International Journal of Safety and Security Engineering
Vol. 13, No. 1, February, 2023, pp. 69-79
Journal homepage: http://iieta.org/journals/ijsse

Analysis on Secured Cryptography Models with Robust Authentication and Routing Models in Smart Grid

Chadalavada Naga Priyanka*, Nandhakumar Ramachandran

School of Computer Science and Engineering, VIT-AP University, G-30, Inavolu, Beside AP Secretariat Amaravati, Andhra Pradesh 522237, India

Corresponding Author Email: nandhakumarr03@gmail.com

https://doi.org/10.18280/ijsse.130108

Received: 15 December 2022
Accepted: 17 January 2023

Keywords:
smart grid, network, quality of service, routing, cryptography, attack detection

ABSTRACT

Power Grid improvements over the last few decades have led to an enormous growth in both the economic and social aspects of the industry. Another thing to consider is that the layout of the electrical system has remained mostly unchanged. The "smart grid" was created to remedy the current grid's weaknesses. Existing electrical power grids could become smarter in the future if communication and networking capabilities were integrated into them. A significant number of embedded appliances are often coupled via communication methods in a smart grid, therefore the network must be accessible, reliable, and effective. Price signals are used by the smart grid to regulate electricity use. The ability of power producers and consumers to talk to one another is crucial in a smart grid. Smart grid awards are at danger if the performance degrades in the form of delays or outages. The grid server gathers data from multiple smart grid devices in a system. These statistics are crucial for the distribution of energy and the maintenance of a healthy equilibrium between energy producers and consumers. A hacker might potentially disrupt or imbalance the flow of energy by tampering with these data as they go from smart grid gadgets to utility computers. As a result, an authentication model is required to ensure the integrity of devices and utility servers and to prevent tampering attacks. To achieve this goal, cryptography techniques are used for smart grid demand–response security. For smart grid communication systems, Quality-of-Service (QoS) techniques have been created that incorporate the derivation of QoS requirements as well as QoS routing in the communications network to meet the needs. The dynamics of the power grid and the price-load linkage are used to determine QoS needs. The impact of several QoS indicators, such as the delay, power usage, routing is investigated. To determine the quality of service (QoS), a routing optimization model that maximises revenue must be analysed. This paper presents a brief survey on cryptography models with robust authentication and routing models in smart grid.

1. INTRODUCTION

Power grids are used to distribute electricity across a large area. There are three components to a power grid: generation, transmission, and distribution [1]. There is a shortage of energy available to consumers in a traditional power system if supply and demand don't match up. Losses on power lines and a lack of information increase inefficient power management, which is made worse by the ageing grid's problems [2]. For example, the old grid maintains a constant flow of electricity both during and after peak demand. The regular grid has a number of limitations that must be overcome [3]. Electricity needs to be modernised in order to meet the needs of modern society [4]. There are hopes that a new smart grid would replace the existing one, giving better performance while being flexible enough to suit the upcoming industrial developments.

As the network expands in size and complexity, more and more options for intelligent grid communications become accessible. In recent years, the electric power communications system maintenance unit has paid increasing attention to quality-of-service assurance and service level enhancement due to the rapid growth of smart grid technologies [5]. With the help of analysis of connection business requirements, smart grid routing algorithm research will establish the foundation for improving smart grid safety and efficiency [6].

Due to 100ms transmission delay and high requirements, dispatching automation is frequently handled by deploying control centres to control grids [7]. Power systems security and stability are the fundamental goals of the security and stability control industry, which ensures the safety and stability of regional and superior power grids when power plants are shut down. Security and stability control Transmission time between the power station and the dispatch centre is typically under 30 milliseconds, and the error rate is below 10-8. In the grid's production planning and control sector [8], a few hundred milliseconds are the maximum transmission delay that can occur. The grid running control class has a higher need for information precision, even though the error rate is only 10-6.

Using a smart grid, real-time data collection is possible. Security, dependability and scaling are among the smart grid network's most critical aspects. The network handles all

aspects of data processing, data routing, and node monitoring. To maintain the safety of its members, it employs a variety of communication methods [9]. An advanced metering information management system, smart metres can communicate via this grid. To handle large amounts of data, a distributed network strategy is essential [10]. Smart grid electricity management strategy is centred on the needs of its customers. Among other things, Advanced Metering Infrastructure (AMI) gives information about consumer voltage data, customer outage data, periodic metre readings load control, and other pertinent data [11]. The topmost layer is called "Home Area Network (HAN)". Households that participate in pricing are referred to as "HANs" by the word. For AMI purposes, the smart metre will receive data from every home in the network [12].

Using multicast routing, data can be sent from a single source to several destinations at once. Traffic from a multicast source, such a live video conference, is sent in a single stream to the group. Computers, gadgets, and IP phones are all examples of receivers that make up the multicast group in a smart grid. Due to the fact that multicast allows for a single source of information to reach numerous recipients simultaneously in the grid, network traffic is drastically reduced [13]. It will always have place in networking since it is a great technique to distribute data to many servers at once.

Meters record the amount of energy consumers use and the amount of money they spend. When compared to traditional wired connections, wireless makes it simpler and less expensive to add and remove devices. The average HAN area ranges from 1 to 100 square metres. NAN stands for Neighborhood Area Network. NAN uses a network of smart metres and routers to transmit data. A group of HANs is required for AMI applications. The NAN system consists of the Centralized Control Unit (CCU), the Smart Meter Recording Unit (SMRU), and NAN IDs. For energy suppliers, the CCU acts as a conduit to connect with a wide range of HANs. Smart metres communicate with SMRUs, which are typically wireless nodes that maintain track of all the data from the metres [14]. The vast majority of the region covered by HAN falls within the range of 100m to 10km. The communication types in smart grid is shown in Figure 1.

Smart grids use communication channels to monitor local power usage and react automatically. There is a need for a renewable energy source, Smart Meter (SM), and smart home devices. The smart grid's two-way transmission medium allows consumers to interact with the grid [15]. The advantages of this technology over the traditional grid benefits everyone: customers, providers, and government organisations alike. Energy use is reduced while the cost of power to the user is reduced in a clever way. Power and data can move in both directions on the smart grid. Distributed energy resources like wind, solar, and others and storage devices allow any user to dynamically push or take electricity from the grid. This means that each grid node is unique in terms of the quantity of energy it generates and consumes [16]. The energy provided by nodes inside a local area may well be linked if they are exposed to the same weather conditions. a node that absorbs energy from the grid is referred to as an energy demand node [17]. Energy supply node is a node that returns surplus energy to the grid. Supply-nodes and demand-nodes can be used to balance the smart grid's energy supply and demand [18]. The Figure 2 represents the smart grid structure.

