# A Security Key Recovery System with Channel Quality Awareness for Smart Grid Applications

**Prachya Huadpaknam**[1], **Chaiyod Pirak**[2], and **Rudolf Mathar**[3], Non-members

## ABSTRACT

In this paper, a security key recovery system with channel quality awareness (SKRS-CQA) for smart grid applications has been proposed. Firstly, the proper key recovery agents (KRAs) are determined based on the signal-to-noise ratio (SNR) outage probability. The result of such selection includes the number and the index of selected KRAs. Then, the session key (KS) of a Smart Meter Unit (SMU) will be divided into many different pieces according to the proposed key partitioning algorithm and stored in the selected KRAs for the future key recovery if the data concentrator unit (DCU) has lost the key in unexpected events. The outage probability of SNR, the probability of KRA failure, and the probability of key compromising are also investigated. In addition, a 128-bit AES-GCM encryption algorithm is used in each KRA for authentication and identification mechanisms based on a DLMS/COSEM protocol. As shown in the system performance analysis, the system reliability, the system availability, and the data confidentiality have been improved compared with the conventional scheme. Moreover, a cooperative communication network with an amplify-and-forward relaying protocol and an optimal power allocation has been employed for improving the system reliability. From computer simulation results, it showed that the reliability of the proposed system with a cooperative scheme has been improved significantly.

**Keywords**: Smart Grid, Wireless Sensor Networks, Key Recovery System, Outage Probability, AES-GCM, DLMS/COSEM, Probability of Failure, Cooperative Communication Scheme

## 1. INTRODUCTION

Recently, a smart grid technology has dramatically gained the attention of society in such a way that the power grid has been mobilized by an advanced metering infrastructure (AMI), an advanced communication network, and a mass data management system. The benefits of smart grids include an improvement of efficiency, cost, energy utilization, and reliability of the energy supply chain [1].

One of the essential elements of a smart grid is the advanced communication networks for both trunk and last mile networks. In the last mile network, the wireless communication technology has been widely adopted, such as wireless sensor networks and cellular networks. The wireless sensor network (WSN) is a low cost, low power consumption, and small form-factor communication network. It has been deployed in a variety of application for information exchanging. Despite a wide range of WSN applications, the use of WSN in smart grids has only recently been explored, such as in the SMU and the DCU [2].

**Various** application layer protocols have been compared with regard to their support for smart metering applications. Those protocols are the smart message language (SML), the device language message specification and companion specification for energy metering (DLMS/COSEM), and the manufacturing messages specification (MMS) and simple object access protocol (SOAP) mappings of IEC 61850. The SML protocol was developed as part of the synchronous modular meter project. The DLMS/COSEM forms together an application layer communication protocol and an interface model for metering applications. It does not only support clock synchronization and transmission of measurement profiles, but also includes authentication and confidentiality services based on a symmetric encryption. Additionally, IEC 61850 is a group of standards originally designed for the use in substation automation, and SML is the only protocol that supports the communication of digital signatures. DLMS/COSEM has the advantage over SML in such a way that it is already an international standard. IEC 61850 has the advantage that it can also be used for other smart grid applications besides smart metering. The comparison of SML, DLMS/COSEM, and IEC 61850 has shown that no single protocol is superior in all aspects. Nevertheless, the analysis and comparison of the message size has depicted that DLMS and the MMS IEC 61850 clearly outperform the SML but the DLMS/COSEM TCP payload size in bytes as a function of the num-

Manuscript received on May 10, 2015 ; revised on November 17, 2015.

Final manuscript received on December 8, 2015.

[1,2] The authors are with The Sirindhorn International Thai-German Graduate School of Engineering (TGGS), King Mongkut's University of Technology North Bangkok, Thailand, E-mail: huad65@yahoo.com and chaiyod.p.ce@tggs-bangkok.org

[3] The author is with The author is with Theoretical Information Technology (TI) at RWTH Aachen University, Germany, E-mail: mathar@ti.rwth-aachen.de

ber of measurement values requested has smaller size than the MMS IEC 61850 TCP payload size [3].

The information in the electric grid includes the electricity energy consumption data, the power quality, and the billing information. Therefore, the security issues should be strictly considered as the threats to the electric grid become more critical in the modern smart grid. Cyber security for the system is one of the biggest challenges facing smart grid development; therefore, the highest level of security is crucially needed [4].

Cryptography techniques can solve such security issue. The raw information in the wireless sensor nodes will be encrypted by the appropriate security key in order to prevent data penetration from attackers and reduce the risk of information vulnerability [5]. As the WSN is the resource constraint network, an asymmetric key cryptography is not suitable. The random key pre-distribution scheme based on a symmetric key cryptography is more preferable [6]. The data encryption standard (DES), a Feistel network architecture was once a predominant symmetric-key algorithm but the 56 key bits was too short and vulnerable for the brute force attack. The advanced encryption standard (AES) algorithm has been developed to replace the DES. AES employs a substitution-permutation network (SPN) architecture. The block length of AES is 128 bits, and the key length is selected from 128, 196 and 256 bits. One of the authentication and encryption (AE) algorithms providing both message confidentiality and authenticity is AES-GCM. The Galois/Counter Mode of Operation (GCM) is the latest modes of operation standardized by NIST. GCM uses universal hashing in the finite field *GF(2w)* for generating a message authentication code (MAC). The advantage of using *GF(2w)* is that the computation cost of multiplication under *GF(2w)* is less than integer multiplication. The AES-GCM algorithm achieved higher throughput than other AE modes of operation such as offset code book (OCB), counter with CBC-MAC (CCM) and EAX, a combination of a type of CBC-MAC and CTR mode encryption [7].

In some circumstances, the wireless sensor nodes in the smart grid may lose their decryption key. The owner of the encrypted data would be unable to decrypt its own information. To cope with this problem, the key recovery system (KRS) or key escrow system (KES) could be used to backup a decryption key; therefore, authorized agents are allowed to decrypt the ciphered text with the help of data recovery keys supplied by a trusted third party [8].

A KRS or KES is an encryption system with a backup decryption capability that allows authorized persons, under certain conditions, to obtain the keys needed to decrypt cipher text [8]. A key recovery field (KRF) is created for all KRAs. It contains portions of the $K_S$ for later key recovery. Various methods of key recovery have been developed. In 1993, U.S. government proposed the key escrow cryptosystem called Skipjack that is a symmetric-key cipher algorithm designed by the National Security Agency (NSA). The tamper resistant hardware encryption modules called "Clipper chip" had been used to replace a data encryption standard (DES) chip in the system.

A more advanced chip, Capstone, includes additional cryptographic components for authentication and integrity checking. The Clipper chip was used for real-time encryption in telephones, but the Capstone chip can encrypt an e-mail and produce digital signatures. In 1994, Federal Information Processing Standard (FIPS) announced the standard for Escrowed Encryption Standard (EES).

In August 1994, a commercial KES was released to address the objection to Clipper by not sacrificing the government's law enforcement interests. The design employs a data recovery center (DRC) established by a commercial entity. Every time the escrow encrypt program encrypts a file or message, it would add a data recovery field (DRF) that contains the KS and user's identity encrypted in the DRC's public key and the DRC's public identifier. There are three main components in an KES: user security component (USC), key escrow component (KEC), and data recovery center (DRC). In 1997, Trusted Information Systems (TIS) updated the term of key escrow with key recovery. The only different component between KRS and KES is a recovery agent component (RAC).

In [8], Leighton and Micali proposed key escrow with key agreement. Kilian and Leighton failsafe key escrow, which are user's keys, are generated jointly by the user and key escrow agents so that the user cannot avoid the key escrow such that any two users can find a shared secret key from their own private key and the identifier of the other. Micali and Sidney resilient Clipper-like key escrow allows keys to be split so that the key recovery is possible even if some of the escrow agents compromise or fail to produce their key components.

RSA Secure provides data recovery through an escrowed master public key, which can be split among up to eight trustees using a threshold scheme. Shamir partial key escrow proposed to escrow all but 48 bits of a long (256-bit) key. For threshold decryption, a secret key can be shared by a group of escrow agents through collaboration of the agents. Therefore, information can be decrypted without the agents releasing their individual key components. A key recovery field (KRF) is created for all KRAs. It contains portions of the $K_S$ for later key recovery. Multi-agent KRS (M-KRS) requires the collaboration of at least two KRAs that can provide services with or without the need of KRC [9]. *SHAM-KRS*: a simple high-availability multiple-agent KRS has been proposed in [10]. This system can avoid the problem of single point of failure of KRA. *HADM-KRS* (V1,V2): a high-availability decentralized multi agent KRS was later proposed without the need of KRC [11]. They used simple and flexible principles of the secure $K_S$ management with an appropriate design of key recovery function and the new format of KRF. At last, the number of participating KRAs can be specified by HADM-KRS V2 for successful session of key recovery.

