2020 Emerging Technology in Computing, Communication and Electronics (ETCCE)

On the Security of an Authentication Scheme for Smart Metering Infrastructure

Khalid Yahya
Department of Mechatronics Engineering
Istanbul Gelisim University
34310 Istanbul, Turkey
koyahya@gelisim.edu.tr

Shehzad Ashraf Chaudhry
Department of Computer Engineering
Istanbul Gelisim University
34310 Istanbul, Turkey
sashraf@gelisim.edu.tr

Fadi Al-Turjman
Artificial Intelligence dept.
Research Center for AI and IoT
Near East University
Nicosia, Mersin 10, Turkey
fadi.alturjman@neu.edu.tr

2020 Emerging Technology in Computing, Communication and Electronics (ETCCE) | 978-1-6654-1962-8 /20/$31.00 ©2020 IEEE | DOI: 10.1109/ETCCE51779.2020.9350916

***Abstract*—Recently, in 2019, Kumar et al. (IEEE Transactions on Smart Grid 10.4 (2018): 4349-4359) proposed an ECC based lightweight authentication and Key agreement scheme (LAKA) to secure the communication among a smart meter (SM) and a neighbourhood area network (NAN) gateway. The LAKA scheme was proved as secure and efficient as per the comparisons performed by Kumar et al. Specifically, it was argued through security analysis that LAKA provides anonymity and resistance to related attacks. However, the specific analysis in this paper contradicts their claim and it is shown here that in addition to ephemeral secret leakage attack and lack of untraceability, the LAKA is also vulnerable to stolen verifier attack.**

***Index Terms*—Smart Grid Authentication, Smart City Security , Smart Home, Ephemeral Secret Leakage attack.**

I. Introduction

Globally, there have been concerns over the sustainability of energy sources that the human race has relied on since the onset of civilization and yonder. As such, there has been a paradigm shift towards innovation and the use of sources of energy [1]. One such innovation that is expected to steer future energy needs is the smart energy network (SEN). Some of the factors that make SEN an ideal energy source include; low carbon emissions, continuous and sufficient energy supply, and automated billing. The identified qualities enable SEN to serve all energy needs reliably and effectively. Energy needs could be domestic or industrial [2]. The most remarkable feature of SEN is the smart metering infrastructure (SMI) which is lauded for its numerous advantages over traditional metering systems. The infrastructure ensures that both the company supplying power and consumers can collaboratively manage energy. This explains why internationally, numerous smart metering projects are being undertaken [2]. For instance, in Italy, some 30 million smart meters (SMs) are being used. Similar projects are also at the piloting stage in Germany. The German projects include E-DeMa and SmartWatts. The Netherlands and Great Britain have also rolled out smart gas and smart electricity meters as part of their smart metering infrastructure. Other countries within the European Union are various stages of implementing smart metering infrastructure [3]. As an intelligent network, Smart Energy Networks (SEN) relies on various devices and communication networks to facilitate interactions between companies engaged in supplying energy and their consumers [4], [5]. One example of a smart metering infrastructure network is the home area network (HAN) [6]. In this approach, resource-constrained smart meters (SM) are relied on in collecting, controlling, and managing utility consumption in a home. Additionally, Transmitting the SM and receiving data occurs when the two way communication technology is implemented. It also controls commands to and from the neighborhood area networks (NAN) gateway and ultimately to and from the utility server (US) [1], [7]. Smart gas and electricity meters are usually installed in open areas outside homes. As such, pedestal enclosures are used in shielding them from environmental impact. Apart from environmental impacts, the pedestal enclosures help in deterring possible interference from unauthorized users who can easily alter the consumption of the home appliances relying on the smart meter (SM) [8]. Additionally, such an intruder is capable of counterfeiting the (SM) by tampering with the data. Such unauthorized operations are characterized by falsification of data which can easily trigger power disconnection. Further, the (SM) monitors consumption by sending periodic consumption within an hour or prescribed minutes [9]. Without a proper pedestal enclosure, an intruder is likely to tap wireless communication channels and subsequently disclose consumption data for personal gains. The disclosed information can then be used to overrun the privacy of the user. These can include the times within which the user is at home or away from home. This poses obvious risks to such a home. For instance, the intruders can easily damage the affected home, office, society, or even the city. A good example is the December 23, 2015 cyber-attack of three Ukrainian energy supply companies which

translated into power disconnection for hours unending. The main vulnerability that catalyzed the attack was the inadequate authentication that the attackers exploited. As a result, the attackers were able to intrude into the control systems of the grid [2], [9].

