Noname manuscript No.
(will be inserted by the editor)

Research on SSDF attack detection algorithm in cognitive Internet of Things

Liu Miao[1*] Xu Di[2] Zhuo-Miao Huo[2] · Zhen-Xing Sun[3,1] ·

Received: date / Accepted: date

Abstract The Internet of Things (IoT) is a new paradigm for connecting various heterogeneous networks.cognitive radio (CR) adopts cooperative spectrum sensing (CSS) to realize the secondary utilization of idle spectrum by unauthorized IoT devices,so that IoT objects can effectively use spectrum resources.However, the abnormal IoT devices in the cognitive Internet of Things will disrupt the CSS process. For this attack, we propose a spectrum sensing strategy based on the weighted combining of the Hidden Markov Model. In this method, Hidden Markov Model is used to detect the probability of malicious attack of each node and report it to the fusion center (FC). FC allocates a reasonable weight value according to the evaluation of the submitted observation results to improve the accuracy of the sensing results.Simulation results show that the detection performance of spectrum sensing data forgery(SSDF) attack in cognitive Internet of Things is better than that of K rank criterion in hard combining.

Keywords Internet of Things · Cognitive Internet of Things · Cognitive radio · Hidden Markov Model · SSDF

1 Introduction

The IoT can be defined as a network composed of interconnected objects and people who provide services. They share data to complete tasks in various applications [1].The IoT realizes the interconnection between various devices, including computers, sensors, household appliances, phones, personal devices, business devices, and any device that can connect to the network and communicate with other devices.With the development of technology and the increase in market demand, the number of IoT connected devices has achieved explosive growth. It is expected that sensors will be attached to all objects around us in the future.In order to manage a large number of devices in the IoT, context-aware methods are used to analyze the incoming data from sensors, and context-awareness plays a key role in data processing [2].However, the context-awareness method in the IoT only processes the incoming data, reduces unnecessary data entering the network, and does not really solve the network congestion problem caused by a large number of devices in the IoT.At present, our IoT devices have a high usage rate in unlicensed frequency bands, but the licensed frequency bands are not fully utilized. Therefore, the static allocation and management of spectrum resources cannot effectively meet the needs of these IoT devices and applications.The dynamic spectrum allocation method in cognitive radio can effectively overcome the shortcomings of the traditional static spectrum allocation method and alleviate the current situation of spectrum resource shortage[3, 4]. Through collaborative spectrum sharing, unlicensed IoT devices can access the licensed spectrum band without interfering with the primary user (PU),

Liu Miao
E-mail: lm_jlu@163.com
Xu Di
E-mail: xudi177819@163.com
Zhuo-Miao Huo
E-mail: yiminy_huo@163.com
Zhen-xing Sun
E-mail: 55577519@qq.com
[1] Northeast Petroleum University-Qinhuangdao, Qinhuangdao, China;
[2] Northeast Petroleum University, School of Physics and Electronic Engineering, Daqing 163318, China;
[3] School of Computer Science and Engineering Northeastern University, Shenyang, China. No.143 Taishan Road, Economic and Technological Development Zone, Qinhuangdao City 066004, Hebei Province, P. R. China;

which effectively improves the spectrum utilization of the IoT network [5].

Literature [6] proposed a new concept of cognitive Internet of Things (CIoT). CIoT is an IoT with cognitive and cooperative mechanisms. Integrating these mechanisms can improve performance and complete intelligent services. CIoT gives the current high-level intelligent "brain" of the current IoT, thinking and understanding the material and social world, so that it can analyze the current network conditions that it perceives, and make intelligent decisions to maximize network performance [7].While proposing the concept of the cognitive Internet of Things, a CIoT architecture was developed, combining the scalability of IoT with cognitive computing tools, and integrating knowledge models and self-learning information into the platform. The proposed architecture solves the problem of the lack of large-scale applications of CIoT [8].On this basis, we combine cognitive radio with the IoT based on the cognitive function of the IoT, and use CRN to establish an IoT intelligent network to solve the problem of scarcity of the IoT spectrum.The CR technology merges with the IoT and is called the cognitive radio Internet of Things (CRIoT) [9]. The combination of cognitive radio and the IoT enables IoT devices to perceive the spectrum resources that are not fully utilized by the primary user.

