Mobile Netw Appl
https://doi.org/10.1007/s11036-017-0956-0

Hybrid Cryptography Algorithm with Precomputation for Advanced Metering Infrastructure Networks

Samer Khasawneh[1] · **Michel Kadoch**[1]

Abstract Two-way communication has been identified as the smart grid flagship feature that enables the smart grid to attain its outcomes over the legacy power grid. Integrating communication networks into the power grid will motivate malicious attackers to target information exchange. Therefore, achieving secure and authentic communication in the smart grid networks is an indispensable requirement. In this paper, we propose a sophisticated hybrid encryption scheme that incorporates public and symmetric key encryptions to secure smart metering network. Elliptic Curve Integrated Encryption Scheme (ECIES) and Advanced Encryption Scheme (AES) are chosen as the building blocks for the proposed scheme. In order to optimize the computation overhead of ECIES, a precomputation procedure is presented to provide faster encryption/decryption. The proposed technique provides data integrity, confidentiality and authenticity as well as it resists against false data injection and message reply attacks. Simulation results show that the proposed approach surpasses some of the existing schemes in terms of computation, communication and storage overhead.

Keywords AMI networks · Hybrid encryption · Elliptic curve cryptography · ECIES · Precomputation

✉ Samer Khasawneh
samer.khasawneh.1@ens.etsmtl.ca

Michel Kadoch
michel.kadoch@etsmtl.ca

[1] Department of Electrical Engineering, École de Technologie Supérieure, University of Quebec, Montreal, QC, Canada

1 Introduction

The legacy power grid has been serving our electricity needs for decades. However, the increasing human population, the inefficient utilization and integration of renewable energy sources, the one-way communication scheme in addition to the high management cost resulted in an inefficient power generation, distribution and management [1]. This requires the development of a "smart" power generation and distribution to replace the conventional power grid. Consequently, the features of the smart grid (SG) are envisioned to offer abundant advantages over the legacy grid in terms of scalability, reliability, flexibility, resiliency, sustainability and intelligence [2]. However, such features are predicated on the presence of a sophisticated and well-designed communication paradigm that will play a vital role in the power system management.

Internet of Things (IoT) is an emerging concept that represents the expansion of the internet and networking to cover unforeseen fields such as transportation, health services, manufacturing factories and power grids [3, 4]. In this technology, the physical objects are connected to enable them to monitor, collect, interpret and exchange the information of each other. SG is composed of millions of interconnected devices and the majority of the SG applications and services depend on the existence of a sophisticated communication scheme that enables such devices to efficiently communicate with each other. Therefore, applying IoT to the power grid can empower the implementation of the SG due to the similar characteristics between IoT and SG.

SG is an intelligent replacement to the obsolete power grid, where robust control, better power quality with economic efficiencies is realized. It is considered the future power grid as it can respond to current and future customers

Published online: 27 October 2017

need for electricity. The improvements SG offers over the legacy power grid are due to the integrating of digital computation and communication technologies that can provide consistent and efficient delivery of electricity and exchange of information between utility companies and consumers [5]. The most important characteristics of the smart grid are:

1. **Information communication.** Two-way communication is the main feature that characterizes the smart grid operation.
2. **Controllable prices grow-up.** SG customers will have better control over which appliances should be turned-off; in addition they will be able to contribute in power production.
3. **Better Energy management.** Integrating communication allows schemes such as Demand-Response (DR) [6], load profiling [7] and peak shaving [8] to gain better control over the power grid which will reduce power outages and blackouts.
4. **Permit optimal integration of distributed resources.** SG permits the deployment of distributed resources like renewable energy sources [9].
5. **Resist attacks.** In opposite to the conventional power grid, SG is supposed to withstand a variety of cyber and physical attacks [10].
6. **Self-healing.** SG has the capability to detect and respond to certain failures without human intervention. This is done through digital components and intelligent real-time communications technologies [11]. It can segregate outages by redirecting the electricity to meet customers demand.

SG consists of appliances, meters, sensing devices, information gateways in addition to power generation and transmission utilities all operating in near real-time to achieve the desired operating requirements [12]. The meters are responsible for accumulating energy consumption of appliances, broadcasting energy loss/restoration information and reporting the pricing information to customers. The sensing devices are deployed to monitor the system performance and detect any operation malfunction. They can transmit control messages to the control center upon detecting any failure. Due to the fact that smart meters are located far from the utility, intermediate devices are needed to route the smart meters data to the utility. Gateways (sometimes called concentrators) collect smart meter's data and send it to the utility over WAN connection. Control information is carried also through such gateways to the smart meters. The architecture of the smart grid requires the smart meters, sensing devices, gateways and the control centers to lie in the path between the customers and the power providers in order to realize the two-way communications [13].

1.1 Two-way communication in smart grid

In opposite to the conventional power grid that sends power in one direction, SG efficiently integrates computerized two-way communication networks to enable real-time operations. Information is exchanged back and forth between the smart grid entities to implement new functionalities such as Demand-Response, self-healing and distributed management. Several frameworks are found on the literature describing the two-way communication model; however the most convenient one is the hierarchical model [14, 15]. In this model, the SG is partitioned into three layers. The lower layer is the closest to the customer premises and it comprises Home Area Networks (HAN), Building Area Networks (BAN) and Infrastructure Area Network (IAN). These networks span small geographic areas and are connected to smart meters and energy management devices in order to enable real-time transmission of users power consumption in addition to sending/receiving other control commands to/from the grid. Neighborhood Area Networks (NAN) and Field Area Networks (FAN) are two networks found in the middle layer. They span larger geographic areas and are responsible for collecting and aggregating the smart meters readings before forwarding them to the top layer. A single NAN may contain multiple HANs as shown in Fig. 1. Remote Terminal Units (RTUs) and Phasor Measurement Units (PMUs) are found in the middle layer as well. The top layer of this model contains Wide Area Networks (WAN) that delivers the aggregated data from multiple NANs to the utility. The head end utility software SCADA (Supervisory Control And Data Acquisition) is responsible for receiving, processing, presenting and managing data. It can issue several control commands such as load shedding and demand response. In addition, distributed generation and transmission networks are considered part of this layer [8].

Advance Metering Infrastructure (AMI) is an integral part of the smart grid as it represents the architecture that provides the two-way communications. The AMI system is designed to use meters, concentrators, metering control system and Meter Data Management System (MDMS) in addition to NAN and WAN networks. Its architecture begins at the customer premise and ends at the MDMS, where the in-between devices and networks are responsible for communicating the metering information. The security solution provided in this paper is designed to secure the communication in AMI networks.