Nevertheless, the reliability is still questionable. Their KRS relied on the collaboration of KRAs, the flexibility to manage the number of KRAs, the high secrecy of the KS, and the ability to detect the counterfeit KRAs. When some KRA in the group are unable to recover a portion of the $K_S$ , the next neighbor is assigned to recover the key. The disadvantage of those KRS is the variation of the WSN communication environment, the wireless channel can cause fading signals among those senders, KRAs, and a receiver. The selection algorithm for the KRAs has not been mentioned. In addition, the existing HADM-KRS also assumed that the probability of KRA failure is fixed at 5% [11], which is not quite general. In order to improve a reliability of sensor node's connectivity, the channel quality and the SNR outage probability must be considered jointly with the probability of KRA failure and the probability of key compromising. However, there is a lack of thorough investigation on the KRA selection process considering the time-varying wireless channel of WSN. In addition, an extensive performance analysis has to be explored. The contributions of this paper are as follows.

A KRA selection algorithm has been proposed that takes into account the effect of a SNR outage probability and a probability of KRA failure in different channel conditions. In addition, an algorithm to split the key, rearrange the key into sub group, and recover the complete $K_S$ has also been proposed. A probability of key compromising in the performance analysis has been considered for evaluating the level of confidentiality of the proposed algorithm. In addition, a cooperative communication network with an amplify-and-forward relaying protocol and an optimal power allocation [12] has been adopted for improving the system reliability. It can illustrate that the KRS reliability of the proposed algorithm can be improved in such a way that the probability of KRA failure is drastically reduced compared with an existing KRS algorithm, especially in the wireless channel environment.

This paper is organized as follows. In section 2, the system model is described. In section 3, the SKRS-CQA, the received signal model, the relationship between a SNR and an outage probability, the proposed algorithm of KRAs selection, the proposed key partition methodology, and the process of key recovery are proposed and described. In section 4, The performance analysis such as the probability of KRA failure, the probability of key compromising, is investigated and the performance enhancement with a cooperative communication scheme is discussed in section 5. A computer simulation has been used for examining the system reliability, the system availability, and the system confidentiality of the proposed framework. A cooperative scheme has been compared with the conventional scheme in section 6. Finally, we conclude the paper in section 7.

## 2. SYSTEM MODEL

In this section, the system model of a SKRS-CQA for smart grid applications is considered.

### 2.1 SKRS-CQA model

The proposed system model of the SKRS-CQA for smart grid applications is depicted in Fig.1.

In Fig.1, we investigate a basic last mile communication in smart grids where the ZigBee network, representing the WSN [13], is employed to bridge a desired smart meter unit (SMU) and a data concentrator unit (DCU). The other SMUs will act as KRAs used for key recovery process. In addition, a Key Distribution Center (KDC) is employed to incorporate the SMU, DCU, and KRAs in the pre-key distributed process.

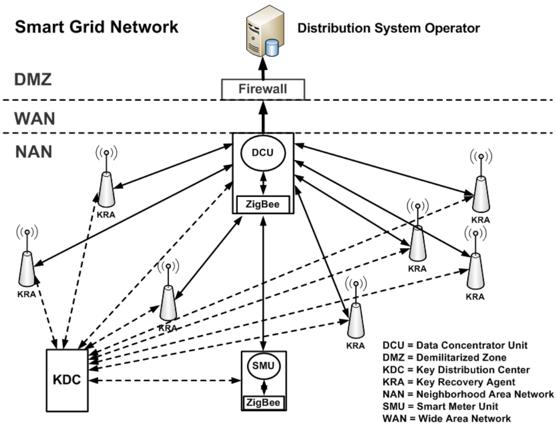

***Fig.1:*** *A system model of the SKRS-CQA for smart grid applications.*

The SMU acts as a sender to send a cipher text message to the DCU who receives and decrypts the encrypted data by the $K_S$ by means of cryptographic mechanism over a public key infrastructure (PKI) together with the AES-GCM encryption algorithm [14, 15, 16]. In a normal situation, the DCU can perform the successful $K_S$ decryption under their PKI agreement. Unfortunately, in some situations, if the DCU loses its private key, or the SMU's messages have been encrypted by the DCU's expired public key (masquerading attacks) or by the law enforcement (LE), then the $K_S$ cannot be obtained from the thriving decryption. By this reason, the DCU or a law enforcement agency should recover the $K_S$ back from a group of selected KRAs, which carry some parts of the pre-distributed $K_S$.

### 2.2 Basic requirements of the proposed SKRS-CQA

Basic requirements of the proposed SKRS-CQA are listed as follows:

1. The key recovery process should be done under the authority of end users or a security policy of an organization. In this circumstance, the binding problem is not an issue. Thus, a law enforcement access field (LEAF) is not included in an encapsulated Key Recovery Field (KRF) in communication messages.

2. The key recovery process is limited to the $K_S$ used for decrypting the encrypted data. Thus, we can use the key encapsulation technique due to the smaller size of the $K_S$ comparing with the data package size.

3. The key recovery protocol is executed within a conventional PKI at the beginning of the communication process inside the key recovery group. Thus, we assume that the SMU, DCU, and all KRAs in our purposed system are distributed securely and issued under the PKI environment. It contains a public key and information for identification and authentication. Each KRA can use a trust model based on a Gateway Certificate Authority (GWCA) [17, 18], that is designed to allow a certification to other different kinds of certificate authority (CA) located anywhere in the global trusted network. The public keys and the certificate of each KRA are issued by the KDC.

4. The key recovery system will be investigated under Rayleigh flat-fading wireless channel environment [12].

## 3. THE PROPOSED SKRS-CQA FOR SMART GRID APPLICATIONS

The proposed SKRS-CQA consists of a security domain, as shown in Fig. 2. The key recovery mechanism only provides services to restrictedly identified clients within the security domain in order to ensure a top security policy. The KDC will act as a certificate authority where the public key and $K_S$ will be issued, and the service requested from an individual user will be checked for the access right. If an authenticated user meets all prescribed conditions, the KDC can issue access permission as requested by the user. The SMU will provide the energy consumption data for home or businesses and automatically deliver to the utility company for data processing.

The SMU also provides the utility company with greater information about how much the total electricity is being consumed throughout their service areas. In the proposed system, the SMU uses ZigBee as the wireless sensor network for communication with the smart grid network. The encrypted information will be exchanged between the SMU and the DCU back to the grid. Moreover, the SMU will generate the KRF for recovering purposes from its own public key and information from the selected KRAs. The DCU will collect a $K_S$ or an encrypted data from the SMUs within their network, decrypt, and forward these information to the smart grid network. In case of law enforcement or key lost, the DCU will use some parts of information from the selected KRAs to recover the key or encrypted data. KRAs are the other SMUs that do not exchange information with the DCU at the same time. Some parts of the key from the desired SMU will be split and encrypted in a form of KRF, and they are securely kept here. If the channel quality between the KRA and the DCU is higher than the predetermined threshold, then such KRA will be selected for the cooperative recovery function. A government agency or law enforcement is the official representative who wants to discover the key. At some situation, the $K_S$ may be lost due to disaster or law enforcement. The DCU will not be able to decrypt the key as usual. The key recovery process will offer the best solution for solving this problem, which will be presented as follows.

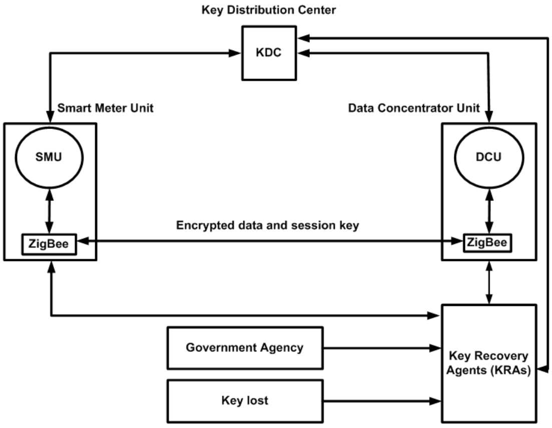

***Fig.2:*** *A security domain of the proposed SKRS-CQA.*

1. Initialization phase: To increase the degree of confidentiality [19], the public keys of all agents and information for identification and authentication are distributed after certificates for agents have been issued by an authorized KDC, as shown in Fig. 3.

