Lightweight Key Management Scheme for Wireless Communication System of Distribution Network

Lingda Kong1, Feng Zhai1, Yingjie Zhao1, Liying Yu2*, Junhao Zhou2, Peng Yan2, Shaotang Cai2

1 China Electric Power Research Institute, Beijing, 100192, China
2 Tianjin University, Tianjin, 300010, China

*Corresponding author’s e-mail: yly@tju.edu.cn

ABSTRACT: Key management is the key to ensuring the information security of the intelligent distribution network. Based on the analysis of the communication characteristics and key management requirements of the intelligent distribution network, this paper proposes a lightweight intelligent distribution network key management scheme DNKMS. According to the storage and computing capabilities of power distribution terminals, electronic distribution stations and power distribution master stations, task distribution is optimized, and the design idea of the scheme and the process of key generation, distribution, update, and destruction are described in detail. The analysis results show that the proposed scheme has less time overhead and higher efficiency, can reduce the communication and calculation load required in key management, and meet the security requirements of key management in smart distribution networks.

1. Introduction

The wireless communication system of the distribution network is an important part of the power system. As a carrier of various information transmission in the distribution network, it is used to realize the information exchange between the distribution terminal and the system. It has multi-service bearing, information transmission, and network management and other functions [1]. As an important link in the smart grid, the distribution network has complex information security requirements, and faces severe information security threats [2]. Encrypted transmission of information using modern cryptographic methods is a common measure to ensure information security. Not only that, the security of keys is the key to various cryptographic systems and an important prerequisite for cryptographic systems to effectively ensure information security [3-4]. Therefore, an efficient key management scheme is very important to the security of the wireless communication system of the distribution network.

[5] proposed a key management scheme based on elliptic curve cipher and symmetric encryption algorithm, which is suitable for the overall key management requirements of smart grid and has good scalability. However, this scheme cannot resist man-in-the-middle attacks. [6] proposed an efficient identity verification and key management mechanism for smart grid communication based on the PKI mechanism, which has a large amount of calculation and high bandwidth requirements. [7] proposed a lightweight smart substation key management method that considers substation information interaction and IED processing capabilities. But this scheme has less analysis of key management security. [8] proposed a lightweight key management scheme suitable for charging piles, which can resist replay, forgery and man-in-the-middle attacks, and has computational overhead and the key storage space is
small, but this method does not consider the conflict problem caused by the unsynchronized key update message. [9] designed an information center network method ICN-AMI specifically for the smart grid advanced measurement system (AMI), which can support mobility and control network congestion.

In this paper, we propose a lightweight distribution network wireless communication system key management scheme (Distribution Network Key Management Scheme, DNKMS). First, analyze the communication characteristics and key management requirements of the wireless communication system of the distribution network; secondly, design the overall architecture of the key management scheme of the wireless communication system of the distribution network, and divide the system into power distribution terminals, power distribution stations and power distribution master stations. Then, design the key management program process, including key generation, key distribution, key update and key destruction methods; finally, conduct security analysis and efficiency analysis on DNKMS.

2. Model description
The key management scheme in this article makes some assumptions based on the actual situation of the distribution network. Specific assumptions include:

(1) Social factors: The staff involved in the key management of the distribution network are honest and reliable, and will not disclose any key information related to network security.

(2) Physical factors: The physical medium used to store private information such as keys is unbreakable, it has physical security protection measures such as fire prevention, anti-theft, and anti-vandalism, and will not cause the leakage of private information due to external accidents or attacks.

(3) Encryption algorithm: The attacker will not use brute force cracking methods to encrypt the information within the validity period of the key. The encryption algorithm used in the key management scheme is safe.

According to the characteristics of the hierarchical structure of the power distribution system, a three-tier key management scheme consisting of distribution stations, distribution master stations and distribution terminals is established, as shown in Figure 1. Add a lightweight key management module to the information platform of the distribution station and the distribution master station. The key management module of the distribution master station performs key management information communication with the power distribution station through the power communication backbone network. The key management module communicates key management information with the lower-level distribution terminal and the upper-level distribution master station.

In order to achieve lightweight management of keys based on ensuring key security, the key management scheme in this paper is designed to use three types of keys, namely the main key $Key_M$, the session key $Key_S$ and the temporary key $Key_T$. $Key_M$ is a key based on the unique ID of the device. It is used to encrypt and distribute $Key_S$ messages and messages to update $Key_S$ when the device exits. $Key_S$ is the key used to encrypt and decrypt messages between the power distribution master station, the power distribution station, and the power distribution terminal during normal operation. $Key_T$ is a temporarily generated key subject to time constraints, and is used to encrypt the message that distributes $Key_M$ to the newly added device.
In order to save management overhead and improve distribution efficiency, the power distribution master station generates a key library before the key distribution. When the key is distributed to the power distribution terminal and the electronic distribution station, the random number generation method is used directly from the key library extract $Key_M$ and $Key_S$.

