IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 16, 2018, accepted November 16, 2018, date of publication November 27, 2018,
date of current version December 27, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2883657

Secure Session Key Management Scheme for Meter-Reading System Based on LoRa Technology

ZHUOQUN XIA[1,2], HONG ZHOU[1,2], KE GU[1,2], BO YIN[1,2], YOUYOU ZENG[1], AND MING XU[3]

[1]Hunan Provincial Key Laboratory of Intelligent Processing of Big Data on Transportation, Changsha University of Science and Technology, Changsha 410114, China
[2]School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410114, China
[3]School of Computer, National University of Defense Technology, Changsha 410073, China

Corresponding author: Ke Gu (gk4572@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61572514, in part by the National Natural Science Foundation of Hunan under Grant 2018JJ2445, in part by the Technology Progress and Innovation Project of the Hunan Communications and Transportation Department under Grant 201405, and in part by the CCF-Beijing Venustech Inc., Hongyan Research Funding Project under Grant 14JJ7043.

ABSTRACT Long range (LoRa) technology is a wireless communication technology, which may provide low-power, low-rate, and LoRa communication. It may widely be used into many applications, such as smart metering and factory monitoring. However, some features of LoRa technology also bring new security weaknesses. Therefore, we propose an improved session key management to secure the meter-reading system based on LoRa technology. In our proposed scheme, we add a trusted key distribution server for the related devices to generate their session keys and manage all the keys, where the symmetric session keys are used to protect the communication data between the servers and the terminal devices. In addition, in order to maintain the long-term security of the proposed meter reading system, our proposed lightweight key management scheme can update the session keys automatically and remotely. Finally, we make analysis and experiments to evaluate our proposed key management scheme for the meter-reading system, the related results show our proposed scheme is secure and effective.

INDEX TERMS LoRa, wireless communication, meter-reading system, key management, security.

I. INTRODUCTION

A. BACKGROUND

Smart grid is an enhanced power grid that uses digital communications technology to increase grid efficiency, sustainability and reliability. One of the most significant advantages is that entities in smart grid can make communication each other in real time. Smart meter, which is a basic function device in smart grid, not only can meter the basic electricity consumption as the traditional electric energy meter, but also have two-way multi-rate measurement function, user-terminal control function, bidirectional data communication function based on multiple data transmission modes, and anti-theft function [1]. It allows a power supplier to obtain user electricity consumption remotely and timely, and re-allocates the electricity resources to meet the users' demand without unnecessary waste. Also, meter-reading system has generally gone through three phases: manual meter reading phase, IC card prepaid meter reading phase and automatic meter reading phase. Currently intelligent and remote meter reading system using wireless communication technology can save a lot of manpower and financial resources. Therefore, with the development of smart gird, wireless meter reading devices are being improved, many traditional short-distance wireless data transmission methods are not able to meet the accuracy requirements of future wireless meter reading devices [2]. Also, with the construction of smart city, the existing 3G/4G cellular networks and close-range networks cannot both meet the needs of smart gird. Therefore, based on a low-power wide-area wireless network technology, it needs to be researched that how to construct intelligent monitoring and measurement [3], [4]. Currently, wireless technologies used in Internet of Things, such as WiFi, Bluetooth, etc., limit the scope of communication and have more power requirements. ZigBee technology is related to the inherent scalability limitation of network. Other wireless technologies

such as GPRS, LTE and EDGE support a wider scope of communication, but their communication devices are required to consume a lot of power [5]–[7]. In the last two years, a new low-power wide-area network (LPWAN), LoRa technology has rapidly been developed with its low power consumption, wide coverage and strong penetrability. It makes up the insufficiency of other communication technologies. LoRa technology can provide long-distance wireless communication and longer battery lifecycle due to low power consumption. Also, LoRa technology has the ability to connect thousands of nodes to gateway, and provides secure transfer and adaptive data rate (ADR). So, it is being applied to multiple fields [8]–[11]. Currently, it is a new attempt that LPWAN is introduced into electric-power meter-reading system to design an electric-power meter-reading system based on LoRa wireless communication technology.

LoRa is a wireless communication technology, which may provide low-power, low-rate and long-range communication [12]. It uses the free ISM band (industrial, scientific and medical radio band). A LoRa network consists of four different components: network devices, network gateways, network servers and application services. The communication setup of LoRa network is similar to that of WiFi network, where network devices make communication through LoRa gateways. Gateways usually need to scan corresponding spectrum, receive LoRa data packets from terminal devices and forward the data to corresponding application services in network servers which may process the data packets, where network server is also used to store metering data and application server is used for users to look up metering data. Also, every terminal device must have a LoRa transceiver chip which is designed and manufactured by the Semtech corporation. Figure 1 shows the system architecture of meter-reading system based on LoRa technology, where the network server and the application server both are managed in the power management center. Because LoRa technology uses the free ISM band and its communication range can achieve up to 22 kilometers, LoRa technology can be a choice to be used for meter-reading system.

As smart grid that relies on information networking can expose the weaknesses of network system, it first needs to be researched whether the electric-power meter-reading system based on LoRa technology may bring new risk of network attacks [13]. In the electric-power meter-reading system, the collected readings from electric-power meters may face the threats of being sniffed, intercepted or altered. For example, an intruder may steal a private key from an insecure meter node [14], and then connect to the system network and attempt to decrypt the exchanged messages to control the meter node. The work in [15] found that LoRa terminal devices also have security weakness when they enter some networks. As smart meters are resource-constrained nodes, some cryptographic solutions are not ideal for providing security. Therefore, implementing a lightweight encryption solution to protect user privacy and meter reading integrity is critical to smart meter computing, communications and storage.

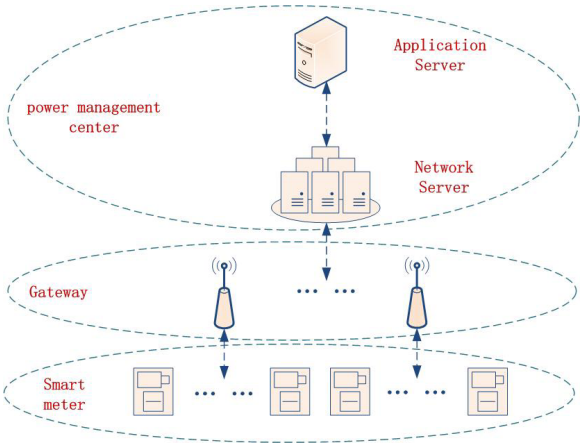


FIGURE 1. System architecture of meter-reading system based on LoRa technology.