The first consideration in integrating CR technology into the IoT is the security issues in the IoT. The heterogeneity and complexity of the IoT make it more difficult to deal with the security of the IoT[10].There is usually a three-tier architecture in the IoT, and we implement different security principles in each layer to ensure the security of the IoT.Only by solving the security issues related to it, can the future of the IoT framework be ensured [11].In the IoT, threats such as sensitive information leakage, denial of service attacks, and unauthorized network access are all attack methods that undermine the security of the IoT [12].These common attacks have been studied. Zhen Li, Tao Jing and others used physical layer methods to solve the security problems in CIoT networks based on dynamic spectrum allocation, and proposed the use of cooperative interference to achieve secure transmission [13].Pin-Yu Chen et al. adopted a security availability and quality-aware channel allocation method for channel allocation under interference attacks in IoT-based cognitive radio networks with time-sensitive services [14].Xiaofan He et al. proposed a synchronous Q learning algorithm based on wideband spectrum sensing and greedy strategy to actively avoid channel interference [15].Khaled Mohammed Saifuddin et al. proposed a fusion-based defense mechanism for the damage caused by intentional attacks on the IoT infrastructure under the complex network structure, and introduced a game method between the opponent and the defender, using the game equilibrium the results to evaluate the effectiveness of defense mechanism [16].

Although the security of the IoT has been extensively discussed and resolved, some problems in the security of spectrum sensing still need further research.One of the main requirements of CRIoT security is to ensure that the PU is not interfered by cognitive users and can obtain data at any time.In CRIoT, due to the path shadow and fading in the spectrum sensing process, the local spectrum sensing performed by a single IoT device is usually inaccurate.Compared with the traditional single-node spectrum sensing method, CSS can reduce the influence of channel fading and shadow on the accuracy of data fusion to a certain extent. After the IoT device senses the data, it can make the judgment whether the PU occupies the current frequency band by itself and also can share information with other IoT devices to complete the judgment together or FC collects the perception data of each IoT device and uses certain data fusion rules to complete the final decision.However, the CSS mechanism provides an opportunity for malicious IoT Devices (MIDs) to launch attacks. primary user emulation(PUE) attacks and SSDF attacks are two common types of attacks. PUE attacks are mainly MIDs by acquiring PU-related characteristics and disguising them as PU, destroying the system environment [17].SSDF attack is also called Byzantine attack. This attack is MIDs tampering with local sensing data and affecting FC's final decision [18].There are two main purposes for MIDs to launch Byzantine attacks. One is to monopolize the entire channel and maximize benefits. When the PU does not occupy the authorized spectrum, the MIDs will signal the PU occupancy of the authorized spectrum to other IoT devices, so that other devices cannot intervene in the authorized spectrum. The second is to interfere with the transmission of the PU and destroy the performance of the entire network. When the PU occupies the authorized spectrum, MIDs signal that the authorized spectrum is idle to other IoT devices, causing a large number of devices to intervene in the authorized spectrum, leading to system chaos. Therefore, in either case, the damage to the normal operation of the network is serious.

On this basis, we propose a weighted combining attack detection method based on Hidden Markov Model. This method can use the channel state sensed by previous IoT devices as a data set to calculate normal IoT devices (NIDs) and probabilistic models of various attackers, and the FC evaluates the submitted observa-

tion results and assigns reasonable weight values, and finally makes a global decision.

The following are the major contributions of this paper:

• This article describes a method for discovering and detecting malicious IoT devices in the cognitive IoT.

• Proposed a weighted combining scheme based on Hidden Markov Model to discover malicious attack devices in CRIoT, so that the final decision made by FC has high accuracy.

• Use Hidden Markov Model to determine the size of the weight, and it has a higher detection rate when there are more malicious devices.

• The weighted combining scheme greatly reduces the inaccuracy of a single node's perception.

• The improvement of the detection rate of MIDs improves the overall spectrum utilization efficiency.

Rest of the paper is organized as follows: Section 2 introduces related work. Section 3 describes the system model. Section 4 describes the model of resisting SSDF attacks based on the hidden Markov model. In Section 5, experimental simulations are carried out and the results are analyzed. Section 6 concludes the paper.

2 Related works

At present, a lot of research work has been done on SSDF attack. The common ways of SSDF attack are collusive attack and independent attack. In collusive attacks, malicious users conspire together to attack and degrade CSS performance[19]. For collusive attacks, Fan Jin et al. proposed a detection strategy based on Eclat algorithm to detect collusive malicious nodes [20] . Suchmita Bhattacharjee et al. studied the design of collusive nodes in cooperative spectrum sensing and found that the performance degradation of collusive attacks is more severe than that of independent attacks[21]. Jingyu Feng et al. propose a two-level defense called FeedGuard to defend against such attacks, which can be used to improve cognitive trust assessments and reduce the perceived trust of CFF attackers[22].

