Review of key management techniques for advanced metering infrastructure

Otisitswe Kebotogetse, Ravi Samikannu and Abid Yahya

Abstract
The electricity industry has been developed through the introduction of the smart grid. This has brought about two-way communication to the grid and its components. The smart grid has managed to increase the efficiency and reliability of the traditional power grid over the years. A smart grid has a system that is used to measure and collect readings for power consumption reflection, and the system is known as the Advanced Metering Infrastructure. The advanced metering infrastructure has its components too which are the smart metre, metre control system, collector or concentrator and communication networks (wide area network, neighbourhood area network, and home area network). The communication networks in the advanced metering infrastructure have created a vulnerability to cyber-attacks over the years. The reliability of the power grid to consumers relies on the readings from the smart metre, and this brings about the need to secure the smart metre data. This article presents a review of key management methods in advanced metering infrastructure environments. The article begins with an overview of advanced metering infrastructure and then shows the relationship between the advanced metering infrastructure and the smart grid. The review then provides the security issues related to advanced metering infrastructure. Finally, the article provides existing works of key management methods in advanced metering infrastructure and future directions in securing advanced metering infrastructure and the smart grid.

Keywords
Advanced metering infrastructure, key management, smart grid, smart metre

Date received: 30 March 2021; accepted: 27 July 2021
Handling Editor: Yanjiao Chen

Introduction
Every country’s economic and social welfare relies mostly on electricity. Electricity is responsible for daily operations in industries and is used for domestic purposes. At home, electricity is used for cooking, lighting, house appliances and other domestic/household chores. Electricity providers face challenges of managing the generation, transmission and distribution of electricity efficiently, and at the same time making profit. The demand for renewable energy supply and numerous technological advancements that are increasing has motivated providers to develop smart grids. The adoption of smart grids has brought about a solution to these challenges faced by providers, as it has many advantages than disadvantages over traditional power systems or one-way power systems. Smart grids use digital technology to intelligently implement the actions of all users connected to them. Smart Grids are characterized by huge and complicated interconnections of
networks carrying electricity flows. European Union (EU) definition for smart grid is an electricity network that can intelligently integrate the behaviour and actions of all users to ensure sustainable, economic and secure electricity supply. The definition of US Department of Energy (DoE) states that a smart grid has digital technology that improves reliability, security and efficiency of electrical systems. The smart grid is made up of four components which are the advanced metering infrastructure (AMI), supervisory control and data acquisition (SCADA), plug-in hybrid electric vehicle (PHEV) and communication protocols and standards.

Information and communication technology (ICT) is the core component of the smart grid. ICT empowers the power grids of today by giving them a two-way communication capability, restoring and isolating power outages faster, encouraging the integration of renewable electricity sources into the network and enabling the consumer to optimize their power consumption. This leads to a progressively significant part within the communication infrastructure and a heavier reliance on the execution of the complete control framework on the communication networks’ execution. As technology continues to be enhanced and improved for power grids’ capabilities, they become complex and vulnerable to different types of attacks. Figure 1 shows an example of some of the components of the smart grid.

Smart metres remain the most widely used application of the Internet of Things (IoT) today. A report for the smart metre market for the years 2019–2024 estimates smart metre usage worldwide to have exceeded 14% in 2019. Thus, 14% of metres used for energy have been replaced by smart metres now. The Asia-Pacific is the world’s leading continent in smart metres, followed by Europe and third on the list is North America. Asia-Pacific demands around 110–200 million electricity metres annually, with China being the leading country at 70% of the volume. The AMI constitutes network, a management system (billing information, account management and other data) and smart metres as shown in Figure 2; all these play a vital role in the bi-directional flow of information between the power grid and the smart metering.

AMI has four main components: smart metre, metre data management system (MDMS), data concentrator, and communication networks.

**Smart meter**

Smart metre is an electronic device that records data indicating consumption of energy, water or natural gas in a house or home. Power utilities highly use the device to monitor customers’ consumption of electricity. Smart metres are also used to forecast for production of electricity to meet the demand. Smart metre sends readings to the MDMS.

**MDMS**

This is the control sever of AMI. The MDMS receives data from the collector and process billing information.
MDMS also commands the smart metre to perform required actions.\textsuperscript{12}

**Data concentrator**

This is also known as the collector. It is an intermediate device that collects data from the smart metre and directs it to the MDMS.

