Energies **2015**, *8*, 11883-11915; doi:10.3390/en81011883

OPEN ACCESS

energies

ISSN 1996-1073

www.mdpi.com/journal/energies

Review

State of the Art Authentication, Access Control, and Secure Integration in Smart Grid

Neetesh Saxena [1,2,*] and Bong Jun Choi [1,2,*]

[1] Department of Computer Science, State University of New York (SUNY) Korea, 119 Songdo, Moonhwa-ro, Yeonsu-Gu, Incheon 406840, Korea

[2] Department of Computer Science, Stony Brook University, New York, NY 11794, USA

***** Authors to whom correspondence should be addressed;
E-Mails: mr.neetesh.saxena@ieee.org (N.S.); bjchoi@sunykorea.ac.kr (B.J.C.);
Tel.: +82-32-626-1216 (N.S. & B.J.C.); Fax: +82-32-626-1559 (N.S. & B.J.C.).

Academic Editor: Neville Watson

Received: 16 July 2015 / Accepted: 12 October 2015 / Published: 21 October 2015

Abstract: The smart grid (SG) is a promising platform for providing more reliable, efficient, and cost effective electricity to the consumers in a secure manner. Numerous initiatives across the globe are taken by both industry and academia in order to compile various security issues in the smart grid network. Unfortunately, there is no impactful survey paper available in the literature on authentications in the smart grid network. Therefore, this paper addresses the required objectives of an authentication protocol in the smart grid network along with the focus on mutual authentication, access control, and secure integration among different SG components. We review the existing authentication protocols, and analyze mutual authentication, privacy, trust, integrity, and confidentiality of communicating information in the smart grid network. We review authentications between the communicated entities in the smart grid, such as smart appliance, smart meter, energy provider, control center (CC), and home/building/neighborhood area network gateways (GW). We also review the existing authentication schemes for the vehicle-to-grid (V2G) communication network along with various available secure integration and access control schemes. We also discuss the importance of the mutual authentication among SG entities while providing confidentiality and privacy preservation, seamless integration, and required access control with lower overhead, cost, and delay. This paper will help to provide a better understanding of current authentication, authorization, and secure integration issues in the smart grid network and directions to create interest among researchers to further explore these promising areas.

Keywords: smart grid (SG); authentication; authorization; vehicle-to-grid (V2G); privacy

1. Introduction

The smart grid (SG) refers to a revolutionary power delivery system with several notable features like balancing supply-demand, monitoring inflicted loads, and integrating distributed and renewable energy that provides electric power to the consumers in a more efficient, reliable, and stable manner [1]. It is expected that in the future smart grid, the demand response (DR) technology will enable consumers to efficiently use and pay for the required electricity by reducing or shifting the usage during peak hours in order to maintain the demand-supply balance in the electric grid [2]. Similarly, monitoring dynamic loads and the integration of distributed and renewable energy enable the maximum utilization of sharing energy resources and efficient management of the power requirement in the system. In the traditional power grid, the electricity is delivered to the consumers with one-way flow. On the other hand, the SG provides a two-way electricity and information flow between the supplier and the consumers of electric power. To enable these features, information exchange between different components of the smart grid is necessary. Generally, a neighboring gateway (NAN-GW) collects electricity consumption information from smart meters (SMs) and sends it to the CC of the nearest substation through remote terminal units (RTUs) via wireless networks or wired link [3]. An overview of the smart grid network architecture is illustrated in Figure 1.

Security and privacy issues are one of the most important challenges faced by the future smart grid. These issues include lack of mutual authentication between communicated entities, risk of various cyber-attacks, unauthorized access to the resources, revealing of device's and network's private information to the communicating entity, *etc.* The requirements of the SG network are different from that of the traditional information network. Most of the information network deals with confidential information. Hence, they prioritize the confidentiality first then the integrity, and least the availability of information. On the other hand, the SG network is primarily responsible for the availability of information, as well as the integrity protection of the message, and then the data confidentiality and privacy [4].

Before allowing any entity to have an access over a network and its associated resources, it is required to authenticate the entity, which may be a device or a user, and then verify the authorization and control policy based on the entity's identity. Authentication verifies the user's identity while the authorization verifies whether the user has valid permissions to access the requested resource. Authentication is one of the key challenges in the SG communication. The modern power grid makes use of supervisory control and data acquisition (SCADA) systems with communication protocols. Unfortunately, protocols used in these systems are often vulnerable to man-in-the-middle (MITM) attacks, replay attacks, impersonation attacks, and the cryptographic keys used in various devices of the system might be compromised [5]. Connecting the SCADA system with other communication networks (e.g., Internet) significantly increases security and privacy threats [6], and is one of the major challenges in many countries around the globe [7]. Many researchers are actively working to build secure and efficient authentication protocols in order to solve various communication challenges, and security and privacy

issues exist in the SCADA [8,9], home SG environment [10], security management and the SG operation [11], message delivery in the SG [12], and vehicle-to-grid (V2G) systems [13].

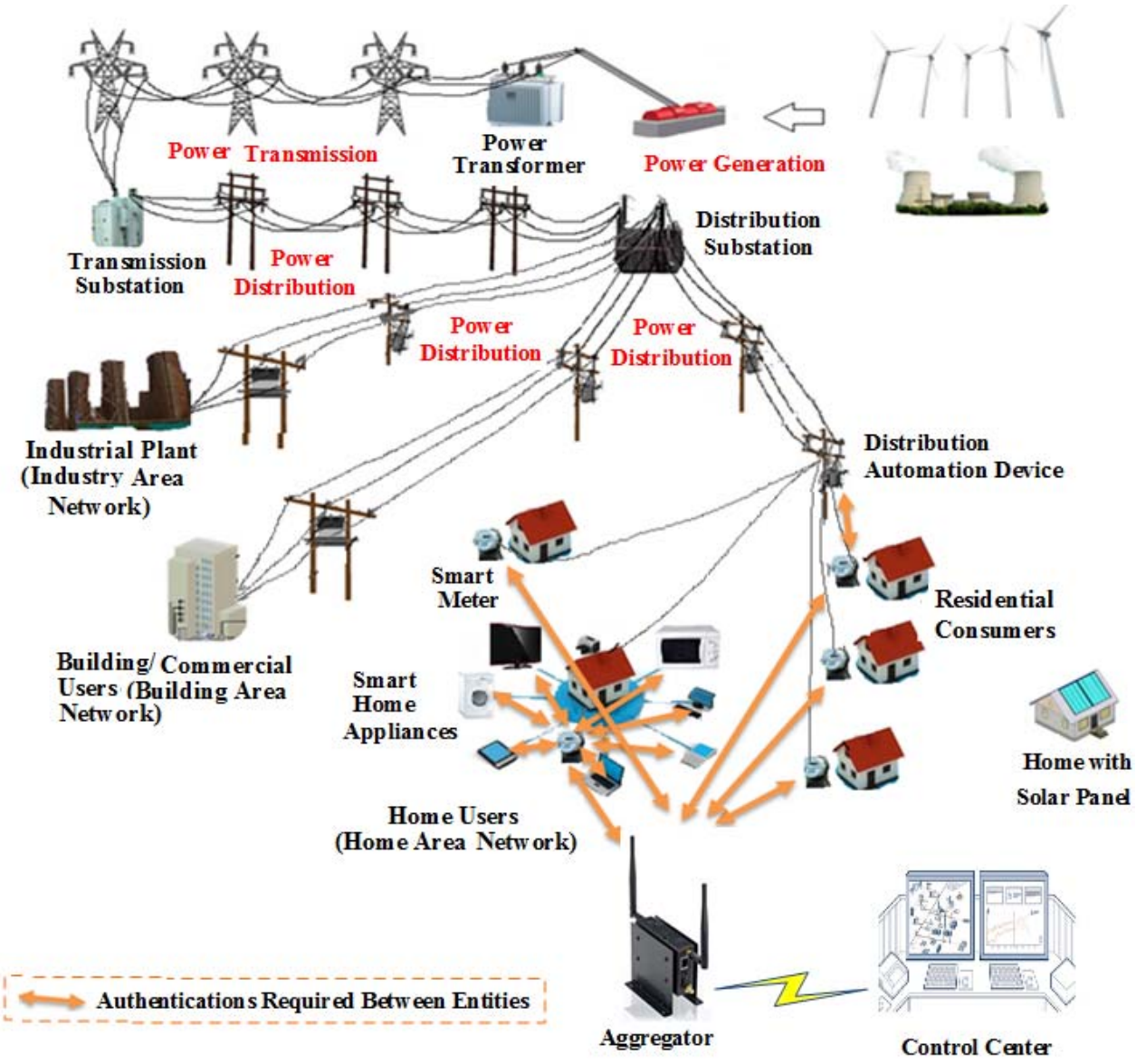

Figure 1. Overview of smart grid (SG) network architecture.

Secure integration in the SG network is also strongly required as various modules and entities receive data input from different other modules and send data output to several modules and entities. In such scenarios, maintaining data integrity and the secure integrated communication among various entities and control modules are necessary. Data integrity refers to maintaining accuracy and consistency of the data in the database or when transmitted over the network, while secure integrated communication allows a reliable real-time information exchange within the system. Data integrity can be maintained by using either hash functions, such as SHA1, SHA256, *etc.*, in which variable length input is converted into a fixed length hash code, or by the message authentication code (MAC) functions, such as cipher-based message authentication code (CMAC), hash-based message authentication code (HMAC), one-time MAC, *etc.*, where variable length input with a secret key is mapped to a fixed length MAC code. MAC functions provide data integrity as well as authenticity of the message.

Various communication technologies have been proposed to support integration of SG entities. A comparison chart among various wireless technologies, such as microwave, worldwide interoperability for microwave access (WiMAX), mesh, long term evolution (LTE), 3G cellular, wireless local area network (WLAN), and Zigbee is presented in [14]. Wireless technologies are proposed for backhaul transport in SCADA (Microwave, WiMAX, and LTE) and advanced metering infrastructure (AMI) (Microwave, WiMAX, LTE, mesh, and 3G cellular). Microwave can also be used for backbone transport in SCADA and AMI. Further, demand response can be implemented using microwave, WiMAX, LTE, and mesh, while the distribution automation can be managed by microwave and mesh technologies. WLAN and Zigbee can be used to manage home area network (HAN), smart meter, and home automation. Power line communication (PLC) is also an adopted communication technology in smart meters. In some applications, such as automated meter reading (AMR), street light control, and EV charging, narrowband PLC has captured lot of attention due to its longer range up to several kilometers. On the other hand, broadband PLC has proposed to use in the last mile technology of various applications, like Internet access and home networking and control [15]. The obvious advantage using PLC is the widespread availability of electrical infrastructure and a full control over the physical medium without depending on third party providers, such as telecommunication companies or cellular operators [16]. Although PLC connection has several advantages over the wireless connection, the quality of the connection still depends on the domestic electrical system. Improper wiring and circuit breakers in between the connected cables can negatively affect the performance, and can cause connection interruptions.

Many researchers proposed their schemes for the SG and V2G networks in consideration with vehicular ad-hoc network (VANET) and radio frequency identifier (RFID) technology. However, the communication techniques used in VANET and RFID are not directly applicable to the V2G as the entities of these networks behave differently, which are summarized in Tables 1 and 2. The primary concerns of VANET are vehicle safety and optimization of route and traffic flow. On the other hand, the V2G system focuses on battery charge state of electric vehicles (EVs) and management of the availability of parking slots. In the V2G, EVs use charging stations (CSs) according to their ranking and rates of charging, while in the VANET, the vehicles focus on their consumption and emissions [17]. Many researchers proposed RFID-based authentication schemes for the SG network, such as an untraceable server-independent scheme by Wang and Ma [18], to prevent tracing attacks, a mobile RFID-based scheme by Vaidya *et al.* [19], for the SG network, and ADDRESS Box scheme by Rodriguez-Mondejar *et al.* [20], to manage the home load. In the RFID-based systems, coexistence proof mainly presents the simultaneous scanning of multiple tags at the same time and place by a reader [21,22]. However, this approach cannot be directly applied in the V2G as it requires a central proof initiator entity. However, in the V2G distributed network, there is no such entity as all the involved entities (EVs) are of the same role. In order to sort out this issue, Liu *et al.* [22] presented the simultaneous existence of multiple vehicles as a whole group is verified by an aggregator (AG), while "WINSmartEV" project tracks-on the charging usage and the preference of EVs by a RFID-based scheme [23]. Thus, researchers must first observe the difference of the V2G system with other wireless networks when they design a protocol for the V2G system.