II. Related Work

Authentication refers to the process of determining the identification of users of a system. This makes it an essential aspect of protection against unauthorized access. Subsequently, it eradicates instances of security attacks. With the innovation of smart metering infrastructure, there have been researches geared towards ensuring authentication in these energy systems. Most of the protocols proposed towards SMI authentication seem to adopt one-way authentication as opposed to two-way authentication. For instance, the most popular approach has been the use of enhanced public key infrastructure (PKI) in securing the smart grid networks [10]. This scheme is based on one-way authentication from a (SM) to the neighborhood area network gateway. Data specialists that have adopted the PKI strategy are convinced that digital signatures could be more effective in preventing service attack. In an effort to rationalize the viability of the enhanced scheme, data specialists have also implemented elliptic curve cryptography (ECC) for restricted (SM) [11] and it's imperative to have low complexity at the meter. However, there have been proposed the adoption of a privacy-preserving schemes [12]. In such schemes, cryptographic commitment is used for sending consumption rates from the meter to the utility through the neighborhood area networks utility. This approach also relies on one-way authentication as a strategy for achieving privacy. Although this approach too can be relied on in authenticating SM at the NAN gateway, it is unable to verify the legality of the NAN gateway. Subsequently, this approach is discouraged because it presents numerous security threats. For instance, the (SM) might accept unverified control commands from an intruder given that the (SM) does not verify the NAN gateway. This can easily result in power interruptions for the affected house. This is an indication that one-way authentication might not be a solution in securing two-way communication [10], [11], [13]. Alternative protocols used usually perform mutual authentication in the smart grid [11]. However, a majority of these schemes usually require high computational overhead which can easily lead to performance hitches in sensitive infrastructure. It would be better to use lightweight and secure authentication when performing mutual authentication. This is likely to help in verifying the SM prior to its communication with any other entity. One solution that has been suggested in this front is the use of the Diffie-Helman protocol. This protocol is essential in establishing mutual authentication and establishing a single session key between the (SM) and the neighborhood area network [14], [15]. There are also proposals that a secure session key between a SM and an authentication server can be used in mutual verification of communicating entities. In such approaches, a key generator is used in refreshing public and private keys together with multicasting keys. These are broadcasted periodically to smart meters [12]. However, similar schemes are faulted for being impractical and inefficient when dealing with smart meters. The justification for this disapproval is that the heavy computation required by this approach is unfeasible for smart meters [12]. Another proposal has been the use of a secure anonymous key distribution scheme for smart grid communications. The approach capitalizes on the use of identity-based signature to aid in mutual authentication and anonymity at a favorable cost [12] [16]. Further, the approach is capable of resisting several attacks including impersonation and replay. However, this scheme is faulted for failing to provide session key security and smart meter's credentials privacy using the Canetti-Krawczyk's attack model [17]. In order to address these shortcomings, there have been proposals to achieve authentication using a low computational cost that is relatively secure compared to the previously identified schemes. However, such schemes are also faulted for being vulnerable to impersonation attacks which in most instances result in the forgery of messages. This further poses integrity issues. One way of addressing these concerns is through the use of lightweight, and anonymous key distribution (AKD) scheme. The AKD usually relies on Schnorr's signature procedure which helps it achieve efficiency [12], [17], [18]. Another scheme proposed for authenticating smart metering networks entails using an identity based key establishment scheme [18]. The proponents of this scheme argue that it can help in securing attacks such as impersonation and replay attacks. The scheme is however faulted for its inability to endure spoofing attack given that the SM identity is usually in plain-text [16]. Additional contributions indicate that with consideration to PKI, a lightweight message authentication scheme can be used for smart grids. This needs the use of a hybrid cryptosystems [19]. From this scheme, it was realized that the operation of public keys such as encryption is attainable. However, this does not apply to the use of private keys given the time they consume. Another outsider and insider attack mitigation strategy in smart grids capitalizes on individual authentication and authorization before when accessing the SM. This entails the use of attribute-based access control which helps in confirming the identity of the user and the device [20]. However, this approach is faulted for having a higher overall overhead at 328.37 bytes, which is beyond the computational capabilities of most SMs. The scheme also strains the transmission capability and the energy source. This would affect a smart gas meter more than it would affect a smart electricity meter given that they are usually connected to the main supply. The gas meters, on the other hand, are battery-powered. This scheme will not be sustainable for the later given that the SM is bound to send periodic consumption trends that require more energy for the packets to be sent. This emphasizes the need for energy-efficient approaches necessary for maximizing the lifetime of the SM with the expected level of security [1], [3], [13], [21].Some latest development are also defined in [7], [22]–[26]. However, the scheme proposed in [22] was proved as weak to ephemeral secret leakage attack by [27]; moreover, owing to the use of pairing based