2. Communication and KRF composition phase: The DCU secretly chooses a group of KRAs among a pool of KRAs according to our proposed KRAs selection algorithm, see also section 3.2. The desired SMU generates the KRF by using its private key, a $K_S$ obtained from the KDC, in which such a key will be divided into N pieces at the SMU in agreement with the chosen KRAs information from the DCU. Then, the KRF is composed and encapsulated within a communication message, which will be discussed later in section 3.3. Then, the encrypted message is sent to the DCU.

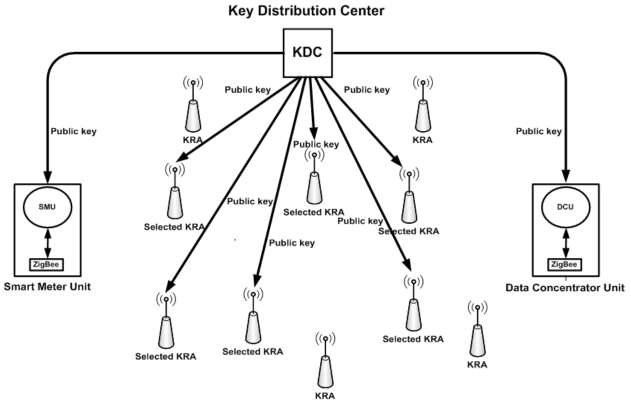

*Fig.3:* *A KDC sends certificate and public key to the SMU, DCU, and all selected KRAs.*

The DCU will remove the encapsulated message with its private key, and decrypts the $K_S$ from the KRF for a $K_S$ recovery. However, the DCU may not have the ability to decrypt the KRF and the cipher text message if it has lost the private key, or the message has been encrypted by its expired public key, or even if the security team of the organization has founded that some SMUs violated the security policy of the organization (or government). Then, they will not allow the DCU to reveal the encrypted message.

3. Key recovery phase: The DCU or a law enforced third party, who has the privilege to recover the encrypted message requests a partition key in a form of KRF1-KRFN from the selected KRAs, as shown in Fig. 4. Then, the DCU extracts the $KRF_1$-$KRF_N$ to get the partition key, and combines them to fulfill the complete KRF for a $K_S$ decryption. Furthermore, these pieces of $K_S$ will be reassembled again at the DCU for the key recovery process. In section 3.4, the $K_S$ recovery will be described in details.

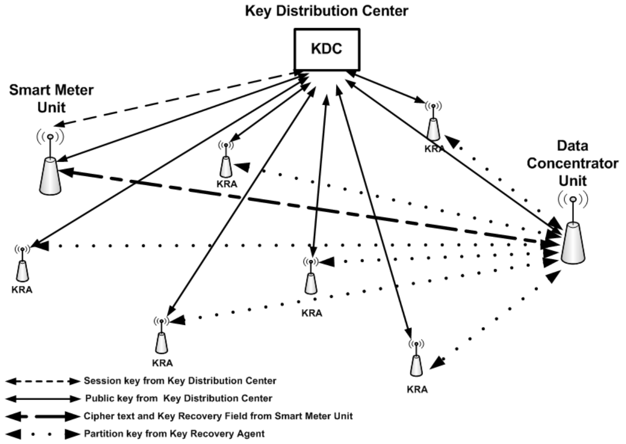
Key Distribution Center
KDC
Smart Meter Unit
Data Concentrator Unit
KRA
KRA
KRA
KRA
KRA
KRA
Session key from Key Distribution Center
Public key from Key Distribution Center
Cipher text and Key Recovery Field from Smart Meter Unit
Partition key from Key Recovery Agent

*Fig.4:* *A key recovery process under PKI environment.*

### 3.1 Received signal model

Before selecting the proper KRAs for key recovery process, the availability of KRAs in the session group must be deliberately examined [18]. At the beginning of the process, we assume that all KRAs in the group are able to send the pilot signal to the receiver (i.e., the DCU in this case); therefore, the DCU will be able to qualify the channel quality through the signal to noise ratio (SNR) outage probability of each KRA. The received signal model [12] at the DCU transmitted from each KRA could be expressed as,

$$y = \sqrt{P}hx + w \tag{1}$$

where $P$ is the transmitted power of KRA, $x$ is the pilot symbol, $h$ is the channel coefficients from the KRA to the DCU, which is modeled as a zero-mean, complex Gaussian random variable with variance $\sigma^2$, and w is an additive AWGN noise, which is modeled as a zero-mean, complex Gaussian random variable with variance $N_o$. The expression of the signal to noise ratio [12] could be readily expressed as

$$SNR = \frac{P\sigma^2}{N_o} \tag{2}$$

The outage probability is defined by considering the event that the received SNR at the DCU for each KRA is below a specific SNR threshold $\gamma_{\text{th}}$. From [12], the outage probability can be described by

$$P_{out} = 1 - e^{\frac{-\gamma_{th} N_o}{P\sigma^2}} \tag{3}$$

where $P_{out}$ is the outage probability of KRA, $P$ is the transmitted power of KRA, $\sigma^2$ is a channel variances, $\gamma_{\text{th}}$ is a specific SNR threshold, and $N_o$ is a noise variance modeled as a complex Gaussian random variable.

### 3.2 KRAs authentication and selection processes

The KRAs selection process begins when the SMU (sender) wants to send data to the DCU (receiver). The SMU will request a certificate, a group identification (GID) and an authentication from the KDC in order to get $K_S$ under the PKI environment. Next, the DCU will command all KRAs in the group for their pilot signal transmission, authentication and identification. The KDC will then acknowledge such request, and then start the PKI process for authentication and identification, and send the $K_S$ to the SMU for key recovery field (KRF) composition. Simultaneously, each KRA in the recovery group will send the channel state information (CSI) with its identity to the requesting DCU. The KRA authentication and selection process is shown in Fig.5.

The DCU will evaluate the authentication and identification from each KRA. If the authentication and identification are passed, the SNR outage probability ($P_{out}$) of each KRA will be calculated. Consequently, the DCU chooses at least M out of N KRAs when $P_{out} < \beta_0$, where $\beta_0$ is the outage probability threshold according to predetermined SNR threshold $\gamma_{th}$, M is the minimum number of KRAs that will be used to complete the key recovery i.e., $M \geq 2$, and N is the total number of KRAs in the recovery group that are ready to perform the key recovery process, as shown in Fig. 5.

It is worth noticing that N must be greater than or equal to two in order to avoid the highest probability of key compromising. We can define the number of failed KRAs as K. Hence, the receiver could not recover the key when K > M+1.

### 3.3 The key splitting, key recovery field generation, and key partitioning processes

The key recovery preparation steps are as follows.

1. The SMU splits $K_S$ into N parts according to the number of selected KRAs from the KRA authentication and selection processes, as shown in Fig. 6. Next, the secret sharing [10] will be used to split $K_S$ into N parts of $K_{Si}$'s (i = 1, 2, 3,…, N), which are equal to the number of participating KRAs.

2. The KRF generation and encapsulation processes will be performed to construct a key recovery field $KRF_i$ for each selected KRA [12]. Essentially, $KRF_i$ consists of a part of splitting session key ($K_{Si}$), a group identification (GID), an agent secret number ($ASN_i$), and some other information, as shown in Fig. 7. Furthermore, the encapsulation procedure will be performed by the KRF encryption with the public key ($Pbag_i$) of $KRA_i$. The encapsulated $KRF_i$ is illustrated as $Pbag_i$ [$KRF_i$] = $Pbag_i$ [$K_{Si}$ || GID || $ASN_i$'s||other information].

The KRF is then sent together with the message that has been encapsulated with the ($K_s$[Msg]) to the DCU. Given N being the total number of selected KRAs and M being the number of qualified KRAs at the key recovery moment, the key recovery field, i.e. $KRF_1$,…, $KRF_N$,

which are generated at the SMU for the selected KRAs, must consist of at least R = N-M+1 parts of each key in order to avoid key compromising. In Fig.8, for example, it shows that the first part, i.e. $KRF_1$, serves as a fixed base part which is a non-overlapping key part with respect to other KRAs, and other N-M parts are overlapping key parts. One can see that the minimum number of qualified KRAs M, which will be used to complete the key recovery, should follows M = N-R+1.

