than the specified threshold.

Djedjig et al. [21] offered a "Metric-Based RPL trustworthiness" scheme. It also uses an extended RPL node trustworthiness metric to mitigate attacks. Trust among the nodes is evaluated by two methods: direct and indirect. No simulation is done and no specific network attacks are mentioned or mitigated in this paper. Djedjig et al. [22] presented the Metric-based RPL trustworthiness Scheme to mitigate RPL network attacks. The node's trustworthiness is calculated by its direct and indirect neighborhood observations. Pu et al. [20] presented an RPL technique to spot and counteract against the malicious nodes. In this research, a new node establishes a link with the network and publishes different messages to different nodes, making the nodes reset repeatedly and pass the malicious data. A Gini Index-based approach is used to measure the malicious node. Airehrour et al. [23] proposed two techniques for mitigating the RPL attacks, i.e., MRHOF's RPL and Sec-trust RPL technique, an RPL routing protocol for securing RPL from different routing attacks. Node's trust is calculated by its neighbor node, making it bad-mouthing or good-mouthing attacks. Hassan et al. [3] proposed a different technique for

TABLE 1. State-of-the-art details.

Ref.	Trust type	Trust model	Trust parameters	Simulator used	Nodes used	Simulation Time	Result
[3]	Global	Fuzzy	Energy Consumption	Cooja	30	60 min	Isolate 10% more bad nodes and save energy consumption up to 35
[9]	Direct, Indirect	Bayesian	Energy overhead and throughput	COOJA	10-20	3600 sec	PLR < 5%
[10]	Direct	Fuzzy	Energy consumption	COOJA	30,40,50	5 min	Detect DDOS attacks efficiently.
[20]	Direct	Bayesian	Rank, Transfer packet rate and time consumption	OMNet++	20	100 sec	Energy loss reduced.
[17]	Direct	Fuzzy	Packet Forwarding	MATLAB	500-1500	-	Detect 80% of malicious nodes
[18]	Direct, Indirect	Fuzzy	Packet Forwarding	COOJA	30	60 min	PLR < 28%
[19]	Direct	Fuzzy	PDR and throughput	COOJA	30	60 min	PLR < 18%
[21]	Direct, Indirect	Fuzzy	Rank	COOJA	13	-	Energy loss reduced.
[22]	Direct, Indirect	Fuzzy	Packet forwarding and PDR	COOJA	30	1 hour	Reduce energy loss
[23]	Indirect	Fuzzy	Packet forwarding and PDR	COOJA	30	5 min	PLR < 28%
[24]	Direct	Fuzzy	Packet loss ratio	COOJA	12	5400 sec	PLR < 27%
[25]	Direct	Statistical Based	Packet loss rate	COOJA	15	1440 sec	PLR < 20%
[26]	Direct	Fuzzy	Packet loss ratio and true positive rate	COOJA	61	30 min	TPR 90-94%
[27]	Direct	-	PDR and PLR	COOJA	20	60 min	PLR < 20% PDR is almost 100accurate.
[28]	Direct	Bayesian	Packet loss ratio	COOJA	5-30	60 min	PLR < 28%

detecting and mitigating internal attacks. This paper mainly works on the detection and mitigation of blackhole attacks. It uses the global trust value for calculating the trust of nodes.

Bhalaji et al. [24] proposed different techniques for calculating trust. The techniques used were inter-DODAG level trust and intra-DODAG level trust. It decreased the packer loss ratio from 40% to 27%. Jiang et al. [25] proposed a new trust technique to mitigate and isolate blackhole attacks. It reduced the packet loss ratio from 40% to 20%. Kaliyar et al. [26] proposed a trust-RPL technique to mitigate Sybil and wormhole attacks and calculated the trust of nodes by the direct trust method based on packet loss and true positive rate parameters. The packet loss rate is reduced to 10% while true positive rate values vary from 90-94%. Almusaylim et al. [27] proposed the new SRPL-RP technique for calculating trust at the node level. The parameters used for trust calculation were packet drop ratio and energy consumption. Different trust techniques were used, and experiments showed significant results with the packet drop ratio dropping to 20%. Airehrour et al. [18] proposed the Sec-trust RPL technique to mitigate the RPL routing protocol attacks. Both direct and indirect trust model calculates trust. Sec-trust RPL outperformed and experienced a packet loss ratio under 28%. Mehta et al. [28] proposed a lightweight trust mechanism using direct trust. The packet loss rate is reduced from 60% to 20-30%.

Sybil attacks in RPL-based LLNs may be detected and prevented using a Gini index-based deterrent proposed in [29]. The malicious node quickly consumes the finite energy resource of legitimate nodes by forcing them to refresh the Trickle algorithm often and broadcasting a large number of DODAG Information Object (DIO) communications. It also broadcasts a considerable proportion of DODAG Information Solicitation (DIS) messages with various fictitious identities. Full-scale simulation studies for performance analysis and comparison may be performed with OMNeT++. To quickly assess the state of the network and respond to various forms of assault, they propose using a responsive DIO message response rate to determine the number of DIO control messages to be sent during each observation window. If a Sybil assault is discovered, the node that made the discovery will send a message to all other nodes to warn them.

Farooq et al. [4] proposed a multi-agent trust approach to mitigate Sybil attacks in wireless sensor networks. The suggested method uses multiple agents to fetch trust-related data and ship it to the fog layer for analysis. The simulation results demonstrate that the proposed approach performs better than the state-of-the-art approaches regarding message, memory, and computation overheads. A Bayesian network-based method for identifying forwarding misbehavior in RPL-based IoT networks was proposed by Liu et al. [30]. The method uses the node trust values and link quality to determine the likelihood of forwarding misbehavior. The authors' experiments evaluating the proposed approach demonstrate that it can successfully identify forwarding misbehavior. The method, however, makes the erroneous assumption that trust metrics and link quality are reliable, which may not always be the case in a real environment.

A Deep Q-Learning-based approach for anomaly detection and defense in distributed IoT-based cyber-physical systems was proposed by Liu et al. [31]. The method employs a deep neural network to identify irregularities in system behavior and Q-Learning to determine the best defense strategy against cyber-attacks. The results demonstrate that the suggested approach can successfully detect and defend against various cyber-attacks when applied to a real-world dataset. However, the method's reliance on the availability of labeled data for training can be a drawback in some circumstances. In the IoT context, Saleem et al. [32] discuss a trust management strategy based on beta reputation for wireless sensor networks. The plan aims to manage trust between network nodes to increase the security and dependability of IoT networks. The article thoroughly explains the proposed scheme and presents simulation results to assess its effectiveness. A fuzzy logic based trust management strategy was put forth in [33] to protect RPL-based IoT networks from selective forwarding attacks. The proposed method uses a trust value determined by the node's network behavior and packet delivery ratio. The evaluation's findings demonstrate how well the suggested scheme can identify and stop selective forwarding attacks. However, the approach's scalability and applicability to other types of attacks are not thoroughly examined in the paper. A Deep Q-Network-based security framework for IoT was proposed by Wang et al. [34] to detect flooding attacks. Using a Q-learning algorithm, the framework determines the best action in response to network states. Despite limitations in scalability and applicability to other types of attacks, the proposed approach yields encouraging results.

Table 1 summarises the details of different trust models concerning trust type (i.e., direct or indirect trust), trust model used, trust parameters, simulation tool, number of nodes, simulation time, and results. Out of all, 75% papers used the direct trust model to calculate each node's trust at the node level, showing that they are straining resource-constrained SG devices. Whereas 60-65% use the packet loss ratio parameter to calculate trust as it is one of the crucial trust parameters for assessing a node's credibility. Determining trust parameters and methods in resource-constrained LLNs is challenging. Specific parameters are not scalable or adaptable because of the changing network dynamics, which consume more energy and power in LLNs. Since LLNs are highly resource-constrained, traditional security measures, such as cryptography and trust-based mechanisms, may drain their limited memory, power, and computing resources. Therefore, this study targets internal attacks preserving LLNs' limited resources to improve network lifetime and performance.

Table 2 compares different mitigation methods using trust mechanisms for RPL-based routing attacks.

TABLE 2. Comparison of trust-based approaches for detecting attacks in RPL-based IoT networks.

Reference	Trust Type	Trust Model	Trust Parameters	Simulator Used	Nodes Used	Simulation Time	Result
[35]	Direct	Learning Automata	L, ϵ	Cooja	100	900s	Sybil attack detection
[30]	Direct	Bayesian Network	Trust value, energy, memory	Cooja	40	1800s	Detection of forwarding misbehavior
[31]	Indirect	Distributed Q-Learning	Q-value, state-action pairs	Cooja	50	3600s	Detection of puppet attack
[32]	Direct	Beta Reputation	Trust value, number of packets, energy	Castalia	50	3600s	Detection of energy depletion attack
[33]	Direct	Fuzzy Logic	Trust value, packet delivery ratio	Cooja	50	3600s	Detection of spam DIS attack
[34]	Direct	Deep Q-Network	Q-value, state-action pairs	Cooja	100	1800s	Detection of flooding attack

III. BACKGROUND

This section details the background techniques and models used in the proposed framework.

A. ROUTING PROTOCOL FOR LLN (RPL)

RPL is the accepted SG routing protocol for communication. RPL, while operational, works by finding different routes. On inception, an RPL protocol makes a tree-like topology known as a Directed Acyclic Graph (DAG). Each sensor node in an RPL network chooses a parent node that works as a packet entryway for that specific node [36]. Data concerning the topology of the Routing Protocol for LLNs is kept up as a chart-like construction called Destination Oriented Directed Acyclic Graph.

DODAG comprises paths between sender and sink nodes. The rank of each node is kept up during routing, compared with its situation in the DODAG tree, and each DODAG is populated with parent data, which incorporate control and course. Data are utilized for network security and routing. The data utilized by DODAG will be DODAG Information Solicitation and DODAG Information Object for sending the DODAG details. For RPL, route choice is a vital factor, and unlike traditional routing protocol, RPL uses various variables to figure out the best path [20]. Different routing measurements, route limitations, and target elements, such as Objective Functions (OF), are a few variables utilized during directing. Directing choices depend on indicated OFs like bounce tally, energy minimization, and idleness.

B. GINI INDEX THEORY

The Gini index is an impurity value-based criterion. This value evaluates the probability of two chosen values and determines their divergence. The Gini impurity measures how likely a randomly chosen characteristic would lead to misclassification. It may be considered pure if all the components are connected with a single class. The Gini index may take on values between 0 and 1, where 0 indicates perfect categorization, whereby all data points are assigned to a single category. While 1 demonstrates the random distribution of components across different classes. The Gini Index 0.5 reflects an equal distribution of components across several classifications. It is a statistics-based strategy. As represented in Eq.(1), it uses statistical concepts to detect divergence.

$$Gini(y_{test}, S_{train}) = 1 - \sum (\frac{\sigma_{y_{test}} = c_j S_{train}}{|S_{train}|})^2 \quad (1)$$

where S_{train} represents the training set, y_{test} represents the testing set, and c_j is constant. Further details are provided in Section V.

C. SYBIL ATTACKS

Sybil attack is a devious attack. A malevolent node executing this kind of assault could take on the appearance of a few elements. To propel its assaults, a Sybil node can additionally dispatch Byzantine assaults on the network. It creates a deception that numerous malevolent hubs work inside the organization, overpowering it and disturbing the network's topology. Although a few strategies have been suggested to address the weaknesses in the security of the RPL protocol, these strategies show differences. However, trust is a good idea effectively explored, intending to

TABLE 3. Routing and Internal Attacks' state-of-the-art.

Ref.	Attack	Limitations
[3]	Blackhole	Message overhead
[9]	Rank, Greyhole and Blackhole	Not applicable to any other attack's detection or mitigation
[10]	Rank and DDoS	Use only one parameter to calculate trust that may result in misleading trust results
[20]	Sybil	Only one parameter is used, which may result in misleading trust results.
[17]	Network Level attacks	Does not address specific attacks. It uses only one parameter to calculate trust that may result in misleading trust results
[18]	Rank and Sybil	Use only one parameter to measure trust, i.e., Packet forwarding that may result in misleading trust results
[19]	Rank, Sybil and Blackhole	Memory and Computationally expensive model
[21]	Blackhole and Greyhole	Message overhead and excellent energy consumption. It is also computationally expensive
[22]	Rank, Sybil, and Blackhole	Focus of the paper is only on a single point of failure
[23]	Blackhole	Only uses one parameter for mitigating attacks that may result in misleading trust results
[24]	Blackhole	Message and computation overhead
[25]	Blackhole	Only single trust parameter that may result in misleading trust results
[26]	Blackhole	Message and energy overheads
[27]	Sybil and Rank	Energy consumption issue. Legitimate nodes are also considered bad nodes.
[28]	Sybil	Use only one parameter to measure trust that may result in misleading trust results

address security weaknesses in the RPL protocol. Table 3 represents different routing and internal attack state-of-the-art limitations.