**Communication networks**

Communication networks are the base of the two-way communication flow within the AMI. There are three networks which are home area network (HAN), neighbourhood area network (NAN) and wide area network (WAN).\textsuperscript{13} HAN uses Zigbee technology, NAN uses Wi-Fi technology and WAN uses the Global System for Mobile Communications (GSM) technology. Figure 3 illustrates the three communication networks.

AMI just like other systems needs to follow or obey the security requirements: confidentiality, integrity, accountability and availability.

**Confidentiality**

This is keeping data private or secret from unauthorized access. In AMI, confidentiality is practised by keeping private the customer’s consumption pattern and personal information of the customer.\textsuperscript{15} Only authorized entities can access these data.

**Integrity**

This is the state of being honest and whole without any division. In AMI, integrity is practised by maintaining the system to be whole, and this is done by detecting illegal tempering with data.

**Accountability**

This is being responsible or answerable to all the actions. In AMI, accountability is practised by responding to commands within a timely manner and not denying actions of receiving or transmitting data.

**Availability**

This is the state of being unoccupied and able to be used. In AMI, availability is practised when an authorized user gets access to the data required whenever they are on demand. Whenever the system does not provide required data on demand, the system will be violating the availability aspect.

Cryptographic techniques should be adopted for the security requirements discussed above to be ensured in AMI. Key management systems that are efficient are needed for the cryptographic techniques to secure AMI.\textsuperscript{16} The most important aspects to consider before any AMI installation are as follows:

- Customer data should be protected through confidentiality security aspect.
- Messages should be authenticated (messages for metre readings, load control and other messages that are shared in AMI).

Over the years, there have been security threats to smart metre readings aggregation and consumers’ privacy. The data transmitted during these processes should be guaranteed to have integrity and confidentiality. The proposed research works addressing these security concerns have been developed. Some works focus on deploying hardware devices at the consumer’s side, which is very expensive as the devices will be needed for each smart metre in the grid.\textsuperscript{17,18} Other research works focus on the distortion of the readings at the transmitter and reconstructing them at the receiver, requiring complex computations.\textsuperscript{19,20} Cryptographic security schemes have proven to be useful in guaranteeing security and privacy without the need for expensive or complex devices.\textsuperscript{21,22} However, most of the proposed cryptographic security schemes are of high computation and smart metres have low computational abilities. This created the need to come up with schemes that are

![Figure 3. Communication network connection of AMI.\textsuperscript{14}]
lightweight but at the same time providing privacy and following all security requirements.

**Security issues and challenges related to AMI**

As the smart grid deployments and enhancements continue to grow, the AMI was developed as one of the enhancements. The development of AMI came with security challenges, and these challenges can be addressed in three aspects which are end user privacy, system resisting cyber-attacks and illegal power consumption.

**End user privacy**

There are three approaches for end user privacy in AMI applications. The three approaches are anonymization, hybrid and non-anonymization. The utility provider determines the best privacy approach as a mutual agreement between them and customers.

**Anonymization.** This is a privacy approach whereby data cannot be retrieved when they are on transit or when in the smart metre or at the utility provider’s side. The privacy approach is usually done when disassociating customer ID and consumption data. The utility provider here cannot generate any billing information because they cannot match any customer ID to consumption data.

**Hybrid.** This is a privacy approach whereby only the customer ID is revealed at the utility provider’s side but the consumption data are not revealed to the utility provider. The consumption data are modified before being transmitted to the utility provider making it difficult for the utility provider to make correct conclusions. In this case, the utility provider receives data from the specified customer ID, but the consumption data do not reveal the customer’s correct consumption.

**Non-anonymization.** This is a privacy approach whereby privacy is provided only when data are in transit, thus when transmission of consumption data from the smart metre to the utility provider occurs. The utility provider can retrieve customer ID and correct consumption data after receiving data from the smart metre. This is the most used approach as utility providers are trusted with customer’s data. Encryption occurs during the transmission of data.

**System resisting cyber-attacks**

The operation or deployment of AMI in the smart grid has brought about vulnerability to cyber-attacks. Attackers target smart metre readings, billing information and customer information. The attackers or intruders are usually highly skilled in cyber, and they look for different weaknesses of the system to exploit the necessary information they are looking for. They usually access AMI configuration by cyber means and temper with the firmware.