1.2 Security in AMI networks

In order to manage the complex structure of the smart grid; high-speed bidirectional communication networks are needed. For this reason, AMI networks utilize the Internet Protocol (IP) to support the two-way communication, where each one of the smart appliances and meters (in addition to gateways certainly) is assigned a unique IP address [16]. The utilization

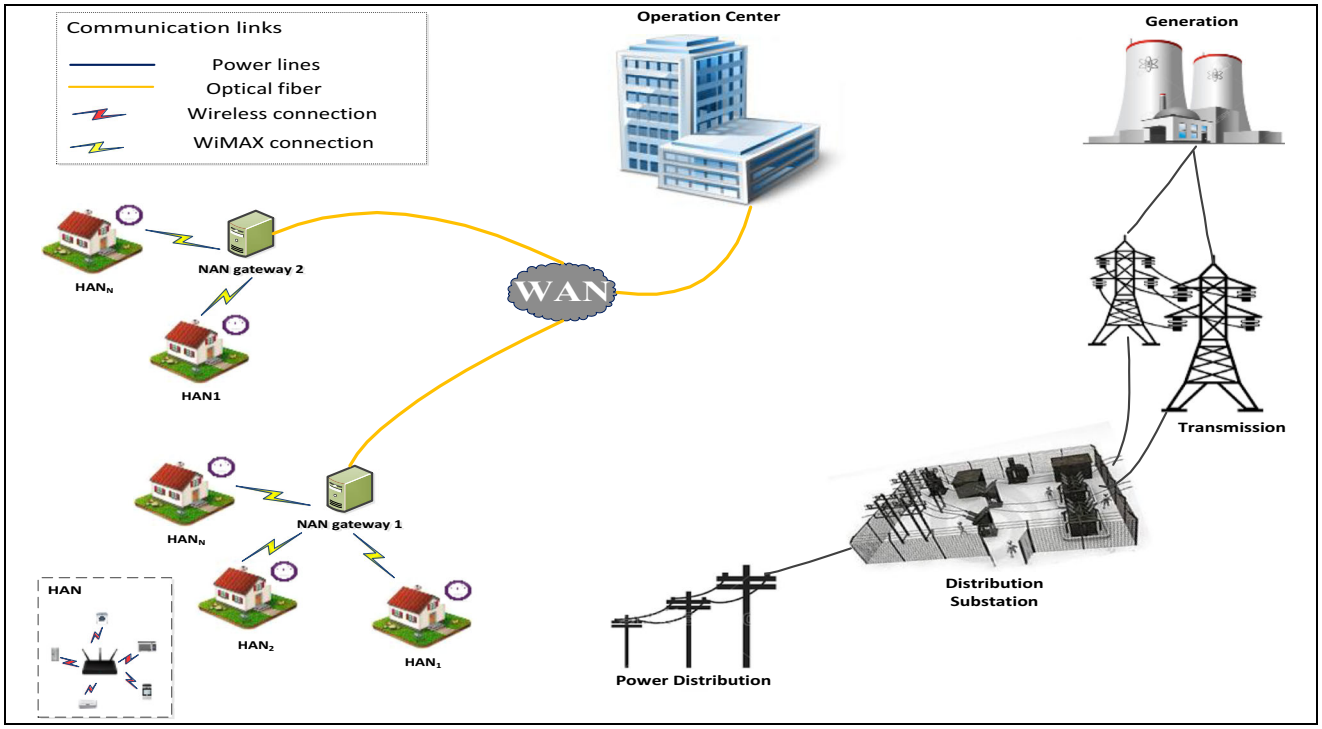

Fig. 1 Smart grid communication architecture

of IP-based protocols along with the use of insecure wireless communication channels introduces several security threats. Therefore, AMI networks are subject to various active and passive attacks such as eavesdropping, traffic analysis, Denial of Service (DoS), false data injection, reply attack and impersonation [17]. It is worth mentioning that the current power grid is already facing various cyber security risks, however the higher degree of interconnection between the different SG components introduces additional security vulnerabilities.

In any information system, there exist three fundamental information security goals namely: integrity, confidentiality and availability. Smart grid is no exception, where the three previously mentioned goals must be guaranteed in order to achieve the desired performance gain. However, designing a security measure for AMI communications requires an efficient, low overhead, scalable, and robust Key Management System (KMS) that is able to support the very large number of smart meters. The role of KMS in AMI networks is to generate cryptographic keys with suitable length and then use the different communication links to distribute the keys to the communicating parties such as utility, smart meters and gateways. Therefore, designing a framework to achieve secure communication in AMI networks is twofold: designing appropriate key management system in addition to the security framework itself.

The rest of the paper is organized as follows. In Section 2, we present the related work. The system models and design goals are demonstrated in section 3. Sections 4 sheds light on the concept of hybrid encryption and describes the details of Elliptic Curve Integrated Encryption Scheme (ECIES). In section 5, we present the implementation of the proposed hybrid encryption cryptosystem. The analysis and evaluation are conducted in section 6. Section 7 concludes the paper.

2 Related work

An end-end security for AMI networks is proposed in [18]. The model is based on using weak Physically Unclonable Functions (PUFs) as a security primitive to provide strong hardware based authentication for smart meters and collectors. During the initialization phase, the utility generates three hash functions and a pair of challenges. The challenges are used to trigger PUF responses, whereas, the hash functions are used to obtain hash codes and compute smart meter symmetric key/passwords. In order to support multicast communications, the proposal utilizes Broadcast Group Key Management (BGKM) scheme. This is the first work to consider weak PUF for security purposes, while strong PUFs seem to be vulnerable to some attacks. When compared to other schemes ([19, 20]), the storage overhead of the proposed scheme is high especially when the size of the broadcast set is large.

Fangming Zhao et al. [21], proposed a cryptographic key exchange and authentication scheme based on media key block and the broadcast encryption protocol. The proposal provides key management for secure key exchange and revocation in the smart grid network. The protocol views the smart grid as a

binary tree and it has two phases of operation: key sharing between un-revoked devices and an authentication scheme. In key sharing phase, leaf nodes who wish to communicate with each other use a pre-established media key to obtain a common key. Once the communication takes place, the identities of the devices are verified using the second phase. Although the proposal provides low communication and storage overhead, it does not take into consideration the different possible transmission modes (unicast, multicast, broadcast).

The authors in [22] proposed a key management protocol to secure smart grid communication. The protocol assumes three types of transmission modes: unicast, multicast and broadcast. The smart grid network is partitioned into macro grid network that is controlled by the government and multiple micro grid networks operated by the service provider. The proposed key management uses three sub-protocols: the system initialization, the key management for broadcast communications, and the key management for unicast and multicast communications. A secret broadcast key that is known to all communication parties is used for broadcast encryption, whereas a secret key that is shared only between DR project members is used to secure unicast and multicast communications.

