J. Appl. Environ. Biol. Sci., 6(3S)127-133, 2016

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

A Novel Secure Multicast Communication in Smart Grid Based on Signcryption

Nizamuddin, Arif Iqbal Umar, Noor Ul Amin, Abdul Waheed

Department of Information Technology, Hazara University Mansehra, Pakistan

Received: January7, 2016
Accepted: March 2, 2016

ABSTRACT

Smart grids are emerging to promote sustainable ways of living. Due to hierarchal structure, multicast is envisioning in many smart grid applications such as various operation and control, wide area protection, demand-response and in-substation protection. Security and privacy of multicast messages is one of the important and challenging concerns. We proposed a novel secure multicast communication protocol based on multi receiver signcryption. It provides the functionality of confidential and authenticated multicast session key agreement and instant secure message communication. It is efficient in term of computation and communication cost and suitable for secure multicast communication in smart grid.

KEYWORDS: Smart Grid; Secure Multicast; Key Agreement; Signcryption

1. INTRODUCTION

The safety of power grids infrastructure is vital for safety of human life, economic growth and functional routine life. Traditional grids evolved to Smart Grid (SG) for efficient and balance demand response of resources utilization. Intelligent communication system is the core of smart grid. It links grid components in an efficient manner and enables flow of electricity and information among the producer, service provider and consumers.

As an interlinked network, security of smart grid communications is one of major concern. Security breach can potentially harm it such as miss billing, black outs etc.

Multicast is an efficient mean of one-to-many communications and has tremendous applications in smart grid as: For wide area protection and cascaded failures prevention, Phasor Measurement Units (PMUs), measure system parameters and multicast the information to control centers, which take appropriate actions. Utility centers multicast demand-response command to customer, to reduce energy demands in peak hour by temporarily turning off home appliances.

Safety critical system is one whose incorrect functioning may have very serious consequences.To insure multicast authenticated and confidential information dissemination, this paper presents an efficient authenticated and confidential multicast key exchange and real time information dissemination scheme based on multi receiver signcryption using elliptic curve. It provides security features like confidentiality, integrity, unforgeability and verifiability. It is resources efficient and attractive for secure multicast communication in smart grid.

2. RELATED WORK

Smart grid security attracted research community and organization including IEEE, NIST and North American Electrical Reliability Corporation-Critical Infrastructure Protection etc [1]. *Liu et al.* [2] proposed key management schemes for unicast, multicast and broadcast, modes for AMI system based on the key graph. Key refreshing policies with inbound in the computational resources are designed. However Wan et al [3] shows that this scheme is vulnerable to *de-synchronization attack* a type of DoS attack can cause interruption of communication and lack of scalability. They proposed Scalable Key Management (SKM) using identity-based cryptosystem and key tree. *Fouda et al.* [4] proposed a hash-based authentication and session key exchange scheme based on the Diffie–Hellman (DH) key exchange protocol between home area network and building area network gateways. Due to DH protocol, the scheme is inefficient and vulnerable to man-in-the-middle attack. Xia and Wang [5] found vulnerability to the man-in-the-middle attack in the scheme

* **Corresponding Author:** Nizamuddin, Department of Information Technology, Hazara University Mansehra, Pakistan
sahibzadanizam@yahoo.com,

of Wu-Zhou and proposed a key management protocol based on the Needham-Schroeder protocol. Both the schemes do not support frequently used secure multicast communication in smart grid. Zhang and Gunter[6] proposed and design an abstract multicast application-aware model for secure multicast groups communication that derives group memberships and verifies configuration and a prototype system Secure SCL is implemented. Mahmoud et al [7] proposed scalable public key infrastructure scheme for smart grid communication using multiple hashing operation. Yaghmaee and Hassani [8] presented unicast and broadcast key management scheme based on elliptic curve. The limitation is that it requires a secure channel to distribute secret parameters between operation and control center and smart meters.

3. Smart Grid System Model

National Institute of Standards and Technology (NIST) the conceptual model of smart grid infrastructure as a set of seven domains [9]: Power Generation, Transmission, Distribution, Customer, Operation & Control, Market and Service Provider system. Each domain is further comprises of heterogeneous entities include organizations, buildings, individuals, systems, system resources etc.

Power generation domain generates electricity from other resources such as renewable variable (solar, wind), renewable Non-variable (hydro, biomass, geothermal, pump storage) and Non-Renewable Non-Variable (gas, coal, nuclear) etc and provide to transmission domain. It shares information and control interfaces with the operations and markets.

