TELKOMNIKA, Vol.17, No.3, June 2019, pp.1584~1594
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v17i3.11437

Authentication techniques in smart grid: a systematic review

Malik Qasaimeh*1, Rawan Turab2, Raad S. Al-Qassas3
1Department of Software Engineering, Princess Sumaya University for Technology,
P.O. Box 1438 Amman 11941 Jordan
2,3Department of Computer Science, Princess Sumaya University for Technology,
P.O. Box 1438 Amman 11941 Jordan
*Corresponding author, e-mail: m.qasaimeh@psut.edu.jo

Abstract

Smart Grid (SG) provides enhancement to existing grids with two-way communication between the utility, sensors, and consumers, by deploying smart sensors to monitor and manage power consumption. However due to the vulnerability of SG, secure component authenticity necessitates robust authentication approaches relative to limited resource availability (i.e. in terms of memory and computational power). SG communication entails optimum efficiency of authentication approaches to avoid any extraneous burden. This systematic review analyses 27 papers on SG authentication techniques and their effectiveness in mitigating certain attacks. This provides a basis for the design and use of optimized SG authentication approaches.

Keywords*: authentication, key management, smart grid, smart meter*

1. Introduction

Existing grids are enhanced in the case of smart grids (SGs) by the introduction of bilateral communication between consumers, utilities, and sensors, which in the case of smart sensors and meters enables monitoring and management of the consumption of electrical power [1, 2]. More advanced sensor solutions, e.g. Phasor Measurement Units (PMUs), enable energy saving by re-routing power automatically, relative to consumer demand, facilitating reduced energy wastage and optimum stability, including error detection and reporting (e.g. during power outages), and faster diagnosis and troubleshooting to enable system restoration in the event of problems [3]. Advantages of SGs include reduced costs, less energy consumption (with the potential for reduced carbon emissions and other detrimental environmental impacts), fewer failures and quicker repair, and less potential for theft [4]. There are three main network types in SG architectures:

- Wide Area Network (WAN)
- Neighborhood Area Network (NAN): this gathers data from PMUs and smart meters for the utility company [3]
- Home Area Network (HAN): within Home Energy Management System (HEMS), this facilitates data collection concerning consumption [5]

Conventional systems' security features [6-8] must be conserved by SG and IoT applications; indeed, they ought to be enhanced and improved, in terms of service and utility availability, integrity, and confidentiality [9]. Additionally, they must face new dangers associated with smart technologies, including such attacks as denial of service (DoS), replaying, spoofing, traffic analysis and eavesdropping [10, 11]. The effects of such attacks range from relatively innocuous (though by no means trivial) impacts such as passively collecting user electricity consumption data (e.g. for market research) to altering smart meter values (thus manipulating customer bills and power provider revenues), and even corrupting system utilities [12].

A review of SG authentication mechanisms by Bayindir et al. [4] evaluated the use of Kerberos, public key authentication, one-time password, biometric authentication, and identity-based authentication, but it did not relate the analysis to actual potential threats faced in real-world applications. Nevertheless, the authors found that password-based authentication fails to provide mutual authentication, although it is useful in access control; and that certificate-less authentication is appropriate for SG authentication.

Received November 12, 2018; Revised January 28, 2019; Accepted March 5, 2019

SG multicast authentication one-time signature schemes were analyzed by Lei et al.[12], in terms of the parameters of suitability, key management effectiveness, and storage cost. The study found that the optimum theoretical solution was Time-Valid One-Time Signature (TV-OTS), a technique whereby signature-generating and private keys are intermittently refreshed, but more empirical research is necessary to substantiate this solution.

Various SG cryptography algorithms and associated key generation techniques were evaluated by A. Kumar and A. Agarwal [13]. The security of such solutions fundamentally depends on key randomness. It was found that in SG applications, lightweight algorithms are optimal due to system limitations, as they have lower memory requirements, and asymmetric algorithms are more germane, while symmetric algorithms are better solutions for the encryption of messages during the authentication process.

This paper systematically reviews literature concerning SG authentication approaches in order to identity optimized solutions for SG components relative to attacks, and analyses their effectiveness in mitigating certain attacks to provide a basis for the design and use of optimized SG authentication solution. Section 2 explains the research method. Section 3 sets out and analyses the results, while section 4 concludes the paper.

2. Research Method

This systematic review includes papers on SG authentication techniques published during the period 2010 and June 2018 in Springer Link (Springer), IEEE Xplore (IEEE), and ScienceDirect (Elsevier) libraries. Searching utilized the combination of keywords to yield hits pertinent to the research questions, subjected to inclusion and exclusion criteria phases, as shown and explained in Figure 1.

