AI-Based Joint Optimization of QoS and Security for 6G Energy Harvesting Internet of Things

Bomin Mao, *Member, IEEE*, Yuichi Kawamoto, *Member, IEEE*, and Nei Kato, *Fellow, IEEE*

***Abstract*—The data privacy and confidentiality in Internet-of-Things (IoT) networks have been one of the most concerned problems due to increasing threats. The commonly utilized IoT chips adopt a fixed authentication and encryption scheme in the link layer even though multiple options are usually supported. As different authentication and encryption operations mean dissimilar protections and various energy consumption, the fixed security strategy neglects the remaining energy, dynamic threats, and diverse service requirements, leading to low energy efficiency. Moreover, fixed high-level security protections consume too much energy even though the security requirement may be low, which results in a short working time. To address this problem, we propose an artificial intelligence (AI)-based adaptive security specification method for 6G IoT networks where the IoT devices are connected to cellular networks via different frequency bands, including terahertz (THz) and millimeter wave (mmWave). The IoT sensing devices are assumed to support the energy harvesting technique which is expected to be widely adopted in 6G. In our proposal, the extended Kalman filtering (EKF) method is first adopted to predict future harvesting power. Then, in each energy-aware cycle, we design a mathematical model to calculate the required energy of different security strategies and choose the supported highest level protection which can meet service requirement and avoid energy exhaustion. The simulation results illustrate that the proposal can not only provide satisfied security protection for different services but also adjust the security protection to avoid the energy exhaustion, leading to a significant improvement of throughput and working time.**

***Index Terms*—6G Internet of Things (IoT), artificial intelligence (AI), energy harvesting, Quality of Service (QoS), security.**

I. Introduction

RECENTLY, the 5G specification gets nearly completed and researchers have paid their attention to 6G [1]. The mobile communication carriers in many countries are competing to deploy the new generation of infrastructure since a great number of new Internet services are expected to become new profit growth points. Among the various potential Internet services, it has been widely acknowledged that the Internet of Things (IoT) is projected to grow significantly over the coming years since it can incorporate transparently and seamlessly a large number of heterogeneous end nodes to provide users with great convenience. To provide high-speed access service, a massive number of IoT devices are expected to be connected to 6G via heterogeneous base stations as shown in Fig. 1. Different from traditional IoT networks, 6G IoT also has some new characteristics. First, the limitations of constrained battery and computation capacity will be significantly alleviated by the energy harvesting and mobile-edge computing (MEC) techniques [2]. Various energy sources, such as the solar and radio-frequency signals will be utilized to offer IoT devices energy continuously. Some latency-sensitive computation tasks will be offloaded to the edge servers instead of being transferred to the cloud servers to realize real-time data processing. Second, the radio resource in high-frequency bands, including the millimeter wave (mmWave) and terahertz (THz) is expected to be adopted in the short-range bandwidth-aggressive IoT services [1]. Then, the achievable peak data rate of 6G IoT services can be much higher than that of 5G IoT. For the long-range IoT services as shown in Fig. 1, the unmanned aerial vehicles (UAVs) have been acknowledged as the efficient and practical NodeB to provide intime communication and computation assistance as well as to enlarge the coverage area of base stations [2]. Finally, 6G will widely adopt the artificial intelligence (AI), including the deep learning and other machine learning techniques to realize intelligent communication and networking as shown in Fig. 1 [3], [4].

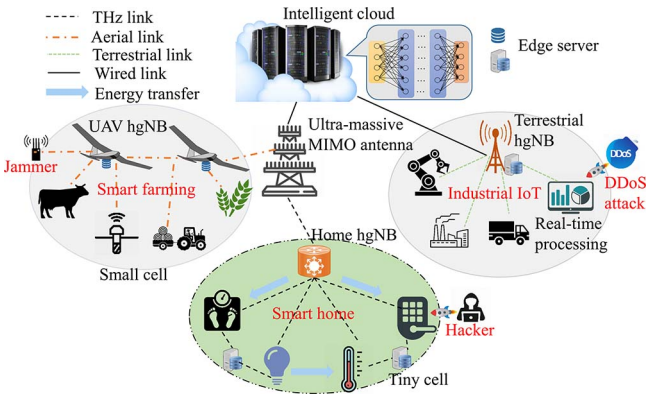

Fig. 1. Intelligent 6G IoT network scenarios.

Due to the exponentially increasing network threatens, data privacy and confidentiality will be one of the most concerned problems for future 6G networks [5], [6]. The IoT network threats usually consist of the computer virus, DDoS attacks, and eavesdroppers, which not only threaten the message safety but also deteriorate the Quality of Service (QoS) [7], [8]. To protect the message safety, various policies have been

Manuscript received December 7, 2019; revised February 23, 2020; accepted March 9, 2020. Date of publication March 23, 2020; date of current version August 12, 2020. *(Corresponding author: Bomin Mao.)*

The authors are with the Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan (e-mail: bomin.mao@it.is.tohoku.ac.jp; youpsan@it.is.tohoku.ac.jp; kato@it.is.tohoku.ac.jp).

Digital Object Identifier 10.1109/JIOT.2020.2982417

developed, which mainly concentrate on the physical layer [9], [10] and link layer [11], [12]. As we know, the link-layer security protection of IoT networks is mainly realized by the data authentication and encryption process. Existing encryption and authentication methods have parameter configurations, including the key lengths and the adopted algorithm, which result in diverse security protection and various energy consumption. Even though current IoT chips usually support multiple security specifications, the common manner is to fix the encryption and authentication configuration in the chip initialization process, which simplifies the network configuration and fits for the resource-constrained IoT chips.

However, this fixed security configuration may not meet the stringent service requirement of 6G networks for network QoS, energy efficiency, and message safety. This is because the network threats are usually dynamic, which may be far beyond the provided fixed low-level protection. Also, the security protection means extra energy consumption and a fixed high-level security configuration can quickly run out of batteries, resulting in the cease of service provision, which means that the fixed security configuration has the limitation of low energy efficiency. Considering the widely adopted energy harvesting techniques and service requirements in future 6G networks [13], the ideal security configuration should be adaptive to the available energy and network threats, which can jointly improve the security protection and network performance. However, due to the network threats are usually unknown, the practical strategy is to try to improve the security protection according to the available energy. Specifically, when the harvesting source does not provide enough power or the IoT devices have a heavy sensing workload, we can consider the minimum level of required security protection to maximize working time. Otherwise, when the harvesting power is large, the provided security protection can be improved for better message safety. Another problem is that the sacrifice of network QoS caused by the extra communication overhead and energy consumption to provide security protection is usually neglected. For the 6G IoT, as the network QoS is also very important, the sacrifice due to the security should be minimized. Therefore, the goal of our research is the joint optimization of QoS and security for the harvesting-based 6G IoT networks.

In this article, we consider a 6G IoT network as shown in Fig. 1 and the adopted IoT devices commonly denoted as user equipment (UE) support multiple security configurations. As we mentioned above, we consider the service requirements and available energy when designing the security configuration method. Generally, the service requirement is usually available, thus, we need to obtain the available energy in a short period. For the harvesting-enabled IoT networks, the available energy depends on the battery and harvesting source. Some harvesting sources are predictable, such as the radio frequency and solar, while the others are unpredictable including the vibrations in an indoor environment [14]. For the predictable harvesting sources, some lightweight AI techniques including the extended Kalman filtering (EKF) can be adopted to forecast the harvesting power in a short period [15]. In this article, we consider the predictable energy sources and utilize the EKF technique to predict the harvesting power. It should be noted that the energy consumption is a long-term process, while the prediction of harvesting power is limited in a short period, which can be regarded as an energy-aware cycle. The energy-aware cycle can be further divided into many small time slots, during which the harvesting power is assumed as constant. Then, in each time slot, we can calculate the consumption of different security specifications and find the supported security suites. If there is no supported suite, the IoT devices stop generating packets in that time slot. Otherwise, we iteratively find the best security protection in each time slot which does not affect the working states of the following time slots in the energy-aware cycle. Therefore, our proposal can try to improve the security protection and guarantee the maximum working time in each energy-aware cycle. The contributions of this article can be summarized as follows.

