Elgamal Elliptic Curve Based Secure Communication Architecture for Microgrids

Authors:

Sarmadullah Khan, Rafiullah Khan

Date Submitted: 2020-06-23

Keywords: secure communication, microgrid, security

Abstract:

Microgrids play an important role in today's power systems as the distributed generation is becoming increasingly common. They can operate in two possible modes: (i) standalone and (ii) grid-connected. The transitional state from standalone to grid-connected mode is very critical and requires the microgrid to be synchronized with the main grid. Thus, secure, reliable and trustworthy control and communication is utmost necessary to prevent out-of-sync connection which could severely damage the microgrid and/or the main grid. Existing solutions consume more resources and take long time to establish a secure connection. The objective of the proposed work is to reduce the connection establishment time by using efficient computational algorithms and save the resources. This paper proposes a secure authentication and key establishment mechanism for ensuring safe operation and control of the microgrids. The proposed approach uses the concept of Elgamal with slight modification. Private key of the sender is used instead of a random number. The proposed modification ensures the non repudiation. This paper also presents a system threat model along with security network architecture and evaluates the performance of proposed algorithm in protecting microgrid communication against man in the middle attacks and replay attacks that could delay the packets to damage the system and need to be detected. Mathematical modeling and simulation results show that the proposed algorithm performs better than the existing protocols in terms of connection establishment, resource consumption and security level.

Record Type: Published Article

Submitted To: LAPSE (Living Archive for Process Systems Engineering)

Citation (overall record, always the latest version):	LAPSE:2020.0716
Citation (this specific file, latest version):	LAPSE:2020.0716-1
Citation (this specific file, this version):	LAPSE:2020.0716-1v1

DOI of Published Version: https://doi.org/10.3390/en11040759

energies

MDPI

Article

Elgamal Elliptic Curve Based Secure Communication Architecture for Microgrids

Sarmadullah Khan [1,*] and Rafiullah Khan [2]

[1] School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK
[2] School of Electronics, Electrical Engineering and Computer Science (EEECS), Queen's University Belfast, Belfast BT7 1NN, UK; rafiullah.khan@qub.ac.uk
* Correspondence: sarmadullah.khan@dmu.ac.uk

Received: 28 February 2018; Accepted: 22 March 2018; Published: 27 March 2018

Abstract: Microgrids play an important role in today's power systems as the distributed generation is becoming increasingly common. They can operate in two possible modes: (i) standalone and (ii) grid-connected. The transitional state from standalone to grid-connected mode is very critical and requires the microgrid to be synchronized with the main grid. Thus, secure, reliable and trustworthy control and communication is utmost necessary to prevent out-of-sync connection which could severely damage the microgrid and/or the main grid. Existing solutions consume more resources and take long time to establish a secure connection. The objective of the proposed work is to reduce the connection establishment time by using efficient computational algorithms and save the resources. This paper proposes a secure authentication and key establishment mechanism for ensuring safe operation and control of the microgrids. The proposed approach uses the concept of Elgamal with slight modification. Private key of the sender is used instead of a random number. The proposed modification ensures the non repudiation. This paper also presents a system threat model along with security network architecture and evaluates the performance of proposed algorithm in protecting microgrid communication against man in the middle attacks and replay attacks that could delay the packets to damage the system and need to be detected. Mathematical modeling and simulation results show that the proposed algorithm performs better than the existing protocols in terms of connection establishment, resource consumption and security level.

Keywords: secure communication; microgrid; security

1. Introduction

The microgrid is one of the most feasible approaches to provide electricity and power to small location (e.g., homes, healthcare centers, armed forces bases, etc.) and also helps to integrate wind and solar energy generation systems into the main grid [1–3]. Key components of a microgrid include (1) connection from and to the main power grid (2) electrical loads and (3) a mean of backup energy source (e.g., renewable resources, etc.). However, the basic requirement for a microgrid is its capability to operate in both standalone mode and grid connected mode. In standalone mode, it usually provides voltage and frequency stability to meet the required local power demand and reduces the risk of blackout or disturbance during its transition phase from one mode to another. Microgrids also have the capabilities to resynchronize themselves while connecting to the main grid to avoid any disruption of power to sensitive loads.

For proper functioning of a microgrid, communication among its different components and communication with the main grid must be secure and reliable. The targeted communication is the microgrid control systems supported communication. To do so, control system can be divided into hierarchical layers, i.e., (1) primary (2) secondary and (3) tertiary layers [4–6]. The responsibility of

the primary control layer is to stabilize voltage and frequency during the transition period of the microgrid while to compensate any frequency or voltage deviation during the primary control layer is the responsibility of secondary control layer. Tertiary control layer is responsible for power flow management between the main grid and microgrid along with the coordination with other microgrids.

Each control layer consists of multiple different physical equipment having different computational resources. From the implementation point of view, each controller of the top layer in hierarchy takes input from the layer below it and generates parameters which are provided back to the lower layer controllers to perform appropriate control actions. This process of-course consumes time and different controllers working at different layers have their own timing constraints. Therefore an efficient communication algorithm needs to be developed to compensate unwanted communication delays between the layers and within a layer. Moreover, the security architecture must be capable to support various communication patterns (i.e., broadcast, multicast and unicast). Author [7] presented an Rivest–Shamir–Adleman (RSA) based security algorithm to cope with these timing constrains. RSA-based approaches are normally very expensive in term of computational time and resources consumption. The reasons behind the RSA computational cost are (1) large key length ranges between 1024–4096 bits and (2) expensive power and multiplication operations.

This paper proposes a secure communication architecture for microgrid control system that is based on Elgamal approach [8] and all the mathematical operations involved are addition and subtraction that are less computationally expensive as compared to the RSA operations. Also in the Elgamal approach, sender uses the public key of receiver and a random number to encrypt the message. However, this simple approach is prone to the man in the middle attack. We modified this simple approach by using the private key of sender to encrypt the message instead of a random number. As the computation involves the discrete logrithmic problem over a cyclic group, it does not reveal the sender private key. In addition, the receiver can verify and prove in future that the message was sent by the actual sender. In this way the non repudiation properties is achieved. Key features of the paper include (1) authentication of various devices used in microgrid control system, (2) development of secure communication algorithm that support real time communication among various components including resource constrained devices, (3) support various communication variants (i.e., multicast, broadcast and unicast) and (4) data confidentiality and data authentication.