B. OUR CONTRIBUTIONS

Aim at solving the security weaknesses of the electric-power meter-reading system based on LoRa technology, we propose a secure session key management scheme for meter-reading system based on LoRa Technology. In our proposed protocol, when a smart meter joins a meter-reading system, we add a trusted key distribution server (KDS) in the power management center to help the smart meter to calculate and manage the network session keys and the application session keys. In the process of meter reading transmission, we use the session keys to cryptographically protect data between the smart meter and the network server. Further, our proposed lightweight key management method can update the session keys automatically and remotely. Our contributions are as follows:

1) In meter-reading system based on LoRa technology, we propose a new solution to add a trusted key distribution server. The improved LoRa-WAN architecture consists of electric meters (built-in LoRa module), LoRa gateways, network server, application server and key distribution server (KDS). For the security perspective, electric meters and LoRa gateways are untrusted entities, network server, application server and key distribution server are trusted entities, where network server is also used to store metering data. During the stage that one terminal device (electric meter) connects into the LoRa-WAN, KDS is responsible for the terminal device to generate its session key and transmitting it securely to the network server and application server, where the symmetric session key is used to protect the communication data between the network server and the terminal device.
2) To secure communication between LoRa-WAN entities, each message must contain a timestamp to

prevent replay attack, and the communication peer stores the last received timestamp value. Each time an entity receives a message, it checks the received timestamp and the stored (last) timestamp. Additionally, because it is high risk to use a fixed symmetric key for a long time, all the symmetric keys shared by the communication entities in our proposed key management scheme are updated dynamically.

3) Based on the security requirement of meter-reading system, we analyze the security and efficiency of our proposed scheme. Our proposed scheme can provide end-to-end security, session key protection, verification and confidentiality of updating session keys and resisting replay attack. Also, the experiments show our proposed scheme is efficient.

C. ORGANIZATION

The rest of this paper is organized as follows. In Section 2, we discuss the related works about meter-reading system, LoRa technology and their security problems. In Section 3, we propose a secure session key management scheme for meter-reading system based on LoRa Technology. In Section 4, we analyze the security and efficiency of the proposed scheme. In Section 5, we make some experiments to test the efficiency of the proposed scheme. Finally, we draw our conclusions in Section 6.

II. RELATED WORK

The traditional meter reading technologies for smart meter mainly include wireless meter reading technology and mobile cellular network meter reading technology. Currently, some wireless meter reading technologies, such as WiFi and ZigBee, have limited coverage, lack of anti-interference ability and low receiving sensitivity, thus the technologies cannot be used for long time. Additionally, mobile cellular network meter reading technology and related terminal devices based on 4G-based Internet of Things both need additional software and hardware costs [14]. Long range technology (LoRa) is a new solution proposed by the Semtech corporation, whose frequency bandwidth is below 1 GHz. LoRa is mainly used to radio modulation and demodulation based on non-authorized spectrum under a long-range, multi-nodes and low-power wide area network [15].

Currently the LoRa technology union defines the LoRa-WAN architecture, which consists of terminal devices, gateways, a network server and an application server [16]. Further, LoRa-WAN describes its network layer architecture that can support LoRa system and its physical layer function that can provide long-range communication through LoRa modulation. Also, the related document proposed by the LoRa technology union describes two modes to activate terminal devices in LoRa-WAN, including Over The Air Activation (OTAA) and Activation By Personalization (ABP). In the mode of OTAA, terminal device must execute the joining process to participate in data exchange with network server, where the joining process includes two messages: the ''joining request'' message sent by the terminal device and the ''joining permission'' responded by the network server. In the mode of ABP, terminal device loads all the related information that can be permitted to access LoRa network when it starts. In [16], [17], the LoRa technology union further describes some characteristics of LoRa-WAN, compared with the other existing solutions. First, the communication mode between terminal nodes is asynchronous, where terminal nodes only make communication while they need to send data, thus the mode is more advantageous than other solutions that require much energy cost to synchronize terminal nodes. Second, LoRa-WAN provides high network capacity by using adaptive data rate and multi-channel multi-mode transceiver in gateway, which allows simultaneous transmission through a large number of terminal nodes and multiple channels. Thirdly, LoRa-WAN constructs two security layers to ensure its whole security, which include the network security layer that ensures the authenticity of network nodes and the application security layer that protects user's data from being accessed by network operators; also, LoRa-WAN [16] guarantees the security of its data among LoRa devices through symmetric encryption. Although LoRa-WAN provides enough methods to secure its functions, LoRa devices are still vulnerable to some attacks. For example, an attacker may repeat or delay the transmitted messages to the terminal device or the network server through the LoRa-WAN network.

At present, some researches on the application of LoRa technology to meter reading system mainly involves the reliability of data transmission of LoRa devices and the protocol security of terminal devices accessing to LoRa-WAN. Aras *et al.* [18] investigated potential security vulnerabilities in LoRa technology, where they use commercial-off-the-shelf hardware to detect the sensitivity of LoRa devices against different types of attacks. It is proved that a malicious attacker may make a replay attack to LoRa devices when the attacker obtains a transferred message by sniffing the transmission between terminal LoRa device and gateway. Additionally, lack of secure key management may also expose important information from terminal devices and gateways to malicious users. Cheng *et al.* [19] proposed a secure smart metering infrastructure based on LoRa technology for electric meter data transmission. Their proposed scheme uses symmetric encryption technology to protect the end-to-end communication between substation automation system (SAS) and smart meter. Furthermore, in order to maintain a long-term security of the proposed metering system, they designed a key management protocol to update all the keys dynamically. However, in their proposed scheme random temporary numbers are used to prevent replay attacks, thus it is a load for the electric meters with limited memory. Tomasin *et al.* [13] studied the security of the initial connection process between terminal devices and network servers in the LoRa-WAN protocol. In order to avoid replay attack, random number technology is used into transmitted data packet. Also, their experiment analyzed the inaccuracy of

random number generator and the potential vulnerabilities of LoRa-WAN protocol against DoS attack. Naoui *et al.* [20] proposed a solution to improve the security of Lora-WAN protocol. The gateways are used to secure the communication between terminal devices, networks and application servers, where every gateway helps terminal device to calculate its session key by performing the corresponding cryptographic operations. Every gateway only calculates a part of session key associated with terminal device without being able to calculate out the final session key. However, the replay attack may still occur between terminal devices and network servers in their proposed scheme. Naoui *et al.* [21] proposed an improved solution to enhance the security of Lora-WAN protocol. It adds a third-party entity to secure the communication between terminal devices, networks and application servers. The third party helps terminal device to calculate its session key by performing the corresponding cryptographic operations. However, to update session key, the previous same steps must be again executed for a new joining procedure, which is tedious and energy-intensive, and influences the data transmission of electric meter.