3. As shown in Fig.9, where N=6, M=3, and R=4, the key recovery process at the DCU will combine the fixed base parts of the KRFs, i.e. 4th, 5th, and 6th parts, and the remaining parts of the KRF, i.e. 1st, 2nd, and 3rd, from the qualified KRAs to complete a key assembly. Therefore, after a proper key-part ar-

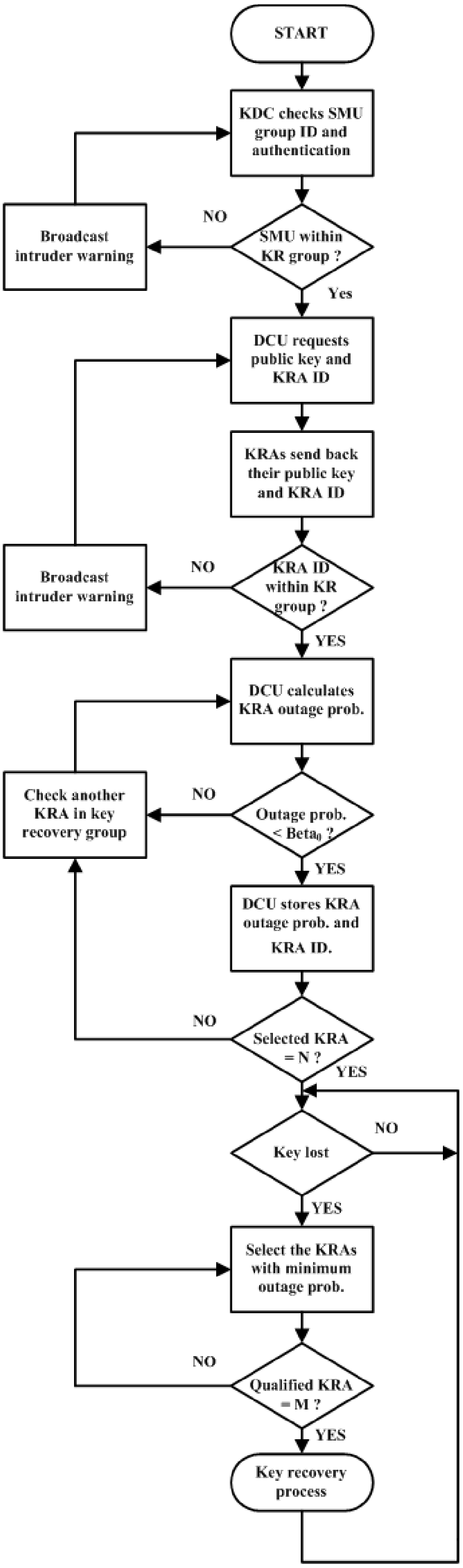
START
KDC checks SMU group ID and authentication
NO
Broadcast intruder warning
SMU within KR group ?
Yes
DCU requests public key and KRA ID
KRAs send back their public key and KRA ID
NO
Broadcast intruder warning
KRA ID within KR group ?
YES
DCU calculates KRA outage prob.
Check another KRA in key recovery group
NO
Outage prob. < Beta0 ?
YES
DCU stores KRA outage prob. and KRA ID.
NO
Selected KRA = N ?
YES
NO
Key lost
YES
Select the KRAs with minimum outage prob.
NO
Qualified KRA = M ?
YES
Key recovery process

***Fig.5:*** *The proposed KRA authentication and selection processes.*

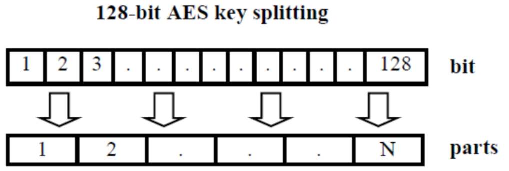

***Fig.6:*** *An 128-bit AES session key splitting.*

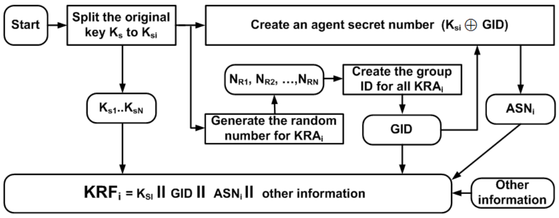
Start
Split the original key $K_s$ to $K_{si}$
Create an agent secret number ($K_{si} \oplus$ GID)
$N_{R1}, N_{R2}, \ldots, N_{RN}$
Create the group ID for all $KRA_i$
$K_{s1}..K_{sN}$
Generate the random number for $KRA_i$
GID
$ASN_i$
$KRF_i = K_{Si}$ II GID II $ASN_i$ II other information
Other information

***Fig.7:*** *A key recovery field generation for the qualified KRAs.*

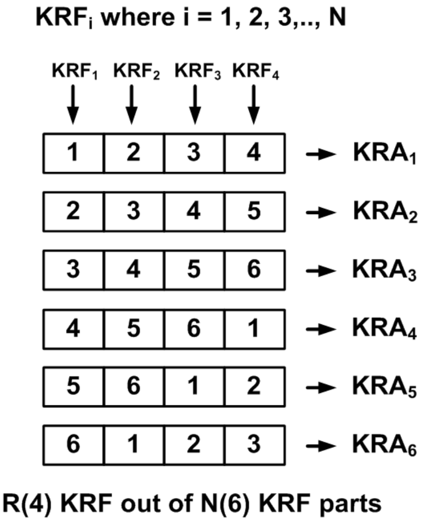

***Fig.8:*** *A key recovery field partitioning methodology.*

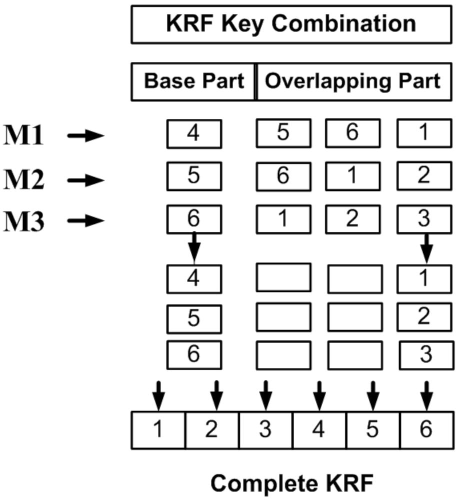

***Fig.9:*** *A key recovery field combining.*

rangement, the complete key recovery field combining could be achieved.

### 3.4 The key recovery process

The $K_S$ can then be recovered by combining all $K_{Si}$ by the exclusive-OR operation from $KRF_1$ - $KRF_N$. This step can strengthen the security of the system, and it can always securely recover $K_S$ through the concept of secret sharing to circumvent the collusion of unfaithful KRAs.

In Fig. 10, a session key recovery process starts by KRF extraction at the DCU for getting all encrypted partial KRFi. For a partial $K_S$ recovery at each $KRA_i$, $Pbag_i[KRF_i i]$ is sent to $KRA_i$, where i = 1,. . ., N. $KRA_i$ decrypts $Pbag_i[KRF_i]$ with its private key ($Pvag_i$) to get $KRF_i$, and reveals $K_{Si}$, GID, and other information. $KRA_i$ verifies GID and the public key certificate of the DCU.