The rest of the paper is organized as follows. A literature survey is provided in Section 2 while an overview of microgrids and their challenges is discussed in Section 3. Section 4 provides the details of adopted system model, attack scenarios and data communication. The proposed security algorithm is discussed in Section 5. The performance evaluation of the proposed algorithm is presented in Section 6. Finally, Section 7 concludes the paper.

Main Contributions

The key contributions of the proposed algorithm are:

- develop a secure communication architecture at low cost in terms of time and packet size,
- secure the network communication against well know attacks,
- reduce the energy consumption by controlling the packet size and reducing the communication overhead.

The proposed algorithm is compared theoretically and through simulations with other existing algorithms discussed in this paper. A results comparison shows that the proposed solution performs better than the existing algorithms in terms of computation resources, memory (storage) consumption and security level.

2. Literature

A detailed literature survey on cyber security was conducted in [9] considering the smart grid scenario. Here, we are highlighting only the relevant portion of this survey. IEC 62351 have

addressed many real time critical security features in smart grid communication. For example, data authentication and integrity is normally provided using digital signature, hashing function and access control mechanisms. Intrusion detection system is used to monitor any malicious activity within the network. To generate a digital signature, a hash of a message is created using one of the hashing algorithm (SHA, MD5, etc.). The generated hash is encrypted with the private key of the sender using RSA. This encrypted hash works as a digital signature. This is because, it can only be decrypted by the sender's public key. When a receiver receives a message, it separates encrypted hash from the actual message. The message is given to same hashing function at receiver side to generate a new hash. The receiver decrypts the received hash using the public key of sender. The receiver compares the new generated hash with the decrypted hash. If both are same, the receiver accepts the message as an authentic message. This approach is time consuming and has low acceptance rate at industry level. A low-latency, high-integrity security retrofit for legacy Supervisory Control And Data Acquisition (SCADA) systems is presented in [10]. In this paper, a bump in the wire approach is used to provide the security for serial communication among the devices in SCADA network (ad hoc network) using HMAC and AES. As AES is symmetric key approach and works on the shared key concepts, compromising one device can reveal the secret key and compromise the all the communication in network. Also this approach is feasible for ad hoc network where all the devices reside within a network and only the operator communicate with the devices locally or remotely. However, in case of microgrid approach where the devices of microgrid communicate with main grid and can be controlled locally or remotely, symmetric key approach is more prone to the key cmpromission attacks.

Recent researches [11,12] have proposed different security approaches for time constrained applications that are based on (1) RSA (2) message authentication code (MAC) and (3) using one time signature (OTS). MAC schemes are based on single common key between sender and receiver. For example, Timed Efficient Stream Loss-tolerant Authentication (TESLA) [11] is one of the famous MAC scheme that divides time into slot to provide a timed efficient stream loss-tolerant authentication. The sender usually signs messages using different keys for different time intervals. Once the key is expired, sender make it public. Hence all the receivers who have buffered the received messages from sender can now verify the authenticity of messages using this public key. Meanwhile, sender uses another new key for MAC. This approach help multiple receivers to verify a single message using only one key. However, memory requirement of this approach is high as each receiver needs to buffer all the received messages until they are not verified. This approach is not suitable for real time communication in microgrid scenario. To overcome this drawback, sender shares a key with each individual receiver and then signs the MAC using this shared key for each receiver. Receiver uses the same common key to verify the MAC. However, this approach has a high communication overhead as each message carries n MACs for n receivers.

One time signature schemes [12] tried to solve the issue of replay attacks. One approach [13] uses the precomputed hash chain to verify and authenticate data. In this approach, a mapping is first created between the data and precomputed hashes. However this approach suffers from large precomputation overhead and memory cost.

Recent researches focus on the smart grid security and very little attention is given to microgrid security. A survey on the microgrid architecture, protocols and possible security threats is conducted in [14]. This survey mainly focused on grouping together the microgrid equipments of the same functionality. However communication security in terms of authentication and secure channel establishment among different control elements is not discussed. A novel locality algorithm and peer-to-peer communication infrastructure for optimizing network performance in smart microgrids is proposed in [15] but it did not focus on the security aspects of mircogrid communication. This paper proposes an efficient authentication and secure channel establishment procedure based on the Elgamal elliptic curve concept.

3. Overview of Microgrid System

A medium voltage DC microgrid was proposed by [16,17] to supply electrical energy to offshore companies. Its objective was to supply power to run large motors, pumping and drilling of surfaces along with other equipment (e.g., lighting, heating, cooling, etc.). Figure 1 shows the architecture of a microgrid power system. 5 MW wind turbines are used to produce AC current that is fed as the main electricity source while diesel electric generators are used for backup supply at each individual platform. The generated AC power from wind turbines is converted into DC electric power using a three level clamped rectifier that generate DC bus voltage of 5 KV. DC/DC converters are used to establish an interface between a DC bus and offshore production platform. The purpose of the controller is to transform DC voltages in the system and provide paths for power flow. The main load on this platform is the load of induction motors that are used to run drilling machines and other equipment. These loads are usually in megawatts and are considered as constant loads.

Both machine current and its flux are controlled by primary controller using dq-axis control. Secondary controller controls the supply to DC/DC converters. These controllers take inputs from the primary controllers. The details of the control algorithms are given in [16].