The vulnerabilities discussed above are usually avoided or prevented by introducing four security aspects in AMI infrastructure which are confidentiality, integrity, availability and accountability. Cheating of customers is avoided by the introduction of these security aspects. Attackers usually develop hacking tools which are targeting systems without these strong security aspects. In AMI, the four aspects are vital during the deployment of the system. Cyber-attacks can also be targeting a nation or state as a form of terrorism. Attackers may take control of the whole grid in demand for money or power from a nation or state. If the security aspects are in place, it is difficult for these intruders to take over the system.

**Illegal power consumption**

The most popular way of illegal consumption of power is tapping the energy from transmission lines. Illegal consumers can also manipulate metres to consume from the grid illegally. The techniques used or adopted by these illegal consumers use magnetic materials to destroy the memory of the energy metre, introduction of unwanted harmonics, interchanging metre terminals and others. The introduction of AMI has led to a reduction to most if not all the illegal consumption of electricity. Smart metres notify the utility provider whenever the readings are tempered with. The utility provider can study each customer’s consumption pattern from previous readings, which means whenever the pattern changes, an investigation is made. Attackers targeting tempering with metre readings during transit often forget that there is an associated log that goes along for every activity. Monitoring of logs in the AMI makes it easier for the detection of illegal power consumption.

**Attacks on AMI**

There are five main components of the smart metre: central unit, metrology system, the collector, HAN, and optical interface. All the components have attacks related to compromising the general security of AMI as highlighted by Table 1. Hardware and reverse engineering can impact the control unit and metrology system, enabling the attacker to access information and privileges that they can use to exploit data. Attackers may also modify the control unit circuit board, enabling remote control of the smart metre on their side.
Modification of the control unit may also deny legitimate users access to the system as their data are tampered with. The communication between the smart metre and AMI happens through the collector in the smart metre. The communication between the two can be consumption readings, commands on firmware updates, and configurations. The attacks that may arise from this communication or flow of data disturb the power grid, theft of power, and denial of service.30 On the HAN, the possible attacks that occur are stealing of data and blocking data flow. The optical interface is where a technician installs and configures software in the smart metre. The attacks in the optical interface are interception and firmware attacks, resulting in power denial and disruption of the power grid in general.

Key management methods

There are three transmission modes in key management, which are unicast, multicast and broadcast.

Unicast transmission mode

This transmission mode is used for communications between two points.31 The data are transmitted from the sender and go directly to one specified receiver. Only these two devices participate in the communication and other devices in the network stay idle.32 In the AMI network, unicast transmission or communication occurs when the smart metre sends consumption data to the utility provider.33

Multicast transmission mode

This transmission mode is used for communication between one point and many specified points, referred to as a group.34 Multicast transmission can also be a group of senders to a group of receivers thus when many senders communicate to many receivers simultaneously,35 group to group. In the AMI network, multicast transmission or communication takes place when the utility provider sends out notification messages to a group of smart metres in the same location or demand response (DR) group; the DR group can be smart metres for businesses, and the group depends on the DR project or classification.36 In multicast communication, only the chosen DR group receives the message and other groups do not receive the message.

Broadcast transmission mode

This transmission mode is used for communication between one point and all other points in the network.37 Broadcast transmission was first used in the AM radio, and now it is continuously used in both radio and television for distribution of audio and video, respectively. In the AMI network, broadcast transmission or communication occurs when the utility company communicates changes in electricity pricing to all consumers and when notifying the consumers of power outages or any other ongoing project that may interrupt the service of power distribution.38 In broadcast communication, privacy is not key; thus, anyone in the network receives the message.

In the key management systems, different approaches are adopted for efficient management of keys.36 Table 2 shows the different approaches and the techniques used in each approach.

Related works

Over the years, some work has been carried out in key management techniques for security of the smart metre and the smart grid in general.

