International Journal of Safety and Security Engineering
Vol. 13, No. 4, August, 2023, pp. 611-623
Journal homepage: http://iieta.org/journals/ijsse

SE-CDR: Enhancing Security and Efficiency of Key Management in Internet of Energy Consumer Demand-Response Communications

Mourad Benmalek[1*], Kamel Harkat[2], Kamel-Dine Haouam[1], Zakaria Gheid[3]

[1] Computer Engineering Department, College of Engineering and Architecture, Al Yamamah University, Riyadh 13541, Saudi Arabia
[2] Ecole Nationale Supérieure d'Informatique, Oued-Smar 16309, Algeria
[3] Department of Mathematics and Computer Science, Souk Ahras University, Souk Ahras 41000, Algeria

Corresponding Author Email: m_benmalek@yu.edu.sa

https://doi.org/10.18280/ijsse.130403

Received: 5 February 2023
Revised: 24 July 2023
Accepted: 13 August 2023
Available online: 28 September 2023

Keywords:
security, efficiency, key management, consumer demand response communications, internet of energy

ABSTRACT

The burgeoning Internet of Energy (IoE) paradigm, a fusion of the Internet of Things (IoT) and Smart Grid (SG) technologies, holds the promise of significantly enhancing the reliability and efficiency of energy production, transmission, and consumption across the entire energy chain, from generation to the end user. Two central technical aspects that enable this innovation are the advent of smart consumer electronics and the establishment of bidirectional IoT communications. These developments have facilitated the incorporation of novel applications into the Smart Grid, including smart metering, Consumer Demand-Response (CDR) management, and prepayment. In this study, our focus lies primarily on the development of a secure and efficient key management system for CDR communications. It is demonstrated herein that a previous key graph-based scheme, called EDR, is susceptible to collusion attacks and lacks support for broadcast CDR communications. In response to these vulnerabilities, we propose a novel key management scheme, referred to as Secure and Efficient key management scheme for CDR communications (SE-CDR). This scheme retains the strengths of the EDR while introducing a modified multi-group key graph technique, designed to ensure the secure, efficient, and scalable management of unicast, multicast, and broadcast CDR communications. The presented security analysis and performance evaluation results establish the robust security of the SE-CDR scheme. Moreover, a comparative analysis revealed that this new approach offers significant improvements in terms of storage and communication efficiency, outperforming existing state-of-the-art methods. This study thus presents a promising advancement in the realm of secure and efficient key management for the Internet of Energy paradigm.

1. INTRODUCTION

The escalating demand for efficient energy management and distribution has emerged as a potent catalyst for research into the Internet of Energy (IoE) paradigm. The IoE concept is a product of the synergistic integration of the Internet of Things (IoT) and Smart Grids (SG) visions [1, 2]. The application of the IoT communication paradigm to oversee power generation, distribution, and management has been demonstrated to enhance the dependability, effectiveness, flexibility, and cost-effectiveness of the SG.

In recent times, Consumer Demand-Response (CDR) management has been identified as a critical element for augmenting the efficiency of power networks, offering benefits to consumers and power utilities alike [3]. CDR programs, which are agreements between consumers and power utilities stipulating specific prices and load conditions, facilitate consumers in overseeing their energy usage and reconfiguring their energy consumption patterns in return for incentives or favorable pricing [4, 5]. The implementation of CDR can involve postponing high-energy tasks or shutting down appliances like heaters, air conditioners, and washing machines. Examples of such programs include the Emergency Demand Reduction (EDR) program [6], Real-Time Pricing (RTP) program [7], and Direct Load Control (DLC) program [8].

Given its pivotal role in the power network, CDR management has become an attractive target for potential attacks. For example, compromising the real-time pricing channel could lead to energy theft or unauthorized manipulation of appliances, thus presenting a considerable challenge for ensuring the security of CDR communications [9, 10]. In general, the security requirements for CDR programs are:

(1) *Confidentiality*: Ensuring that sensitive information, such as consumer data and energy usage patterns, is protected from unauthorized access or disclosure.

(2) *Integrity*: Guaranteeing that the data and instructions exchanged between consumers and the energy system remain intact and unaltered throughout the transmission and processing stages.

(3) *Authentication*: Verifying the identities of consumers and energy system components to prevent unauthorized access and ensure that only authorized entities can participate in Demand-Response activities.

(4) *Availability*: Ensuring that the energy system and its

Demand-Response capabilities remain accessible and operational, allowing consumers to interact with the system and respond to energy demands effectively.

(5) *Non-repudiation*: Preventing any party from denying their participation or the actions they have taken in the Demand-Response program, establishing accountability and traceability for all involved entities.

To meet these security requirements, an effective Key Management Scheme (KMS) must be implemented. However, it is critical that security operations, such as key updates, are also secure as inadequate key update procedures pose risks of potential key exposure, thereby undermining the overall objective of CDR management.

The KMS in IoE networks must also exhibit efficiency in minimizing overhead, given that key management operations are often conducted frequently among a multitude of entities with constrained resources [11-16].

Moreover, the KMS should be *scalable* in the sense that it must be able to handle large networks of IoT devices, potentially numbering in the millions, while still maintaining its performance even if expansion is needed. The KMS must also be *versatile*, capable of supporting all forms of communication, including [10]:

(1) *Unicast communications* employed, for instance, when a SM shares its energy data and projected power requirements with the control center.

(2) *Broadcast communications* used, for instance, when the control center sends a message that includes "maintenance schedule announcement" or "emergency shutdown command" to all the consumers.

(3) *Multicast communications* utilized, for instance, when the control center dispatches a remote load control message to a group of consumers who have subscribed to the same program.

1.1 Related work

Over the past several years, the scientific community has made substantial strides in proposing a variety of Key Management Schemes (KMS) designed to secure communications within the framework of Internet of Energy (IoE) networks [17-33]. However, a minority of these efforts have been aimed at developing a secure, efficient, and versatile KMS specifically for Consumer Demand-Response (CDR) communications.

A scalable and fault-tolerant KMS was presented by Wu and Zhou [17], which incorporated symmetric key techniques and Elliptic Curve Cryptography (ECC). Despite its innovative approach, this scheme was later found to be vulnerable to Man-In-The-Middle (MITM) attacks, as highlighted by Xia and Wang [18].

Building on previous work, Liu et al. [19] developed a flexible KMS for securing CDR communications. Their approach, which leveraged simple mathematical functions for key agreement and renewal, was particularly suited to addressing the resource constraints of smart meters. Following a similar line of thought, Yu et al. [20] proposed a novel KMS for Information Centric Networking in the IoE, dubbed ICN-KMS. Regrettably, these schemes proved susceptible to desynchronization attacks, as demonstrated by Wan et al. [21]. In response, Wan et al. offered an efficient scheme that combined an effective key graph technique with an Identity-Based Cryptosystem (IBC) to secure CDR communications.

Tsai and Lo [22] designed an innovative IBC-based scheme with a tamper-proof module, aiming to ensure efficient key distribution and ward off probing attacks. However, this proposed solution was later found to be insecure against impersonation and ephemeral key compromise attacks, as noted by Odelu et al. [23]. Meanwhile, Yan et al. [24] introduced a lightweight approach designed to provide a key agreement and mutual authentication mechanism. This solution, however, was later shown to be susceptible to various attacks like Denial of Service (DoS) and replay attacks as noted by Shariat and Safkhani [34].

Mahmood et al. [25] proposed a solution that relied on ECC to facilitate peer-to-peer communication within the Smart Grid (SG). Despite its potential, Abbasinezhad-Mood and Nikooghadam [26] identified weaknesses in this scheme, including a lack of perfect forward secrecy. A versatile and scalable KMS for CDR communication security was proposed by Benmalek et al. [27], but it was found that the proposed broadcast update process led to excessive communication overhead.

In a further development, Mohammadali et al. [28] created two distinct authenticated key agreement schemes that relied on ECC. Later, Zhang et al. [29] proposed an efficient authenticated key agreement protocol that utilized symmetric encryption and secure hash functions to achieve Smart Meter (SM) anonymity and untraceability, while maintaining a low computational overhead.

Gope [30] proposed a scheme for establishing privacy-preserving multi-factor authentication keys that relied on one-way hash functions, reverse fuzzy extractors, and Physical Uncloneable Functions (PUFs). This scheme provided mutual authentication and untraceability. Concurrently, Benmalek et al. [31] focused on securing CDR programs and introduced a novel KMS, termed EDR, for secure CDR communications. This scheme employed a novel key graph technique to enhance the security of multicast and unicast CDR communications within extensive IoE networks. Moreover, this scheme facilitated the administration of dynamic CDR programs.

Most recently, Xiang and Cao [32] proposed an authenticated key agreement protocol that ensures privacy-preservation for IoE communications. Concurrently, Nkurunziza et al. [33] proposed a secure certificateless key agreement and authentication protocol, specifically designed to meet the resource constraints of devices, while ensuring secure communication between legitimate parties.

In summary, while the field has seen substantial progress, the development of a secure, efficient, and versatile KMS for CDR communications remains a critical area of research. The challenges in this domain are complex and multi-faceted, necessitating further investigation and innovative solutions.