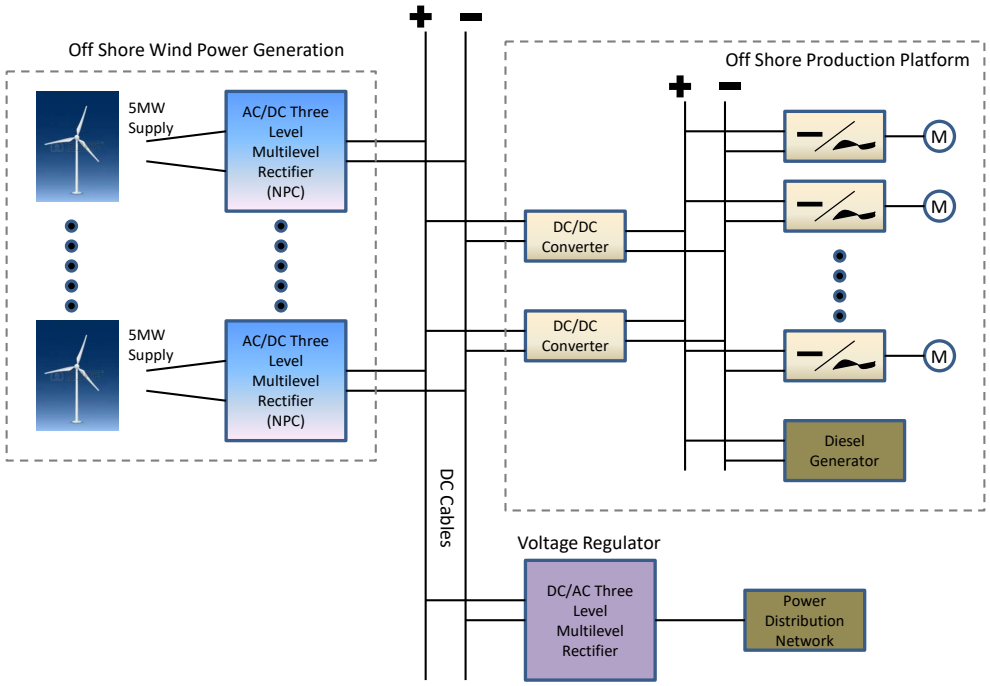

Figure 1. Offshore production platform with offshore wind power generation.

In general, offshore platforms are powered by wind turbines that makes a interconnected microgrid system. Figure 2 shows the control and communication architecture of the system [17]. For the purpose of power protection and regulation, a number of logical communication channels with the communication architecture are developed inside the microgrid. For example, from primary controller to the secondary controller and from secondary controller to the DC/DC converters, backup generator, voltage regulator, and breakers. Secondary controller usually provides and receives information from tertiary controller regarding power flow in and out of the microgrid. So tertiary controller of one microgrid communicates with the tertiary controllers of other microgrid as shown in Figure 2.

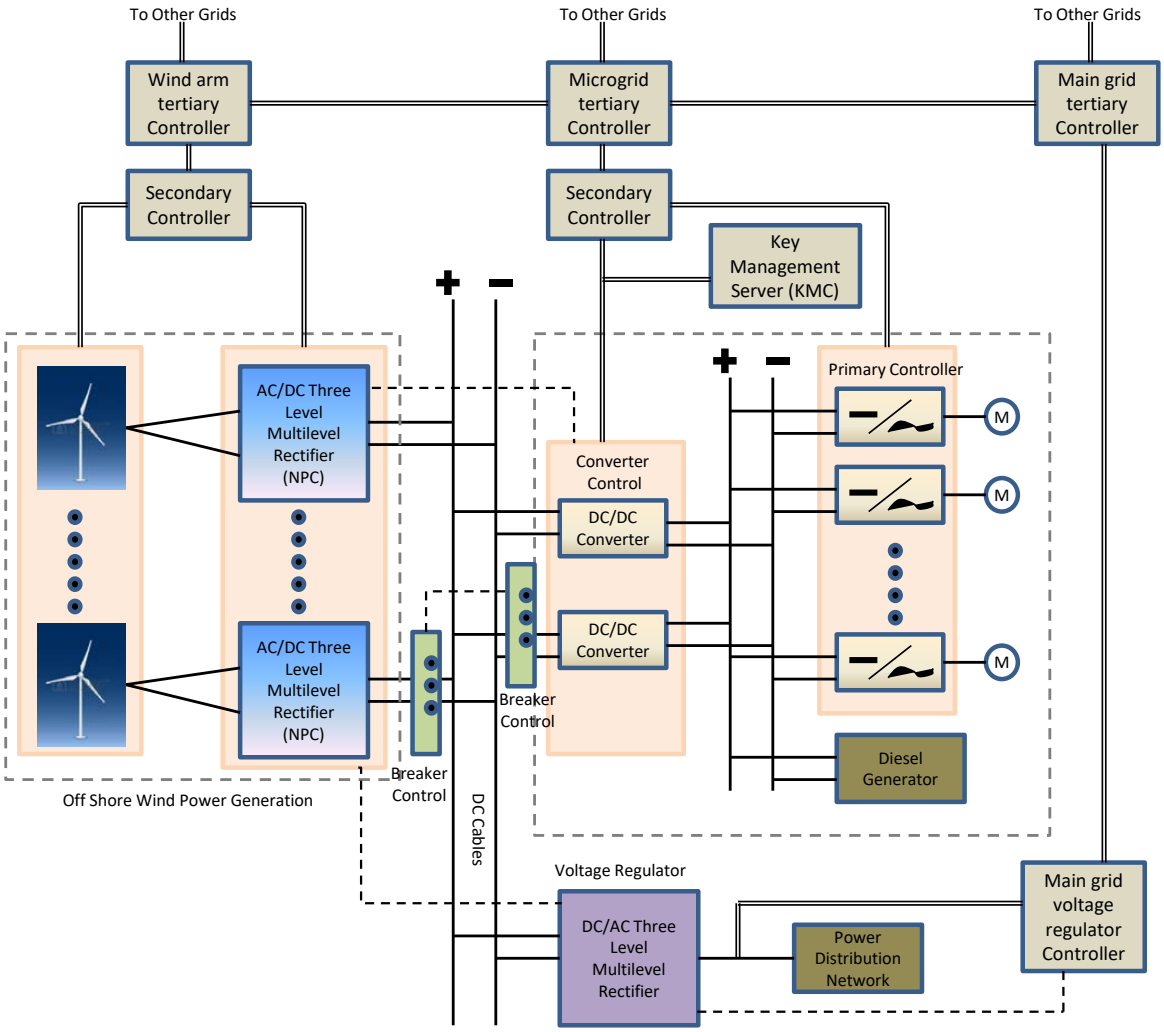

Figure 2. Offshore platform microgrid control and communication architecture.