Smart grid refers to electric power transmission and distribution networks that incorporate Information and Communication Technology (ICT). A smart grid is required to accurately bill customers and efficiently manage and distribute electricity [19]. The Smart Meter is one of the most critical components of a smart grid. SM implementation raises concerns about metre tempering and consumer privacy [20]. There needs to be legislation in place to govern SMs. Confidentiality is ensured by a number of privacy-related properties such as secrecy, integrity, authenticity and availability [21]. If an opponent gets their hands on an SM, they can tamper with its data. Cryptographic keys can be easily obtained if the security module is compromised. A common vulnerability can be exploited by a large number of SMs to control real-time use. An access control system is required so that metre hacking may be avoided and saved data can be used for invoicing and other added value services [22].

Encryption and analysis of smart grid systems vulnerabilities help understand the weaknesses of attackers. It is possible to make decisions about cybersecurity monitoring and protection using a game theory method that uses interactions inside formalised incentive structures [23]. The coordination of cyberattacks can also boost security [24]. In order to maintain the current grid's dependability, energy sector groups are in charge of managing cybersecurity and vital power supply functions. It is also worth noting that intelligent optimization approaches such as genetic algorithms and neural networks have made the most important contributions to the electrical network's dependability [25], safety, and efficiency, as well as other techniques. There have been previous approaches used to study how formalised security organisations respond to the demands of the energy market. Current SG control and monitoring systems have made it possible to quickly identify critical infrastructure components.

The reliability of smart grids depends on the security, reliability, and availability of communication application systems. Information that can be used in the making of business choices is derived from a huge number of datasets processed by computers and networks [26]. Users can observe how the advancements in hardware, programming, networking, and database systems operate together to achieve a common goal using the big framework and architecture. As all devices communicate data via the Internet, the Internet Protocol (IP) is one of the most vulnerable parts of integrating ICTs into SG. As a result of its recognised flaws, this protocol is subject to intrusions and data tampering [27]. Despite this, there are numerous security flaws that need to be patched up. Consequently, data security and privacy are essential to the safety of the smart grid.

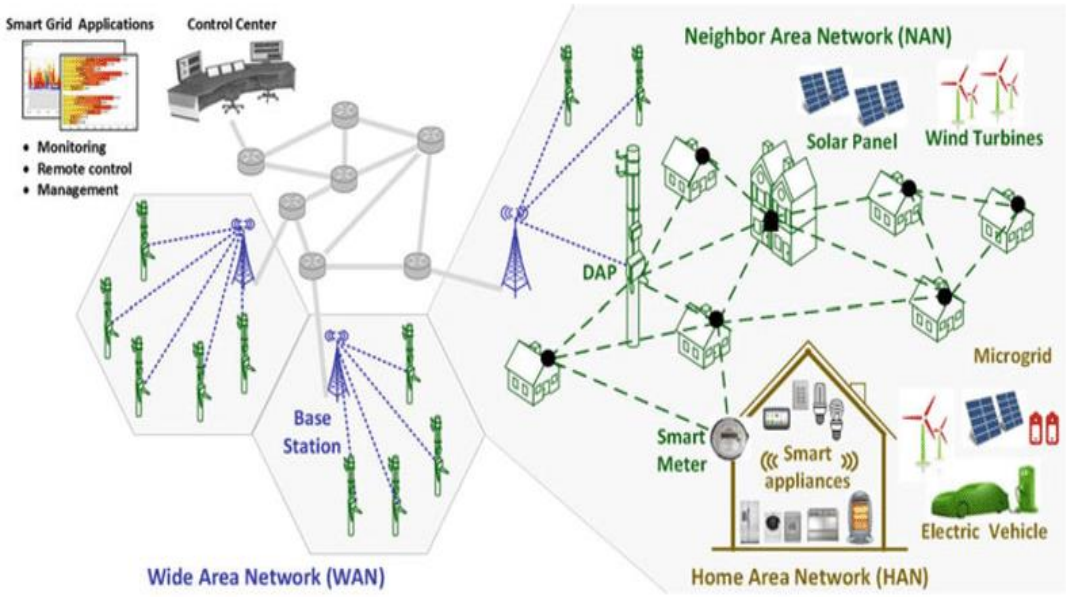

Figure 1. Communication types in smart grid [28]

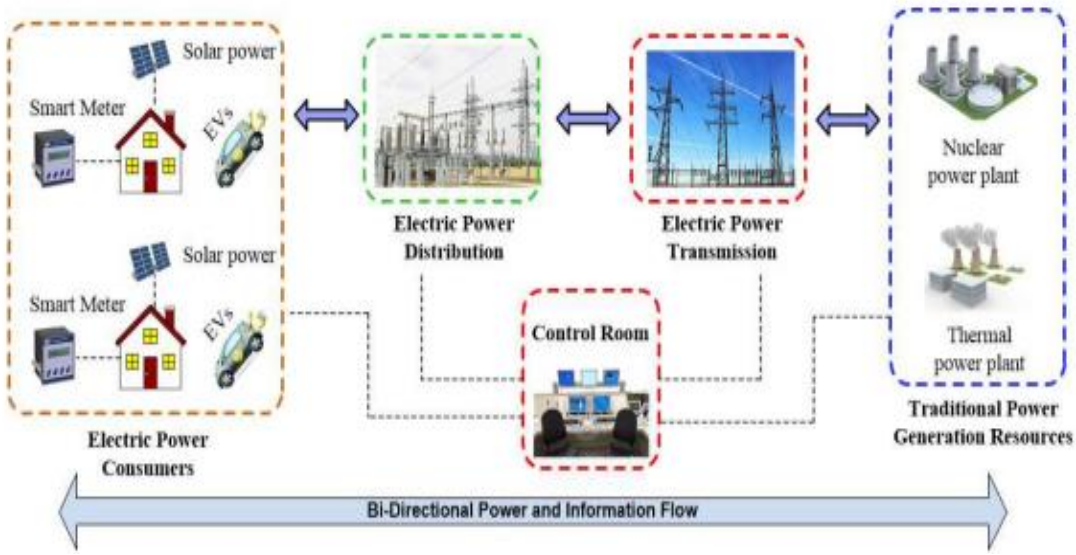

Figure 2. Structure of the smart grid [29]

In order to gather data from the power grid and disseminate control commands to the control devices, a sophisticated communication network is essential to the operation of a smart grid. Confidentiality of data transmitted via networks is a must for protecting the power grid. Symmetric cryptography relies on the exchange of secret keys between communicating parties; QKD protocols facilitate the generation and dissemination of these keys [28]. Information secrecy can be guaranteed even to an eavesdropper with unlimited resources when using QKD techniques in conjunction with symmetric cryptography, as this combination is known to be completely safe.