III. SECURE SESSION KEY MANAGEMENT SCHEME TO METER-READING SYSTEM BASED ON LORA TECHNOLOGY

In meter-reading system based on LoRa technology, when smart meter is added to LoRa-WAN, they (terminal devices) must be activated by the modes of OTAA or ABP. So, considering the existing problems in the two modes, we improve the mode of OTAA. Our proposed system aims to enable remote metering by a secure and cost-efficient way through adopting an improved session key management protocol in the meter-reading system based on LoRa-WAN architecture.

A. LORA-WAN ARCHITECTURE BASED ON IMPROVED SESSION KEY MANAGEMENT

In meter-reading system based on LoRa technology, we propose a new solution to add a trusted key distribution server. Thus, the improved LoRa-WAN architecture consists of electric meters (built-in LoRa module), LoRa gateways, network server, application server and key distribution server (KDS). LoRa gateways mainly relay messages between electric meters and network server through transparent manner. Application server is used for users to look up metering data. So, for the security perspective, electric meters and LoRa gateways are untrusted entities, network server, application server and key distribution server are trusted entities, where they are located in the power management center. During the stage that one terminal device (electric meter) connects into the LoRa-WAN, KDS is responsible for the terminal device to generate its session key and transmitting it securely to the network server and application server, where the symmetric session key is used to protect the communication data between the network server and the terminal device. So, in our proposed scheme, in order to maintain long-term security of meter-reading system, KDS manages all the keys. The system architecture is shown in Figure 2.

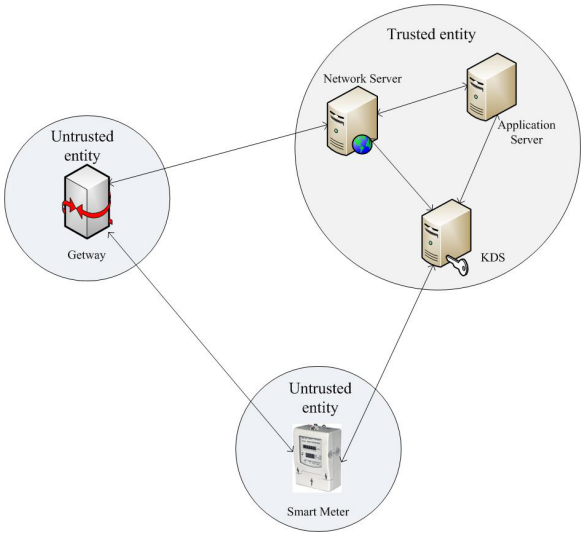


FIGURE 2. LoRa-WAN architecture based on improved session key management.

B. SESSION KEY MANAGEMENT FOR LoRa-WAN ARCHITECTURE

In the section, we propose a key management scheme for LoRa-WAN architecture. To secure communication between LoRa-WAN entities, each message must contain a timestamp to prevent replay attack, and the communication peer stores the last received timestamp value. Each time an entity receives a message, it subtracts the received timestamp from the stored (last) timestamp, if the computed value is less than the preset value, then the received message may be accepted. Our proposed scheme uses symmetric keys to protect data transmitted between the network server and other devices embedded with LoRa module, where each smart meter embedded with LoRa module shares a secret symmetric key with the network server. By encrypting transferred data on a symmetric key, we prevent the transferred data from being sniffed or changed. However, it is high risk to use a fixed symmetric key for a long time. In order to solve this problem, all the symmetric keys shared by the communication peers in our proposed key management scheme are updated dynamically, where a symmetric key K_i is only used to verify for the $i-$th time period. Our proposed key management scheme is described as the following stages.

1) SYSTEM SETUP

According to our proposed system architecture, the trusted KDS respectively generates two session keys SK_1 and SK_2 with the network server and application server through asymmetric encryption, where the two keys are used to respectively secure the communication between KDS and the two servers. Additionally, each terminal device (smart meter) is initially embedded with a terminal device unique identifier (*DevEUI*) and a unique 128-bit AES Key (*AppKey*) being used to verify. Therefore, when smart meter based on LoRa is initially added

to LoRa-WAN, the key *AppKey* is used to secure the communication between KDS and smart meter in our proposed scheme. Compared with the existing solution [16], the key *AppKey* is only stored in the KDS. All the related symbols used in the proposed scheme are shown in Figure 3.

Symbol	Description
AppEUI	Application unique identifier
DevEUI	Terminal device unique identifier
DevTS	Terminal device timestamp
AppKey	Pre-shared key between terminal device and KDS
KDSTS	KDS timestamp
SK_1	Session key created between KDS and network server
SK_2	Session key created between KDS and application server
MIC	Message Integrity Code
NwkTS	Network server timestamp
NetID	Network identifier
RxDelay	RF delay parameter
CFList	Related channel parameter

FIGURE 3. Notation.