computation extensive operation, the scheme [22] was not appropriate for communication infrastructure of smart grid. Likewise, the incorrectness of the scheme proposed by Challa et al. [25] was explained by Chaudhry et al. [26] and the scheme [7] was proved to have incorrect authentication phase in [28].

From the analysis of existing one-way authentication schemes and factors such as high computational costs and communication costs, various questions are raised over two-way authentication in smart energy communication. As earlier indicated, in smart energy networks communication, the integrity of messages is essential just like any other security priorities. This is justified by the fact that message integrity is a reassurance that the messages are accurate despite being in transit. This is in line with recommendations from various regulatory bodies including National Institute Standards Technology (NIST) [11] [17] [29]. In the absence of integrity, the information is distorted. Subsequently, irregular decisions can be made in smart energy networks.

A. Motivation & Contributions

It is evident that some of the schemes that have been proposed lately are vulnerable. As such, these schemes can be easily attacked leading to violation of message integrity. This justifies the need for a mutual authentication which can sustain dynamic key agreement in realizing efficiency while at the same time providing significant levels of security functionalities. In such a move, very recently, Kumar et al. [2] introduced a lightweight authentication and key agreement (LAKA) scheme for smart metering infrastructure in smart energy networks, the work of Kumar et al. was structured over Elliptic Curve Cryptography (ECC), symmetric block ciphers, and hash functions. As per their claim the cost of the scheme was noted as a lower amount considering the fact that it is developed on the ECC, embraced symmetric encryption, and had a hash function and message authentication code. Moreover, the security analysis of the LAKA was carried out through AVISPA tool. The LAKA was also compared with respect to efficiency and performance with related schemes. However, in contrary to their claim, we show that the LAKA by Kumar et al. is insecure against ephemeral secret leakage attack. We also show that LAKA lacks untraceability and has weaknesses against stolen verifier attack.

B. System model

The system model as adopted from Kumar et al. [2] is shown in Fig. 1 with an exception of a specific trusted authority (TA), where a number of smart meters (SMs) are installed at different location and are connected with neighbourhood area network (NAN) gateway. The SMs are installed in building, homes and commercial/industrial units. The NAN gateway acts as an intermediate agent to provide on demand electricity and the communication between a SM and a NAN is always on insecure channel. Before, deployment, each SM and NAN gateway are registered by TA. Kumar et al. considered NAN gateway as trusted, which also acts as a regustration authority.

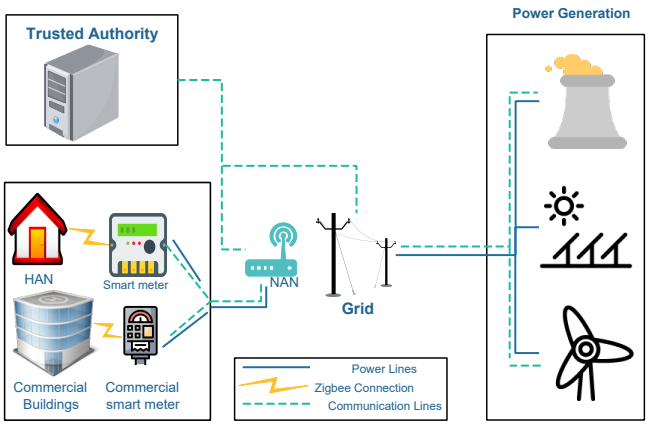

Fig. 1: Smart Grid Infrastructure

However, it is not a true depiction of the SG scenario. For the sake of keeping consistency and keeping the same assumption of NAN gateway trustworthiness, we also keep NAN gateway as trusted. However, in reality there is always a TA responsible for registration of both the SMs and NAN gateways.