$Key_T$ is used as the transition of key initialization between the distribution station and the distribution terminal. It is destroyed after one use and is time-constrained and distributed manually during the device initialization phase, and keeps secrets from other members except those that need to be initialized.

$Key_M$ corresponds to the unique identification of the device in the wireless communication system of the power distribution network. The hardware serial number of the distribution terminal or distribution station is used to generate $Key_T$. It is used to realize the operation of $Key_M$ request distribution and complete the negotiation certification. Take the distribution terminal master key distribution process as an example:

**Step1:** Distribute $Key_T$ to the distribution terminal manually, and the distribution terminal uses $Key_T$ to encrypt the request message of $Key_M$. The distribution terminal sends the encrypted message to the distribution station, and the message content includes the distribution terminal identity $ID$, timestep $Q$, and $Key_M$ request information. The timestep $Q$ is only used for this $Key_M$ request, which has time-sensitive characteristics and can effectively prevent replay attacks.

**Step2:** After the distribution station receives the $Key_M$ request message, it uses a random number generation algorithm to select a key from the key library as $Key_M$, and makes it uniquely correspond to the identity of the distribution terminal. Then the distribution station uses the $Key_T$ of the distribution terminal to encrypt the distribution message of $Key_M$, and sends the encrypted message to the distribution terminal. The message content includes the distribution terminal identity $ID$, timestep $Q$, and $Key_M$.

**Step3:** After receiving the $Key_M$ distribution message, the distribution terminal uses $Key_T$ to decrypt the message to obtain $Key_M$. Then, the distribution terminal uses the obtained $Key_M$ to encrypt the master key to confirm the received message and send the message to the distribution station. The message content includes the distribution terminal identity $ID$, timestep $Q$, and $Key_M$ reception information.

**Step4:** After the distribution station receives the $Key_M$ received message, it uses $Key_M$ to encrypt the message that the master key distribution ends, and sends the message to the distribution terminal. The content of the message includes the electronic distribution station identity $ID$, timestep $Q$ and $Key_M$ distribution end information. At this time, $Key_M$ is successfully enabled and $Key_T$ will be destroyed.

In the same way, the distribution of the $Key_M$ of the electronic distribution station can also be
realized by the above method.

*Key*$_S$ is used for the communication between the distribution terminal and the distribution station, the distribution station and the distribution master station. Take the distribution terminal session key distribution process as an example:

Step1: The distribution station randomly selects multiple keys from the key library as *Key*$_S$, and makes each *Key*$_S$ uniquely correspond to the identity of each distribution terminal. Then the distribution station uses the *Key*$_M$ of the distribution terminal to encrypt the distribution message of *Key*$_S$, and sends the encrypted message to each distribution terminal in a multicast manner. The message content includes the timestep $Q$ and *Key*$_S$.

Step2: After receiving the *Key*$_S$ distribution message, the distribution terminal uses *Key*$_M$ to decrypt the message to obtain *Key*$_S$. Then, the distribution terminal uses the obtained *Key*$_S$ to encrypt the session key to confirm the received message and send the message to the electronic distribution station. The message content includes the distribution terminal identity ID, timestep $Q$, and *Key*$_S$ reception information.

Step3: After the distribution station receives the *Key*$_S$ received message, it uses *Key*$_S$ to encrypt the message after the session key distribution ends, and sends the message to each distribution terminal in a multicast manner. The message content includes timestep $Q$ and *Key*$_S$ distribution end information. At this time, *Key*$_S$ is successfully enabled.

The master key is used when the session key is distributed and updated, so the update cycle can be longer. We set the master key update cycle as the maintenance cycle of the distribution station or distribution terminal, that is, months or years.

When a new distribution terminal joins the network, other terminal devices in the same jurisdiction need to update the session key to prevent *Key*$_S$ from being cracked back. The session key update process is like the session key distribution process. The difference is that the key update process is that the distribution station uses the current session key *Key*$_S$ to encrypt the new *Key*$_S$ distribution message, while the key distribution process uses the *Key*$_M$ encryption.