Table 1. Vehicular ad-hoc network (VANET) *vs.* vehicle-to-grid (V2G). EV: electric vehicle.

Role	VANET	V2G
Vehicle priority	Vehicle safety	EV's battery charge state
Management	Route optimization, traffic management	Availability of parking slots
Power focus	Consumptions and emissions	Charging according to rank and rates

Table 2. Radio frequency identifier (RFID) *vs.* V2G.

Role	RFID	V2G
Central role	Proof initiator, one central entity	Distributed network, no entity with central role
Communication technique	Coexistence proof technique	Cannot use coexistence proof technique directly

In this paper, we provide a comprehensive overview of various security and privacy issues in the SG with focuses on mutual authentication, access control, and secure integration. The existing survey paper by Liu *et al.* [24] provides a comprehensive overview on device issues, networking issues, dispatching and management, and anomaly detection. Different from the existing survey, we also take into account the authentication issues in the HAN and the V2G network. Furthermore, we present the state of the art solutions to secure access control and integration in the SG. The following is a summary of our contribution in this work:

(1) We organize the requirements of mutual authentication and privacy preservation among various SG entities (devices, user, and network) and highlight the objectives for developing an efficient and secure authentication protocol for the SG.
(2) We perform a critical analysis of the existing work. We observe that there is no such protocol that provides mutual authentication among HAN environments, energy providers (EP) and GW, and AMI network.
(3) We discuss the V2G communication (using DR technology) requirement in comparison with VANET and RFID technology. Further, we perform a careful evaluation of existing literature in terms of efficiency and security.
(4) We also summarize and explain the secure integration and authorization that is essential to further enhance the secure communication in the SG system.

The rest of the paper is organized as follows: Section 2 discusses the requirement of mutual authentications in the SG network along with the existing authentication protocols. Section 3 discusses various available protocols for the V2G network. The existing authentication protocols considering authorization and integration in the SG are presented in Section 4 and Section 5, respectively. Section 6 highlights the current issues and future directions. Finally, Section 7 provides the conclusion of this work.

2. Authentication in the Smart Grid (SG) Network

Authentication is the process of proving an identity to a given system, including users, applications, and devices [7]. In a typical SG network, there are millions of devices interacting among each other. For information exchange in the SG network, involved entities must be bi-directionally authenticated.

2.1. Authentication Types in the Smart Grid (SG) Network

Mutual authentications in the distributed SG network can be categorized as follows:

(1) Device-to-device (e.g., SM-to-GW/AG, GW-to-RTU, RTU-to-CC);
(2) Device-to-network (e.g., vehicles and SG network in V2G system, home appliances (HAs) and HAN network);
(3) User-to-network/device (HAs and network interaction).

2.1.1. Device-to-Device Authentication

In the smart home environment, various smart devices and HAs communicate with each other via HAN. Secure communication among devices is a vital for SG security. The authentication server (AS) of the SG system must authenticate all the associated SMs of HAN. Apart from this, the SMs and the other HAs must be secured from various attacks such as impersonation, data forgery attack, *etc.* A couple of identity-based authentication and public key infrastructure (PKI) mechanisms are proposed by Lee *et al.* [25] to offer mutual authentication between smart devices. However, the security analysis of the scheme is not discussed.

2.1.2. Device-to-Network Authentication

A mutual authentication between all the devices and the HAN is required. During an authentication, the cryptographic key of each device must be protected against any theft, attack, or misuse over the network. Current approaches of protecting cryptographic keys require user interaction, which is again a drawback or a loophole in the SG security system if the bi-directional authentication is not provided between the user and the system. Paverd and Martin [26] designed a system, which provides hardware security to the cryptographic key of specific device using dynamic root of trust for measurement (DRTM) late-launch functionality.

2.1.3. User-to-Network/Device Authentication

Users play an important role when initially setting up the devices and the network. It is important as the malicious devices and forged connections can reveal the private information of users. This can be achieved by setting up a user password to each device and the network so that users have control over these entities. Vaidya *et al.* [19] proposed an authentication scheme for a mobile RFID (radio frequency identification)-based SG network, but the scheme generates memory overhead and incurs additional cost.

2.2. Authentication Protocols

In this subsection, we discuss the challenges and desired objectives of authentication protocols in the SG network, and the existing solutions with their pros and cons towards meeting these objectives.

There are some standardized protocols exist in the literature for the SG, which support authentication process, such as device language message specification/companion specification for energy metering (DLMS/COSEM) for the AMI network and OpenADR for the demand response program. The DLMS is an application layer communication protocol and COSEM is a data model. Both together provide an

interface model for metering applications belonging to IEC 62056 standards, such as electricity [27]. Basically, three authentication procedures are used by DLMS/COSEM, *i.e.*, no security (public access with no identity verification), low level security authentication (server identifies client by password), and high level security authentication (mutual identification) with exchange challenges. DLMS/COSEM specifies its own security services (authentication and confidentiality), which may not necessarily be an advantage as it is restricted to symmetric key encryption. If smart meters combine their measured data with digital signatures, the meters would need asymmetric keys that can be used in secure sockets layer/transport layer security (SSL/TLS). However, DLMS/COSEM does not allow the use of TLS/SSL. The support for asymmetric encryption is done by the European committee for electro-technical standardization CENELEC TC-13 [28]. Further, DLMS/COSEM protocol is suitable only for the AMI network of the smart grid in which a large number of smart meters are involved. Similarly in demand response, OpenADR, a standard development effort supports authentication based on public key cryptography with exchange of certificates [29]. This standard maintains a hierarchy of certified authorities and requires a PKI to use three-tier PKI technology, which ultimately results in high cost.

In addition, some standardized authentication protocols also exist, such as remote authentication dial-in user service (RADIUS) and diameter protocols for the 2G, 3G, and 4G cellular networks. RADIUS is used to provide remote user authentication and accounting in 2G, 3G, and 4G networks, and WLAN interworking and Wi-Fi offload situations [30]. It provides centralized services and maintains a central database. However, the smart grid requires decentralized solutions as a single-point-of-failure can massively affect the centralized system. Furthermore, RADIUS has poor scalability and uses the user datagram protocol (UDP), which does not provide reliable data transfer. Therefore, it is not suitable for the smart grid where the availability of information is extremely important. Further, diameter protocol is an authentication, authorization, and accounting protocol used in networking, which supports transmission control protocol (TCP) instead of UDP. However, it does not provide transition support and application level congestion control [31]. Additionally, its supported capabilities are sometimes more expansive. Diameter implementation supports peer authentication between communication endpoints using a pre-shared key. Hence, it brings some key management issues and is not suitable for large systems, such as the smart grid. Further, RADIUS and diameter protocols do not directly protect against denial-of-service (DoS) attacks carried out by flooding the target equipment with bogus traffic. In the case of V2G network having mobile vehicles, a modified diameter with scalable asymmetric cryptographic support may be used to prevent against well-known attacks.

Unlike the other communication systems, the SG system requires timely authentication. The proposed authentication protocol in the SG network should be cost effective and efficient in terms of overhead as the authentication process happens to be frequently executed among billions of the entities (users, devices, *etc.*). Furthermore, if the system is not secure against various security attacks and failures, the adversary can compromise the system resources and can affect the authentication process. This may happen if the adversary is able to drop some information or control message that is needed to complete the authentication process. In this case, even if the authentication is fast and efficient, it will never complete. Since there are billions of entities involved in the SG network, installation and uninstallation of the devices in a secure and authentic manner requires trust among these entities. In other words, the device, as well as the engineer, must be verified by the controller in the SG network when these operations are performed that may require trusted hardware setup.

A secure and efficient buffer management may be required at the AGs in the SG network, which are responsible for receiving a large volume of information from the various SMs, and at the memory stack of controlling devices in the SCADA system to prevent buffer overflow-based DoS attacks. Furthermore, the confidentiality is strongly required along with the privacy preservation of the information. In the SG network, we need to hide the identity and other relevant information of the devices, such as SMs and EVs, from the other entities. For example, a compromised AG may breach the privacy of the SM and can harm/mislead the user by tracing its pattern and energy consumption details. Similarly, some personal information, such as consumed units in every time slot, need to be encrypted over the network when providing it to an untrusted entity, such as an AG.

Moreover, the performance of the system is important for satisfying the system requirements as well as supporting a huge number of devices. The evaluation metrics comprise of communication and computation overheads generated by the protocol, execution time of the protocol, delay at intermediate entities, and message transmission time. A solution is scalable, if it can support the authentication for a huge number of devices and can be further extended if required, with reasonable execution time and low overheads. Timing accuracy in the SG varies from few microseconds to few seconds depending upon different communication scenarios among various entities. In power communication networks, such as smart grid, reliability, security, and real-time message delivery have higher priorities than providing high throughput. Therefore, latency requirement is much more important in smart grid system [32]. The communication latency needed for the transmission system protection is in the order of a few milliseconds [33] and authentication time varies up to few seconds [1]. Furthermore, the computation complexity of various functions used in the protocol should be as low as possible to be scalable.

The security and performance objectives for developing a secure and efficient authentication protocol with secure network environment in the SG network end-to-end at power distribution among various entities, such as users, devices, CC, utility provider, *etc.*, are listed as follows:

Obj-1: Low execution and protocol delay;
Obj-2: Low computational and storage cost;
Obj-3: Low communication and computation overhead;
Obj-4: Resistance to attacks and failures;
Obj-5: Trust among SG entities;
Obj-6: Buffer management;
Obj-7: Confidentiality and privacy.

2.2.1. Obj-1: Low Execution and Protocol Delay

The authentication protocol in the SG must be fast enough and should use the system resources as less as possible. In certain cases (such as IEC 61850 Protection Class 2/3), multicast messages in the transmission substation network should be delivered within 4 ms as mentioned by Wang *et al.* [34] and Khurana *et al.* [35]. Since several mutual authentications must be performed among various SG entities in a distributed manner, the protocol execution time and the end-to-end delay are critical in the SG system. Fast authentication with low delay improves the overall efficiency of the system and enables the computations under the threshold. Sule *et al.* [36] made a change in the message authentication protocol by Fouda *et al.* [37] and used a variable MAC between the AMI devices and the controller nodes instead

of HMAC to reduce the time for verification. However, it involves only HAN-GW and BAN (building area network)-GW communication. Lee *et al.* [38] analyzed the security requirements in the SG environments and proposed a certification structure and a chip design for an efficient message authentication between a SM and the HAs. Further, Tsang and Smith [39] presented a bump-in-the-wire (BITW) solution, which maintains security during time-critical communications over bandwidth-limited serial links between the devices in the legacy SCADA system. Their solution guarantees data authenticity and freshness, and achieves low latency. A time-valid one-time-signature (TV-OTS) as a data authentication protocol for potential use in the SG applications is proposed to enable secure multicast, low latency, and sufficient lifespan even at high data rates [40].