2) JOINING LoRa-WAN STAGE

In the section, we describe the procedure that smart meter joins LoRa-WAN, where smart meter makes interaction with other entities according to Figure 4. The specific steps are described as follows:

- **Step 1**: The terminal device (smart meter) sends a "**Join Request 1**" message signcrypted by the shared key *AppKey* to the KDS, where the message contains the terminal device unique identifier *DevEUI*, the application unique identifier *AppEUI* and the terminal device timestamp *DevTS*. The message is signcrypted to generate a 4-byte **MIC** according to the following calculations:

$$\begin{aligned} en &= \textbf{aes128encrypt}(AppKey, \textbf{JoinRequest} \\ &\quad \textbf{1} :: AppEUI||DevEUI||DevTS), \\ mc &= \textbf{aes128cmac}(AppKey, en), \\ \textbf{MIC} &= \textbf{Func}_{[0-3]}(mc), \end{aligned}$$

  where **aes128encrypt** is an encryption function defined by the LoRa Alliance, **aes128cmac** is a signature function, $\textbf{Func}_{[0-3]}$ is an intercepting function of bytes for generating a 4-byte **MIC**, and **MIC** is a message integrity code obtained by performing the $\textbf{Func}_{[0-3]}$ on one message, which is used to check whether the encrypted content had been tampered with.
- **Step 2**: The KDS uses the key *AppKey* to verify the received **MIC** by recomputing its own **MIC** on the received message, if the message is valid, then the KDS continues to decrypt the received message. Then the KDS stores the terminal device timestamp *DevTS* into its database. Also, the KDS also generates a timestamp *KDSTS* and sends a "**Join Request 2**" message encrypted by the key SK_1 to the network server, where the message includes *DevEUI*, *AppEUI* and *KDSTS*. The message is also signcrypted to generate a 4-byte **MIC** according to the following calculations:

$$\begin{aligned} en &= \textbf{aes128encrypt}(SK_1, \textbf{JoinRequest} \\ &\quad \textbf{2} :: AppEUI||DevEUI||KDSTS), \\ mc &= \textbf{aes128cmac}(SK_1, en), \\ \textbf{MIC} &= \textbf{Func}_{[0-3]}(mc). \end{aligned}$$

- **Step 3**: The network server uses the key SK_1 to verify the received **MIC** by recomputing its own **MIC** on the received message, if the message is valid, then the network server continues to decrypt the received message. Then the network server stores the timestamp *KDSTS* into its database and then sends the message "**Join Accepting 1**" encrypted by the key SK_1 to the KDS, where the message includes the network server timestamp *NwkTS*, the network identifier *NetID*, the terminal device address *DevAddr* and some other configuration parameters (*RxDelay* and *CFList*) used for RF delay and related channels. The message is also signcrypted to generate a 4-byte **MIC** according to the following calculations:

$$\begin{aligned} en &= \textbf{aes128encrypt}(SK_1, \textbf{JoinAccepting1} :: \\ &\quad NwkTS||DevAddr||NetID||RxDelay||CFList), \\ mc &= \textbf{aes128cmac}(SK_1, en), \\ \textbf{MIC} &= \textbf{Func}_{[0-3]}(mc). \end{aligned}$$

- **Step 4**: The KDS uses the key SK_1 to verify the received **MIC** by recomputing its own **MIC** on the received message, if the message is valid, then the KDS continues to decrypt the received message. Then the KDS stores the timestamp *NwkTS* into its database. Then the KDS generates two random values r_1 and r_2, and computes two session keys as follows:

$$\begin{aligned} NwkSKey &= \textbf{aes128encrypt} \\ &\quad (AppKey, 0x01||NwkTS||NetID|| \\ &\quad sDevTS||r_1||pad16), \\ AppSKey &= \textbf{aes128encrypt} \\ &\quad (AppKey, 0x01||NwkTS||NetID|| \\ &\quad DevTS||r_2||pad16). \end{aligned}$$

  Finally, the KDS sends the message "**Join Accepting 2**" encrypted by the key *AppKey* to the smart meter, where the message includes *NwkTS*, *KDSTS*, *NetID*, r_1, r_2, *DevAddr*, *RxDelay* and *CFList*. The message is also signcrypted to generate a 4-byte **MIC** according to the following calculations:

$$\begin{aligned} en &= \textbf{aes128encrypt}(AppKey, \textbf{JoinAccepting} \\ &\quad 2 :: NwkTS||KDSTS||DevAddr||NetID||r_1||r_2|| \\ &\quad RxDelay||CFList), \\ mc &= \textbf{aes128cmac}(AppKey, en), \\ \textbf{MIC} &= \textbf{Func}_{[0-3]}(mc). \end{aligned}$$

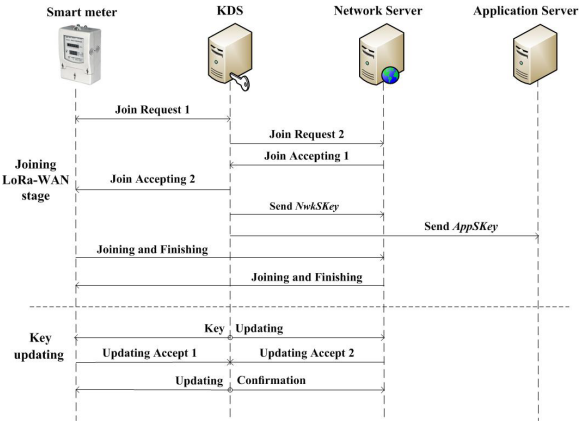


FIGURE 4. Secure LoRa-WAN key management protocol.

- **Step 5**: The smart meter uses the key *AppKey* to verify the received **MIC** by recomputing its own **MIC** on the received message, if the message is valid, then the smart meter continues to decrypt the received message. Then the smart meter stores the timestamps *NwkTS* and *KDSTS* into its database. Also, the smart meter sets K^0 = *NwkSKey* as its initial session key with the network server and clears all intermediate computed results.
- **Step 6**: Similarly the KDS sends the *NwkSKey* with the new timestamp and the corresponding computed **MIC** signed by the key SK_1 to the network server, and sends the *AppSKey* with the new timestamp and the corresponding computed MIC signed by the key SK_2 to the application server. Then, the KDS adds a record for the corresponding smart meter in its key managing table, sets and stores $i = 0$ and K^i= *NwkSKey*, and sets the expiration time for K^0, where i is the index of numbers of key life-cycle and clears all intermediate computed results.
- **Step 7**: Finally the smart meter and the network server exchange the "**Joining and Finishing**" messages, and if the corresponding **MIC**s on the messages are equal, then it denotes that the two entities have received the same session key, where the messages both include *DevEUI* and *NetID*. The messages are signcrypted to generate two same 4-byte **MIC**s according to the following calculations:

$$\begin{aligned} en &= \textbf{aes128encrypt}(NwkSKey, \\ &\quad \textbf{Joining and Finishing} :: DevEUI||NetID), \\ mc &= \textbf{aes128cmac}(NwkSKey, en), \\ \textbf{MIC} &= \textbf{Func}_{[0-3]}(mc). \end{aligned}$$