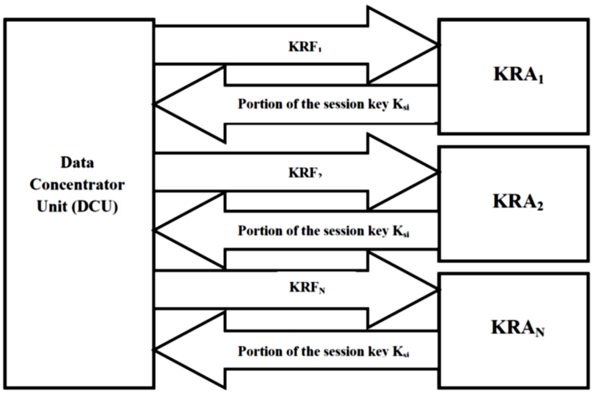
Data Concentrator Unit (DCU)
$KRF_1$
Portion of the session key $K_{si}$
$KRA_1$
$KRF_2$
Portion of the session key $K_{si}$
$KRA_2$
$KRF_N$
Portion of the session kev $K_{si}$
$KRA_N$

***Fig.10:*** *A DCU session key recovery process from KRFs.*

$KRA_i$ will encrypt $K_{Si}$ and GID with the public key of the DCU (Pbreq). Then, $KRA_i$ sends $Pb_{req}[KS||GID]$ to the DCU for the compilation and construction of $K_{Si}$. In case of some KRAs are out of service, all $K_{Si}$ cannot be collected. In this case, the DCU will collect the lost portions of the $K_S$ from the associated active KRAs. As a medium security case, the DCU calculates the lost $K_S$ by adopting $ASN_i$ of $KRA_i$. Each $K_{Si}$ is then re-calculated as $K_{Si} = ASN_i \oplus$ GID. Upon completing the collection of all $K_{Si}$, the DCU can now construct $K_S$.

For a full $K_S$ recovery, the $K_S$ could be reconstructed by the DCU, in which the DCU can decrypt $Pb_{req}[K_{Si} ||GID]$ with its private key ($Pv_{req}$) in order to obtain $K_{Si}$ and GID. In addition, $K_{Si}$ of $KRA_i$ could be verified by using GID. Therefore, $K_S$ is completely calculated as $K_S = K_{S1} \oplus K_{S2} \oplus \ldots \oplus K_{SN}$. This process is illustrated in Fig.11.

For a better understanding (see also Fig.8 and 9), a case of N = 6 and R = 4, which is chosen to avoid a low probability of key compromising, is considered. In this case, the SMU will divide the 128-bit key AES

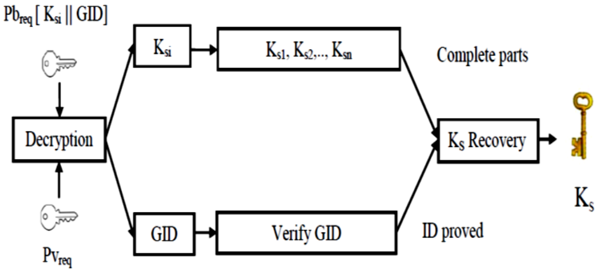

***Fig.11:*** *A session key recovery.*

into 6 parts. The minimum number of KRAs to recover the key is M = N-R+1, i.e. (6-4) + 1= 3. Assuming that KRA$_4$, KRA$_5$, KRA$_6$ are the candidate for M1, M2, M3 KRAs, respectively, where the outage probability is below the threshold $\beta_0$, one can see that a part number 4, 5, 6, and 1 are in KRA$_4$; a part number 5, 6, 1, and 2 are in KRA$_5$; and a part number 6, 1, 2, and 3 are in KRA$_6$. The base part numbers, which are 4, 5, and 6, are already there but the remaining part numbers, which are 1, 2, and 3, are needed from the overlapping parts. By skipping the repeated part number and concatenating a round key, we will accomplish the 6 completed part numbers of the 128-bit AES key, that is, the part number 4, 5, and 6 from the base part numbers, the part number 1 from KRA$_4$, the part number 2 from KRA$_5$, the part number 3 from KRA$_6$, and joined them together for completing the full KRF at the DCU.

## 4. THE PERFORMANCE ANALYSIS

In this section, the performance of the proposed KRS system, including the system's reliability, system availability, data confidentiality, and probability of key compromising will be discussed.

### 4.1 Probability of KRA failure

We determine the reliability of the KRS system from the probability of KRA failure in the same key recovery group. As a reference, the predecessor research, i.e., SHAM-KRS, HADM-KRS (V1, V2), defined the ability of their system to be continuously operating without failure at 95% [10]. By this analysis, we use a binomial distribution method to analyze the probability of KRA failure from its outage probability [23]. This will evaluate the reliability of the system for key recovery service. In this paper, we assume that the key recovery system has N KRAs. Let t being the probability of the individual KRA failure, q being the probability of succeed KRA which is equal to 1-t, K being the number of concurrently failed agents in the same group, where K can be 0,1,2,3,. . .,N, and N denotes the number of KRAs, where N $\geq$ 2. We can show that the probability of KRA failure is derived by [21]

$$P_f(K) = \frac{N!}{K!(N-K)!} t^K q^{N-K} \tag{4}$$

The probability of KRA failure: $P_f$(K) depends on the total number of key recovery agent N, and the failed agent K in the same group. We evaluate the reliability of the system by two cases;

Case 1. The reliability of KRS without KRA failure.

$$R = Pf(K=0) * 100 \tag{5}$$

where R is KRS reliability and P$f$(K=0) is the probability of KRA failure when K = 0.

Case 2. The reliability of KRS with some KRA failure, where R' is KRS reliability and P$f$(K=N-2) is the probability of KRA failure, when K=N-2. The equation is expressed as follows.

$$R' = \{1 - Pf(K=N-2)\} * 100 \tag{6}$$

It is worth noticing that the concurrently failed KRAs K should be less than or equal to R, i.e. K $\leq$ M-N+1, in order to ensure a full key recovery capability of the proposed KRS system.

### 4.2 System Availability

recovery services offered by KRS must be available when it is needed. In addition, the system availability is the property that legitimate principals are able to access a service within a timely manner whenever they may need. Let A$'$ being the system availability, and F$'$ being the ratio of failure KRA to a unit time of the KRS, we could describe the KRS system failure as follows [10]. Given K = 1, 2,. . ., 4, the KRS system failure with KRA failure is expressed as

$$F' = \frac{1}{P(N-2)} \tag{7}$$

The KRS system availability with KRA failure is expressed as

$$A' = \frac{F'}{F' + (\frac{1}{p})} \tag{8}$$

where $p$ is the average of the maximum acceptable repair rate [10].The KRS system failure without KRA failure is expressed as

$$F = \frac{1}{1 - P(N-2)} \tag{9}$$

and the KRS system availability without KRA failure is expressed as

$$A = \frac{F}{F + (\frac{1}{p})} \tag{10}$$

### 4.3 Confidentiality

To make sure that only authorized sensor nodes can obtain the content of messages, the original sensing data and the intermediate aggregation results should not be disclosed to the unauthorized parties during the transmission process [19]. Data or key encryption is a technology used to ensure confidentiality of information by transforming it in a way that it is incomprehensible to everyone, except to those it was intended. PKI infrastructure is used together with 128-bit AES-GCM for our cryptography. At the initial phase, the PKI mechanism starts the authentication and the identification by using a set of public and private keys and certificate trust. After verification, AES-GCM is being used for $\mathrm{K_S}$ encapsulation. We have the KRF that encapsulated a $\mathrm{K_S}$, a group identification (GID), an agent secret number ($\mathrm{ASN}_i$) for the key recovery process. The isolation is made by the forgery agent from the group member. The possible key combination of 128-bit AES-GCM could strengthen our confidentiality to prevent breaking the key by hackers.

### 4.4 Probability of key compromising

It is worth noticing that a more number of key parts stored in each KRA, a higher risk the KRA being successfully hacked by an attacker. Hence, the probability of key compromising ($Pc$) is able to fairly indicate the vulnerability of the KRA to be intruded, and it could provide an effective performance trade off to the probability of KRA failure $P_f$(K). One can see that the number of key parts stored per KRA is N-M+1. Hence, we can define the probability of key compromising as in [23]

$$Pc = \frac{N-M+1}{N} \tag{11}$$

where $N$ is the total number of KRA in the recovery group, $M$ is the minimum of KRA for key recovery; when $M = N-K+1$, and K is the number of failed agents in the same group.

## 5. PERFORMANCE ENHANCEMENT

After a selection of the proper KRAs that pass our setting threshold for the key recovering process, one can see that N-M KRAs are not selected. In fact, these KRAs could help re-transmitting the messages from the primarily selected KRAs by the mean of cooperative communications [11-13]. The benefit of such communication technique is that the channel diversity gain could be exploited as a virtual number of transmit antenna increased. Therefore, the reliability of the proposed key recovery system will be enhanced. Furthermore, the optimal power allocation could be also employed for an additional performance improvement. By an optimal power allocation strategy, the reliability of the proposed system will be even more improved.