In the independent attack, the malicious user will launch the attack independently without collusion with other users, this kind of attack is quite common, this paper studies the independent attack in the SSDF attack. At present, many schemes based on reputation mechanism are used to detect independent attacks. Tao Qin and his colleagues propose a trust-aware hybrid spectrum sensing scheme, which can detect the behavior of secondary users and filter their reported spectrum sensing results from the decision-making process[23]. Fang Ye and others put forward a comprehensive reputation-based security mechanism. According to SU's current and historical perception behavior, the reliability of SU in cooperative perception is measured by comprehensive reputation value, and a penalty strategy is proposed to modify reputation[24].Ming Zhou and others proposed a cooperative spectrum sensing scheme based on CRN Bayesian Reputation Model. The key idea is to treat cooperation as a service evaluation process, and SU's reputation reflects their quality of service[25]. M. Yul. Morozov et al. used combinatorial methods to mitigate the SSDF attacks, first using a reputation method to isolate the initially untrusted nodes, and then using a special q-out-of-m fusion rule to mitigate the residual attacks[26]. In addition to reputation-based schemes, a number of other algorithms have been incorporated into some countermeasures against SSDF attacks. Muhammad Sajjad Khan et al proposed a soft decision fusion scheme based on genetic algorithm to determine the optimal coefficient vector of multiple secondary user sensor reports[27]. Wangjam Niranjan Singh et al. proposed a distance-based outlier detection method to detect and isolate such malicious users on FC[28]. Zhixu Cheng et al have studied the detection of interactive M-ary quantization data against SSDF attacks in CSS networks, and proposed an interactive detection algorithm[29]. Amrapali Shivajirao Chavan et al. designed a situational awareness framework for distributed systems and mobile cognitive radio ad hoc networks to help prevent persistent SSDF attack [30]. Based on the Markov model, Xiaofan He et al have developed a new malicious user detection method using two proposed conditional frequency check statistics to improve the cooperative spectrum sensing performance [31]. Roshni Rajkumari et al proposed a method to detect SSDF attacks based on dissimilarity scores. SU calculates the dissimilarity scores of his neighbors based on the messages he receives from his h-hop neighbors[32]. Zeng Kun et al. proposed a simple robust secure cooperative SS scheme to counter SSDF attacks in the case of hard decision combination. In this approach, only binary decisions from the report OSA node are required to significantly reduce the overhead of the control channel[33]. In order to resist SSDF attacks, Yuanhua Fu, Zhiming He and others proposed a low complexity confidence weighted CSS scheme based on entropy, the scheme evaluates the weight of each sensor node according to the inconsistent characteristics of the data received by the FC in two continuous sensing slots[34]. Ye Fang and others proposed an algorithm based on evidence theory and fuzzy entropy to resist the attack of SSDF. In this algorithm, the membership function and the basic probability distribution function

are obtained for the secondary users based on the local energy detection results. According to the distance of evidence and the classical conflict coefficient, the new conflict coefficient is calculated, and the conflict weight of evidence is obtained. The fuzzy weight is calculated by fuzzy entropy, and the weight of credibility is obtained by updating credibility [35]. Our scheme also uses a weighted fusion approach, the difference is that we use Hidden Markov Model to determine the weight of nodes. Changlong Chen, Min Song et al used a decentralized scheme to detect malicious users in cooperative spectrum sensing, and used the spatial correlation of received signal intensity between closely adjacent secondary users, and based on Robustness's outlier detection technique[36].

Machine learning methods such as SVM, neural network, Naive Bayes and Ensemble classifier are also widely used to detect SSDF attacks in CRN[37]. Sarmah R et al developed a sliding window trust model based on Bayesian inference to identify and eliminate independent cooperative SSDF attackers[38]. Muhammad Sajjad Khan and others proposed a support vector machine machine learning algorithm to classify normal users and malicious users in the network [39].

However, the above work does not solve the situation where there are many malicious devices in the cognitive Internet of Things. The weight value obtained by our proposed method using the Hidden Markov Model is more accurate and can well find a large number of malicious attacks in CRIoT. Equipment, the final decision made by FC has a high accuracy rate.