2. LITERATURE SURVEY

2.1 Routing models

Zhang and Leung [1] improved load flow routing and V2G scheduling for regulatory service delivery using a hierarchical system model is proposed. Firstly, the author introduced PFRs into the power system to formulate the problem of OPF routing at the grid level. Using the semidefinite programming (SDP) relaxation, the author turned the original NP-hard issue into a convex problem, which can be solved in linear time. Das and Bera [2] discussed the novel advancement of ZigBee-based tunable clustering scale-free neighbourhood area networking (TSFNAN) for establishing smart grid connectivity. Using the hop minimization feature of scale-free and customizable clustering techniques, the complexity of ZigBee-based multihop mesh networks between gateways and smart metres (SMs) is lowered.

Critical information should be routed to safe pathways in the event of smart grid cyber-physical coupling failures, which is expected [3]. Equality of information flow is a priority in power communication networks. Information flow is critical, but the value it provides depends on the current condition of the power system.

Author Name/s	Year of Publication	Proposed Model	Limitations
Zhang and Leung [1]	2022	Improved load flow routing and V2G planning for regulatory service delivery using a hierarchical system model is proposed. Firstly, the author introduced PFRs into the power system to address the problem of OPF routing at the grid level. Using the semidefinite programming (SDP) reduction, the author turned the original NP-hard issue into a convex problem, which can be solved in linear time.	The suggested model uses a set of criteria to determine the optimal path to take. Weak data transmission rates are observed in this model as a result of the chosen methods. When taking LAN into account, this paradigm places a significant computational burden on the system.
Das and Bera [2]	2023	The author discussed the novel advancement of ZigBee-based tunable clustering scale-free neighbourhood area networking (TSFNAN) for establishing smart grid connectivity. Using the hop minimization feature of scale-free and customizable clustering techniques, the complexity of ZigBee-based multihop mesh networks between gateway and smart metres (SMs) is lowered.	The model does not verify the nodes but instead assumes that all nodes are participating in the conversation. Threat actors have a high window of opportunity to compromise a network and reduce its efficiency.
Xuet et al. [3]	2019	The author proposed a model in which the information flow's cyber-physical sensitivity is assessed to determine its worth. The next step is to construct a CPS robust routing model (CPS-RRM) with a priority mechanism that accounts for cyber-physical disturbances. An altered version of the CCG method is utilised to solve the reformulated CPS-RRM utilising the Big-M technique.	The process of handling multiple attacks in the model is not satisfactory and the delay levels are high that reduces the system performance.
Velusamy and Pugalendhi [4]	2020	The author created a new way to evaluate trust in packet routing by automatically fine-tuning the rule set and memberships functions for the decision variable. Optimal rules and locations for membership models are calculated.	The model uses trust factor for node recognition and the process of calculating trust involves basic operations as it is easy for attacker to know the trust identities to insert malicious attacks.
Kong [5]	2020	A model was created to evaluate the risk of communication channel failure and to quantify the impact of this failure in terms of lost load. We devised an optimization approach to lessen the impact of an initial route failure. A NP-hard method is required to calculate how much power is being wasted. Dynamic programming is further transformed by using Bellman's optimality equation to solve	The model computational overhead is very high that degrades the system performance and the data transmission rate is also to be improved.

By analysing the information flow's cyber-physical sensitivity, the model presented by Xu et al. [3] can be used to calculate its value. A CPS-RRM (CPS-RRM) with a priority mechanism that takes into account cyber-physical disturbances is the next phase. For the Big-M solution of the reformulated CPS-RRM, an updated version of the CCG method is used instead of the standard one.

The dynamic nature of SGCNs makes it difficult to pinpoint the best way for reliably transmitting data. When trusted routing is used, no matter how logically constructed the rule set and membership function were in earlier fuzzy logic systems, they waste computational memory and reduce node energy efficiency. When Velusamy and Pugalendhi [4] used the water cycle algorithm (WCA), they developed an approach for automatically fine-tuning rule sets and membership functions for decision variables. WCA-based exploitation, evaporation, and rainfall can be used to discover the near-optimal rules and locations for membership functions. Network Simulator-2 is used to evaluate the SGCN routing algorithm in an experimental setup (NS2). The suggested model is put through its paces in three distinct scenarios, each with its own set of tests: Each can be evaluated on its own; the relationship between them can be evaluated separately; and the relationship between them can be evaluated as a whole.

A smart grid's power system and communications network are tightly intertwined. A malfunction in one network might have a domino effect on other networks, causing even more problems. A model was created by Kong [5] to evaluate the risk of communication channel failure and to quantify the impact of this failure in terms of lost load. We devised an optimization approach to lessen the impact of an initial route failure. A NP-hard method is required to calculate how much power is being wasted. Dynamic programming is further transformed by using Bellman's optimality equation to solve the problem. A Gauss-Seidel value iteration strategy, which the author offer, can be used to address the dynamic programming problem.

2.2 Security models

As the Smart Grid is created, the safety of the communication network must be considered. Hostile attacks can be conducted at any time since the wireless network is open and unpredictable. Using Bayesian inference and the Dempster-Shafer (D-S) theory, Velusamy et al. [6] created a new framework for measuring direct and indirect trust. The node's trustworthiness in the analytical hierarchy process is determined by cross-layer attributes such as rate of transmission, absorption rate, and signal strength (AHP). Fuzzy theory combines fairness when computing link trust and reliable routing using cross-layer metrics. To test the proposed fuzzy-based trust routing approach, extensive testing were carried out with malicious nodes.

The high cost of phase shift measurement equipment has made it a popular study topic for some time now. A system cannot be made visible solely by Phasor Measurement Unit (PMUs). An appropriate communication network has to be in place to transfer all PMU data [7]. In order to ensure full observability of a power system, Zhu et al. [7] proposed a model in which OPLP examines the appropriate placement of PMUs and communication links(CLs). Each CL's communication capability, as well as the locations of PMUs and CLs, is captured in the OPLP issue. This ensures that

PMU data is transmitted reliably and on time.

There is a direct link between a cyber-physical system and the electrical grid. Because of their dependence on interconnected systems, smart grids are at risk of failures piling on top of one another. Power grid failures could be caused by a breakdown in the communication network, and vice versa. Keeping an initial failure from spreading can stop a cascading network disaster.