In [23], data aggregation protocol based on homomorphic encryption is proposed to protect user privacy in AMI networks. The performance of Fully Homomorphic Encryption (FHE) is assessed to provide its feasibility for AMI networks as such technique results in large aggregated data size. The problem of packet reassembly is identified when the aggregated packets are transmitted via TCP with variable window size. The receiving meter needs to know the size of data packets from each child meter to perform data aggregation accurately. The study presented a novel solution to reassembly problem by adding a presentation layer above the transport layer to include packet size information at the sender side.

A mutual message authentication protocol that uses two cryptosystems is presented in [24]. The protocol provides authentication for the messages exchanged in the smart grid network through running two different processes one for message authentication and another for secure message transmission. The scheme is based upon Diffie-Hellman that employed RSA and AES for message authentication, whereas it employs HMAC to ensure message integrity. Despite the authors considering the protocol light weighted, the communication and computation overhead are considered high when compared to other authentication schemes such as [13, 25]. The authors of this paper presented a preliminary hybrid encryption scheme for AMI networks [26]. The proposal presents a novel mechanism to accommodate public key cryptography with secret key encryption to generate secure messages between the different AMI devices. Despite its resiliency to numerous attacks, the computation overhead of the proposed scheme is considerable due to the point multiplication involved in the elliptic curve encryption. Furthermore, the model requires inflexible security setup as the communicating parties are required to modify the security primitives of the elliptic curve encryption for every message exchange.

The contributions of this paper are twofold:

Firstly, a hybrid encryption scheme that exploits symmetric and asymmetric encryption is proposed. The proposal employs elliptic curve cryptography, where a precomputation stage is introduced to minimize the computation overhead of elliptic curve encryption by eliminating the time required to perform the scalar-point multiplication.
Secondly, the precomputed values can be changed dynamically to improve the strength of the cryptosystem.
Thirdly, performance analysis is carried out to assess the performance of the proposed scheme in terms of computation, communication and storage overhead. The simulation results demonstrate the validity of the proposal for AMI networks.

3 Models and design goals

In this paper, we are proposing a hybrid encryption scheme that exploits the secret-key encryption with the public key cryptography. This work is based on the model we presented in [26], with a major improvement. We optimized the performance of the elliptic curve encryption algorithm by precomputing the scalar-point multiplication. The details of the proposed scheme will be presented in the next sections. We will demonstrate AMI network model, threat model in addition to design goals in this section.

3.1 AMI network model

In our model, the communication will be carried out between the smart meters, NAN gateways and the utility master computer (UMC) as shown in Fig. 2 Smart meters and UMC exchanges data and control messages that are routed through the intermediate gateways. For simplicity, we assume that the smart meters and UMC are one hop in distance. UMC is equipped with high storage and processing capabilities in opposite to the smart meters that are equipped with very limited storage and communication capabilities. As shown in the network model, neighborhood area gateway routes information sourced from multiple smart meters. Encryption and decryption operations could be done at any one of the three devices simultaneously and asynchronously.

3.2 Threat model

In our threat model, we consider an external adversary *A* that can capture network messages by intercepting on the communication links. The adversary *A* cannot compromise UMC or

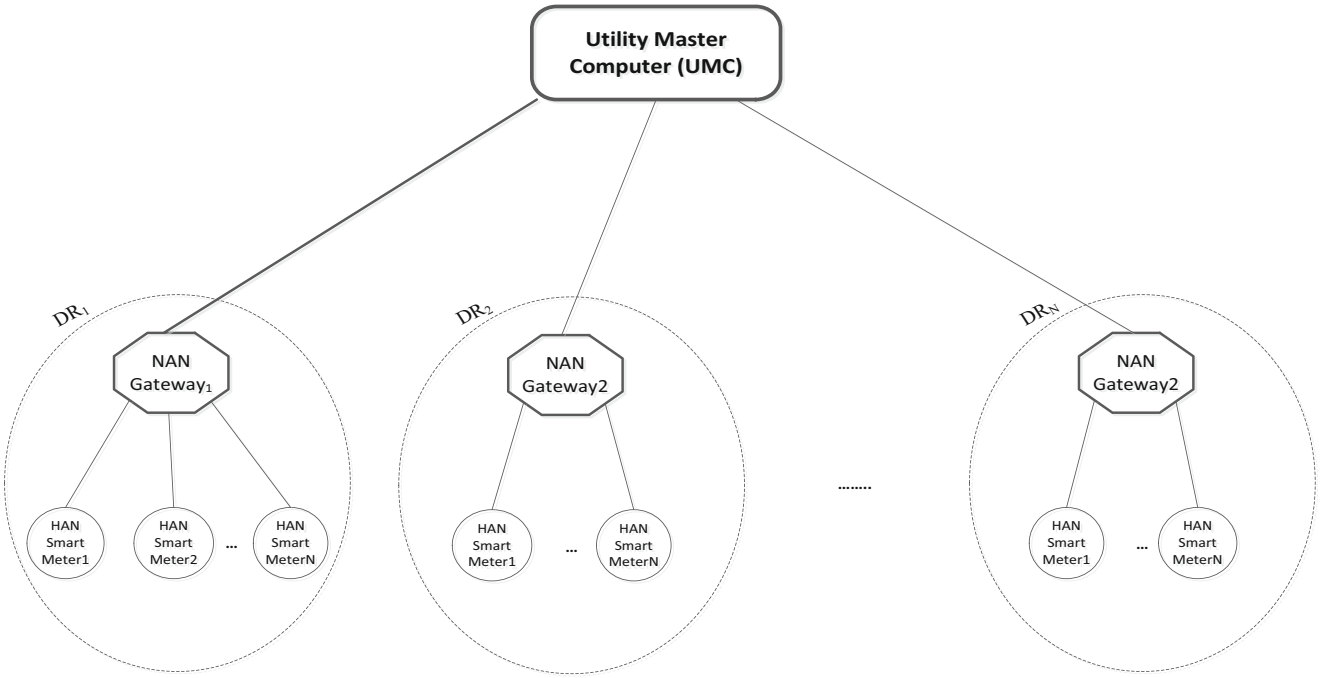

Fig. 2 AMI network model

NAN gateway databases. Based on sufficient power and knowledge, we assume that the adversary *A* is able to launch the following set of attacks:

1. Passive attacks (eavesdropping and traffic analysis). Adversary *A* can sniff AMI messages with no intention to corrupt the communication. He rather invades the privacy of the power grid users.
2. Message modification attack. Adversary *A* alters AMI communication by tampering with or dropping the captured messages.
3. Message injection attack. Adversary *A* injects falsified messages into the network to obtain undesirable performance deterioration.
4. Reply attack. Adversary *A* intercept AMI message and maliciously retransmits those obsolete messages to NAN gateway or smart meters. Obviously, replay attack can occur even if the exchanged messages are encrypted or digitally singed.