Transmission is responsible for bulk electrical power transfer from power generation sources through multiple substations to Distribution, operated by Transmission-owning utility, Regional Transmission Operator or Independent System Operator. It is primarily responsible for maintaining stability on the electric grid by balancing supply with demand across the transmission network.

Distribution domain is responsible for electrical interconnection between the Transmission and Customer domain in a hierarchical way. It may also contain distributed energy resources such as electrical storage or peaking generation units.

Markets domain is responsible for grid virtual and physical (shares, equipments etc) assets buying, selling and defining future requirement of smart grid.

Service domain provides services to support the business processes of smart grid. From low-level utility services such as billing and customer accounts management to high level customer services such as energy management usage and home renewable variable energy generation. It creates innovative products and services to meet the customer requirements and create opportunities for economic growth.

Operations domain is responsible for the smooth operation of the smart grid. It performs monitoring, control, fault management, reporting and statistics, network management, operation planning, maintenance and construction, extension planning and customer support of smart grid.

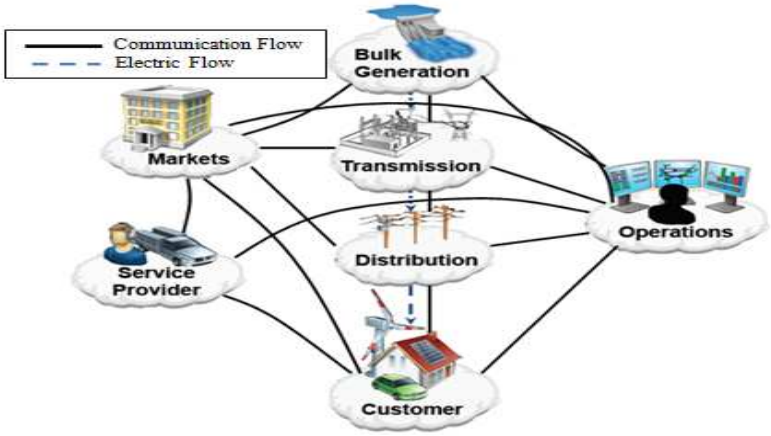

Figure 1.1 Smart Grids Conceptual Model

4. Multicast in Smart Grid

Smart Grid has hierarchical structure and has a natural multicast communication flow as depicted in figure 1.2. It plays an important role in smart grid applications as wide area protection, Demand-Response,

Operation & Control and In-Substation Protection etc.

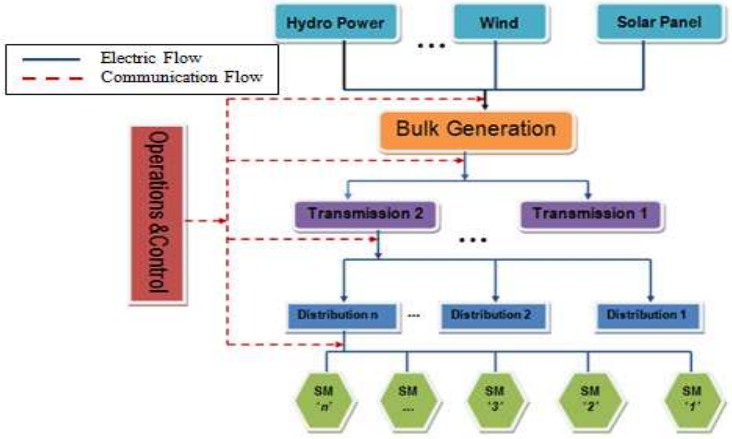

Figure 1.2 Multicast Communication Flow

4.1. **Wide Area Protection**

Unexpected loss of power generators, fault in transmission line or load, caused the well-known blackouts such as northeast blackout of 2003 in USA, India blackout July 2012, Bangladesh blackout November 2014 and Pakistan blackout 2015 effected 55, 620, 150 and 140 million people respectively. PMUs measure and multicast system parameters (current, voltage) at precisely synchronized time to the control centers. It detects problems like electricity frequency from received data and issue control commands to close or open appropriate switches and prevent large-area blackout.

4.2**. Demand-Response**

Peak period energy consumption; can be tackled as temporarily turn off nonessential appliances and reduce power consumption. Utility companies preferred multicast alerts and resultant power reductions avoid building an additional power plant.

4.3**. Operation and Control**

In case of emergency, when power grid cannot supply all consumer loads, the control center multicasts emergency shutdown messages through the Supervisory Control and Data Acquisition (SCADA) system to a fraction of substations to disconnect less-important consumers instead of disconnecting a high-load transmission line, which avoid large-area blackout and revenue loss.