2.2.2. Obj-2: Low Computational and Storage Cost and Obj-3: Low Communication and Computation Overhead

Since there are numerous entities involved in the SG system, computation and storage costs are big issue. As well, communication and computation overhead are also a major concern, as it will affect the bandwidth requirement and the overall efficiency of the SG system. In order to accomplish these objectives, multicast authentication can be used in various applications of SG, such as wide area network (WAN) security, demand-response protection, substation security management, *etc.* However, the existing multicast authentication solutions are not suitable for the SG due to the requirements of fast authentication (low delay) and small computation and storage costs. The schemes relying on per-packet signature and verification introduce substantial computation cost. In this direction, Li and Cao [41] have introduced a one-time signature scheme for multicast authentication in the SG, which reduces the storage cost by eight-times and lowers signature size by 40% as compared to HORS by Reyzin and Reyzin [42], and prevents message forgery attacks. After that, a batch verification and signature authorization protocol that generates low overhead and provides fault tolerance was proposed by Li *et al.* [43]. However, the protocol does not provide authentication among SM, HAN, and HAs. Nicanfar *et al.* [44] proposed a scheme that provides the mutual authentication between the SM and the AS of the SG. This scheme is based on an identity-based PKI and reduces the exchanged packets during authentication, but, generates a large overhead. Zigbee authentication protocol also has some security weaknesses that were overcome by Im and Oh [45]. This scheme reduces the number of key distribution messages per node. A matrix based homomorphic hash is used by Kim and Heo [46] to decreases the amount of computations at SM as compared to the exponential operation based hash. Further, a scheme presented by Lu *et al.* [47] reduces the pairing operations in aggregation and verification to improve the computational efficiency in the SG network. Many schemes are not well suited in the SG due to their large key sizes. In order to match this requirement, a one-time signature scheme that uses fewer resources at the receiver with modest signature sizes and lower sender computations is proposed by Katti *et al.* [48].

2.2.3. Obj-4: Resistance to Attacks and Failures

Due to having IP-based communication networks, (e.g., Internet), the SG networks are likely to be challenged by a variety of malicious attacks, such as replay, MITM, traffic analysis, impersonation, and DoS. There are certain situations in the SG where the multicast message must be authenticated and its integrity is protected so that the involved entity can know that the received message has come from a

legitimate source and has not been tampered over the network. This can happen when phasor measurement units (PMUs) measure voltage and current in a WAN and multicast these parameters to the CCs [49]. Another situation may arise when utility centers multicast demand-response commands to different home appliances and request them to turn-off power during the maintenance or during peak hours of power consumption [50]. In the absence of authentication, an attacker can easily tamper with the message, replay the previous message, or send a fake message to the device that results in an inconsistent state of the SG.

In this paper, we consider four broad categories of cyber-attacks in the smart grid communication: interrupting availability, violating integrity, compromising confidentiality, and compromising privacy [32,51]. Attacks interrupting availability include DoS attack, replay attack, and delay, block or corrupt the communication in the SG. Attacks violating integrity include modification of data exchanged by malicious user and false data injection attack in the SG. Attacks compromising confidentiality in the SG include unauthorized information from network resources, MITM attack, impersonation attack, and attacks on aggregation. Attacks compromising privacy in the SG include user tracing attack, identity theft attack, and attacks on billing systems.

Various researchers have proposed solutions to resist the SG system against different attacks. We discuss some recent solutions in this paper. Oh and Kwak [52] proposed a scheme that provides mutual authentication between the SM and the data concentration unit (DCU). They claimed that the scheme provides confidentiality and integrity to the transmitted messages and disallows impersonation and MITM attacks between SM and DCU. However, their scheme neither discusses the generated overhead nor provides a complete authentication in HAN. Further, in order to prevent these attacks, Fouda *et al.* [37,53] presented a light-weight authentication scheme, which is based on the Diffie-Hellman key exchange protocol and a hash-based MAC. This scheme provides the mutual authentication between only the HAN-GW and the BAN-GW. Chan and Zhou [54] proposed a two-factor cyber-physical device authentication protocol in order to prevent cyber-physical attacks in the SG. Their protocol is a combination of contextual factors based on physical connectivity and the conventional authentication factor in the challenge-response protocol. Their solution provides assurance on digital identity of a device as well as its controllability in the physical domain. Recently, Li *et al.* [55] proposed an authentication scheme for the SG system that protects against replay, injection and message modification attacks, by using a Merkle hash tree technique for secure SG communication. However, only a scenario between the HAN and the NAN is considered. Three different authentication mechanisms for the devices in the HAN between gateway—smart meter, smart appliances—HAN, and transient devices—HAN are proposed by Ayday and Rajagopal [56]. However, security and overheads of these approaches are not discussed. A robust and efficient protocol based on the elliptic curve cryptography is proposed by Zhang *et al.* in [57], to achieve mutual authentication and key agreement between the substation and the smart appliances.

Further, a solution for substation-level authentication using server-aided verification was provided by Vaidya *et al*. [58], in which IEDs and other resource-constrained devices can be authenticated by any remote users with the help of the substation controller (SSC). Unfortunately, this scheme is vulnerable to replay attacks and message integrity can be easily violated. Authentication and key management protocols for unicast and multicast communications are discussed by Nicanfar *et al.* [59]. These protocols provide resistance against various security attacks and generate low overheads. Since the

modern password-based authentication mechanisms are inadequate, an approach using biometrics is proposed by Gao [60] to authenticate users accessing the SG. Moreover, a scalable password-changing protocol SCAPACH for the device authentication is proposed by Tabassum *et al.* [61] based on asymmetric, as well as symmetric, key cryptography. It employs physical per-operator, per-pole-device information, and changeable secret salts to generate new unique passwords and secret keys every time a pole device is accessed.

2.2.4. Obj-5: Trust Management

Since control systems in the SG are distributed in nature, the establishment and the maintenance of the chain of trust is important [7]. During authentication and communication, the trust among the SG entities such as user-to-network, device-to-network, and device-to-device should be maintained. This can be achieved by introducing a protocol with a trust element or verifying the identity/certificate of the entity, e.g., device attestation.

Metke and Ekl [62] stated that a strong authentication technique is a requisite for all users and devices within the SG network. It is expected that in the near future, the current protocols may not be fast enough requiring a scalable key and trust management system. A Diffie-Hellman-based security aggregation scheme for collecting data, proposed by Kursawe *et al.* [63], generates lower computation and communication overhead, but, does not consider SMs authentication. Recently, Fadul *et al.* [64] discussed the trust management toolkit, which uses network-flow techniques and reputation-based trust to improve the SG protection system that can work well in the presence of an untrusted SG entity.

2.2.5. Obj-6: Buffer Management

According to the study of buffer-flooding attacks by Dong *et al*. [65], on distributed network protocol (DNP3)-based SCADA networks with actual hardware and software, the present SCADA system is quite vulnerable to DoS attacks. In a scenario where the messages received by SMs have some predefined size, there is a possibility of buffer overflow attacks that enables an adversary to modify system parameters present in the memory stack [66]. The buffer or the memory stack that stores various parameters/variables related to protocol must be secured against buffer-related attacks, such as DoS attack (sends flood to the SG entity with fake command messages and drops the original authentication commands), overflow attack (stop sending the messages to recipient if overflow occurs), *etc.*, so that the authentication process is not affected. Choi *et al.* [67] analyzed the buffer overflow attack detection and its affected parameters. Wang *et al.* [34] proposed a scheme based on one-time signature and hash chaining, which provides fast signing and verification of messages and buffer-free data processing. Further, Tsang *et al.* [39] applied a MAC to the byte streams with less buffering.

2.2.6. Obj-7: Confidentiality and Privacy

Data confidentiality is required when we need to send some information in unreadable format over the network. For example, the AMI is accountable of collecting and transferring data and commands among the central controllers, AGs, and SMs. All the SMs send their data to the AG in the encrypted form so that the untrusted AG can no longer know the exact metering data values received from each

SM. In authentication schemes, the sender needs to send a secret key or some number value to the recipient in a secure manner. The AMI is also prone to many privacy concerns. The privacy of the customer in terms of power usage, billing, and other information must be preserved during the authentication along with the privacy issues related to the SMs, such as data collection, transmission and other information. We also need to protect (hide) the actual identity of each device, such as SM, over the SG network so that the adversary cannot keep a track. Many times, it requires that the AG or CC should not know some specific information of the home users. In such situation we should implement both, privacy (to hide the actual SM/user identity over the network) as well as confidentiality (to send secret key or other parameter to the recipient over the SG network). An authentication scheme must overcome these privacy concerns and generate as little overhead as possible among AMI entities. In fact, we need to provide authentication, integrity, and confidentiality services together for a secure authentication scheme. In this direction, Bekara *et al.* [68] proposed an identity-based authentication protocol, which offers source authentication, data integrity, and non-repudiation services. This scheme also preserves customers' privacy in AMI. However, it does not justify other expected protocol capabilities, including overhead, cost, and efficiency. Yan *et al.* [69] presented an integrated authentication and confidentiality (IAC) protocol, which provides mutual authentication between the SM and the AMI network, and enables data privacy, integrity, confidentiality, and trust services. The IAC scheme performs better in terms of packet loss and end-to-end delay. Although, it also proposes a hop-by-hop data aggregation using a network routing backbone [70], which is a deciding factor for information route optimization [71], it does not provide a full authentication in the HAN-AMI environment. Sikora [72] proposed an open metering system (OMS) security protocol for secure SM communication, which employ a mutually-authenticated SSL protocol also in the local metrological network using an additional authentication and fragmentation layer (AFL).

In order to prevent from revealing the electricity usage patterns, a privacy-preserving scheme using a tamper-resistant device and pseudo identities is adopted by Chim *et al.*, in [73]. However, the attack analysis and overheads computations are not performed. Recently, a privacy-preserved scheme is proposed by Chim *et al.*, that does not allow the CC (power operator) to know which user has made the request using more/less power until the power is actually used [74]. Cho *et al.* [75] proposed an efficient privacy-preserving authentication for lossless data aggregation scheme (PALDA) that provides privacy preservation when collecting total sum of energy usage for a group of smart meters and when collecting individual energy usage of individual smart meters for a desired period of time. However, security analysis of the scheme is not discussed in detail.

Based on these objectives, we evaluate existing protocols in terms of security and efficiency. Table 3 summarizes the existing authentication protocols.

Table 3. Summary of existing authentication protocols/schemes. SCADA: supervisory control and data acquisition; HMAC: hash-based message authentication code; PMU: phasor measurement units; IED: intelligent electronic device; RTU: remote terminal units; PKI: public key infrastructure; HAN: home area network; BAN: building area network; GW: network gateways; SMs: smart meters; SSC: substation controller; EP: energy providers.

Protocols	Security and Performance Objectives							Involved Entities in the Protocols/Schemes	Description (Pros & Cons)
	1	2	3	4	5	6	7		
Tsang *et al.* [39]: (2008)	√	-	-	-	-	√	-	SCADA	*Pros:* low end-to-end communication latency and buffering by constructing a HMAC based bump-in-the-wire (BITW) secure solution within timing constraints. *Cons:* higher latency than some of the existing solutions.
Wang *et al.* [34]: (2009)	-	-	-	-	√	√	-	PMU, relay	*Pros:* fast signing/verification by combining one-way hash chains with time valid one-time signature scheme, avoid frequent public key distribution, and buffer-free data processing as one-time signature is used. *Cons:* relatively large public key of size 8KB to 10KB and need synchronization among entities.
Metke and Ekl [62]: (2010)	-	-	-	-	√	-	-	Certified authority (CA), trust anchor (TA), security server, IED, RTU	*Pros:* scalable key support and trust management; device attestation prevents the system against malicious activities. *Cons:* high cost from using PKI; upgrades in SG require significant dependence on distributed intelligence and broadband communication capabilities.
Fouda *et al.* [37]: (2011)	-	√	√	-	-	-	-	HAN-GW, BAN-GW	*Pros:* achieves mutual authentication, low storage cost and overhead by establishing a shared session key between SMs with Diffie-Hellman exchange protocol and a hash-based authentication code. *Cons:* long execution time for a large number of messages, the delay is around 11 s or 140 SMs per BAN.
Li and Cao *et al.* [41]: (2011)	-	√	-	√	-	-	-	SCADA	*Pros:* signature scheme with low signature size reduces storage cost; limited storage is needed for home appliances and field devices; computation cost is manageable as computations can be flexibly allocated to the sender or receiver based on their computing resources; secure against message forgery attacks. *Cons:* has large public key size and requires 7168 one-way hash functions; may not be cost effective for low computation process.