3.3 Design goals

The design goal is to develop a hybrid encryption scheme for AMI networks in order to deliver the following objectives:

1. The proposed scheme provides a lightweight key management scheme to reduce the overhead of key generation, distribution and renewal to cope with AMI constraints.
2. The proposed scheme is being designed to achieve high efficiency by combining the strength of public key cryptography with the speed of private key cryptography.
3. The proposed scheme optimizes the performance of the elliptic curve encryption by having the point multiplication step done in advance.
4. The proposed scheme should be resilient against the attacks discussed in the threat model.

4 The hybrid encryption

In cryptography, choosing between symmetric and public key encryption depends on the use case. Symmetric encryption is based on sharing the same secret (key) between the set of authorized entities. The same key is used for encrypting the plain text and decrypting the cipher text. This type of encryption is suitable for the applications that require low computation overhead as it tends to be fast. The main drawback of symmetric encryption is that it requires the communicating parties to share the secret key before the communication takes place. Contrary, public key cryptography can provide secure communication over unsecure channels. It is based on a trapdoor function and pair of keys. This function is easy to compute in one direction, but computationally infeasible to reverse unless certain information is available. Discrete logarithmic problem is an example of such trapdoor function. Public key encryption is known to achieve higher security levels when compared to symmetric encryption, but with considerable

computational overhead. Therefore, public key encryption is used to encrypt short sized message and could not be used efficiently in resource-constrained systems.

Hybrid Cryptosystems (HC) is a mode of encryption that combines the strength of public key cryptography with the efficiency of symmetric encryption. HC is composed of two subsystems namely: data encapsulation and key encapsulation systems. Data encapsulation system is a symmetric key cryptosystem, where the plain text is encrypted with an arbitrary key using one of the symmetric encryption algorithms. On the other hand, key encapsulation system is a public key cryptosystem that is used to encrypt the arbitrary key using one of the asymmetric encryption algorithms. The secure message is formed by merging the results of the two encapsulation systems. The receiver of the digital envelop will use asymmetric decryption to recover the key that will be used to decrypt the data. The details of hybrid encryption are given in Fig. 3. In summary, HC is public key cryptosystems that inherits the efficiency of the symmetric algorithms with the security of the public key cryptography.

AMI applications have unique constraints and requirements, thereby the cryptosystems that will be used for data and key encapsulation must be carefully designed in order to achieve the desired security level without having the performance degraded. In our scheme, we will use Advance Encryption standard (AES) for the data encapsulation cryptosystem and Elliptic curve encryption for the key encapsulation cryptosystem. AES is used in most of US federal government organization, it has different key sizes, secure block size and known to be efficient in hardware and software. Elliptic curve encryption is used instead of the well know Rivest Shamir Adleman (RSA) cryptosystem because it appears to offer equal security with smaller key size [27].

4.1 Elliptic curve integrated encryption scheme (ECIES)

Several approaches for encryption/decryption using elliptic curves have been analyzed in the literature, yet very few could be applied to secure AMI communication. Encode-Then-Encrypt [28] is the simplest and the least secure elliptic curve encryption. The plain text is mapped to elliptic curve point(s), and then each point is encrypted separately. This scheme requires considerable storage to track the points mapping. Hashed ElGamal Elliptic Curve Encryption is analyzed in [30]. This technique does not map the plain text into points, rather it uses symmetric encryption algorithm to encrypt the plain text with a key generated by a Key Derivation Function (KDF). The main drawback of this scheme is that it does not provide message authentication services. In our cryptosystem, we employ ECIES as it requires no point mapping in addition to providing authentication services.

ECIES is an elliptic curve cryptosystem that is part of the ANSI X9.63 standard [31]. This scheme is quite similar to ElGamal hashed elliptic curve, except for the addition of message authentication that can protect against integrity and authenticity violations. Consider the private and public keys α and αG respectively. The procedure of this scheme involves the following steps:

1. Choose a random r such that $r \in [1, n-1]$, and generate a point $Q \in E_q(a, b)$ such that $Q = r\,G$
2. Generates a pair of keys $(K_e, K_h) = KDF(rP)$
3. Encrypt the message, $M' = SYMM_{ENCK_e}(M)$
4. Compute the authentication code, $AUTH = HMAC_{K_h}(M')$
5. Send $(Q, M', AUTH)$

Q is used to recover the encryption and authentication keys. Upon receiving the cipher text, the receiver computes the value of $AUTH$ and compares it with the received one, if the values are found equal the ciphertext is processed to obtain

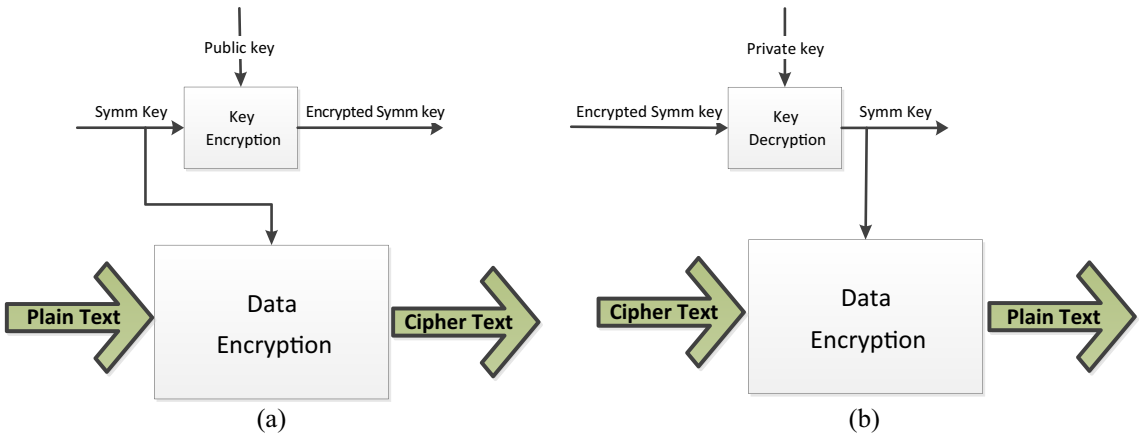

Fig. 3 The structure of hybrid encryption cryptosystem. **a** Encryption. **b** Decryption

Table 1 Computation time for one scalar-point multiplication

Elliptic curve	SECP112r1	SECP160K1	SECP192K1	SECP224K1	SECP384K1
Time (ms)	0.89	1.63	2.21	2.79	5.14

the plain text, otherwise the information is ignored. In opposite to Encode-Then-Encrypt, ECIES has small storage overhead. For the purpose of authenticating AMI messages, 128 or 256 are added to each message. Although this amount of extra bits is considered acceptable, the communication overhead of this scheme is larger than Encode-Then-Encrypt and Hashed ElGamal. It worth mentioning that ECIES provides the best functionalities with an acceptable performance overhead; consequently we will utilize it for building the key encapsulation module in the proposed hybrid encryption cryptosystem.