1) We discuss the authentication and encryption methods in the IoT link layer. After analyzing the energy consumption of different security schemes, a tradeoff between the security and QoS is given in this article.
2) To predict the harvesting power, a lightweight AI method is adopted and the complexity is studied. The results evaluate the high accuracy rate of the proposed AI method.
3) A mathematical model considering the diverse service requirements as well as the energy harvesting is proposed to choose the security configurations in 6G IoT networks. Through this method, we jointly optimize the security provision and network QoS, which further results in the improved Quality of Experience (QoE).

The remainder of this article consists of six parts. Section II introduces the existing research about the security protection of IoT networks. The following section gives some preliminaries of existing security operations in the IoT link layer and the adopted EKF method. In Section IV, we introduce the considered system model and explain the problems of conventional security configuration methods. Then, the proposed method and performance analysis are given in Sections V and VI, respectively. Finally, we conclude this article in Section VII.

II. Related Research Work

As we know, a growing number of IoT services are concerned with personal information, which results in the increasing importance for the network service providers to offer qualified security protection. According to Sastry and Wagner's research [14], the link-layer security consists of access control, message integrity, confidentiality, and replay protection. To provide qualified security protection, multiple strategies have been defined in different IoT access protocols. For example, IEEE 802.15.4 defines eight different security suites to meet the various requirements for link-layer security. As described in [14], the process of encryption and authentication can secure the provided services, but increase packet length, which leads to more resource cost for their transmissions. Alharby *et al.* [16] first discussed the energy consumption of different security levels, and then studied their impacts on data latency and throughput. The result shows that the maximum

authentication length can decrease the throughput by almost 53%, while encryption and authentication together by almost 62%. For the resource-constrained IoT devices in conventional IoT networks, the security protection means the sacrifice of network QoS. Then, Nieto and Lopez [17] analyzed the tradeoff between security and QoS for resource-constrained networks, which illustrates the necessity to consider QoS when conducting the security configuration.

To achieve a balance between the security level and network QoS has aroused researchers' interest and some joint optimization methods have been proposed. Fadlullah *et al.* [18] utilized the game theory to select the security scheme and conducted the bandwidth allocation in order to overcome the threats as well as optimize QoS to meet the diversified requirements in heterogeneous networks. Haleem *et al.* [19] adopted mathematical models to capture the security-throughput tradeoff and proposed the opportunistic encryption to maximize the network throughput. Shen and Thomas [20] studied the mechanisms to optimize the QoS/security while maintaining a minimum user acceptable level of security/QoS for a distributed dynamic management system. The simulation results evaluate the performance improvement. However, these works mainly focus on the general cellular networks and do not consider the resources, including battery and computation capacity for IoT devices. Aman *et al.* [21] proposed a token-based security protocol for IoT networks which can achieve dynamic energy–quality tradeoff. Aman *et al.* [22] focused on the authentication and privacy preservation in IoT systems and an energy-saving security protocol is proposed. We can find these papers mainly concentrate on the security protocol design to reduce the energy consumption. For 6G IoT scenarios where the energy harvesting technique is expected to be widely adopted, the security configuration method should be further studied.

III. Preliminaries of the Link-Layer Security and Extended Kalman Filtering Technique

In this section, we first give some introductions and basic strategies about the link-layer security. Then, we discuss the utilized EKF method, including its theory and equations.

A. Link-Layer Security

Generally speaking, the link-layer security strategies should provide the protection consisting of access control, message integrity, confidentiality, and replay protection [14]. The following paragraphs discuss these services and introduce the basic theory, after which some commonly utilized schemes in IoT networks are studied.

In the link layer, the access control and message integrity can be realized by authentication operations [23]. Specifically, the access control means that the unauthorized IoT devices should be rejected to participate in the network and messages from illegal nodes need to be detected by legitimate ones. In a secure network, the legitimate users should share the session keys for authentication operations. Moreover, the sender can utilize the keys to compute a cryptographically secure checksum for the message named message integrity code (MIC) and include it in the message. The authorized users can utilize the shared keys to recompute the MIC to check whether the packets have been forged or not. For the hacker, it is necessary to revise the payload as well as the MIC in order to deceive the authorized recipient. Then, a longer MIC can increase the difficulty in decoding the authenticated messages. On the other hand, the longer MIC also means more communication and computation overhead. Various authentication strategies have been proposed for the IoT networks, such as the cipher block chaining MIC (CBC-MIC) and hash-based MIC [24].

The information confidentiality is protected by the encryption process in IoT networks. As many IoT services are concerned with personal or privacy information, including the smart health and industrial IoT, it becomes increasingly important to protect the packets against the intruders or hackers. Generally, the encryption process is to use the encryption key to encode the messages and authorized recipient can read the messages after the decryption process. The effectiveness of the encryption process depends on the key length. For a key with N bits, there are 2^N different combinations. Therefore, the brute force attacks need to be conducted 2^N time for success decryption by illegal nodes. However, the longer encryption keys also mean higher complexity in the encryption and decryption process. The commonly used encryption algorithms in the IoT network consist of the data decryption standard (DES), tripleDES, RSA, advanced encryption standard (AES), and twofish. For a key of N bits, there are 2^N possible combinations. Therefore, to crack the key, the brute force attacks need to be repeated for 2^N times in the worst case. This motivates us a choice of security measure $S^{(N)}$ to be as follows:

$$S^{(N)} = \log_2 N. \tag{1}$$

This equation also applies to measure the security protection provided by MICs of different lengths. For example, for an MIC of N bit, the probability of successful forgery is 2^{-N}.

The replay protection is usually realized via a sequence number assigned by the sender. The sequence number can be utilized by the receiver to judge whether the message is from the authorized sender or eavesdropper. Since the impact of replay protection on the energy consumption is much smaller than the authentication and encryption process, we can just assume the replay protection is adopted for every IoT device and ignore its impacts. More details can be referred to [14].

B. Basic Theory of the Extended Kalman Filtering Technique

As we mentioned above, the knowledge of future harvesting power can help to improve the security configurations. Even though many energy sources have the nature of stochastic, such as the solar, winding, and some radio frequency signals [25], the correlation between further harvesting power and the most recent data. Additionally, the factors which have impacts on the amount of harvesting energy are not our focus in this article. We consider the EKF method due to its ability to adapt to the stochastic characteristic of predicted metric [26]. To make the prediction process more practical, it is reasonable to assume that the harvesting power keeps constant for

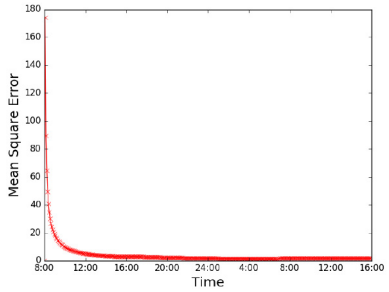

Fig. 2. MSE of the prediction process.

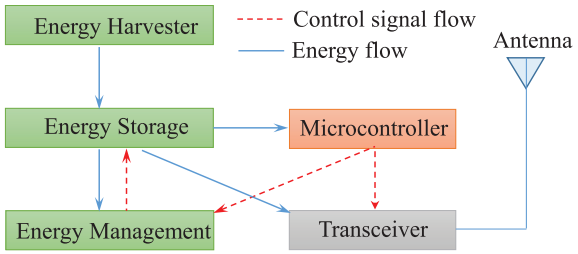

Fig. 3. Structure of considered UE.

a short time slot. Then, it is a discrete-time prediction process to forecast the harvesting power in each time slot. The EKF method belongs to the lightweight prediction methods, allowing easy deployment in IoT scenarios. The following paragraphs introduce the equations of EKF.