1.2 Our contributions

In this study, an initial examination is made of the EDR scheme [31] which reveals a lack of versatility, particularly in supporting broadcast Consumer Demand-Response (CDR) communications. Furthermore, the scheme is identified as susceptible to collusion attacks. To address these shortcomings, we propose a more efficient, scalable, secure, and versatile Key Management Scheme (KMS) specifically tailored for secure CDR communications. The pivotal findings of this study are as follows:

(1) We analyze EDR scheme [31] and show that it is vulnerable to collusion attacks.

(2) We propose an improved KMS (SE-CDR) to enhance

the security of EDR scheme. SE-CDR maintains the merits and covers the demerits of the original scheme by ensuring backward/forward secrecy, and ensuring resistance to the collusion attacks.

(3) We modify the EDR's key graph structure, and we design an efficient broadcast key update mechanism.

(4) We present an analysis of performance and security, along with simulations and a comparison against existing schemes, demonstrating the superior efficiency and security of the proposed solution.

1.3 Paper organization

The structure of this study unfolds as follows: A comprehensive system model is delineated in Section 2, accompanied by an outline of the key management design objectives. Section 3 embarks on a scrutinizing review of the existing Key Management Scheme (KMS) as proposed by Benmalek et al. [31], shedding light on its inherent weaknesses. Armed with the identification of these shortcomings, an improved KMS is proposed in Section 4, wherein the design of this refined scheme is presented and its enhancements thoroughly discussed.

Section 5 is dedicated to a rigorous performance and security evaluation of the proposed solution, providing a robust assessment of its efficacy. The comparative analysis undertaken in Section 6 juxtaposes the proposed scheme against four existing schemes across both performance and security metrics [19-21, 31]. The study concludes in the final section, encapsulating the key findings and underlining the significant contributions of this research.

In essence, this study embarks on a critical examination of the existing KMS, identifies its shortcomings, and proposes an improved system. Through a series of rigorous analyses, evaluations, and comparative studies, the efficacy, performance, and security enhancements of the proposed scheme are conclusively demonstrated. The study concludes by summarizing these key findings and emphasizing the significant contributions to the field, setting the stage for further research and innovation.

2. SYSTEM MODEL AND KEY MANAGEMENT REQUIREMENTS

In the upcoming section, we will describe the system model and outline the security and performance requirements associated with key management in IoE.

2.1 System model

The Internet of Energy network adheres to the structure depicted in Figure 1. It comprises:

(1) *Control Center (CC):* It plays a vital role in managing and monitoring the power distribution and demand-response operations. It coordinates the overall functioning of the IoE network, including load balancing, demand forecasting, and real-time monitoring of energy consumption. Additionally, it facilitates the implementation of demand-response programs and ensures the efficient utilization of energy resources.

(2) *Smart Meters (SMs):* They represent sophisticated devices installed at the locations of consumers to measure and document energy usage periodically. They provide granular data on energy usage, including real-time measurements, usage patterns, and peak demand periods.

(3) *Distributed Energy Resources (DERs):* They encompass various decentralized energy sources, including wind turbines, solar panels, and energy storage units. DERs generate and supply electricity to the grid while also enabling two-way communication between consumers and utility providers.

(4) *Smart Consumer Electronics:* They include appliances such as air conditioners and washing machines. These devices are equipped with communication capabilities and can interact with the network to optimize energy consumption, participate in Demand-Response programs, and provide valuable data for load management.

(5) *Communication Networks:* The IoE network relies on different communication networks to establish connectivity between the utility side and the consumer side. These networks utilize various communication technologies such as Wi-Fi, Zigbee, or cellular networks to enable broader communication between the utility infrastructure and consumers via the Internet.

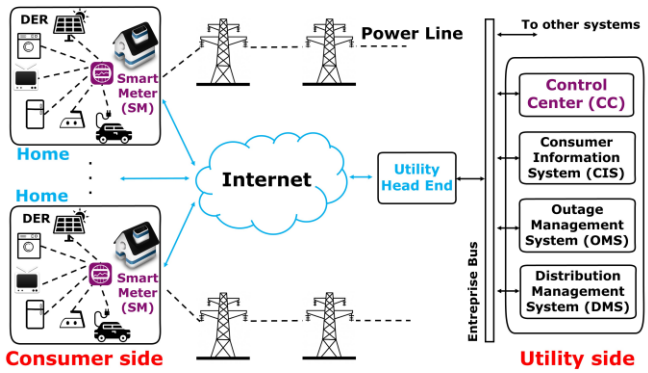

Figure 1. System Model for IoE network

2.2 Key management requirements

In the subsequent sections, we examine the fundamental security and performance requirements essential for an efficient and secure KMS.

2.2.1 Security requirements

Below are the summarized security requirements that a KMS must verify to ensure secure CDR communications.

(1) *Forward secrecy*. This means that a consumer who leaves a CDR program or the IoE network should not be able to access future secret keys. By enforcing forward secrecy, we prevent any unauthorized access to confidential information and mitigate the risk of compromising the security of future communications.

(2) *Backward secrecy*. This means that a consumer who joins a CDR program or the IoE network should not be able to access previously used secret keys. This requirement is essential in scenarios where unauthorized access to past secret keys could potentially lead to the compromise of sensitive information and the integrity of the system.

(3) *Collusion freedom*. This means that a group of consumers who leave a CDR program or the IoE network should not be able to deduce the current used CDRs group keys or the current used broadcast key through collusion. By guaranteeing collusion freedom, we mitigate the risk of malicious activities and unauthorized key sharing among consumers. This is particularly important in the context of

CDR programs, where maintaining the confidentiality and integrity of communication among participants is of utmost importance to prevent unauthorized access and potential manipulation of sensitive data.

(4) *Immediate keys update:* Requiring an immediate update of keys when a new consumer joins or leaves from a CDR program or the IoE network. This ensures that security is maintained even in the presence of changing participants, bolstering the system's resilience against unauthorized access and potential breaches.

2.2.2 Non-security requirements

Satisfying the following performance requirements is of great importance for an effective KMS.

(1) *Versatility*. This means that the scheme should support the broadcast, multicast and unicast communications.

(2) *Efficiency*. This means that the KMS must be designed in a way that it consumes minimal memory and computational resources, so as to not overload the limited resources devices. Additionally, the key update process should result in minimal communication overhead, which is crucial for time-sensitive CDR communications within IoE networks.

(3) *Scalability*. This means that the KMS should be capable of handling the huge number of intelligent consumer electronics in the IoE network, and should allow for growth and expansion without significantly hindering the performance of the system.

3. REVIEW OF EDR SCHEME

EDR scheme was proposed to provide secure CDR communications in IoE [31]. It uses a key graph approach to efficiently manage keys for both unicast and multicast communications, reducing storage and communication costs. In the following, we will briefly examine the two KMS (i.e., unicast and multicast key management protocols) of EDR scheme and highlight their vulnerabilities.

3.1 Description of EDR scheme

EDR scheme consists of two key management protocols:

3.1.1 Unicast key management

A secure method of exchanging keys is employed to set up *individual symmetric keys* $\{k_1, \dots, k_n\}$ between the SMs and the *CC*. These symmetric keys are employed for the secure unicast CDR communications.

3.1.2 Multicast key management

The previous individual keys are used to form a key graph structure used to secure the multicast CDR communications between the *control center* and the *smart meters*. The designed structure enables the handling of dynamic and multiple CDR programs for each consumer simultaneously.

As depicted in Figure 2, the formed key graph structure is designed as follows:

(1) At the lower level, consumers are organized into key trees based on their subscriptions. A key tree, known as *SubG-tree*, is created for each Subscription Group $SubG_i$ (which refers to a group of consumers who subscribed simultaneously to the same set of CDR programs). The use of binary One-way Function Trees (OFT) addresses the flexibility and scalability concerns [35].

(2) At the upper level, the root of each subscription tree is linked to the Group Keys (GKs) of the CDR programs that are part of this subscription. Thus, a key tree, referred to as *CDrG-tree*, is created for each CDR Group (which refers to all consumers who subscribed to a specific CDR program). Because a CDR program (CDR_i) may be included in multiple subscriptions, Logical Key Hierarchy (LKH) trees are used to connect GK_i with the roots of the shared subscription trees [36]. Moreover, the proposed key graph structure has the following properties:

(a) A consumer is associated with only one SubG-tree that corresponds to his subscription. He possesses a copy of his individual key and all the keys in the path from his individual key to the root of the SubG-tree.

(b) A consumer possesses a copy of all the keys along the path from their SubG-tree to the GKs of the CDR programs he subscribed to.

(c) If a consumer joins/leaves one/more CDR programs, he will shift to the SubG-tree corresponding to his new subscription.

As the consumers subscribed to CDR programs are not fixed, the proposed multicast KMS efficiently updates the CDR Group members while ensuring *group secrecy*, *backward secrecy* and *forward secrecy*.