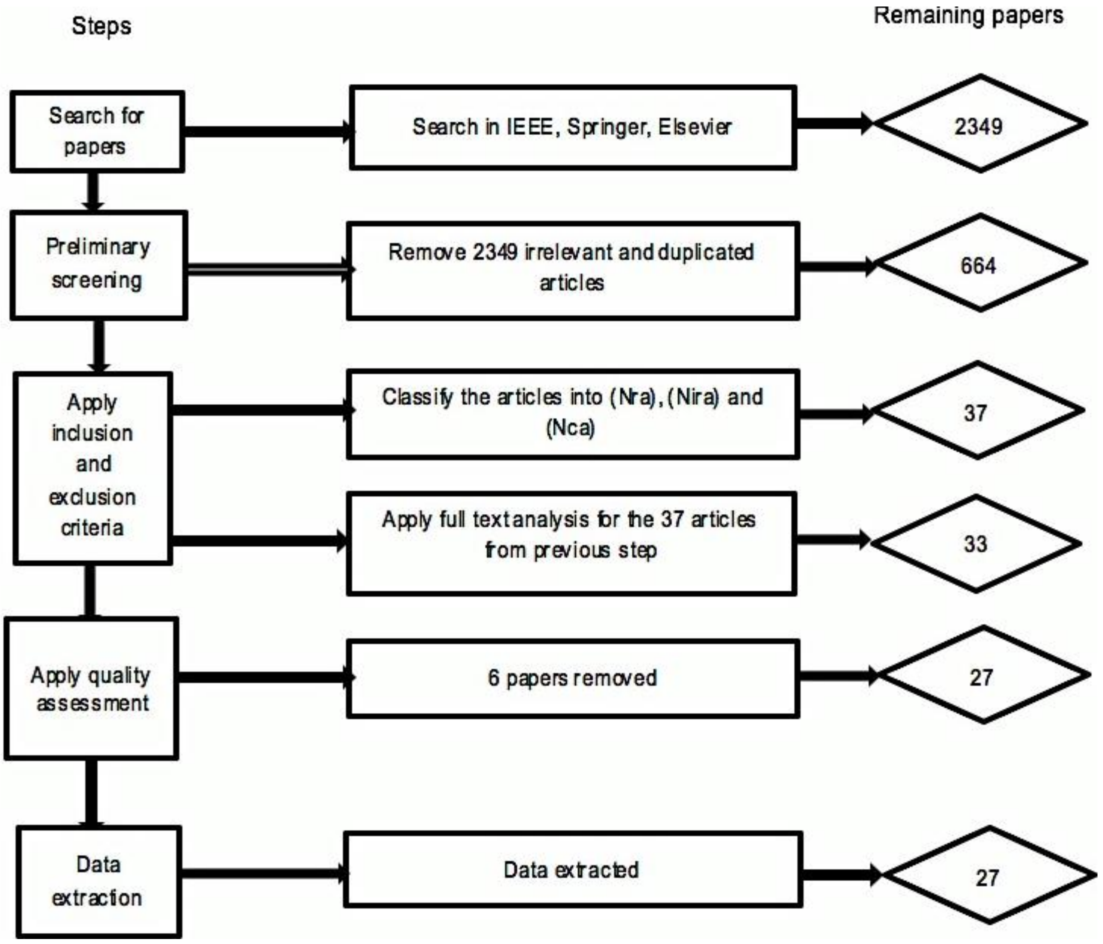
Steps
Remaining papers
Search for papers
Search in IEEE, Springer, Elsevier
2349
Preliminary screening
Remove 2349 irrelevant and duplicated articles
664
Apply inclusion and exclusion criteria
Classify the articles into (Nra), (Nira) and (Nca)
37
Apply full textanalysis for the 37 articles from previous step
33
Apply quality assessment
6 papers removed
27
Data extraction
Data extracted
27

Figure 1. Inclusion and exclusion process flow

2.1. Research Questions

The following key research questions guided this systematic review.

2.1.1. RQ1: What SG Authentication Approaches Exist?

This question targets particular techniques developed and tested in primary studies to give robust SG authentication solutions, with the objective of investigating common techniques and security models applied to enhance SG authentication.

2.1.2. RQ2: What Attack Types are Mitigated by these Authentication Approaches?

As explained previously, SG components are susceptible to numerous forms of attack (e.g. DoS and malicious software attacks). This research question aims to explore the application of identified authentication approach to prevent or manage common attacks on SG systems.

2.2. Search Process

2.2.1. Digital Libraries Search

The selected digital libraries (Springer Link, IEEE Xplore, and ScienceDirect) were searched for recent papers (published during 2010-June, 2018) on SG authentication, utilizing Scopus indexing, which purports to comprise the greatest database of peer-reviewed articles. Direct searching with key search terms was undertaken as shown in Table 1.

Table 1. Search Keywords

Keywords	Closely matched keywords	Combination using AND/OR (key string)
Smart grid	Electrical grid	Smart grid AND effective AND authentication technique OR key management (S1) Electrical grid AND effective AND authentication technique OR key management (S2)
Authentication techniques	Key management, digital signatures	Smart grid AND effective OR high quality AND digital signatures (S3) Electrical grid AND effective OR high quality AND digital signatures (S4)
Effective	High quality	Smart grid AND high quality AND authentication technique OR key management (S5) Electrical grid AND high quality AND authentication technique OR key management (S6)

2.2.2. Selection Execution

All of the searched libraries yielded differing volumes of articles using the key strings. Articles identified (i.e. hits) were compiled in CSV spreadsheets, then a script code was executed to identify duplications and intersections between the articles. The consequent mass of articles was refined by further selection, including examining the relevance of articles to the research questions based on their titles, which reduced the set to 664 by excluding studies not directly related to SG authentication techniques.