D. SMART GRID

The Smart Grid is an intelligent electricity network that integrates advanced communication, information, and control technologies into the traditional power grid to enhance efficiency, reliability, and sustainability [37]. It enables two-way communication between the power supplier and the consumers, providing a more efficient and sustainable energy management system, as shown in Fig. 1. Several components of the SG work together to achieve its goals. The major components of the SGs are discussed below:

1) Advanced Metering Infrastructure (AMI):
AMI is a smart-meter system that regularly measures and records energy consumption data and transmits it to the utility company in real-time. It allows utilities to monitor energy usage patterns and manage the grid more effectively. AMI also enables customers to monitor their energy usage and make informed decisions about their energy consumption [38].
2) Distribution Automation (DA):
DA involves advanced sensors, control systems, and communication technologies to monitor and control the distribution of electricity on the grid. It allows utilities to detect and respond to power outages more quickly and efficiently, reducing downtime and improving customer satisfaction. It also helps optimize energy resource use, reduce carbon emissions, and increase the reliability and resilience of the grid [39].
3) Demand Response (DR):
DR enables utilities to incentivize customers to reduce their energy consumption during peak hours by providing them with financial rewards or other incentives. It helps to balance the supply and demand of energy on the grid and reduces the need for expensive and polluting peaker plants. It also enables customers to save money on their energy bills and contribute to the sustainability of the grid [40].
4) Energy Storage Systems (ESS):
ESS are devices that store energy in the form of electricity or other forms of energy, such as thermal or chemical energy. They can store excess energy generated during off-peak hours and release it during peak hours when demand is high. It also enables the integration of renewable energy sources, such as solar and wind power, into the grid by providing a buffer for the intermittent output of these sources [41].
5) Microgrids:
Microgrids are small-scale, self-contained electricity networks operating independently or in conjunction with the main grid. They can provide power to remote or isolated communities and backup power in power outages or other emergencies. Microgrids can also be used to integrate renewable energy sources, such as solar and wind power, into the grid by providing a local source of energy generation [42]
These are just a few of the significant components of the SG, and there are many others, such as electric vehicle charging infrastructure, grid analytics, and cybersecurity, which are also important. The SG has the

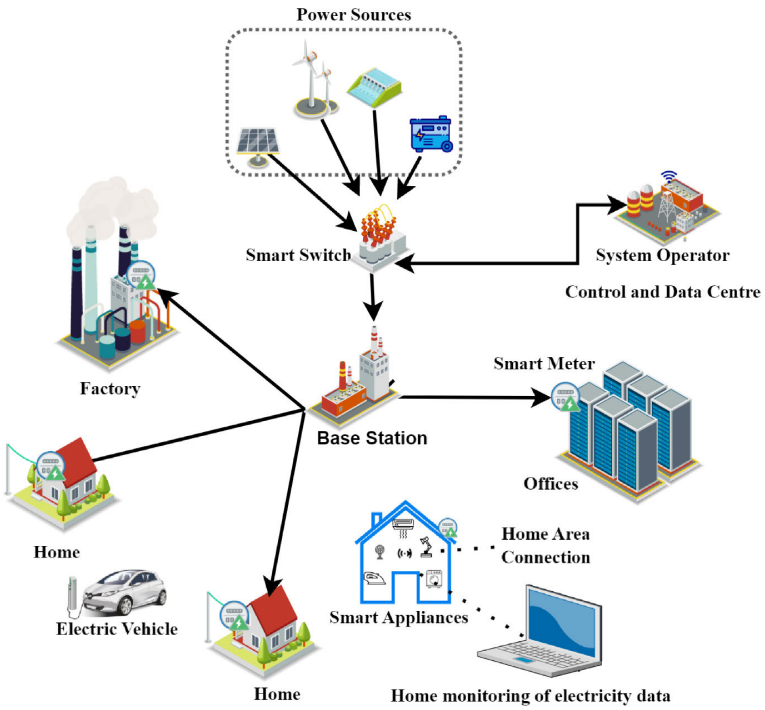


FIGURE 1. A generic smart grid infrastructure.

potential to transform the energy industry and provide a more sustainable and efficient energy management system for the future; therefore, its security is inevitable.

E. EFFECTS OF SYBIL ATTACK IN A SMART GRID SCENARIO

A Sybil attack is a security attack in which an attacker creates multiple fake identities or nodes to gain control of a network or system. In a smart grid scenario, a Sybil attack can have severe consequences as it can lead to the manipulation of energy data, causing disruptions in the supply and demand balance and ultimately impacting the stability and reliability of the grid. Smart grid systems rely on a network of sensors, communication channels, and control devices to monitor and manage the flow of electricity. These devices need to be authenticated and authorized to ensure the integrity and security of the system. Sybil attacks can undermine this security by creating fake nodes or devices that appear to be legitimate but are controlled by the attacker.

One way a Sybil attack can work in a smart grid scenario is by the attacker creating multiple fake smart meters. These meters can generate false data, showing lower or higher energy usage than the actual consumption. It can cause a mismatch between the energy demand and supply, leading to an imbalance in the grid. As a result, the grid operator may take incorrect actions, such as reducing or increasing the energy supply, which can have severe consequences for the grid's stability. Another way a Sybil attack can also work in a smart grid scenario is by creating fake nodes on the communication network. These nodes can intercept, modify or inject messages into the communication channels, leading to unauthorized access to the grid or manipulation of the energy data.

Physical and software-based security measures are required to prevent Sybil attacks in a smart grid. For instance, physical security measures such as secure communication channels and access control mechanisms can prevent unauthorized access to the smart grid infrastructure. Meanwhile, software-based security measures such as authentication, encryption, and intrusion detection systems can help prevent Sybil attacks by detecting and blocking the creation of fake nodes or devices.

In conclusion, Sybil attacks can severely impact the security and stability of SGs. As such, it is crucial to implement strong security measures to prevent such attacks and ensure the integrity and reliability of the smart grid infrastructure. Table 4 summarizes recent cyber attacks on SG Networks.

F. SYBIL ATTACK IN SMART GRIDS: THREAT MODELS AND FORMAL DESCRIPTION

1) THREAT MODEL 1

A Sybil attack happens when a single entity creates multiple fake identities to control or manipulate a network. In the context of smart grids, a Sybil attack can be launched against the communication infrastructure used by AMI to collect and transmit data from smart meters to the utility company. The threat model for a Sybil attack in smart grids can be expressed

TABLE 4. Recent cyber attacks on SG networks.

year	Country	Attack	Impact
2007	United States	Cyber Espionage	Chinese hackers gain access to the US electricity grid and install malware to monitor and potentially disrupt operations [43]
2010	Ukraine	Cyber Attack	Russian hackers remotely access the control systems of a power plant and shut down a large portion of the grid, leaving over 200,000 people without power for several hours [44]
2015	Ukraine	Malware	Russian hackers again target the Ukrainian grid, using malware to cause a widespread power outage that lasted for several hours and affected over 225,000 customers [45]
2016	United States	Distributed Denial of Services (DDoS)	A group of Russian hackers gain access to a utility company's network and attempt to breach the grid's operational systems, but are ultimately unsuccessful [46]
2017	Ukraine	Malware	Russian hackers use malware to target the Ukrainian grid once again, causing a power outage that affected over 230,000 customers for several hours [47]
2018	United States	Malware	Iranian hackers gain access to a US power company's network and deploy malware that could potentially disrupt grid operations [48]
2019	Chile	Ransomware	A ransomware attack targets a major energy company in Chile, disrupting its billing and customer service systems [49]
2020	United States	Phishing	A phishing campaign targets US utilities, attempting to gain access to their networks and potentially disrupt grid operations [50]
2021	United States	Ransomware	A ransomware attack targets a major fuel pipeline in the US, causing widespread fuel shortages and price increases [51]
2021	Germany	Ransomware	A hacking group targets a German energy company, gaining access to its IT systems and potentially being able to disrupt grid operations [52]

as a tuple in Eq. 2.

$$TM = \{A, C, V\} \tag{2}$$

where $A = \{s, m1, m2, \ldots, mn, u\}$ is the set of assets at risk. Here, s represents the Sybil node(s) created by the attacker, $m1, m2, \ldots, mn$ are the legitimate smart meters, and u is the utility company server that receives the data from the smart meters. Let $C = \{k, p\}$ be the set of attacker capabilities and motivations. Here, k represents the attacker's knowledge of the AMI infrastructure and communication protocols, and p represents the attacker's motivation to manipulate or disrupt the data transmitted by the smart meters. Let $V = \{rpl, vl\}$ be the set of vulnerabilities that may be exploited. Here, rpl represents the Routing Protocol for Low-power and lossy networks used for routing data between smart meters and the utility company server. The vulnerabilities vl in RPL can be exploited by the attacker to create Sybil nodes and manipulate the data transmitted by legitimate smart meters. The Sybil attack threat model can be used to design and implement appropriate security measures to protect against the identified threats. In particular, the proposed mechanism can be used to detect and isolate Sybil nodes and prevent them from manipulating the data transmitted by legitimate smart meters.

2) CASE STUDY 1: SYBIL ATTACKS IN SMART GRIDS

a: OVERVIEW

In the Sybil attack scenario, a malicious node fosters multiple fake identities, or Sybil nodes, in a network to deceive and disrupt the functionality of legitimate nodes. Sybil attacks can devastate SGs, including energy theft, inaccurate data collection, and even cascading blackouts.

b: FORMAL DESCRIPTION

In a Sybil attack scenario on SGs, the attacker creates multiple fictitious smart meters that imitate the network's legitimate smart meters. These fake meters can generate false data, transmit bogus control messages, and impersonate legitimate smart meters in the network. Using the forged data, the attacker can manipulate the network's behavior, cause power imbalances, and potentially cause blackouts.

c: MATHEMATICAL MODEL

Let the mart grid network be $G = \{V_n, E_g\}$, where V is the set of nodes and E is the set of edges. Let S_y represent the attacker-created Sybil nodes. The attacker seeks to maximize the Sybil attack's impact by creating many Sybil nodes while minimizing the possibility of detection. The objective of the attack is to convince legitimate nodes in the network that Sybil nodes are legitimate. The Sybil nodes generate false data and transmit false control messages to manipulate the network's behavior. Network manipulation allows attackers to achieve their goals, such as power imbalances, energy theft, or blackouts.

d: FORMAL DEFINITIONS

Sybil nodes can be formally defined as follows:

Let N represent the set of network nodes, and $f : N \rightarrow [0, 1]$ represent a function that assigns each node a reputation score. A node $v \in N$ is a Sybil node if it has created one or more fake identities $\{v_1, v_2, \ldots, v_k\}$ to deceive other nodes into believing that there are more nodes in the network controlled by different entities. Formally, a node $v \in N$ is considered Sybil if there exists a set of nodes $S = \{v_1, v_2, \ldots, v_k\}$, where $k \geq 1$, such that: $S \cap N = \emptyset$, i.e., none of the fictitious identities in S have yet become a network member. $f(v) < \frac{1}{k+1}$ indicates that the reputation score of the Sybil node v is less than the average score of the nodes in $S \cup v$. v_i has no immediate link to any other node in $N \setminus S$; therefore, the fake identities do not have an immediate link to any legitimate node. Notably, the preceding definition assumes

that the reputation scores of network nodes are known and that Sybil nodes are attempting to deceive other nodes by creating fake identities.

- Sybil Nodes: A group of fictitious nodes created by an attacker in a smart grid network to fool reliable nodes.
- False Data: Information generated by Sybil nodes that is inconsistent with actual readings.
- Bogus Control Messages: Sybil node-generated messages that do not match the control commands.
- Manipulated Network: It refers to a network whose behavior has been changed by Sybil nodes to serve the attacker's purposes.

e: PROPOSITION

Let S represent the Sybil attack that causes cz, which includes wrong information collection, energy theft, power imbalances, and cascading blackouts within the network N. Let $s_n \in S = s_1, s_2, s_3, \ldots, s_n$ denote a set of randomly chosen fictitious Sybil identities as nodes. D be the degree of difficulty in locating and mitigating s_n within N, while T be the trust-based mechanisms assessing the nodes' atypical behavior ab.

f: PROOF

The presence of S in N leads to several undesirable consequences, including cz. To identify ab and augment D, T measures the impact I based on T_P (Trust parameters) in N. T can effectively mitigate S and reduce the degree of difficulty (D) associated with locating and handling s_n within the network N.

G. THREAT MODEL AND SECURITY ANALYSIS

Utilising cutting-edge technologies, smart grids increase the efficiency and dependability of electricity distribution while facilitating two-way communication between power suppliers and consumers. Smart meters, sensors, communication networks, and control systems are just a few of the system's various parts, all linked to a centralized management system. The central management system uses the data from the smart meters to monitor and manage the energy distribution network. The smart meters gather information on electricity consumption and send it there. Figure 2 represents a Sybil attack scenario in a smart grid infrastructure with smart meters, smart homes, and RPL nodes. The wireless network connects the RPL nodes, ranging from 1 to 7. The RPL protocol is used in the network to route data packets. In this case, an attacker compromises Node 1 and creates four fictitious identities with the names 1a, 1b, 1c, and 1d. The network is subjected to a Sybil attack using these fictitious identities. The attacker modifies the routing information in the network and introduces fake data packets using the Sybil nodes. Attackers can choose which packets to forward and which to drop using the Sybil nodes to carry out selective forwarding attacks. The legitimate nodes in the network use the RPL protocol, which offers a mechanism for routing and forwarding data packets between nodes based on the topology details and the routing metrics. However, a Sybil node in the network can alter the topology data and routing messages to deceive the trusted nodes and create fictitious routes. It can result in many security risks, including data tampering, data injection, and denial of service attacks.