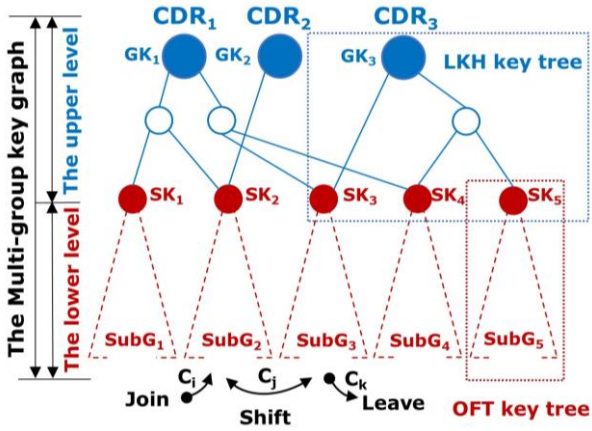

Figure 2. Example of EDR's key graph structure

3.2 Weaknesses of EDR scheme

EDR scheme has the following weaknesses: 1) Binary OFT key trees form the lower layer in the key graph structure for EDR. The classical OFT mechanism is used to update the keys in SubG-trees. Then, the keys of the lower level are used to update those of the upper level. However, this scheme is vulnerable to the collusion attack and does not guarantee either backward or forward secrecy; 2) EDR does not support secure broadcast CDR communications.

3.2.1 Collusion attack on EDR scheme

The collusion attack can be described as follows:

(1) Initially (at t_0), the used key graph structure is illustrated in Figure 3. By definition, the $SubG_4$ group key is $SK_{4(t0)} = f(g(k_{1\text{-}3(t0)}), g(k_{4\text{-}5(t0)}))$.

(2) Suppose Alice, identified by C_2, unsubscribes from CDR_1 at time t_1. As a result, she will switch from $SubG_4$ to $SubG_5$, and the key graph structure will be updated as depicted in Figure 4 (updated keys are shown in gray). The keys in the lower level (i.e., the keys in $SubG\text{-}tree_4$ and $SubG\text{-}tree_5$) will be updated using the conventional OFT update mechanism.

The new $SubG_4$ group key, noted $SK_{4(t1)}$, will be $SK_{4(t1)} = f(g(k_{1\text{-}3(t1)}), g(k_{4\text{-}5(t0)}))$, where $k_{1\text{-}3(t1)}$ is the new key associated with $k_{1\text{-}3}$. At this point, the blinded key $g(k_{4\text{-}5(t0)})$ which is known by Alice remains unchanged. In the upper level, $SK_{3\text{-}4(t0)}$ is updated to $SK_{3\text{-}4(t1)}$ and distributed to consumers in $SubG\text{-}tree_3$ and $SubG\text{-}tree_4$ as follows:

$$CC \rightarrow SubG_3: Encrypt\ (SK_{3-4(t1)}, SK_{3(t0)}) \quad (1)$$

$$CC \rightarrow SubG_4: Encrypt\ (SK_{3-4(t1)}, SK_{4(t1)}) \quad (2)$$

Then, the CDR_1 group key $GK_{1(t0)}$ is updated to $GK_{1(t1)}$ and distributed to consumers in $SubG\text{-}tree_1$ and $SubG\text{-}tree_2$:

$$CC \rightarrow SubG_1, SubG_2: Encrypt\ (GK_{1(t1)}, SK_{1\text{-}2(t0)}) \quad (3)$$

Finally, $GK_{1(t1)}$ is distributed to consumers belonging to $SubG\text{-}tree_3$ and $SubG\text{-}tree_4$ as follows:

$$CC \rightarrow SubG_3, SubG_4: Encrypt\ (GK_{1(t1)}, SK_{3\text{-}4(t1)}) \quad (4)$$

(3) Suppose Bob, identified by C_7, unsubscribes from CDR_1 at time t_2 ($> t_1$). This causes him to switch from $SubG_5$ to $SubG_4$ and the key graph structure is updated as depicted in Figure 5 (*updated keys are in gray*). The keys at the lower level (i.e., keys in $SubG\text{-}tree_4$ and $SubG\text{-}tree_5$) are updated using the standard OFT update process. If there are no rekeying operations during the time period $[t_1, t_2]$, the new $SubG_4$ group key will be $SK_{4(t2)} = f(g(k_{1\text{-}3(t1)}), g(k_{4\text{-}5(t2)}))$, where $k_{4\text{-}5(t2)}$ is the new key associated with $k_{4\text{-}5}$. It should be noted that Bob now has knowledge of the blinded key $g(k_{1\text{-}3(t1)})$. In the upper level, the keys $\{SK_{3\text{-}4(t1)}, GK_{1(t1)}\}$ are updated to $\{SK_{3\text{-}4(t2)}, GK_{1(t2)}\}$ using a hash function. The CC increases the counter of the updated keys. This means that consumers in $SubG\text{-}tree_1$, $SubG\text{-}tree_2$, $SubG\text{-}tree_3$, and $SubG\text{-}tree_4$ will be aware of the key update and calculate the new versions of the updated keys by applying the same hash function.

(4) Now, since Alice knows $g(k_{4-5(t0)})$ and Bob knows $g(k_{1-3(t1)})$, they can collude to compute the key $SK_{4(t1)} = f(g(k_{1-3(t1)}), g(k_{4-5(t0)}))$. Then, they can decrypt $SK_{3-4(t1)}$ distributed in (2). After that, they can use $SK_{3-4(t1)}$ to decrypt $GK_{1(t1)}$ distributed in (4) and which they should not know. As a consequence, *the EDR scheme fails to provide both forward and secrecy (forward secrecy against Alice and backward secrecy against Bob)*.

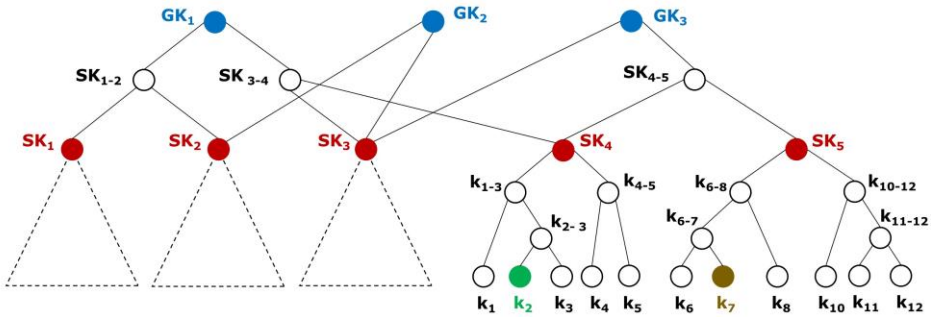

Figure 3. EDR's key graph structure at t_0

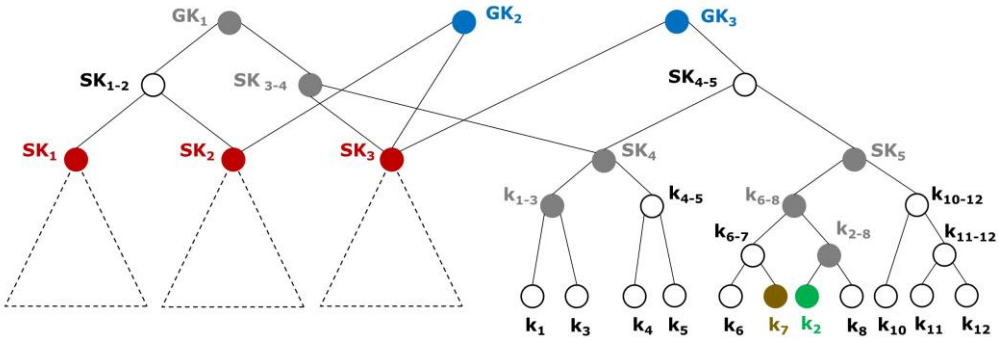

Figure 4. EDR's key graph structure at t_1

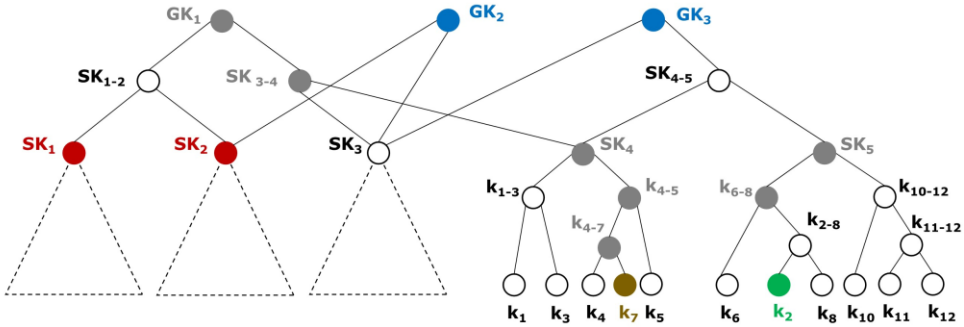

Figure 5. EDR's key graph structure at t_2

4. SE-CDR: A MORE SECURE AND EFFICIENT KEY MANAGEMENT SCHEME FOR CDR COMMUNICATIONS

In order to overcome the weaknesses described in Section 3.2, we propose a more Secure and Efficient key management scheme for CDR communications, named SE-CDR. Our improved scheme not only inherits the advantages of EDR scheme in terms of efficiency, but it also enhances the security. In the proposed scheme, we use a new key graph approach to ensure efficient management of the CDR communications. Later, we will show that our KMS scales to large IoE networks while meeting consumer SM's resource constraints. Table 1 summarizes the terminology used to describe our proposed scheme.