The first and second authors (i.e. reviewers) were engaged to independently examine the 664 articles with regard to the inclusion and exclusion criteria, again to exclude articles not directly evaluating SG authentication techniques or threat mitigation, this time based on reading their abstracts as well as titles. Outcomes were classed as relevant articles (Nra); conceivably relevant articles (Nca); and irrelevant articles (Nira). Articles excluded at this stage included those whose abstracts did not specify authentication techniques [14] or the mitigation of threats [15]. It was noted by the reviewers that some authentication techniques had been replicated in numerous studies by the same authors, with varying objectives or experimental methods; in such cases the most recent study relevant to the study inclusion and exclusion criteria was used.

A total of 35 and 31 articles were considered relevant (Nra) by the first and second reviewers (respectively), then they reviewed their pooled Nra, Nira, and Nca selections to judge 37 as relevant (Nra). To avoid any possibility of bias, the outcomes of the reviewers' assessments were conveyed to a third reviewer for checking, and all reviewers subsequently met to verify the exclusion of articles considered irrelevant by one or more reviewers, subsequently yielding a final collection of articles with consensus among the reviewers on their relevance to this study. As displayed in Figure 1. Finally, full-text analysis led to a total of

33 articles. Quality assessment criteria were subsequently used to guarantee the rigor and validity of the primary studies and 6 papers was eliminated.

2.2.3. Quality Assessment

The quality assessment decreased bias in article selection and made sure rigorous criteria were used in assessing the selected articles' quality as described in Table 2. Quality scoring used the following criteria: Yes indicates that an article unambiguously meets the assessment criteria (and thus is scored 1); No indicates that an article unequivocally fails to meet the criteria (scored 0); and Indistinctive refers to doubt in whether the article meets the criteria, necessitating more detailed analysis or correspondence with the author(s) to seek clarification or partially meet the criteria (scored 0.5). Studies that scored over 50% in the qualitative assessment are listed in Table 3.

2.3. Extracting Information

The extraction of information relevant to the research questions concerned:

- The SG component authentication technique.
- The attack the technique is intended to mitigate.
- The system vulnerabilities addressed.

Table 2. Criteria for Quality Assessment

S/N	Question	Answer
Q1	Is the research purpose clearly stated in the article?	Yes/ No/ Indistinctive
Q2	Does the paper topic cover the power generation domain?	Yes/ No/ Indistinctive
Q3	Does the paper use a mechanism, tool, framework, or methodology?	Yes/ No/ Indistinctive
Q4	Is the mechanism, tool, framework, or methodology used in the paper relevant to the research questions?	Yes/ No/ Indistinctive
Q5	Are the authentication approaches fully defined?	Yes/ No/ Indistinctive
Q6	Are the authentication approaches verified?	Yes/ No/ Indistinctive

Table 3. Results of Qualitative Assessment

Article ID		Source	Year	Q1	Q2	Q3	Q4	Q5	Q6	Total	Percentage compliance
PS1	[16]	IEEE	2012	1	1	1	1	1	1	6	100
PS2	[17]	IEEE	2012	1	1	1	1	1	0.5	5.5	91.66
PS3	[18]	IEEE	2017	0.5	1	1	1	0.5	0.5	4.5	83.33
PS4	[19]	IEEE	2013	1	1	1	1	1	0.5	5.5	.75
PS5	[20]	IEEE	2015	0.5	1	0.5	1	0.5	0.5	4	83.33
PS6	[21]	IEEE	2011	1	1	1	1	1	0.5	5.5	66.66
PS7	[22]	IEEE	2013	1	1	1	1	0.5	1	5.5	91.67
PS8	[23]	IEEE	2011	0.5	1	0.5	0.5	1	0.5	4	66.66
PS9	[24]	IEEE	2011	1	1	1	1	1	1	6	100
PS10	[25]	IEEE	2013	0.5	1	0.5	0.5	0.5	0.5	3.5	58.33
PS11	[26]	IEEE	2014	1	1	1	0.5	1	1	5.5	91.67
PS12	[27]	IEEE	2017	1	1	1	1	1	1	6	100
PS13	[28]	IEEE	2012	1	1	1	0.5	1	1	5.5	91.67
PS14	[29]	IEEE	2018	1	1	1	1	1	1	6	100
PS15	[30]	IEEE	2018	1	1	1	1	1	1	6	100
PS16	[31]	Science Direct	2017	1	1	1	1	1	1	6	100
PS17	[32]	Science Direct	2016	1	1	1	1	1	1	6	100
PS18	[33]	Science Direct	2018	1	1	1	1	1	1	6	100
PS19	[34]	Science Direct	2015	1	1	1	1	1	1	6	100
PS20	[35]	Science Direct	2018	1	1	1	1	1	1	6	100
PS21	[36]	Science Direct	2018	1	1	1		1	0.5	5.5	91.67
PS22	[31]	Springer Link	2016	1	1	1	0.5	1	0.5	5	83.34
PS23	[37]	Springer Link	2016	1	1	1	1	1	1	6	100
PS24	[38]	Springer Link	2013	0.5	1	1	1	1	0.5	5	83.34
PS25	[39]	Springer Link	2017	1	1	1	1	1	1	6	100
PS26	[40]	Springer Link	2015	1	1	1	1	1	1	6	100
PS27	[41]	IEEE	2014	1	1	1	1	1	11	6	100