Table 3. *Cont.*

Protocols	Security and Performance Objectives							Involved Entities in the Protocols/Schemes	Description (Pros & Cons)
	1	2	3	4	5	6	7		
Kursawe *et al.* [63]: (2011)	-	-	√	-	-	-	-	SM, AG	*Pros:* privately compute aggregate meter measurements; allowing for fraud and leakage detection; individual meter reading privacy preservation; low computation and communication overhead. *Cons:* large number of keys is used; changing the meter group requires expensive re-keying.
Vaidya *et al.* [58]: (2011)	-	√	√	-	-	-	-	IED, substation controller (SSC) server	*Pros:* lightweight solution using server-aided verification mechanism; efficient for the remote access to the IEDs. *Cons:* does not defeat some of the security attacks.
Nicanfar *et al.* [59]: (2011)	-	-	√	√	-	-	-	SM, AG, security associate (SA)	*Pros:* presents authentication and key management protocols that defeat security attacks and incur lower overhead by generating and broadcasting only one function periodically by the server. *Cons:* large number of keys is generated and computed.
Sule *et al.* [36]: (2012)	√	-	-	-	-	-	-	HAN-GW, BAN-GW	*Pros:* a variable length fast message authentication code between AMI devices and collector nodes is used that reduced verification time. *Cons:* not efficient for a large number of HAN-GW as compared to batch verification approach. However, HAN-GW can wait and combine several messages together to have single tag and send it across to BAN-GW.
Li *et al.* [43]: (2012)	-	√	√	-	-	-	-	NAN, SM	*Pros:* authentication with data aggregation (AG signatures in a batch) provides fault tolerance and generates low overhead. *Cons:* the process is time consuming that involves deploying signature aggregation, batch verification and signature amortization.
Oh and Kwak [52]: (2012)	-	-	-	√	-	-	√	SM, concentration unit (DCU)	*Pros:* provides mutual authentication and session key establishment between the smart meter and DCU; secure against impersonation, MITM, providing message confidentiality and integrity. *Cons:* significant computational overhead.
Bekara *et al.* [68]: (2012)	-	-	-	-	-	-	√	SM, HAN-GW, HA, EP	*Pros:* certificateless Identity-based and asymmetric key cryptography-based protocol provides integrity, non-repudiation, users' privacy. *Cons:* generates high overhead; ECDSA signature scheme is used while other more efficient schemes are available in the literature.

Table 3. *Cont.*

Protocols	Security and Performance Objectives							Involved Entities in the Protocols/Schemes	Description (Pros & Cons)
	1	2	3	4	5	6	7		
Choi *et al.* [67]: (2012)	-	-	-	-	-	√	-	Sensors, actuators, IED	*Pros:* effective detection process of decision tree algorithms for buffer overflow attack using the Waikato environment for knowledge analysis (WEKA). *Cons:* buffer is used when traffic stopped; SG attacks are not considered.
Gao [60]: (2012)	-	-	-	√	-	-	-	Users in the smart grid	*Pros:* a privacy-enhanced method of applying fingerprint in biometric authentication improves the security of users accessing to the SG. *Cons:* requires additional device/hardware for biometric purposes.
Kim and Heo [46]: (2012)	√	√	-	-	-	-	-	SM, DCU, AS	*Pros:* matrix-based homomorphic hash-based protocol lowers computations as compared to homomorphic hash based on exponential operation. *Cons:* overall huge overhead, security against attacks is not discussed.
Lee *et al.* [38]: (2013)	√	-	-	-	-	-	-	SM, HA	*Pros:* efficient message authentication with certification structure between a SM and the HAs by using a simple hash function. *Cons:* not efficient when a large number of entities communicate with each other because the file structure is used.
Yan *et al.* [69]: (2013)	√	-	-	-	√	-	√	SM, AMI network	*Pros:* low packet loss and end-to-end delay using the symmetric key for the message authentication code; also provides data privacy, integrity, and confidentiality. *Cons:* not efficient for the sparse deployment of few smart meters; large number of encryption and decryption operations shows down the performance.
Lu *et al.* [47]: (2013)	-	-	√	-	-	-	-	Sensors, CC	*Pros:* aggregates protocol generates comparatively lower overhead; eliminates the Map-To-Hash hash and reduce the pairing operations in aggregation and verification to improve the computational efficiency. *Cons:* security against various other attacks is not discussed.
Nicanfar *et al.* [44]: (2014)	-	√	-	-	-	-	-	SM, AS	*Pros:* reduces the number of exchanged packets by decreasing the steps of secure remote password protocol from five to three. *Cons:* high cost from using PKI, and periodically need to refresh all public/private key pairs as well as any multicast keys in all the nodes using only one newly generated function broadcasted by the key generator entity.

Table 3. *Cont.*

Protocols	Security and Performance Objectives							Involved Entities in the Protocols/Schemes	Description (Pros & Cons)
	1	2	3	4	5	6	7		
Chan and Zhou [54]: (2014)	-	-	-	√	-	-	-	EV, IED, CS, backend server	*Pros:* protects against cyber-physical attacks by a two-factor authentication protocol that combines a novel contextual factor based on physical connectivity in the power grid with the conventional authentication factor in the challenge–response. *Cons:* privacy of device's identity is not preserved and may lead to user tracing and identity theft attacks.
Li *et al.* [55]: (2014)	-	-	-	√	-	-	-	HAN, NAN-GW	*Pros:* uses the Merkle hash tree based technique that generate low computation overhead; solution is secure against replay, injection, message modification. *Cons:* large hash function computations; topmost node is crucial as a single point of failure or compromization may massively affect the solution.
Fadul *et al.* [64]: (2014)	-	-	-	-	√	-	-	SCADA	*Pros:* network-flow and reputation-based trust toolkit; automatic diagnosis of some types of hardware/software failures; potential to detect calibration errors; ability to operate protection schemes through failures. *Cons:* additional complexity and need of a communication infrastructure.
Cho *et al.* [75]: (2014)	√	-	√	-	-	-	√	SM, AG, CC	*Pros:* guarantees privacy-preserving for (1) collecting total sum of energy usage for a group of SMs, and (2) collecting individual energy usage of individual SM for a desired period of time; lower communication overhead using a homomorphic encryption algorithm; relatively fast execution. *Cons:* security analysis is not provided in detail.
Chim *et al.* [74]: (2015)	√	-	-	-	-	-	√	SM, HAN, BAN, NAN, CC	*Pros:* filters messages before they reach the CC, which reduces the impact of attacking traffic; maintains privacy-preservation during aggregation. *Cons:* more overhead, prevention against attacks is not discussed.

Security and performance objectives: 1-Low execution and protocol delay; 2-Low computational and storage cost; 3-Low communication and computation overhead; 4-Resistance to attacks and failures; 5-Trust Management; 6-Buffer management; 7-Confidentiality and privacy.

3. Batch Authentication in the Vehicle-to-Grid (V2G) Network

Apart from the home environment (HAN, SM, HAs, AMI) authentication, another crucial requirement for the authentication are in the V2G communication network. The geographically-distributed vehicles' energy can be used to provide electricity for power load balance in the SG networks. In order to balance the power outage between the supply and the demand, the EVs or plugged-in hybrid electric vehicles (PHEVs) charge during off-peak periods and discharge during on-peak periods. Figure 2 illustrates a V2G communication scenario. Many messages exchanged during communication between vehicles, AGs, and CCs require a careful resistant investigation against various attacks, privacy protection, bi-directional authentication, information integrity, *etc.*

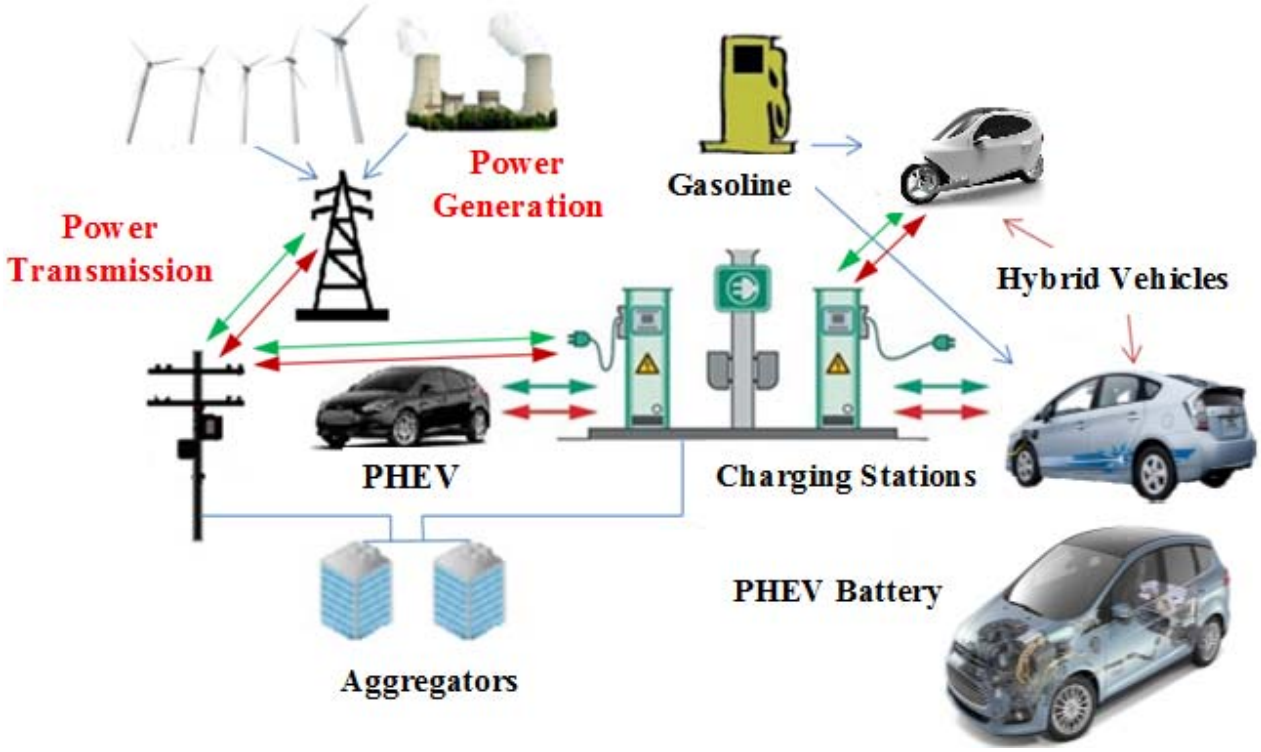

Figure 2. V2G communication in the SG network.

3.1. Security and Privacy Challenges in the Vehicle-to-Grid (V2G) Network

The specific protocols are required in the V2G network as the vehicles are allowed to charge, as well as discharge, their battery to the grid many times in a real-time environment. The authentication scheme must enable joining and disjoining of the vehicle dynamically for charging/discharging purposes. Further, the mobility of the vehicle is another issue. The vehicle can perform these operations within HAN as well as in the visiting area network (outside of the home network). The design of authentication protocol also varies when we consider distributed, as well as centralized, V2G network for vehicle charging and discharging.

The ISO 15118 standard specifies the scope of the automotive as well as the infrastructure (load-balancing) side. For the automotive side, it discusses the human-machine interface (HMI) interactions and the integration with the standardized V2G message flow. On the infrastructure side, the communication with the head-end systems is enabled using the DLMS/COSEM AMI [76].