Table 1. Notation table

Notation	Description
m	Number of CDR programs
N	Number of consumers in IoT network
d	LKH key tree degree
$H(.)$	One-way hash function
$Encrypt(msg, k)$	Encrypt msg with key k
C_i	The i^{th} consumer
GK_i	The i^{th} CDR program's group key
SK_i	The i^{th} Subscription Group key
CDR_i	The i^{th} CDR program
$SubG_i$	The i^{th} Subscription Group
$CDrG_i$	The i^{th} CDR Group
$\|CDrG_i\|$	Number of subscribers in $CDrG_i$
$\|SubG_i\|$	Number of subscribers in $SubG_i$
$X \rightarrow Y: msg$	X sends a msg to Y

4.1 Initialization

(1) Each consumer C_i first needs to register his smart meter SM_i to the CC as to becoming a valid consumer of the power utility as follows:

- $SM_i \rightarrow CC$: The consumer's SM sends a registration request message including its identity ID_i to the CC through a secure channel of communication.
- $CC \rightarrow SM_i$: After the CC receives the request, it creates an entry in its database with the following information $\{ID_i, k_i\}$ where k_i is a randomly generated secret key. Then, the CC sends a response message including $\{ID_i, k_i\}$ to SM_i through the secure channel of communication.
- After receiving the response message, SM_i stores $\{ID_i, k_i\}$ in its memory for later use during the CDR communications and the key update processes.

(2) After the previous phase, the CC and each SM_i establish a shared individual key k_i. These keys will be used to secure unicast CDR communications between the CC and SM_i.

(3) Subsequently, the individual keys $\{k_1, ..., k_N\}$ are used to generate the multi-group key graph structure for secure multicast and broadcast CDR communications.

(4) In SE-CDR, every key holds the secret material known as the key content and a key selector. The key selector consists of two components: (1) a distinctive identifier that remains unchanged, regardless of any alterations to the key content, and (2) a counter that reflects updates in the key material. This counter is increased each time the key is processed via a one-way hash function.

(5) It is assumed that all SMs are tamper proof. Additionally, to counter physical attacks, SMs equipped with Physical Uncloneable Functions (PUFs) can be used. By assuming tamper-proof SMs, it is expected that the IoE system is more secure against physical attacks, such as tampering with the meter's hardware, wiring, or firmware. This assumption implies that the system is built to withstand various physical threats, thus reducing the risks of fraudulent activities, data manipulation, or unauthorized usage. Moreover, PUFs can ensure secure SMs authentication by leveraging unique physical variations in SMs to generate unpredictable and difficult-to-replicate responses to challenge queries. By securely storing and utilizing the SM-specific PUF response during authentication, PUFs verify the authenticity of SMs, preventing unauthorized SMs from being introduced into the system and enhancing the overall security of the system.

4.2 SE-CDR key graph structure

Efficient and scalable broadcast key management can be achieved by using key graph techniques. An easy approach is to use a separate LKH key tree for the broadcast rekeying process. However, if a consumer subscribes to one or multiple CDR programs at the same time, he has to store: (1) keys from the key graph structure used for secure multicast CDR communication, and (2) keys from the new LKH tree used for secure broadcast CDR communication. Thus, the application use of a separate LKH tree for broadcast key management results in a significant overhead for key storage.

To this end, we propose to exploit the advantage of EDR's key graph structure and modify it so that we reduce the number of stored keys. The new key graph structure can be modeled as shown in Figure 6. Indeed, in addition to EDR's key graph structure properties, our new key graph structure has the following properties:

(1) All consumers subscribe to a virtual CDR program, denoted by CDR_0. GK_0 denotes the group key of this program. *The later is used as the broadcast key*.

(2) Consumers who do not subscribe to any CDR program (except CDR_0) form the subscription group $SubG_0$.

(3) If a consumer *subscribes to one or many CDR programs*, he only belongs to the SubG-tree corresponding to his subscription (e.g., $SubG\text{-}tree_i$). He maintains a copy of his individual symmetric key and all keys in the path from his individual symmetric key to the root of $SubG\text{-}tree_i$. Further, he maintains also a copy of all keys in the path from $SubG\text{-}tree_i$ to the GKs of the CDR programs to which he subscribed. Furthermore, he holds a copy of the broadcast key GK_0. For instance, in Figure 6, consumer C_{22} belongs to $SubG\text{-}tree_5$. Thus, he maintains the following set of keys $\{k_{22}, k_{22\text{-}24}, SK_5, SK_{4\text{-}5}, GK_3, GK_0\}$.

(4) When a consumer is not subscribed to any CDR program, he is exclusively associated with $SubG\text{-}tree_0$. In this scenario, the consumer possesses a copy of his leaf individual key as well as all the keys associated with the nodes along the path from his leaf to the broadcast key GK_0. For instance, in Figure 6, consumer C_3 is not subscribed to any CDR program, so they maintain the following set of keys: $\{k_3, k_{2\text{-}3}, k_{1\text{-}3}, SK_0, GK_0\}$.

(5) If a consumer unsubscribes from all CDR programs, he will shift to $SubG\text{-}tree_0$. After shifting to $SubG\text{-}tree_0$, the consumer can send a request to leave the IoE network.

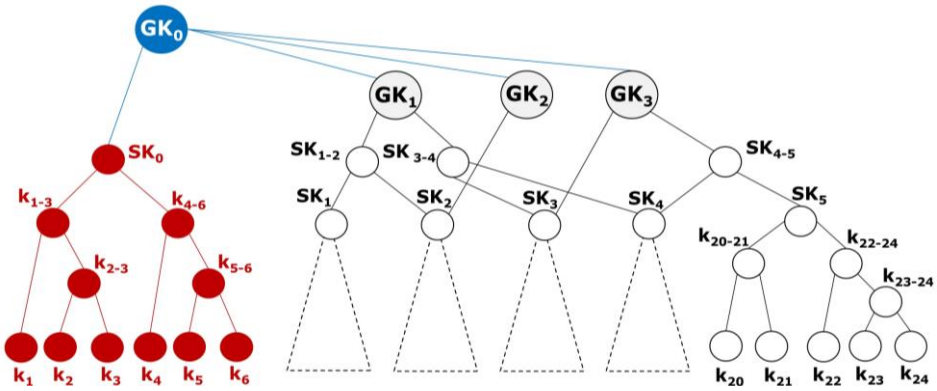

Figure 6. Example of SE-CDR multi-group key graph structure (LKH key tree degree d=2)

4.3 Key management for multicast CDR communications

In order to guarantee *collusion freedom*, we adopt LKH key tree of degree d (instead of binary OFT key trees) as the basis of the lower level in our key graph structure. In LKH, any set of consumers that unsubscribe from a CDR program can't be able to deduce the current used group key, because when any consumer leaves a CDR program, all the affected keys will be replaced and the new keys are independent. Thus, the multicast KMS preserves collusion freedom.

The multicast KMS, proposed in EDR, remains the same in SE-CDR. However, we change the standard OFT keys update process to the standard LKH keys update process in the rekeying operations. Algorithm 1 describes the rekey procedure conducted by the *CC* upon receipt of a consumer C_k's join/leave request (i.e., C_k will switch from $SubG_i$ to $SubG_j$):

(1) Let β_i^k denote the set of keys associated with C_k's *previous position in the upper level* of the key graph structure.

(2) Let β_j^k denote the set of keys associated with C_k's *new position in the upper level* of the key graph structure.

Algorithm 1: Multicast Rekeying Algorithm

1: **Procedure** MulticastRekeying (C_k, $SubG_i$, $SubG_j$)
2: *# The first phase*
Update keys in $SubG\text{-}tree_i$ and $SubG\text{-}tree_j$ using the standard LKH update mechanism;
3: *# The second phase*
Update keys in $\overline{\beta_i^k} \cap \beta_j^k$ by applying a one-way hash function;
4: Update keys in $\beta_i^k \cap \overline{\beta_j^k}$ by generating new keys and distributing them encrypted by their children node keys from bottom to up, similar to the procedure for consumer's departure in LKH protocol;

4.2 Key management for Broadcast CDR communications

In this section, we describe our new KMS for Broadcast CDR communications. It consists of the leaving and joining phases. The main idea is to use the $SubG\text{-}tree_0$ and the m group keys of CDR programs during the key update process.