### 5.1 Cooperative communication scheme

In this section, the amplify-and-forward (AF) relaying cooperative communication protocol has been considered for improving the system performance [12]. The protocol operations are as follows, as shown in Fig.12,

- Firstly, the SMU(source) sends information to its destination, and the information is also received by the cooperative KRA (relay) at the same time. It is worth noticing that such cooperative KRA could be obtained by selecting the most-potential unqualified KRA whose probability of outage is the minimum among a group of them.
- Secondly, the KRA(relay) can help the source by amplifying and forwarding the information to the DCU(destination).

In Fig. 12, the signal transmitted from the source $x$ is received at both relay and destination, expressed as

$$y_{s,r} = \sqrt{P_1} h_{s,r} x + w_{s,r} \tag{12}$$

$$y_{r,d} = \sqrt{P_2} h_{r,d} x + w_{r,d} \tag{13}$$

$$y_{s,d} = \sqrt{P_1} h_{s,d} x + w_{s,d} \tag{14}$$

where $h_{s,r}, h_{r,d}$ and $h_{s,d}$ are the channel coefficients between the source, relay and destination, respectively, and are modeled as Rayleigh flat fading channels. The terms $w_{s,r}, w_{r,d}$, and $w_{s,d}$ denote the additive white Gaussian noise with zero-mean and variance $N_0$. The signal-to-noise ratio at the output of the maximum ratio combining (MRC) [24] is equal to the sum of the received signal-to-noise ratios from both branches. With the knowledge of the channel coefficients $h_{s,r}, h_{r,d}$, and $h_{s,d}$, the output of the MRC detector at the destination can be written as,

$$y = a_1 y_{s,d} + a_2 y_{r,d} \tag{15}$$

where a combining factors

$$a_1 = \frac{\sqrt{P_1} h^*_{s,d}}{N_0} \tag{16}$$

$$\text{and} \quad a_2 = \frac{\sqrt{\dfrac{P_1 P_2}{P_1 |h_{s,r}|^2 + N_0}} h^*_{s,r} h^*_{r,d}}{\left( \dfrac{P_2 |h_{r,d}|^2}{P_1 |h_{s,r}|^2 + N_0} + 1 \right) N_0} \tag{17}$$

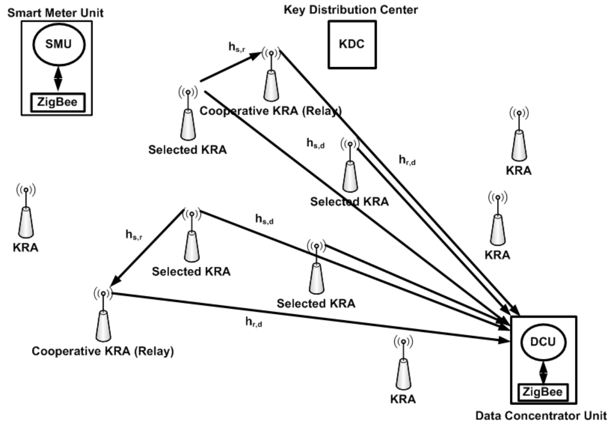

***Fig.12:*** *A cooperative scheme for key recovery system.*

## 5.2 Optimal power allocation

For a fixed total transmitted power $P_1 + P_2 = P$, we are going to optimize $P_1$ and $P_2$ such that the asymptotically tight symbol error rate (SER) approximation is minimized [24]. Equivalently, we try to minimize

$$G(P_1, P_2) = \frac{1}{P_1\delta^2_{s,d}}\left(\frac{1}{P_1\delta^2_{s,r}}\frac{1}{P_2\delta^2_{r,d}}\right) \qquad (18)$$

where G is the channel gain, $\delta^2_{s,d}$, $\delta^2_{s,r}$, and $\delta^2_{r,d}$ are the channel variances of $h_{s,d}$, $h_{s,r}$, and $h_{r,d}$, respectively. Together with the power constraint $P_1 + P_2 = P$, we can solve the above equation and arrive at the following result.

As we can see in Fig. 13 that the optimum ratio of the transmitted power $P1$ at the source over the total power $P$ is less than 1 and larger than 1/2, while the optimum ratio of the power $P2$ used at the relay over the total power $P$ is larger than 0 and less than 1/2. In general, the equal power strategy is not optimum. For example, if $\delta^2_{s,r} = \delta^2_{r,d}$ then the optimal power allocation is

$$P1 = 2/3P \ and \ P2 = 1/3P \qquad (19)$$

In a sufficiently high SNR regime, the optimal power allocation for the AF cooperation systems with either M-PSK or M-QAM modulation is [24]

$$P_1 = \frac{\delta_{s,r} + \sqrt{\delta^2_{s,r} + 8\delta^2_{r,d}}}{3\delta_{s,r}\sqrt{\delta^2_{s,r} + 8\delta^2_{r,d}}}P \qquad (20)$$

and

$$P_2 = \frac{2\delta_{s,r}}{3\delta_{s,r} + \sqrt{\delta^2_{s,r} + 8\delta^2_{r,d}}}P \qquad (21)$$

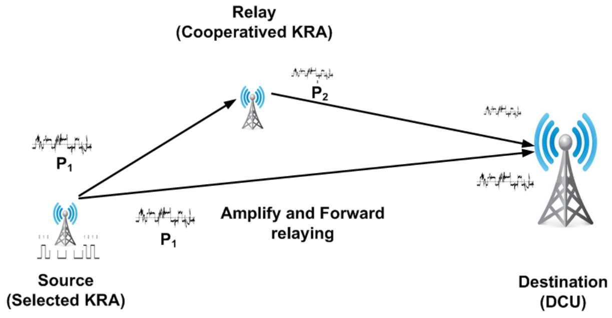

***Fig.13:*** *The cooperative scheme with optimal power allocation SKRS-CQA.*

## 6. SIMULATION RESULTS

In this section, the computer simulation results of the proposed SKRS-CQA for smart grid applications including reliability, availability and confidentiality, will be investigated. In addition, probability of outage, and the probability of KRA failure are examined and compared with the theoretical analysis. We also discuss about the tradeoff between the probability of key compromise and the key secrecy. Moreover, the system enhancement by using cooperative communication scheme will be mentioned.

### 6.1 The implementation parameters

In this section, a DLMS/COSEM protocol with standard 128-bit AES-GCM is adopted [14] for KRA identification and authentication in a wireless-sensor-based. The suitable algorithm for smart grid is a 128-bit Advanced Encrypt Standard Galois Counter Mode (AES-GCM), which operates with our proposed KRA selection algorithm. This is because it offers equivalent security with smaller key sizes, faster computation, lower power consumption, as well as memory and bandwidth savings [15]. GCM is a mode of operation for symmetric key cryptographic block ciphers that has been widely adopted because of its efficiency and performance. GCM throughput rates for state of the art, high speed communication channels can be achieved with reasonable hardware resources.

### 6.2 System reliability with probability of KRA failure

The ability of a system or component to function under stated conditions for a specified period of time or at a specified “moment or interval of time” is described by the system reliability. When the key recovery system uses N = 2, K = 0 meaning that no failed agents, P$f$(0) is about 90%. When N = 6, K = 0, P$f$(0) will be slightly decreased to 73.5%. When we use N = 10, K = 0, P$f$(0) will be slightly decreased to 59.87%.

It means that when the number of key recovery agent N increases and no failed agents, the probability of KRA failure will be slightly decreased. On the contrary, when the number of failed agent increases, the probability of KRA failure will be decreased. However, when the number of key recovery agent increases, at the same number of failed agents, the probability of KRA failure will be increased, as shown in Fig. 14. In conclusion, with some KRA failure, when the number of KRA increases, it will cause the probability of KRA failure gradually increased.

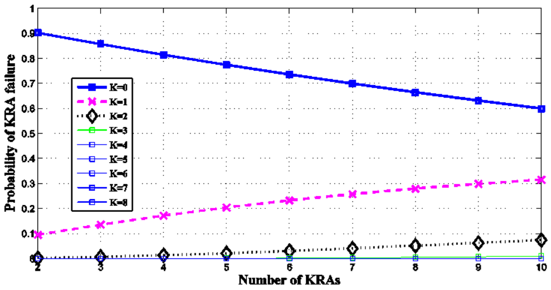

***Fig.14:*** *The probability of key recovery agent failure, for N =10, K= 0,1,2,. . .,8, t = 0.05.*

When the number of N increases, without any failed agents, the probability of KRA failure P$f$(0) will be decreased. On the other hand, when there is one or more failed agents, the probability of KRA failure will be increased, but in a very low value (close to zero).