3) KEY UPDATING

In the section, we describe how to update the session key *NwkSKey* for the smart meter and the network server. In our proposed scheme, the session is generated and managed by KDS. For long-term security, the session key should be valid for a limited period of time and needs to be updated. So, after the session key *NwkSKey* expires over its life-cycle, the KDS must initiate a session key update protocol to update *NwkSKey* between the smart meter and the network server. To prevent that the attacker can predict and attack the updating process, the life-cycle of session key may be dynamic.[1] When a smart meter joins the proposed meter-reading system based on LoRa technology, the KDS stores the initial session key K^0 with the expiration time $time^0$ into its key managing table, and respectively sends the key to the network server and the smart meter as described in the Joining LoRa-WAN stage. We assume that the meter Dev_j ($j \in \{1, 2...m\}$) was added to the proposed meter-reading system, whose initial session key is K^0. When the KDS scans that the session key of Dev_j has expired, the KDS, the network server and the meter Dev_j respectively calculate the new session key using the same hash function. Also, the KDS updates its key managing table for Dev_j and sets the new random value as the next life-cycle. Finally, the meter Dev_j deletes all the intermediate calculated values including K^0. The updating procedure is described as follows (and as shown in Figures 5[2] and 6).

1) The KDS monitors all the session keys for every meter and updates the expired keys. Once the key K_j for the meter Dev_j has expired, the KDS needs to complete the key updating process. The KDS calculates $K_j^{i+1} = \mathbf{H}(K_j^i||R_j)$, where $i \in \{0, 1, 2...n-1\}$, $\mathbf{H}(\cdot)$ is a one-way hash function, n represents the total number of updates in the device management life-cycle, and R_j is a random number. Then, the KDS generates a timestamp $KDSTS_j$ and another random number x_j,

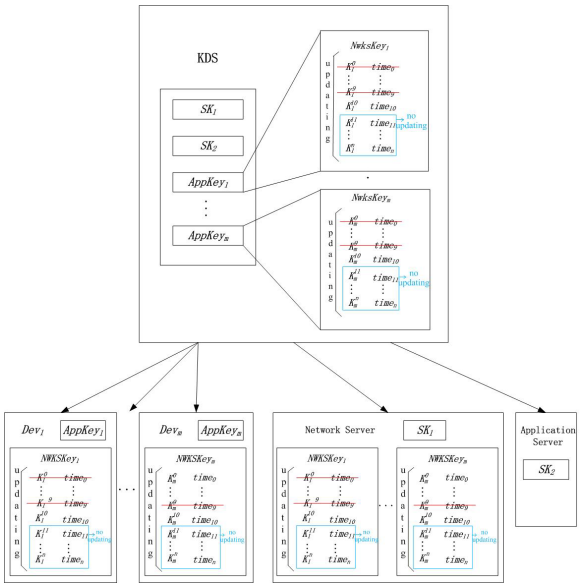


FIGURE 5. Session key updating management.

[1]The two session keys SK_1 and SK_2 in the system setup stage are stored in the key managing table to respectively secure the communication between KDS and other two servers, as described in Step 6 of the joining LoRa-WAN stage.

[2]In the Figure 5, the session keys are being updated to K_j^{10} with $j \in \{1, 2...m\}$ and the previously calculated session keys are cleared in the key managing table.

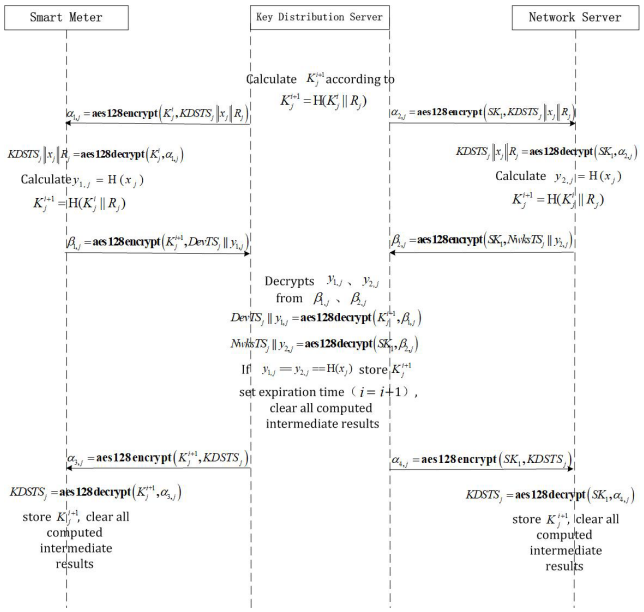


FIGURE 6. Session key updating procedure.

sends a "Key Updating" message to the meter Dev_j and the network server respectively, where the message includes $KDSTS_j$, x_j and R_j. The message respectively needs to be encrypted by the keys K_j^i and SK_1 as follows:

$$\alpha_{1,j} = \textbf{aes128encrypt}(K_j^i, KDSTS_j||x_j||R_j),$$
$$\alpha_{2,j} = \textbf{aes128encrypt}(SK_1, KDSTS_j||x_j||R_j),$$

where $\alpha_{1,j}$ is sent to the meter and $\alpha_{2,j}$ is sent to the network server.

2) The meter Dev_j decrypts the received message $\alpha_{1,j}$ by using K_j^i to obtain R_j,

$$KDSTS_j||x_j||R_j = \textbf{aes128decrypt}(K_j^i, \alpha_{1,j}).$$

Then the meter checks the timestamp $KDSTS_j$, calculates $K_j^{i+1} = \mathbf{H}(K_j^i||R_j)$ and $y_{1,j} = \mathbf{H}(x_j)$. Finally, the meter sends the message "Updating Accept 1" to the KDS, where the message includes $DevTS_j$ and $y_{1,j}$, and the message is encrypted by the key K_j^{i+1}:

$$\beta_{1,j} = \textbf{aes128encrypt}(K_j^{i+1}, DevTS_j||y_{1,j}).$$

3) Similarly, the network server uses SK_1 to decrypt the received message $\alpha_{2,j}$ to obtain R_j,

$$KDSTS_j||x_j||R_j = \textbf{aes128decrypt}(SK_1, \alpha_{2,j}).$$

Then the network server checks the timestamp $KDSTS_j$, calculates $K_j^{i+1} = \mathbf{H}(K_j^i||R_j)$ and $y_{2,j} = \mathbf{H}(x_j)$. Finally, the network server sends the message "Updating Accept 2" to the KDS, where the message includes $NwksTS_j$ and $y_{2,j}$, and the message is encrypted by the key SK_1:

$$\beta_{2,j} = \textbf{aes128encrypt}(SK_1, NwksTS_j||y_{2,j}).$$

4) The KDS receives the two messages respectively from the meter and the network server, and then decrypts them to obtain $y_{1,j}$ and $y_{2,j}$,

$$DevTS_j||y_{1,j} = \textbf{aes128decrypt}(K_j^{i+1}, \beta_{1,j}),$$
$$NwksTS_j||y_{2,j} = \textbf{aes128decrypt}(SK_1, \beta_{2,j}),$$

and checks the corresponding timestamps. If the corresponding timestamps are valid, then the KDS further checks whether $y_{1,j}$, $y_{2,j}$ and the value of $\mathbf{H}()$ on x_j are equal. If they are equal, then the three entities had calculated out the same session key so that the new key is successfully updated. The KDS sends a message "Updating Confirmation" to the meter and the network server respectively, where the message includes $KDSTS_j$. The message is encrypted by K_j^{i+1} and SK_1 respectively,

$$\alpha_{3,j} = \textbf{aes128encrypt}(K_j^{i+1}, KDSTS_j),$$
$$\alpha_{4,j} = \textbf{aes128encrypt}(SK_1, KDSTS_j),$$

where $\alpha_{3,j}$ is sent to the meter and $\alpha_{4,j}$ is sent to the network server. Finally, the KDS updates its key managing table for the meter Dev_j, and clears all computed intermediate results.

5) Finally, the meter and the network server decrypt the received messages respectively, and further check the timestamp $KDSTS_j$s from the decrypted messages,

$$KDSTS_j = \textbf{aes128decrypt}(K_j^{i+1}, \alpha_{3,j}),$$
$$KDSTS_j = \textbf{aes128decrypt}(SK_1, \alpha_{4,j}).$$

If the timestamps are valid, then the meter and the network server will set K_j^{i+1} as the new session key, and clear all computed intermediate results,[3] including K_j^i.

IV. ANALYSIS OF THE PROPOSED SCHEME

A. SECURITY ANALYSIS

In the section, we analyze the security of our proposed scheme.

1) End-to-end security: The communication between the network server and the smart meter is secured by symmetric encryption on their sharing symmetric session key K^i=*NwkSKey*. As data are encrypted, the transmitted meter readings are not available to others, such as network concentrators (because they do not have corresponding session keys). Additionally, although every meter has a symmetric key, the key is valid only for a period of time before the next updating time. Therefore, when an attacker corrodes a meter for its session key, it does not affect other metering devices under the same domain name.
2) Session key protection: In our proposed scheme, the session keys *NwkSKey* and *AppSKey* are calculated

[3] In our proposed scheme, we suggest that the session key of the application server is also updated, where the key updating procedure is the same as that of the network server.

by the KDS instead of the network server in the original LoRa system. Therefore, the network server can no longer calculate the *AppSKey*. Also, to avoid using the same parameters to calculate *NwkSKey* and *AppSKey*, the KDS generates two random numbers for calculating two different session keys. Each session key *NwkSKey* is set with an expiration time for updating, the KDS can dynamically update the session key *NwkSKey* between the network server and the smart meter to maintain long-term security.

3) Verification and confidentiality of updating session keys: in the updating key stage, the session key *NwkSKey* is not directly transferred for updating, only the related entities respectively calculate and updates the session key *NwkSKey*. Also, for the integrity of the updated key, the KDS introduces two random numbers R_j and x_j to control the key updating sequence, where the KDS can check that whether the responding messages of the network server and the smart meter are able to correspond the random numbers, so as to secure the integrity of the updated key.
4) Resisting replay attack: Random number is used to prevent replay attack, and the related entities must store the corresponding random number to avoid replay attack. However, the method is difficult to be applied for some terminal devices, such as smart meter, because the devices have restricted memories to not store a large number of random numbers. So, in the updating key stage, the timestamp *KDSTS* is used into the updating communications among the related entities in our proposed scheme. The network server and the smart meter only need to save the last received timestamp (such as T_1), and then compare it with the current received timestamp (such as T_2). For example, if $T_2 - T_1 > \Delta T$, then the updating message may be accepted; otherwise the message is rejected, and the related entities may further check whether there exists replay attack in the current communication.

B. PERFORMANCE ANALYSIS

In the section, we analyze the performance of the proposed session key management. Considering the response time for the requests from the proposed entities, we make experiments to test the time consumption in the joining LoRa-WAN stage and the key updating stage. In our experiments, time consumption is mainly evaluated from wireless transmission, symmetric encryption and decryption (AES), Hash computation.

1) Joining LoRa-WAN stage
   a) Communication time
   According to the Figure 4, there are 8 communication procedures in the joining LoRa-WAN stage, including 4 wireless transmission procedures. Therefore, the total wireless communication time of the initialization phase is $T_{w_1} = \sum_{i\in\{1,4,7,8\}} T_i$, where T_i is the $i-$th communication time required to transfer the corresponding data packet in the joining LoRa-WAN stage.
   b) Encryption and decryption time
   According to the Figure 4, the encryption and decryption time spent in the three main entities is $T_{ED_1} = 8 \cdot T_{Encry} + 8 \cdot T_{Decry}$, where T_{Encry} and T_{Decry} respectively represent the AES encryption and decryption time on 128-bit key.
2) Key updating stage
   a) Communication time
   After smart meter is connected to LoRa-WAN, the meter reading system may make meter reading from the meter. According to the Figure 4, we can estimate that the wireless communication time in the key updating stage is $T_{w_2} = \sum_{i\in\{1,2,4\}} T_i$, where T_i is the $i-$th communication time required to transfer the corresponding data packet in the key updating stage.
   b) Encryption and decryption time
   According to the key updating protocol in Figure 4, the encryption and decryption time spent in the three main entities is $T_{ED_2} = 6 \cdot T_{Encry} + 6 \cdot T_{Decry}$, where T_{Encry} and T_{Decry} respectively represent the AES encryption and decryption time on 128-bit key.