Microgrid communication network actually provides a mean for its various elements to communicate with each other for proper functioning and its integration with main grid station. Such communication network must fulfill the following requirements: (i) guarantee real time performance (ii) worst case delay performance (iii) reliable and secure communication to provide confidentiality and integrity and (iv) access and availability. However, the propagation delay can be minimized by using high bandwidth communication links but the delays introduced by the control elements that are the main source of communication messages are out of control of the communication network. This is because, most of the control elements (voltage regulators, protection relays etc.) used in microgrid are equipped with low cost and low power processor with very limited memory to execute tasks. Hence the execution time of these equipment must be considered in designing an efficient security algorithm to ensure confidentiality and integrity.

From primary, secondary and tertiary controller point of view, primary controller usually performs operation in milliseconds. Here we need a semi-independent primary controller that takes into account the commands from secondary controller at a frequency in the range of tens of milliseconds or more [18]. For example, secondary controller generates a demand response whenever a supply from renewable energy decreases or energy consumption is increases. Hence secondary controller needs to operate 5–10 times slower than the primary controller. Power management between the main grid and microgrids or among the microgrids is controlled by tertiary controllers.

4. System Model and Attack Model

4.1. System Model

The proposed system model is shown in Figure 3. The meter is considered at front end of the microgid network. Each micorgrid is assumed to have different owner and has an independent security features from each other. It means, other mircogrids are considered insecure and lossy in the worst case condition. Multicast communication approach is considered in the proposed architecture as shown in Figure 3. For example, sender S is communicating with multiple receivers R_i, (where $i = 1, 2, 3, ..., n$). Notations used in this paper are summarized in Table 1.

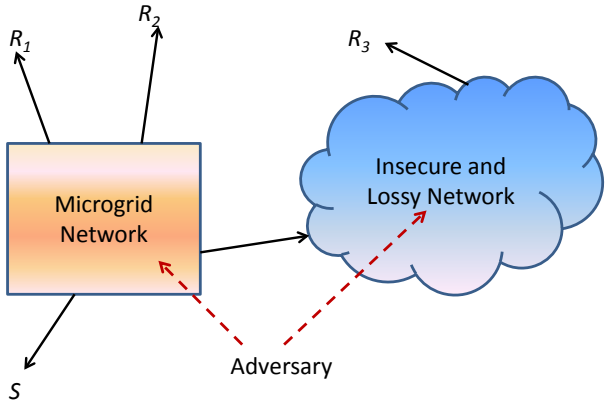

Figure 3. Network Model.

Table 1. Notation Table.

Parameters	Definition
S, R_i, n	sender, i-th receiver, total number of receivers
t_d	Time to deliver a message by the network
t_S	Sender delay (encryption + signing)
t_R	Receiver processing delay (decryption + verification)
K_g	Group key
K_{IED}	Public key
PK_{IED}	Private key
$K_{i\text{-}auth}$	Authentication key
t_{IED}	Time to execute cycle of IED's control logic
d_{msg}	Message size in bits
t_{max}	Maximum end to end delay
KMC	Key Management center
Nonce	Nonce generated by IED (Intelligent Electrical Devices)

End to end communication steps are shown in Figure 4. Here Intelligent Electrical Devices (IEDs) and controller communicate with each other through User Datagram Protocol over Internet Protocol stack.(UDP/IP) This is followed as a standard practice in real time systems [19]. This is because Transmission Control Protocol over Internet Protocol stack (TCP/IP)is not desirable because of its re-transmission characteristics of loss packets. Sometimes retransmission takes long time and till then the information might be useless to the receiver. Periodic transmission of data is key factor to achieve reliability in communication system. Network delay (t_d) as shown in Figure 4 includes both propagation delay and transmission delay while t_S is the time that a device takes to create a packet after receiving a message from the application layer. Receiver after receiving the message takes t_R time to process the packet and gives it to the application layer at the receiving device. t_{max} is the

maximum end-to-end delay for all possible recipients. However, for successful transmission, t_{max} must be greater than $t_S + t_d + t_R$. Based on this assumption, if the message is received after t_{max}, it will be discarded. The optimal value of t_{max} is calculated in such a way to keep the operation of microgrid power control in stable condition. There are many factors that influence end-to-end delays. For example, communication links quality, operating systems, execution time of applications, IED's hardware computation capabilities, and network architecture.

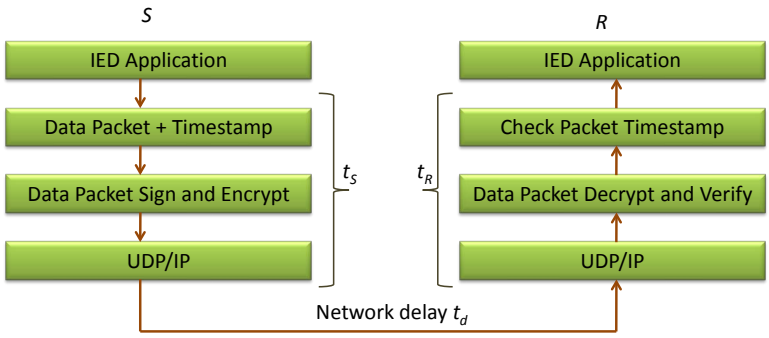

Figure 4. End to end communication model within microgrid.

In the proposed model, we have divided the messages into three different types i.e., (1) data messages that carry actual sensed data (2) safety messages that carry the emergency operations related data (e.g., shutting down the circuits to protect the system from damage) and (3) control messages that controls and sets the power plant network operational profile. For our data modeling, we are using control messages as these are more critical and time sensitive messages.

It is also considered that all IEDs are working in safe mode to protect the system. In the proposed algorithm, the Key Management Center (KMC) is considered as a centralized trusted third party that helps in the authentication and key establishment process among the devices belonging to different microgrids.

4.2. Attack Model

The attack model in this paper consists of an adversary that has the following capabilities.

- It has full access to microgrid network communication.
- It can eavesdrop, capture, replay, drop, delay and modify packets.

With these capabilities, an adversary can easily modify the packet contents and inject fake packets. Adversary can also eavesdrop, intercept, drop or delay packets easily or analyze packets passively to get information from the intercepted packets.