1) CASE STUDY 2: SYBIL ATTACK IN A SMART METERING SYSTEM

A smart meter measures a household's energy usage in a smart metering system and sends that data to the utility provider for billing. Although the smart metering system is intended to be secure, a Sybil attack can damage it. In this case, a Sybil node is installed by an attacker inside the smart metering network. Although the Sybil node in the network seems legitimate, the attacker has control over it. The attacker can use the Sybil node to alter the energy consumption readings of other network nodes, which could result in inaccurate utility billing and potential customer financial loss.

A security flaw in the network allows the attacker access to the smart metering system. They exploit this weakness to introduce a Sybil node into the network that impersonates a genuine node. The Sybil node then starts to tamper with other network nodes' readings on their energy usage. The Sybil node can carry out various attacks, such as reporting the energy usage of specific nodes, either too much or too little. For instance, the attacker might give the Sybil node instructions to over-report a particular household's energy usage, resulting in higher bills for that household.

Alternatively, the attacker might instruct the Sybil node to overstate a specific household's energy usage, resulting in lower bills for that household. The utility company has difficulty identifying the attack because the Sybil node seems to be a legitimate node within the network. If the attacker can access the Sybil node, they can keep changing the energy consumption readings. To prevent this attack, the smart metering system should implement robust security measures, such as secure authentication mechanisms and encryption protocols.

Additionally, the system needs to be regularly checked for suspicious activity, such as odd energy use patterns or sudden network traffic changes. In conclusion, a Sybil attack can jeopardize a smart metering system's integrity, resulting in inaccurate utility billing and possible customer financial loss. To stop these kinds of attacks, smart metering systems must implement robust security measures.

a: FORMAL DESCRIPTION

Let a smart metering network be the graph $G = \{V_n, E_g\}$, where V_n is the set of nodes, and E_g is the set of edges. Let v_s be a Sybil node built by an attacker, and v_i be a valid node in the network. A group of Sybil nodes, denoted as $S = \{v_s1, v_s2, \ldots, v_sk\}$, are under the attacker's control.

Suppose the network's trustworthy nodes use the RPL routing protocol. By creating fictitious routes and transmitting false data, the attacker can attack the network internally using

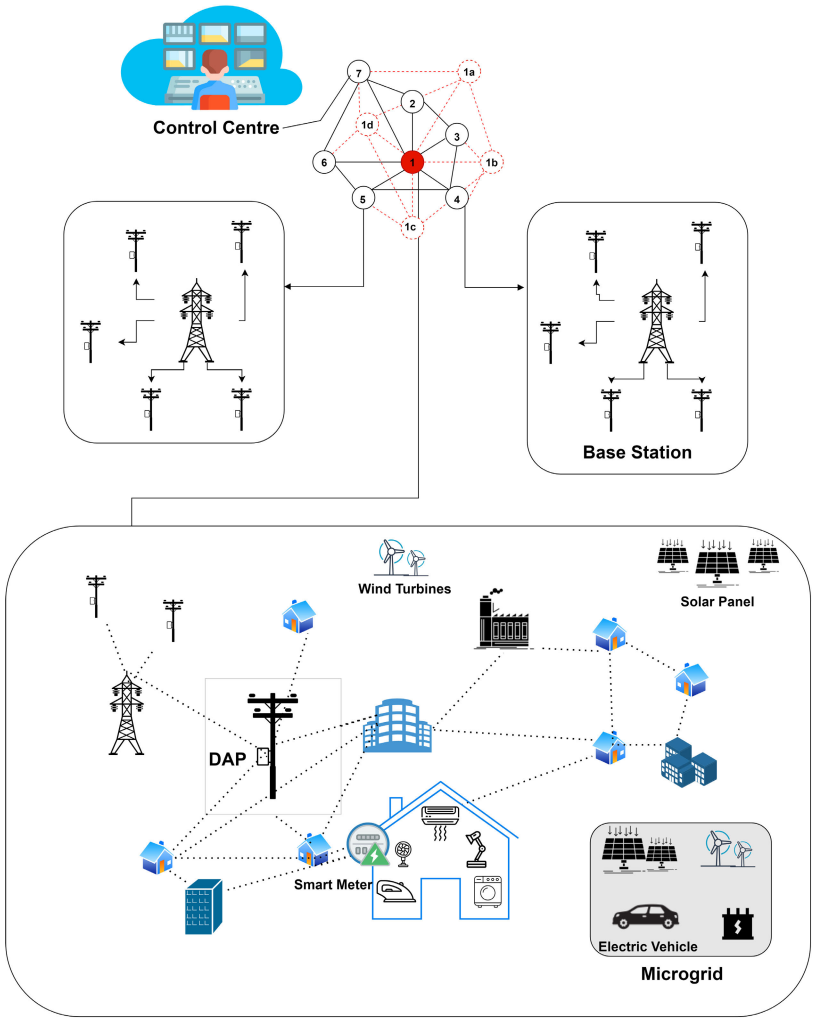


FIGURE 2. A Sybil attack scenario in a smart metering system.

Sybil nodes. Let $D = \{d_1, d_2, \ldots, d_n\}$ represent the data packets set sent over the network. The attacker can create fake routes by falsifying routing messages and changing the network's topology information. Assume that $R = \{r_1, r_2, \ldots, r_m\}$ is the collection of routing messages sent over the network. By forging the packets' source addresses, the attacker can also send fake data packets to legitimate nodes in the network. Let $F = \{f_1, f_2, \ldots, f_l\}$ represent the collection of erroneous data packets sent over the network.

The attacker aims to interfere with the smart metering network's normal operation by introducing false data and fabricating routes. A game between the attacker and the trustworthy nodes in the network can be used to describe the attack. Let A represent the set of possible attacks where the attacker can set up Sybil nodes, forge routing messages, and send false data packets. Let L denote the range of operations that legitimate nodes can perform, such as forwarding legal data packets and identifying and isolating Sybil nodes. By interfering with the network's regular operations and harming the system, the attacker intends to have as much impact as possible. By identifying and isolating the Sybil nodes and filtering out erroneous data packets, the legitimate nodes seek to reduce the attack's impact.

The attack can be represented as a two-player game $G = \{V, A, L, f\}$, where f is a payoff function that measures the impact of the attack. The attacker's payoff is defined as the negative of the impact, while the legitimate nodes' payoff is defined as the positive of the impact. Formally, the payoff function can be defined as presented in Eq. 3.

$$f(A, L) = -w_1 \cdot I - w_2 \cdot R - w_3 \cdot F \tag{3}$$

where w_1, w_2, and w_3 are weights that represent the relative importance of each factor in the attack, I is the impact of the attack, R is the number of forged routing messages, and F is the number of false data packets. Sybil nodes can be identified by keeping an eye on each node's network activity and examining their routing messages. When a Sybil node is found, it can be isolated by having its traffic filtered and its routes eliminated from the network topology. The detection rate and energy consumption, for instance, are two indicators of how well the isolation and detection mechanism (i.e., trust-based security) works. Modifying the

trust model's thresholds and parameters can enhance security against internal attacks.

b: MATHEMATICAL DEFINITION

Assume that the directed graph $G = \{V_n, E_g\}$ represents a smart metering network, with V_n denoting the set of nodes and E_g denoting the set of edges. Let S_m represent the collection of smart meters accountable for informing the central server of their readings. A Sybil attack can create multiple false identities and use them to gain access to a network, interfere with its operation, or tamper with reported measurements.

c: COROLLARY

The integrity, confidentiality, availability of the reported measurements and the proper operation of the network can all be compromised in a smart metering network by a Sybil attack, which can result in monetary losses, safety risks, and privacy violations.

d: PROOF

Assume that a hacker intends to use k Sybil nodes (i.e., $\{S_1, S_2, \ldots, S_k\}$) to launch a Sybil attack against a smart metering network. The attacker may employ social engineering, eavesdropping, or hacking techniques to gather the data required to build the Sybil nodes. The attacker can use the Sybil nodes after they have been created to carry out several malicious tasks, including:

- Data theft: The Sybil nodes can impersonate legitimate smart meters to intercept and steal the measurements they report or compromise the communication channels. The assailant may use the stolen information for extortion, fraud, or identity theft, among other things.
- Data fabrication: The Sybil nodes can create and transmit fictitious measurements to the central server by creating them from scratch or stealing them from other smart meters. The attacker can manipulate the network's billing, load balancing, or demand response using the fabricated data, which could result in losses in revenue or security risks.
- Data jamming: The Sybil nodes can interfere with data transmission between the legitimate smart meters and the central server by sending false messages, overburdening the network, or introducing noise. The attacker can launch a denial-of-service attack, postpone reporting actual events, or conceal other nefarious activities using the jammed data.

In a smart metering network, several security measures, including authentication, encryption, intrusion detection, and anomaly detection, can be used to thwart and detect Sybil attacks. These mechanisms might, however, be subject to trade-offs or restrictions, such as computational costs, communication costs, false positives, or false negatives. A thorough security analysis of the network's topology, protocols, and devices is required to assess the network's resilience to Sybil attacks and other types of attacks.

IV. THREAT MODEL IN OUR CASE

Let $G = \{V_r, E_g\}$ be an AMI network with V_r being the set of nodes and E_r being the set of communication links between them. Let us divide the nodes in V_r into two types legitimate (i.e., L) and Sybil (i.e., S) nodes. Table 5 represents the parameters (used in this threat model) and their description.

The threat model can formally be described as follows: A Sybil node masquerades as multiple legitimate nodes, creating a false sense of network trust. Let f be the probability that a node is a Sybil node, and $f(1-p)$ be the probability of a communication link between a legitimate node and a Sybil node. The proposed GITM mechanism seeks to detect and isolate Sybil nodes with minimal energy consumption at the node level while decreasing isolation latency and enhancing attack detection rates to optimize network lifespan and performance. Let c be the control messages required for Sybil attack detection and isolation. Malicious behavior can be characterized as misrouting or selective forwarding s_f. α represents the proportion of legitimate nodes that exhibit malicious behavior.

Let us assume that the communication links between nodes are either stable with a probability of p or unstable with a probability of q. Unstable links can result in significant packet loss and lagging transmission rates, resulting in insufficient data and instability in correspondence links. Due to the limited resources of IoT devices, LLNs must also take energy consumption into consideration. To minimize node-level energy consumption and memory overhead, trust-related computations to the upper (fog) layer. It is to be noted that message overhead costs will also decrease since nodes will not resend lost messages due to attacks (as malicious nodes will be isolated). This results in improved network performance and conserved total network energy consumption E_{total}, which results in a longer network lifetime $N_{lifetime}$ compared to the existing work.

A. SCENARIO

This section presents the GINI index as a trust-based model to identify nodes' trustworthiness in the above scenario. In the given scenario of a smart metering system, we can use the Gini index as a trust-based model to identify the trustworthiness of nodes in the network. The Gini index is a measure of statistical dispersion that is commonly used to represent the distribution of income or wealth in a population. In the context of trust-based models, the Gini index can represent the distribution of trust values among the nodes in a network. Assume that the network has n nodes, each having a trust value represented by T_i. A definition of the Gini index is represented in Eq. 4:

$$G = \frac{1}{n}\left[\frac{2\sum_{i=1}^{n} i \cdot T_i}{\sum_{i=1}^{n} T_i} - (n+1)\right] \tag{4}$$

where n is the total number of nodes in the network, T_i is the trust value of node i, and G is the Gini index. The Gini index ranges from 0 to 1, with 0 denoting an equal distribution of trust values among the nodes and 1 denoting an entirely

TABLE 5. Parameter Description for Threat Model 1.

Parameter	Description
$n = \|V_r\|$	Total number of nodes in the network
$m = \|E_g\|$	Total number of communication links in the network
f	Fraction of Sybil nodes in the network
p	Probability that a communication link between two nodes is stable
q	Probability that a communication link between two nodes is unstable (i.e., there is a high failure rate and low information)
α	Fraction of legitimate nodes that behave maliciously (i.e., internal attacks)
d	End-to-end delay of a message in the network
c	Number of control messages needed for Sybil attack detection and isolation
E_{total}	Total energy consumption of the network

unequal distribution. We can compute the Gini index for each node in the network based on their trust values to use it as a trust-based model. Since there is a greater concentration of trust values among a smaller number of nodes in nodes with higher Gini index values, they will be regarded as less reliable. On the other hand, nodes with lower Gini index values will be regarded as more trustworthy because they have an even distribution of trust values.

a: COROLLARY

The trustworthiness of nodes in a smart metering system can be determined using the Gini index G as a model based on trust.

b: PROOF

Let us assume that the smart metering system has n nodes, each of which has a trust value denoted by T_i. Based on the trust values of each node in the network, we can calculate the G for each node by performing the following steps:

1) Determine the ST value, representing the network's overall trustworthiness: ST: $ST = \sum_{i=1}^{n} T_i$.
2) According to their trust values, rank the nodes from 1 to n in descending order. Rank 1 will be assigned to the node with the highest trust value, and rank n will be assigned to the node with the lowest trust value. In the given scenario, the Lorenz curve can be represented in Eq. 5.

$$L(p) = \frac{1}{S_T} \sum_{i=1}^{n} T_i \cdot \mathbf{1}_{i/n \leq p} \tag{5}$$

where the cumulative percentage of the total trust value is represented by $L(p)$ with a given percentile p, T_i denotes the trust value of node i, S_T denotes the aggregate trust value of all nodes in the network, n denotes the total number of nodes in the network, and $\mathbf{1}_{i/n \leq p}$ is the indicator function that returns 1 if $i/n \leq p$ otherwise a 0. This model can determine the Lorenz curve for a specific set of trust values in a smart metering system. The Gini index formula can then determine the degree of inequality in the distribution of trust values among the nodes.