3. Results and Analysis

3.1. SG authentication Approaches (RQ1)

Answering RQ1 was directly related to analyzing authentication techniques of SG; a concise summary is presented in Table 4. Subsequently, the identified techniques were categorized into approaches as described in Table 5. Almost every included study deployed some degree of cryptography in authentication, but we considered the approaches to be based on cryptography if they used known techniques of cryptography, including hash function, symmetric key encryption, and Diffie-Hellman. If they did not use such techniques, they were classified under the general category of the approach used, as declared by the authors. For instance, if password techniques were used for authentication of SG components with an encryption technique in a constituent phase, the approach was classed as a password-based one. Exceptional cases that could not be easily classified on this basis were included in the hybrid encryption category, which included primary studies using no clear classification of approach or multiple encryption techniques (e.g. public and symmetric key encryption) as illustrated in Table 5 and Figure 2. The categories of cryptographic approaches deployed in SG authentication are explained below.

Table 4. Smart Grid Authentication Approaches

Article ID		Authentication approach	Classification
PS1	[16]	Biometric fingerprint authentication	Biometric
PS2	[17]	Broadcasting symmetric key encryption using MKB (media key block) to distribute and extract the keys	Cryptography
PS3	[18]	Cryptography symmetric key encryption using a hash function to distribute keys	Cryptography
PS4	[19]	Scalable and automated password-changing approach	Password
PS5	[20]	TESLA-based source authentication	Cryptography
PS6	[21]	Cryptography using pair-wise keys, including message authentication code to check key integrity	Cryptography
PS7	[22]	Signature-based using (TV-OTS)	Signature-based
PS8	[23]	Cryptographic mutual authentication and two secret values to ensure non-repudiation and integrity	Cryptography
PS9	[24]	Cryptography using hash-based message authentication code and Diffie-Hellman key establishment	Cryptography
PS10	[25]	The secure chip that stores the provider credentials such as IP address, provider address, and associated phone number in a file included in the chip	Hardware
PS11	[26]	Cryptography using Merkel trees depending on a hash function	Cryptography
PS12	[27]	Hardware authentication approach using ring oscillator physically unclonable function (RO PUF) to derive keys	Hardware
PS13	[28]	Password and symmetric key, and one hash function to ensure key integrity	Password
PS14	[29]	Authentication approach based on certificateless cryptosystem	Cryptography
PS15	[30]	Lightweight authentication approach using elliptic curve	Cryptography
PS16	[31]	Cryptography using Diffie-Hellman key establishment and timestamps	Cryptography
PS17	[32]	Cryptography based on lightweight Diffie-Hellman	Cryptography
PS18	[33]	Authentication approach using elliptic curve cryptography	Cryptography
PS19	[34]	Cryptography using PUF to derive keys	Hardware
PS20	[35]	Enhanced elliptic curve cryptography-based authentication	Cryptography
PS21	[36]	Lightweight elliptic curve approach using third party	Cryptography
PS22	[31]	Cryptography using public key scheme with password data validation at server	Password
PS23	[37]	Source authentication based on the concept of *inf*-TESLA	Cryptography
PS24	[38]	Cryptography using a hash function with a secret key shared between parties, hash-based message authentication code (HMAC)	Cryptography
PS25	[39]	Cryptography used a key exchanged protocol based on chaotic maps	Cryptography
PS26	[40]	Signature and secret key based efficient authentication protocol against pollution attack (EAPA)	Signature
PS27	[41]	Merkle-tree-based authentication scheme for SG	Cryptography

3.1.1. Cryptographic-Based Approaches

The greatest number of studies fitting into a single category was for those using hybrid encryption for SG authentication, with 18.5% of primary studies, comprising 27.7% of cryptography-based approaches, as in PS5, PS6, PS14, PS23, and PS24. These approaches sought to conserve limited computational resources in SG components (i.e. energy and power). For instance, Timed Efficient Stream Loss-tolerant Authentication (TESLA) was used by PS5 and PS23, with the distinguishing characteristics of less overhead packet communication, greater toleration of packet loss, and lower computation overhead. TESLA is based on one-way chains generating symmetric keys that are subsequently revealed in reversed order, with messages being buffered prior to authentication. It is thus of utility for SG components that need to be generally synchronized for speed-efficient assimilation of energy data rather than real-time data processing speed, as in PS5. For high data transfer volumes and longer durations of communication, PS23 suggested the use of inf-TESLA (i.e. for multicast streaming data), which deploys dual key chain method to facilitate improved streaming authentication continuity, preventing resynchronization and signing lag times and other associated problems.

Table 5. Frequency Distribution of Authentication Approaches

Approach		Frequency	Percentage
Cryptography-based	*Classification and mapping*		
	Hybrid encryption	5	66.67
	Hash function	4	
	Diffie-Hellman	3	
	Elliptic curve	4	
	Chaotic maps	1	
	Broadcast encryption	1	
Password-based		3	11.11
Hardware-based		3	11.11
Signature-based		2	7.40
Biometric-based		1	3.70