The work in Rafaeli and Hutchison49 shows that research on group key management has been done over

| Attack | Place of attack | Impact |
|--------|----------------|--------|
| Blocking of service | Remote access to WAN | Malfunctioning of the power grid and also the AMI. |
| Firmware attack | Physically accessing the smart metre/Remotely upgrading WAN via the gateway | Affects the ability of the smart metre to measure. |
| Injection of packet | Accessing WAN | Wrong billings to consumers and utility providers. |
| Eavesdropping | Remotely accessing of WAN | Detect and expose consumer’s privacy. |
| Remote control of the attacker | Accessing WAN | Distortion of metre readings at consumers and being transferred to the whole grid. |
| Interception | On the local metrological network (LMN) or WAN | Wrong readings feed to the gateway. |

WAN: wide area network; AMI: advanced metering infrastructure.
The approaches from previous work are divided into three main categories: centralized group, decentralized architectures and distributed key management protocols.

In Yan et al., an efficient batch authentication scheme for smart grid using binary authentication tree is proposed. The scheme enables the gateway in AMI that verifies smart metre data to batch authenticate data.

Kamto et al. proposed a key management scheme that combined Needham–Schroeder authentication protocol and a cryptographic method known as elliptic curve. The key management scheme uses a trust anchor to establish a session key. In Wen et al., a technology that provides strong hardware-based authentication for smart metres and provides efficient key management to assure confidentiality and integrity of communication between the smart metre and the utility provider is proposed. The technology is called a physically unclonable function (PUF). The system is directly installed in existing smart metre communication without the need for modification of the metre.

In Benmalek and Challal, a scalable multi group key management method to be used in AMI is proposed. The work supports the three modes of communication: unicast, multicast and broadcast by using multi group key technique. The method is very applicable to large-scale smart grids.

The work in Benmalek et al. proposes four key management schemes for AMI, to secure

| Table 2. Different key management approaches. |
| Key approach | Technique | Description | Related work |
|---------------|-----------|-------------|--------------|
| Double encryption | Authentication based | The method uses two servers and these servers function without increasing the number of packet overheads. | Parvez et al. |
| Tree key graph | Key graph | The method is based on the use of key graphs. The key graph controls keys of individual smart metres, ensuring the security requirements. In this method, the data are kept private to avoid unauthorized access to consumer’s daily habits. | Liu et al. and Yu et al. |
| Broadcast group key management | PUF based | This method uses weak physical unclonable functions (PUFs). PUF is an electronic connection that deploys variations in manufacturing to produce unique digital finger prints. These PUFs provide robust authentication to smart metre and data collector in the AMI. | Nabeel et al. |
| Hash chain | PUF based | This method uses PUFs and brings in the Schnorr protocol for authentication broadcast messaging protocol in AMI. | Delavar et al. |
| Multi group key graph | Key graph | The method creates secure cryptographic keys for every smart metre and MDMS over a public channel. The keys are made in such a way that they refresh after every transmission for assurance of security. | Benmalek et al. |
| Enhanced identity-based cryptography | Authentication based | This method authenticates the smart metre with a server in the smart grid. The approach adopts a key management protocol for secure communication using public key. | Nicanfar et al. |
| ID-based encryption | Hybrid | The method combines private and public key cryptography. Different encryption algorithms can be used here to achieve the combination or the double encryption/decryption system. The known work of this method used elliptic curve cryptosystem. In this method, public key certificate is not needed. | Wan et al. |
| Advanced encryption standard | Hybrid | The method has an initial stage to eliminate or reduce computation overhead that uses elliptic curve cryptography. The method provides data encapsulation and its initial stage provides key encapsulation. | Khasawneh and Kadoch |

AMI: advanced metering infrastructure; MDMS: metre data management system.
communication in the smart grid. The proposed schemes are based on individual and batch rekeying operations and support unicasts, multicasts and broadcast communications.

In Benmalek et al., a new key management scheme called iVerSAMI is proposed. The proposed scheme is aimed at addressing the efficiency flaws in broadcast key management protocol suffered by VerSAMI key graph–based scheme. The work shows that iVerSAMI is more secure and efficient than VerSAMI in terms of storage and communication overheads.

The work in Manjul and Mishra proposed an approach known as elliptic curve cryptography (ECC)-based secure group communication. The approach is aimed at providing an efficient and improved mechanism for group key management solutions. The method minimizes rekeying cost and reduces computational and communication overheads.