4.4.1 Leaving phase

When a consumer C_i sends a request to leave the system to the *CC*, GK_0 and the other keys that C_i owns should immediately be updated to protect broadcast CDR communications from unauthorized access by this leaving consumer. To do this, the *CC* will execute the following operations (Algorithm 2):

Algorithm 2: Broadcast Leaving Algorithm

1: **Procedure** BroadcastLeaving (Ci, CDR_0)
2: Update the keys for consumers in $SubG\text{-}tree_0$ using the standard LKH update mechanism;
3: Generate the new broadcast key (GK'_0), and send it to consumers in $SubG\text{-}tree_0$ encrypted by the newly-generated SK'_0;
4: Send GK'_0 to consumers subscribed to the other CDR_j encrypted, respectively, by the j^{th} group key GK_j;

For instance, when the consumer C_5 shown in Figure 6 sends a request to leave the IoE network, the key $k_{5\text{-}6}$ is deleted and $\{k_{4\text{-}6}, SK_0\}$ are updated to $\{k'_{4\text{-}6}, SK'_0\}$ and distributed as follows:

$$CC \rightarrow \{C_6\}: Encrypt\ (k'_{4\text{-}6}, k_5) \quad (5)$$

$$CC \rightarrow \{C_4\}: Encrypt\ (k'_{4\text{-}6}, k_4) \quad (6)$$

$$CC \rightarrow \{C_4, C_6\}: Encrypt\ (SK'_0, k'_{4\text{-}6}) \quad (7)$$

$$CC \rightarrow \{C_1, C_2, C_3\}: Encrypt\ (SK'_0, k_{1\text{-}3}) \quad (8)$$

Then, the new broadcast key GK'_0 is sent to consumers in $SubG\text{-}tree_0$ as follows:

$$CC \rightarrow SubG_0: Encrypt\ (GK'_0, SK'_0) \quad (9)$$

After that, GK'_0 is sent to consumers subscribed to CDR_1, CDR_2 and CDR_3, respectively, as follows:

$$CC \rightarrow CDrG_1: Encrypt\ (GK'_0, GK_1) \quad (10)$$

$$CC \rightarrow CDrG_2: Encrypt\ (GK'_0, GK_2) \quad (11)$$

$$CC \rightarrow CDrG_3: Encrypt\ (GK'_0, GK_3) \quad (12)$$

4.4.2 Joining phase

When a new consumer C_i sends a request to join the IoE network, the broadcast key GK_0 should be updated to prevent this joining consumer from illegally accessing the previously performed broadcast CDR communications. To this end, the *CC* will add the joining consumer into the $SubG\text{-}tree_0$, update all the keys affected by the joining operation (the broadcast key GK_0, the root key of $SubG\text{-}tree_0$ and some internal keys) using a one-way hash function, and increase the counter of these new keys. Thus, the other consumers in $SubG_0$ will know about the keys change when being used and compute the new keys using the same one-way hash function. All the other consumers in $CDrG_0$ will also compute the new $GK'_0 = H(GK_0)$.

Thus, no rekeying messages are necessary for the joining phase and the *CC* has only to send keys for the newly joining consumer encrypted with its individual key.

5. SECURITY AND PERFORMANCE ANALYSIS

In this section, we delve into the examination of security and performance aspects.

5.1 Security analysis

SE-CDR scheme satisfies the following properties:

5.1.1 SE-CDR ensures forward secrecy.

A consumer who leaves a CDR program or the IoE network should not be able to access future secret keys.

Proof: When a consumer C_i sends a request to leave the IoE network, all keys known by the departing consumer in both lower and upper level (k_i, internal keys in $SubG{-}tree_0$, SK_0 and GK_0) are changed and redistributed securely by the *CC*. According to Algorithm 2, the new generated keys are independents and encrypted when being broadcasted, which prevents the departing consumer from having access to the new keys without knowing the decryption keys. On the other hand, and according to the proposed multicast key management (Section 4.3), the keys update process avoids any consumer who leaves a CDR program from decrypting the future multicast CDR communications. Hence, SE-CDR ensures forward secrecy for both broadcast and multicast communications.

5.1.2 SE-CDR ensures backward secrecy

A consumer who joins a CDR program or the IoE network should not be able to access previously used secret keys.

Proof: When a new consumer C_i sends a request to join the IoE network, the *CC* changes all the affected keys in both lower and upper level (using a one-way hash function). This ensures that none of the old keys can be recovered by the new coming consumer. Moreover, the proposed multicast key management updates all the affected keys in the *CDrG-tree* and *SubG-trees* when a new consumer joins a CDR program and the newly joined consumer can't get access to previous communications used in this CDR program. Hence, SE-CDR ensures backward secrecy for both broadcast and multicast communications.

5.1.3 SE-CDR guarantees collusion freedom

This means that a group of consumers who leave a CDR program or the IoE network should not be able to deduce the current used CDRs group keys or the current used broadcast key through collusion.

Proof: According to the rekeying operations, evicted consumers can't get the new broadcast key GK'_0 by cooperating. As SE-CDR uses LKH as the basis of both lower and upper level, whenever a consumer leaves the IoE network, all affected keys are updated. Moreover, *all the new keys are independent and unknown to any previously removed consumers*. Likewise for the multicast key management protocol. Hence, SE-CDR guarantees collusion freedom for both broadcast and multicast communications.

5.2 Performance analysis

In this section, we analyze the performance of SE-CDR with respect to two aspects: storage and communication.

Let us assume that each subscription contains the same number of consumers denoted by $\{\forall j \neq 0: |SubG_j| = |SubG|\}$. Likewise, we assume that the CDR groups contain the same number of consumers denoted by $\{\forall k \neq 0: |CDrG_k| = |CDrG|\}$. Moreover, it is assumed that used key trees are fully loaded (i.e., each node in the tree contains a key associated with it) and constructed as a balanced trees (i.e., the tree remains relatively balanced in terms of its shape, which allows for efficient search, insertion, and deletion operations).

5.2.1 Storage cost

We estimate the storage cost with the number of keys stored in SMs, and used for secure broadcast, unicast and multicast CDR communications. As mentioned earlier, the storage cost in SMs can't be neglected due to the facts that: (1) SM's storage ability is limited and (2) the secret keys need to be stored in a secure storage space [11-16]. As a result, the reduction in key storage is desirable.

Let $Stor(SM_i)$ denote the storage cost at the SM_i. In SE-CDR, two types of consumers are considered:

(1) *Consumer-Type1*: A consumer C_i who does not subscribe to any CDR program. This consumer stores: (1) the broadcast key, (2) his individual key, and (3) all keys in the path from his individual key to the root in $SubG\text{-}tree_0$. Thus, the storage cost at SM_i is:

$$Stor(SM_i) = \log_d(|SubG_0|) + 2 \tag{13}$$

When $|SubG_0| \to \infty$, Eq. (13) leads to:

$$Stor(SM_i) \sim O(\log(|SubG_0|)) \tag{14}$$

(2) *Consumer-Type2*: A consumer C_i who subscribes to one or many CDR programs. It is shown by Benmalek et al. [31] that the storage cost at SM_i is:

$$Stor(SM_i) \sim O(\log(|SubG|)) \tag{15}$$

5.2.2 Communication cost

We estimate the communication cost by considering the number of rekeying messages disseminated during the joining/leaving phase of the broadcast key management scheme. Note that, the communication cost for the multicast key management is in the order of $O(\log(|SubG|))$ for both joining and leaving phases as shown by Benmalek et al. [31].

Let $Com_{join}(C_i, CDR_0)$ and $Com_{leave}(C_i, CDR_0)$ denote the communication cost of our broadcast KMS when a consumer C_i sends a request to join/leave the IoE network.

(1) For the leaving phase, the *CC* distributes $[d\log_d(|SubG_0|) - 1]$ rekeying messages to update the keys for consumers belonging to *SubG-tree0*, and $(m+1)$ rekeying messages to update GK_0 for consumers belonging to the different DrG-trees (i.e., $CDrG\text{-}tree_j: \forall j \in [0..m]$). Therefore, the cost for one consumer departure is:

$$Com_{leave}(C_i, CDR_0) = d\log_d(|SubG_0|) + m \tag{16}$$

When $|SubG_0| \to \infty$, we can see that:

$$Com_{leave}(C_i, CDR_0) \sim O(\log(|SubG_0|)) \tag{17}$$

(2) During the joining phase, there is no need for rekeying messages. The *CC* accomplishes this by updating the

affected keys in the key graph through a one-way hash function and incrementing the counter for these new keys. As a result, other consumers in $SubG_0$ and $CDrG_0$ are informed about the key update and can calculate the new keys using the same hash function. Hence, the CC only needs to transmit keys encrypted with the individual key of the newly joining consumer, leading to minimal communication cost:

$$Com_{join}(C_i, CDR_0) \sim O(1) \quad (18)$$

6. PERFORMANCE COMPARISON

We compare our KMS with the following four schemes: KMSCC [19], SKM [20], ICN-KMS [21], and EDR [31]. We make the comparison according to the storage cost needed on consumer side and the communication cost required by the multicast/broadcast key management schemes.

6.1 Simulation model

We perform simulations with a custom script in Python to model an IoE network with the following parameters. The power utility provides the following 6 CDR programs to consumers:

(1) *Capacity Market (CM) program*: It is a dynamic mechanism designed to ensure a reliable and resilient energy system. It facilitates the exchange of capacity obligations and resources among diverse energy stakeholders, enabling efficient allocation of power generation, storage, and demand response assets. By incentivizing participants to guarantee available capacity during peak demand periods, the CM program enhances grid stability, minimizes the risk of supply shortages, and promotes the integration of renewable energy sources into the broader energy ecosystem [37].

(2) *Emergency Demand Reduction (EDR) program*: It is a responsive initiative aimed at maintaining grid stability during critical situations. By incentivizing consumers and businesses to voluntarily curtail their energy usage during peak demand or emergency events, the EDR program effectively reduces strain on the energy infrastructure. This demand-side approach enhances grid resilience, prevents potential blackouts, and supports the overall reliability of the energy system, while also contributing to broader energy efficiency and sustainability goals [8].

(3) *Direct Load Control (DLC) program*: It is a strategic mechanism for managing energy demand in real-time. Through this program, utility providers or grid operators can remotely adjust the energy consumption of specific appliances or loads during periods of high demand or supply constraints. By temporarily reducing or shifting the energy usage of enrolled participants, the DLC program optimizes grid stability, mitigates the risk of overloads, and promotes efficient energy utilization [10].