The EKF algorithm assumes the true state at time k is evolved from the state at $k-1$ and the measurement value is affected by the system and noise, which can be expressed in the following equations:

$$\boldsymbol{x}_k = f(\boldsymbol{x}_{k-1}, u_k) + \boldsymbol{\omega}_k \tag{2}$$

$$z_k = h(\boldsymbol{x}_k) + \boldsymbol{v}_k \tag{3}$$

where $\boldsymbol{x}_k$ and $\boldsymbol{x}_{k-1}$ are the true state values at time k and $k-1$, respectively. z_k is the measurement state value. $\boldsymbol{u}_k$ is the control vector. $\boldsymbol{\omega}_k$ and $\boldsymbol{v}_k$ represent the process noise and observation noise which are both assumed to be zero-mean multivariate Guassian noises with covariance $\boldsymbol{Q}_k$ and $\boldsymbol{R}_k$: $\boldsymbol{\omega}_k \backsim N(0, \boldsymbol{Q}_k)$ and $\boldsymbol{v}_k \backsim N(0, \boldsymbol{R}_k)$, respectively. Functions f and h are usually unknown and cannot be applied to the covariance directly. The common manner is to compute the Jacobian matrices $\boldsymbol{F}_k$ and $\boldsymbol{H}_k$ through the partial derivation process. The notations in bold mean vectors for multiple metric estimation and can be replaced with scalars for single metric case.

From (2) and (3), it can be found that the true state value is predicted only by last state recursively. Current measurement value is related to the true state value $\boldsymbol{x}_k$. Therefore, the EKF works in a two-step process: 1) the prediction step and 2) update step. The prediction step follows a recursive manner and the prediction uncertainty is also given according to the following equations:

$$\hat{\boldsymbol{x}}_k = f(\hat{\boldsymbol{x}}_{k-1}, u_k) \tag{4}$$

$$\boldsymbol{P}_k = \boldsymbol{F}_{k-1}\boldsymbol{P}_{k-1}\boldsymbol{F}_{k-1}^{\mathrm{T}} + \boldsymbol{Q}_{k-1} \tag{5}$$

where $\hat{\boldsymbol{x}}$ is the predicted value, $\boldsymbol{F}^{\mathrm{T}}$ represents the transpose of $\boldsymbol{F}$, and $\boldsymbol{P}$ is the error covariance. It can be found the prediction step in EKF is *a priori* estimation process which utilizes the previous state instead of current measurement. After the prediction process, the update process can be conducted to adjust the values of predicted state value and its error covariance as follows:

$$3\boldsymbol{G}_k = \boldsymbol{P}_k\boldsymbol{H}_k^{\mathrm{T}}\left(\boldsymbol{H}_k\boldsymbol{P}_k\boldsymbol{H}_k^{\mathrm{T}} + \boldsymbol{R}\right)^{-1} \tag{6}$$

$$\hat{\boldsymbol{x}}_k \leftarrow \hat{\boldsymbol{x}}_k + \boldsymbol{G}_k\left(z_k - h(\hat{\boldsymbol{x}}_k)\right) \tag{7}$$

$$\boldsymbol{P}_k \leftarrow (\boldsymbol{I} - \boldsymbol{G}_k\boldsymbol{H}_k)\boldsymbol{P}_k \tag{8}$$

where $\boldsymbol{G}$ represents the Kalman gain matrix. From (7), the measurement value z_k is utilized to update the prediction of $\boldsymbol{x}$, for which this is *a posteriori* process.

To show the performance of the EKF technique, we conduct some simulations with the data from online [27]. We adopt the EKF model to predict the harvesting solar power in two serial days and calculate the mean square error (MSE) as shown in Fig. 2. We can find that the value of MSE decreases very fast and reaches nearly 0 after 16:00 on the first day. This means that the EKF method can achieve a highly accurate estimation of harvesting power.

IV. Considered System Model and Problem Statement

In this section, we first introduce the considered system model, including the network scenario and energy consumption. Then, we make some analysis about the existing problem of the conventional security configuration method.

A. System Model

In this article, we consider the cellular-based IoT networks, where the IoT devices denoted as UEs are connected to the heterogeneous NodeBs (hgNBs) which consist of the terrestrial hgNBs, the aerial hgNBs (UAVs), and the home hgNBs as shown in Fig. 1. In this article, the uplink for UEs utilizes the single carrier-frequency-division multiple access (SC-FDMA) scheme, while the downlink considers the orthogonal frequency-division multiple access (OFDMA) strategy, which is widely applied in the cellular communication networks [28]. Since the energy consumption of UEs is mainly from the packet generation and transmission to the hgNBs, we only consider the uplink transmissions.

First, we give a simple structure of the considered harvesting-enabled IoT devices as shown in Fig. 3. The most important parts for UEs mainly consist of the microcontroller and energy storage unit. The former is mainly in charge of packet processing and energy management, while the latter is responsible for saving and offering energy for every part. In Fig. 3, the energy prediction part can forecast the harvesting power and then calculate the available energy before generating the packets. For each UE, the energy consumption to send a packet to the hgNB can be denoted as follows:

$$E = E_{\mathrm{comp}} + E_{\mathrm{comm}} \tag{9}$$

where E represents the total energy consumption for computation E_{comp} and communication E_{comm}. The computation work

for a UE includes generating a packet as well as required authentication and encryption operations. Generally, the value of E_{comp} is growing with the increasing packet length and operation complexity. The detailed value is dependent on the adopted chips and can be obtained by experiments. However, as the supported security scheme is usually fixed for a given chip, the value of E_{comp} can be regarded as the hardware specifications, which are usually available from the manufacturers. Since we only consider the uplink communication process in this article, the communication energy consumption mainly comes from packet transmissions from UEs to hgNBs, therefore we can get the following equation:

$$E_{\text{comm}} = E_t = P_t t \tag{10}$$

where P_t denotes the transmit power and t represents the time cost to send a packet. t can be easily calculated since the transmission rate and packet length are usually available. The value of P_t needs to be calculated according to the service signal-to-interference-plus-noise ratio (SINR) requirement and the definition of SINR is given as follows:

$$\begin{aligned} \text{SINR} &= \frac{P_r}{I + N_0} \\ &= \frac{P_t}{L(I + N_0)} \end{aligned} \tag{11}$$

where P_r is the received power at the hgNB side. N_0 and I denote the noise power and intercell interference. L is the path loss.

B. Problem Statement

To describe the problem more clearly, we consider a simple scenario where a UE periodically generates and transmits packets to hgNB at a constant rate. The UE has a battery of 1000 mAh and is not harvesting enabled. Thus, the UE's lifetime ends once it uses up the battery. For simplicity, we consider the transmission power is 20 mW and 2 packets are transmitted every second. The IoT service provided by the UE is concerned with no privacy, meaning that only authentication operation is required. We adopt the MIC to authenticate the packets and the length of MIC ranges from 0 to 256 b. The packet payload is fixed at 40 B, meaning that the total length is dependent on the MIC. The packet transmission rate is 250 Kb/s. As the energy consumption of encryption and authentication operations depends on not only the algorithm complexity but also the adopted hardware and operation systems, it is difficult to calculate the detailed value of E_{comp}. Here, we just assume that E_{comp} is equal to 15% of the communication energy consumption E_{comm}, which is an average value according to the research [16]. Then, we can compare the lifetime of UE with the security protection of different MIC lengths as shown in Fig. 4.