The work of Kumar et al. proposed a key management scheme designed for HAN having low rekeying overheads and robustness that is enhanced, allowing the smart metres and HAN to share a session key among themselves. The scheme does not require update to the keys whenever a smart metre leaves or joins the system. This has reduced the rekeying cost compared to other existing key management schemes.

In El-Hajjar and Hanzo, a novel key management scheme based on the key graph method is proposed. The scheme had three different key management processes designed for hybrid transmission modes, unicasts, multicasts and broadcasts. Key management problems in AMI were addressed in Liu et al. with the proposed novel Key Management Systems (KMS). In Kumar et al., the work of securing communication between multiple users using key graphs is proposed. The method was later found to be weak by Wan et al. The work found that the method was vulnerable to the denial of service attack and proposed a solution to address this problem. Wan et al. addresses the problem of de-synchronization attack and lack of scalability due to inefficient key management in Liu et al. The proposed new scalable key management method combined identity-based cryptosystem and efficient key tree method. The solution was meant for securing smart metre and MDMS communication.

The work in Thomas et al. describes and implements a signature-based station-to-station protocol for exchanging the secret shared keys among the AMI applications to eliminate undesirable security threats. Secure Hash Algorithm (SHA-1) hashing algorithm is used for creation digital signatures using private key encryption.

A secure IP multicasting system using encryption key management in an iNet environment was proposed by Maharjan et al. The system delivers keys between multiple users and provides a link between key management centre and multicast network.

In Benmalek et al., a scalable multi group key management scheme for AMI is proposed. The scheme introduced low storage overheads when compared to others and also indicated low communication overheads.

In Parvez et al., a key management-based scheme having two simple servers is proposed. The scheme focuses on a two-level encryption that does not result in increased packet overhead. Encryption secret keys are generated by using hash functions in Kiarie et al. The method is anticipated to be a good approach to deal with 128 bit keys in encryption.

**Future directions**

AMI communication network security issues and challenges continue to be a major concern regardless of previous researchers’ huge efforts. There is still need for future research ventures related to the smart grid, particularly key management in AMI. The AMI network comprises smart metres, customers and also the utility providers. The ‘Related works’ section describes the research efforts made over the years to provide security to AMI systems. However, there are still vulnerabilities and issues that arise and this has provided potential research areas. The areas such as scalable architecture, consumer privacy and security, defensive mechanisms to address attacks and threats and content-centric networking still have room for research ventures in AMI and key management. The smart grid has a large number of sensors connected to it. The sensors are connected over a wide area to control and monitor activities in the smart grid. Building a scalable architecture for AMI network to deal with large amounts of data from these sensors is a major challenge faced by the smart grid. It has been evident from the past research works that most solutions do not address the issue of scalability in the smart grid which is a major requirement of a growing grid. Scalability and efficiency of AMI communication will make secure and efficient meter data collection and distribution of messages. A few works address the issue of scalability, which are seen in Benmalek et al. and Wan et al. The proposed solutions that address scalability have shown that key management in AMI is a promising outcome, which means that work in the future should focus on the design of robust, scalable AMI communication.

Protection and security of consumers is one of the major requirements of the smart grid AMI communication. To address the requirement, smart metres should be installed and encrypted with the latest security components for reliable storage. Smart metres should be
able to allow only authorized personnel to access them. Smart metres work on making sure that consumers' protection and privacy are ongoing and they are being encrypted with secure storage components for high security. It is also evident that key management is a very important component in securing AMI in smart grid from the above literature. The use of key management systems minimizes factors like overhead, and this brings about the need to have new and more efficient key management systems. The smart metres have low computational abilities, and this requires the proposed security mechanisms to be lightweight.

A method that uses hash functions to generate keys is proposed as hash functions have low resource consumption. Smart metres have low memory, and this provides the need to have a security mechanism scheme that reduces memory usage. The mechanism or scheme proposed must avoid node compromise attacks. The security must allow the network to add more smart metres to the existing network, thus improving scalability.

Conclusion

In this review article, the work focuses on studying the key management methods used in AMI. The article starts with a brief history of the introduction of smart grid and shows the smart grid and AMI relationship. Second, the article states the security issues and challenges related to AMI. The key management methods that can be used to secure or protect AMI communication network are described, and the works from previous researchers are discussed. Finally, the article shows the future directions that can be adopted to improve AMI's security and the smart grid. This article provides the reader with information about the previous work done in securing AMI systems and the existing gaps open for future work in the security of AMI communication.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.