Author Name/s	Year of Publication	Proposed Model	Limitations
Velusamyet et al. [6]	2020	The author used Bayesian inference and the Dempster-Shafer (D-S) theory to create a new framework for estimating direct and indirect trust. Cross-layer properties such as transmission rate, absorption rate, and signal strength are used to determine the node's trustworthiness in the analytical hierarchy process (AHP).	The routing process is effective but it does not concentrate on dynamic route selection if any issues occur with the route. Delay is high in rerouting process that need to be overcome.
Zhuet et al. [7]	2019	The author proposed a model in which OPLP examines the appropriate placement of PMUs and communication links(CLs). Each CL's communication capability, as well as the locations of PMUs and CLs, is captured in the OPLP issue.	The location finding process in this model is complex that increases the load on the system resulting in high delay.
Kong [8]	2019	The number of power-disjoint pathways can be used as a metric of rigidity. Reducing reliance between the electrical grid and communication networks is the model proposed. The author determined which power source powers which communication node and which communication line connects which power source to the control centre by using this type of relationship.	The process of communication is not secured as the model is vulnerable to attacks that impacts the network security levels.
Li et al. [9]	2020	The author describedSecGrid, an SGX-enabled smart grid system. Grid utilities employing the system can process confidential customer data swiftly and securely because of the usage of SGX-certified technology. Only the smart metres require AES encryption, with SecGrid's well-designed security procedures.	The model encryption model is effective but the key size considered is less that has less security with the attackers. The number of rounds can be still increased to improve the security level.
Zuo et al. [10]	2021	A decentralised decryption system based on ElGamal homomorphic cryptography is presented. It is also important to note that the proposed method does not rely on an authority that is not totally trustworthy in the real world.	The cryptography models used is efficient but the procedure of recognition of attacks is less thus resulting in degradation of model performance.

A sufficient number of electricity communication lines between power nodes as well as the control centre is required to accomplish this. The number of power-disjoint pathways can be used as a metric of rigidity. Reducing reliance between the electrical grid and communication networks is the model proposed by Kong [8] ensuring that systems are as resilient as possible. The author determined which power source powers which communication node and which communication line connects which power source to the control centre by using this type of relationship. To solve a Maxflow problem generated from this connection Menger's Theorem is applied.

The smart grid uses two-way communication and extensive features to promote sustainability and efficiency, but these features also raise serious privacy concerns for users. Individual privacy is protected in smart grid systems via cryptographic techniques like encryption algorithms, which can only provide limited and simple functionality. According to Menger's theorem, the size of a minimal cut set in a finite graph is equal to the greatest number of disconnected paths between any two vertices. In order to analyse the maximum flow problem, we assume that (1) all arc capacities are integers and (2) whenever the defined as the sharing arc I j), the network also has arc I j) (j, i). Since we permit arcs with zero capacity, the second possibility is lenient. Because of the limited resources of smart metres, these solutions need the use of complex asymmetric cryptography. Li et al. [9] describedSecGrid, an SGX-enabled smart grid system. Grid utilities employing the system can process confidential customer data swiftly and securely because of the usage of SGX-certified technology. Only the smart metres require AES encryption, with SecGrid's well-designed security procedures. To verify the models design's superiority, security analyses and experiments are conducted.

A key part of the smart grid is data aggregation that protects user privacy while simultaneously expanding the applications of data aggregation and meeting the demands of fine-grained data analysis. Customers may worry about their privacy as a result of the fact that classic multidimensional data-aggregation systems are vulnerable to coalition attacks from the gateway and control centre, which rely on an established authority. A decentralised decryption system based on ElGamal homomorphic cryptography is presented by Zuo et al. [10], which can withstand the coalition assault from both the Gateway (GW) and the Control Center (CC). It is also important to note that the proposed method does not rely on an authority that is not totally trustworthy in the real world. According to a thorough security analysis, the proposed technology is capable of meeting the security criteria of the smart grid.

2.3 Cryptography models

Secure communication between smart metres and the smart grid is only possible if an authenticated key protocol can be developed, which has recently received substantial attention. In most circumstances, a mutual authentication method can be reached without the involvement of a trusted third-party. Elliptic Curve Qu-Vanstone (ECQV) implicit certificates were used by Qi and Chen [11] to construct an authenticated key agreement method for the smart grid and

achieve some significant advancements in this sector. There is no need for any pairing in order to assure mutual authentication scheme agreement and strong credential privacy with minimum computation and communication costs in the suggested approach.

Smart IoT devices can now be linked in new ecosystems to improve energy systems' efficiency and reliability by managing various energy sources. The amount of data generated by smart grid IoT devices necessitates the use of a cloud server. Because the cloud server's data is accessible to many people, it must be authentic and confidential. Using proxy re-encryption, a third party can decrypt an encrypted file and re-encrypt it without viewing the original content. This is the best choice for this type of communication. There are currently no smart grid encryption systems that do not demand a significant amount of bandwidth and computing time. Hussain et al. [12] offer an IoT device certificate-based signcryption with proxy re-encryption (CBSRE) to reduce communication and computation expenses. The suggested CBSRE approach relies on a hyperelliptic curve cryptosystem with minimal parameters and an 80-bit key size to provide security and efficiency.

For resource-constrained smart metres, Garg et al. [13] proposed a lightweight and safe authentication approach that provides security, anonymity and mutual authentication. In order to create a key agreement procedure that can be verified by both parties, elliptic curve cryptography and one-way hashing algorithms are employed. In addition, it gives the capacity to establish and verify trust and understanding between SMs and neighbour area networks. Because these organisations communicate over an insecure network, smart metering relies on it. Long-term testing has proven that this protocol is more secure than the industry's existing standard while also consuming less communication and compute resources.

The new phase of electronic power networks is represented by the terms of smart grid. Electricity is tracked by sensors, communications, and control devices as it travels from the source to the end user. For clients who want to know exactly how much energy they're using at any one time, a growing number of smart metres are being placed across the globe. With less network traffic and processing resources, increased energy efficiency, and accuracy of data, privacy in industrial ecosystems may have to be given more concern. Computer resources, communication overhead, and hiring a trustworthy third party have all been used to assault the privacy of customers in various researchers. Ali et al. [14] proposed a symmetric encryption approach for industrial ecosystems in the IoT context. The proposed model exhibits better encryption accuracy rate.

It's essential that the smart grid be protected against cyberattacks. SG's security demands necessitate the proper implementation of key establishment processes. In recent years, Singapore has seen a spate of diverse proposals for large new skyscrapers. There are, however, only two smart metres that are capable of ensuring the highest level of privacy for their users. In the smart grid, utilities and customers share data and electricity in a two-way exchange. A smart meter's data can be sent to service providers (SPs) and also control signals in the other direction. Users can better utilise electricity resources by evaluating the present condition of production and supply through this two-way interaction. Abbasinezhad-Mood et al. [15] proposed an efficient and secure key agreement technique to address the issue of key escrow, while avoiding the security issues of earlier anonymous schemes.