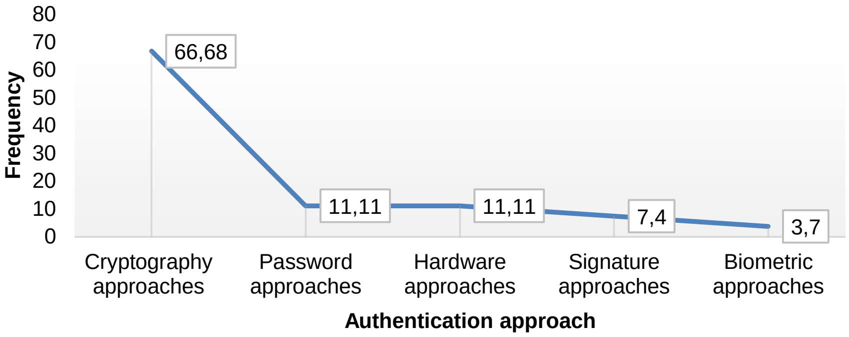

Figure 2. Frequency distribution of authentication approaches

The approach developed by PS6 for SG authentication used symmetric key encryption, with the sharing of pairwise keys between SG components, whereby all transmissions are encrypted prior to transmission; this approach was intended to optimize power efficiency (i.e. to function with the low computational power of SG components). PS14 used an authentication technique deploying a cryptosystem with certificate-less, using instead a blend of identity-based cryptography and public key technique to avoid the prohibitive cost of public key infrastructure (PKI) for private key generation, due to using a key generation center (KGC). PS24 used hash-based message authentication code (HMAC) and symmetric key encryption for SG components' mutual authentication, according to which components' authentication requires multiple proofs.

Hash-based approaches for authentication were deployed in PS3, PS8, PS11, and PS27, accounting for 22.22% of systematically reviewed primary studies, and 14.81% of those classified as cryptography-based. PS3 and PS8 used one-way hash function to address vulnerability to impersonation attack and repudiation attack (respectively). PS11 and PS27 used Merkle tree (a binary tree consisting of lead tokens, with each internal tree nodes being a hash of the right and left child nodes) for robust SG component authentication.

Elliptic curve approaches were declared by four of the systematically reviewed studies: PS15, PS35, PS37, and PS38. These accounted for 14.81% of selected primary studies, and 22.22% of cryptography-based techniques. PS15 used SM2 elliptical curve for SG components' mutual authentication, initiated with the connection between terminals and the SG center. The system monitored connections to detect time-out status, which prompted session closure. This provide efficient and fast computation and limited power drag. PS18 used elliptic curve to address limitations identified in [36] pertaining to perfect secrecy and vulnerability in terms of the Canetti–Krawczyk model. Similarly, PS20 tested an improved version of an elliptic curve used in a previous study, in this case another primary paper: PS15. A lightweight elliptic curve technique was proposed by PS21 that used third-party registration of participants in order to begin authentication, with the authentication process ending after the exchange of the key session.

Diffie-Hellman authentication comprised 11.11% of systematically reviewed studies, and 16.66% of those using cryptography-based techniques (PS9, PS16, and PS17). Hashing code and Diffie-Hellman exchange protocol was used in PS9 for mutual authentication and session key sharing. Using Diffie-Hellman, PS16 apply the concept of discrete logarithm problems to authenticate the transmitted messages. Similarly, advanced encryption standard (AES) and Rivest, Shamir, and Adelman (RSA) encryption were used in conjunction with Diffie-Hellman technique in PS17. Broadcast encryption and chaotic maps were used for key distribution only in PS2 and PS25, respectively.

3.1.2. Password-Based Approaches

Password-based approaches were used for authentication in 11.11% of included studies (PS4, PS13, and PS22). PS4 presented SCAPACH, a password-based authentication technique that generates novel, short-lived passwords automatically when initiating every session of authentication, using parameters including device ID, geographical location, and local time etc. SG-MCPEAK protocol was tested in PS13, with symmetric keys for multilayer password authentication. SSCA and PSCAb protocols of password authentication were tested in PS22, the former of which deployed symmetric key encryption, while the latter used public key encryption.

3.1.3. Hardware-Based Approaches

Hardware-based approaches accounted for 11.11% of systematically reviewed studies (PS10, PS12 and PS19). PS10 provided SG component authentication with improved data processing performance, mobility, and security using a smart chip integrated with multiple reliable crypto algorithms, including hash function and public and symmetric keys. Physically Unclonable Function (PUF) was implemented with Xilinx Spartan 3E FPGA boards to provide authentication using end-to-end hardware by PS12. Microprocessor integration with PUF offers unique identity for SG component devices. In PS19, PUF was also used for a hardware solution meeting the needs for Advanced Metering Infrastructures (AMIs) authentication.

3.1.4. Signature-Based Approaches

Signature-based authentication approaches accounted for 7.4% of included studies (PS7and PS26). Individual signatures were created using Time-Valid One-Time-Signature (TV-OTS) in PS7, with new secret keys periodically initiated by Hash of Random Subsets (HORS). This authentication technique provided multicasting, secure, real-time, dynamic authentication. While PS26 might be considered to be a hybrid technique of encryption, on balance the reviewers classified it as a signature-based method due to the relative scarcity of studies using signatures during authentication. PS26 deployed message authentication codes (MAC) in addition to homomorphic signature for authentication, the latter of which signed data packets when initiated at source, while MAC generated unique tags for every data packet.

3.1.5. Biometric-Based Approaches

Biometric-based approaches accounted for 3.7% of included studies. PS1 investigated the use of multiple authentication approaches in modern networks, with AES for the privacy of fingerprinting used in authentication of SG system users. Database storage of fingerprints included categorization into rich minutiae and sparse fingerprint types.