4.4**. In-Substation Protection**

Dissemination of time-critical messages like fault alerts multicast are used In-substation, if detect a fault across substation LANs to the appropriate circuit breakers to disconnect the faulty circuits. Multicast protocol such as link layer multicast protocol is designed in IEC61850 [1].

5. Proposed Scheme

Proposed scheme consists of five phases; Initialization, Public keys generation and distribution, Multicast session key distribution, Secure multicast instant message dissemination, and Key updates.

5.1. **Initialization**

In this phase the system security parameters presented in Table 1 are generated and distributed.

Table 1 Notation Guide

Notation	Description
Q	a large prime of order $q > 2^{160}$
$\mathbb{E}$	An elliptic curve $\mathbb{E}: y^2 = x^3 + ax + b$ and $4a^3 + 27b^2 \neq 0$
N	large prime number of order $n > 2^{160}$
G	a base point on elliptic curve $\mathbb{E}$ over F_q

h/h_k	One way Hash function/keyed one way hash function
$E_k(.)\|D_k(.)$	Symmetric encryption/decryption algorithm (AES) using key k
i	Number of multicast message receivers in Smart Grid
m/c	Message/Ciphertext
$\perp$	Reject

5.2**. Key Generation Phase**

Originator (Operation and control center) randomly generates private key $d_{cs} \in \{1,2,\dots n-1\}$ and computes public key $P_{cs} = d_{cs}.G$. Each entity in the smart grid such as power generators, distribution actors, transmission actors and customer randomly generates private keys $d_{mr_i} \in \{1,2,\dots n-1\}$ and compute public keys $P_{mr_i} = d_{mr_i}.G$. Each entity obtain certificate of public key from certificate authority and announce public key.

5.3**. Multicast Session Key Establishment Phase**

Operation and control center establish multicast session key with different group members for critical message m and confidential communication with multicast group members having identities $\{ID_1, ID_2, \dots ID_t\}$ using probabilistic *algorithm 1*.

Algorithm 1. Multicast Signcryption

Input: $Multicast\ Group\ Member\ List\ \{ID_1, ID_2, \dots ID_t\}, m,\ d_{cs}, P_{mr_1}, P_{mr_2}, \dots, P_{mr_t}$

Output: *Multicast Signcrypted text* Ψ

Procedure

1. *Verify each group member public key* P_{mr_i} *using their certificates*
2. *Randomly generate* $x \in \{1,2,\dots n-1\}$
3. *Randomly generate Multicast Session Key* $M_{sk} \in \{1,2,\dots n-1\}$
4. *Split* x *into* K_e *and* K_h
5. *Computes* $r = h_k\ (M_{sk} \parallel K_h)$
6. *Computes* $c = E_{K_e}(M_{sk})$
7. *For each recipient in the multicast group member*
   a. *Computes* $K_i = x.P_{mr_i}$
   b. *Computes* $K_{e_i} = h(K_i)$
   c. *Generate* $c_i = E_{K_{e_i}}(x)$
   d. $\Omega = (c_1, \dots c_t)$
   e. *Computes* $s = x/(r + d_{cs}) mod\ n$
8. $\Psi = (c, r, s, \Omega)$

Multicast signcrypted text Ψ *to group members*

End

Each receiver in the group gets multicast signcrypted session key Ψ sent by control and operation center verifies the authenticity of its contents and obtain using deterministic *Algorithm 2*

Algorithm 2. Unsigncryption

Input: P_{cs}, d_{mr_i}, Ψ

Output: M_{sk} *or* $\perp$

Procedure

1. *Verify Control and Operation Center public key* P_{cs} *by using his certificate*
2. *Extract* $(c,\ r, s,\ c_k)$ *from* $(c,\ r, s,\ c_1, \dots c_t)$
3. *Computes* $u = s.d_{mr_i}$
4. *Computes* $K_i = u.(P_{cs} + r.G)$
5. *Computes* $K_{e_i} = h(K_i)$
6. *Computes* $x = D_{K_{e_i}}(c_i)$
7. *Split* x *into* K_e *and* K_h *of appropriate length*

8. *Computes* $M_{sk} = D_{K_e}(c)$
9. *Computes* $Y = h_k\,(M_{sk} \parallel K_h)$
10. *Verifies* $Y = r$ *If it is true accept* M_{sk} *else* $\perp$

End

Theorem. The multicast session key establishment is correct if the signcryption/unsigncryption of the equation $x.P_{mr_i} = u.(P_{cs} + \mathrm{r.G})$ holds.