3) Starting with the node with the highest trust value, compute the Lorenz curve, which depicts the cumulative percentage of the total trust value held by the nodes. The Lorenz curve can be visualized as a set of points $\{x_i, y_i\}$, where x_i denotes the total number of nodes (i/n) and y_i denotes the total amount of trust value held by the nodes $\left(\sum_{j=1}^{i} T_j/ST\right)$.
4) The Gini index is calculated as given in Eq. 6:

$$G = \frac{1}{n}\left[\frac{2\sum_{i=1}^{n} i \cdot T_i}{ST} - (n+1)\right] \tag{6}$$

Hence to determine whether a node in a smart metering system can be trusted, the Gini index can be used as a trust-based model. The Gini index G can be calculated using Eq. 7.

$$G = \frac{1}{n-1} \sum_{i=1}^{n} \sum_{j=1}^{n} |x_i - x_j| \tag{7}$$

The Gini index ranges from 0 to 1, where 0 represents perfect equality (all nodes have equal trust scores), and 1 represents perfect inequality (one node has all the trust scores and the others have none). The Gini index can be used as a trust-based model to identify the trustworthiness of nodes in an SG network. Nodes with higher trust scores are considered more trustworthy, while nodes with lower trust scores are considered less trustworthy.

c: LORENZ CURVE

A set of n non-negative numbers representing the cumulative share of a population's overall trust or reputation scores in a smart grid network be $\{x_1, x_2, \ldots, x_n\}$. The total share is normalized such that $x_n = 1$, and these values are sorted in non-decreasing order such that $\{x_1 \leq x_2 \leq \ldots \leq x_n\}$. The Lorenz curve represents the cumulative share of the population and the cumulative share of the population's trust or reputation scores. Mathematically, it is defined in Eq. 8.

$$L(p) = \frac{1}{\sum_{i=1}^{n} x_i} \sum_{i=1}^{p} x_i \tag{8}$$

where p is a number between 1 and n, representing the proportion of the population being considered, $L(p)$ is the cumulative share of trust or reputation scores held by the bottom p proportion of the population.

d: GINI COEFFICIENT

The Gini coefficient is a measure of inequality calculated from the Lorenz curve. It is defined as twice the area between the Lorenz curve and the line of perfect equality (the diagonal

TABLE 6. Nomenclature.

Description	Symbol
Trace Table	TT
Total No of detected Sybil Attacks	TD_{sa}
Total No of Observation windows	TO_{win}
Detection of Sybil attack	AD_{sa}
System Parameters	α, β, γ
Replying DIO message rate	RR^{dio}
Certain threshold	CT_{sa}
Observation window period	O_{win}
Number of classes	N_c
Nodes	n_x, n_y
Current System Time	tcs
Gini Threshold Value	$TV_{gini,i}$
Constant	K

line from $(0, 0)$ to $(1, 1)$), mathematically, it is defined in Eq. 9.

$$G = 1 - 2 \int_0^1 L(p)dp \tag{9}$$

The value of G ranges from 0 to 1, with 0 representing perfect equality and 1 representing perfect inequality.

e: LORENZ INEQUALITY

The Lorenzic function is a measure of the degree of deviation from perfect equality in a distribution of non-negative numbers. It is defined in Eq. 10.

$$L_{ic}(x) = \frac{\int_0^x L(p)dp}{x} \tag{10}$$

where $L(p)$ is the Lorenz curve of the distribution. The Lorenz curve can detect a Sybil attack in a smart grid network. In a Sybil attack, malicious nodes create false identities to pass for various nodes and control the network's behavior. Using the Lorenz curve, we can visualize the cumulative distribution of the nodes based on their trust or reputation scores. A Sybil attack may cause an uneven distribution of trust scores if the curve significantly deviates from the ideal 45-degree line.

V. PROPOSED ARCHITECTURE

This section first lists the assumptions we made to narrow down the scope of the study and addresses the proposed mechanism, which allows for analyzing SG nodes' behavior using the GINI index, fog, and device layers.

A. ASSUMPTIONS

The crucial assumptions that we made are as follows:

1) The fog layer is reliable, secure, and trustworthy.
2) The sink node is reliable and has sufficient energy.
3) The channel is secure and reliable with a minimal error rate.

B. GINI RPL-ENABLED SG NETWORK SYSTEM ARCHITECTURE

This section provides a thorough explanation of the proposed framework's functionality. The proposed architecture is demonstrated in Fig. 3, which comprises a device layer and a fog layer. Whereas, Fig. 4 shows the complete accessibility of all layers and what functions or processes are being performed in these layers. It also details the flow of DIS message gathering, computation of Gini values, and then separation of malicious nodes, and ultimately updating Gini values, computation of Gini values, and then separating malicious nodes and updating Gini values.

Moreover, the complete working of the proposed architecture and layers and their working is also elucidated. The suggested architecture, i.e., the GINI countermeasure, uses statistical characteristics of the identities corresponding to the Sybil attack. Using the Gini index theory to identify a Sybil network node, the GINI measures the distribution of the identifiers inside the received DIS messages [20]. Nevertheless, there are other measures of inequality that can be used to detect Sybils, such as the Theil index [53]. The Theil index is a well-known indicator of income inequality used in several fields, including social networks, ecology, and epidemiology. It gauges the relative distribution of a resource or attribute among a group of entities based on entropy. It can be broken down into components that reflect various sources of inequality, unlike the Gini index, which only measures between-group inequality. The Gini index, as opposed to the Theil index, is a better indicator for Sybil detection in smart metering networks. The Gini index has been widely used to detect Sybil attacks in the literature, and research has shown that it is successful under various conditions. For instance, the Gini index was used in many studies (e.g., [29], [54]) to identify Sybil attacks on the power grid, and it was found to perform better than other metrics like the Theil index and the Herfindahl index. The network size and the number of legitimate nodes impact the Gini index less than the degree of concentration and the number of Sybil nodes. In addition, the Gini index is easier to understand and has a few advantages over the Theil index. The Lorenz curve and degree of concentration can be used to interpret the Gini index, a well-known indicator of inequality. The Theil index is a more intricate metric that uses the exponential and logarithmic functions and may be less apparent to non-experts. Theil index's robustness and dependability in the presence of noise or anomalies may also be impacted because it may be more sensitive to extreme values and outliers.

1) Device Layer
   SG devices (i.e., actuators and sensor nodes) are installed as LLNs in this layer, and devices deployed in this layer act as a cluster. These nodes/devices gather, sense, and pre-process data from the environment before forwarding it to the root node. These are stagnant and installed at random, considering the stability of nodes. Via symmetric ties, each node is linked to all of its neighbors. This layer's two key processes are DIS message collection and Trace Table (TT) creation.
   a) Creation of Trace Table by DIS Messages:
      Every time a new DIS message is received, each node stores the trace of that message in

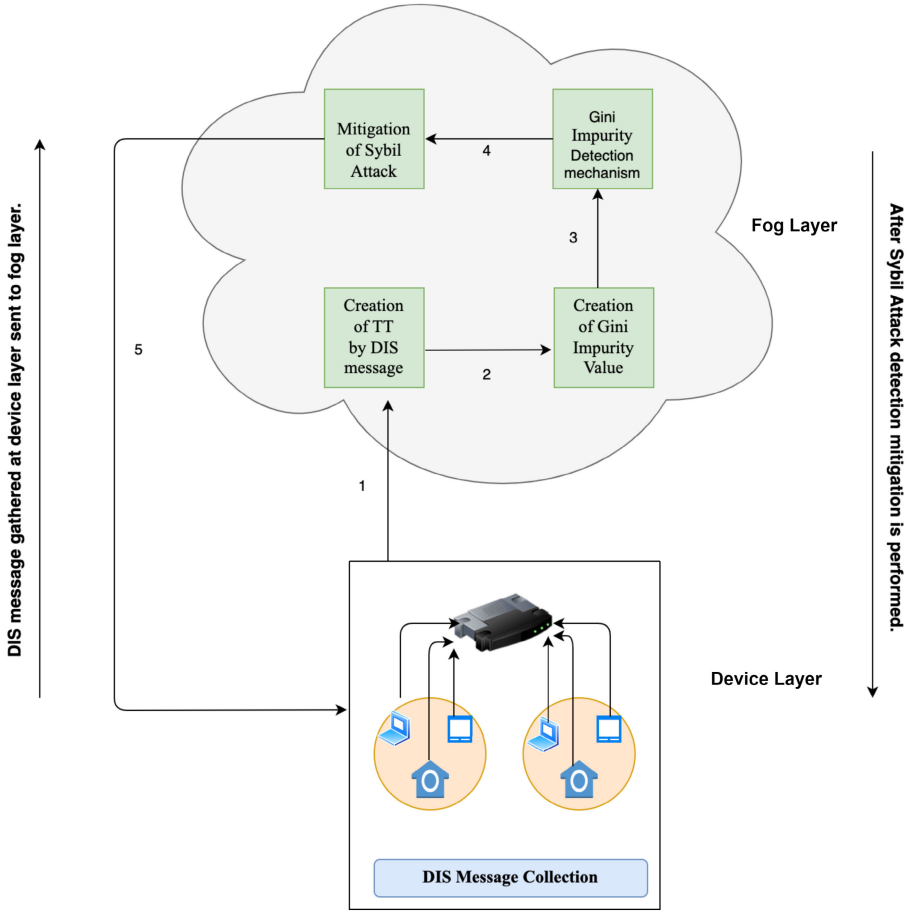


FIGURE 3. The proposed GITM architecture.

its TT. This table monitors any possible DIS message-forwarding misbehavior by the linked nodes. A lack of storage space necessitates the removal of traces from the preceding observation window period with a timestamp of less than $tcs - Owin$. Please note that the TT is moved to the fog layer after each observation window $Owin$ is completed. A system parameter that affects performance is the current system time (tcs). The received DIS message's node identification ($nmac$) and timestamp form an item in the $TT(ts)$. To join an existing network, a new node nx broadcasts a DIS message and listens for a data packet from other nodes in the area. When nY, for example, receives a DIS message, it adds an item to the TT, $TTf = TTf[nx, tcs]$. If a DIO message were scheduled to be sent, it would be broadcast with recent routing information piggybacked on top of a restarted Trickle algorithm.

2) Fog Layer
In the fog layer, the maximum working of architecture is performed. In this layer, three main processes are performed. By adding a fog layer, nodes present in the network are not calculating trust in themselves. Because it consumes much energy, network nodes can also be attacked and compromised, leading to security issues [3], [18]. Therefore, all the trust calculations will be done in the fog layer, which is fully trusted. It shows the perfect result, and the energy consumption of these nodes will be minimized. The functionalities of the fog layer are as follows:

a) Creation of Gini Impurity Value:
After an observation window Owin closes, each node uses Gini index theory to calculate the dispersion of new node identities. The Gini index is a criterion based on impurity determining how much the target attribute's value diverges the probability distributions. In (11), suppose a set X has N_c classes' samples, and P_i represents the relative samples frequency of class I in X. It will produce the Gini Impurity Value of set X.

$$Gini(X) = 1 - \sum_{i=1}^{N_c} P_i^2 \tag{11}$$

b) Gini Impurity Detection Mechanism:
This study employs a Gini impurity level to identify a suspected Sybil assault by evaluating the prevalence of node identification for transmitted

DIS control messages. Without a Sybil attack, the Gini impurity value of freshly connected node identities fluctuates. The ratio of newly connected nodes is minimal, and the identity distribution is relatively stable. The Gini impurity value influences the received DIS control messages. When a Sybil attack occurs, the attacker multicasts an abundance of DIS control messages with various false identities, and the range exceeds the average limit. Equation 12 is used to determine the Gini impurity.

$$SA(D_i) = \begin{cases} 1 & \text{when} \dfrac{Gini(D_i) - Gini(D_{i-1})}{Gini(D_{i-1})} \\ & > TV_{Gini,i} \\ 0 & \text{when} \dfrac{Gini(D_i) - Gini(D_{i-1})}{Gini(D_{i-1})} \\ & \leq TV_{Gini,i} \end{cases} \tag{12}$$

$SA(D_i) = 1$ represents a Sybil attack and $TV.Gini, i$ is the threshold set and gets updated with a filter gain constant K using a low pass filter.

$$TV_{Gini,i} = K \times TV^{avg}_{Gini,i} + (1 - K) \times TV_{Gini,i} \tag{13}$$

In (13), $TV^{avg}_{Gini,i}$ represents an average threshold set for Gini impurity against the entire observation window stage, and $TV_{Gini,i-1}$ represents a Gini impurity threshold in the $i - 1^{th}$ observation window stage.

c) Mitigation of Sybil Attack:
When the Gini impurity detection system identifies a Sybil attack, the attack mitigation mechanism reduces the DIO control message response rate and moderates the Sybil assault. To quickly assess the state of the network and respond to various forms of assault, we propose using an adaptive DIO message response rate to determine the number of DIO control messages to be sent during each observation window. If a Sybil assault is discovered, the node that made the discovery will send a message to all other nodes to warn them. When a node gets an alarm packet, it employs the DIO function to reduce the Response Rate of the DIO (RR_{dio}) control message in the next observation window during the following observation window. RR_{dio} can be calculated using (14).

$$RR^{dio} = \alpha - \beta.e^{1-AD_{sa}.\gamma} \tag{14}$$

In (14), α, β, γ represents parameters of the system. The α represents the asymptote ensuring that the RR^{dio} never reaches 0, AD_{sa} is the cumulative detection probability of Sybil attacks, as shown in (15).