4.2 Optimizing the computation overhead of ECIES

As mentioned earlier, the hybrid encryption scheme proposed in this paper is based on our model previously published in [26]. However, we found that the computation overhead of ECIES could be improved by precomputing the scalar-point multiplication operations ($r.\ G$ and $r.\ P$). The precomputation technique aims to eliminate the computation overhead of scalar-point multiplication when encrypting a plain text or decrypting a cipher text. In this section, we will show that this multiplication requires considerable time overhead and will demonstrate how it could be precomputed ahead to reduce the computation overhead of ECIES.

We have developed a C++ code to measure the time required to perform scalar-point multiplication over the prime finite field Z_q for the set of recommend elliptic curves presented in [29]. The simulation results shown in Table 1 indicate that the time required to perform one scalar-point multiplication is significant. However for AMI networks the computation overhead will be greater than what is shown in the table for two reasons: 1) ECIES requires two scalar-point multiplications, therefore the overhead will double. 2) In AMI networks, NAN gateway will be responsible for hundreds or thousands of smart meters, therefore it must perform hundreds of multiplications leading to considerable delay. Consequently, optimizing the multiplication operation will greatly improves the performance of ECIES and the hybrid cryptosystem as well.

Considering the fact that the multiplication operation is independent of the message to be processes, the point Q in addition to KDF input could be precomputed in advance to elevate the computation overhead at the moment of encrypting or decryption. Every one of the communicating parties chooses the private value r, computes $Q = r.\ G$ and sends the result to the node it wishes to communicate with, all of this is done before exchanging ciphered messages. The receiving node precomputes KDF input by multiplying the received value by its public key.

Table 2 Notation guide

Notation	Description	Notation	Description
E_q	Elliptic curve over prime field q	K_e	Encryption/decryption key
a, b	Elliptic curve parameters	K_h	Authentication key
q	Prime Number	B_i	Block i of cipher text
G	Elliptic curve generator	m	Message
n	Generator order	M	Plain text
h	Elliptic curve cofactor (used as 1)	M'	Cipher text
Q	Elliptic curve point $\in E_q$	θ	Clock tolerance
r	Random integer $\in [1, n-1]$	$SYNC$	Timestamp
α, β	Private keys for Elliptic curve cryptosystem	$SYMM_{ENCK_e}$	Symmetric encryption using key K_e
X, Y	Private values used for precomputation	$SYMM_{DECK_e}$	Symmetric decryption using key K_e
P, P_1, P_2	Public keys for Elliptic curve cryptosystem	$AUTH$	authentication code
K_r	Random session key	$HMAC_{K_h}$	Cryptographic keyed-hash message authentication function using K_h
$K_r^{'}$	Encrypted random session key	MIC	Message Integrity code

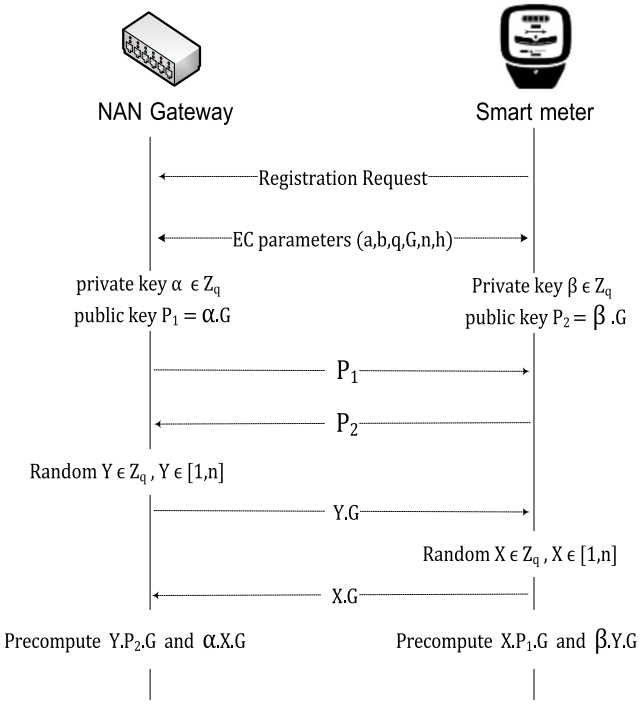

Fig. 4 The initialization phase of the proposed scheme

The same procedure will be repeated each time the communicating nodes wish to change KDF inputs. In the next section, the precomputation procedure is fully explained in the context of the proposed hybrid encryption cryptosystem.

5 The proposed hybrid encryption cryptosystem

This section elaborates the proposed hybrid encryption cryptosystem. Table 2 provides the notation that will guide to understand the scheme. The operation of the proposal can be divided into three phases illustrated as follows:

5.1 Initialization

Whenever new smart meter or NAN gateway joins the AMI network, it initiates the procedure shown in Fig. 4 with the device it will communicate with. Public/private key pair is generated after agreeing on the elliptic curve parameters. The devices then generate and exchange random points (*XG* and *YG*) that will be used to derive the precomputation parameters. Such parameters will be used by KDF to generate encryption/decryption and authentication keys.

For example, the smart meter will use XP_1G to derive encryption and authentication keys and βYG to derive decryption and authentication keys. The precomputation parameters could be changed frequently to improve the resiliency of ECIES.