Author Name/s	Year of Publication	Proposed Model	Limitations
Qi and Chen [11]	2020	The author proposed a new authenticated key agreement technique for smart grid using the Elliptic Curve Qu-Vanstone (ECQV) implicit certificate in order to build a secure authenticated key agreement method for the smart grid and make some breakthroughs in this field. The proposed method does not require any pairing in order to guarantee mutual authentication scheme agreement and robust credential privacy with minimal computation and communication costs.	The proposed authentication model is strong but it can handle a less number of nodes in network. If nodes are adding dynamically, the load on the authentication model is high.
Hussain et al.[12]	2020	A certificate-based signcryption with a proxy re-encryption (CBSRE) technique for IoT devices is proposed. In order to ensure the security and efficiency of the proposed CBSRE method, a hyperelliptic curve cryptosystem is used with simple parameters and 80-bit key size.	The IoTsmartgrid security model is efficient but the signcryption model operations are complex that can be reduced with less complexity so that load can be reduced for better performance.
Garg et al.[13]	2019	The author proposed a lightweight and safe authentication approach that provides security, anonymity and mutual authentication. In order to create a key agreement procedure that can be verified by both parties, elliptic curve cryptography and one-way hashing algorithms are employed.	The cryptography model used is used for authentication to provide security. However, the masquerade attacks and replay attack can be done still that reduces the security levels.
Ali et al. [14]	2020	Computer resources, communication overhead, and hiring a trustworthy third party have all been used to assault the privacy of customers in various researchers. The authorproposed a symmetric encryption approach for industrial ecosystems in the IoT context. The proposed model exhibits better encryption accuracy rate.	The trust factor that is considered in the model is used for privacy maintaining used to secure the data. The cryptography model can be still enhanced by considering the large sized keys.
Abbasinezhad-Mood et al. [15]	2020	A smart meter's data can be sent to service providers (SPs) and also control signals in the other direction. Users can better utilise electricity resources by evaluating the present condition of production and supply through this two-way interaction. The author proposed an efficient and secure key agreement technique to address the issue of key escrow, while avoiding the security issues of earlier anonymous schemes.	The key generation model generates the keys for securing the data. The key reusing need to be avoided by the attackers to improve the system performance.

2.4 Malicious user detection models

Analyzing and making use of massive amounts of metre data can be beneficial to decision-makers. As a result, the processing of data from several metres has received a great deal of attention in recent years. Even so, it has the potential to reveal personal information about its users. Data processing methods for smart grids that are effective and private are presented by Shen et al. [16]. Using Horner's Rule and homomorphic encryption, the proposed technique keeps metre data private while randomly permuting it on a huge scale. Without understanding where the data comes from, analysis centres can simultaneously execute a variety of operations such as variance, comparison, and linear regression analysis. The proposed technology is capable of ensuring data security and source anonymity, according to the results of an investigation. In terms of computation and communication, the proposed protocol is shown to be cost-effective.

The employment of cutting-edge technology and equipment in the smart grid provides substantial advantages over traditional electrical networks. There are a slew of new security issues brought on by the smart grid's new hardware and software. Malicious individuals aiming to steal electricity can gain access to smart metres at any time and from any location. This has the effect of making it more difficult to catch people who steal electrical equipment. User authentication analysis is one way researchers have used to track down attackers. Due to either a lack of precision or prohibitive expenses for installing monitoring devices, these solutions are not ideal. A limited number of monitoring devices will be used to locate malicious users as fast as feasible. Investigations of power theft begin with a thorough review of prior records of electricity theft and discrepancies between reported and projected normal consumptions. Based on these findings, a suspicion honest assessment inspection (SAI) method has been devised by Xia et al. [17], in which the most suspected users are first investigated. The other users will be investigated using a binary tree-based examination approach. The user's hunches guide the creation of the binary tree. Binary tree node inspection order is also influenced by the suspicions.

To regulate the flow of real power, power grid phase shifters are utilised by Chakrabartyand Sikdar [18]. Due to contractual obligations, transmission lines might become overcrowded and cross-network power flows can become unpredictable. These phase shift directions are communicated via Supervisory control and data acquisition (SCADA) networks in a smart/automated grid. Consequently, it is vulnerable to cyberattacks, especially those conducted in secret. It is possible for malicious phase shift directives to disrupt important transmission lines by interfering with cross-network trading. Although this control system is vital, little attention has been paid to cyber-attacks against it. An algorithm or approach to detect various attacks, including some that are undetectable, is proposed for the first time in this research. The suggested algorithm is based on the current-to-terminal-voltage ratios of branches or nodes. These indexes have been demonstrated to be effective in the detecting context through the use of mathematical models. With these indices, it was found that the proposed technique worked well with phase shifters in the IEEE 118-bus system and was computationally light and simple to implement.

A real-time non-probabilistic assurance can be used to detect load redistribution (LR) assaults on the smart grid that intend to overflow. A reliable and complex detection method is essential in the event that the standard bad-data detectors fail to detect LR attacks. Kaviani and Hedman [19] proposed a detection strategy based on a fundamental knowledge of the physics of the electric grid. It is able to uncover a structure beneath the surface that may be abused by an attacker to solve the root of the problem. The most successful attack paths and the most vulnerable transmission assets are then identified, and an efficient method is provided. The ideal attack and sensitive buses revealed in this study were used to develop an index that may be used in practise with minimal disruption.

Using a monitoring method called state estimation (SE), smart power grids will play an important role in the future of smart cities. Edge computing-based Internet of Things (IoT) is used to estimate the state of the imbalanced home distribution grid in the region. Future control actions depend on the SE results, but the accuracy of the data collected by the distributed measuring devices is as important concept. Because of this, the SE module is at risk from attacks based on manipulated data. At this time, the most attention is being paid to an attack known as fake data injection (FDI), which has the potential to impair routine network operations while remaining undetected. Tranet et al. [20] proposed a nonlinear physical constraint model for a stealthy attack on FDI systems. For testing purposes, an IEEE 13-node test feeder and WSCC 9-bus system are employed.