5. Security Algorithm

The motivation behind the proposed security architecture is to enable the entities/devices in microgrids to authenticate each other and communicate securely. Also the algorithm must be resilient to the impersonation attacks, man in the middle attacks and replay attacks. To this aim, each entity/device needs to decrypt and verify the messages within the maximum time period i.e., t_{max}. Similarly if adversary inject some malicious or fake data, the devices must be able to recognize and discard it. In the proposed architecture, we also assume an independent and standalone Key Management Center (KMC). The proposed key generation algorithm is based on Elgamal Elliptic Curve Cryptography. This approach uses a key of length 130–160 bits. It does not require to share a common key like in symmetric key approach.

5.1. Key Pre-Distribution

Each IED is given an initial one time authentication key $K_{i\text{-}auth}$ during the manufacturing process by the company. Once the IED is installed in microgrid architecture, it sends a join request to KMC. This join request is encrypted with $K_{i\text{-}auth}$. The KMC contacts the IED's Manufacturing Company (IMC) through secure link (secured by public key infrastructure approach) and requests for the IED's authentication key $K_{i\text{-}auth}$. The IED's manufacturing company sends the encrypted version of $K_{i\text{-}auth}$ using the KMC public key and signed by its own private key. This ensures the authenticity and integrity of the received $K_{i\text{-}auth}$.

$$\text{IED} \rightarrow \text{KMC} : \{\text{IED}, Nonce\}_{K_{i\text{-}auth}} \tag{1}$$

$$\text{KMC} \rightarrow \text{IMC} : \{Req.K_{i\text{-}auth}\}_{K_{\text{IMC}}} \tag{2}$$

$$\text{IMC} \rightarrow \text{KMC} : \{K_{i\text{-}auth}\}_{K_{\text{KMC}}} || H\{K_{i\text{-}auth}\} \tag{3}$$

where K_{IMC} and K_{KMC} are the public keys of IMC and KMC respectively.

After receiving $K_{i\text{-}auth}$, KMC decrypts the join request containing a *Nonce*. KMC increments the received *Nonce*, encrypts it using $K_{i\text{-}auth}$ and sends it back to the IED along with the elliptic curve parameters $E_P(a, b)$, KMC public key and list of other IEDs installed.

$$\begin{aligned} \text{KMC} \rightarrow \text{IED} : \{Nonce + 1\}_{K_{i\text{-}auth}} || E_P(a, b) \\ || K_{\text{KMC}} || \text{IED's IDs} \end{aligned} \tag{4}$$

As the IED receives an incremented *Nonce* and verified successfully by $K_{i\text{-}auth}$, it generates its own public/private key pair ($K_{\text{IED}}/PK_{\text{IED}}$) based on the received elliptic curve information and sends its public key back to KMC for registration, signed by $K_{i\text{-}auth}$. KMC registers public keys of all the IEDs after verification.

$$\text{IED} \rightarrow \text{KMC} : K_{\text{IED}} \,||\, H_{K_{i\text{-}auth}}(K_{\text{IED}}) \tag{5}$$

In order to communicate with other IEDs in the network, IED$_i$sends a request to KMC for the public key of IED$_j$. KMC sends the public key of IED$_j$ to IED$_i$ signed by its own private key for the authentication purpose.

$$\text{IED}_i \rightarrow \text{KMC} : \text{Request } K_{\text{IED}_j} \tag{6}$$

$$\text{KMC} \rightarrow \text{IED}_i : K_{\text{IED}_j} \,||\, H_{PK_{\text{KMC}}}(K_{\text{IED}_j}) \tag{7}$$

where PK_{KMC} is the private counter part of K_{KMC} and is only known to KMC.

5.2. Key Generation Procedure

This section describes the details of public and private key generation using elliptic curve cryptography as shown in Algorithm 1. Before starting to generate a public/private key pair, an KMC/IED selects an elliptic curve $E_P(a, b)$. KMC/IED then chooses a point on this elliptic curve i.e., E_1 and a random number R. This random number R acts as a private key and it describes that how many times E_1 must be added with itself to generate E_2. KMC/IED keeps R secret as its private key and announces E_1, E_2 and P as public key to other devices.

Algorithm 1 Key Generation

Select an elliptic curve $E_P(a, b)$
Select a point E_1 *on* $E_P(a, b)$
Select a private key d
Calculate $E_2 = RE_1$
Keep d secret as private key
Make (E_1 *,* E_2*,* $E_P(a, b)$*) public*

5.3. Secure Communication

In the proposed communication protocol, we first encrypt the message and then generate its hash (i.e., MAC). This approach helps the receiver to verify the message first and then decrypt. If receiver receives a fake message, it will not be able to verify the message and hence receiver will not try to decrypt it. This reduces the unnecessary decryption and save the resource of devices.

5.3.1. Unicast Communication

The proposed one-to-one secure communication model works as follow:

- For an IED_i to communicate with other IED_j, it requests the public key of IED_j from the KMC as shown in Equations (6) and (7).
- IED_i encrypts the message (M) using its own private key (R_i) and public key of IED_j (E_{j1}, E_{j2}, E_P) as follow:

$$C_1 = R_i E_{j1} \tag{8}$$

$$C_2 = M + R_i E_{j2} \tag{9}$$

  C_1 and C_2 are the two cipher texts generated for the message M.
- Once the message is encrypted, IED_i generates a MAC from the encrypted message and signs it with its own private key as.

$$\text{MAC} = \{H(C_1 + C_2)\}_{R_i} \tag{10}$$

  where H is a hashing function used to generate a hash that acts as a message authentication code MAC.
- IED_i sends C_1, C_2 and MAC to IED_j

$$\text{IED}_i \rightarrow \text{IED}_j : [C_1 \,||\, C_2 \,||\, \text{MAC}] \tag{11}$$

- IED_j creates MAC′ from the received message using the same hashing function H and compares it with the received decrypted MAC as

$$\text{MAC}' = H(C_1 + C_2) \tag{12}$$

$$\text{MAC} = \{H(C_1 + C_2)_{PK_{\text{IED}_i}}\}_{K_{\text{IED}_i}} = H(C_1 + C_2) \tag{13}$$

- If the received decrypted MAC is equal to the new calculated MAC′, it accepts the message and decrypts the entire message as

$$M = C_2 - (R_j \times C_1) \tag{14}$$

$$M = M + R_i E_{j2} - (R_j \times R_i E_{j1}) \tag{15}$$

$$M = M + R_i R_j E_{j1} - R_j R_i E_{j1} \tag{16}$$

$$M = M \tag{17}$$

  otherwise it discards the messages.