5.2 Description of the proposed HC scheme

The proposed hybrid encryption cryptosystem is composed of three units: symmetric encryption module, asymmetric encryption module and message integrity module (keyed hashing module). The symmetric encryption module is used to encrypt AMI messages using AES-128 with an arbitrary key (K_r) produced by random generation unit. The asymmetric encryption module is used to encrypt the arbitrary key used by the symmetric encryption module. It is a public key cryptosystem that uses ECIES with the precomputation parameters established during the initialization phase. The symmetric encryption module acts as data encapsulation system, while the second module acts as key encapsulation system. Message integrity module is used to generate the

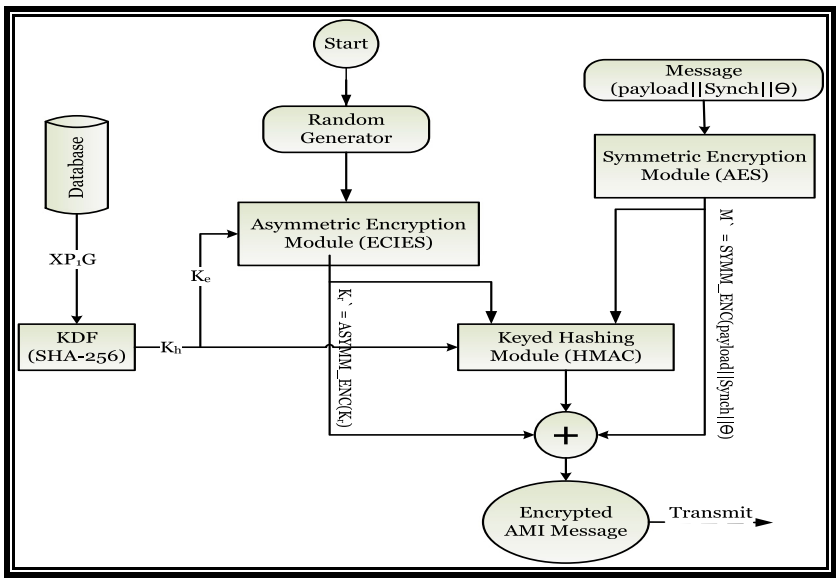

Fig. 5 The structure of the proposed hybrid cryptosystem

integrity code that enables detecting any tampering with the secure message. The structure of the proposed hybrid cryptosystem is shown in Fig. 5.

The messages that will be exchanged using the proposed protocol must have the format shown in Fig. 6. The payload field stores the information that needs to be sent to the destination. The size of this field is variable and is determined by the amount of information that needs to be transferred to the destination. Synch and clock tolerance fields are used to protect against reply attack. Synch is 128 bits that stores the message timestamp corresponds to message creation time, whereas clock tolerance (32 bits) indicates for how long (in milliseconds) the message will be valid. When a message is received, synch field is compared with the current time; if the difference between the current time and synch is greater than the value of the clock tolerance, the message is considered replayed and is ignored. The choice of clock tolerance value depends on many factors such as computation speed, network bandwidth, network congestion status and the packet delay requirements. The precomputation parameter is used to improve the security of the proposed protocol by frequently updating the precomputed values that are used to derive the cryptographic keys. The input to KDF is updated once a new precomputation parameter is received by multiplying the received value by the private key. Zeros in the precomputation field indicates that the sender wants to keep using the same values. The size of this field depends on the elliptic curve in use.

As explained earlier, hybrid cryptosystems encrypt the arbitrary key and appends it to the message. The encrypted key is stored in key field. The size of this field depends on: original key size and the public key algorithm used to encrypt the key. Message Integrity Code (MIC) is used to protect message integrity and authenticity. A message that is tamped with or originated from an unauthorized source is detected when MIC field is checked. The shaded fields shown in Fig. 6 are encrypted. The algorithm shown in Fig. 7 illustrates that procedure for decrypting a message constructed using the proposed hybrid cryptosystem.

Algorithm 2: Process Encrypted Message

```
XP1G ← get_param ( )
(Ke, Kh) ← H(XP1G)
//Verify message integrity and authenticity
IF (MIC == HMAC_Kh(M'|| K'r))
    Kr = AES_D(K'r, Ke)
    FOREACH (Bi ∈ {B0, B1, ....., BSIZE−1}) LOOP
        m = AES_D(Bi, Kr)
        M = [M|| m ]
    END FOREACH
    (Payload, SYNCH , θ, XP1G) = PARTITION(M)
    IF (TIMEOFDAY( ) − SYNCH < θ)
        // process message
        IF(XQR != 0)
        UPDATE_PRECOMM_PARA(XP1R)
        END IF
    END IF
    ELSE
        // ignore replayed message
    END ELSE
END IF
ELSE
    // ignore invalid message
END ELSE
```

Fig. 7 Message decryption procedure

6 Performance analysis

In order to evaluate the feasibility of the proposed hybrid cryptosystem, we implemented the proposal in software to simulate its operation and asses its performance. The implementation was executed on an Intel Pentium IV 2.7-GHz machine with 8GB RAM running Linux Mint 18.1 mate operating system. The performance of the proposed scheme is compared with our base model presented in [26] (referred as HC), RSA and the Merkle-tree hash-based scheme presented in [20]. We used 128 bit AES for the symmetric encryption module and 256 bits Secure Hash Algorithm (SHA) for key derivation function. In this section, we denoted the Hybrid Cryptosystem with Precomputation scheme presented in this paper by HC-P.

6.1 Computation overhead

Computation overhead is the time required to produce the cipher text in the format that will be transmitted in the network or the time required to decipher the cipher text to obtain the corresponding plain text. Figure 8 shows the computation time incurred by NAN gateway when the proposed scheme is implemented to support different number of smart meters. We assume that each smart meter is generating messages of 32 KB in length.

6.2 Communication overhead

Communication overhead is measured by the amount of extra bits added to the message in order to secure it. Due to the fact that AMI networks have limited bandwidth; cryptographic schemes should consider minimizing the communication overhead a priority. In our proposed scheme, three fields are added to the message: the precomputation parameter (Q), the encrypted arbitrary key and the integrity codes (MIC). The size of Q depends on the elliptic curve used. The size of the encrypted key is determined by the size of key used by the symmetric encryption algorithm, while the size of MIC field depends on the choice of the keyed hashing function. In the