Proof:

$$u.(P_{cs} + \mathrm{r.G}) = \mathrm{s}.d_{mr_i}(d_{cs}.G + \mathrm{r.G}) = \frac{x.d_{mr_i}}{r+d_{cs}}(d_{cs}.G + \mathrm{r.G})$$

$$= \frac{x.d_{mr_i}}{r+d_{cs}} G(d_{cs} + \mathrm{r}) = x.d_{mr_i}.G$$

$$= x.P_{mr_i}$$

The equation established so the multicast key establishment is correct.

5.4. **Secure Multicast Messages Transmission**

Multicast message dissemination is categorized on the basis of certain parameters that highlights the importance of instant messages as depicted in Table 2.

Table 2 Summary of Smart Grid Multicast Communications [10]

Category	Sender	Sender Resources	Allowable Delay	Frequency	Receiver	Receiver Resources
Wide Area Protection	PMU	Limited or moderate	A few ten of *ms*	High (30/s)	Control Center	Sufficient
Demand-Response	Control Center	Sufficient	A few seconds	Low	Home appliance	Limited
Operation And Control	Control Center	Sufficient	Ten or hundred of *ms*	Low	Field Device	Limited or moderate
In-Substation Protection	Protective Relay	Limited or moderate	A few *ms*	Low	Circuit Breaker	Limited

Operation and control center encrypts and computes hash value of the messages using probabilistic Algorithm 3 and multicast to concern members for necessary action.

ALGORITHM 3. Multicast Authenticated encryption

Input: m, M_{sk}
Output C_{ci}
Procedure

1. *Computes* $r = h_{M_{sk1}}(m_{ri})$
2. *Computes* $C_{ci} = E_{M_{sk2}}(m, r)$

Multicast C_{ci} *to MS*

End

Each member in the multicast group receives authenticated encrypted message and obtains the information using deterministic *algorithm 4*.

ALGORITHM 4. Decryption and Verification

Input: m, M_{sk}
Output $m, \perp$
Procedure

1. *Computes* $m, r = D_{M_{sk2}}(C_{ci})$
2. *Computes* $h_{M_{sk1}}(m_{ri})$
3. *Verifies* $h_{M_{sk1}}(m_{ri}) = r$ *If it is true accept* m *else* $\perp$

End

5.5 **Key Update Phase**

Key updating is one of the essential features of the proposed scheme providing renewal of session key for each multicast communication round with assurance of forward and backward secrecy. Proposed scheme updates session key in case a member leaves, joins or a time interval expires using algorithms 1&2.

6. Security Analysis

Our proposed multicast instant message communication protocol ensures the basic security properties of confidentiality, authentication, integrity, unforgeability, non-repudiation and public verifiability under the assumption of ECDLP.

Definition1. (ECDLP): Let G Q be a base point on an $Curve\ C$ and Q be a point on C Find an integer $k \leq n-1$, such that $Q = k.G$.

6.1. **Confidentiality:** Our proposed scheme ensures the multicast session key confidentiality. Whenever an eavesdropper gets multicast signcrypted session key and wants to break confidentiality first must compute the secret key K_{e_i}. To compute K_{e_i} eavesdropper should compute operation and control center privet key d_{cs} from $P_{cs} = d_{cs}.G$ or any multicast group member privet key $d_{mr_i}$from $P_{mr_i} = d_{mr_i}.G$. These both or equivalent to solve computational infeasible hard problem known as ECDLP.

It also ensures multicast message confidentiality when AES cipher is used to encrypt the message, as AES is secure in todays computational resources with key size of 128 so an eavesdropper cannot compute message from multicast encrypted message.

6.2. **Integrity:** It ensures that there have no changes occur during dissemination of message via insecure channel. Our proposed scheme ensures integrity. Operation and control center use collision resistive key hash function. If an attacker, changes ciphertext c to $\acute{c}$ the corresponding message also change from m to $\acute{m}$ and message digest r to $\acute{r}$. It is infeasible for an attacker to change $m \neq \acute{m}$ and $r \neq \acute{r}$.

6.3. **Unforgeability:** Proposed scheme ensures infeasibility for attacker/ legitimate receiver to compute valid signature without knowing secret key. Let an attacker/ legitimate forges valid parameters (m, r, s) to (m', r', s'), requires to compute x from $K_i = x.P_{mr_i}$.

If an evesdropper forges multicast message, should obtain multicast session key firstly which is infeasible as proved in section 6.1.