From Fig. 4(a), it can be clearly found that the lifetime decreases with the increasing length of MIC. Moreover, compared with no security scheme where the MIC length is 0, the lifetime with MIC of 256 b is much shorter even though it can provide the best protection, which means that a tradeoff exists between the lifetime and security protection. To show

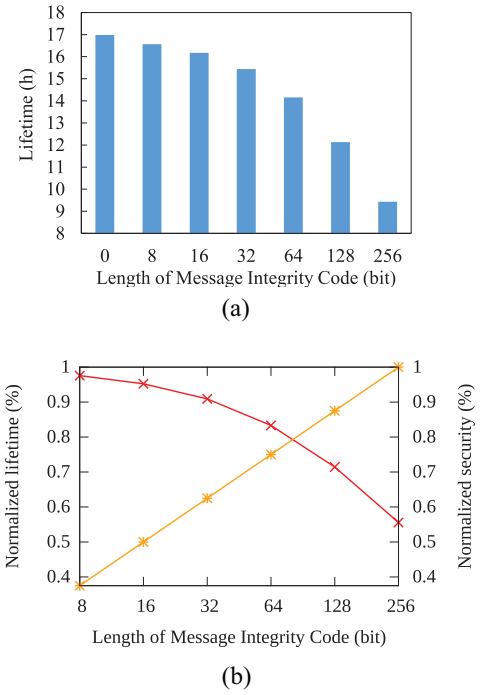

Fig. 4. Lifetime and provided security quality with different authentication schemes. (a) Lifetime with different authentication schemes. (b) Normalized lifetime and security with different authentication schemes.

the tradeoff more clearly, we normalize the lifetime and provided security by their maximum values and give the result in Fig. 4(b). We can find that the improvement of security protection is at the sacrifice of UE lifetime. Here, it should be noted that the security protection is calculated by (1). The assumption that the UE generates two packets every second is much higher than practical applications, which leads to much shorter lifetime. In our real-life use, the UE may generate only one or two packets every day for some services such as the air quality monitoring, where our conclusion still applies.

Considering the network threats are usually dynamic, the fixed security configuration is not suitable for the battery-constrained IoT devices. This is because a fixed high-security protection costs too much energy according to the above analysis, while the fixed low scheme cannot provide qualified protection when the serious threats exist in the network. However, the conventional security strategy usually adopts a fixed high-security scheme to prevent any potential attacker even though current IoT end devices usually support multiple security specifications. Considering 6G networks will widely utilize the energy harvesting technique to address the energy constraints, the varying available energy is another factor to motivate us to develop an adaptive security scheme to meet the diverse service requirements and changing network threatens [29]. The following section will introduce our proposal of adaptive security protection considering the harvesting power, service requirements, and network threatens.

V. Proposed Joint QoS and Security Optimization Method

In this article, we consider that all the UEs can harvest the energy and the power is predicted with the EKF technique.

The UEs periodically generate packets and send to the hgNBs. In the packet generation process, the UEs need to choose the security configuration to protect the messages, since different safety schemes result in various energy consumption. To guarantee the received messages can be accurately decoded, we assume each IoT service has a minimum SINR threshold at the receiver side which is a common way to measure the quality of wireless links. In our proposal, what the UEs need to do consists of two parts: 1) predicting the harvesting power and 2) choosing the security configurations. The results of harvesting power prediction with the EKF method can be adopted to calculate the available energy. For each UE, the transmission power can be calculated according to the SINR requirement, which is further utilized to measure the energy consumption of processing and transmitting a packet with different security protection schemes. Then, the UEs can select the security scheme to provide qualified protection as well as maximize the working time. If the available energy cannot support any qualified security scheme, the IoT devices are assumed to stop work. Here, we assume the service requirement for security is available and the packet generation rate is constant. Thus, the QoS optimization is equal to maximize the working time. However, it is a nonconvex and complex problem to optimize the security protection and working time in the whole life of UEs since we cannot know the harvesting power during the whole life of each IoT device. Considering the EKF technique can only predict the harvesting power in a short period using the most recent data, we divide the time into many cycles of equal length denoted as ΔT and the EKF method can predict the harvesting power in one cycle each time. Additionally, we attempt to divide the long-term process into many short intervals, each of which has a length of Δt. In each Δt, it is reasonable to assume the harvesting power is a constant for a UE, even though the harvesting power is dynamic in ΔT. Furthermore, the energy-aware cycle ΔT satisfies the relationship: $\Delta T = K\Delta t$. The following paragraphs introduce our proposed mathematical model and algorithm to optimize the working time and security protection.

A. Proposed Mathematical Model to Optimize QoS and Security

As the harvesting power is dependent on the harvesting sources which are dynamic, the research aims to adjust the security protection to maximize the working time and provide qualified protection. Moreover, the security configuration should consider the service requirements as well as the available energy. Then, the studied problem can be expressed as follows:

$$\max \sum_{i=1}^{K} w(i)\Delta t \tag{12}$$

$$\text{s.t. } w(i) \in \{0, 1\} \tag{13}$$

$$\sum_{i=1}^{K'} E(i)r(i)w(i)\Delta t \le E_r + \sum_{i=1}^{K'} P_h(i)\Delta t \tag{14}$$

$$S(i) \ge S_{\text{req}}(i) \tag{15}$$

$$\text{SINR}(i) \ge \text{SINR}_r \tag{16}$$

where the binary parameter $w(i)$ represents whether the UE works in the ith time slot of the energy-aware cycle ΔT. Then, (12) can describe our goal to maximize the total working time in the energy-aware cycle. Equation (14) gives the energy constraint that the energy consumption cannot exceed the available energy, including the remaining battery E_r, and harvesting energy. Here, $E(i)$, $r(i)$, and $P_h(i)$ denote the energy consumption, packet generation rate, and harvesting power at the ith time slot, respectively. It should be noted that in (14), the value of K' equals $\{1, 2, \ldots, K\}$, meaning that the energy constraint should be satisfied in each time slot. The value of $E(i)$ is deeply related to the chosen security level $S(i)$ and the transmission power $P_t(i)$ in the ith time slot. The value of $r(i)$ can be assumed available. The value of $P_h(i)$ is predicted by the EKF method. Furthermore, considering the diversified service requirements, we utilize $S_{\text{req}}(i)$ to denote the lower bound of service requirement for security in the ith time slot as shown in (15). Different IoT services have various SINR requirements SINR_r, which is described in (16).

The above equations can be utilized to obtain the working slots, of which the orders can be denoted as $W = \{i | w(i) = 1\}$. The number of units in W represents the maximum number of working time slots in the energy-aware cycle. Moreover, for each time slot in W, there may exist multiple qualified security schemes. In this case, the security protection should be optimized because the network threats are unavailable. Then, we can construct the following model to optimize the provided security protection in each working slot:

$$\max S(k) \tag{17}$$

$$\text{s.t. } w(k) = 1 \tag{18}$$

$$w(i) = 1 \quad \text{for} \quad i \in W \tag{19}$$

where (18) means that we only focus on the security for the working time slots. Also, the configuration of security in any time slot should not sacrifice the following working slots in W as shown in (19).