V. EXPERIMENTS

In the section, we make experiments to evaluate our proposed key management scheme for the meter-reading system based on LoRa technology. Our experimental environment mainly consists of a network server, a key management center (server) and some terminal devices. Also, the AES encryption and decryption are based on 128-bit key, where all the related programs are finished by java1.6 and Eclipse_6.0 to simulate the key management procedure. In the experiment, the execution times of hashing computation and AES algorithm are very short for some small data packets, thus the influence of the two operations to the whole key management procedure may be almost ignored in our proposed key management scheme (The transferred data packets are very small in our proposed scheme.).

1) Communication time in joining LoRa-WAN stage
   According to the Figure 4, there are 4 wireless transmission procedures in the joining LoRa-WAN stage, where the format and size of transferred message are shown in Figure 7, where every data packet is related to one step from the joining LoRa-WAN stage.[4]
   The experiment simulates the wireless transmission procedure on 4 different data packets, the executed

[4]In the **Step 7**, we respectively test for smart meter and network server.

Step	Message Format（bytes）											Size of Data Packet
1	*MHDR*	*APPEUI*	*DevEUI*	*DevTS*	*MIC*							25
	1	8	8	4	4							
4	*MHDR*	*DevAddr*	*NetID*	*NwkTS*	*KDSTS*	*RxDelay*	r_1	r_2	*DLSettings*	*CFList*	*MIC*	49
	1	4	3	4	4	1	4	4	4	0/16	4	
7 Smart meter	*MHDR*	*DevEUI*	*NetID*	*MIC*								16
	1	8	3	4								
7 Network server	*MHDR*	*DevEUI*	*NetID*	*MIC*								16
	1	8	3	4								

FIGURE 7. Message format 1.

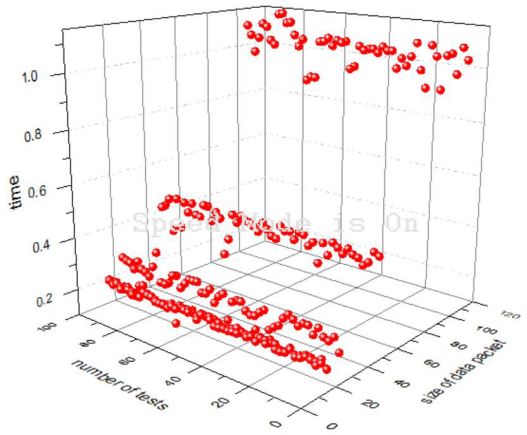


FIGURE 8. The wireless transmission time on 4 different data packets.

Step	Message Format（bytes）			Size of Data Packet
1	*KDSTS*	*x*	*R*	40
	4	32	4	
2	*DevTS*	*y*		8
	4	4		
4	*KDSTS*			4
	4			

FIGURE 9. Message format 2.

times are shown in Figure 8. Figure 8 shows 100 executed times on 4 different data packets, where a red point represents one executed time. From the Figure 8, we may know the executed time is increased while the size of data packet is increased. So, the wireless transmission procedure is efficient on 4 different data packets.

2) Communication time in key updating stage

According to the Figure 4, there are 3 wireless transmission procedures in the key updating stage. In the experiment, the size of our session key *NwksKey* is 16 bytes, the size of R_j is 32 bytes, the sizes of the random number and the timestamp are both 4 bytes. So, the format and size of transferred message are shown in Figure 9, where every data packet is related to one step from the key updating stage.

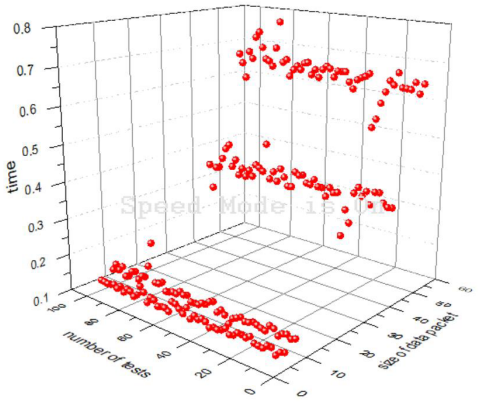


FIGURE 10. The wireless transmission time on 3 different data packets.

The experiment simulates the wireless transmission procedure on 3 different data packets, the executed times are shown in Figure 10. Figure 10 shows 100 executed times on 3 different data packets. Similarly we may know that the executed time is increased while the size of data packet is increased, and in the key updating stage the wireless transmission procedure is efficient on 3 different data packets.

VI. CONCLUSIONS

LoRa is a wireless communication technology, which may provide low-power, low-rate and long-range communication. In this paper, we propose a secure session key management to secure the meter-reading system based on LoRa technology. In our proposed scheme, we add a trusted key distribution server for the related devices to generate their session keys and manage all the keys. Also, our proposed lightweight key management scheme can update the session keys automatically and remotely. So, our proposed key management method can be used to the LoRa-WAN architecture to realize more secure, fast access and remote communication for smart meters. Finally, we make analysis and experiments to evaluate our proposed key management scheme for the meter-reading system, the related results show our proposed scheme is secure and effective.

REFERENCES

[1] D. C. Stancu, D. Federenciuc, N. Golovanov, and D. Stanescu, "New functionalities of smart grid-enabled networks," *CIRED-Open Access Proc. J.*, vol. 2017, no. 1, pp. 1903–1906, Oct. 2017, doi: 10.1049/OAP-CIRED.2017.1039.

[2] S. Verma and P. Rana, "Wireless communication application in smart grid: An overview," in *Proc. CIPECH*, Ghaziabad, India, Nov. 2014, pp. 310–314, doi: 10.1109/CIPECH.2014.7019038.

[3] G. Pasolini *et al.*, "Smart city pilot projects using LoRa and IEEE802.15.4 technologies," *Sensors*, vol. 18, no. 4, p. 1118, Apr. 2018, doi: 10.3390/S18041118.

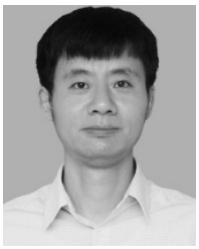
[4] J. Sanchez-Gomez, R. Sanchez-Iborra, and A. Skarmeta, "Transmission technologies comparison for IoT communications in smart-cities," in *Proc. GLOBECOM*, Singapore, Dec. 2017, pp. 1–6, doi: 10.1109/GLOCOM.2017.8254530.