There is also a possibility that an IED communicates with other IED of other networks. This usually happens if there are two circuit breakers installed at both ends of a long power line. These two IEDs might belongs to two different networks. In this scenario, an IED gets the public key of other networks IED through its own KMC. KMC of one network IED contacts with KMC of other network IED to get the public key of that IED.

5.3.2. Broadcast and Multicast Communication

Sometimes IEDs need to broadcast or multicast a message. More specifically, IEDs do broadcasting or multicasting in an emergency scenarios in order to let other IEDs to either shutdown or brake

circuits. To this aim, an broadcast or multicast authentication and encryption key, called group key K_g, is generated by KMC for its member IEDs and distributed among those IEDs. This means that K_g is only valid for those IEDs that are part of KMC and are not known to those IEDs that belongs to other KMCs.

6. Evaluation

In order to evaluate the performance of the proposed scheme, it is compared with some well known algorithms i.e., RSA-based Public Key Infrastructure (PKI), Digital Signature Algorithm (DSA) and Time Valid Hash to Obtain Random Subsets (TV-HORS).

6.1. Key Length

In order to evaluate the performance of the proposed algorithm, time is considered one of the most important parameter. Table 2 shows the time consumption comparison of different algorithms using a 600 MHz microprocessor. The key lifetime is limited to 2^{48} according the National Institute of Standards and Technology (NIST) recommendations. The proposed security scheme is based on elliptic curve crytography approach used for both (1) authentication and (2) secure communication.

Table 2. Security Algorithm Time Performance Statistics.

OpenSSL Performance Statistics for VIA Eden 600 MHz	
Microgrid message payload (d_{msg}) [17]	42 bytes
Time for 160-ECC encryption/decryption	0.007 ms
Time for 192-AES encryption/decryption	0.008 ms
Time for 192-AES CMAC auth. tag	0.008 ms
Time for SHA-256 digest	0.007 ms
Time for RSA-2048 signature	312.5 ms
Time for RSA-2048 signature verification	9.1 ms
Time for DSA signature	91.7 ms
Time for DSA signature verification	111.1 ms

In the proposed algorithm, the key size to achieve the required minimum key lifetime is 160 bits while we need a key of size 2014-bits in case of RSA PKI, 256-bit for DSA. The OTS protocol used for comparison is TV-HORS. This has much better performance than the other OTS algorithms [20]. For the required minimum key lifetime, at least 500 KBytes of key length is required for TV-HORS [13]. Each primary controller in offshore microgrid sends a message at every 80 ms. Hence a total of 13 messages send per second. The minimum time required to bootstrap a key in TV-HORS approach is 120 s which makes the lifetime of key equals to 840 s. Each IED is need to refresh its key after every 840 s (14 min). However, bootstrapping a new key takes 120 s (2 min) and this solution is not practically feasible.

6.2. Theoretical Analysis

Although there is no standard benchmark for t_{max}, we assumed it to be 3 ms according to IEC 61850. Table 3 presents the comparative analysis in terms of key size and total number of keys stored. In the proposed scheme, if there are n IEDs in the network, each one stores only $K_{i\text{-}auth}$, $K_{\text{IED}}/PK_{\text{IED}}$ and K_g keys while [7] needs to store k_c, two KS keys, and $2(n-1)$ session secret keys and thus have a high communication overhead specially in the broadcast scenario. In order to calculate the packetization delay t_S, we considered only the encryption and authentication process while t_R is the time to verify the messages at the receiver. Since TV-HORS does precomputation, its delay is minimum than the RSA and DSA. Normally packetization and verification time in RSA and DSA exceed 3 ms which is the standard end to end delay in microgrid communication. Therefore RSA-based PKI approaches are not considered suitable for microgrid communication. Communication overhead of the RSA scheme is 2048 bits per message.

Table 3. Comparative Analysis of Microgrid Security Algorithms.

Security Algorithm	Storage per IED	t_S (ms)	t_R (ms)	Packet Size (bits)	Max. R_i	Clock Sync Required
Proposed	4×160 bits	$\approx n \times 0.007$	≈ 0.014	$d_{msg} + 160$	Unlimited	No
Reference [7]	$(3 + (2n - 1)) \times 192$ bits	$\approx n \times 0.008$	≈ 0.016	$d_{msg} + (n - 1) \times 96$	>300	No
RSA	2048 bits	≈ 312.5	≈ 9.1	$d_{msg} + 2048$	0	No
DSA	256 bits	≈ 91.7	≈ 111.1	$d_{msg} + 160$	0	No
TV-HORS	>500 KB	≈ 0.0015	≈ 0.0015	$d_{msg} + 11.256$	Unlimited	Yes

Figure 2 represents a communication network connecting IEDs with each other and it has Key Management Center (KMC), circuit breaker controls, DC/DC converters, DC generator and voltage regulator, 10 primary controllers, secondary controllers and tertiary controllers. This communication network consists of less than 50 IEDs. t_{IED} represents the time consumed by IED application, t_{pri} is the time taken by primary controller, t_{sec} is the time taken by secondary controller, t_{ter} is the time taken by tertiary controller, t_{conv} is DC/DC conversion time and t_{reg} is the time consumed by the voltage regulators. The execution time of the control loop is the total time duration between the sensing event (performed by sensing IED) and action event (performed by action IED). In this paper, we only consider the execution time of the primary-secondary control loop and tertiary-secondary control loop. Within the microgrid communication network, IEDs are connected to each other through a link having a capacity of (0.1–10 Gb/s) while IEDs data generation rate is (10–100 kb/s). Hence there will be no congestion over the microgrid communication network. Intermediate routers and switches delay is ignored in this work.