B. Proposed Joint QoS and Security Optimization Algorithm

As we mentioned above, the chips utilized by current UEs usually support at least one pair of encryption and authentication algorithms. The encryption key can support variable lengths, while the adopted authentication algorithms can also have diverse complexity, which results in different energy consumption. Different from the message integrity which is needed for all kinds of services, the encryption operation is only necessary for the private information to provide the confidentiality protection. Therefore, it is reasonable to divide the supported security configurations into three groups: 1) no security; 2) authentication only; and 3) both authentication and encryption, which can be represented by S_{no}, S_a, and S_{ae}, respectively. The different security suites in latter two groups can be arranged in the order of increasing security protection, which can be denoted as $S_a = \{s_{a,i} \in S_a | i = 1, 2, \ldots, m\}$ and $S_{ae} = \{s_{ae,i} \in S_{ae} | i = 1, 2, \ldots, n\}$. When a UE chooses the security configuration, it needs to consider the corresponding energy consumption to process and transfer the

Algorithm 1 Energy-Aware Security Configuration Method
Input: $SINR_r$, d, E_r, $E_h(i)$, and $S_{req}(i)$, where $i = 1, 2, \ldots, K$

1: Calculate the transmission power
2: Select the allowable security suite group S_k according to the requirement
3: $i = 1$
4: **while** $i < K$ **do**
5: **for** $i \le j \le K$ **do**
6: Calculate $E_{max}(j) = \frac{E_a(j)}{(j-i+1)\Delta t}$
7: Choose the allowable highest security suite, S_r, according to the supported maximum power
8: **end for**
9: Find $r^* = min\{r\}$
10: Find $i^* = max\{arg\{r^*\}\}$
11: The chosen security suite between the i^{th} and i^{*th} time slots is S_{r^*}
12: $i \leftarrow i^* + 1$
13: **end while**

packets to the hgNB. Here, we can use E_{no}, $E_a = \{E_{a,i} \in E_a | i = 1, 2, \ldots, m\}$, and $E_{ae} = \{E_{ae,i} \in E_{ae} | i = 1, 2, \ldots, n\}$ to denote the energy consumption of security groups S_{no}, S_a, and S_{ae}, respectively. It is reasonable to assume that in each security suite group, the better security protection means more energy consumption. Therefore, the relationships $E_{a,1} < E_{a,2} < \cdots < E_{a,m}$ and $E_{ae,1} < E_{ae,2} < \cdots < E_{ae,n}$ are satisfied. Additionally, E_{no} has the minimum value, while $E_{a,i}$ is smaller than $E_{ae,i}$.

After introducing the available security suites and their energy consumption, we discuss the proposed method to select the security schemes as shown in Algorithm 1. The method to calculate the interference I and noise power N_0 is not the focus of this article and we just assume that they are available. Therefore, the UEs can calculate the minimum transmission power according to required SINR and distances to hgNBs with (11). Then, the UEs can calculate the energy consumption of different security suites and then choose the satisfied security suites S_k as shown in steps 1 and 2. Here, if the provided IoT services are confidential, the UEs need to consider the security group S_{ae}, while S_a is adopted by the services requiring only message integrity. S_{no} is usually not adopted and considered here as a benchmark method. Then, we focus on the security selection in the energy-aware cycle ΔT and choose the suite for each constant power interval Δt. The details are given by steps 5–8 in Algorithm 1. We first calculate the supported maximum energy consumption in each Δt as in step 6, which can be utilized to find the supported highest level of security scheme S_r as shown in step 7. Then, shown in steps 9 and 10, we find the minimum security level S_{r^*} among the maximum security schemes for all intervals, and the index of corresponding time interval i^*. Next, we adopt security suite S_{r^*} from the ith interval to the i^*th interval, which can provide the required security protection as well as continuous service. We repeat the process for the following time intervals until the security suites for the whole ΔT are decided. It should be noted that if the available energy is not enough for any security scheme, the UEs will not generate packets and only harvest the energy. We can find that the proposed security configuration is adaptive to the energy harvesting and all the packets sent by the UEs satisfy the service requirements for safety. Moreover, this method can maximize the working time and optimize the offered security protection.

After introducing the proposal, we analyze its complexity. According to our introduction, the proposal mainly consists of two parts: 1) the harvesting power prediction and 2) adaptive security suite selection. The harvesting power prediction is realized by the EKF technique. For each IoT device, the complexity to predict the power in K time slots is $O(K)$ according to (2)–(8). In the following security selection process, the complexity for each UE is $O(K^2)$ as shown in Algorithm 1. Therefore, for each UE, the total complexity of our proposal is $O(K^2+K)$. Moreover, if we consider the edge servers conduct the proposed security configuration strategy, the complexity is $O(nK^2)$, where n is the number of IoT devices covered by each edge server. As the value of K is usually very small to guarantee the accuracy rate of energy prediction, the relationship $n \gg K$ satisfies. Thus, if the proposal is run in the centralized manner, the complexity for each edge server can be regarded as $O(n)$, while that for each UE is $O(1)$ in a distributed way. It can be found that the proposal has very low complexity no matter the proposal is conducted in a distributed manner or centralized manner.

VI. Performance Evaluation

To evaluate the performance of our proposal, we conduct the simulation considering three 6G IoT scenarios as shown in Fig. 1. Even though the three scenarios: 1) smart farming; 2) smart home; and 3) industrial IoT have been widely applied in 5G networks, they will have some new characteristics in 6G era. In the smart home scenario, the carrier frequency band up to 1 THz will be considered, and then the transmission range of each hgNB is shortened to within 10 m. Therefore, at least one hgNB will be deployed in each house to realize full coverage. For each UE in the smart home scenario, the considered peak data rate is 20 Mb/s, which enables the transmissions of multimedia messages for future 6G IoT services. The industrial IoT application utilizes mmWave as the carrier and the frequency band is up to 30 GHz. The peak data rate provided to each UE is 5 Mb/s and the edge computing servers are deployed at the hgNBs for local real-time processing. The wireless channels of UEs and hgNBs using THz and mmWave frequencies are expected to experience approximately 35-dB/km attenuation due to the atmospheric absorption in the natural Friis free space [30]. In the smart farming scenario, the UAVs are assumed to be widely adopted as hgNBs and provide periodical communication services for the UEs. As the IoT sensing devices in the smart farming scenario usually have limited routine workload, the operating frequency is considered as 2 GHz and the peak data rate for each UE is 250 Kb/s. The values of key parameters are shown in Table I. In the three IoT scenarios, we consider three adjacent cells which adopt orthogonal channels to avoid the intercell interference for simplicity. Therefore, only the noise is considered in the simulation process to calculate the transmit power for each UE. In this article, the calculated white noise power at the hgNB side is -96 dBm. The proposed strategies can be also applied for the scenarios considering the intercell interference.

Even though there exist different IoT devices in the considered three scenarios, to illustrate the conclusion more clearly,

TABLE I
SIMULATION PARAMETER VALUES FOR SMART HOME, INDUSTRIAL IOT, AND SMART FARMING SCENARIOS

Parameter	Value
Carrier frequency	1 THz
Cell radius	10 m
#cell	3
#UE	50
Transmission rate	20 Mbps
Payload length	65 byte

Parameter	Value
Carrier frequency	30 GHz
Cell radius	1 km
#cell	3
#UE	1000
Transmission rate	5 Mbps
Payload length	100 byte

Parameter	Value
Carrier frequency	2 GHz
Coverage diameter	5 km
#UAV	3
#UE	500
Transmission rate	250 kbps
Payload length	50 byte

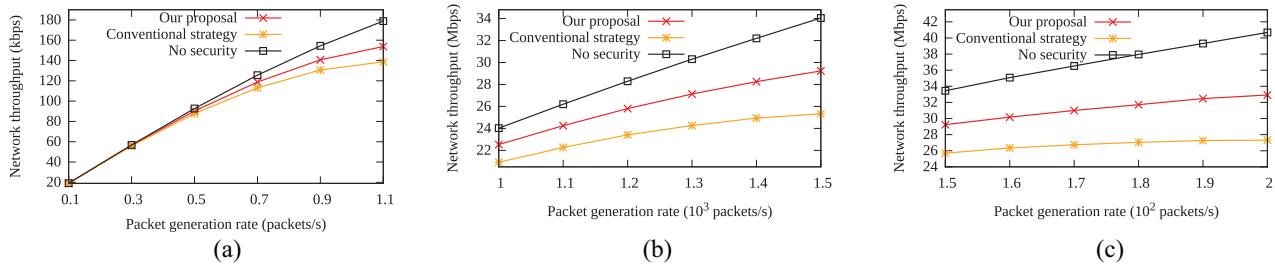

Fig. 5. Comparison of our proposal and conventional security strategies in terms of aggregate throughput in three 6G IoT scenarios. (a) Aggregate throughput in the smart farming scenario. (b) Aggregate throughput in the smart home scenario. (c) Aggregate throughput in the industrial IoT scenario.