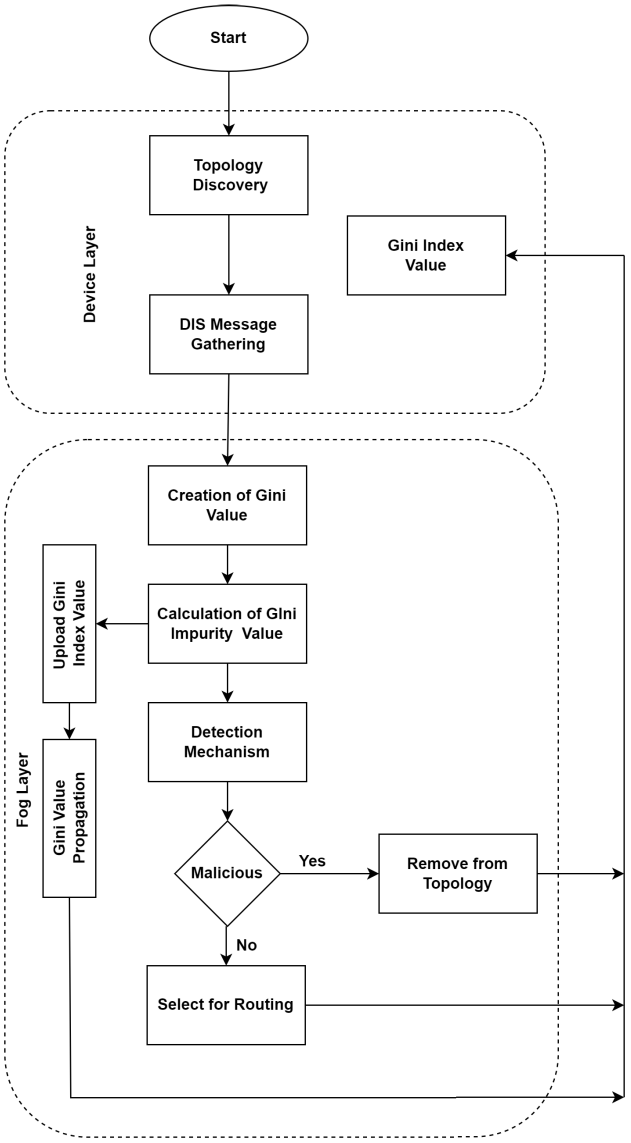


FIGURE 4. Flowchart of the proposed GITM.

$$AD_{sa} = \frac{TD_{sa}}{TO_{win}} \tag{15}$$

The maximum count of Sybil attacks identified is TD_{sa}, and the total observation windows are TO_{win}. Since the DIO message responding rate $RR^d io$ might fluctuate depending on network circumstances, this architecture stands to reason. DIO message replies at $RR^d io$ rate decreases rapidly during an aggressive assault before slowly increasing after the attack. The $RR^d io$ may be kept high if there is no Sybil attack. When the total number of Sybil assaults identified in a region reaches a specific threshold value (i.e., ξ), an Isolate packet is generated and sent to all of that region's one-hop neighbors in order

to prevent those neighbors prevent receiving any DIS messages from of the local area.

Algorithm 1 presents GINI Index-based Trust Mechanism. All required parameters such as TT, N_c, $GINI(D)$, TD_{sa}, AD_{sa}, TO_{win}, RR_{dio}, α, β, γ, CT_{sa}, mac_i, d^* σ are mentioned as input. After evaluation of the packet communicated between nodes (n_x, n_y), the packet is added in TT. Then for all nodes value of P_i is calculated. The value of P_i is used for the Gini Index value. When these data are compared to a threshold, a node is classified as a Sybil attack or a legitimate node. The isolation procedure is done if the nodes are marked as Sybil attack.

Algorithm 1 Proposed GINI Index-Based Trust Mechanism

initialize variables: $TT, N_c, GINI(D), TD_{sa}, AD_{sa}, TO_{win}, RR_{dio}, \alpha, \beta, \gamma, CT_{sa}, mac_i, d^*\sigma$
if $rec(n_x, n_y, DIS) == true$ **then**
  $TT_i = TT_iU[n_y, t_{cs}]$
end if
while $i <= N$ **do**
  if $t_{cs} < \sigma_{ik}$ **then**
    $P_i = \frac{mac_i}{d^*}$
    $Gini(X) = 1 - \sum_{i=1}^{N_c} P_i^2$
    if $\frac{Gini(D_i) - Gini(D_{i-1})}{Gini(D_{i-1})} > TV$ **then**
      $TD_{sa} += 1$
      Broadcast Alarm Packet;
    end if
    $AD_{sa} = \frac{TD_sa}{TO_{win}}$
    $RR^d io = \alpha - \beta.e^{1-AD_sa}$
    if $TD_{sa} > CT_{sa}$ **then**
      Broadcast Isolate Message;
    end if

VI. EXPERIMENTATION AND RESULTS

To evaluate the effectiveness of the proposed model, we carry out a series of extensive simulation-based experiments using the COOJA Network Simulator 2.7. The network area under consideration is a 100 m × 100 m network region in which one DODAG root and thirty hubs are regularly transmitting. The radio model reproduces the CC2420 protocol at an average speed of 250 Kbps when the 802.15.4 MAC/PHY controls in its default mode in the 2.4 GHz band. The transmission rate of each hub is 30 meters per second—random placement of one to three malicious nodes around the network. The Sybil attack rate for malicious DIS packets ranges from 0.1 to 3.0 per second. Sybil attacks occur when a rogue node continuously sends out a large number of DIS packets with fictitious identifiers. We simulate for 60 minutes overall for solid-state performance measures, with each configuration running five times. The number of nodes varies from 30 to 90. Similarly, we set different rounds from 10 to 90 to check the scalability and constancy.

TABLE 7. Table of Experimentation parameters.

Simulation Parameters	Value
Simulation tool	Contiki/Cooja 2.7
Coverage area for simulation	100 m × 100 m
Number of nodes	30 - 90
Malicious nodes	3 - 9
Malicious to attacker node ratio	1: 10
RX ratio	30% to 100%
TX ratio	100%
TX range	50 m
Interference range	55 m
Routing protocol	RPL
Network protocol	IP based
Simulation time	60 min
Number of rounds	10 - 90
Energy Model	As provided in Reference [14]

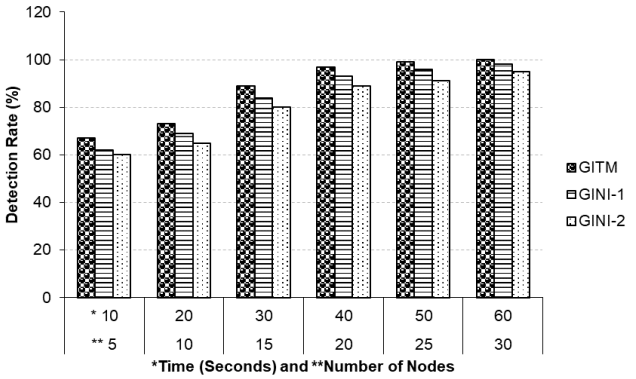


FIGURE 5. Sybil attack detection rate.

This study is evaluated based on the detection rate, energy consumption, end-to-end latency, and the number of control messages exchanged. Table 6 contains the symbols used in the paper for convenient reference, whereas Table 7 contains all the simulation details.

A. EVALUATION METRICS

This section discusses the evaluation metrics used in the experimentation. We do a quantitative evaluation of our proposed countermeasure's efficacy in detecting attacks, as assessed by the proportion of successfully identified malicious nodes to the overall number of harmful nodes in the network. In support of that, we choose attack detection rate, energy consumption, end-to-end delay, number of control messages exchanged, and the isolation latency as evaluation metrics. The metric attack detection rate shows how effectively the proposed mechanism detects the Sybil attack with varying the number of nodes and attacker nodes. Several control messages and energy consumption metrics are also calculated with and without Sybil attack to evaluate its effects on the network.

1) Sybil Attack Detection Rate
The Sybil attack rate is preserved in incremental order to estimate the detection rate, as shown in Fig. 5. When the number of Sybil attacks rises, the overall detection rates of the proposed GITM, the

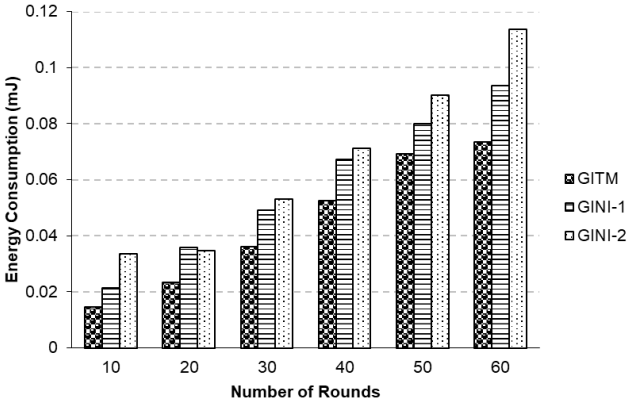


FIGURE 6. Energy consumption.

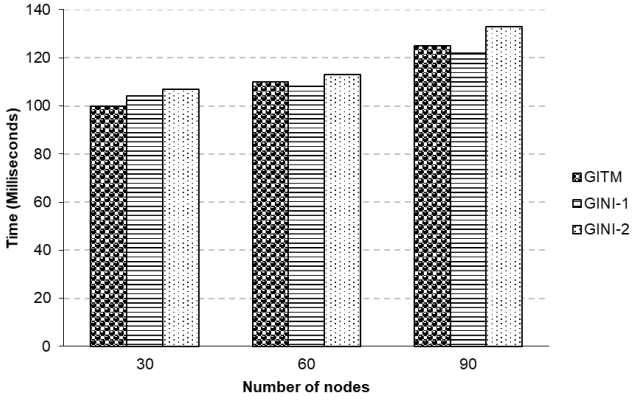


FIGURE 7. End-to-end delay.

GINI-1 [29] and the GINI-2 [20] increase significantly. It happens because of the increased production and distribution of malicious DIS messages containing fictitious identities. When paired with an increased Sybil attack rate, it allows for the recognition of more Sybil attack attempts. The overall detection rate rises as a result. More Sybil attacks may be recognized. A greater detection rate may be achieved due to each node computing the Gini index for two consecutive observational windows and spotting any anomalous fluctuation inside the DIS message receipt rate. The GINI transmits a pre-determined number of DIS signals to detect the Sybil assault and stop it.

On the other hand, the Sybil attack is undetectable when the quantity of malicious DIS messages is smaller than the total number of harmful DIS messages. A consequence is that the overall number of perceived Sybil attacks diminishes, and the detection rate of GINI lowers to a level lower than the level of this model. The simulation is run iteratively, and the Sybil attack number increases with each iteration. The results show that when the simulation is run for 60 seconds with 30 malicious nodes, the attack detection rate of [20] is 95%, [29] is 98%, and for the proposed GITM, it is 100%. On average, the Sybil attack detection rate increases by 4.48% in our case. The GITM algorithm performs better than GINI-1 and GINI-2 in detecting Sybil attacks and identifying nodes across all time intervals. GITM has a higher detection rate than GINI-1 in all cases, with the percentage difference ranging from 2.0% to 8.1%. Meanwhile, GITM outperforms GINI-2 with a percentage difference that ranges from 5.3% to 12.3%.

We can retain this level of precision by using current and prior history in our search for malicious nodes. These findings suggest that GITM is more effective in detecting and isolating Sybil nodes in RPL-based IoT networks due to its enhanced trust assessment framework and energy-efficient design. GITM's trust assessment framework uses robust metrics to evaluate node behavior, including packet forwarding, MAC address changing rate, DIO message rate, the node's remaining energy, and current system time. By analyzing a wide range of trust metrics, GITM provides a more comprehensive and accurate evaluation of node trustworthiness, resulting in higher detection rates than GINI-1 and GINI-2.