6.2.1. Primary-Secondary Control Loop

The job of the primary controller is to measure the speed and torque of a motor and provides this information to secondary controller after every t_{pri} seconds. Upon receiving this information, secondary controller calculates duty cycle for each DC/DC converter. In this way, power to the machines is controlled. The total time consumed in measuring the speed and torque and then taking appropriate action for power adjustment is known as the delay of primary-secondary control loop $T_{pri\text{-}sec}$. It is shown in Figure 5. Normally, primary controller and DC/DC converters operate in parallel but secondary controller waits to receive all the data before taking any action. Hence an additional delay of $n_{pri} \times t_R$ occurs due to n_{pri} number of primary controllers. Therefore, the delay $T_{pri\text{-}sec}$ of primary-secondary control loop is

$$T_{pri\text{-}sec} = t_{pri} + t_{sec} + t_{conv} + 2 \times t_S + 2 \times t_d + (n_{pri} + 1) \times t_R. \tag{18}$$

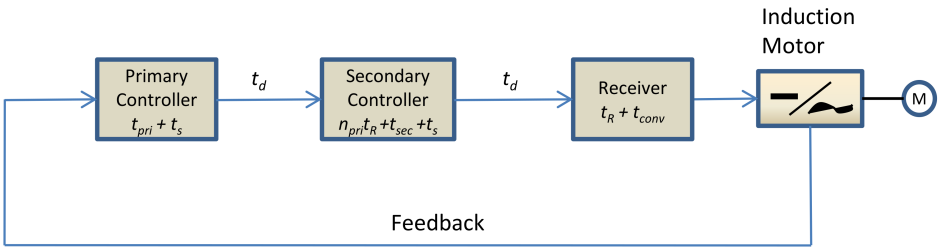

Figure 5. Microgrid's primary and secondary distribution control loop.

For example, if the bandwidth of the communication link is 100 Mbps and using Table 2, approximate propagation delay t_d is 0.04 ms. From the literature, t_{sec} is set to 500 ms, t_{conv} is set to 500 ms [6], and t_{pri} is set to 80 ms [18]. Final control loop delay for security purpose of the proposed algorithm is 1070 ms. While the CMAC-192-based approach has a delay of around 1080 ms, the RSA-based approach has a delay of 1805 ms and DSA has a total delay of around 2485 ms.

6.2.2. Tertiary-Secondary Control Loop

The tertiary-secondary control loop delay is also calculated in the same way as described above. The total delay is represented as:

$$T_{ter\text{-}sec} = t_{ter} + t_{sec} + t_{conv} + 2 \times t_S + 2 \times t_d + 2 \times t_R \quad (19)$$

In case of the broadcast scenario, total delay of the proposed algorithm is 1460 ms while CMAC-based approach has a delay of 1570 ms, RSA has a delay of 2144 ms.

6.3. Simulation Setup and Results

The simulation environment to evaluate the performance of the proposed microgrid architecture consists of MATLAB (Version 8, Mathworks, Natick, MA, USA) and OMNeT++ (Version 4.1, OpenSim Ltd., Stanford, CA, USA). Communication network simulation is performed in OMNeT++ simulator while power system is evaluated using MATLAB [16]. User Datagram Protocol (UDP) protocol is used as transport layer protocol to avoid handshake delay and retransmission delay and used 100 Mbps Ethernet links for connection. Custom adaptive scheduler is used for interfacing two simulators. Since the two simulators interact with each other based on the action and decision of each controller, scheduler take care of the speed, execution time and event handler to synchronize the operation of two simulators.

For the attack scenarios, all the communication among IEDs is made available to the attackers and the attacker device is made to accept all the traffic within the network. In this way, the attacker has access to all the public parameters and messages shared among different IEDs through wireless channel. To implement, man in the middle attack, the attacker device is made a first hop neighbor of sending IED while all other receiving IEDs are made second hop neighbors of sending IEDs. The attacking device changes the content of the message while it does not drop the message. This is because communication is UDP-based and messages normally follow more than one path so dropping of messages by attacker is ignored in this simulation.

The results are obtained by varying the total number of receivers in a multicast environment. In each scenario, induction motors and primary controller start with the interval of 1 s. In order to rectify the disturbance introduce by the induction motor, secondary controllers send duty cycle to DC converters. Once microgrid comes in full running sate, it does the transition from island mode to the grid connected mode.

Primary-secondary control loop delay is observed when all the IEDs were active. Table 4 shows the maximum observed primary-secondary control loop delay. The difference between the theoretical delay and simulation delay is due to the intermediate nodes of the simulation environment and also because of fact that secondary controller emits action only when it receives all the information from all primary controllers. The proposed solution is also compared with the CMAC, RSA and DSA approaches that have higher delays. Moreover, RSA and DSA have also stability issues in power system because of their large delay. TV-HORS is not considered as it has a very long key bootstrap time and results in unstable behavior of power system as well.

Table 4. Maximum Distributed Control Loop Delay.

Protocol	Distributed Control Loop Delay [Theoretical/Simulation]
Proposed ECC Based	1070/1099.5 ms
CMAC-192, CMAC-96	1080/1128.5 ms
RSA	1805/2093.7 ms
DSA	2485/4424.3 ms

6.4. Man in the Middle Attack (MMA)

The Man in the Middle Attack (MMA) is one the dangerous attacks that is very difficult to detect in a normal scenario. In this attack, an attacker comes in the middle between sender (S) and receiver (R) if both S and R are not in the radio coverage range of each other. Attacker impersonates itself as R for S and S for R without being detected. In this way, attacker can modify, read or inject fake packets.

In the simulation of the proposed scheme, a malicious node acts as man-in-the-middle is introduced in such a way that all the messages exchange between the S and R passes through this node. The features of malicious node are (1) store each message for future use and (2) corrupt message by replacing the message payload without changing the header. As S and R have been assigned K_{auth}, it is used to encrypt and sign the join message that passes through the malicious node. Malicious node changes the payload of the message. As malicious node does not have K_{auth}, it cannot encrypt the new payload and cannot replace the signature. When the destination receives the message, it decrypts it using K_{auth}, generates signature (hash) from the decrypted message and compare it with the received signature. As the received signature does not match the geneated signature of the message, receiver discard the message because of message corruption. It also gives an indication to the receiver that there is man-in-the-middle attack.