Author Name/s	Year of Publication	Proposed Model	Limitations
Shen et al. [16]	2021	Data processing methods for smart grids that are effective and private are presented by the author. Using Horner's Rule and homomorphic encryption, the proposed technique keeps metre data private while randomly permuting it on a huge scale.	The attackers detection is poor in this model as the cracking of keys can be easily done and the data can be accessed that need to be avoided.
Xia et al. [17]	2020	Based on these findings, a suspicion honest assessment inspection (SAI) method is proposed, in which the most suspected users are first investigated. The other users will be investigated using a binary tree-based examination approach. The user's hunches guide the creation of the binary tree. Binary tree node inspection order	The proposed model is capable of detecting attacks strongly but only limited attacks can be avoided. New attacks cannot be detected that reduces the security levels.
Chakrabarty and Sikdar [18]	2021	To regulate the flow of real power, power grid phase shifters are utilised. Due to contractual obligations, transmission lines might become overcrowded and cross-network power flows can become unpredictable.	The operations used in malicious node detection is strong and complex that can be simplified to reduce the load and delay in the network.

Kaviani and Hedman[19]	2021	The author proposed a detection strategy based on a fundamental knowledge of the physics of the electric grid. It is able to uncover a structure beneath the surface that may be abused by an attacker to solve the root of the problem. The most successful attack paths and the most vulnerable transmission assets are then identified, and an efficient method is provided.	The load distribution model is best and the accuracy is also high. The model does not concentrate on mobility nodes. The load distribution to the suddenly left out nodes is not discussed.
Tran et al.[20]	2021	The most attention is being paid to an attack known as fake data injection (FDI), which has the potential to impair routine network operations while remaining undetected. The author proposed a nonlinear physical constraint model for a stealthy attack on FDI systems. For testing purposes, an IEEE 13-node test feeder and WSCC 9-bus system are employed.	The balancing of load can be still enhanced to avoid the data attacks. Strong cryptography models can be applied to secure the smart grid from attacks.

2.5 Attack detection models

The Smart Grid Monitoring System (SGMS) is a critical component in ensuring the safety of the smart grid. Due to the overwhelming volume of notifications generated by SGMS, executives are usually left perplexed. When it comes to handling alarms and extracting attack events, smart grids confront significant difficulties. It is impossible to apply most existing security event analysis methods to the power grid because of its high reliability and limited attack tolerance. SGMS warnings could be utilised to detect attacks, according to this research. Using IP correlation, Zhang et al. [21] generated an approach that generates an alert graph, which is then aggregated into a prospective attack chain. On the other hand, the number of early attack chains is reduced by negative causal correlations and non-cascading events.

Cyber-physical (CP) attacks, vulnerabilities and mitigation approaches for the smart grid applications are examined by Amin et al. [22]. Due to cyber risks, the performance of the smart grid is critically impacted by the rapid development of physical technologies in power electronics for connecting renewable energy sources that include cyber frameworks. There is a risk of major cyber-attacks because of the use of electronic equipment connected to communication networks in smart grid applications If this happens, one approach is to physically isolate digital controllers. Cyber-physical systems demand additional attention and security for power electronic systems in the smart grid because of CPSs.

A data integrity attack (DIA) is one sort of cyber-attack that puts the IoT-based smart grid at risk. As long as the attacker has complete or insufficient knowledge of the system's architecture and branch parameters, it is impossible to detect and undermine smart grid state estimate with the highly synthesised DIA. The branch parameters can't be easily accessed or deduced by an attacker in practise. They can change or be disrupted at any point in time. Zhang et al. [23] provided the zero-parameter-information DIA (ZDIA) so that the attacker can carry out stealthy data manipulation attacks without knowing anything about the branch parameters. The cut line's geometry is all that is required for this assault type. If an attacker has access to all the buses in a group of one-degree super-buses that are only connected to the outside by a single cut line, users can arbitrary modify the state estimations of all of them.

A vital role for ICT is played in today's smart cities in controlling demand response management. In a smart grid environment, sensors are used extensively to keep track of everything. These devices are used to alert the central control station when a high-tension power supply line is malfunctioning. Due to their location on high-tension electrical lines in an open environment, sensors may be vulnerable to both physical and cyberattacks. As a final resort, a hacker could pretend to be a sensor, gateway, or control centre. Cyber and physical attacks on a smart grid must be averted in order to maintain a secure and effective monitoring system. Inspired by these considerations, Badar et al. [24] proposed an identity-based authentication method for power supply line surveillance in a smart grid. When tested thoroughly, the protocol designed is impervious to both physical and cyber-attacks on sensors. Reduced calculation needs make this protocol more cost-effective than other relevant ones.

Over time, concerns about power grid cybersecurity have increased as communication technologies have become more intertwined. State Estimator (SE) must be secured against cyberattacks because of its critical role in the control of electricity grid. False Data Injection Attacks (FDIA), a subtype of assaults targeting this module, have received a lot of attention. A model for detecting FDIA was proposed by Jorjani et al. [25]. It is impossible to get back to the original values of grid variables that have been tampered with. Using an adaptive optimization method, grid elements that were targeted inside the attack can be recovered while making as few changes as possible to those that were not. It has been suggested that the recovery algorithm's effectiveness be measured using the Recovery Quality Index (RQI).

Developing an AMI is essential to implement smart grids. Reliability and security of the smart grid are directly impacted by the security of AMI's digital infrastructure. Analytical models established by Zhang et al. [26] are used to test the AMI system's resilience against Distributed Denial-of-Service (DDoS) assaults. In order to create a model of how the state of an AMI communication network varies over time, this research aims to create and describe a dynamic differential system for the network as a whole. An attack on AMI's dynamic differential system is examined, and a defence technique is proposed that best distributes AMI system security resources to minimise defensive losses and costs.

The traditional routing models performs mitigation of the negative effects of both proactive and reactive routing systems. There is no delay caused by establishing a route while communicating across short distances. Decreased overhead caused by reactive routing for distant destinations is observed.