ORCID iDs

Otisitswe Kebotogetse https://orcid.org/0000-0002-9653-5223
Ravi Samikannu https://orcid.org/0000-0002-6945-6562

References

1. Schmalensee R. The future of the US electric grid. Cambridge, MA: The MIT Press, 2015.
2. Zhu Z, Lambotharan S, Chin WH, et al. Overview of demand management in smart grid and enabling wireless communication technologies. IEEE Wirel Commun 2012; 19: 48–56.
3. Halim F, Yussof S and Rusli ME. Cyber security issues in smart meter and their solutions. Int J Comput Sci Netw Secur 2018; 18(3): 99–109.
4. Li W and Zhang X. Simulation of the smart grid communications: challenges, techniques, and future trends. Comput Electr Eng 2014; 40(1): 270–288.
5. ‘Nikki’ Fried N. The smart grid. My Florida Home Energy. 2015, https://www.myfloridahomeenergy.com/help/library/energy-services/smart-grid/#sthash.dQYqxs89.dpys
6. Scully P. Smart meter market 2019: global penetration reached 14% – North America, Europe ahead, 2019, https://iot-analytics.com/smart-meter-market-2019-global-penetration-reached-14-percent/
7. Rausser G, Strielkowski W and Štreimikiene D. Smart meters and household electricity consumption: a case study in Ireland. Energ Environ 2018; 29(1): 131–146.
8. Research and Markets. Global smart metering market 2019: in-depth analysis and unique insights into Europe, Asia-Pacific and North America, 2019, https://www.prnewswire.com/news-releases/global-smart-metering-market-2019-in-depth-analysis-and-unique-insights-into-europe-asia-pacific-north-america-300884650.html
9. Komninos N, Philippou E and Pitsillides A. Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun Surv Tut 2014; 16: 1933–1954.
10. Wang Y, Chen Q, Hong T, et al. Review of smart meter data analytics: applications, methodologies, and challenges. IEEE T Smart Grid 2019; 10(3): 3125–3148.
11. Patel Umang M and Modi Mitul M. A review on smart meter system. Int J Innovat Res Electr Electron Instrum Contr Eng 2015; 3(12): 70–73.
12. Young W. Meter data management system, 2007, https://www.smart-energy.com/wp-content/uploads/latest%20JEAC%20MDMS%20Overview%20-%20%20AMI%20MDM%20AUG07a.pdf
13. De Carvalho RS, Sen PK, Velaga YN, et al. Communication system design for an advanced metering infrastructure. Sensors 2018; 18(11): 3734.
14. Faisal MA, Aung Z, Williams JR, et al. Securing advanced metering infrastructure using intrusion detection system with data stream mining. In: Chau M, Wang GA, Yue WT, et al. (eds) Intelligence and security informatics (PAISI 2012), vol. 7299. Berlin; Heidelberg: Springer, 2012, pp.96–111.
15. Ye F, Qian Y and Hu RQ. A security protocol for advanced metering infrastructure in smart grid. In: Proceedings of the 2014 IEEE global communications conference (GLOBECOM'2014), Austin, TX, 8–12 December 2014, pp.649–654. New York: IEEE.
16. Alohalhi B, Kifayat K, Shi Q, et al. A survey on cryptography key management schemes for smart grid. J Comput Sci Appl 2015; 3(3A): 27–39.
17. Chen Z, Min L, Huang C, et al. Demand side energy management under emergency conditions. In: Proceedings of the 2018 IEEE power and energy society general meeting, Portland, OR, 5–10 August 2018. New York: IEEE.

18. Mo Y, Kim THJ, Brancik K, et al. Cyber–physical security of a smart grid infrastructure. P IEEE 2012; 100(1): 195–209.

19. Jia W, Zhu H, Cao Z, et al. Human-factor-aware privacy-preserving aggregation in smart grid. IEEE Syst J 2014; 8(2): 598–607.

20. Jia W, Zhu H, Cao Z, et al. Human-factor-aware privacy-preserving aggregation in smart grid. IEEE Syst J 2014; 8(2): 598–607.