During the normal operation, each device signs the messages using its private key. Malicious node does not know the private key of every other node of the network. Hence malicious node cannot replace the signature or modify the message as it is easily detected at the receiving side.

6.5. Replay Attacks

As explained above, malicious node is given the capability to store the received messages, it can also replay the captured packets after some time to disrupt the proper functionality of microgrid. In the proposed architecture, we stamps each message with a timestamp as shown in Figure 4. This helps the receiver to differentiate between the new message and an old replayed message. This is because, if the message is received after t_{max}, it is discarded by the receiver. In this way, proposed security architecture works well against the replay attacks.

7. Conclusions

In this paper, a secure authentication and key establishment algorithm is proposed for microgrid architecture that is less computationally expensive and supports the microgrid communication environment without disturbing its operation. The proposed model is based on a modified version of Elgamal that improved the cipher text authenticity as well as achieved the non repudiation property. In terms of time, the proposed solution performed better than the existing key establishment algorithms. The simulation results using OMNeT++ ensured the security of the proposed algorithm against man in the middle attacks and replay attacks. The analytical and simulation results showed the effectiveness of the proposed algorithm over the existing state of the art algorithms in terms of speed, memory consumption and computational power.

Author Contributions: All authors equally contributed to this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Piagi, P.; Lasseter, R.H. Autonomous control of microgrids. In Proceedings of the 2006 IEEE Power Engineering Society General Meeting, Montreal, QC, Canada, 18–22 June 2006; p. 8.
2. Prodanovic, M.; Green, T.C. High-Quality Power Generation Through Distributed Control of a Power Park Microgrid. *IEEE Trans. Ind. Electron.* **2006**, *53*, 1471–1482.
3. Anand, S.; Fernandes, B.G.; Guerrero, J. Distributed Control to Ensure Proportional Load Sharing and Improve Voltage Regulation in Low-Voltage DC Microgrids. *IEEE Trans. Power Electron.* **2013**, *28*, 1900–1913.

4. Lasseter, R.H.; Paigi, P. Microgrid: A conceptual solution. In Proceedings of the 2004 IEEE 35th Annual Power Electronics Specialists Conference (IEEE Cat. No.04CH37551), Aachen, Germany, 20–25 June 2004; Volume 6, pp. 4285–4290.
5. Bidram, A.; Davoudi, A. Hierarchical Structure of Microgrids Control System. *IEEE Trans. Smart Grid* **2012**, *3*, 1963–1976.
6. Guerrero, J.M.; Vasquez, J.C.; Matas, J.; de Vicuna, L.G.; Castilla, M. Hierarchical Control of Droop-Controlled AC and DC Microgrids—A General Approach Toward Standardization. *IEEE Trans. Ind. Electron.* **2011**, *58*, 158–172.
7. Kounev, V.; Tipper, D.; Yavuz, A.A.; Grainger, B.M.; Reed, G.F. A Secure Communication Architecture for Distributed Microgrid Control. *IEEE Trans. Smart Grid* **2015**, *6*, 2484–2492.
8. Elgamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* **1985**, *31*, 469–472.
9. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A Survey on Cyber Security for Smart Grid Communications. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 998–1010.
10. Tsang, P.P.; Smith, S.W. YASIR: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems. In *Proceedings of The Ifip Tc 11 23rd International Information Security Conference*; Jajodia, S., Samarati, P., Cimato, S., Eds.; Springer: Boston, MA, USA, 2008; pp. 445–459.
11. Perrig, A.; Canetti, R.; Tygar, J.D.; Song, D. Efficient authentication and signing of multicast streams over lossy channels. In Proceedings of the 2000 IEEE Symposium on Security and Privacy, S&P 2000, Berkeley, CA, USA, 14–17 May 2000; pp. 56–73.
12. Cairns, K.; Hauser, C.; Gamage, T. Flexible data authentication evaluated for the smart grid. In Proceedings of the 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm), Vancouver, BC, Canada, 21–24 October 2013; pp. 492–497.
13. Wang, Q.; Khurana, H.; Huang, Y.; Nahrstedt, K. Time Valid One-Time Signature for Time-Critical Multicast Data Authentication. In Proceedings of the IEEE INFOCOM 2009, Rio de Janeiro, Brazil, 19–25 April 2009; pp. 1233–1241.
14. Veitch, C.K.; Henry, J.M.; Richardson, B.T.; Hart, D.H. *Microgrid Cyber Security Reference Architecture*; Sandia Nat. Lab.(Hierarch. SNL-NM): Albuquerque, NM, USA, 2013.
15. Marzal, S.; Gonzlez-Medina, R.; Salas-Puente, R.; Figueres, E.; Garcer, G. A novel locality algorithm and peer-to-peer communication infrastructure for optimizing network performance in smart microgrids. *Energies* **2017**, *10*, 9.
16. Grainger, B.M.; Reed, G.F.; McDermott, T.E.; Mao, Z.H.; Kounev, V.; Tipper, D. Analysis of an offshore medium voltage DC microgrid environment—Part I: Power sharing controller design. In Proceedings of the 2014 IEEE PES T&D Conference and Exposition, Chicago, IL, USA, 14–17 April 2014; pp. 1–5.
17. Kounev, V.; Tipper, D.; Grainger, B.M.; Reed, G. Analysis of an offshore medium voltage DC microgrid environment—Part II: Communication network architecture. In Proceedings of the 2014 IEEE PES T&D Conference and Exposition, Chicago, IL, USA, 14–17 April 2014; pp. 1–5.
18. Guerrero, J.M.; Vasquez, J.C.; Matas, J.; Castilla, M.; Garcia de Vicuna, L. Control Strategy for Flexible Microgrid Based on Parallel Line-Interactive UPS Systems. *IEEE Trans. Ind. Electron.* **2009**, *56*, 726–736.
19. Won-jong Kim, K.J.; Ambike, A. Real-time operating environmentfor networked control systems. *IEEE Trans. Autom. Sci. Eng.* **2006**, *3*, 287–296.
20. Law, Y.W.; Gong, Z.; Luo, T.; Marusic, S.; Palaniswami, M. Comparative study of multicast authentication schemes with application to wide-area measurement system. In Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (ASIA CCS '13), Hangzhou, China, 8–10 May 2013; pp. 287–298.