(4) *Time-of-Use (ToU) program*: It is a dynamic pricing strategy that encourages electricity consumers to adapt their usage patterns based on varying energy demand throughout the day. Under this program, electricity rates are structured to reflect peak and off-peak periods, incentivizing users to shift their energy-intensive activities to times when demand and costs are lower. By promoting more efficient energy consumption during off-peak hours and reducing strain on the grid during peak times, the ToU program optimizes overall system efficiency, minimizes energy costs, and fosters a more sustainable energy consumption behavior among consumers and businesses [36].

(5) *Real-Time Pricing (RTP) program*: It is a responsive pricing mechanism that reflects the actual, moment-to-moment fluctuations in electricity supply and demand. This program provides consumers with real-time pricing information that aligns with the dynamic conditions of the energy market. By offering varying rates throughout the day based on grid conditions, the RTP program incentivizes users to adjust their energy consumption in sync with market fluctuations, encouraging them to reduce usage during high-demand periods and capitalize on lower-cost periods. This approach enhances grid stability, optimizes energy utilization, and empowers consumers to make informed choices about their energy consumption, promoting efficiency and sustainability in the broader energy ecosystem [9].

(6) *Critical Peak Pricing (CPP) program*: It is a dynamic pricing strategy designed to address periods of exceptionally high electricity demand. Under this program, consumers are charged higher rates during designated critical peak periods when energy demand is at its highest and the grid is under stress. By providing advance notice of these peak periods, the CPP program encourages participants to curtail their energy usage or shift it to off-peak times, thereby reducing strain on the grid during crucial moments. This approach enhances grid stability, minimizes the risk of blackouts, and encourages energy-efficient behavior while enabling consumers to manage their costs more effectively [38].

We assume that 50% of the Consumers-Type2 only subscribe to one CDR program and 50% subscribe to multiple CDR programs [39]. In the Key Management Scheme (KMS) proposed herein, 4-ary key trees are employed, echoing the findings of previous investigations which demonstrated that the Logical Key Hierarchy (LKH) key tree exhibits optimal performance when $d = 4$ [36, 40, 41].

6.2 Simulation results

6.2.1 Storage cost

Figure 7 shows the average storage cost at SMs for *Consumers-Type1* (i.e., who do not subscribe to any CDR program) with respect to $CDrG_0$ group's size. In KMSCC and ICN-KMS, the storage cost is not affected by the number of consumers in $CDrG_0$ (the storage cost is equal to 2) because each consumer only stores his individual key and the broadcast group key. Moreover, SE-CDR (which is key graph-based scheme) produces little more storage cost compared to the two other schemes. However, this cost is minor regarding the overall advantages of SE-CDR, mainly when considering the low communication cost induced during the broadcast rekeying operations. Indeed, KMSCC and ICN-KMS do not exploit the advantage of key graph during the broadcast key management. As a consequence, these two schemes induces low storage cost (in the order of $O(1)$) and very high communication cost.

Figure 8 shows the average storage cost at SMs for *Consumers-Type2* (i.e., who subscribe to one or many CDR programs) with respect to the number of subscribers in CDR programs under the assumption that the power utility provides 6 CDR programs. In both KMSCC and ICN-KMS, a SM only stores his individual key and the *CDrG* group keys. As a consequence, the *CDrG* groups size does not affect the storage cost (which is in the order of $O(1)$). Whereas, SKM, EDR and SE-CDR adopt a key graph technique to manage the different

CDrG groups. Thus, the *CDrG* groups size affects the storage cost for these schemes. As the number of consumers subscribed to CDR programs increases, the storage cost increases due to the rise of the height of the used key trees. However, SE-CDR decreases the storage cost by 73% and by 39%, respectively, compared with SKM and EDR.

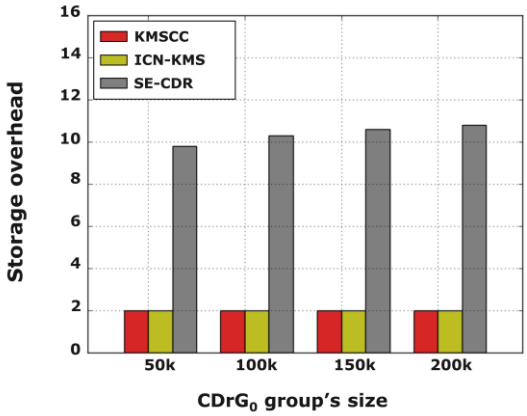

Figure 7. Storage cost for Consumer-Type1 with respect to *CDrG₀* group's size

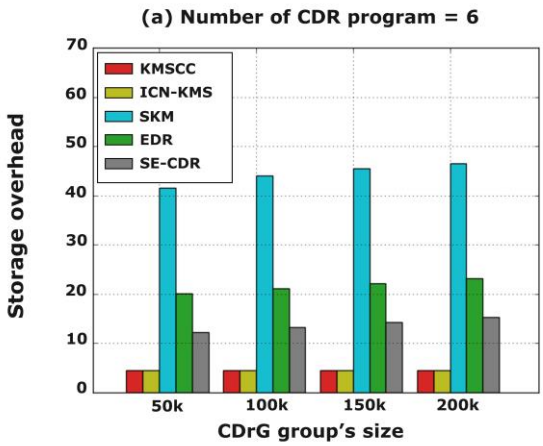

Figure 8. Storage cost for Consumer-Type2 with respect to *CDrG* group's size

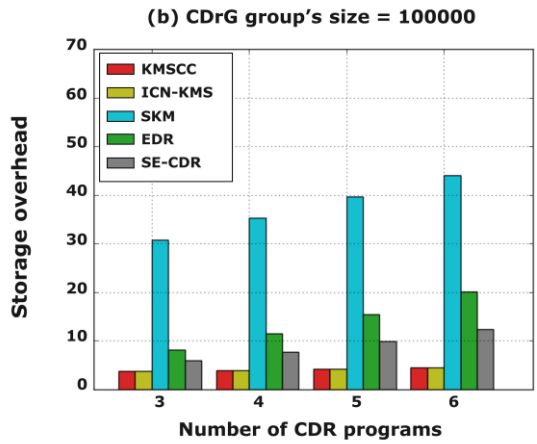

Figure 9. Storage cost for Consumer-Type2 with respect to the number of CDR programs

Figure 9 shows how the storage cost varies for *Consumers-Type2* as a function of the number of provided CDR programs. We assume that an average number of 100000 consumers subscribe to each CDR program. We note that the storage costs of the two schemes KMSCC and ICN-KMS (which do not adopt a key graph technique as mentioned earlier) are less affected by the number of CDR programs than the other schemes (i.e., SKM, EDR, and SE-CDR). In the key graph-based schemes, we can notice that in SE-CDR, a smart meter retains significantly fewer keys compared to the two other schemes SKM and EDR. Indeed, since SKM uses and independent-tree for each CDR program, the storage cost increases proportionally with the number of subscribed CDR programs.

From the above results, it is seen that our proposed scheme SE-CDR is less sensitive to the *CDrG* group's size and the number of provided CDR programs compared to the other key graph-based schemes (i.e., SKM and EDR), and it can reduce the per-consumer storage cost more efficiently.

6.2.2 Communication cost

(1) *Multicast key management*

Figure 10 and Figure 11 show the average number of rekeying messages per event (join/leave) with respect to the number of subscribers in CDR programs under the assumption that the power utility provides 6 CDR programs (as mentioned in Section 6.1). In both KMSCC and ICN-KMS, when a consumer subscribes/unsubscribes to/from a CDR program (CDR_i) the *CC* updates the CDR_i's group key and sends the new key individually for all consumers subscribed to this CDR program. Thus, the communication cost increases linearly with the number of CDR program subscribers (which is in the order of $O(|CDrG_i|)$, with $|CDrG_i|$ being the number of consumers subscribed to CDR_i). Whereas, the cost remains much lower in the other schemes (i.e., SKM, EDR and SE-CDR) as shown in Figure 11. Through the used key-graph structure, the rekeying efficiency of EDR and SE-CDR is decreased compared to SKM (which is based on the usage of multiple separate OFT key trees). However, the extra communication cost induced by EDR and SE-CDR remains minimal when compared to the benefits of these schemes, mainly when considering the storage cost as indicated above.

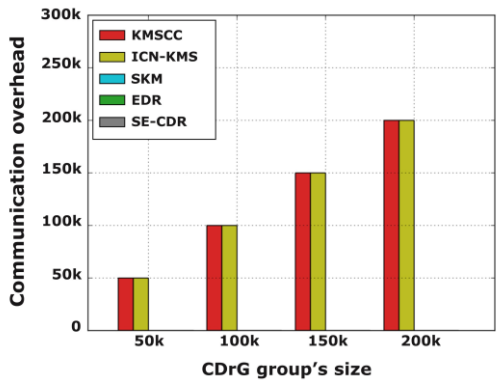

Figure 10. Average multicast communication cost with respect to *CDrG* group's size

Figure 12 and Figure 13 show the average number of rekeying messages per event against the number of CDR programs. We consider CDR programs of average 100000 subscribers. This indicates that the communication costs of KMSCC and ICN-KMS are significantly greater compared to the other three schemes due to their inefficient multicast key

management. On the other hand, SKM is less affected by the number of CDR programs. However, the use of multiple OFT key trees requires larger storage cost when the number of CDR programs increases. Moreover, we notice that the number of provided CDR programs does not significantly affect the communication cost of EDR and SE-CDR due to the proposed key graph structure.