3.2. Mitigated Threats (RQ2)

Answering RQ2 involved analyzing types of attacks and threats mitigated by the studied authentication approaches. Table 6 lists the foremost varieties of attacks identified, which were studied in terms of frequency and distribution. Figure 3 displays the mitigated attacks' frequency distribution. The most common types of attacks mitigated are, in descending order: MiTM, replay, impersonation, eavesdropping, brute force, dictionary, spoofing, repudiation, and other. The 'other; category collectively accounts for 15%, denoting the fourth rank, but each constituent threat in this group was considered in only one systematically reviewed study, comprising *data forgery*, *DoS*, *information leakage*, *insider*, *modification*, *pollution*, and *quantum computer*.

With 21.66% of all attacks, MiTM was the most common mitigated attack. Some analysts note that MiTM and impersonation attacks are fundamentally similar, but they were classified as distinct categories in this paper following the example of the taxonomies used by most of the primary studies analyzed; for instance, PS6, PS14, PS15, PS16, and PS21 have particular techniques of MiTM mitigation and others for impersonation attack. The latter was also commonly studied in its own right by 16.66% of primary studies. For both impersonation and MiTM attacks, the main aim of authentication is to prevent unauthorized (i.e. malicious) components such as fake smart meters from imitating genuine components, in order to prevent unauthorized access by third parties attempting to access SG components' data during exchange, to avoid damage including stopping or reducing the quality of SG network performance, corrupting or dropping data packets, or initiating secondary attacks within the system, such as DoS attacks and data flooding.

Replay attack comprised 18.36% of the total of identified attacks in included studies (PS13, PS14, PS15, PS16, PS17, PS18, PS20, PS21, PS25, P26 and PS27). Authentication approaches seeking to protect data transmission between SG components from replay attack seek to prevent attackers intercepting, modifying and replaying data. Eavesdropping accounted for 10% of attacks mitigated in included studies (PS4, PS5, PS12, PS15, PS17, and PS25), seeking to protect data from attackers recording transmission or listening to data exchanged between SG components, especially consumer applications and smart meters. Eavesdropping is essentially an issue of system privacy and is particularly important where it relates to attackers stealing sensitive data and customer identity, with potential for fraudulent use.

Table 6. Threats Mitigated using Authentication Approaches

S/N	Reference		Threat (attack) mitigated
1	PS1	[16]	Impersonation
2	PS2	[17]	Information leakage by crackers
3	PS3	[18]	Impersonation
4	PS4	[19]	Eavesdropping, brute force
5	PS5	[20]	Eavesdropping, MiTM
6	PS6	[21]	MiTM, impersonation
7	PS7	[22]	Brute force
8	PS8	[23]	Repudiation
9	PS9	[24]	Spoofing, MiTM
10	PS10	[25]	Impersonation, data forgery
11	PS11	[26]	Quantum computer
12	PS12	[27]	Eavesdropping, spoofing, MiTM
13	PS13	[28]	MiTM, off-line dictionary, replay
14	PS14	[29]	Impersonation, MiTM, repudiation, replay
15	PS15	[30]	Replay, impersonation, message injection, MiTM, eavesdropping
16	PS16	[31]	Impersonation, MiTM, replay
17	PS17	[32]	Replay, MiTM, eavesdropping
18	PS18	[33]	Impersonation, MiTM, replay
19	PS19	[34]	Spoofing
20	PS20	[35]	Replay, modification, DoS, insider
21	PS21	[36]	Replay, impersonation, MiTM
22	PS22	[31]	Off-line dictionary
23	PS23	[37]	MiTM
24	PS24	[38]	Brute force, impersonation
25	PS25	[39]	Eavesdropping, dictionary, replay
26	PS26	[40]	Pollution (inject fake data packets), replay
27	PS27	[41]	Replay, modification

Spoofing, dictionary, and brute force attacks each accounted for 5% of attacks considered by the primary studies. SG entities used mutual authentication to avoid spoofing attacks, inhibiting attackers from accessing encryption (and/ or decryption) keys, and from disrupting authentication mechanisms. Dictionary and brute force attacks were mitigated using passwords for authentication between SG components and users, including utility companies, data aggregation points, and gateways. Tables are typically used to store passwords, with related authentication approaches preventing unauthorized access. Other attacks collectively accounted for 15% of attacks mitigated, comprising data forgery, DoS, information leakage, insider, modification, pollution, and quantum computer attacks.