[5] K. Mikhaylov, J. Petaejaejaervi, and T. Haenninen, "Analysis of capacity and scalability of the LoRa low power wide area network technology," in *Proc. Eur. Wireless*, Oulu, Finland, May 2016, pp. 1–6.

[6] Y. Zhang, R. Yu, W. Yao, S. Xie, Y. Xiao, and M. Guizani, "Home M2M networks: Architectures, standards, and QoS improvement," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 44–52, Apr. 2011, doi: 10.1109/MCOM.2011.5741145.
[7] Y. Zhang, R. Yu, M. Nekovee, Y. Liu, S. Xie, and S. Gjessing, "Cognitive machine-to-machine communications: Visions and potentials for the smart grid," *IEEE Netw. Mag.*, vol. 26, no. 3, pp. 6–13, May 2012, doi: 10.1109/MNET.2012.6201210.
[8] D. Baimel, S. Tapuchi, and N. Baimel, "Smart grid communication technologies- overview, research challenges and opportunities," in *Proc. SPEEDAM*, Anacapri, Italy, Jun. 2016, pp. 116–120, doi: 10.1109/SPEEDAM.2016.7526014.
[9] Y. Li, X. Yan, L. Zeng, and H. Wu, "Research on water meter reading system based on LoRa communication," in *Proc. ICSGSC*, Singapore, Jul. 2017, pp. 248–251, doi: 10.1109/ICSGSC.2017.8038585.
[10] M. Lauridsen, B. Vejlgaard, I. Z. Kovacs, H. Nguyen, and P. Mogensen, "Interference measurements in the European 868 MHz ISM band with focus on LoRa and SigFox," in *Proc. WCNC*, San Francisco, CA, USA, Mar. 2017, pp. 1–6, doi: 10.1109/WCNC.2017.7925650.
[11] A. Ouya, B. M. De Aragon, C. Bouette, G. Habault, N. Montavont, and G. Z. Papadopoulos, "An efficient electric vehicle charging architecture based on LoRa communication," in *Proc. SmartGridComm*, Dresden, Germany, Oct. 2017, pp. 381–386, doi: 10.1109/SmartGridComm.2017.8340723.
[12] A. Lavric and V. Popa, "LoRa wide-area networks from an Internet of Things perspective," in *Proc. ECAI*, Targoviste, Romania, Jun./Jul. 2017, pp. 1–4, doi: 10.1109/ECAI.2017.8166397.
[13] S. Tomasin, S. Zulian, and L. Vangelista, "Security analysis of LoRaWAN join procedure for Internet of Things networks," in *Proc. WCNCW*, San Francisco, CA, USA, Mar. 2017, pp. 1–6, doi: 10.1109/WCNCW.2017.7919091.
[14] H. Tao and M. Zhang, "Solar LED street light control system for wireless sensor networks based on ZigBee," *Adv. Mater. Res.*, vol. 664, p. 10411045, Feb. 2013, doi: 10.4028/WWW.SCIENTIFIC.NET/AMR.664.1041.
[15] L. Vangelista, A. Zanella, and M. Zorzi, "Long-range IoT technologies: The dawn of LoRa," in *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*, 2015, pp. 51–58, doi: 10.1007/978-3-319-27072-2_7.
[16] *LoRaWAN Specification*, LoRa Alliance, Beaverton, OR, USA, 2015.
[17] *LoRaWAN Certification*, LoRa Alliance, Beaverton, OR, USA, 2015.
[18] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, "Exploring the security vulnerabilities of LoRa," in *Proc. CYBCONF*, Exeter, U.K., Jun. 2017, pp. 1–6, doi: 10.1109/CYBConf.2017.7985777.
[19] Y. Cheng, H. Saputra, L. M. Goh, and Y. Wu, "Secure smart metering based on LoRa technology," in *Proc. ISBA*, Singapore, Jan. 2018, pp. 1–8, doi: 10.1109/ISBA.2018.8311466.
[20] S. Naoui, M. E. Elhdhili, and L. A. Saidane, "Enhancing the security of the IoT LoRaWAN architecture," in *Proc. PEMWN*, Paris, France, Nov. 2017, pp. 1–7, doi: 10.1109/PEMWN.2016.7842904.
[21] S. Naoui, M. E. Elhdhili, and L. A. Saidane, "Trusted third party based key management for enhancing LoRaWAN security," in *Proc. AICCSA*, Hammamet, Tunisia, Oct./Nov. 2017, pp. 1306–1313, doi: 10.1109/AICCSA.2017.73.

ZHUOQUN XIA received the Ph.D. degree from the School of Information Science and Engineering, Central South University, Changsha, China, in 2012. He joined the School of Computer and Communication Engineering, Changsha University of Science and Technology, in 2000, where he is currently a Full Professor. His research interests include smart grid, and network and information security. He has published more than 50 research papers in journals or conferences.

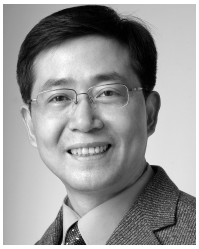
HONG ZHOU is currently pursuing the master's degree with the School of Computer and Communication Engineering, Changsha University of Science and Technology. Her research interests include smart grid and its security.



KE GU received the Ph.D. degree from the School of Information Science and Engineering, Central South University, Changsha, China, in 2012. He joined the School of Computer and Communication Engineering, Changsha University of Science and Technology, in 2013, wher he is currently an Assistant Professor. His research interests include smart grid, and network and information security. He has published more than 50 research papers in journals or conferences.

BO YIN received the Ph.D. degree from the School of Information Science and Engineering, Hunan University, Changsha, China, in 2013. She joined the Hunan Provincial Key Laboratory of Intelligent Processing of Big Data on Transportation in 2013, where she is currently an Assistant Professor. Her research interests include data mining, data process, and network and information security. She has published more than 20 research papers in journals or conferences.

YOUYOU ZENG is currently pursuing the master's degree from the School of Computer and Communication Engineering, Changsha University of Science and Technology. Her research interests include smart grid and its security.



MING XU received the B.S. and M.Sc. degrees from Wuhan University in 1984 and 1987, respectively, the Ph.D. degree from the National University of Defense Technology (NUDT) in 1995. Since 1987, he has been with the School of Computer, NUDT. He is currently a Full Professor. His research interests include wireless networks, mobile computing, cloud computing, and network security. He has published four co-authored books and more than 180 research papers.