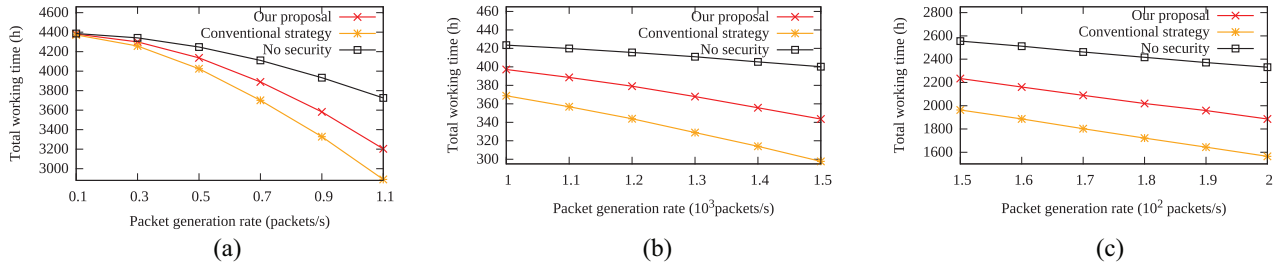

Fig. 6. Comparison of our proposal and conventional security strategies in terms of total working time in three 6G IoT scenarios. (a) Total working time in the smart farming scenario. (b) Total working time in the smart home scenario. (c) Total working time in the industrial IoT scenario.

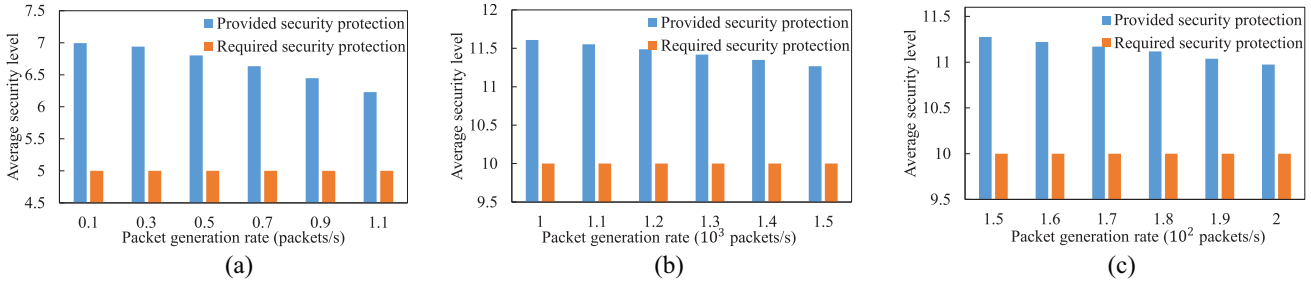

Fig. 7. Provided the average security level of our proposal in three 6G IoT scenarios. (a) Provided security protection in the smart farming scenario. (b) Provided security protection in the smart home scenario. (c) Provided security protection in the industrial IoT scenario.

we focus on the most common requirements for SINR, confidentiality, and message accuracy, which can be further divided into three levels denoted as high, common, and low. Generally, in the smart farming scenario, the IoT services, such as the humidity and temperature monitoring usually have low privacy requirement, meaning that only the authentication is necessary to prevent the potential advisory forgery. Also, its requirement for SINR is low due to the limited data rate. As the packets are not continuously collected by the UAVs, the message integrity is important for this service. On the other hand, the smart home services including the smart surveillance cameras usually contain a lot of personal information privacy, which is the target of hackers and eavesdroppers. It also generates more packets than smart farming services and needs higher SINR. Moreover, the repeated measurement in this service can minimize the loss caused by attackers. Therefore, the requirement of smart farming service and smart home service for SINR, confidentiality, and accuracy can be denoted as {low, low, high} and {common, high, common}, respectively. For the industrial IoT service such as the robots, it contains a lot of real-time monitoring work, which requires high SINR to guarantee its bandwidth. The packets often include important information requiring high accuracy. Also, some information should be also secret from the competitors. Therefore, the potential threats for the industrial IoT should consist of the advisory forgery and eavesdroppers. The

requirement for industrial IoT is assumed to be {high, common, high}. We assume that the SINR requirements for the smart farming, smart home, and industrial IoT services are -5, 0, and 5 dB, respectively. The UEs are evenly distributed in each scenario. As we mentioned above, various energy sources will be adopted to meet the stringent green requirement in 6G networks. In the simulation, we assume the batteries have no initial energy and all the energy is harvested from variable sources in each scenario. For example, the energy from the radio frequency signal and the bulk light is harvested by different devices in the smart home application. It is reasonable to assume these harvesting sources are predictable.

For the security part, we adopt the AES algorithm with three different key lengths: 32, 64, and 128 b, denoted as AES-32, AES-64, and AES-128, respectively. The message integrity is protected by the calculated MIC, of which the lengths can be 32, 64, or 128 b, represented as MIC-32, MIC-64, and MIC-128, respectively. The encryption key or MIC of 32 b is provided to service with a common requirement for confidentiality or integrity, while longer key or MIC is tried to be offered for a high requirement. As the value of E_{comp} can only be obtained by practical experiments, we follow some existing research [16] and assume that $E_{\text{comp}} = 0.15\ E_{\text{comm}}$. As the SINR requirement, payload length, distance to the hgNB, and data rate are given, we can calculate the communication energy consumption with different security suites, which can be further utilized to obtain the total energy cost. We assume the harvesting power keeps constant for 5 min and can be predicted in half-hour advance, meaning that $\Delta t = 5$ min and $\Delta T = 30$ min. The values of other key parameters are given in Table I. To illustrate the performance of our proposal more clearly, we choose the conventional strategy as a benchmark method. Generally, the conventional fixed security strategy neglects the available energy, which may increase the complexity of security configuration, further leading to extra energy consumption. On the other hand, if the IoT services have a high requirement for confidentiality or message integrity, then the traditional security strategy usually adopts the highest level of protection as the network threats are unknown. This means that the considered security suites for smart farming, smart home, and industrial IoT services are MIC-128, AES-128-MIC-32, and AES-32-MIC-128, respectively. We also study the performance when no security protection is conducted to show the tradeoff between the QoS and security. The performance comparison is adopted in terms of network throughput and total working time. Moreover, we analyze the average level of provided security protection of our proposal for each packet. Finally, we give a new definition of the mean opinion score (MOS) to measure the QoE by jointly considering the provided security and QoS. In all the simulations, we vary the packet generation rate and analyze the performance.

A. Analysis of Network QoS and Security Protection

We first conduct the simulation to analyze network QoS, including the aggregate throughput and total working time in each scenario. For a constant packet generation rate, higher aggregate throughput usually means smaller latency and lower packet loss rates. Moreover, as energy harvesting power is dynamic, if the available energy cannot support the minimum level of required security, the provision of IoT services may cease. Thus, for a given period, the total working time of devices is an important metric to measure the energy efficiency. As shown in Figs. 5 and 6, we give the network aggregate throughput and total working time of three security configuration methods in three 6G IoT scenarios. From these figures, it can be clearly found that the method to provide no security protection can achieve the highest network throughput and longest working time. However, this method is usually not considered by the service providers since the information can be easily forged by or leaked to the attackers, which may cause serious loss. Moreover, compared with the conventional strategy, our proposal can achieve better aggregate throughput and working time than the conventional strategy and the advantage increases with the growing workload. The reason is that the proposed approach can adjust the security configuration according to the service requirement and available energy. Definitely, whether the encryption or authentication process is necessary and is adopted as the baseline. Then, the UEs can decide which level of security configuration is provided to protect the more important factor according to the available energy. For example, the AES-128-MIC-32 and AES-32-MIC-32 may be chosen for smart home service in the cases of enough energy and limited energy, respectively.