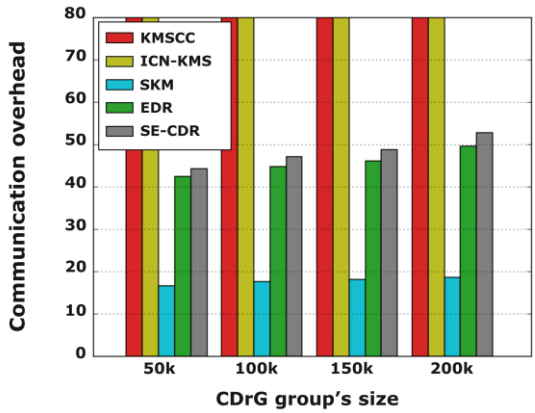

Figure 11. Zoom of Figure 10

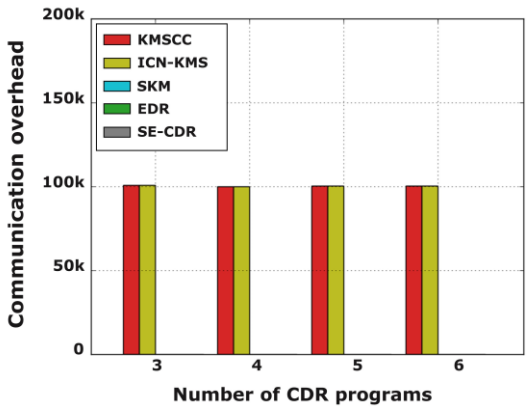

Figure 12. Average multicast communication cost with respect to number of CDR programs

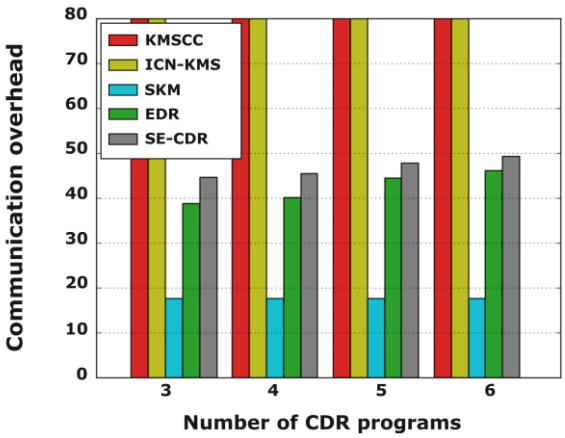

Figure 13. Zoom of Figure 12

(2) *Broadcast key management*

According to Table 2, SKM and EDR do not have the capability to facilitate secure broadcast CDR communications, which is a crucial aspect with diverse applications in CDR management. However, the three other schemes (KMSCC, ICN-KMS and SE-CDR) are versatile.

Figure 14 and Figure 15 show a comparison of communication cost per event (leave/join) for the three schemes (KMSCC, ICN-KMS and SE-CDR) with respect to the number of *Consumers-Type1*. We consider CDR programs of average 100000 subscribers.

Figure 14 and Figure 15 show that the average broadcast communication cost in KMSCC and ICN-KMS is remarkably high. In fact, it scales with the total number of consumers in the Internet of Energy (IoE) network, denoted as *N*, following an order of *O(N)*. Moreover, this cost increases linearly as the size of the $CDrG_0$ group grows. In contrast, the SE-CDR scheme shows significantly lower communication cost compared to the other two schemes.

The efficiency of SE-CDR originates from its streamlined broadcast rekeying process. This efficient approach significantly minimizes the volume of rekeying messages that are exchanged during both the joining and leaving phases of the system. By implementing this optimized procedure, SE-CDR markedly reduces the communication cost that is typically associated with such cryptographic systems. Impressively, SE-CDR achieves an exceptional reduction of over 99% when compared to the two other methods KMSCC and INC-KMS. This not only demonstrates SE-CDR's superior efficiency but also underscores its potential to drastically enhance resource utilization, communication speed, and overall system performance within cooperative data replication scenarios.

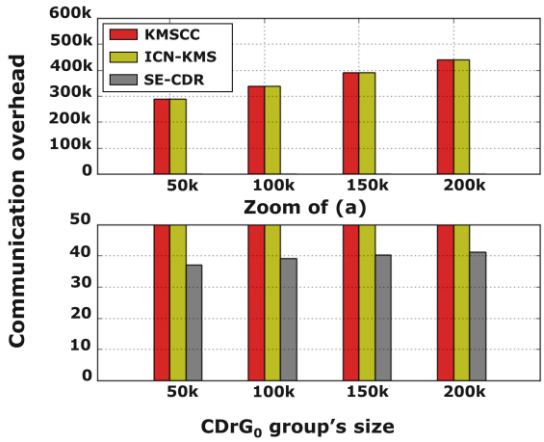

Figure 14. Average broadcast communication cost per "leave event" with respect to $CDrG_0$ group's size

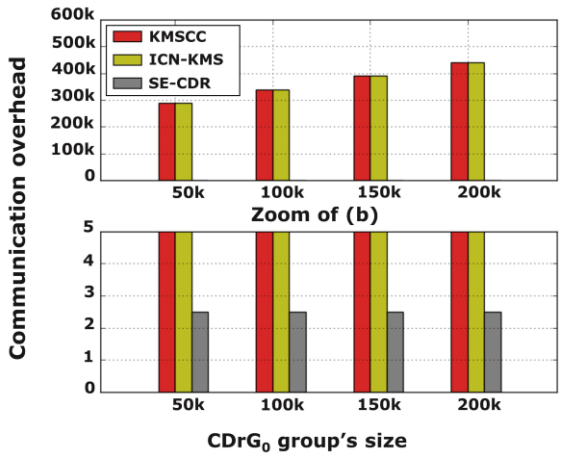

Figure 15. Average broadcast communication cost per "join event" with respect to $CDrG_0$ group's size

Table 2. Comparison of key management schemes

				[19]	[20]	[21]	[31]	SE-CDR
Security	Immediate keys update			✓	✓	✓	✓	✓
	Forward secrecy			✓	x	✓	x	✓
	Backward secrecy			✓	x	✓	x	✓
	Collusion freedom			✓	x	✓	x	✓
Versatility	Unicast communications			✓	✓	✓	✓	✓
	Multicast communications			✓	✓	✓	✓	✓
	Broadcast communications			✓	x	✓	x	✓
Efficiency	Storage cost	Consumer-Type1		*O(1)*	-	*O(1)*	-	*O(log(|SubG₀|))*
		Consumer-Type2		*O(1)*	*O(log(|CDrG|))*	*O(1)*	*O(log(|SubG|))*	*O(log(|SubG|))*
	Communication cost	Multicast	Join	*O(|CDrG|)*	*O(log(|CDrG|))*	*O(|CDrG|)*	*O(log(|SubG|))*	*O(log(|SubG|))*
			Leave	*O(|CDrG|)*	*O(log(|CDrG|))*	*O(|CDrG|)*	*O(log(|SubG|))*	*O(log(|SubG|))*
		Broadcast	Join	*O(N)*	-	*O(N)*	-	*O(1)*
			Leave	*O(N)*	-	*O(N)*	-	*O(log(|SubG₀|))*

7. CONCLUSION

In this work, we proposed new efficient, versatile, secure and scalable KMS for CDR communications. We have identified weaknesses in EDR scheme. To remedy its security and efficiency flaws, we have proposed a more secure and efficient KMS (called SE-CDR), which allows dynamic and multiple CDR programs' subscriptions while ensuring the immediate key update, group secrecy, forward/backward secrecy and collusion freedom. Our performance analysis and simulations reveal that SE-CDR induces low storage cost at consumers' SM in comparison to existing schemes. Moreover, the communication cost induced by SE-CDR is far less than all other schemes. Hence, SE-CDR fulfills the diverse requirements of the power utility. As a potential avenue for future research, the development of a more advanced statistical dynamic membership model would allow for a comprehensive examination of the impact of consumer behaviors and a more thorough assessment of the efficiency of our scheme.