3 System Model

3.1 Spectrum-aware model

CRIoT is divided into four levels, namely the application layer, the transmission layer, the perception layer, and the sensing layer. The upper three layers constitute a basic IoT architecture. Combined with CR technology, a sensing layer is added to the three-layer architecture of the IoT, and the sensing layer provides an empty spectrum bandwidth for data transmission [40]. The focus of this paper is to solve the security problem of spectrum sensing in the sensing layer. In the cooperative spectrum sensing scenario, the CRIoT is composed of PU, FC, and N IoT devices. Among all IoT devices, there are MIDs, and the number is M. In the process of spectrum sensing, the number of NIDs is N-M. It senses the usage status of a specific spectrum channel in the sensing time slot, and sends the sensing report to the FC faithfully. The FC makes a global decision on the channel status based on all received reports, and then sends the decision result to the IoT device. And MIDs will choose to forge the perceived data, affecting FC to make incorrect decisions. The signal received by one of the IoT devices can be expressed as follows

$$Y_i[k] = \begin{cases} Z_i[k] & H_0 \\ h_i S[k] + Z_i[k] & H_1 \end{cases}, i = 1, 2, ..., N \tag{1}$$

The k_{th} sensing time slot, the signal received by the i_{th} IoT device is $Y_i[k]$, the PU signal is $S[k]$, $Z_i[k]$ is the additive white Gaussian noise of the i_{th} IoT device, and $Z_i[k]$ and $S[k]$ are independent of each other.h_i is the channel gain of the communication between the i_{th} IoT device and the PU. H_0 is the current frequency band is free, and H_1 is the current frequency band is occupied [41].

The test statistic T_i of L samples of the i_{th} sensor node can be given by

$$T_i = \sum_{t=1}^{L} |y_i(t)|^2 \tag{2}$$

The local perception result $G[i]$ made by each sensor node can be expressed as

$$G[i] = \begin{cases} 0, & if\ T_i > \lambda \\ 1, & if\ T_i \leq \lambda \end{cases} \tag{3}$$

λ is the threshold of each sensor node.

After obtaining the perception results of all N IoT devices, FC will use a certain integration strategy to make a global decision. If FC finds the result of PU existence, one of the IoT devices may start to transmit data on this channel. When the FC finds that the PU does not exist, the IoT device continues to perceive whether the next channel is occupied.

3.2 SSDF attack model

In Figure1, the sensing layer of CIoT may be subject to malicious attacks from different IoT devices. These MIDs may tamper with local sensing results, affect FC's global decision making, cause conflicts in the accessed spectrum, and disrupt the normal network communication, causing system chaos. Therefore, in cooperative spectrum sensing, identifying MIDs is very important for FC to make correct decisions. Two indicators are used in the SSDF attack to measure the performance of local perception. p_f, it represents the probability of false alarm, that is, detecting the presence of the PU when the PU does not actually exist; p_d, it represents the probability of detection, and correctly detecting the existence of the PU.

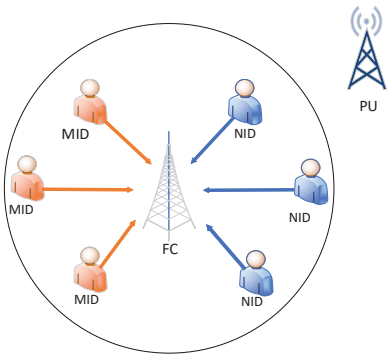


Fig. 1 System model

There are three main types of SSDF attacks launched on the cognitive Internet of Things.

• "random yes" attack: When sensing that the PU does not exist, MIDs send the local perception report as 1, and the probability of conversion is ρ_{01}. When $\rho_{01} = 1$, it is called an "always yes" attack.

• "random no" attack: When the presence of a PU is sensed, MIDs send a local perception report as 0, and the probability of conversion is ρ_{10}. When $\rho_{10} = 1$, it is called a "always no" attack.

• "random false" attack: MIDs reverse the local perception report with a conversion probability of ρ_{01} or ρ_{10} [42].

For three different attackers, because the behavior and conversion probability of each attack are different, the final detection probability and false alarm probability are also different. Not all attackers will definitely launch an attack, and MIDs are not always aware of the existence of the PU.With reference to three different attack types, the detection probability and false alarm probability of NIDs and three SSDF attackers can be obtained.