Furthermore, comparing Fig. 5(a) [or Fig. 6(a)] with Fig. 5(b) and (c) [or Fig. 6(b) and (c)], we can find the gap between our proposal and conventional strategy is different. This is caused by the diverse requirements for SINR and different packet generation rates. Generally, the smart farming service usually has much less workload compared with the smart home and industrial IoT services. The strict bandwidth requirement of the industrial IoT services asks the providers to guarantee high SINR value at the hgNB side. Therefore, in our considered scenario, the energy is more frequently consumed up by the devices in the industrial IoT UEs. Therefore, the security protection of industrial IoT services shows more obvious impacts on network performance than that of smart farming services. This can also explain the growing gap among three strategies with increasing packet generation rate in Figs. 5 and 6.

In this part, we also analyze the provided security protection by our proposal as shown in Fig. 7. Since the network threats are assumed unknown, the security protection can be only conducted according to the available energy and rough service requirement for message integrity and confidentiality. As we mentioned above, the message integrity is important for all services, while no privacy needs to be protected in the smart farming scenario. The required minimum level of security suites to provide to the smart farming, smart home, and industrial IoT services are MIC-32, AES-32-MIC-32, and AES-32-MIC-32, respectively. A higher level of security protection can be offered if the energy is enough. We adopt the metric introduced in Section III-A to measure the security protection quality and the results are shown in Fig. 7. It can be clearly found that the provided security protection is

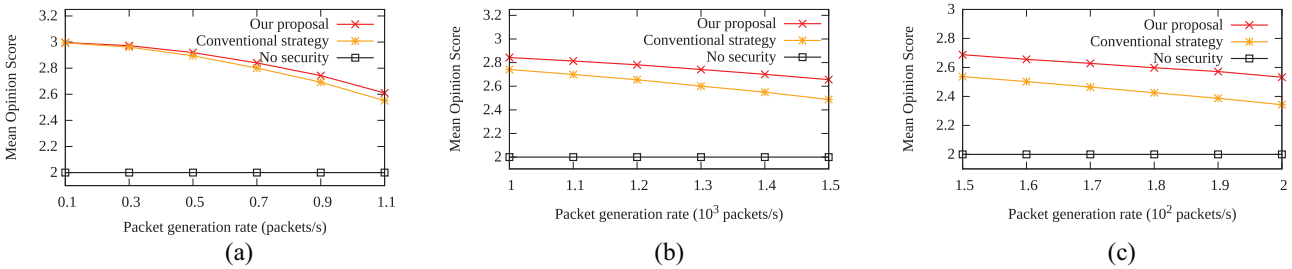

Fig. 8. Comparison of our proposal and conventional security strategies in terms of MOS in three 6G IoT scenarios. (a) MOS in the smart farming scenario. (b) MOS in the smart home scenario. (c) MOS in the industrial IoT scenario.

much higher than the minimum requirement. Moreover, the offered security protection level decreases with the growing packet generation rate for the three services. This illustrates that our proposal can adjust the security protection to extend the working time, which can improve the network QoS.

B. Analysis of Overall Network Quality of Experience

After analyzing the performance of schemes with and without security protection, it can be easily found that some tradeoff exists between the network QoS and message safety. To compare the three strategies more clearly, the concept of QoE has been proposed to measure the performance from the users' perspective. In this part, we adopt the metric MOS, which is originally utilized in the media quality evaluation, to illustrate the QoE of our considered system. We follow the definition given in (20) and consider that the network throughput, total working time, and provided security protection denoted as TH, Tt, and S, have the same importance for simplicity, which means the three weights $\omega_1 = \omega_2 = \omega_3 = 1$. For fairness, we also need to normalize the three metrics by their maximum values as follows:

$$\text{MOS} = \omega_1 \frac{\text{TH}}{\text{TH}_{\max}} + \omega_2 \frac{Tt}{Tt_{\max}} + \omega_3 \frac{S}{S_{\max}}. \tag{20}$$

As we mentioned above, the aggregate throughput and total working time can achieve the maximum values under no security protection. For security protection, we consider the highest requirement of the corresponding services, which means MIC-128, AES-128-MIC-32, and AES-32-MIC-128 for the smart farming, smart home, and industrial IoT services, respectively. Then, we can find that the value of MOS ranges from 0 to 3. Fig. 8 gives the MOS values of three strategies under varying workloads. It can be clearly found that the MOS for no security protection has a constant value of 2, while the MOS of other two strategies is above 2. Moreover, the MOS has a decreasing tendency with the growing workloads for our proposal and conventional scheme. More importantly, our proposal achieves much better MOS value than the conventional strategy, which means the improved QoE for users. Additionally, the different gap between our proposal and conventional strategy means various advantages of the proposed method in three 6G IoT scenarios, which is the same as the performance in Figs. 5 and 6.

VII. Conclusion

In this article, we focused on the link-layer security in the harvesting-based 6G IoT networks and proposed an adaptive security configuration method considering the service requirements and limited energy. In the proposal, the EKF technique was adopted to predict the harvesting power with high accuracy. Then, the UEs can utilize the prediction results to select the security suites in order to meet the requirements as well as guarantee the continuous service. Compared with the commonly utilized security configuration method, the proposal has been evaluated the performance improvement in terms of network throughput and working time. Also, the provided services can be safely protected, which finally leads to the improvement of QoE. Last but not least, the proposed security configuration method has very low complexity, which is suitable for the energy and capacity-constrained IoT devices.

References

[1] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The roadmap to 6G: AI empowered wireless networks," *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 84–90, Aug. 2019.

[2] *Key Drivers and Research for 6G Ubiquitous Wireless Intelligence*. Accessed: Nov. 2019. [Online]. Available: http://jultika.oulu.fi/files/isbn9789526223544.pdf

[3] N. Kato, B. Mao, F. Tang, Y. Kawamoto, and J. Liu, "Ten challenges in advancing machine learning technologies towards 6G," *IEEE Wireless Commun. Mag.*, early access, doi: 10.1109/MWC.001.1900476.

[4] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security and intelligence," *IEEE Wireless Commun. Mag.*, early access, Mar. 3, 2020, doi: 10.1109/MWC.001.1900516.

[5] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Balancing security and efficiency for smart metering against misbehaving collectors," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1225–1236, Mar. 2019.

[6] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.

[7] Z. Ma, Y. Liu, X. Liu, J. Ma, and K. Ren, "Lightweight privacy-preserving ensemble classification for face recognition," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5778–5790, Jun. 2019.

[8] K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin, "The security of autonomous driving: Threats, defenses, and future directions," *Proc. IEEE*, vol. 108, no. 2, pp. 357–372, Feb. 2020.

[9] L. Wang, J. Liu, M. Chen, G. Gui, and H. Sari, "Optimization-based access assignment scheme for physical-layer security in D2D communications underlaying a cellular network," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 5766–5777, Jul. 2018.

[10] D. Chen *et al.*, "An LDPC code based physical layer message authentication scheme with prefect security," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 748–761, Apr. 2018.

[11] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, Feb. 2019.

[12] Y. S. Dabbagh and W. Saad, "Authentication of wireless devices in the Internet of Things: Learning and environmental effects," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6692–6705, Aug. 2019.

[13] J. Ni, X. Lin, and X. S. Shen, "Toward edge-assisted Internet of Things: From security and efficiency perspectives," *IEEE Netw.*, vol. 33, no. 2, pp. 50–57, Mar./Apr. 2019.