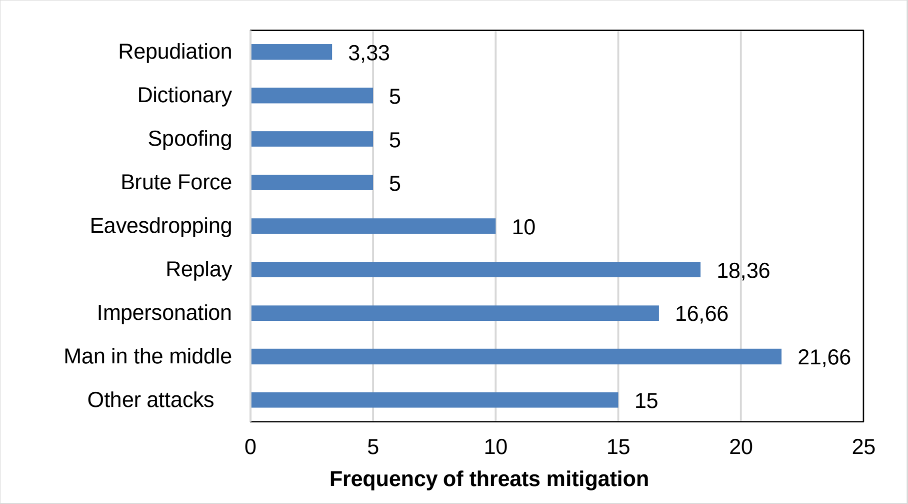

Figure 3. Frequency distribution of threats mitigation in smart grid

4. Conclusion

A total of 27 primary studies were systematically reviewed in this study, revealing that most researches deployed cryptographic techniques for SG component authentication, including hash function, symmetric key encryption, and Diffie-Hellman. The most common attack mitigated by the approaches was MiTM (21.66%), with impersonation attack being the third most common (16.66%). In both of these attack types, SG authentication approaches seek to inhibit access by impostor smart meters and thus prevent unauthorized third party access to data exchanged within the SG, avoiding damage including corrupting or dropping data packets.

The second most common attack was replay attack (18.33%), followed by eavesdropping (10%), which pertain to protecting customer identity and avoiding fraudulent use or manipulation of consumer data. Brute force, dictionary, and spoofing attacks each comprised 5% of attacks considered in systematically reviewed studies, while small numbers of studies considered other forms of attack (e.g. modification, insider, pollution, data forgery, DoS, information leakage, and quantum computer), collectively accounting 15%. While this research accomplished its objectives, it was limited by the relatively small number of directly relevant papers, and replication of this research with more extensive studies addressing new research questions concerning privacy and security attributes are recommended, to increase in-depth knowledge of SG security.

References

[1] M Faheem, SBH Shah, RA Butt, B Raza, M Anwar, MW Ashraf, *et al.*, Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. *Computer Science Review.* 2018; 30: 1-30.

[2] K Demir, H Ismail, T Vateva-Gurova, N Suri. Securing the cloud-assisted smart grid. *International Journal of Critical Infrastructure Protection.* 2018; 23: 100-111.

[3] M Kuzlu, M Pipattanasomporn, S Rahman. Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Computer Networks.* 2014; 67: 74-88.

[4] R Bayindir, I Colak, G Fulli, K Demirtas. Smart grid technologies and applications. *Renewable and Sustainable Energy Reviews.* 2016; 66: 499-516.

[5] CL Nge, IU Ranaweera, OM Midtgård, L Norum. A real-time energy management system for smart grid integrated photovoltaic generation with battery storage. *Renewable Energy.* 2019; 130: 774-785.

[6] M Qasaimeh, RS Al-Qassas. Comparative Randomness Analysis of DES Variants. *Recent Patents on Computer Science.* 2017; 10: 230-237.

[7] M Qasaimeh, RS Al-Qassas, S Tedmori. Software randomness analysis and evaluation of lightweight ciphers: the prospective for IoT security. *Multimedia Tools and Applications.* 2018; 77: 18415-18449.

[8] F Nzanywayingoma, Y Yang. Efficient resource management techniques in cloud computing environment: Review and discussion. *TELKOMNIKA Telecommunication Computing Electronics and Control.* 2017; 15: 1917-1933.

[9] YAAS Aldeen, KN Qureshi. New trends in internet of things, applications, challenges, and solutions. *TELKOMNIKA Telecommunication Computing Electronics and Control.* 2018; 16: 1114-1119.

[10] J Kim and L Tong. Against Data Attacks on Smart Grid Operations: Attack Mechanisms and Security Measures Cyber Physical Systems Approach to Smart Electric Power Grid, SK Khaitan, JD McCalley, CC Liu. *Eds., ed Berlin, Heidelberg: Springer Berlin Heidelberg*. 2015: 359-383.

[11] P Kettunen, N Mäkitalo. Future smart energy software houses. *European Journal of Futures Research.* 2019: 7; 1.

[12] H Lei, B Chen, KL Butler-Purry, C Singh. Security and Reliability Perspectives in Cyber-Physical Smart Grids. *IEEE Innovative Smart Grid Technologies*. 2018: 42-47.

[13] A Kumar, A Agarwal. *Research issues related to cryptography algorithms and key generation for smart grid: A survey*. in 7th India International Conference on Power Electronics (IICPE). 2016: 1-5.

[14] S Chang, T William, W Wu, B Cheng, H Chen, P Hsu. *Design of an authentication and key management system for a smart meter gateway in AMI.* in IEEE 6th Global Conference on Consumer Electronics, Nagoya. 2017: 1-5.

[15] S Cho, H Li, BJ Choi. *PALDA: Efficient privacy-preserving authentication for lossless data aggregation in Smart Grids*. in IEEE International Conference on Smart Grid Communications, Venice. 2014: 914-919.

[16] G Qinghai. *Biometric authentication in Smart Grid.* in 2012 International Energy and Sustainability Conference, Farmingdale. 2012: 1-5.

[17] Z Fangming, Y Hanatani, Y Komano, B Smyth, S Ito, T Kambayashi. *Secure authenticated key exchange with revocation for smart grid*. in IEEE PES Innovative Smart Grid Technologies. 2012: 1-8.