Payload	*Synch*	*Clock Tolerance(θ)*	*precomputation parameter (Q)*	*key*	*MIC*

Fig. 6 The message format of the proposed hybrid cryptosystem

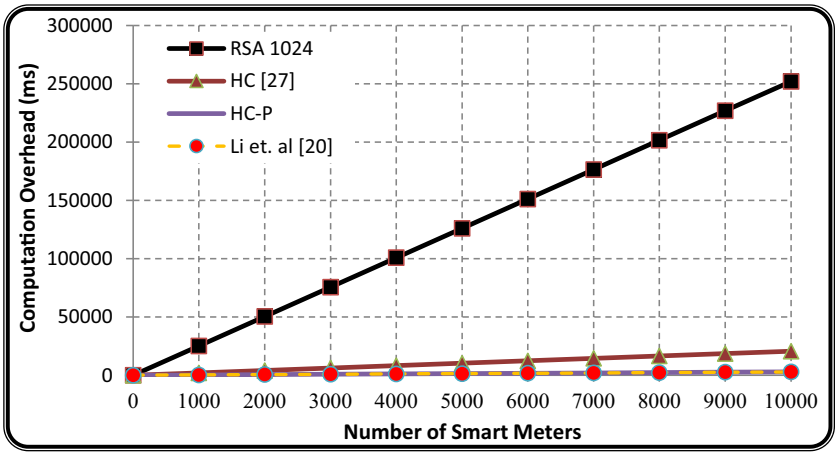

Fig. 8 The computation time of the proposed hybrid cryptosystem on NAN gateway

simulations conducted, we implemented AES and keyed hash function with 128 bits key. Consequently, the communication overhead will be 256 bits plus the size of elliptic curve point. The cryptosystem presented in this paper and our base model [26] achieves the same communication overhead. The scheme proposed in [20] adds authentication path information (API) to every report generated by a smart meter with a total size of 896 bits. On the other hand, the size of digital signature generated by RSA is 1024 bit. The communication overhead for an AMI network with different number of smart meters is shown in Fig. 9. It can be easily seen that the computation overhead of the proposed protocol implemented using different variations of elliptic curves achieves the lowest communication overhead.

6.3 Storage overhead

The main three components in AMI networks are the utility computer, the gateways and the smart meters. In opposite to utility computer, gateways and smart meters are equipped with limited storage capabilities (gateways have larger storage to accommodate storing routing information). As gateways and smart meters are not supposed to store large amount of information, the storage requirement of any cryptosystem is crucial. We analyzed the storage needed by the smart meters and NAN gateways individually. The results are shown in Table 3 and Fig. 10.

In our scheme, smart meters need to store: elliptic curve parameters, public/private key pair and the precomputed encryption/decryption parameters. RSA on the other hand, requires the smart meters to store three keys in addition to the parameters needed to generate the keys (such as p,q, n and Ø). The storage requirement for the scheme presented in [20] is very high, as it requires to store a special table called electricity report collection table. Every tuple in this table stores identification information, timestamp and authentication path information.

In AMI networks, NAN gateway must store information related to each one of the smart meters to enable them communicate securely, therefore the cryptographic information need to be stored in the gateways is considerable. Fig. 10 shows the storage requirement for a single NAN gateway responsible for routing the data sourced from multiple smart meters subscribing to the same DR project. As the number of smart meters increases, the gateway is required to store more

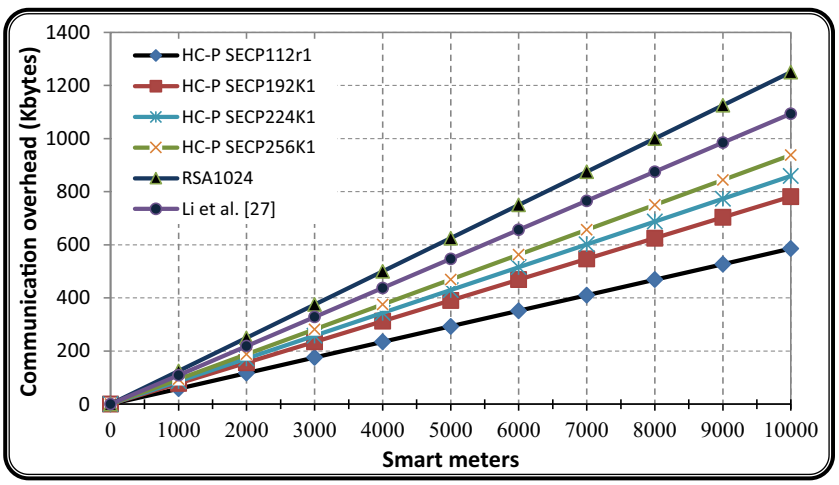

Fig. 9 Communication overhead of NAN gateway

Table 3 Storage requirement for smart meters

Scheme	HC-P secp112r1	HC-P secp192k1	HC-P secp224K1	HC–P Secp256r1	RSA1024	RSA2048	Li et al. [20]
Storage (bit)	1344	2304	2688	3072	3072	6144	$13*2^{13}$

cryptographic parameters. It is shown that [20] stores the least amount of information on NAN gateway. Compared to RSA, the proposed scheme has excellent storage requirement. It worth mentioning that the comparison should be done based on the security level provided by the algorithm, therefore HC-P with 224 and 256 bits should be compared with RSA2048. Table 3 and Fig. 10 demonstrate that implementing the proposed cryptosystem requires small storage space on smart meters and an acceptable storage space on NAN gateways.

6.4 Security analysis

The results obtained previously show that the proposed scheme is efficient in terms of computation overhead, storage requirements and communication overhead. Here, we will analyze the resiliency of the proposed scheme against the attacks cited in the threat model presented in section 3.

The proposed scheme ensures message confidentiality, therefore it protects against eavesdropping and traffic analysis. The communicated messages are transmitted encrypted, thereby an attacker that manages to collect messages from the network will not be able to read the content of the messages or gather any useful information regarding the sender of those messages. As a result, passive attacks are prevented and customer privacy is preserved.

The message integrity code that is attached to every message can ensure its integrity. The receiver of the message recomputes MIC value and compares it with the received one; if the two values are found different the receiver will infer that the message is tampered with and it will not get processed. For this reason, MIC can detect any manipulation to the content of message, key and MIC fields.

Before the initialization phase, the identity of the smart meter is verified by the gateway. Therefore, any smart meter that manages to share the elliptic curve parameters with NAN gateway is considered authentic. MIC is generated using a keyed hashed function; therefore verifying MIC of a message indicates that the message is originated from a legitimate source. Ensuring message integrity and authenticity can resist false data injection attack.

The proposed scheme is designed to prevent reply attack by adding timestamp (synch) and clock tolerance. Suppose that an external adversary captures a fresh message, stores it for some time and retransmits it later. The receiver of the message will compare the message timestamp with current time. The message is considered obsolete and replayed if the difference between the current time and the timestamp is found greater than the clock tolerance.