21. Sankar L, Raj Rajagopalan S, Mohajer S, et al. Smart meter privacy: a theoretical framework. IEEE T Smart Grid 2013; 4(2): 837–846.

22. Namboodiri V, Aravinthan V, Mohapatra SN, et al. Toward a secure wireless-based home area network for metering in smart grids. IEEE Syst J 2014; 8: 509–520.

23. Esayas SY. The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the ‘all or nothing’ approach. Eur J Law Technol 2015; 6(2): 1–28.

24. Saputro N and Akkaya K. On preserving user privacy in Smart Grid advanced metering infrastructure applications. Secur Commun Netw 2014; 7(1): 206–220.

25. Anzalchi A and Sarwat A. A survey on security assessment of metering infrastructure in Smart Grid system. In: Proceedings of the IEEE SoutheastCon, Fort Lauderdale, FL, 9–12 April 2015. New York: IEEE.

26. Parks RC. Advanced metering infrastructure security considerations. Sandia report, 2007, pp.1–34. Sandia National Laboratories, https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/20-AMI_Security _Considerations.pdf

27. Depuru SSSR. Modeling, detection, and prevention of electricity theft for enhanced performance and security of power grid. PhD Thesis, The University of Toledo, Toledo, OH, August 2012, p.141.

28. Taranu M, Sharma D and Singh D. A survey of monitoring and controlling power theft problem in local area. Int J Adv Res Idea Innov Technol 2017; 3: 401–405.

29. Khattak AM, Khanji S and Khan WA. Smart meter security: vulnerabilities, threat impacts, and countermeasures. In: Proceedings of the 13th international conference on ubiquitous information management and communication (IMCOM), Phuket, Thailand, 4–6 January 2019. Cham: Springer.

30. Yi P, Zhu T, Zhang Q, et al. Puppet attack: a denial of service attack in advanced metering infrastructure network. J Netw Comput Appl 2016; 59: 325–332.

31. Zhao J, Gündüz D, Simeone O, et al. Non-orthogonal unicast and broadcast transmission via joint beamforming and LDM in cellular networks. IEEE T Broadcast 2020; 66(2): 216–228.

32. Liu N, Chen J, Zhu L, et al. A key management scheme for secure communications of advanced metering infrastructure in smart grid. IEEE T Ind Electron 2013; 60(1): 4746–4756.

33. Nicanfar H, Jokar P and Leung VCM. Smart grid authentication and key management for unicast and multicast communications. In: Proceedings of the 2011 IEEE PES innovative smart grid technologies, Perth, WA, Australia, 13–16 November 2011. New York: IEEE.

34. Maharjan N, Moten D and Dean R. Secure IP multicasting with encryption key management. Int Telem J 2011; 47: 1–10.

35. Bihani A. An analysis of routing protocols in MANETs. Int J Eng Trends Tech 2014; 7(1): 31–35.

36. Ghosal A and Conti M. Key management systems for smart grid advanced metering infrastructure: a survey. IEEE Commun Surv Tut 2019; 21(3): 2831–2848.

37. El-Hajjar M and Hanzo L. A survey of digital television broadcast transmission techniques. IEEE Commun Surv Tut 2013; 15(4): 1924–1949.

38. International Telecommunication Union (ITU). Handbook on Digital Terrestrial Television broadcasting networks and systems implementation, 2016, p. 318, https://www.itu.int/dms_pub/itu-r/oth/0a/07/R0A0700003B001_PDF/PDF

39. Parvez I, Islam A and Kaleem F. A key management-based two-level encryption method for AMI. In: Proceedings of the 2014 IEEE power energy society general meeting, National Harbor, MD, 27–31 July 2014, pp.1–5. New York: IEEE.

40. Yu K, Arifuzzaman M, Wen Z, et al. A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid. IEEE T Instrum Meas 2015; 64(8): 2072–2085.

41. Gu C, Hanley N, McWilliams G, et al. Physical Uncloneable Functions (PUFs) for smart meter security, 2016, https://project-sparks.eu/wp-content/uploads/2016/09/03-puf-belfast-workshop-20160826.pdf

42. Nabeel M, Kerr S, Ding X, et al. Authentication and key management for advanced metering infrastructures utilizing physically uncloneable functions. In: Proceedings of the 2012 IEEE 3rd international conference on smart grid communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012, pp.324–329. New York: IEEE.