6.4. **Authenticity:** Proposed scheme assures, received message sent by legitimate sender, each receiver having public key of operation and control center P_{cs} with its certificate issuing by trusted authority, generate session key K_i using P_{cs} $K_i = u.(P_{cs} + r.G)$ and further verify multicast session key using $r = KH(M_{sk} \parallel K_h)$.

6.5. **Non-Repudiation:** In public key infrastructure public key having certificate associated with its private key. Operation and control center can deny from sent multicast key if denies sent messages then any third party can verify the message contents using Zero knowledge protocol. Our proposed scheme provides the property of non-repudiation.

6.6. **Verifiability:** Proposed scheme provides public verifiability property in case of dispute occured between the sender of the message and receiver of the multicast group. Receiver of the message provides parameters (c, c_i, K_i, r) to the third party to verify the contents of the received message, either sent by legitimate sender or other one else.

7. Efficiency Analysis

We analyzed the efficiency of the proposed scheme in multicast key distribution phase and secure multicast instant message dissemination phase.

Secure multicast instant message dissemination phase involve one symmetric encryption and hash on operation and control center and one symmetric decryption and hash function at each receiver which is in range of delay acceptable level in smart grid.

7.1. **Computational Cost**

In key distribution phase proposed scheme have t elliptic curve point multplication 1 moduler inversion 1 hash and t symetric encryption operation on operation and control center while 2 elliptic curve point multplication 1 hash and 1 symetric decryption operation on each member in multicast group.

In Secure Instant Message Dismination phase, proposed scheme has 1 hash and 1 symetric encryption operation on operation and control center while 1 hash and 1 symmetric decryption operation on each member in multicast group.

7.2. **Communication Overhead**

The communication overhead is extra bits appended for security functions while sending data from sender to multi receivers. On the basis of National Institute of Science and Technology (NIST), recommended parameters size communication cost is $|c| = |m|, |c_i| = 128\ bits, |h| = 160\ bits\ and\ \ |n| = 128\ bits$.

In key distribution phase, proposed scheme has $c + t|c_i| + |h| + |n|$ bits in communication cost. While In Secure Instant Message Dismination phase, proposed scheme has $|c| + |h|$ bits in communication cost.

8. Conclusion

This paper presented a multicast key establishment and secure instant and critical message dissemination scheme for multicast communications in the smart grid applications such as various operation and control, wide area protection, demand-response and in-substation protection. Multicast key distribution is based on efficient crypto primitive signcryption using the ECC parameters with small key size. Our proposed novel scheme provides the functionality of confidential and authenticated multicast session key agreement and instant secure message communication. Due to its computation time and communication cost efficiency, our scheme is suitable for secure multicast communication in smart grid.

REFERENCES

[1] A. Mahmood, N. Javaid, and S. Razzaq, "A review of wireless communications for smart grid," *Renew. Sustain. Energy Rev.*, vol. 41, pp. 248–260, 2015.

[2] N. Liu, J. Zhang, Y. He, L. Zhu, and J. Chen, "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid," *IEEE Trans. Ind. Electron.*, vol. 60, no. 10, pp. 4746–4756, 2013.

[3] Z. Wan, G. Wang, Y. Yang, and S. Shi, "SKM: Scalable Key Management for Advanced Metering Infrastructure in Smart Grids," *IEEE Trans. Ind. Electron.*, vol. 0046, no. 12, pp. 1–1, 2014.

[4] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, 2011.

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

[6] J. Z. J. Zhang and C. a. Gunter, "Application-Aware Secure Multicast for Power Grid Communications," *Smart Grid Commun. (SmartGridComm), 2010 First IEEE Int. Conf.*, vol. 6, no. 1, pp. 40–52, 2010.

[7] M. M. E. a Mahmoud, J. Misic, and X. Shen, "A scalable public key infrastructure for smart grid communications," *GLOBECOM - IEEE Glob. Telecommun. Conf.*, pp. 784–789, 2013.

[8] M. H. Yaghmaee, M. Electric, E. Distribution, A. J. Hassani, M. Electric, and E. Distribution, "Secure Key Management Scheme for AMI IN Smart Grid," in *CIRED Workshop*, 2014, pp. 1–5.

[9] U.S. Department of Commerce, *NIST Special Publication 1108r3 NIST Framework and Roadmap for Smart Grid Interoperability NIST Special Publication 1108r3 NIST Framework and Roadmap for Smart Grid Interoperability*. 2014.

[10] Q. Li and G. Cao, "Multicast authentication in the smart grid with one-time signature," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 686–696, 2011.