7 Conclusion

In order to update the existing power grid into a smart grid, efficient integration of two-way communication must be achieved. Integrating distributed communication jeopardizes the smart grid network to countless number of security threats. We presented a hybrid encryption scheme that incorporates symmetric and public key encryption in order to benefit from the strengths of each one of them. We optimized the computation overhead of the elliptic curve encryption by precomputing the point-scalar multiplication in priori. We designed the message format to allow flexible level of security. Simulation results have shown that the proposed scheme

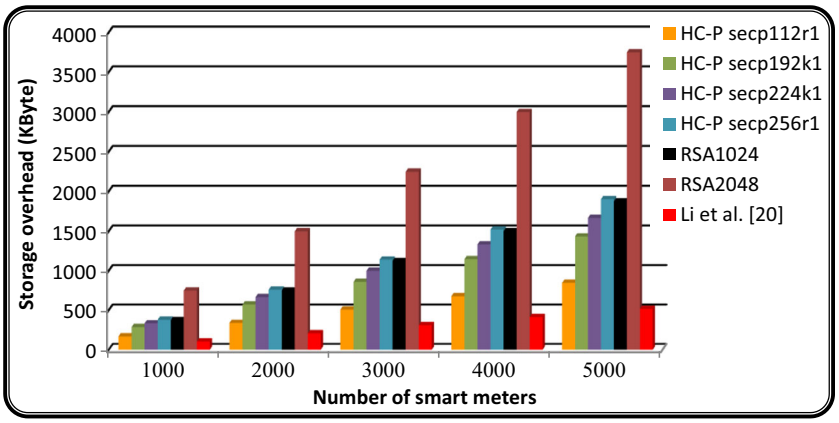

Fig. 10 Storage overhead of NAN Gateway

requires acceptable computation, communication and storage overhead. Additionally, the proposed protocol can ensure message integrity, confidentiality and authenticity. Furthermore, it can protect against false data inject and reply attacks.

References

1. Overman TM, Sack man RW (2010) High assurance smart grid: smart grid control systems communications architecture. In: First IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, pp 19–24
2. Yarali A, Rahman S (2012) Smart grid networks: promises and challenges. J Commun 7(6):409–417
3. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (IoT): a vision, architectural elements, and future directions. Futur Gener Comput Syst 29(7):1645–1660
4. Spanò E, Niccolini L, Di Pascoli S, Iannacconeluca G (2015) Last-meter smart grid embedded in an internet-of-things platform. IEEE Trans Smart Grid 6(1):468–476
5. Gungor VC, Sahin D, Kocak T, Ergut S, Buccella C, Cecati C, Hancke GP (2013) A survey on smart grid potential applications and communication requirements. IEEE Trans Ind Inform 9(1):28–43
6. Kamyab F, Amini M, Sheykhha S, Hasanpour M, Jalali MM (2016) Demand response program in smart grid using supply function bidding mechanism. IEEE Trans Smart Grid 7(3):1277–1284
7. Logenthiran T, Srinivasan D, Shun TZ (2012) Demand side management in smart grid using heuristic optimization. IEEE Trans Smart Grid 3(3):1244–1252
8. Komninos N, Philippou E, Pitsillides A (2014) Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun Surv Tutorials 16(4):1933–1954
9. Hassan R, Radman G (2010) Survey on smart grid. In: Proceedings of the IEEE SoutheastCon (SoutheastCon), Concord, pp 210–213
10. Arghandeh R, von Meier A, Mehrmanesh L, Mili L (2016) On the definition of cyber-physical resilience in power systems. Renew Sust Energ Rev 58:1060–1069
11. Amin M (2014) A smart self-healing grid: In Pursuit of a more reliable and resilient system [in my view]. IEEE power and energy magazine, 12(1), 112–110
12. Gao J, Xiao Y, Liu J, Liang W, Chen CP (2012) A survey of communication/networking in smart grids. Futur Gener Comput Syst 28(2):391–404
13. Fouda MM, Fadlullah ZM, Kato N, Lu R, Shen XS (2011) A lightweight message authentication scheme for smart grid communications. IEEE Trans Smart Grid 2(4):675–685
14. Li X, Liang X, Lu R, Shen X, Lin X, Zhu H (2012) Securing smart grid: cyber attacks, countermeasures, and challenges. IEEE Commun Mag 50(8):38–45
15. Zhang Y, Wang L, Sun W, Green IIRC, Alam M (2011) Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Trans Smart Grid 2(4):796–808
16. Al-Ali AR, Aburukba R (2015) Role of internet of things in the smart grid technology. J Comput Commun 3(05):229
17. Lee EK, Gerla M, Oh SY (2012) Physical layer security in wireless smart grid. IEEE Commun Mag 50(8)
18. Nabeel M, Ding X, Seo SH, Bertino E (2015) Scalable end-to-end security for advanced metering infrastructures. Inf Syst 53:213–223
19. Liu N, Chen J, Zhu L, Zhang J, He Y (2013) A key management scheme for secure communications of advanced metering infrastructure in smart grid. IEEE Trans Ind Electron 60(10):4746–4756
20. Li H, Lu R, Zhou L, Yang B, Shen X (2014) An efficient merkle-tree-based authentication scheme for smart grid. IEEE Syst J 8(2):655–663
21. Zhao F, Hanatani Y, Komano Y, Smyth B, Ito S, Kambayashi T (2012) Secure authenticated key exchange with revocation for smart grid. In: IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, pp 1–8
22. Kim JY, Choi HK (2012) An efficient and versatile key management protocol for secure smart grid communications. In: IEEE wireless communications and networking conference (WCNC), Shanghai, pp 1823–1828
23. Tonyali S, Akkaya K, Saputro N, Uluagac AS (2016) A reliable data aggregation mechanism with homomorphic encryption in smart grid AMI networks. In: 13th IEEE consumer communications & networking conference (CCNC), Las Vegas, pp 550–555
24. Mahmood K, Chaudhry SA, Naqvi H, Shon T, Ahmad HF (2016) A lightweight message authentication scheme for smart grid communications in power sector. Comput Electr Eng 52:114–124
25. Sule R, Katti RS, Kavasseri RG (2012) A variable length fast message authentication code for secure communication in smart grids. In: IEEE power and energy society general meeting, San Diego, pp 1–6
26. Khasawneh S, Kadoch M (2017) A hybrid encryption scheme for advanced metering infrastructure networks. In: The proceedings of the 1st EAI international conference on smart grid assisted internet of things, Sault Ste. Marie, pp 1–11
27. Lenstra AK, Verheul ER (2001) Selecting cryptographic key sizes. J Cryptol 14(4):255–293
28. Stallings W (2011) Cryptography and network security. 5th edition, New York, Pearson
29. SEC 2: Recommended elliptic curve domain parameters, Certicom research 2000
30. Abdalla M, Bellare M, Rogaway P. The oracle Diffie-Hellman assumptions and an analysis of DHIES. In: Cryptographers track at the RSA conference. Springer, Berlin, pp 143–158
31. ANSI Standards Committee X9, Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography, ANSI X9.63–2001