Author Name/s	Year of Publication	Proposed Model	Limitations
Zhang et al. [21]	2019	Using IP correlation, the author generated an approach that generates an alert graph, which is then aggregated into a prospective attack chain. On the other hand, the number of early attack chains is reduced by negative causal correlations and non-cascading events.	The attack detection model is efficient and accurate. However, the model need to concentrate on reducing the false alarms in the smart grid.
Amin et al. [22]	2021	Cyber-physical (CP) attacks, vulnerabilities and mitigation approaches for the smart grid applications are examined in this research. Due to cyber risks, the performance of the smart grid is critically impacted by the rapid development of physical technologies in power electronics for connecting renewable energy sources that include cyber frameworks	The power consumption in smart grid can still be reduced by using a switching control model that makes several nodes as idle to avoid power consumption.
Zhang et al. [23]	2021	The author provided the zero-parameter-information DIA (ZDIA) so that the attacker can carry out stealthy data manipulation attacks without knowing anything about the branch parameters. The cut line's geometry is all that is required for this assault type.	The data integrity levels is satisfactory, however it is better to concentrate on node authentication or considering a trust factor for strict authentication and access control.
Badar et al. [24]	2021	The author proposed an identity-based authentication method for power supply line surveillance in a smart grid. When tested thoroughly, the protocol designed is impervious to both physical and cyber-attacks on sensors. Reduced calculation needs make this protocol more cost-effective than other relevant ones.	The cost of managing the model is high as the resources utilization and requirement is high. The resource sharing can be applied on the model and also node behaviour can be considered for better performance levels.
Jorjani et al. [25]	2021	False Data Injection Attacks (FDIA), a subtype of assaults targeting this module, have received a lot of attention. A model for detecting FDIA was proposed in this research. It is impossible to get back to the original values of grid variables that have been tampered with.	The optimization model for attacks on grids can be further enhanced by reducing the delay rate and also to avoid attacks by strong cryptography based authentication model.
Zhang et al. [26]	2020	Analytical models established that is used to test the AMI system's resilience against Distributed Denial-of-Service (DDoS) assaults. In order to create a model of how the state of an AMI communication network varies over time, this research aims to create and describe a dynamic differential system for the network as a whole.	There is a strong requirement of detecting malicious nodes in smart grid that impacts the grid performance and data transmission rate.

3. PROPOSED MODEL

The standards and technology used to protect data transfer between utilities and smart metres must be evaluated in order to ensure a safe and reliable Smart Grid. Malicious malware, viruses, and worms have been used to impair the smart grid's communications system via Distributed Denial of Service (DDoS) attacks. Attacks like these are meant to cause widespread damage to critical infrastructure by interrupting industrial control and automation systems. Although improvements in sensor and data processing technologies have made it more difficult for security breaches to occur, more safeguards may be necessary. Because of its importance in so many different types of monitoring applications, a wireless sensor network is a good fit for these setups even in the harshest of environments. Proactive and reactive measures that smart grids can take to reduce interruptions and separate impacted areas in the event of a natural catastrophe have led to optimism about their potential for increased reliability.

Consumers will be less dependent on the grid as a result of the enhanced distribution generation capacity. In the event of a grid failure or power outage, electrical converters and inverters can be used to enable islanding mode. The WSN can offer real-time information on these kinds of events. The research sensing phase would not have been complete without the Sensor Nodes. WSN is an interesting technology in power grid management and reviewing because of its compact size and adaptability to a wide range of network topologies. RF frequencies and extremely low power are used by the WSN transceiver module to transmit data over the wireless network. Intermediary transmission is used to deliver the electricity generated by power converters to utility grids.

While both energy suppliers and consumers are enthused about the possibilities of this technology, a fundamental security risk is hindering its adoption and restricting its utility. Data sharing between smart metres and network management is essential for generating consumption bills for the quantity of energy consumed. Because it is transmitted across an unprotected network, this data is more vulnerable to compromise, control, and invalidation by an attacker who can alter the smart grid's behaviour and performance.

Aside from this, the development of efficient models adds to the difficulty. Network distribution managers and smart metres talk to each other over the network, but the proposed research focuses on safeguarding those relationships based on the limitations observed. An authenticated key agreement security method needs to be implemented to ensure privacy while allowing for variable and unpredictable behaviour with the purpose of delivering a higher level of security for any shared communication.

To overcome the limitations observed in this survey, there is strong requirement to create a smart grid networking paradigm that solely relies on trusted nodes to connect and share data.The development of an effective cryptography-based identification architecture with the preservation of trust factors is required in order to regulate network access and data transmission. By considering the trust factors, a priority-based clustering strategy for sharing data among the smart grid network can be created by recognising malicious nodes in the network.To provide secure data flow in the smart grid, a group key management method can be implemented based on cryptography and data aggregation.

4. CONCLUSION

Power grids are used to distribute electricity across a large area. There are three components to a power grid: generation, transmission, and distribution. There is a shortage of energy available to consumers in a traditional power system if supply and demand do not match up. Losses on transmission system and an absence of information increase inefficient power management, which is made worse by the ageing grid's problems. There is a growing consensus that cyber security is a worldwide problem that has to be addressed. Electronic data efficiency, comfort, and sustainability can all be improved with smart grid metering and control systems. This research presented a brief survey on some of the most important management and cryptography models in smart grid. Depending on the application, a pre-deployed key or a dynamically generated key is commonly used for initial network authentication. A symmetric key is favoured by most schemes because of low processing power required, the short computation time, and the low storage requirements due to the lower key length. There are also schemes that use upstream servers to act as trusted authorities. Asymmetric cryptography is used for the initial authentication scheme exchange. The design of routing protocols to fit the needs of SG applications is becoming more common. Before routing protocols for SG can be designed, there are many difficulties that need to be resolved. The most significant technology for the grid is the integration of information and the most recent communication technologies with enhanced security levels. The key concern is the safety of the grid's distribution system. The study focused on smart grids and the security issues they pose. The difficulty can be solved by integrating a chip for cryptography encryption and decryption. This research is helpful for researchers to identify the limitations and security concerns in smart grids that can be overcome in future.

REFERENCES

[1] Zhang, S., Leung, K.C. (2020). Joint optimal power flow routing and vehicle-to-grid scheduling: Theory and algorithms. IEEE Transactions on Intelligent Transportation Systems, 23(1): 499-512. https://doi.org/10.1109/TITS.2020.3012489

[2] Das, R., Bera, J.N. (2022). Quality of service improvement in neighborhood area networking for AMI with ZigBee-based tunable clustered scale-free topology and RPL routing. IEEE Transactions on Smart Grid, 14(1): 453-463. https://doi.org/10.1109/TSG.2022.3191358

[3] Xu, L., Guo, Q., Yang, T., Sun, H. (2018). Robust routing optimization for smart grids considering cyber-physical interdependence. IEEE Transactions on Smart Grid, 10(5): 5620-5629. https://doi.org/10.1109/TSG.2018.2888629

[4] Velusamy, D., Pugalendhi, G. (2020). Water cycle algorithm tuned fuzzy expert system for trusted routing in smart grid communication network. IEEE Transactions on Fuzzy Systems, 28(6): 1167-1177. https://doi.org/10.1109/TFUZZ.2020.2968833

[5] Kong, P.Y. (2020). Routing in communication networks with interdependent power grid. IEEE/ACM Transactions on Networking, 28(4): 1899-1911. https://doi.org/10.1109/TNET.2020.3001759