REFERENCES

[1] Bui, N., Castellani, A.P., Casari, P., Zorzi, M. (2012). The internet of energy: A web-enabled smart grid system. IEEE Network, 26(4): 39-45. https://doi.org/10.1109/MNET.2012.6246751

[2] Aguida, M.A., Ouchani, S., Benmalek, M. (2020). A review on cyber physical systems: Models and architectures. 2020 IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), pp. 1-4. https://doi.org/10.1109/WETICE49692.2020.00060

[3] Deng R., Yang, Z.Y., Chow, M.Y., Chen, J.M. (2015). A survey on demand response in smart grids: mathematical models and approaches. IEEE Transactions on Industrial Informatics, 11(3): 570-582. https://doi.org/10.1109/TII.2015.2414719

[4] Albadi, M., El-Saadany, E. (2008). A summary of demand response in electricity markets. Electric Power Systems Research, 78(11): 1989-1996. https://doi.org/10.1016/j.epsr.2008.04.002

[5] Ancillotti, E., Bruno, R., Conti, M. (2013). The role of communication systems in smart grids: Architectures, technical solutions and research challenges. Computer Communications, 37(17-18): 1665-1697. https://doi.org/10.1016/j.comcom.2013.09.004

[6] Fan, Z., Kulkarni, P., Gormus, S., Efthymiou, C., Kalogridis, G., Sooriyabandara, M., Zhu, Z., Lambotharan, S., Chin, W.H. (2013). Smart grid communications: overview of research challenges, solutions, and standardization activities. IEEE Communications Surveys & Tutorials, 15(1): 21-38. https://doi.org/10.1109/SURV.2011.122211.00021

[7] Kuzlu, M., Pipattanasomporn, M., Rahman, S. (2014). Communication network requirements for major SG applications in HAN, NAN and WAN. Computer Networks, 67: 74-88. https://doi.org/10.1016/j.comnet.2014.03.029

[8] Tyagi, R., Black, J.W. (2010). Emergency demand response for distribution system contingencies. Proceedings of IEEE PES T&D, pp. 1-4. https://doi.org/10.1109/TDC.2010.5484598

[9] Tan, R., Krishna, V.B., Yau, D.K.Y., Kalbarczyk, Z. (2015). Integrity attacks on real-time pricing in electric power grids. ACM Transactions on Information and System Security, 18(2): 5:1-5:33. https://doi.org/10.1145/2790298

[10] Ericson, T. (2009). Direct load control of residential water heaters. Energy Policy, 37(9): 3502-3512. https://doi.org/10.1016/j.enpol.2009.03.063

[11] Li, H., Lu, R., Zhou, L., Yang, B., Shen, X. (2014). An efficient Merkle-tree-based authentication scheme for smart grid. IEEE Systems Journal, 8(2): 655-663. https://doi.org/10.1109/jsyst.2013.2271537

[12] Das, S., Ohba, Y., Kanda, M., Famolari, D., Das, S.K. (2013). A key management framework for AMI in SG. IEEE Communications Magazine, 50(8): 30-37. https://doi.org/10.1109/MCOM.2012.6257524

[13] Benmalek, M., Challal, Y. (2015). eSKAMI: Efficient and scalable multi-group key management for advanced metering infrastructure in smart grid. 2015 IEEE Trustcom/BigDataSE/ISPA, pp. 782-789. https://doi.org/10.1109/Trustcom.2015.447

[14] Benmalek, M., Challal, Y. (2016). MK-AMI: Efficient multi-group key management scheme for secure communications in AMI systems. 2016 IEEE Wireless Communications and Networking Conference, pp. 1-6. https://doi.org/10.1109/WCNC.2016.7565124

[15] Liu, Y., Cheng, C., Gu, T., Jiang, T., Li, X. (2016). A lightweight authenticated communication scheme for smart grid. IEEE Sensors Journal, 16(3): 836-842. https://doi.org/10.1109/JSEN.2015.2489258

[16] Benmalek M., Challal Y., Derhab A. (2019).

Authentication for smart grid AMI systems: Threat models, solutions, and challenges. 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), pp. 208-213. https://doi.org/10.1109/WETICE.2019.00052

[17] Wu, D., Zhou, C. (2011). Fault-tolerant and scalable key management for smart grid. IEEE Transactions on Smart Grid, 2(2): 375-381. https://doi.org/10.1109/TSG.2011.2120634

[18] Xia, J., Wang, Y. (2012). Secure key distribution for the smart grid. IEEE Transactions on Smart Grid, 3(3): 1437-1443. https://doi.org/10.1109/TSG.2012.2199141

[19] Liu, N., Chen, J., Zhu, L., Zhang, J., He, Y. (2013). A key management scheme for secure communications of advanced metering infrastructure in smart grid. IEEE Transactions on Industrial Electronics, 60(10): 4746-4756. https://doi.org/10.1109/TIE.2012.2216237

[20] Yu, K., Arifuzzaman, M., Wen, Z., Zhang, D., Sato, T. (2015). A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid. IEEE Transactions on Instrumentation & Measurement, 64(8): 2072-2085. https://doi.org/10.1109/TIM.2015.2444238

[21] Wan, Z., Wang, G., Yang, Y., Shi, S. (2014). SKM: scalable key management for advanced metering infrastructure in smart grids. IEEE Transactions on Industrial Electronics, 61(12): 7055-7066. https://doi.org/10.1109/TIE.2014.2331014

[22] Tsai, J.L., Lo, N.W. (2016). Secure anonymous key distribution scheme for smart grid. IEEE Transactions on Smart Grid, 7(2): 906-914. https://doi.org/10.1109/TSG.2015.2440658

[23] Odelu, V., Das, A.K., Kumari, S., Huang, X.Y., Wazid, M. (2017). Provably secure authenticated key agreement scheme for distributed mobile cloud computing services. Future Generation Computer Systems, 68: 74-88. https://doi.org/10.1016/j.future.2016.09.009

[24] Yan, L., Chang, Y., Zhang, S. (2017). A lightweight authentication and key agreement scheme for smart grid. International Journal of Distributed Sensor Networks, 13(2): 1-7. https://doi.org/10.1177/1550147717694173

[25] Mahmood, K., Chaudhry, S.A., Naqvi, H., Kumari, S., Li, X., Sangaiah, A.K. (2018). An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. Future Generation Computer Systems, 81: 557-565. https://doi.org/10.1016/j.future.2017.05.002

[26] Abbasinezhad-Mood, D., Nikooghadam, M. (2018). Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications. Future Generation Computer Systems, 84: 47-57. https://doi.org/10.1016/j.future.2018.02.034

[27] Benmalek, M., Challal, Y., Derhab, A., Bouabdallah, A. (2018). VerSAMI: Versatile and scalable key management for smart grid AMI systems. Computer Networks, 132: 161-179. https://doi.org/10.1016/j.comnet.2018.01.010

[28] Mohammadali, A., Sayad Haghighi, M., Tadayon, M.H., Mohammadi-Nodooshan, A. (2018). A novel identity-based key establishment method for advanced metering infrastructure in smart grid. IEEE Transactions on Smart Grid, 9(4): 2834-2842. https://doi.org/10.1109/TSG.2016.2620939

[29] Zhang, L., Zhao, L.C., Yin, S.J., Chi, C.H., Liu, R., Zhang, Y.X. (2019). A lightweight authentication scheme with privacy protection for SG communications. Future Generation Computer Systems, 100: 770-778. https://doi.org/10.1016/j.future.2019.05.069

[30] Gope, P. (2020). PMAKE: Privacy-aware multi-factor authenticated key establishment scheme for advance metering infrastructure in smart grid. Computer Communications, 152: 338-344. https://doi.org/10.1016/j.comcom.2019.12.042

[31] Benmalek, M., Challal, Y., Derhab, A., Gheid, Z. (2020). An efficient key management scheme for secure demand-response communications in smart grid. 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), pp. 1-6. https://doi.org/10.1109/AECT47998.2020.9194168

[32] Xiang, X., Cao, J. (2022). An efficient authenticated key agreement scheme supporting privacy-preservation for SG communication. Electric Power Systems Research, 203: 107630. https://doi.org/10.1016/j.epsr.2021.107630

[33] Nkurunziza, E., Tandoh, L., Elfadul, I., Li, F. (2022). ECAAP-SG: Efficient certificateless anonymous authentication protocol for Smart Grid. Security and Privacy, 6(1): e273. https://doi.org/10.1002/spy2.273

[34] Shariat, M., Safkhani, M. (2017). How the control over smart meters is lost in the Yan et al. lightweight AKA scheme for smart grids. 2017 9th International Conference on Information and Knowledge Technology, pp. 82-84. https://doi.org/10.1109/IKT.2017.8258622

[35] Grew, D.A.M., Sherman, A.T. (2003). Key establishment in large dynamic groups: using one-way function trees. IEEE Transactions on Software Engineering, 29(5): 444-458. https://doi.org/10.1109/TSE.2003.1199073

[36] Wong, C.K., Gouda, M., Lam, S. (2000). Secure group communication using key graphs. IEEE/ACM Transactions on Networking, 8(1): 16-30. https://doi.org/10.1109/90.836475

[37] Herter K. (2007). Residential implementation of critical-peak pricing of electricity. Energy Policy, 35(4): 2121-2130. https://doi.org/10.1016/j.enpol.2006.06.019

[38] Albadi, M.H., El-Saadany, E.F. (2008). A summary of demand response in electricity markets. Electric Power Systems Research, 78(11): 1989-1996. https://doi.org/10.1016/j.epsr.2008.04.002

[39] Benmalek, M., Challal, Y., Derhab, A. (2019). An improved key graph based key management scheme for smart grid AMI systems. 2019 IEEE Wireless Communications and Networking Conference, pp. 1-6. https://doi.org/10.1109/WCNC.2019.8885646

[40] Bruhadeshwar, B., Kulkarni, S.S. (2011). Balancing revocation and storage trade-offs in secure group communication. IEEE Transactions on Dependable and Secure Computing. 8(1): 58-73. https://doi.org/10.1109/TDSC.2009.27

[41] Mehdizadeh, A., Hashim, F., Othman, M. (2014). Lightweight decentralized multicast–unicast key management method in wireless IPv6 networks. Journal of Network and Computer Applications. 42: 59-69. https://doi.org/10.1016/j.jnca.2014.03.013