C. Adversary Model

In this paper, we consider the eCK [30] adversary model. In which the adversary $\mathcal{A}$ has more capabilities as compared with D-Y model [31]. $\mathcal{A}$ under eCK model [32], has authority over the public channel and can perform any task including sending , receiving/listening, forging and blocking a legitimate message. $\mathcal{A}$ can expose the information stored on a captured SM [32]. $\mathcal{A}$ has access to all public information and SMs are not trusted, which means and dishonest SM can act as an attacker. Under eCK model, $\mathcal{A}$ can launch a key compromise impersonation attack as well.

III. Revisiting LAKA

Kumar et al.'s scheme (LAKA) involves two entities for authentication and key agreement. These include the SM and the neighborhood area networks gateway (NAN). LAKA is explained briefly in following subsections:

A. System Setup Phase

Since the NAN gateway is a trusted entity, it is expected to accomplish off-line tasks. Assigning security parameters, assigning the SM identity along with keeping access log are considered as offline tasks. The NAN gateway security parameters are as follows; The NAN selects an elliptic curve E together with point P of order n above E. A master key (M_k) and public key $P_s = M_k.P$. It then chooses one-way secure hash function $(e.g.H())$. Lastly, the M_k is kept in secure own database by publishing $F_p, P, E, n, P_s, H()$.