Our proposed system has the same reliability as the HADM-KRS, as shown in table 1, as we grant some failure of KRA without lost of any portion of the key. When the number of KRA equals 2, the reliability is very low. Furthermore, the reliability increases when the number of KRA increases for the system with some KRA failure; however, for the system with no KRA failure, the reliability decreases when the number of KRA increases.

***Table 1:*** *The reliability comparison between HADM-KRS and the proposed KRS with KRA failure (K = N-2) and KRS without KRA failure (K = 0).*

| Number of KRA (N) | The reliability of HADM-KRS (%) | | The reliability of the proposed KRS (%) | |
|---|---|---|---|---|
| | K = N-2 | K = 0 | K = N-2 | K = 0 |
| 2 | 9.75 | 90.25 | 9.75 | 90.25 |
| 3 | 86.46 | 85.74 | 86.46 | 85.74 |
| 4 | 96.46 | 81.45 | 96.46 | 81.45 |
| 5 | 99.89 | 77.38 | 99.89 | 77.38 |
| 6 | 99.99 | 73.51 | 99.99 | 73.51 |

## 6.3 System Availability

In HADM-KRS, the average of maintenance rate p is fixed to 5% or 0.05 [10] and the system availability could not achieved 100%. However, in our proposed system when we set the value of the outage probability threshold Pth obtained from the channel quality between sender (SMU) and receiver (DCU or KRAs), to be 11% or 0.11, the system availability of 100% could be achieved.

***Table 2:*** *The system availability comparison between HADM-KRS and the proposed KRS with KRA failure (K = N-2) and KRS without KRA failure (K = 0).*

| Number of KRA (N) | The availability of HADM-KRS (%) | | The availability of proposed KRS (%) | |
|---|---|---|---|---|
| | K = N-2 | K = 0 | K = N-2 | K = 0 |
| 2 | 33.90 | 33.90 | 100 | 100 |
| 3 | 26.97 | 25.96 | 100 | 100 |
| 4 | 78.69 | 21.23 | 100 | 100 |
| 5 | 97.79 | 18.10 | 100 | 100 |
| 6 | 99.83 | 15.88 | 100 | 100 |

## 6.4 Data Confidentiality

There is also a physical argument that a 128-bit symmetric key is computationally secure against brute-force attack. For a faster supercomputer, a number of years to crack AES with 128-bit Key, shown in table 3, is $(3.4 \times 10^{38})$ / $[(10.51 \times 10^{12}) \times 31536000] = 1.02 \times 10^{18}$ or approximate 1 billion billion years. That result depicts a very long effort to crack the 128-bit key.

In addition, the AES-GCM algorithm used in the proposed KRS system can provide higher throughput with less resource utilization [15]. It is also an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality. The GCM is also defined for block ciphers with a block size of 128 bits. Moreover, the GCM mode accepts initialized vectors of arbitrary length. These are the reason why the DLMS/COSEM protocol for smart metering recommends such algorithm for the data security. In Table 3, the more number of key bits will result in the more complexity of its possible recovery key. Moreover, it will spend enormous time to reveal the secret key with a higher number of key bits. Notice that the exponential increase is observed in possible combinations as the key size increases.

***Table 3:*** *The possible combinations for each key size.*

| Key size | Possible key combinations | Key size | Possible key combinations |
|---|---|---|---|
| 4-bit | 16 | 128-bit(AES) | $3.4{\times}10^{38}$ |
| 8-bit | 256 | 192-bit(AES) | $6.2{\times}10^{57}$ |
| 16-bit | 65536 | 256-bit(AES) | $1.1{\times}10^{77}$ |

## 6.5 Probability of key compromising

Assuming that our key recovery system uses N = 6 KRAs and M = 3, the probability of key compromise will be 2/3 or 66.67%. If the number of qualified KRAs for recovering the key is increased to 5, the probability of key compromising will be decreased to 1/3 or 33.33%. However, If M = 2, the probability of key compromising will be increased to 5/6 or 83.33%, which is not acceptable for the security. One could see that when K increases, the probability of KRA failure decreases at the same SNR level, at the price of lowering the probability of key compromising.

### 6.6 The probability of failure from the predetermined threshold for KRA selection algorithm

The quality of channel between SMU, KRAs, and DCU is determined by sending the pilot signal to learn the channel state information (CSI). According to SNR and outage probability of each KRA, the DCU can select which KRA is qualified for running the key recovery service, and send that information to SMU. In this experiment, the predetermined threshold is $\beta_0 = 0.5$ which means that the acceptable outage probability of SNR is 50%, which is considered as a worst case scenario. The other predetermined threshold is the SNR threshold $\gamma_{\text{th}} = 0$ dB which means that the signal and noise powers are equal representing the worst case scenario too.

In Fig. 15, it shows that when SNR is below 4 dB, there is no KRA that passes the outage probability threshold meaning that this SNR regime is not suitable for the proposed SKRS-CQA. For the SNR regimes which are more than 5dB, the probability of KRA failure is reduced when SNR increases. It is also worth noticing that the probability of failure for a higher value of K is lower than that of a smaller value of K because it is normally less probable in the system that a large number of concurrently failed KRA is happened in any single event.

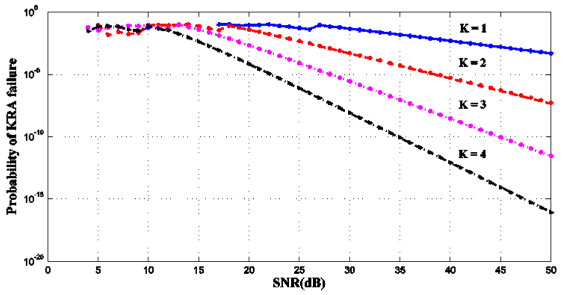

***Fig.15:*** *The performance of our proposed SKRS-CQA with N = 6, beta = 0.5, K = 1, 2, 3, 4.*

Therefore, this result could be used as a guideline for the SKRS-CQA design if the engineer could specify the nominal range of system's SNR. For example, if the specific system's SNR = 30 dB and the desired probability of failure is less than or equal to 10-4, then the case of K= 3 and K =4 should be considered. If K = 4 is considered, then M = N-K+1 is equal to 6-4+1 = 3 and the probability of key compromising is 4/6 = 66.67%. This results in more system reliability, but low security because each KRA has to store 4 out of 6 parts of the key recovery field. In contrast, if K=3 is considered, then M is equal to 6-3+1=4 and probability of key compromising is $^1/_2$ = 50%. This results in less system reliability, but higher system security because each KRA has to store 3 out of 6 parts of the key recovery field. Hence, the system designer has to tradeoff these pros and cons.

### 6.7 The cooperative SKRS-CQA versus the conventional KRS

The performance of our proposed SKRS-CQA with cooperative scheme for N = 6, beta = 0.5, and K = 1, 2, 3, 4 is illustrated in Fig.16.

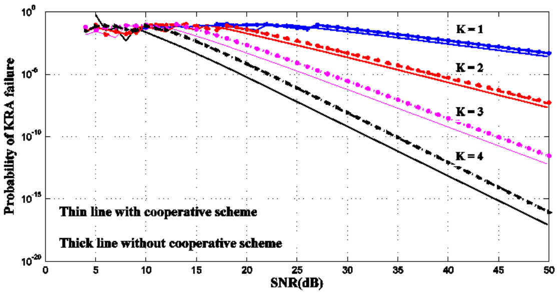

***Fig.16:*** *The performance comparison between conventional KRS and our proposed SKRS-CQA with cooperative scheme for N = 6, beta0 = 0.5, K = 1, 2, 3,4 .*

Our proposed scheme with cooperatiive scheme requires less SNR than a conventional KRS system without a cooperative scheme. This is due to the diversity gain obtained from the cooperative KRA. Therefore, the system designer could better design the system with higher system reliability and higher system security.