[6] Velusamy, D., Pugalendhi, G., Ramasamy, K. (2019). A cross-layer trust evaluation protocol for secured routing in communication network of smart grid. IEEE Journal on Selected Areas in Communications, 38(1): 193-204. https://doi.org/10.1109/JSAC.2019.2952035

[7] Zhu, X., Wen, M.H., Li, V.O., Leung, K.C. (2018). Optimal PMU-communication link placement for smart grid wide-area measurement systems. IEEE Transactions on Smart Grid, 10(4): 4446-4456. https://doi.org/10.1109/TSG.2018.2860622

[8] Kong, P.Y. (2019). Optimal configuration of interdependence between communication network and power grid. IEEE Transactions on Industrial Informatics, 15(7): 4054-4065. https://doi.org/10.1109/TII.2019.2893132

[9] Li, S., Xue, K., Wei, D. S., Yue, H., Yu, N., Hong, P. (2019). SecGrid: A secure and efficient SGX-enabled smart grid system with rich functionalities. IEEE Transactions on Information Forensics and Security, 15: 1318-1330. https://doi.org/10.1109/TIFS.2019.2938875

[10] Zuo, X., Li, L., Peng, H., Luo, S., Yang, Y. (2020). Privacy-preserving multidimensional data aggregation scheme without trusted authority in smart grid. IEEE Systems Journal, 15(1): 395-406. https://doi.org/10.1109/JSYST.2020.2994363

[11] Qi, M., Chen, J. (2020). Two-pass privacy preserving authenticated key agreement scheme for smart grid. IEEE Systems Journal, 15(3): 3201-3207. https://doi.org/10.1109/JSYST.2020.2991174

[12] Hussain, S., Ullah, I., Khattak, H., Adnan, M., Kumari, S., Ullah, S.S., Khan, M.A., Khattak, S.J. (2020). A lightweight and formally secure certificate based signcryption with proxy re-encryption (CBSRE) for Internet of Things enabled smart grid. IEEE Access, 8: 93230-93248. https://doi.org/10.1109/ACCESS.2020.2994988

[13] Garg, S., Kaur, K., Kaddoum, G., Rodrigues, J.J., Guizani, M. (2019). Secure and lightweight authentication scheme for smart metering infrastructure in smart grid. IEEE Transactions on Industrial Informatics, 16(5): 3548-3557. https://doi.org/10.1109/TII.2019.2944880

[14] Ali, W., Din, I.U., Almogren, A., Guizani, M., Zuair, M. (2020). A lightweight privacy-aware IoT-based metering scheme for smart industrial ecosystems. IEEE Transactions on Industrial Informatics, 17(9): 6134-6143. https://doi.org/10.1109/TII.2020.2984366

[15] Abbasinezhad-Mood, D., Ostad-Sharif, A., Nikooghadam, M., Mazinani, S.M. (2019). A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid. IEEE Transactions on Industrial Informatics, 16(3): 1495-1502. https://doi.org/10.1109/TII.2019.2927512

[16] Shen, H., Zhang, M., Wang, H., Guo, F., Susilo, W. (2021). Efficient and privacy-preserving massive data processing for smart grids. IEEE Access, 9: 70616-70627. https://doi.org/10.1109/ACCESS.2021.3078629

[17] Xia, X., Xiao, Y., Liang, W. (2019). SAI: A suspicion assessment-based inspection algorithm to detect malicious users in smart grid. IEEE Transactions on Information Forensics and Security, 15: 361-374. https://doi.org/10.1109/TIFS.2019.2921232

[18] Chakrabarty, S., Sikdar, B. (2020). Detection of

malicious command injection attacks on phase shifter control in power systems. IEEE Transactions on Power Systems, 36(1): 271-280. https://doi.org/10.1109/TPWRS.2020.3008184

[19] Kaviani, R., Hedman, K.W. (2020). A detection mechanism against load-redistribution attacks in smart grids. IEEE Transactions on Smart Grid, 12(1): 704-714. https://doi.org/10.1109/TSG.2020.3017562

[20] Tran, N.N., Pota, H.R., Tran, Q.N., Hu, J. (2021). Designing constraint-based false data-injection attacks against the unbalanced distribution smart grids. IEEE Internet of Things Journal, 8(11): 9422-9435. https://doi.org/10.1109/JIOT.2021.3056649

[21] Zhang, H., Jin, X., Li, Y., Jiang, Z., Liang, Y., Jin, Z., Wen, Q. (2019). A multi-step attack detection model based on alerts of smart grid monitoring system. IEEE Access, 8: 1031-1047. https://doi.org/10.1109/ACCESS.2019.2961517

[22] Amin, M., El-Sousy, F.F., Aziz, G.A.A., Gaber, K., Mohammed, O.A. (2021). CPS attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: A review. IEEE Access, 9: 38571-38601. https://doi.org/10.1109/ACCESS.2021.3063229

[23] Zhang, Z., Deng, R., Yau, D.K., Chen, P. (2021). Zero-parameter-information data integrity attacks and countermeasures in IoT-based smart grid. IEEE Internet of Things Journal, 8(8): 6608-6623. https://doi.org/10.1109/JIOT.2021.3049818

[24] Badar, H.M.S., Qadri, S., Shamshad, S., Ayub, M.F., Mahmood, K., Kumar, N. (2021). An identity based authentication protocol for smart grid environment using physical uncloneable function. IEEE Transactions on Smart Grid, 12(5): 4426-4434. https://doi.org/10.1109/TSG.2021.3072244

[25] Jorjani, M., Seifi, H., Varjani, A.Y., Delkhosh, H. (2021). An optimization-based approach to recover the detected attacked grid variables after false data injection attack. IEEE Transactions on Smart Grid, 12(6): 5322-5334. https://doi.org/10.1109/TSG.2021.3103556

[26] Zhang, C., Luo, F., Sun, M., Ranzi, G. (2020). Modeling and defending advanced metering infrastructure subjected to distributed denial-of-service attacks. IEEE Transactions on Network Science and Engineering, 8(3): 2106-2117. https://doi.org/10.1109/TNSE.2020.3015220

[27] Kong, P.Y., Jiang, Y. (2022). VNF orchestration and power-disjoint traffic flow routing for optimal communication robustness in smart grid with cyber-physical interdependence. IEEE Transactions on Network and Service Management, 19(4): 4479-4490. https://doi.org/10.1109/TNSM.2022.3165219

[28] Kong, P.Y. (2020). A review of quantum key distribution protocols in the perspective of smart grid communication security. IEEE Systems Journal, 16(1): 41-54. https://doi.org/10.1109/JSYST.2020.3024956