43. Seurin Y. On the exact security of Schnorr-type signatures in the Random Oracle Model. In: Pointcheval D and Johansson T (eds) Advances in Cryptology – EUROCRYPT 2012, vol. 7237 (Lecture Notes in Computer Science), 2012, pp.554–571.

44. Delavar M, Mirzakuchaki S, Ameri MH, et al. PUFBased solutions for secure communications in Advanced Metering Infrastructure (AMI). Int J Commun Syst 2017; 30(9): e3195.

45. Benmalek M, Challal Y and Bouabdallah A. Scalable multi-group key management for advanced metering infrastructure. In: Proceedings of the 2015 IEEE international conference on computer and information technology; ubiquitous computing and communications; dependable, autonomic and secure computing; pervasive intelligence and computing (CIT/JUCC/DASC/PICOM), Liverpool, 26–28 October 2015. New York: IEEE.

46. Nicanfar H, Jokar P, Beznosov K, et al. Efficient authentication and key management mechanisms for smart grid communications. IEEE Syst J 2014; 8(2): 629–640.
47. Wan Z, Wang G, Yang Y, et al. SKM: scalable key management for advanced metering infrastructure in smart grids. *IEEE T Ind Electron* 2014; 61(12): 7055–7066.

48. Khasawneh S and Kadoch M. Hybrid cryptography algorithm with precomputation for advanced metering infrastructure networks. *Mobile Netw Appl* 2018; 23(4): 982–993.

49. Rafaeli S and Hutchison D. A survey of key management for secure group communication. *ACM Comput Surv* 2003; 35(3): 309–329.

50. Yan L, Chang Y and Zhang S. An efficiency batch authentication scheme for smart grid using binary authentication tree. *Int Arab J Inf Techn* 2019; 16(3): 435–441.

51. Kamto J, Qian L, Fuller J, et al. Light-weight key distribution and management for Advanced Metering Infrastructure. In: *Proceedings of the 2011 IEEE GLOBECOM workshops (GC Wkshps)*, Houston, TX, 5–9 December 2011, pp.1216–1220. New York: IEEE.

52. Wen J, Ma H and Zhang X. Optimization of the occlusion strategy in visual tracking. *Tsinghua Sci Technol* 2016; 21(2): 221–230.

53. Benmalek M and Challal Y. eSKAMI: efficient and scalable multi-group key management for advanced metering infrastructure in smart grid. In: *Proceedings of the 14th IEEE international conference Trustcom/BigDataSE/ISPA*, Helsinki, 20–22 August 2015, vol. 1, pp.782–789. New York: IEEE.

54. Benmalek M, Challal Y, Derhab A, et al. VerSAMI: versatile and scalable key management for smart grid AMI systems. *Comput Netw* 2018; 132: 161–179.

55. Benmalek M, Challal Y and Derhab A. An improved key graph based key management scheme for smart grid AMI systems. In: *Proceedings of the 2019 IEEE wireless communications and networking conference (WCNC)*, Marrakesh, 15–18 April 2019, pp.1–6. New York: IEEE.

56. Manjul M and Mishra R. Secure group communication based on elliptic curve cryptography. *Trans Netw Commun* 2014; 2(1): 1–26.

57. Kumar V, Kumar R and Pandey SK. LKM-AMI: a light-weight key management scheme for secure two way communications between smart meters and HAN devices of AMI system in smart grid. *Peer Peer Netw Appl* 2021; 14: 82–100.

58. Kumar A, Sri Lakshmi R and Preethi M. Implementing secure group communications using key graphs. *Defence Sci J* 2007; 57(2): 279–286.

59. Thomas MS, Ali I and Gupta N. A secure way of exchanging the secret keys in advanced metering infrastructure. In: *Proceedings of the 2012 IEEE international conference on power system technology (POWERCON)*, Auckland, New Zealand, 30 October–2 November 2012, pp.1–7. New York: IEEE.

60. Kiarie LK, Langat PK and Muriithi CM. Key generation for electrical smart meters using hash functions. In: *Proceedings of the 2019 IEEE AFRICON conference*, Accra, 25–27 September 2019, pp.42–45. New York: IEEE.