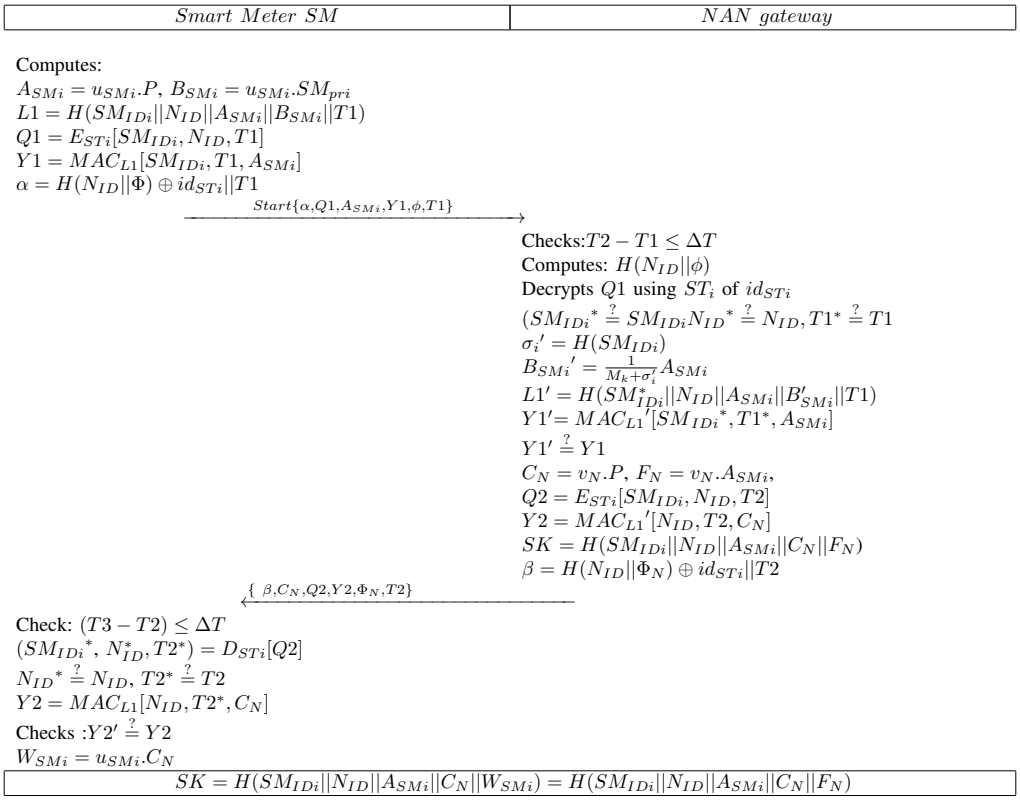

Fig. 2: Flow of Kumar et al.'s scheme

B. Registration Phase

Before a SM is included in the NAN gateway, it is essential to register them. This is done in preparation for participation in the smart energy network. The security parameters are obtained as follows; for every SM (j), the NAN then generates and allots a distinct identity (SM_{ID_i}) and a secret token ST_i with unique identifier (idSTi). It then relies on SM_{ID_i} in computing $\sigma_i = H(SM_{ID_i})$ and public key. That means $SMpub_i = (\sigma_i + M_k).P = \sigma_i P + P_s$. Subsequently, it uses the master key M_k to compute the smart meter's matching private key $SMpr_i = \frac{1}{M_k+\sigma_i}.P \in G$.NAN then stores the security parameters $(F_p, P, E, n, ST_i, id_{ST_i}, H(), \sigma_i, SMpr_i)$ in smart meters' memory which is temper-proof. The SM_{ID_i} and N_{ID} are stored in the memory of the meter which enables it to identify the respective NAN gateway. Lastly, the NAN gateway relies on its storage to keep all the parameters deployed to smart meters.

C. Authentication and Key Establishment Phase

For the LAKA's goals (lightweight authentication and key establishment) to be attained, the following procedure as shown in Fig. 2 is followed as below:

PAK 1: The SM relies on random numbers $u_{SM_i} \in Z_n^*$ followed by computing $A_{SMi} = u_{SMi}.P$ and $B_{SMi} = u_{SMi}.SM_{pri}$. Subsequently, $L1 = H(SM_{IDi}||N_{ID}||A_{SMi}||B_{SMi}||T1)$ and $Q1 = E_{STi}[SM_{IDi}, N_{ID}, T1]$ are computed. $T1$ is the smart mater's time stamp. To uphold the message integrity, the SM computes $Y1 = MAC_{L1}[SM_{IDi}, T1, A_{SMi}]$. As a result, a pseudo number (ϕ) is generated and used in computing $\alpha = H(N_{ID}||\Phi) \oplus id_{STi}||T1$. Ultimately, it sends a message, $\{\alpha, Q1, A_{SMi}, Y1, \phi, T1\}$ to the NAN.

PAK 2: When NAN receives the message, it verifies time validity using $T2 - T1 \leq \Delta T$. In case the time validity is unverified, the process is rejected by the system. Note: $T2$ symbolizes the current time stamp of NAN and ΔT refers to transmission delay. However when the validity is verified, it calculates $H(N_{ID}||\Phi_N)$ to obtain id_{STi} gets matching token (STi) of id_{STi}, and SM_{ID_i} from own database. It will then decrypt $D_{ST_i}[Q1]$ and subsequently obtain $SM^*_{IDi}, N^*_{ID}, T1^*)$. From the checks $SM^*_{IDi} \stackrel{?}{=} SM_{IDi}, N^*_{ID} \stackrel{?}{=} N_{ID}$ and $T1^* = T1$), in the event that the conditions are not verified, the ongoing session is rejected. Subsequently, the NAN gateway proceeds to compute $\sigma_i' = H(SM_{IDi})$, $B_{SMi}{}' = \frac{1}{M_k+\sigma_i'} A_{SMi}$ and $L1' = H(SM^*_{IDi}||N_{ID}||A_{SMi}||B'_{SMi}||T1)$. Additionally, it computes $Y1' = MAC'_{L1}[SM^*_{IDi}, T1^*, A_{SMi}]$. If the verification indicates that $Y1' = Y1$, then it moves to the next step.

PAK 3: NAN gateway then chooses a random number $v_N \in Z_n^*$ then calculates $C_N = v_N.P$, and $F_N = v_N.A_{SM_i}$. This is followed by computing $Q2 = E_{STi}[SM_{IDi}, N_{ID}, T2]$ and $Y2 =$

$MAC_{L1}{}'[N_{ID}, T2, C_N]$. In this step, $T2$ denotes current time stamp of NAN. Subsequently, a session key $SK = H(SM_{IDi}||N_{ID}||A_{SMi}||C_N||F_N)$ is developed. Ultimately, a pseudo number (Φ_N) is generated. This is computed as $\beta = H(N_{ID}||\Phi_N) \oplus id_{STi}||T2)$. The Response = { $\beta, C_N, Q2, Y2, \Phi_N, T2\}$ is then sent to the SM.