When a distribution terminal needs to exit the network, other terminal devices in the same jurisdiction also need to update the session key to prevent *Key*$_S$ from being leaked. Different from the key update process when a new terminal joins the network, the terminal exits the session key update process in which the distribution station uses the *Key*$_M$ to encrypt the distribution message of the new *Key*$_S$. This is because if the attacker obtains the current *Key*$_S$ of the exit terminal, the session key update message can be decrypted through the current *Key*$_S$, which makes the key update meaningless.

When the network is in a stable state, the session key still needs to be updated regularly to ensure network security. The session key periodical update process is like the session key update process when a new terminal joins. The current session key *Key*$_S$ is used to encrypt the new *Key*$_S$ distribution message.

When a distribution terminal or distribution station exits, the *Key*$_M$ shared with the device stored in the upper level device needs to be destroyed. When the master key is updated, the old master keys stored by all device members need to be destroyed. When the session key update is completed, the old session keys stored by all device members need to be destroyed to save storage space.

4. Experimental simulation analysis

Time overhead is mainly divided into computing time overhead and transmission time overhead. We take the successful completion of the session key distribution process during group initialization of $x$ ($x \geq 2$) terminals as an example to analyze the time overhead of DNKMS and NSSK [12].

In the key distribution process, each station and terminal must perform various operations such as encryption, decryption, and timeliness judgment. Among these operations, the time of encryption and decryption far exceeds other operations. Therefore, we only consider the process of the device performing encryption and decryption operations. The time for the distribution station to complete a data encryption and decryption is recorded as $T_{\text{Station} \_E}$ and $T_{\text{Station} \_D}$, and the time for the distribution terminal to complete a data encryption and decryption is recorded as $T_{\text{End} \_E}$ and $T_{\text{End} \_D}$. 
In the NSSK scheme, the distribution station performs \( x-1 \) encryption operations and \( x \) decryption operations. As the responder node with the largest amount of calculation, the distribution terminal has 1 encryption operation and 2 decryption operations. However, the electronic station in the DNKMS in this project has \( 2x \) encryption operations and \( x \) decryption operations. The initiator of key distribution in DNKMS is the distribution station. Therefore, all distribution terminals perform the same operation, and each distribution terminal completes a total of 1 encryption operation and 2 decryption operations.

| Key management scheme | Operating time cost of distribution station | Operating time cost of distribution terminal | Transmission time overhead |
|-----------------------|--------------------------------------------|---------------------------------------------|---------------------------|
| NSSK                  | \( xT_{Station}E \)                         | \( (x-1)T_{End}E + xT_{End}D \)            | \( 3x-1\) \( T_{Trans} \) |
| DNKMS                 | \( 2xT_{Station}E + xT_{Station}D \)       | \( T_{End}E + 2T_{End}D \)                 | \( 3x\) \( T_{Trans} \) |

To simplify the analysis, we assume that the single transmission time between each device in the wireless communication system of the distribution network is fixed and equal, denoted as \( T_{Trans} \). NSSK has a total of \( 3x-1 \) data transmission processes, while DNKMS has completed a total of \( 3x \) data transmission processes. In summary, the time overhead results of NSSK and DNKMS are shown in Table 1.

It can be seen from Table 1 that the transmission time overhead of the two schemes is basically the same. DNKMS is much larger than NSSK in terms of computing time overhead of electronic distribution stations. However, the computing time overhead of the distribution terminal in DNKMS is much smaller than that of NSSK. Considering that the data processing capability of the distribution station is much better than that of the distribution terminal, the overall efficiency of the DNKMS is better than NSSK.

Assuming the total number of distribution stations is \( N_{Station} \), the number of distribution terminals that each distribution station is responsible for is \( N_{End} \), the intra-station communication group that each distribution terminal participates in is \( M_{Inter} \), the inter-station communication group that each distribution terminal participates in is \( M_{Exter} \), and each distribution station is responsible for the number of distribution terminals participating in cross-site communication is \( H_{Exter} \).

The keys that the distribution terminal needs to save include its own master key, intra-site session key, and cross-site session key. It is easy to know that the numbers are \( 1 \), \( M_{Inter} \), and \( M_{Exter} \). The keys to be stored in the distribution station are more complicated, including:

\[
(1, N_{End}, 1, \sum_{Inter=1}^{N_{End}} M_{Inter}, \sum_{Inter=1}^{N_{End}} M_{Exter})
\]

which means own master key, master key of the distribution terminal, session key with the distribution master station, session keys in the distribution terminal station and station session keys.