The available security in DLMS/COSEM is security suite zero defined by AES-GCM-128 for authenticated encryption and AES128 for key wrapping. In order to enable the communication interoperability between the different deployed systems, ISO and IEC are working together for developing standards for the V2G communication interface, which is the protocol family ISO/IEC 15118. It specifies messages to be exchanged between the electric vehicle communication controller (EVCC) and the supply equipment communication controller (SECC) based on PLC. These protocols depend on the charging mode and scenario, identification, and authentication methods.

Security requirements of the V2G network include authentication, message integrity, and data confidentiality. According to IEC 15118-2 only unilateral authentication (only server side authentication) is mandatory and mutual authentication (both server and EV authentication) is optional [77]. However, mutual authentication is one of the mandatory requirements for an authentication scheme in order to defeat redirection and impersonation attacks, where the vehicle and the local AG verify each other's identity. The secret information should be sent over the network in such a way that only the respective recipient can extract the information. For example, the vehicles input their personal preferences at the charging station and are further sent to the AG/server. Additionally, the integrity of each message sent over the network must be maintained. There are some privacy issues that exist in the V2G network as well, such as vehicle's identity, vehicle charging/discharging location, battery status of the vehicle, selection of operation (charging or discharging) to be performed, and time duration for such an operation. An adversary or any untrusted entity in the SG network can misuse this information and can also trace the users' patterns and behavior. It may lead to some serious privacy issues. Therefore, the security and privacy issues are more challenging in the V2G network [24,35]. In the following subsections, we will examine the existing authentication protocols for the V2G system.

3.2. Existing Authentication Protocols in the Vehicle-to-Grid (V2G)

In this subsection, we discuss different types of existing authentication protocols for the V2G network.

3.2.1. Digital Signature Algorithm (DSA)-Based Protocols

Naccache *et al.* [78] constructed a digital signature algorithm (DSA)-based batch verification protocol where a signer generates n-signatures through the interactions with the verifier, and then the verifier validates these n-signatures simultaneously. After that, Harn [79] introduced an interactive batch protocol, in which the same private key (same sender) is used to sign a batch of packets. However, this scheme is inefficient due to pre-computation of all generated signatures for the batch. Bellare *et al.* [80] proposed a protocol for a V2G network based on a variant of DSA. However, it increases the authentication time due to large modular exponential and multiplication computations. Further, Harn [81] proposed another multiple DSA-type signature scheme. However, it does not always produce the true results when it groups the same base terms together and adds the exponent terms together.

3.2.2. Hybrid Public Key Infrastructure (PKI)-Based Protocols

In 2010, Guo *et al.* [82] had introduced a hybrid authentication protocol for the V2G system in order to authenticate the messages one-by-one. Further, Vaidya *et al.* [83] proposed a multi-domain

network-based protocol that incorporates a comprehensive hybrid PKI model (hierarchical and peer-to-peer certifications). However, it does not discuss authentication. Afterwards, Guo *et al.* [84] proposed a batch authentication protocol (UBAPV2G) that is able to achieve low authentication delay, computational cost, and communication traffic compared with the one-by-one authentication scheme.

3.2.3. Certificateless Public Key Infrastructure (PKI)-Based Protocols

Tseng [85] introduced a certificateless PKI-based privacy-preserving protocol, which protects the identities of vehicle owners using a partially-blind signature scheme, and maintains identity and location privacy, confidentiality, and integrity of communications. Hwoever, authors have not discussed efficiency, cost, and generated overhead during authentication. Then, Yang *et al.* [86] proposed an identity blind signature-based framework for vehicle monitoring. However, it is not clear whether the protocol is resistant against security attacks.

3.2.4. Aggregated Identifier-based Protocols

In 2012, Liu *et al.* [22] proposed an aggregated-proof-based privacy-preserving authentication scheme (AP3A), which works under home and visitor modes. Since, the vehicles are interacting with the different groups, different security and privacy requirements need to be considered. Using this approach, multiple battery vehicles (BVs) can be simultaneously authenticated by an AG to conserve communication resources without revealing the individual's privacy. Later, Liu *et al.* [87] suggested a battery status-aware authentication scheme (BASA) to address the battery-related issues of vehicles in the V2G networks. This scheme introduced an aggregated-identifier to hide each vehicle's identity from revealing the location related information. The scheme improves the anonymous power data transmission using an aggregated-status for data protection. However, both protocols [22,87], are inefficient since they generate large overhead during the V2G authentication.

In summary, although some privacy-preserved authentication protocols exist for the V2G network, these protocols either generate huge overhead or do not present security analysis to justify that they defeat various security attacks. Therefore, there still remain many research challenges to develop a privacy-preserved, secure, and efficient authentication protocol in the V2G network.

4. Authorization and Access Control in the Smart Grid (SG) Network

Authentication and authorization (AA) are two completely independent concepts that are essential for secure design of the system. Authentication mechanism verifies the identity of the entity (user, device, *etc.*). By enabling mutual authentication, the involved entities can verify whether they are connected to the legitimate entity at the other end or not. On the other end, authorization mechanism verifies whether the entity has required permissions or rights to access the desired entity/resource or perform desired operation. Authorization is close to access control, but they are exactly the same. Authorization generally refers to the decision policy of whether a user is allowed/denied, while the access control refers to the enforcement mechanism for the required security with base access controls on physical attributes, sets of rules, lists of individuals' identities, *etc.* A fine-grained authorization refers to an expansion of access controls. It is a mechanism to protect the privacy of various entities by authorizing each entity with different

capabilities of accessing resources. It clearly differentiates between a legitimate and an invalid user. Hence, it is an important property for maintaining privacy protection in the SG network.

Authentication, authorization, and control policy together are also referred as an access control mechanism. It is strongly required in the SG system as various users with different roles access billions of devices in the network. Generally, there are three types of access control mechanisms: user-based access control (UBAC), role-based access control (RBAC), and attribute-based access control (ABAC). Access control mechanism can be centralized or decentralized with static or dynamic attributes/functional policy in nature. In a centralized access control, all data are stored and managed in a central location in different modules, such as control panels and reader control modules. It is simple and easy to manage. However, a single point of failure can affect the system massively or even stops the service. On the other hand, decentralized access control enables more flexibility to individuals and usually follows a rule-based policy. Adding and/or deleting a control module using a decentralized access control policy does not affect the whole system, rather it reduces the cost and long distance connections. Furthermore, unlike general or static access control, dynamic access control uses place, time, and purpose according to the context information as conditions for access permissions [88].

In this direction, Bobba *et al.* [89] proposed a policy-based access control scheme, which is based on the centralized key distribution center (KDC). Unfortunately, the online requirement and having a single central body of the system (the single-point-of-failure will shut down the complete system), KDC rather becomes the drawback. Chen and Kim [90] discussed the relation distribution over a control system and approach to identify the access privileges in the HAN network. They proposed a RBAC scheme, which authenticates the privileges using a message hash code. However, the security of this system is not justified. The highly demanded access control among SG entities results in security threats and vulnerabilities. In order to control these issues, Kim *et al.* [91] proposed an access control mechanism that supports scalability, interoperability and flexibility of multi-domain smart grid system. They proposed a domain-of-domain (DoD) approach based on role attributes based-access control (RABAC) to fulfil the scalability and interoperability in the SG network. However, the security of the proposed approach is not verified. After that, Ruj and Nayak [92] suggested a decentralized security framework for the SG network that carries out access control as well as data aggregation. Their approach is based on the additive homomorphic encryption scheme and the attribute-based encryption that overcomes the drawbacks existing in a scheme by Bobba *et al.* [89]. Wu *et al.* [93] recommended a fault tolerant fine-grained access control scheme, which involves fuzzy identity-based encryption with lattice-based access control and detect error-correction coding. This scheme resists against the corruptions implied by the noisy channels and the environmental interferences. Recently, Yeo *et al.* [88] introduced a dynamic access model for secure user services in the SG, which is based on the appropriate access context type for the SG users. The approach applies a context-based user security policy to enable users' dynamic access control.

There are many other authorization schemes for the SG based on a service oriented architecture (SOA), reference architecture, modeling for interconnected domains, RBAC modeling, multi-authority access control for attribute revocation, and multilevel multi-factor authentication and attribute-based authorization. The SOA based on web services is proposed by Jung *et al.* [94] as a convenient way to provide data infrastructure capabilities on the exchanged information such as customer energy feedback, billing and invoicing of variable tariffs, demand side management, and efficient charging of EVs in the SG. However, system overheads are not discussed. Further, Ryba *et al.* [95] proposed authorization as a

service architecture in the SG and Zhang and Chen [96] proposed a data-centric access control for the SG services. Various challenges in defining and enforcing consistent authorization policy are described by Lakshminarayanan [97], but the paper does not describe the implementation part and other important aspects, such as overheads and execution time. Further, a new model that extends the network access control from a single security domain to multiple domains for interconnected microgrids, is presented by Cheung *et al.* [98]. However, it is not clear whether for a large SG network this policy would be effective. A RBAC model-based access control mechanism is extended for the SG systems by Rosic *et al.* [99] considering the regional division and a concept of areas of responsibility (AOR) for providing an efficient and consistent policy with a greater level of granularity. However, the RBAC based model may significantly increase complexity. Further, a multi-authority access control with efficient attribute revocation (MAAC-AR) scheme for the SG by Liu *et al.* [100] achieves fine-grained access control, collusion resistance, privacy preservation, and secure attribute revocation. Yet, this scheme generates a large storage overhead. Further, a lightweight and efficient security solution for substation automation system is proposed by Vaidya *et al.* [101] to provide multilevel multi-factor authentication and attribute-based authorization by deploying public key certificates, and zero-knowledge protocol-based server-aided verification.

As we discussed in this section, authorization is important for supporting secure communication among various entities of the SG. National Institute of Standards and Technology (NIST) also suggested a distinct need for a lightweight, secure, and efficient AA protocol to mitigate intrusion and distributed DoS (DDoS) attacks targeting resource-intense AA mechanisms [7]. In the view of large network systems, such as smart grid, a decentralized access control scheme is recommended in order to reduce the overall cost of adding and deleting entities in the system. Furthermore, ABAC is preferred over the user-based and the RBAC when the system is defined with large attributes or the user role is computed dynamically. Although some researchers presented attribute-based decentralized access control scheme, such as [92] and [88], they either do not justify resistance against security attacks or generate large overhead.

5. Secure Integration in the Smart Grid (SG) Network

Integrity refers to preventing unnoticed alteration of information by an adversary while secure integrated communication allows a reliable and efficient real-time control and information exchange. In the SG and V2G networks, various modules and entities communicate with each other. Thus, the integrity of information and secure integration among the various modules of these networks are essential. It is important to understand the different directions and areas of integration in the SG network to securely integrate various SG entities. These integrations in the SG can be the technology integration [102], data integration [103], Internet-of-things (IoT) integration [104], customer-oriented integration [105], renewable generation integration [106], SOA-based smart grid integration architecture [107], secure integration of the home energy management system to the battery management system [108], *etc.*

There have been some standardization efforts for secure integrations in the SG. The IEC 61850-80-4 standard defines a one-to-one mapping of the IEC 62056 object identification system (OBIS) codes to the logical nodes for seamless integration [109]. The objective is to expand the availability of meter information to other smart grid applications defined within the IEC 61850 framework. Reilly *et al.* [110]

examined that the implementation of advanced control capabilities in the integration of IEC 61850 devices from different suppliers within the substation as well as integrating IEC 61850 with other types of protocols are presented, but still require information to be available in a timely manner for making decisions. It is also challenging to properly integrate these large applications from different vendors, each with a different method of implementing IEC 61850 in their devices, to an upgraded platform. There are also some integration issues due to redundant GW. Similarly, the industrial challenge is to develop more comprehensive common information model (CIM) that covers majority of the utility requirements for the integration. Current CIM Interoperability tests demonstrate how multiple vendors can interoperate using CIM compliant integration only with limited functionality [111]. In summary, the integration software must support device independence and should be user friendly.