PAK 4: The SM checks $(T3 - T2) \leq \Delta T$ and terminates the session in the event that the verification produces negative results. However, if it obtains id_{STi} from β and subsequently, SM decrypts $D_{STi}[Q2]$ and obtains $SM_{IDi}{}^*$, $N_{ID}{}^*, T2^*$ then verification is attained. This is signified by $N_{ID}{}^* \stackrel{?}{=} N_{ID}$ and $T2^* \stackrel{?}{=} T2$. if the conditions turn out not to be true, then the session will be terminated. Otherwise, the computation would be $Y2 = MAC_{L1}[N_{ID}, T2^*, C_N]$ and verifies $Y2' = Y2$ if the condition proves to be true, then it moves to the next step. Otherwise, the NAN is illegitimate and this warrants termination. Ultimately, the SM computes $W_{SMi} = u_{SMi}.C_N$ leading into generation of the session key $SK = H(SM_{IDi}||N_{ID}||A_{SMi}||C_N||W_{SMi})$ to secure the next communication between the SM and Nan gateway.

IV. Weaknesses of LAKA

In this section we argue the weaknesses of LAKA against ephemeral secret leakage attack (KCIA), stolen verifier attack along with LAKA's inability to provide traceability:

A. Ephemeral Secret Leakage Attack

The security of the LAKA scheme by Kumar et al. is based on four types of parameters: 1) public parameters SM_{IDi}, 2) the parameters sent on public channel A_{SMi}, C_N, 3) the shared parameter N_{ID} among all SMs connected with a NAN gateway and 4) Temporary session parameters u_{smj}, v_N. The public parameters and parameters sent on public channel are accessible to all entities, while the shared parameter N_{ID} can be easily extracted from any captured smart meter. Now as per above argument, the security of the session key relies only on two temporary variables u_{smj}, v_N and if any of these parameters is leaked, the session key may be compromised. Like, if u_{smj} is leaked, $\mathcal{A}$ can compute $W_{SMi} = u_{SMi}.C_N$ and $SK = H(SM_{IDi}||N_{ID}||A_{SMi}||C_N||W_{SMi})$. Similarly, if v_N is exposed $\mathcal{A}$ can compute $F_N = v_N.A_{SMi}$ and the session key $Sk = H(SM_{IDi}||N_{ID}||A_{SMi}||C_N||F_{Nj})$. Hence, the LAKA scheme by is insecure against ephemeral secret leakage attack.

B. Traceability Attack

The SM in LAKA scheme by Kumar et al. is also insecure against traceability attack. Any attacker $\mathcal{A}$ can get N_{ID} from a captured SM and can use this value to trace any SM requesting for AKA. Let a SM initiates an AKA request through message $\{\alpha, Q1, A_{SMi}, Y1, \phi, T1\}$, the $\mathcal{A}$ using N_{ID} and the intercepted ϕ computes $H(N_{ID}||\phi)$ and now using the computed value, $\mathcal{A}$ can compute $id_{STi}||T1 = H(N_{ID}||\Phi) \oplus \alpha$, where $T1$ is the current timestamp and id_{STi} is the unique identifier of a SM. Hence, SM in LAKA scheme has weaknesses against traceability attack.

C. Stolen Verifier Attack

In LAKA scheme, the NAN gateway stores ST_i and id_{STi} tuples for each SM in a verifier/database. This verifier/database is subject to stolen verifier attack.

V. Conclusion

The analysis in this article shows that the smart grid authentication scheme (LAKA) by Kumar et al. has weaknesses against ephemeral secret leakage attack. An attacker after exposing the ephemeral secrets of any of the NAN gateway or SM can compute any session key shared among both. Moreover, it is also shown that LAKA cannot protect untraceability and has weaknesses against stolen verifier attack. In future, we intend to design a computation restricted SM grid authentication scheme with traceability, with out verifer tables and resistant to ephemeral secret leakage attack.

References

[1] N. Saxena et al., "State of the art authentication, access control, and secure integration in smart grid," *Energies*, vol. 8, no. 10, pp. 11 883–11 915, 2015.