[14] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in *Proc. 3rd ACM Workshop Wireless Security*, New York, NY, USA, Oct. 2004, pp. 32–42.
[15] T. D. Nguyen, J. Y. Khan, and D. T. Ngo, "A distributed energy-harvesting-aware routing algorithm for heterogeneous IoT networks," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 4, pp. 1115–1127, Dec. 2018.
[16] S. Alharby, N. Harris, A. Weddell, and J. Reeve, "The security trade-offs in resource constrained nodes for IoT application," *Int. Scholarly Sci. Res. Innov.*, vol. 12, pp. 52–59, Jan. 2018.
[17] A. Nieto and J. Lopez, "Analysis and taxonomy of security/QoS trade-off solutions for the future Internet," *Security Commun. Netw.*, vol. 7, pp. 2778–2803, Jul. 2014.
[18] Z. M. Fadlullah, C. Wei, Z. Shi, and N. Kato, "GT-QoSec: A game-theoretic joint optimization of QoS and security for differentiated services in next generation heterogeneous networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1037–1050, Feb. 2017.
[19] M. Haleem, C. Mathur, R. Chandramouli, and K. Subbalakshmi, "Opportunistic encryption: A trade-off between security and throughput in wireless networks," *IEEE Trans. Depend. Secure Comput.*, vol. 4, no. 4, pp. 313–324, Oct. 2007.
[20] Z. Shen and J. P. Thomas, "Security and QoS self-optimization in mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 7, no. 9, pp. 1138–1151, Sep. 2008.
[21] M. N. Aman, S. Taneja, B. Sikdar, K. C. Chua, and M. Alioto, "Token-based security for the Internet of Things with dynamic energy-quality tradeoff," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2843–2859, Apr. 2019.
[22] M. N. Aman, M. H. Basheer, and B. Sikdar, "Data provenance for IoT with light weight authentication and privacy preservation," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10441–10457, Dec. 2019.
[23] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018.
[24] *Authentication and Encryption Algorithms*. Accessed: Nov. 2019. [Online]. Available: https://docs.oracle.com/cd/E19683-01/806-4075/ipsec-ov-11/index.html
[25] A. Kansal, J. Hsu, S. Zahedi, and M. B. Srivastava, "Power management in energy harvesting sensor networks," *ACM Trans. Embed. Comput. Syst.*, vol. 6, no. 4, p. 32, Sep. 2007.
[26] *An Introduction to the Extended Kalman Filter*. Accessed: Nov. 2019. [Online]. Available: https://www.goddardconsulting.ca/extended-kalman-filter.html
[27] *Solar Power Data for Integration Studies*. Accessed: Nov. 2019. [Online]. Available: https://www.nrel.gov/grid/solar-power-data.html
[28] X. Mao, A. Maaref, and K. H. Teo, "Adaptive soft frequency reuse for inter-cell interference coordination in SC-FDMA based 3GPP LTE uplinks," in *Proc. IEEE Global Telecommun. Conf.*, Nov. 2008, pp. 1–6.
[29] B. Mao, Y. Kawamoto, J. Liu, and N. Kato, "Harvesting and threat aware security configuration strategy for IEEE 802.15.4 based IoT networks," *IEEE Commun. Lett.*, vol. 23, no. 11, pp. 2130–2134, Nov. 2019.
[30] T. S. Rappaport *et al.*, "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," *IEEE Access*, vol. 7, pp. 78729–78757, 2019.

Bomin Mao (Member, IEEE) received the B.Sc. degree in telecommunications engineering and the M.S. degree in electronics and telecommunications engineering from Xidian University, Xi'an, China, in 2012 and 2015, respectively, and the Ph.D. degree (Hons.) from the Graduate School of Information Sciences (GSIS), Tohoku University, Sendai, Japan, in 2019.

He is currently an Assistant Professor with GSIS, Tohoku University. His research interests are involving wireless networks, software-defined networking, and quality of service, particularly with applications of machine intelligence and deep learning.

Dr. Mao received several best paper awards from IEEE conferences, such as the IEEE Global Communications Conference in 2017 (GLOBECOM'17), GLOBECOM'18, and the IEEE International Conference on Network Infrastructure and Digital Content in 2018. He was a recipient of the prestigious 2020 NiwaYasujiro Outstanding Paper Award due to his exceptional contribution to the improvement of traffic control performance with deep learning and computation acceleration by GPU-based software-defined routers, which has been regarded by the award committees as the encouraging research for future communication networks.

Yuichi Kawamoto (Member, IEEE) received the M.S. and Ph.D. degrees in information science from Tohoku University, Sendai, Japan, in 2013 and 2016, respectively.

He is an Associate Professor with the Graduate School of Information Sciences, Tohoku University. He has published more than 60 peer-reviewed papers, including several high-quality publications in prestigious IEEE journals and conferences. His research interests cover a wide range of areas, including satellite communications, unmanned aircraft system networks, wireless and mobile networks, *ad hoc* and sensor networks, green networking, and network security.

Dr. Kawamoto received best paper awards at many international conferences, including IEEE flagship events, such as the IEEE Global Communications Conference in 2013, the IEEE Wireless Communications and Networking Conference in 2014, and the IEEE International Conference on Communications in 2018. He was also a recipient of the prestigious Dean's Award and President's Award from Tohoku University in 2016. He is a member of the Institute of Electronics, Information, and Communication Engineers.

Nei Kato (Fellow, IEEE) is a Full Professor and the Director of Research Organization of Electrical Communication, Tohoku University, Sendai, Japan. He has published more than 400 papers in prestigious peer-reviewed journals and conferences. He has been engaged in research on computer networking, wireless mobile communications, satellite communications, *ad hoc* and sensor and mesh networks, smart grid, IoT, big data, and pattern recognition.

Prof. Kato was a recipient of several awards include the Minoru Ishida Foundation Research Encouragement Prize in 2003, the Distinguished Contributions to Satellite Communications Award from the IEEE Communications Society, Satellite and Space Communications Technical Committee in 2005, the FUNAI information Science Award in 2007, the TELCOM System Technology Award from Foundation for Electrical Communications Diffusion in 2008, the IEICE Network System Research Award in 2009, the IEICE Satellite Communications Research Award in 2011, the KDDI Foundation Excellent Research Award in 2012, the IEICE Communications Society Distinguished Service Award in 2012, the IEICE Communications Society Best Paper Award in 2012, the Distinguished Contributions to Disaster-Resilient Networks R&D Award from Ministry of Internal Affairs and Communications, Japan, in 2014, the Outstanding Service and Leadership Recognition Award 2016 from IEEE Communications Society Ad Hoc & Sensor Networks Technical Committee, the Radio Achievements Award from Ministry of Internal Affairs and Communications, Japan, in 2016, and the Best Paper Awards from IEEE ICC/GLOBECOM/WCNC/VTC. He was the Vice President (Member and Global Activities) of the IEEE Communications Society from 2018 to 2019, and the Editor-in-Chief of *IEEE Network Magazine* from 2015 to 2017. He has been the Editor-in-Chief of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY since 2017, an Associate Editor-in-Chief of the IEEE INTERNET OF THINGS JOURNAL since 2013, and the Chair of IEEE Communications Society Sendai Chapter. He served as a Member-at-Large on the Board of Governors, IEEE Communications Society from 2014 to 2016, a Vice Chair of Fellow Committee of IEEE Computer Society in 2016, a member of the IEEE Computer Society Award Committee from 2015 to 2016 and the IEEE Communications Society Award Committee from 2015 to 2017. He has also served as the Chair of the Satellite and Space Communications Technical Committee from 2010 to 2012 and Ad Hoc & Sensor Networks Technical Committee from 2014 to 2015 of IEEE Communications Society. He is a Distinguished Lecturer of the IEEE Communications Society and Vehicular Technology Society. He is also a Fellow of IEICE.