Some secure integration approaches have also been proposed by researcher community. In this direction, a secure integration approach was presented by Lee *et al.* [112] in which smart meters with communication ports for third party integration can share the data at the same time to both local building management system and the utilities. Further, feasible technical solutions are proposed by Rui [113] related to the data format translation from legacy data into CIM-based data, security concerns between different applications with time consistent constraints. However, a detail analysis of these solutions is needed. Recently, Jafary *et al.* [108] discussed secure integration of HEMS that supports Ethernet to the battery management system to support controller area network (CAN).

Generally, most of the adversaries in the SG network target the private user information and network management information. In this direction, various researchers either introduced new attacks or evaluated the overall integrated system. In 2009, Liu *et al.* [114] introduced a new attack, called false data injection, to the monitoring center in order to compromise SMs. Then, Papadopoulos *et al.* [115] introduced a model that evaluates various control methods, transient responses, and overall dynamic behavior of the system using the network of SMs. Monacchi *et al.* [116] system architecture focused advanced technologies that can be deployed towards secure integration in the SG network. Further, Guobin *et al.* [117] analyzed the effects of bulk energy generators, distributed energy resources, and storage devices on power grid based on power cumulative cost and service reliability.

Researchers have also introduced new architectures for the V2G system by considering the impact of energy and mobility of vehicles on integrated V2G interfaces. In this direction, recently, Kovacs *et al.* [118] introduced a core system architecture for an end-to-end integration of V2G communications interface under EU co-funded FP7 project "PowerUp" and discussed the critical SG integration aspects for each protocol layer within the V2G communications protocol stack. The impact of energy and mobility with respect to the supporting service and a dedicated infrastructure network is highlighted by Brusaglino [119]. It suggests that an e-mobility management provider should interface energy supply stations with the vehicle drivers through an ICT system to coordinate the charging request or the energy supply opportunity with the grid status. A concrete implementation of a charging management system (including stakeholders' requirements, V2G interface, integration of vehicles, and virtual power plant management) is evaluated by Heuer *et al.*, in [120]. Further, an overview was presented by Einwachter and Sourkounis [121] over already investigated problems and developed solutions in order to draw a general map of grid integration and the utilization of the EVs flexibility.

In summary, the data integrity is focused by the researchers' schemes in the SG as well as V2G networks. However, the secure integrated communications among different control modules and entities

have not been explored and evaluated in detail. These integration points in the SG as well as V2G networks can be a point of attack by the adversary, if sufficient care is not taken.

6. Current Challenges and Future Directions

There are several challenges with the current authentication protocols in terms of efficiency, overhead, cost, delay, privacy, *etc.* One of the major concerns is that unfortunately, there is no such protocol that exists that provides mutual authentication among HAN environments (HAs, SM, HAN-GW), energy provider, BAN-GW, NAN-GW, and AMI network (SM, AG/collector, RTU, and CC). Further, we suggest emphasizing the importance of user involvement when authenticating the HAs (during initial setup), since they generate and send data that belong to a particular user. Further, there is not yet an authentication protocol that fulfills all the proposed security and performance objectives in the SG network. The privacy protection in the home environment as well as in the V2G network is an important requirement for the SG. The protocol must not reveal the confidential and private information related to any entity involved in the authentication process. The access-based scheme is a good solution for providing the sufficient and required access to each entity after the authentication. Further, the V2G network also needs a secure and efficient batch verification-based authentication protocol with manageable overhead, and low end-to-end delay. Additionally, integration of device-to-device (SM-to-HAs, V-to-V) and device-to-network (SM-to-HAN-GW, V-to-RTU/NAN-GW) mutual authentication is needed in the design of future protocols for the home as well as V2G systems.

Lastly, a secure and efficient SCADA architecture (including RTU, IED, programmable logic controller, phasor data consolidator (PDC), PMU) with the optimum routing backbone network is required in order to strengthen the capability to perform secure data transfers in the SG, as the generic industrial control system (ICS)/SCADA system does not consider the existing security issues.

7. Conclusions

We have presented the current state of authentication, access control, and secure integration in the SG. We first defined seven objectives of the authentication protocol in order to fully provide efficient and secure communication environment. We critically evaluated the existing work, and identified future directions for developing efficient and secure authentication protocols for the future SG and V2G systems. We observed that mutual authentication among all entities and privacy prevention of communicated information is still a great challenge in the home environment as well as in the V2G network. We also found that some recent contributions based on access control mechanism are able to overcome some of the existing security and privacy issues. Further, the secure integrated communications among different control modules and entities in the SG need to be explored in detail.

Acknowledgments

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the “ICT Consilience Creative Program” (IITP-2015-R0346-15-1007) supervised by the IITP (Institute for Information & Communications Technology Promotion) and under the “Basic Science Research Program” (2013010489) through the NRF (National Research Foundation).

Author Contributions

Neetesh Saxena and Bong Jun Choi organize the requirements of authentication and privacy preservation in the SG and highlight the objectives for an efficient and secure authentication protocol for the SG. Further, Neetesh Saxena and Bong Jun Choi analyze the V2G communication requirement and perform a careful evaluation of existing literature in terms of efficiency and security. Neetesh Saxena and Bong Jun Choi also summarize and explain the secure integration and access control that is essential to further enhance the secure communication in the SG system.

Conflicts of Interest

The authors declare no conflict of interest.

Acronyms

ABAC	attribute-based access control
AG	aggregator
AMI	advanced metering infrastructure
AS	authentication server
BAN	building area network
CC	control center
CS	charging station
DCU	data concentration unit
DDoS	distributed DoS
DNP	distributed network protocol
DoS	denial-of-service
DR	demand response
DRTM	dynamic root of trust for measurement
DSA	digital signature algorithm
EP	energy providers
GW	gateways
HA	home appliances
HAN	home area network
HMAC	hash-based MAC
KDC	key distribution center
LTE	long term evolution
MAC	message authentication code
MITM	man-in-the-middle
NAN-GW	neighboring gateway
NIST	national institute of standards and technology
OMS	open metering system
PHEV	plugged-in hybrid electric vehicles
PKI	public key infrastructure

PLC	power line communication
RABAC	role attributes based-access control
RBAC	role-based access control
RFID	radio frequency identifier
RTU	remote terminal units
SCADA	supervisory control and data acquisition
SG	smart grid
SM	smart meter
SOA	service oriented architecture
SSC	substation controller
TV-OTS	time-valid one-time-signature
UBAC	user-based access control
VANET	vehicular ad-hoc network
V2G	vehicle-to-grid
WAN	wide area network

References

1. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. Available online: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf (accessed on 2 July 2015).
2. Ding, Y.M.; Hong, S.H.; Li, X.H. A demand response energy management scheme for industrial facilities in smart grid. *IEEE Trans. Ind. Inf.* **2014**, *10*, 2257–2269.
3. Li, H. An efficient authentication scheme in smart grids. In *Enabling Secure and Privacy Preserving Communications in Smart Grids*, 1st ed.; Springer International Publishing: Cham, Switzerland, 2014; pp. 31–46.
4. Guidelines for Smart Grid Cyber Security. Available online: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628 (accessed on 2 July 2015).
5. Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. Available online: http://www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf (accessed on 4 July 2015).
6. Ericsson, G.N. Cyber security and power system communication—Essential parts of a smart grid infrastructure. *IEEE Trans. Power Deliv.* **2010**, *25*, 1501–1507.
7. Forging a Path toward a Digital Grid Global Perspectives on Smart Grid Opportunities. Available online: www.accenture.com/Microsite/digitally-enabled-grid/Documents/pdf/Accenture-Future-Digital-Grid-Report-Digitally-Enabled-Grid.pdf (accessed on 21 August 2015).
8. Mahan, R.E.; Burnette, J.R.; Fluckiger, J.D.; Goranson, C.A.; Clements, S.L.; Kirkham, H.; Tews, C. *Secure Data Transfer Guidance for Industrial Control and SCADA Systems*; Technical Report for Pacific Northwest National Laboratory: Richland, WA, USA, 2011.

9. Taylor, C.R.; Shue, C.A.; Paul, N.R. A Deployable SCADA Authentication Technique for Modern Power Grids. In Proceedings of the IEEE International Energy Conference, Dubrovnik, Croatia, 13–16 May 2014; pp. 696–702.
10. Hamlyn, A.; Cheung, H.; Mander, T.; Wang, L.; Yang, C. Network Security Management and Authentication of Actions for Smart Grids Operations. In Proceedings of the IEEE Canada Electrical Power Conference, Montreal, QC, Canada, 25–26 October 2007; pp. 31–36.
11. Hamlyn, A.; Cheung, H.; Mander, T.; Lin, W.; Cungang, Y.; Cheung, R. Computer Network Security Management and Authentication of Smart Grids Operations. In Proceedings of the IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 20–24 July 2008; pp. 1–7.
12. Lu, X.; Wang, W.; Lu, Z.; Mat, J. From Security to Vulnerability: Data Authentication Undermines Message Delivery in Smart Grid. In Proceedings of the Military Communications Conference, Baltimore, MD, USA, 7–10 November 2011; pp. 1183–1188.
13. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. A survey on smart grid potential applications and communication requirements. *IEEE Trans. Ind. Inf.* **2013**, *9*, 28–42.
14. Smart Grid Wireless Technology Comparison Chart, Aviat Network. Available online: http://www.portals.aviatnetworks.com/exLink.asp?9489648ON51N33I37128896 (accessed on 23 August 2015).
15. Power Line Carrier (PLC) Systems Market (By Technologies-Narrowband & Broadband, Applications-Smart Grid, In-Door Networking, Long Haul & M2M, Verticals-Industrial, Residential & Commercial & Geography)-Global Assessment & Forecast-(2013–2018). Available online: http://www.marketsandmarkets.com/Market-Reports/power-line-communication-plc-market-912.html (accessed on 22 September 2015).
16. Berger, L.T.; Schwager, A.; Escudero-Garzás, J.J. Power line communications for smart grid applications. *J. Electr. Comput. Eng.* **2013**, *2013*, doi:10.1155/2013/712376.
17. Atzori, L.; Meloni, A. VANET in Vehicle-to-Grid. Available online: http://www.noae.com/fileadmin/content/sieger/V2G-Presentation.pdf (accessed on 10 August 2015).
18. Wang, B.; Ma, M. A Server Independent Authentication Scheme for RFID Systems. *IEEE Trans. Ind. Inf.* **2012**, *8*, 689–696.
19. Vaidya, B.; Makrakis, D.; Mouftah, H.T. Authentication Mechanism for Mobile RFID Based Smart Grid Network. In Proceedings of the 27th IEEE Canadian Conference on Electrical and Computer Engineering, Toronto, AB, Canada, 4–7 May 2014; pp. 1–6.
20. Rodriguez-Mondejar, J.A.; Santodomingo, R.; Brown, C. The ADDRESS Energy Box: Design and Implementation. In Proceedings of the IEEE International Energy Conference and Exhibition (ENERGYCON), Florence, Italy, 9–12 September 2012; pp. 629–634.
21. Bianchi, G. Revisiting an RFID identification-free batch authentication approach. *IEEE Commun. Lett.* **2011**, *15*, 632–634.
22. Liu, H.; Ning, H.; Zhang, Y. Aggregated-proofs based privacy preserving authentication for V2G networks in the smart grid. *IEEE Trans. Smart Grid* **2012**, *3*, 1722–1733.
23. WINSmartEV Project. Available online: http://smartgrid.ucla.edu/projects_evgrid.html (accessed on 12 August 2015).