2) Energy Consumption

During a Sybil attack, network energy consumption significantly increases due to creating fake identities and false data. It is expected as the attack requires these actions to be taken. We compare the proposed GITM with two state-of-the-art techniques: 1) [29] referred to as GINI-1 and 2) [20] referred to as GINI-2. All the models are tested to determine their respective energy usage under the Sybil attack and its mitigation, as presented in Fig. 6. The models' detection costs are subdivided into computational and communication costs. The energy needed to send and receive messages is assessed regarding the number of sent and received packets (e.g., DIO and DIS messages). Computing costs are calculated by comparing the current observation window (OW) period's GINI impurity with the last observed time frame. However, the power usage of core activities, such as sending and receiving data via a wireless network interface card, may be overlooked, not the communication processes. The only way to determine how much energy is used is to count how many messages are sent and received. The energy usage of all methods grows as the number of Sybil assaults rises. In the event of an even greater Sybil assault, malicious nodes will broadcast more harmful DIS messages.

Consequently, as in the state-of-the-art, genuine nodes get additional DIS signals and broadcast more DIO messages, resulting in tremendous energy usage. However, GITM consumes less energy than GINI-1 and GINI-2 due to shifting calculations on the upper layer. Our model can assess, identify, and isolate possible Sybil attacks on the fog layer. Secondly, GITM does

this sooner than GINI-1 and GINI-2; the genuine nodes in our model will receive and respond to fewer control messages (e.g., DIO and DIS), resulting in less energy being used. The results show that when the simulation was run for 60 seconds with 30 malicious nodes, the energy consumption of GINI-1 was 0.0936mj, and for GINI-2, it is 0.1136. Furthermore, of proposed GITM is 0.0736mj. Based on the results, it is clear that GITM outperforms GINI-1 in reducing energy consumption. The energy-efficient GINI index-based trust assessment framework, i.e., GITM, accurately identifies Sybil nodes, allowing for targeted isolation and reduced energy consumption—the percentage differences between GITM and GINI-1 range from approximately 13.6% to 35.1%. GITM provides even more significant energy savings than GINI-2, with percentage differences ranging from approximately 23.4% to 56.7%. The proposed GITM algorithm combines advanced energy-efficient techniques and the GINI index to detect and isolate Sybil nodes, reducing energy consumption effectively.

3) End-To-End Delay

The end-to-end latency is the time between the start of packet transmission to a fog layer and its arrival at the DAG's node layer root. It is the total time a packet travels from its origin (i.e., the network node) to its final recipient (i.e., the fog node) through the network. The end-to-end delay result is shown in Fig. 7. On the x-axis is the number of nodes, and on the y-axis is the millisecond delay. The graph shows the average delay for the number of nodes. The study indicates that GITM consistently achieves lower end-to-end delay values than GINI-1 and GINI-2. It was observed across different numbers of nodes, where GITM demonstrated a reduced delay in message transmission and routing, resulting in faster communication between nodes. These results highlight the efficiency of the proposed algorithm in minimizing latency and improving overall network performance. Additionally, GITM maintains its efficiency and performs consistently well as the number of nodes increases, making it suitable for large-scale smart grid deployments.

GITM prioritizes reliable communication paths, reducing delays caused by unreliable or compromised nodes. By leveraging trust metrics and intelligent decision-making algorithms, GITM ensures that messages are routed through trusted nodes, minimizing the chances of delays caused by malicious or unreliable routing paths. In summary, the analysis of the end-to-end delay results confirms that GITM outperforms GINI-1 and GINI-2 in terms of reducing delay and improving overall network performance. It is attributed to its trust-based optimization, efficient routing decisions, and scalability, all of which enhance the reliability and responsiveness of RPL-based smart grid networks.

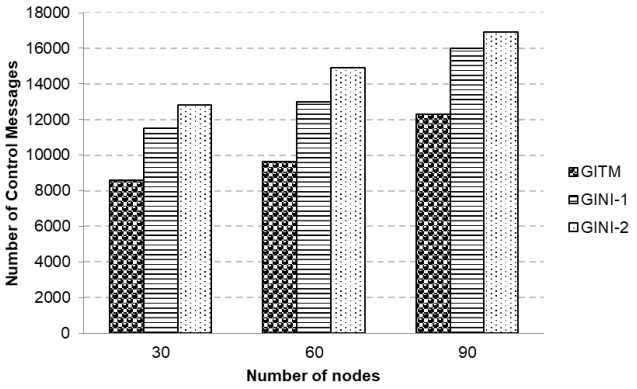


FIGURE 8. Number of control messages.

Moreover, since a layered mechanism has been introduced in the proposed mechanism, it results in slightly more delay than the GINI-1 and GINI-2 mechanism at the start of the simulation. When the Sybil nodes are detected and removed successfully, our mechanism performs better and shows less end-to-end delay afterwards. Trust calculation and propagation are done at the node layer in the base paper, contributing to a relatively lower delay. The average end-to-end delay in our case is a mere 0.30% (in milliseconds) more significant than the state-of-the-art concerning time.

4) Number of Control Messages

Numbers of control messages are exchanged between nodes and attackers during the simulation for topology discovery and other tasks. The following graph shows no control messages overhead under the Sybil attack. Different numbers of nodes are distributed during the simulation. The average value at a particular number of nodes is presented in the graph. Since the attackers were dispersed uniformly over the network in the state-of-the-art approach, the control message overhead grew in proportion to the number of attackers. As a consequence, a large number of legitimate nodes are compromised. Receiving the DIS Multicast through the GINI mechanism leads all nodes within the radio transmission range of the compromised node to reset its Trickle timers, disseminating numerous DIO signals from across the network.

When comparing the number of control messages exchanged, GITM consistently has lower values than GINI-1 and GINI-2. As the number of nodes increases from 30 to 60, there is a 12.21% reduction in control messages for GITM, and when the number of nodes increases from 60 to 90, there is a 27.42% reduction. Fig 8 shows that GITM is more effective at mitigating Sybil attacks in smart grids as the number of nodes increases. GINI-1 also shows improvement, with a 13.04% reduction in control messages between 30 and 60 nodes and a 23.08% reduction between 60 and 90 nodes. However, the percentage differences are

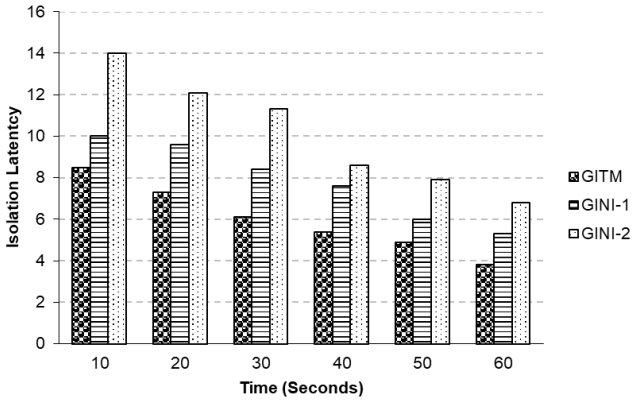


FIGURE 9. Isolation latency of Sybil attacks.

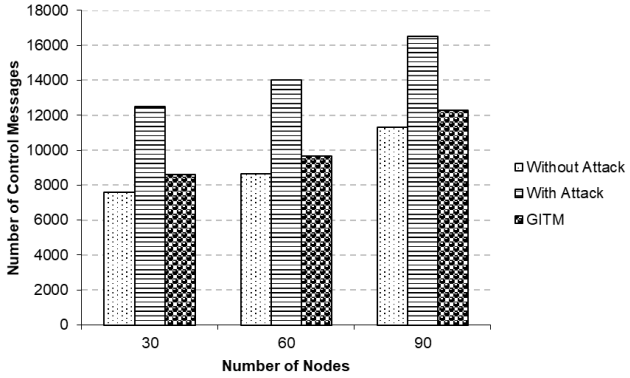


FIGURE 10. Number of control messages with GITM, with- and without Sybil attacks.

slightly lower than GITM. It suggests that GINI-1 is less efficient than GITM in minimizing control messages during Sybil attack mitigation. GINI-2 performs better than GINI-1, with a 16.41% reduction in control messages between 30 and 60 nodes and a 13.42% reduction between 60 and 90 nodes, but still falls short of GITM's performance. Based on the percentage differences and the lower-is-better principle, GITM is the most efficient at mitigating Sybil attacks in smart grids, consistently achieving the lowest number of control messages exchanged. While GINI-1 and GINI-2 show improvements, they are comparatively less efficient in minimizing control messages.

5) Isolation Latency

The attacking node must be isolated as soon as possible following detection. We only consider the isolation latency for the particular attacker nodes that our approach correctly identifies. Our suggested solution's isolation latency is much better because we apply the isolation at the parent selection phase. Fig. 9 shows the isolation latency while detecting the Sybil assault rate. It is the time taken for an isolated packet to be sent before the isolation latency is calculated. We achieved the lowest isolation latency rate using the proposed fog-based layered methodology. Detection of vast numbers of Sybil attacks may be done quickly. Hence, an isolated packet is broadcast early when the number of identified assaults exceeds an extent value. Because the GINI-1 has a lower detection rate, it has a longer isolation delay than the model under consideration. Some Sybil attacks cannot be detected by it. It results in a prolonged isolation delay since the detected Sybil attacks take longer to meet the threshold value for broadcasting isolated packets.

The GITM algorithm consistently demonstrates significantly better isolation latencies than the state-of-the-art GINI-1 and GINI-2 methods. The percentage differences for GINI-1 are from 15 to 29%, while it is much higher in the case of GINI-2, 39 to 46% low in our case. It indicates that GITM is a more efficient and effective approach for detecting and isolating Sybil nodes. The larger percentage differences show that GITM has a clear performance advantage in reducing the time needed for isolating Sybil nodes. These results highlight the superior Sybil detection capabilities of GITM and its ability to promptly identify and isolate Sybil nodes in the network, which is crucial for preventing the spread of malicious activities and maintaining the integrity of the smart grid system. GITM's innovative trust assessment framework contributes to its improved performance in accurately and efficiently detecting Sybil attacks. The results suggest that GITM can be a valuable solution for enhancing the security and reliability of RPL-based smart grid networks. The reduced isolation latencies achieved by GITM contribute to minimizing the potential damage caused by Sybil attacks, thereby improving the overall system performance. The improved efficiency and effectiveness of GITM in isolating Sybil nodes can lead to faster response times, allowing network administrators to take appropriate actions promptly and mitigate the impact of attacks more effectively.

6) Control Messages with GITM, with and without Sybil Attack

The GITM framework aims to reduce control message overhead, primarily when an attack occurs. This framework is designed to optimize control message transmission and improve network efficiency in the case of a Sybil attack. Figure 10 illustrates the control message overhead reduction. A detailed comparison with the "With- and without Attack" scenario is as follows:

a) Scenario 1 (30 nodes): In the GITM scenario, there is a difference of 900 in the control message overhead compared to the scenario without any attack. However, the control message overhead is 3900 less than the "With Attack" scenario, which is significantly less.

b) Scenario 2 (60 nodes): In the GITM scenario, the control message difference is a mere 1850 compared to the scenario without an attack. Whereas the control message overhead is reduced by 4350 compared to the scenario with an attack.
c) Scenario 3 (90 nodes): In the GITM scenario, the control message overhead is 1000 more than the scenario without an attack. In contrast, the amount of control message overhead is 4200 less than in the "With Attack" scenario. This improvement has allowed us to enhance the efficiency of the network and optimize its resources.

When it comes to control message overhead, the GITM approach performs better by reducing messages significantly. The difference in control message overhead between GITM and the "Without Attack" scenario is around 13% to 27%, and between GITM and the "With Attack" scenario, it is around 27% to 41%. It shows that the GITM approach efficiently minimizes control message overhead under Sybil attack and optimizes network resources. It shows that the GITM effectively addresses challenges posed by Sybil attacks in the smart grid network. This approach helps reduce energy consumption, minimize control message overhead, and improve the network's efficiency and performance. The percentage differences indicate significant improvements brought about by the GITM, which confirms its effectiveness in ensuring the secure and efficient operation of the smart grid infrastructure. The observed results are in line with the basic principles and mechanisms of the GITM approach.

7) Energy Consumption with GITM, with and without Sybil Attack

Figure 11 compares the energy overhead with and without Sybil attack and with Sybil and GITM in action. The percentage differences represent the relative increase in energy consumption in the GITM scenario compared to the energy consumption without attack ranging from approximately 10.84% to 34.35%. The highest percentage difference occurs at 30 nodes, indicating a relatively higher increase in energy consumption compared to the "Without Attack" scenario. The lowest percentage difference occurs at 60 nodes, indicating a relatively lower increase in energy consumption compared to the "Without Attack" scenario. Overall, the percentage differences highlight the additional energy consumption introduced by the trust-based approach in the GITM scenario. While there is an increase in energy consumption, it is crucial to consider the trade-off between energy consumption and the enhanced security provided by Sybil attack detection and mitigation. The GITM framework aims to strike a balance between energy efficiency and security, ensuring that the increase in energy consumption is justifiable in preventing significant energy wastage caused by malicious attacks.