[18] M Tavasoli, S Alishahi, M Zabihi, H Khorashadizadeh, AH Mohajerzadeh. *An efficient NSKDP authentication method to secure smart grid.* in IEEE International Conference on Smart Energy Grid Engineering Oshawa. 2017: 276-280.

[19] R Tabassum, K Nahrstedt, E Rogers, K Lui. *SCAPACH: Scalable Password-Changing Protocol for Smart Grid Device Authentication*. in 2013 22nd International Conference on Computer Communication and Networks, Nassau. 2013: 1-5.

[20] I Doh, J Lim, K Chae. *Secure Authentication for Structured Smart Grid System*. in 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Blumenau. 2015: 200-204.

[21] E Ayday, S. Rajagopal. *Secure, intuitive and low-cost device authentication for Smart Grid networks.* in IEEE Consumer Communications and Networking Conference. 2011: 1161-1165.

[22] K Cairns, C Hauser, T Gamage. *Flexible data authentication evaluated for the smart grid*. in IEEE International Conference on Smart Grid Communications, Vancouver. 2013: 492-497.

[23] J Choi, I Shin, J Seo, C Lee. *An Efficient Message Authentication for Non-repudiation of the Smart Metering Service*. in First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering, Jeju Island. 2011: 331-333.

[24] MM Fouda, ZM Fadlullah, N Kato, R Lu, and XS Shen. A Lightweight Message Authentication Scheme for Smart Grid Communications. *IEEE Transactions on Smart Grid*. 2011; 2: 675-685.

[25] Y Lee, E Kim, Y Kim, H Jeon, M Jung. A Study on Secure Chip for Message Authentication between a Smart Meter and Home Appliances in Smart Grid. in 2013 International Conference on IT Convergence and Security (ICITCS). 2013: 1-3.

[26] MC Muñoz, M Moh, T Moh. *Improving smart grid authentication using Merkle Trees.* in 20th IEEE International Conference on Parallel and Distributed Systems. 2014: 793-798.

[27] APD Nath, F Amsaad, M Choudhury, M Niamat. *Hardware-based novel authentication scheme for advanced metering infrastructure*. in IEEE National Aerospace and Electronics Conference (NAECON) and Ohio Innovation Summit, Dayton. 2016: 364-371.

[28] H Nicanfar, VCM Leung. *Smart grid multilayer consensus password-authenticated key exchange protocol*. in IEEE International Conference on Communications Ottawa, 2012: 6716-6720.

[29] N Saxena, BJ Choi. Integrated Distributed Authentication Protocol for Smart Grid Communications. *IEEE Systems Journal.* 2018; 12: 2545-2556.

[30] W Li, R Li, K Wu, R Cheng, L Su, W Cui. Design and Implementation of an SM2-Based Security Authentication Scheme with the Key Agreement for Smart Grid Communications. *IEEE Access.* 2018; 6: 71194-71207.

[31] X Li, F Wu, S Kumari, L Xu, AK Sangaiah, KKR Choo. A provably secure and anonymous message authentication scheme for smart grids. *Journal of Parallel and Distributed Computing.* 2017; 5: 112-121.

[32] K Mahmood, S Ashraf Chaudhry, H Naqvi, T Shon, H Farooq Ahmad. A lightweight message authentication scheme for Smart Grid communications in power sector. *Computers & Electrical Engineering.* 2016; 52: 114-124.

[33] D Abbasinezhad-Mood, M Nikooghadam. Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications. *Future Generation Computer Systems.* 2018; 84: 47-57.

[34] M. Nabeel, X. Ding, S.-H. Seo, and E. Bertino, "Scalable end-to-end security for advanced metering infrastructures," *Information Systems,* vol. 53, pp. 213-223, 2015.

[35] D. N. Abbasinezhad-Mood, Morteza, "Design of an enhanced message authentication scheme for smart grid and its performance analysis on an ARM Cortex-M3 microcontroller," *Journal of Information Security and Applications,* vol. 40, pp. 9-19, 2018.

[36] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Generation Computer Systems,* vol. 81, pp. 557-565, 2018.

[37] S. Câmara, D. Anand, V. Pillitteri, and L. Carmo, "Multicast Delayed Authentication For Streaming Synchrophasor Data in the Smart Grid," *IFIP advances in information and communication technology,* vol. 471, pp. 32-46, 2016.

[38] H. M. N. Al Hamadi, C. Y. Yeun, and M. J. Zemerly, "A Novel Security Scheme for the Smart Grid and SCADA Networks," *Wireless Personal Communications,* vol. 73, pp. 1547-1559, 2013.

[39] M. Bayat, M. B. Atashgah, and M. R. Aref, "A Secure and Efficient Chaotic Maps Based Authenticated Key-Exchange Protocol for Smart Grid," *Wireless Personal Communications,* vol. 97, pp. 2551-2579, 2017.

[40] M. Wen, J. Lei, Z. Bi, and J. Li, "EAPA: An efficient authentication protocol against pollution attack for smart grid," *Peer-to-Peer Networking and Applications,* vol. 8, pp. 1082-1089, 2015.

[41] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An Efficient Merkle-Tree-Based Authentication Scheme for Smart Grid," *IEEE Systems Journal,* vol. 8, pp. 655-663, 2014.