24. Liu, J.; Xiao, Y.; Li, S.; Liang, W.; Chen, C. Cyber security and privacy issues in smart grids. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 981–997.
25. Lee, S.; Bong, J.; Shin, S.; Shin, Y. A Security Mechanism of Smart Grid AMI Network through Smart Device Mutual Authentication. In Proceedings of the International Conference on Information Networking (ICOIN), Phuket, Thailand, 10–12 February 2014; pp. 592–595.
26. Paverd, A.J.; Martin, A.P. Hardware Security for Device Authentication in the Smart Grid. In *Smart Grid Security* Cuellar, J., Ed.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 72–84.
27. IEC 62056-6-2:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 6-2: COSEM interface classes. Available online: https://webstore.iec.ch/publication/6410 (accessed on 22 September 2015).
28. Feuerhahn, S.; Zillgith, M.; Wittwer, C.; Wietfeld, C. Comparison of the communication protocols DLMS/COSEM, SML and IEC 61850 for smart metering applications. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, Belgium, 17–20 October 2011; pp. 410–415.
29. OpenADR and Cyber Security. Available online: http://www.openadr.org/cyber-security (accessed on 24 September 2015).
30. Remote Authentication Dial in User Service—RADIUS, Developing Solutions. Available online: https://www.developingsolutions.com/products/radius (accessed on 24 September 2015).
31. Hosia, A. Comparison between RADIUS and Diameter, 2003. Available online: http://www.tml.tkk.fi/Studies/T-110.551/2003/papers/11.pdf (accessed on 24 September 2015).
32. Wang, W.; Lu, Z. Cyber Security in the Smart Grid: Survey and Challenges. *Comput. Netw.* **2013**, *57*, 1344–1371.
33. Aggarwal, A.; Kunta, S.; Verma, P.K. A Proposed Communications Infrastructure for the Smart Grid. In Proceedings of the IEEE Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD, USA, 19–21 January 2010; pp. 1–5.
34. Wang, Q.; Khurana, H.; Ying, H.; Nahrstedt, K. Time-Valid One-Time Signature for Time-Critical Multicast Data Authentication. In Proceedings of the 28th IEEE INFOCOM, Rio de Janeiro, Brazil, 19–25 April 2009; pp. 1233–1241.
35. Khurana, H.; Hadley, M.; Lu, N. Smart grid security issues. *IEEE Secur. Priv.* **2010**, *8*, 81–85.
36. Sule, R.; Katti, R.S.; Kavasseri, R.G. A Variable Length Fast Message Authentication Code for Secure Communication in Smart Grids. In Proceedings of the IEEE Power and Energy Society General Meeting, San Diego, CA, USA, 16–22 July 2012; pp. 1–6.
37. Fouda, M.M.; Fadlullah, Z.M.; Kato, N.; Lu, R.; Shen, X. A lightweight message authentication scheme for smart grid communications. *IEEE Trans. Smart Grid* **2011**, *2*, 675–685.
38. Lee, Y.S.; Kim, E.; Kim, Y.S.; Jeon, H.Y.; Jung, M.S. A Study on Secure Chip for Message Authentication between a Smart Meter and Home Appliances in Smart Grid. In Proceedings of the International Conference on IT Convergence and Security, Macao, China, 16–18 December 2013; pp. 1–3.
39. Tsang, P.; Smith, S.W. YASIR: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems. In Proceedings of the 23rd International Information Security Conference, Milano, Italy, 7–10 September 2008; pp. 445–459.

40. Cairns, K.; Hauser, C.; Gamage, T. Flexible Data Authentication Evaluated for the Smart Grid. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Vancouver, BC, Canada, 21–24 October 2013; pp. 492–497.
41. Li, Q.; Cao, G. Multicast authentication in the smart grid with one-time signature. *IEEE Trans. Smart Grid* **2011**, *2*, 686–695.
42. Reyzin, L.; Reyzin, N. Better than Biba: Short One-Time Signatures with Fast Signing and Verifying. In Proceedings of the Australian Conference on Information Security and Privacy, Melbourne, Australia, 3–5 July 2002; pp. 144–153.
43. Li, D.; Aung, Z.; Williams, J.R.; Sanchez, A. Efficient Authentication Scheme for Data Aggregation in Smart Grid with Fault Tolerance and Fault Diagnosis. In Proceedings of the IEEE PES Innovative Smart Grid Technologies, Washington, DC, USA, 16–20 January 2012; pp. 1–8.
44. Nicanfar, H.; Jokar, P.; Beznosov, K.; Leung, V.C.M. Efficient authentication and key management mechanisms for smart grid communications. *IEEE Syst. J.* **2014**, *8*, 629–640.
45. Im, S.B.; Oh, Y.H. A study effective ZigBee authentication protocol in smart grid network. *J. Korea Inf. Commun. Soc.* **2011**, *36*, 184–194.
46. Kim, Y.S.; Heo, J. Device authentication protocol for smart grid systems using homomorphic hash. *J. Commun. Netw.* **2012**, *14*, 606–613.
47. Lu, R.; Lin, X.; Shi, Z.; Shen, X. EATH: An Efficient Aggregate Authentication Protocol for Smart Grid Communications. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China, 7–10 April 2013; pp. 1819–1824.
48. Katti, R.S.; Sule, R.; Kavasseri, R.G. Multicast Authentication in the Smart Grid with One-Time Signatures from Sigma-Protocols. In Proceedings of the ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), Philadelphia, PA, USA, 8–11 April 2013; pp. 239–239.
49. Hu, F. *Cyber-Physical Systems: Integrated Computing and Engineering Design*; CRC Press: London, UK, 2013; p. 398.
50. Final report on August 14, 2003 blackout in the United States and Canada: Causes and recommendations. Available online: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf (accessed on 10 July 2015).
51. Li, X.; Liang, X.; Lu, R.; Shen, X.; Lin, X.; Zhu, H. Securing smart grid: Cyber attacks, countermeasures, and challenges. *IEEE Commun. Mag.* **2012**, *50*, 38–45.
52. Oh, S.; Kwak, J. Mutual authentication and key establishment mechanism using DCU certificate in smart grid. *Appl. Math. Inf. Sci.* **2012**, *6*, 257–264.
53. Fouda, M.M.; Fadlullah, Z.M.; Katolt, N.; Lu, R.; Shen, X. Towards a Light-Weight Message Authentication Mechanism Tailored for Smart Grid Communications. In Proceedings of the International Workshop on Security in Computers, Networking and Communications, Shanghai, China, 10–15 April 2011; pp. 1018–1023.
54. Chan, A.C.F.; Zhou, J. Cyber-physical device authentication for smart grid electric vehicle ecosystem. *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1509–1517.
55. Li, H.; Lu, R.; Zhou, L.; Yang, B.; Shen, X. An efficient merkle-tree-based authentication scheme for smart grid. *IEEE Syst. J.* **2014**, *8*, 655–662.

56. Ayday, E.; Rajagopal, S. Secure, Intuitive and Low-Cost Device Authentication for Smart Grid Networks. In Proceedings of the 8th Annual IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 9–12 January 2011; pp. 1161–1165.
57. Zhang, L.; Tang, S.; Jiang, Y.; Ma, Z. Robust and Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Smart Grids. In Proceedings of the IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical, and Social Computing, Green Computing and Communications (GreenCom), Beijing, China, 20–23 August 2013; pp. 2089–2093.
58. Vaidya, B.; Makrakis, D.; Mouftah, H. Provisioning Substation-Level Authentication in the Smart Grid Networks. In Proceedings of the Military Communications Conference, Baltimore, MD, USA, 7–10 November 2011; pp. 1189–1194.
59. Nicanfar, H.; Jokar, P.; Leung, V.C.M. Smart Grid Authentication and Key Management for Unicast and Multicast Communications. In Proceedings of the IEEE PES Innovative Smart Grid Technologies Asia (ISGT), Perth, Australia, 13–16 November 2011; pp. 1–8.
60. Gao, Q. Biometric Authentication in Smart Grid. In Proceedings of the International Conference on Energy and Sustainability (IESC), Farmingdale, NY, USA, 22–23 March 2012; pp. 1–5.
61. Tabassum, R.; Nahrstedt, K.; Rogers, E.; Lui, K.S. SCAPACH: Scalable Password-Changing Protocol for Smart Grid Device Authentication. In Proceedings of the International Conference on Computer Communications and Networks (ICCCN), Nassau, Bahamas, 20 July–2 August 2013; pp. 1–5.
62. Metke, A.R.; Ekl, R.L. Smart Grid Security Technology. In Proceedings of the International Conference on Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD, USA, 19–21 January 2010; pp. 1–7.
63. Kursawe, K.; Danezis, G.; Kohlweiss, M. Privacy-Friendly Aggregation for the Smart Grid. In Proceedings of the 11th International Conference on Privacy Enhancing Technologies, Waterloo, ON, Canada, 27–29 July 2011; pp. 175–191.
64. Fadul, J.E.; Hopkinson, K.M.; Andel, T.R.; Sheffield, C.A. A trust-management toolkit for smart-grid protection systems. *IEEE Trans. Power Deliv.* **2014**, *29*, 1768–1779.
65. Dong, J.; Nicol, D.M.; Guanhua, Y. An Event Buffer Flooding Attack in DNP3 Controlled SCADA Systems. In Proceedings of the Winter Simulation Conference, Phoenix, AZ, USA, 11–14 December 2011; pp. 2614–2626.
66. The Dark Side of the Smart Grid-Smart Meters Security, 2009. Available online: http://www.smartgridinformation.info/pdf/4686_doc_1.pdf (accessed on 13 July 2015).
67. Choi, K.; Chen, X.; Li, S.; Kim, M.; Chae, K.; Na, J.C. Intrusion detection of NSM based DoS attacks using data mining in smart grid. *Energies* **2012**, *5*, 4091–4109.
68. Bekara, C.; Luckenbach, T.; Bekara, K. A Privacy Preserving and Secure Authentication Protocol For the Advanced Metering Infrastructure with Non-Repudiation Service. In Proceedings of the International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies (ENERGY), St. Maarten, The Netherlands, 25–30 March 2012; pp. 60–68.
69. Yan, Y.; Hu, R.; Das, S.; Sharif, H.; Qian, Y. An efficient security protocol for advanced metering infrastructure in smart grid. *IEEE Netw.* **2013**, *27*, 64–71.