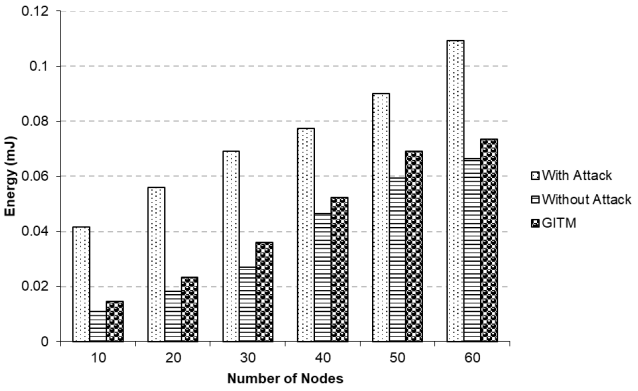


FIGURE 11. Energy consumption with GITM, with- and without Sybil attacks.

The proposed GITM framework has proven effective in reducing energy consumption in the presence of Sybil attacks. By isolating and detecting the Sybil nodes, the framework prevents unnecessary energy consumption caused by malicious nodes. The percentage differences range from approximately 23.18% to 65.66%, indicating the relative decrease in energy consumption achieved by the GITM framework compared to energy consumption with the Sybil attack present. The highest percentage difference is at 10 nodes, indicating a significant energy consumption reduction. The lowest percentage difference is at 50 nodes, indicating a minor reduction compared to other scenarios. The larger the percentage difference, the more significant the energy savings achieved by the GITM framework. The following points may be considered while analyzing the figure in detail:

According to the study, the GITM method successfully detects and minimizes Sybil attacks in RPL-based smart grid networks. Trust evaluation using the GINI Index helps identify and isolate Sybil nodes, resulting in lower energy consumption and message overhead. The approach is consistent with trust-based filtering, energy efficiency, and scalability principles, making it a viable solution for boosting the security and efficiency of smart grid infrastructures.

1) Energy Consumption with Sybil Attack: Energy consumption increases significantly during a Sybil attack. It is expected, as the attack involves the creation of fake identities, generating false data, or resending packets (in case of packet loss), leading to additional energy usage in the network.
2) Energy Consumption without Attack: In the absence of an attack, the energy consumption is relatively lower compared to the scenario with a Sybil attack. It indicates that the network operates more efficiently when no malicious activities affect the nodes.
3) Energy Consumption with GITM: The proposed GITM approach shows improved energy consumption

compared to the scenario with a Sybil attack. The energy consumption with GITM is closer to the energy consumption without an attack, indicating that the trust assessment framework effectively detects and mitigates the Sybil attacks, reducing their impact on energy consumption.

Based on these comparisons, it is evident that energy consumption is significantly higher in the presence of a Sybil attack. However, the proposed GITM approach reduces energy consumption by detecting and isolating Sybil attacks. By leveraging the GINI Index-based trust assessment framework, the proposed approach enables more efficient utilization of network resources, resulting in lower energy consumption.

VII. DISCUSSION

Regarding energy consumption, memory usage, and message overhead, using a fog layer for trust-related computations in resource-constrained nodes has several advantages. Firstly, by offloading trust computations to the fog layer, the underlying nodes can conserve their limited energy resources, allowing them to focus on their primary tasks, such as data sensing, processing, and transmission. It can significantly extend the nodes' lifetime, reducing the need for frequent maintenance and replacement. Secondly, using a fog layer can reduce the memory usage of the underlying nodes. Large amounts of data, such as trust scores, reputation values, and past behavior history, are frequently required for trust-related computations. Underlying nodes can reduce their memory footprint and avoid congestion by performing these computations in the fog layer. Finally, the proposed technique can reduce network message overhead. When a Sybil attack is detected and isolated, the subordinate nodes are no longer required to resend the same packets due to packet loss or corruption caused by the malicious nodes. It can significantly reduce the number of network messages sent, resulting in more efficient use of network resources. As a result, the proposed technique could be a viable option for trust management in resource-constrained IoT networks. The underlying nodes can save energy, reduce memory usage, and avoid message overhead caused by Sybil attacks by offloading trust computations to the fog layer. Here are some significant reasons for the obtained results:

1) Energy Consumption Reduction: The GITM uses the GINI Index to identify and isolate Sybil nodes precisely. It reduces the amount of communication and energy used in the network. As a result, Sybil attacks are detected and prevented efficiently, resulting in lower energy consumption than other methods.
2) Control Message Overhead Reduction: A Sybil attack can cause an increase in message traffic, leading to extra strain on the routing process. However, the GITM approach can detect and isolate Sybil nodes, preventing the need for additional messages. It allows for more efficient use of network resources and reduces overhead. The GITM method employs trust-based filtering using the GINI Index to evaluate node reliability. Nodes exhibiting malicious or untrustworthy behavior are eliminated, and trust scores are assigned based on node behavior. This process ensures that only dependable nodes participate in data forwarding, resulting in highly secure and reliable network communication.
3) Scalability: The GITM approach has been proven effective across different network sizes. Sybil attacks can significantly impact larger networks, causing more energy consumption and control message overhead. Despite this, the GITM approach remains scalable and consistently performs better than other approaches in reducing energy consumption and control message overhead. This scalability is crucial for smart grid deployments in the real world, where networks can vary greatly in size.

Now we discuss the technical aspects of the contributions, highlighting how they can reduce energy consumption in smart grid networks through GITM, as follows:

1) Layered-based Architecture: The paper introduces a novel layered-based architecture that provides a structured approach to analyzing nodes' behavior in RPL-based smart grid networks. This architecture organizes the network into distinct layers, making monitoring and assessing individual nodes' behavior easier, detecting potential attacks like Sybil attacks, and identifying anomalies.
2) Efficient Resource Usage: The proposed framework offers a notable advantage in terms of efficiency in memory, computation, and message overhead expenses at the node level. Traditional security mechanisms for Sybil detection often require significant computational resources and communication overhead, which can lead to increased energy consumption. However, the proposed framework minimizes these expenses, ensuring that energy consumption remains optimized while maintaining high security.
3) Role of Fog Computing: Fog computing is vital in optimizing energy consumption in smart grid networks. By leveraging fog computing resources, specific tasks, and computations can be offloaded from resource-constrained nodes to nearby fog nodes or edge devices. This approach reduces the energy burden on individual nodes, allowing them to operate more efficiently and conserve energy. Integrating fog computing within the layered-based architecture and the trust assessment framework can reduce energy consumption in RPL-based smart grid networks.

Overall, the technical analysis highlights the significance of the layered architecture, the GINI Index-based trust assessment framework, and the role of fog computing in achieving energy-efficient operations in smart grid networks. The proposed approach offers a promising solution for

enhancing smart grid infrastructures' security and energy efficiency by detecting and isolating Sybil attacks while minimizing resource overhead.

In a nutshell, the proposed model has shown better results than the state-of-the-art [29]. The proposed model outperforms all parameters. Regarding the attack detection rate, the proposed model detects the attacker nodes quickly and more efficiently than the GINI-based technique. When we talk about energy consumption, our mechanism consumes much lower energy, and the residual energy of nodes remains high. While in the GINI-based mechanism [29], the node's life fell rapidly. Isolation latency is lower in our model case.

Sybil attack detection is efficient due to diverse parameters. These parameters gave the perfect image of the attacker node and facilitated the proposed mechanism in detection. The primary reason behind the lower energy consumption is the layered architecture. All tasks are divided into layers. The upper layer now handles trust calculation and all complex tasks; it is not part of the node layer. In the case of the GINI-based process, the node's life is quickly removed. Isolation latency is lower in our model scenario. It can be shown that the suggested approach has a lower control message overhead. Control messages are those messages that are routed in the network for different tasks, such as the gathering of parameters for trust evaluation. Regarding all these characteristics, the proposed model improves the GINI-based approach.

VIII. CONCLUSION

The RPL protocol is widely regarded as the industry standard for SG routing. Regarding external assaults, this protocol has a powerful defense mechanism but is susceptible to internal attacks. The objectives of this work were to enhance SG security using RPL. Sybil attack is one of the most challenging internal attacks. This study detected and handled it using a Gini index solution promoting trust-based security. Using a layered system, the proposed framework includes layers of devices and fog. In this model, the processing is separated from nodes, enhancing the security and energy of the whole network. This framework detected Sybil attacks accurately and efficiently, as depicted in extensive simulation results. Furthermore, this strategy significantly improves detection rate, latency, and energy consumption, making it an effective tool against such attacks.

In the future, we aim to create a testbed for the proposed technique. We will also install a real network comprising Telos B nodes. This testbed will work in an interior setting to test the full capability of the suggested countermeasure, since radio reception and network characteristics may not be readily reproduced using simulations. In addition, we would identify and isolate Sybil and other internal attacks using different machine learning models.

REFERENCES

[1] Z. Chen, A. M. Amani, X. Yu, and M. Jalili, "Control and optimisation of power grids using smart meter data: A review," *Sensors*, vol. 23, no. 4, p. 2118, Feb. 2023.

[2] F. Salahdine, T. Han, and N. Zhang, "Security in 5G and beyond recent advances and future challenges," *Secur. Privacy*, vol. 6, no. 1, p. e271, Jan. 2023.

[3] T. U. Hassan, M. Asim, T. Baker, J. Hassan, and N. Tariq, "CTrust-RPL: A control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based Internet of Things applications," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 3, p. e4224, 2021.

[4] U. Farooq, M. Asim, N. Tariq, T. Baker, and A. I. Awad, "Multi-mobile agent trust framework for mitigating internal attacks and augmenting RPL security," *Sensors*, vol. 22, no. 12, p. 4539, Jun. 2022.

[5] T. Mazhar, H. M. Irfan, S. Khan, I. Haq, I. Ullah, M. Iqbal, and H. Hamam, "Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods," *Future Internet*, vol. 15, no. 2, p. 83, Feb. 2023.

[6] S. P. Senthilkumar and B. Subramani, "RPL protocol load balancing schemes in low-power and Lossy networks," *Networks*, vol. 8, pp. 1–8, Feb. 2023.

[7] A. Jahangeer, S. U. Bazai, S. Aslam, S. Marjan, M. Anas, and S. H. Hashemi, "A review on the security of IoT networks: From network layer's perspective," *IEEE Access*, early access, Feb. 16, 2023, doi: 10.1109/ACCESS.2023.3246180.

[8] N. Tariq, M. Asim, and F. A. Khan, "Securing SCADA-based critical infrastructures: Challenges and open issues," *Proc. Comput. Sci.*, vol. 155, pp. 612–617, Jan. 2019.

[9] A. Lahbib, K. Toumi, S. Elleuch, A. Laouiti, and S. Martin, "Link reliable and trust aware RPL routing protocol for Internet of Things," in *Proc. IEEE 16th Int. Symp. Netw. Comput. Appl. (NCA)*, Oct. 2017, pp. 1–5.

[10] U. Rahamathullah and E. Karthikeyan, "A lightweight trust-based system to ensure security on the Internet of Battlefield Things (IoBT) environment," *Int. J. Syst. Assurance Eng. Manage.*, vol. 12, pp. 1–13, Sep. 2021.

[11] R. Sahay, G. Geethakumari, and B. Mitra, "Mitigating the worst parent attack in RPL based Internet of Things," *Cluster Comput.*, vol. 25, no. 2, pp. 1303–1320, Apr. 2022.

[12] N. Tariq, M. Asim, F. A. Khan, T. Baker, U. Khalid, and A. Derhab, "A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in Internet of Things," *Sensors*, vol. 21, no. 1, p. 23, Dec. 2020.

[13] F. A. Khan and A. Gumaei, "A comparative study of machine learning classifiers for network intrusion detection," in *Proc. Artif. Intell. Secur., 5th Int. Conf. (ICAIS)*. New York, NY, USA: Springer, 2019, pp. 75–86.

[14] N. Tariq, M. Asim, Z. Maamar, M. Z. Farooqi, N. Faci, and T. Baker, "A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered IoT," *J. Parallel Distrib. Comput.*, vol. 134, pp. 198–206, Dec. 2019.

[15] J. Al Muhtadi, R. A. Alamri, F. A. Khan, and K. Saleem, "Subjective logic-based trust model for fog computing," *Comput. Commun.*, vol. 178, pp. 221–233, Oct. 2021.

[16] D. Arshad, M. Asim, N. Tariq, T. Baker, H. Tawfik, and D. Al-Jumeily OBE, "THC-RPL: A lightweight trust-enabled routing in RPL-based IoT networks against Sybil attack," *PLoS ONE*, vol. 17, no. 7, Jul. 2022, Art. no. e0271277.

[17] Z. A. Khan, J. Ullrich, A. G. Voyiatzis, and P. Herrmann, "A trust-based resilient routing mechanism for the Internet of Things," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, Aug. 2017, pp. 1–6.

[18] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things," *Future Gener. Comput. Syst.*, vol. 93, pp. 860–876, Apr. 2019.

[19] S. Y. Hashemi and F. S. Aliee, "Dynamic and comprehensive trust model for IoT and its integration into RPL," *J. Supercomput.*, vol. 75, no. 7, pp. 3555–3584, Jul. 2019.

[20] C. Pu, "Sybil attack in RPL-based Internet of Things: Analysis and defenses," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4937–4949, Jun. 2020.