[2] P. Kumar et al., "Lightweight authentication and key agreement for smart metering in smart energy networks," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 4349–4359, 2018.

[3] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1437–1443, September 2012.

[4] M. Asshad et al., "Using moment generating function for performance analysis in non-regenerative cooperative relay networks with max-min relay selection," *AEU-International Journal of Electronics and Communications*, vol. 116, p. 153066, 2020.

[5] S. Chaudhry et al., "A secure and reliable device access control scheme for iot based sensor cloud systems," *IEEE Access*, vol. 8, pp. 139 244–139 254, 2020.

[6] N. Komninos et al., "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts*, vol. 16, no. 4, pp. 1933–1954, 2014.

[7] N. Kumar et al., "Eccauth: A secure authentication protocol for demand response management in a smart grid system," *in IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6572–6582, December 2019.

[8] S. Finster and I. Baumgart, "Privacy-aware smart metering: A survey," *IEEE Commun. Surveys Tuts*, vol. 16, no. 3, pp. 1732–1745, 2015.

[9] Z. Erkin et al., "Privacy-preserving data aggregation in smart metering systems: An overview," *IEEE Signal Process*, vol. 30, no. 2, pp. 75–86, March 2013.

[10] N. Saxena et al., "Authentication and authorization scheme for various user roles and devices in smart grid," *IEEE Trans. Inf Forensics Security*, vol. 11, no. 5, pp. 907–921, May 2016.

[11] M. Fouda et al., "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, December 2011.

[12] T. Chim et al., "Prga: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid," *IEEE Trans. Depend. Secure Comput*, vol. 12, no. 1, pp. 85–97, 2015.

[13] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, 2013.

[14] E. Ayday and S. Rajagopal, *Secure device authentication mechanisms for the smart grid-enabled home area networks*. Rep, 2013.

[15] S. A. Khan et al., "A power control algorithm (pca) and software tool for femtocells in lte-a networks," *Sakarya University Journal of Science*, vol. 22, no. 4, pp. 1124–1129, 2018.

[16] H. Li et al., "An efficient merkletree-based authentication scheme for smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 655–663, June 2014.

[17] M. Nabeel et al., "Authentication and key management for advanced metering infrastructures utilizing physically unclonable functions," in *Proc. IEEE 3rd Int Conf. Smart Grid Commun. (SmartGridComm)*, 2012, pp. 324–329.
[18] D. He et al., "An enhanced public key infrastructure to secure smart grid wireless communication networks," *IEEE Netw.*, vol. 28, no. 1, pp. 10–16, 2014.
[19] H. Nicanfar et al., "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Syst. J.*, vol. 8, no. 2, pp. 629–640, June 2014.
[20] Y. Yan et al., "An efficient security protocol for advanced metering infrastructure in smart grid," *IEEE Netw.*, vol. 27, no. 4, pp. 64–71, 2013.
[21] J. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, March 2016.
[22] K. Mahmood et al., "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Generation Computer Systems*, vol. 88, pp. 491–500, 2018.
[23] S. Chaudhry et al., "Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure," *IEEE Access*, vol. 8, pp. 101 235–101 243, 2020.
[24] K. Mahmood et al., "An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure," *International Journal of Communication Systems*, vol. 32, p. 16, 2019.
[25] S. Challa et al., *Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems*. Future Generation Computer Systems, 2018.
[26] S. Chaudhry et al., "Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems," *Computer Communications*, 2020.
[27] X. Liang et al., "Cryptanalysis of a pairing-based anonymous key agreement scheme for smart grid," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing*. Springer, 2020, pp. 125–131.
[28] S. Chaudhry et al., "10 correctness of an authentication scheme for managing demand response in smart grid," *Smart-Grid in IoT-Enabled Spaces: The Road to Intelligence in Power*, p. 223, 2020.
[29] V. Odelu et al., "Provably secure authenticated key agreement scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2018.
[30] B. LaMacchia et al., "Stronger security of authenticated key exchange," in *International conference on provable security*. Springer, 2007, pp. 1–16.
[31] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.
[32] T. Eisenbarth et al., "On the power of power analysis in the real world: A complete break of the keeloq code hopping scheme," in *Annual International Cryptology Conference*. Springer, 2008, pp. 203–220.