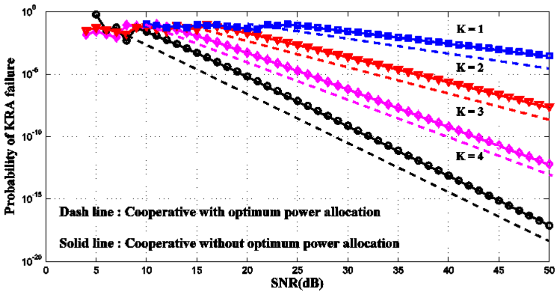

***Fig.17:*** *The performance comparison between our proposed cooperative scheme SKRS-CQA with and without optimal power allocation for N = 6, beta0 = 0.5, K = 1, 2, 3,4.*

The link quality between the source KRA, the relay KRA, and the destination DCU should be properly adjust. If the link quality between source KRA and relay KRA is poor, placed more power at source station. On the contrary, if the link quality from source to relay is good enough, the power at $P_1$ and $P_2$ should have the same amount of energy for the highest efficiency. As shown in Fig.17, at the higher SNR scnenario, the system with optimal power allocation capability (dash line), for every number of failed agent, the probabillity of KRA failure reduce significantly.

## 7. CONCLUSIONS

In this paper, the security key recovery with channel quality awareness (SKRS-CQA) for smart grid applications has been proposed. The KRAs authentication and selection algorithms have also been proposed, which is determined by a proper outage probability threshold, a proper probability of KRA failure and a proper probability of key compromising. The AES-GCM and DLMS/COSEM protocol standard have been applied for authentication, identification and key encryption in exchanging the key on smart grid networks. The capability of the proposed SKRS-CQA is that it could be well utilized in Rayleigh fading wireless channel environment. The computer simulation results showed that at low SNR regimes, the probability of KRA failure increases; as a result, a qualified KRA used for the proposed system is limited to a small number resulting in increasing the probability of key compromising at the expense of losing the system reliability. In higher SNR regimes, the outage probability decreases resulting in the reduction of a number of concurrently failed KRAs; as a result, the acceptable probability of key compromising is achieved, and the complete key recovery process will be fully successful with an extremely low probability of KRA failure. Moreover, we have deliberately examined the proposed system in a real environment with the help of cooperative communications and optimal power allocation. The computer simulation shows that, at the same SNR of 30 dB, the probability of failure of the proposed system with cooperative scheme is at 10-9 while the probability of failure of the KRS system without cooperative scheme is at 10-8. Therefore, the proposed system is suitable for the smart grid application where the wireless sensor network has been employed as a last mile communication infrastructure.

### References

[1] E. Santacana, G. Rackliffe, T. Le, X. Feng, “Getting smart,” *IEEE Power and Energy Magazine*, vol.8, no.2, pp. 41-48, March-April 2010.

[2] J. Yick, B. Mukherjee, D. Ghosal, “Wireless sensor network survey,” *Computer Networks (Elsevier) Journal*, vol. 52, pp. 2292-2330, 2008.

[3] S. Feuerhahn, M. Zillgith, C. Wittwer, & C. Wietfeld, “Comparison of the communication protocols DLMS/COSEM, SML and IEC 61850 for smart metering applications,” *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2011.

[4] A.R. Metke, R.L. Ekl, “Security Technology for Smart Grid Networks,” *Smart Grid, IEEE Transactions on*, vol.1, no.1, pp.99, 107, June 2010.

[5] C. Henk, A. van Tilborg, E. Cronin, “Encyclopedia of Cryptography and Security,” *Third International Conference on Computational Intelligence Modeling & Simulation*, 2011.

[6] T. KUBO, “Key Pre-distribution System as a Key Recovery System,” *Proceedings of PKS’97 Conference*, Toronto, Canada, April 1997.

[7] Y. Hori, A. Satoh, H. Sakane and K. Toda, “Bitstream Encryption and Authentication with AES-GCM in Dynamically Reconfigurable Systems,” *FPL 2008. International Conference*, 8-10 Sept. 2008.

[8] D. E. Denning, D. K. Branstad, “A Taxonomy for Key Recovery Encryption Systems,” *Georgetown University Trusted Information Systems*, May 11, 1997.

[9] S. Lim, S. Kang, and J. Sohn, “Modeling of Multiple Agent Based Cryptographic Key Recovery Protocol,” *Proceedings of the Annual Computer Security Applications Conference*, pp.119-128, 2003.

[10] K. Kanyamee and C. Sathitwiriyawong, “A Simple High-Availability Multiple-Agent Key Recovery System”, *the 4th International Conference for Internet Technology and Secured Transactions.* London, 2010, pp. 734-739.

[11] K. Kanyamee; C. Sathitwiriyawong, “High-Availability Decentralized Cryptographic Multi-agent Key Recovery,” *International Arab Journal of Information Technology (IAJIT)*, vol. 11, issue 1, pp. 52-55, Jan. 2014.

[12] A. Goldsmith, *Wireless Communications*, Cambridge University Press, 2005.

[13] D. Gislason, *ZigBee Wireless Networking*, Newness, 2007.

[14] W. Swasdio, C. Pirak, S. Jitapunkul, G. Ascheid, “Alamouti-coded decode-and-forward protocol with optimum relay selection and power allocation for cooperative communications,” *EURASIP Journal on Wireless Communications and Networking*, 2014.

[15] DLMS User Association, “COSEM Architecture and Protocols,” *Green Book, Eighth Edition*, pp.193.

[16] W. Somkaew, S. Thepphaeng, C. Pirak, “Data Security Implementation over ZigBee Networks for AMI Systems,” *Electrical Engineering/ Electronics, Computer, Telecommunications and In-*

*formation Technology (ECTI-CON) 11th International Conference*, 2014.

[17] Z. Guo, T. Okuyama, and M. F. Finley, "A New Trust Model for PKI Interoperability," *IEEE Computer Society*, 2005.

[18] E. Ayday, F. Delgosha, F. Fekri, "Data Authenticity and Availability in Multi hop Wireless Sensor Networks," *Transactions on Sensor Networks*, vol.8, no. 2, article 10, March 2012.

[19] L. Zhu, Z. Yang, J. Xue, and C. Guo, "An Efficient Confidentiality and Integrity Preserving Aggregation Protocol in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2014.

[20] D. Branstad, M. Smid, E. Barker, "A Framework for Designing Cryptographic Key Management Systems," *NIST Special Publication 800-130*, August 2013.

[21] *The Binomial Distribution*, Hamilton Institute. October 20, 2010.

[22] C. Lv., X.Jia, L. Tiany, J. Jing, and M. Suny, "Efficient Ideal Threshold Secret Sharing Schemes Based on EXCLUSIVE-OR Operations," *Proceedings of the Fourth International Conference on Network and System Security*, pp. 136-143, 2010.

[23] P. Huadpaknam, C. Pirak, R. Mathar, "A novel security key recovery framework for smart grid applications," in *Communications (APCC), 2014 Asia-Pacific Conference on*, vol., no., pp.387-390, 1-3 Oct. 2014.

[24] W. Su, A. K. Sadek, K. J. Ray Liu, "Cooperative Communication Protocols in Wireless Networks: Performance Analysis and Optimum Power Allocation," *Wireless Personal Communications*, Springer, (2008) 44 vol. 2:181-217.

**Prachya Huadpaknam** received his Bachelor degree in electrical engineering from Siam university, Thailand in 1993. He also received Master degree in electrical engineering from King Mongkut's Institute of Technology North Bangkok in 2002. Currently, he serves as an IT and electronics engineer in the Royal Thai Navy. He is also a Ph.D. candidate in mobile communication and embedded laboratory of The Sirindhorn International Thai-German Graduate School of Engineering (TGGS), King Mongkut's University of Technology North Bangkok, Thailand. His research interests are in the areas of cooperative communications, wireless sensor networks, cryptography, and cyber security.

**Chaiyod Pirak** received his Bachelor degree in telecommunication engineering from King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand in 2001, and Ph.D. degree from University of Maryland, College Park, MD, USA in conjunction with Chulalongkorn University in 2005. He is now an Assistant Professor at TGGS, King Mongkut's University of Technology North Bangkok. His research interests include the area of mobile communications, embedded systems and smart grid technology.

**Rudolf Mathar** received his Diploma and Ph.D. degree in mathematics from RWTH Aachen University in 1978 and 1981, respectively. He is currently a member of North-Rhine Westphalia Academy for Sciences and Arts, Vice-chair of the IEEE Information Theory Society Germany chapter. His research interests include mobile communication systems, particularly optimization, cryptography and information theory. He is serving as Pro Rector for Research and Structure and the head of the Institute for Theoretical Information Technology (TI) at RWTH Aachen University.