The distribution master station needs to communicate with the distribution station and manage cross-site information. Therefore, the keys to be stored including:

\[
(N_{Station}, N_{Station}, \sum_{Exter=1}^{N_{Exter}} \sum_{Exter=1}^{H_{Exter}} M_{Exter})
\]

which means master keys for the distribution station, session keys for the distribution station and the distribution master station, and cross-site session keys.

Note that if the distribution master station stores the session keys in the station, the number of corresponding stored session keys in the station will reach

\[
\sum_{Inter=1}^{N_{End}} \sum_{Inter=1}^{N_{End}} M_{Inter}
\]

which is very large. The distribution master station does not directly communicate with the distribution terminal, so the distribution master station does not store the master key of the distribution terminal. Based on ensuring the total number of keys that need to be stored is as small as possible, the distribution station and the power distribution master station share more key storage tasks, and the low-performance...
distribution terminal has lighter key storage tasks. The distribution of key storage is reasonable, as shown in Table 2.

| Types                        | Number of master key | Number of intra-site session key | Number of cross-site session keys |
|------------------------------|----------------------|---------------------------------|----------------------------------|
| Distribution terminal        | 1                    | $M_{\text{Inter}}$              | $M_{\text{Ext}}$                 |
| Distribution station         | $N_{\text{End}}+1$   | $\sum_{\Delta n=1}^{N_{\text{End}}-1} M_{\text{Intr}}$ | $\sum_{\Delta n=1}^{N_{\text{End}}-1} M_{\text{Ext}}$ |
| Main distribution station    | $N_{\text{Station}}$ | $\sum_{\Delta n=1}^{N_{\text{End}}-1} M_{\text{Ext}}$ | $\sum_{\Delta n=1}^{N_{\text{End}}-1} M_{\text{Ext}}$ |

5. Conclusion

This paper constructs a three-tier wireless communication system for power distribution equipment applied to the distribution network, including the distribution terminal layer, the distribution station layer, and the distribution master station layer. A lightweight key management scheme is designed and described in detail in this paper, which include the process of three types of key generation, distribution, update, and destruction of the scheme. The DNKMS proposed in this paper reduces the communication and calculation load required in key management with a light-weight concept, and has smaller calculation overhead and key storage space. The DNKMS program allocates reasonable tasks based on the storage and computing capabilities of the master distribution station, distribution station and distribution terminal. Compared with NSSK, DNKMS has basically the same transmission time overhead, smaller computing time overhead and higher efficiency. Therefore, the DNKMS can be applied to distribution terminals and distribution stations with limited resources. In summary, the DNKMS can ensure the information security requirements of the wireless communication system of the distribution network, and lay the foundation for the implementation and promotion of the power IoT.

Acknowledgments

This paper was supported by the Research on Integrated Energy Metering Collection Technology for Customer Side Energy Internet (No. 1100-201919158A-0-0-00).

References

[1] Liu X., Liu S., Dai Z., et al. (2019) Analysis of communication requirements for typical distribution network business. 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 1414-1417.
[2] Li Z., Tong W., Jin X. (2016) Construction of cyber security defense hierarchy and cyber security testing system of smart grid: thinking and enlightenment for network attack events to national power grid of Ukraine and Israel. Automation of Electric Power Systems, 40(8):147-151.
[3] David M L., John B O. (2015) Secure data networks for electrical distribution applications. Journal of Modern Power Systems and Clean Energy, 3(3): 447-455.
[4] Surnhne L M., Tennoe M T., Henssonow S F., et al . (2010) Kerckhoffs’principle . Betascript Publishing, 11-20.
[5] Wu D P., Zhou C. (2011)Fault-tolerant and scalable key management for smart grid. IEEE Trans on Smart Grid, 6(2):375-381.
[6] Nicanfar H., Jokar P., Beznosov K., et al. (2014) Efficient authentication and key management mechanisms for smart grid communications. IEEE Systems Journal, 8(2):629-640.
[7] Wang Z D., Wang G., Tong J F., et al. (2016) Key Management Method for Intelligent Substations. Automation of Electric Power Systems, 40(13):121-127 (in Chinese).
[8] Tan K., Li Z W., Guan Y D., et al. (2019) Lightweight Key Management Scheme Based on Communication System of Electric Vehicle Charging Piles. Electric Power Construction, 40(09):73-81.
[9] Li Z W., Zhu S T., Cui X S., et al. (2017) Key Management Scheme of Smart Substation Based on
Improved NSSK Protocol. Automation of Electric Power Systems, 41(05):139-146 (in Chinese).