[21] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, "New trust metric for the RPL routing protocol," in *Proc. 8th Int. Conf. Inf. Commun. Syst. (ICICS)*, Apr. 2017, pp. 328–335.

[22] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, "Trust-aware and cooperative routing protocol for IoT security," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102467.
[23] D. Airehrour, J. Gutierrez, and S. K. Ray, "A testbed implementation of a trust-aware RPL routing protocol," in *Proc. 27th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2017, pp. 1–6.
[24] N. Bhalaji, K. Hariharasudan, and K. Aashika, "A trust based mechanism to combat blackhole attack in RPL protocol," in *Proc. Int. Conf. Intell. Comput. Commun. Technol.* Singapore: Springer, 2019, pp. 457–464.
[25] J. Jiang, Y. Liu, and B. Dezfouli, "A root-based defense mechanism against RPL blackhole attacks in Internet of Things networks," in *Proc. Asia–Pacific Signal Inf. Process. Assoc. Annu. Summit Conf. (APSIPA ASC)*, Nov. 2018, pp. 1194–1199.
[26] P. Kaliyar, W. B. Jaballah, M. Conti, and C. Lal, "LiDL: Localization with early detection of Sybil and wormhole attacks in IoT networks," *Comput. Secur.*, vol. 94, Jul. 2020, Art. no. 101849.
[27] Z. A. Almusaylim, N. Z. Jhanjhi, and A. Alhumam, "Detection and mitigation of RPL rank and version number attacks in smart Internet of Things: SRPL-RP," *Sensors*, vol. 20, p. 5997, Oct. 2020.
[28] R. Mehta and M. M. Parmar, "Trust based mechanism for securing IoT routing protocol RPL against Wormhole & Grayhole attacks," in *Proc. 3rd Int. Conf. Converg. Technol. (I2CT)*, Apr. 2018, pp. 1–6.
[29] B. Groves and C. Pu, "A Gini index-based countermeasure against Sybil attack in the Internet of Things," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2019, pp. 1–6.
[30] J. Liu, X. Sun, W. Hu, and Z. Jin, "Detecting forwarding misbehavior in RPL-based IoT networks using Bayesian networks," in *Proc. 16th IEEE Annu. Consum. Commun., Netw. Conf. (CCNC)*, Jun. 2019, pp. 1–6.
[31] S. Liu, Y. Li, J. Hu, R. Lu, X. Shen, Y. Zhang, and P. Zeng, "Anomaly detection and defense for IoT-based distributed cyber-physical system: A deep *Q*-learning approach," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5107–5117, Oct. 2020.
[32] K. Saleem, N. Javaid, Z. Iqbal, M. U. Khan, N. Alrajeh, and M. Guizani, "Beta reputation based trust management scheme for wireless sensor networks in IoT," *Wireless Pers. Commun.*, vol. 113, no. 4, pp. 2021–2038, 2020.
[33] S. Kumar, "Fuzzy-based trust management in RPL-based Internet of Things against selective forwarding attack," *J. Ambient Intell. Hum. Comput.*, vol. 12, no. 12, pp. 5167–5180, 2021.
[34] Y. Wang, P. Jiang, H. Guo, and J. Liu, "A deep Q-network based intelligent security framework for the Internet of Things," in *Proc. IEEE Int. Conf. Comput., Netw. Commun. (ICNC)*, Sep. 2021, pp. 39–43.
[35] A. Rajabi, S. Zolfaghari, and M. Sargolzaei, "An adaptive trust management scheme in RPL-based Internet of Things," *J. Ambient Intell. Hum. Comput.*, vol. 9, no. 1, pp. 155–169, 2018.
[36] D. Airehrour, J. Gutierrez, and S. K. Ray, "Securing RPL routing protocol from blackhole attacks using a trust-based mechanism," in *Proc. 26th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Dec. 2016, pp. 115–120.
[37] M. N. Nafees, N. Saxena, A. Cardenas, S. Grijalva, and P. Burnap, "Smart grid cyber-physical situational awareness of complex operational technology attacks: A review," *ACM Comput. Surv.*, vol. 55, no. 10, pp. 1–36, Oct. 2023.
[38] A. I. Awad, M. Shokry, A. A. M. Khalaf, and M. K. Abd-Ellah, "Assessment of potential security risks in advanced metering infrastructure using the OCTAVE Allegro approach," *Comput. Electr. Eng.*, vol. 108, May 2023, Art. no. 108667.
[39] H. A. Muqeet, R. Liaqat, M. Jamil, and A. A. Khan, "A state-of-the-art review of smart energy systems and their management in a smart grid environment," *Energies*, vol. 16, no. 1, p. 472, Jan. 2023.
[40] P. Faria and Z. Vale, *Demand Response in Smart Grids*. vol. 16, no. 2. Basel, Switzerland: MDPI, 2023, p. 863.
[41] M. Deihimi, N. Rezaei, M. Gholami, and H. Tarimoradi, "Advanced energy storage system in smart grids: Power quality and reliability," in *Emerging Trends in Energy Storage Systems and Industrial Applications*. Amsterdam, The Netherlands: Elsevier, 2023, pp. 409–439.
[42] M. Jafari, A. Kavousi-Fard, T. Chen, and M. Karimi, "A review on digital twin technology in smart grid, transportation system and smart city: Challenges and future," *IEEE Access*, vol. 11, pp. 17471–17484, 2023.
[43] E. Iasiello and P. Sector, "China's three warfares strategy mitigates fallout from cyber espionage activities," *J. Strategic Secur.*, vol. 9, no. 2, pp. 47–71, Jun. 2016.
[44] T. Plėta, M. Tvaronavičiene, S. D. Casa, and K. Agafonov, "Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases," *Insights Into Regional Develop.*, vol. 2, no. 3, pp. 703–715, Sep. 2020.
[45] J. E. Sullivan and D. Kamensky, "How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid," *Electr. J.*, vol. 30, no. 3, pp. 30–35, Apr. 2017.
[46] S. Lawson and M. K. Middleton, "Cyber pearl harbor: Analogy, fear, and the framing of cyber security threats in the United States 1991–2016," *First Monday*, vol. 24, no. 3, Mar. 2019.
[47] E. Ehiorobo, S. Pournouri, S. J. Ghazaani, and J. M. Toms, "Profiling cyber attackers by classification techniques; A case study on Russian hackers," in *Cybersecurity in the Age of Smart Societies*. London, U.K.: Springer, Sep. 2022, pp. 171–201.
[48] C. Anderson, "How cybersecurity regulation for the smart grid could upset the current balance of federal and state jurisdiction in electricity regulation," *Amer. Univ. Nat. Secur. Law Brief*, vol. 8, no. 1, p. 43, 2018.
[49] M. Lehto, "Cyber-attacks against critical infrastructure," in *Cyber Security: Critical Infrastructure Protection*. Switzerland: Springer, 2022, pp. 3–42.
[50] S. Slaughter, "Cybersecurity considerations impacting the us critical infrastructure: An overview," American Counterterrorism Targeting Resilience Institute (ACTRI), Washington, DC, USA, Tech. Rep. 2022.
[51] S. Corbet and J. W. Goodell, "The reputational contagion effects of ransomware attacks," *Finance Res. Lett.*, vol. 47, Jun. 2022, Art. no. 102715.
[52] R. Shandler and M. A. Gomez, "The hidden threat of cyber-attacks–undermining public confidence in government," *J. Inf. Technol., Politics*, vol. 19, pp. 1–16, Aug. 2022.
[53] C. Pu, J. Brown, and L. Carpenter, "A Theil index-based countermeasure against advanced vampire attack in Internet of Things," in *Proc. IEEE 21st Int. Conf. High Perform. Switching Routing (HPSR)*, May 2020, pp. 1–6.
[54] C. Pu, "Sybil attack in RPL-based Internet of Things: Analysis and defenses," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4937–4949, Jun. 2020.

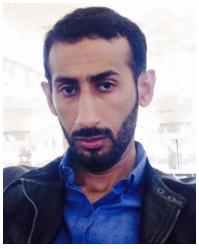
MUHAMMAD HASSAN received the master's degree in computer science from the Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan. He is currently pursuing the Ph.D. degree in information security from the Department of Avionics Engineering and Information Security, Air University, Islamabad. His research interests include RPL security, trust-based security, machine learning, and information and network security.

NOSHINA TARIQ received the M.S. and Ph.D. degrees in computer science from the FAST National University of Computer and Emerging Sciences, Islamabad, Pakistan. She is currently an Assistant Professor with the Department of Avionics Engineering and Information Security, Air University, Islamabad. She is also an accomplished researcher in computer science and cybersecurity. She is serving as a peer reviewer for many high-repute research journals. With her passion for research and dedication to the field, she is poised to contribute further to advancing cybersecurity and computer science. Her research interests include various aspects of cybersecurity, such as network security, the Internet of Things (IoT), wireless sensor networks (WSN), fog and cloud computing, blockchain, and artificial intelligence. She is an active research community member.

AMJAD ALSIRHANI received the bachelor's degree in computer sciences from Jouf University, Saudi Arabia, in 2009, and the M.C.A. and Ph.D. degrees from Dalhousie University, in 2014 and 2019, respectively. He is currently an Assistant Professor with the Faculty of Computer Science, Jouf University, where he is also the Head of the Department of Software Engineering. He is an Adjunct Professor with Dalhousie University, Halifax, Canada. His research interest includes computer security, with a specific emphasis on cybersecurity, network security, and cloud computing security. He has also conducted research in the areas of distributed computing systems, and machine and deep learning. His contributions to these areas have been published in various peer-reviewed journals and conference proceedings, highlighting his expertise and dedication to advancing knowledge in these fields.

ABDULLAH ALOMARI (Member, IEEE) received the bachelor's degree in computer science from Umm Al-Qura University, Saudi Arabia, in 2008, and the M.Sc. and Ph.D. degrees in engineering mathematics and internetworking from Dalhousie University, Halifax, Canada, in 2012 and 2018, respectively. He is currently an Associate Professor of networks and information security with the Department of Computer Science, Al-Baha University, Saudi Arabia. His research interests include cybersecurity, the IoT, and emergent technologies in communication networks. He is a member of the IEEE Communication Society and ACM.

FARRUKH ASLAM KHAN (Senior Member, IEEE) received the M.S. degree in computer system engineering from the Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Pakistan, in 2003, and the Ph.D. degree in computer engineering from Jeju National University, South Korea, in 2007. He also received professional training from the Massachusetts Institute of Technology, New York University, IBM, and other professional institutions. He is currently a Professor of cybersecurity with the Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia. He has more than 130 publications in refereed international journals and conferences. He has co-organized several international conferences and workshops. He has successfully supervised/co-supervised six Ph.D. students and more than 20 M.S. thesis students. Several M.S. and Ph.D. students are currently working under his supervision. His research interests include cybersecurity, body sensor networks and e-health, bio-inspired and evolutionary computation, smart grid, and the Internet of Things. He is a fellow of the British Computer Society (BCS). His name has been listed in the World's Top 2% Scientists in a study conducted by Stanford University, in 2022. He is on the panel of reviewers of more than 40 reputed international journals and numerous international conferences. He serves/served as an Associate Editor for prestigious international journals, including IEEE Access, *PLOS ONE*, *Neurocomputing* (Elsevier), *Ad Hoc and Sensor Wireless Networks*, *KSII Transactions on Internet and Information Systems*, *Human-Centric Computing and Information Sciences* (Springer), *PeerJ Computer Science*, and *Complex and Intelligent Systems* (Springer).



MOHAMMED MUJIB ALSHAHRANI received the B.Sc. degree (Hons.) in computer science from King Khalid University, Abha, Saudi Arabia, the M.Eng. degree (Hons.) in internetworking from Dalhousie University, Halifax, Canada, and the Ph.D. degree (Hons.) in the IoT cybersecurity from the University of Victoria, Victoria, Canada. He is currently an Assistant Professor with the Department of Information Systems, University of Bisha. His research interests include the IoT security, network security, digital forensics, biometrics security, data privacy, blockchain, AI in cybersecurity, and cybersecurity education.

MUHAMMAD ASHRAF received the bachelor's degree in avionics engineering and the M.S. degree in information security from the College of Aeronautical Engineering, National University of Sciences and Technology (NUST), Risalpur, Pakistan, and the Ph.D. degree in cryptography from Middle East Technical University, Ankara, Turkey, in 2013. He is currently the Chair of the Department of Avionics Engineering, Air University, Islamabad. He is also the General Director of the Institute of Avionics and Aeronautics, Air University. His research interests include public key cryptography, efficient computation over finite fields, stream ciphers, elliptic cure-based cryptography, random number generation, and information security.

MAMOONA HUMAYUN received the Ph.D. degree in computer sciences from the Harbin Institute of Technology, China. She has 15 years of teaching and administrative experience internationally. She has an extensive teaching, research supervision, and administrative work background. She has authored several research papers, supervised many postgraduate students, and has an external thesis examiner to her credit. She has strong analytical, problem-solving, interpersonal, and communication skills. Her research interests include cyber security, wireless sensor networks (WSN), the Internet of Things (IoT), requirement engineering, global software development, and knowledge management. She is the guest editor and a reviewer for several reputable journals and conferences around the globe.