70. Guo, H.; Qian, Y.; Lu, K.; Moayeri, N. Backbone Construction for Heterogeneous Wireless Ad Hoc Networks. In Proceedings of the IEEE ICC, Dresden, Germany, 14–18 June 2009; pp. 1–5.
71. Sabbah, A.I.; Mougy, A.E.; Ibnkahla, M. A survey of networking challenges and routing protocols in smart grids. *IEEE Trans. Ind. Inf.* **2014**, *10*, 210–221.
72. Sikora, A. Implementation of Standardized Secure Smart Meter Communication. In Proceedings of the 35th International Telecommunications Energy Conference Smart Power and Efficiency (INTELEC), Hamburg, Germany, 13–17 October 2013; pp. 1–5.
73. Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Li, V.O.K. PASS: Privacy-Preserving Authentication Scheme for Smart Grid Network. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, Belgium, 17–20 October 2011; pp. 196–201.
74. Chim, T.W.; Yiu, S.M.; Li, V.O.K.; Hui, L.C.K.; Jin, Z. PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid. *IEEE Trans. Dependable Secur. Comput.* **2015**, *12*, 85–97.
75. Cho, S.; Li, H.; Choi, B.J. PALDA: Efficient Privacy-Preserving Authentication for Lossless Data Aggregation in Smart Grids. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, Italy, 3–6 November 2014; pp. 914–919.
76. Robert, S.; Andrés, C.; András, K.; Zoltán, J.; Vassilis, K.; John, J.; Auguste, A.; Dave, M.; Daniel, K; Stefano, S.; *et al.* V2G Interface Specifications Between the Electric Vehicle, the Local Smart Meter, and ITS Service Providers. Available online: http://www.power-up.org/wp-content/uploads/2012/07/PowerUp_D4.1_final.pdf (accessed on 13 July 2015).
77. Road Vehicles—Vehicle-to-Grid Communication Interface—Part 2: Network and Application Protocol Requirements. Available online: http://www.iso.org/iso/catalogue_detail.htm?csnumber=55366 (accessed on 13 July 2015).
78. Naccache, D.; Raihi, D.M.; Rapheali, D.; Vaudenay, S. Can DSA be Improved-Complexity Trade-Offs with the Digital Signature Standard. In Proceedings of the Advances in Cryptology-EUROCRYPT, Perugia, Italy, 9–12 May 1994; pp. 85–94.
79. Harn, L. DSA type secure interactive batch verification protocols. *Electron. Lett.* **1995**, *31*, 257–258.
80. Bellare, M.; Garay, J.A.; Rabin, T. Fast Batch Verification for Modular Exponentiation and Digital Signatures. In Proceedings of the Advances in Cryptology-EUROCRYPT, Espoo, Finland, 31 May–4 June 1998; pp. 236–250.
81. Harn, L. Batch verifying multiple DSA-type digital signatures. *Electron. Lett.* **1998**, *34*, 870–871.
82. Guo, H.Q.; Yu, F.; Wong, W.C.; Suhendra, V.; Wu, Y.D. Secure Wireless Communication Platform for EV-to-Grid Research. In Proceedings of the IWCMC, Caen, France, 28 June–2 July 2010; pp. 21–25.
83. Vaidya, B.; Makrakis, D.; Mouftah, H.T. Security Mechanism for Multi-Domain Vehicle-to-Grid Infrastructure. In Proceedings of the IEEE Global Telecommunications Conference, Houston, TX, USA, 5–9 December 2011; pp. 1–5.
84. Guo, H.; Wu, Y.; Bao, F.; Chen, H.; Ma, M. UBAPV2G: A unique batch authentication protocol for vehicle-to-grid communications. *IEEE Trans. Smart Grid* **2011**, *2*, 707–714.
85. Tseng, H.R. A Secure and Privacy-Preserving Communication Protocol for V2G Networks. In Proceedings of the IEEE WCNC, Paris, France, 1–4 April 2012; pp. 2706–2711.

86. Yang, Z.; Yu, S.; Lou, W.; Liu, C. P^2: Privacy-preserving communication and precise reward architecture for V2G networks in smart grid. *IEEE Trans. Smart Grid* **2011**, *2*, 697–706.
87. Liu, H.; Ning, H.; Zhang, Y.; Guizani, M. Battery status-aware authentication scheme for V2G networks in smart grid. *IEEE Trans. Smart Grid* **2013**, *4*, 99–110.
88. Yeo, S.S.; Kim, S.J.; Cho, D.E. Dynamic access control model for security client services in smart grid. *Int. J. Distrib. Sensor Netw.* **2014**, *2014*, doi:10.1155/2014/181760.
89. Bobba, R.; Khurana, H.; Alturki, M.; Ashraf, F. PBES: A Policy Based Encryption System with Application to Data Sharing in the Power Grid. In Proceedings of the ASIACCS, Sydney, Australia, 10–12 March 2009; pp. 262–275.
90. Chen, X.; Kim, H.S. RBAC for home area network based smart grid. *J. Korea Inf. Technol. Converg. Soc.* **2010**, *3*, 95–101.
91. Kim, J.; Kwon, Y.; Lee, Y.; Seo, J.; Kim, H. Access control mechanism supporting scalability, interoperability and flexibility of multi-domain smart grid system. *Inf. Sci. Ind. Appl.* **2012**, *4*, 194–201.
92. Ruj, S.; Nayak, A. A decentralized security framework for data aggregation and access control in smart grids. *IEEE Trans. Smart Grid* **2013**, *4*, 196–205.
93. Wu, J.; Dong, M.; Ota, K.; Zhou, Z.; Duan, B. Towards fault-tolerant fine-grained data access control for smart grid. *Wirel. Personal Commun.* **2014**, *75*, 1787–1808.
94. Jung, M.; Hofer, T.; Dobelt, S.; Kienesberger, G.; Judex, F.; Kastner, W. Access Control for a Smart Grid SOA. In Proceedings of the 7th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 10–12 December 2012; pp. 281–287.
95. Ryba, G.; Jung, M.; Kastner, W. Authorization as a Service in Smart Grids: Evaluating the PaaS Paradigm for XACML Policy Decision Points. In Proceedings of the 18th IEEE Conference on Emerging Technologies & Factory Automation (ETFA), Cagliari, Italy, 10–13 September 2013; pp. 1–4.
96. Zhang, Y.; Chen, J.L. Data-Centric Access Control with Confidentiality for Collaborating Smart Grid Services Based on Publish/Subscribe Paradigm. In Proceedings of the 33rd IEEE International Conference on Distributed Computing Systems Workshops, Philadelphia, PA, USA, 8–11 July 2013; pp. 45–50.
97. Lakshminarayanan, S. Authentication and Authorization for Smart Grid Application Interfaces. In Proceedings of the IEEE/PES Power Systems Conference and Exposition (PSCE), Phoenix, AZ, USA, 20–23 March 2011; pp. 1–5.
98. Cheung, H.; Hamlyn, A.; Mander, T.; Yang, C.; Cheung, R. Strategy and Role-Based Model of Security Access Control for Smart Grids Computer Networks. In Proceedings of the IEEE Canada Electrical Power Conference, Montreal, QC, Canada, 25–26 October 2007; pp. 423–428.
99. Rosic, D.; Novak, U.; Vukmirovic, S. Role-Based Access Control Model Supporting Regional Division in Smart Grid System. In Proceedings of the 5th International Conference on Computational Intelligence, Communication Systems and Networks, Madrid, Spain, 5–7 June 2013; pp. 197–201.
100. Liu, D.; Li, H.; Yang, Y.; Yang, H. Achieving Multi-Authority Access Control with Efficient Attribute Revocation in Smart Grid. In Proceedings of the IEEE ICC-Communication and Information Systems Security Symposium, Sydney, Australia, 10–14 June 2014; pp. 634–639.

101. Vaidya, B.; Makrakis, D.; Mouftah, H.T. Authentication and authorization mechanisms for substation automation in smart grid network. *IEEE Netw.* **2013**, *27*, 5–11.
102. Liu, W.H.E. Analytics and Information Integration for Smart Grid Applications. In Proceedings of the IEEE Power and Energy Society General Meeting, Minneapolis, MN, USA, 25–29 July 2010; pp. 1–3.
103. Lu, B.; Song, W. Research on Heterogeneous Data Integration for Smart Grid. In Proceedings of the IEEE International Conference on Computer Science and Information Technology (ICCSIT), Chengdu, China, 9–11 July 2010; pp. 52–56.
104. Chen, X.; Liu, J.; Li, X.; Sun, L.; Zhen, Y. Integration of IoT with Smart Grid. In Proceedings of the IET International Conference on Communication Technology and Application (ICCTA), Beijing, China, 14–16 October 2011; pp. 723–726.
105. Meiling, S.; Steinbach, T.; Duge, M.; Schmidt, T.C. Consumer-Oriented Integration of Smart Homes and Smart Grids: A Case for Multicast-Enabled Home Gateways? In Proceedings of the IEEE International Conference on Consumer Electronics (ICCE-Berlin), Berlin, Germany, 9–11 September 2013; pp. 279–283.
106. Liu, G.R.; Lin, P.; Fang, Y.; Lin, Y.B. Optimal threshold policy for in-home smart grid with renewable generation integration. *IEEE Trans. Parallel Distrib. Syst.* **2015**, *26*, 1096–1105.
107. Malarvizhi, R.; Kalyani, S. SOA Based Open Data Model for Information Integration in Smart Grid. In Proceedings of the 5th International Conference on Advanced Computing (ICoAC), Chennai, India, 18–20 December 2013; pp. 143–148.
108. Jafary, P.; Repo, S.; Koivisto, H. Secure Integration of the Home Energy Management System to the Battery Management System in the Customer Domain of the Smart Grid. In Proceedings of the IEEE PES General Meeting, Conference & Exposition, National Harbor, MD, USA, 27–31 July 2014; pp. 1–5.
109. IEC 61850-80-4 TS: Communication networks and systems for power utility automation—Part 80-4: Translation from COSEM object model (IEC 62056) to the IEC 61850 data model. Available online: http://www.iec.ch/cgibin/restricted/getfile.pl/57_1602e_DTS.pdf?dir=57&format=pdf&type=_DTS&file=1602e.pdf (accessed on 29 September 2015).
110. Reilly, R.O.; Beng, T.C.; Dogger, G. Hidden Challenges in the Implementation of 61850 in Larger Substation Automation Projects. Available online: http://www.cooperindustries.com/content/dam/public/powersystems/products/grid_automation/resources/Hidden_Challenges_in_the_Implementation_of_61850.pdf (accessed on 22 September 2015).
111. Reinprecht, N.; Torres, J.; Maia, M. IEC CIM architecture for Smart Grid to achieve interoperability International CIM Interop in March 2011. Available online: http://www.gridwiseac.org/pdfs/forum_papers11/ambrosio_paper_gi11.pdf (accessed on 22 September 2015).
112. Lee, P.K.; Lai, L.L. Practical Approach of Smart Metering Integration in Micro-Grid. In Proceedings of the IEEE Power and Energy Society General Meeting, Minneapolis, MN, USA, 25–29 July 2010; pp. 1–5.
113. Rui, S. A CIM-Based System Model for Life-Cycle Assets Management and Control Integration in Smart Grid. In Proceedings of the International Conference on Information Networking and Automation (ICINA), Kunming, China, 18–19 October 2010; pp. 337–341.

114. Liu, Y.; Ning, P.; Reiter, M. False Data Injection Attacks against State Estimation in Electric Power Grids. In Proceedings of the ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009; pp. 21–32.
115. Papadopoulos, P.N.; Chatzisideris, M.D.M.D.; Papadopoulos, T.A.; Marinopoulos, A.G. Integration of Smart Grid Technologies in a Microgrid with PV and FC Units. In Proceedings of the 46th International Universities' Power Engineering Conference, Soest, Germany, 5–8 September 2011; pp. 1–6.
116. Monacchi, A.; Egarter, D.; Elmenreich, W. Integrating Households into the Smart Grid. In Proceedings of the Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, Berkeley, CA, USA, 20–22 May 2013; pp. 1–6.
117. Xu, G.; Moulema, P.; Yu, W. Integrating Distributed Energy Resources in Smart Grid: Modeling and Analysis. In Proceedings of the IEEE Energytech, Cleveland, OH, USA, 21–23 May 2013; pp. 1–5.
118. Kovacs, A.; Marples, D.; Schmidt, R.; Morsztyn, R. Integrating EVs into the Smart-Grid. In Proceedings of the 13th International Conference on ITS Telecommunications, Tampere, Finland, 5–7 November 2013; pp. 413–418.
119. Brusaglino, G. Integration of Road Electric Vehicles into the Smart Grid System. In Proceedings of the International Conference on Clean Electrical Power (ICCEP), Naples, Italy, 11–13 June 2013; pp. 177–182.
120. Heuer, J.; Komarnicki, P.; Styczynski, Z.A. Integration of Electrical Vehicles into the Smart Grid in the Harz.EE-Mobility Research Project. In Proceedings of the IEEE Power and Energy Society General Meeting, San Diego, CA, USA, 24–29 July 2011; pp. 1–6.
121. Einwachter, F.; Sourkounis, C. Accessing Flexibility of Electric Vehicles for Smart Grid Integration. In Proceedings of the International Conference on Ecological Vehicles and Renewable Energies (EVER), Monte-Carlo, Monaco, 25–27 March 2014; pp. 1–8.