For normal IoT devices, p_d^H represents the detection probability, p_f^H represents the false alarm probability, and the two probabilities are respectively given by

$$p_d^H = p_d \tag{4}$$

$$p_f^H = p_f \tag{5}$$

For "random yes" attackers, use p_d^{RY} and p_f^{RY} to represent the probability of detection and the probability of false alarms, which are given by

$$p_d^{RY} = p_d + (1 - p_d) \cdot \rho_{01} \tag{6}$$

$$p_f^{RY} = p_f + (1 - p_f) \cdot \rho_{01} \tag{7}$$

$1 - p_d$ indicates the probability that the PU does not exist when the PU is falsely detected, but the PU actually exists. Assuming that the PU does not exist by mistake is detected, the "random yes" attacker will send a perception report as the PU exists, and the conversion probability is ρ_{01}, so the probability that the PU is finally detected correctly is $(1-p_d)\cdot\rho_{01}.p_d$ represents the probability of correctly detecting the existence of the PU, and finally the detection probability of a "random yes" attacker is (6). $1 - p_f$ represents the probability of correctly detecting that the PU does not exist. Assuming that the PU does not exist correctly is detected, the "random yes" attacker will send a perception report that the PU exists, with a conversion probability of ρ_{01}, so the final result is that the PU does not exist, but the probability of incorrectly detecting that the PU exists is $(1 - p_f) \cdot \rho_{01}$. p_f represents the probability that the PU does not exist, but the existence of the false detection is detected, and the false alarm probability of the "random yes" attacker is finally obtained as (7)[43].

Similarly, for a "random no" attacker, p_d^{RN} and p_f^{RN} are given by

$$1 - p_d^{RN} = p_d \cdot \rho_{10} + (1 - p_d) \tag{8}$$

$$1 - p_f^{RN} = p_f \cdot \rho_{10} + (1 - p_f) \tag{9}$$

Similarly, for a "random false" attacker, p_d^{RF} and p_f^{RF} are given by

$$p_d^{RF} = p_d \cdot (1 - p_{10}) + (1 - p_d) \cdot \rho_{01} \tag{10}$$

$$p_f^{RF} = p_f \cdot (1 - p_{10}) + (1 - p_f) \cdot \rho_{01} \tag{11}$$

Note that at least one of formula ρ_{01} and ρ_{10} is nonzero, otherwise, the behavior of MIDs will be exactly the same as NIDs in a statistical sense.

In the cognitive network of the sensor layer, if these NIDs only exist in individual malicious devices, they can be easily identified through FC's decision fusion standard. However, if the number of MIDs is too large, the fusion strategy adopted by FC will fail, so other methods must be combined to improve the detection accuracy of the Fusion Center.

4 Model of resisting SSDF attack based on Hidden Markov Model

4.1 Attack detection based on Hidden Markov Model

Hidden Markov Model is a time-related probability model. Its process is to randomly generate an unobservable sequence of states from the Hidden Markov Model, and then randomly generate observations from each state to form an observation sequence [44].

In local spectrum sensing, $Q = \{q_1, q_2\}$ is the hidden state set of the channel, $q_1 = 1$ and $q_2 = 0$ represent channel occupancy and idle respectively;$V = \{v_1, v_2\}$ is

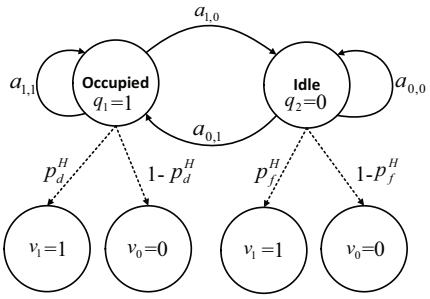


Fig. 2 NIDs HMM model

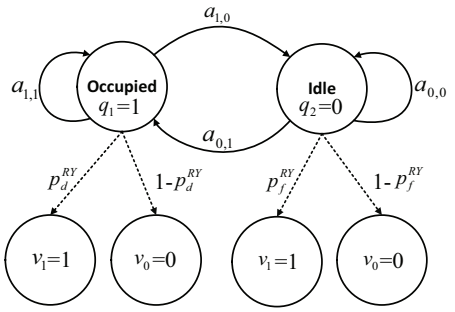


Fig. 3 "random yes" attacker HMM Model

the channel state set of the spectrum sensed,$v_1 = 1$ and $v_2 = 0$ respectively indicate that the results of spectrum sensing are occupied and idle.q_t represents the channel state of the channel at the time slot t, and o_t represents the corresponding observation value. $A = \{a_{ij}\}$ is the channel state transition probability matrix, where

$$a_{ij} = P(i_{t+1} = q_j | i_t = q_i), 1 \leq i, j \leq N \tag{12}$$

$B = \{b_j(k)\}$ means the hidden channel state is q_j and the channel state detected by the cognitive user is a conditional probability matrix of v_k, where

$$b_j(k) = P(o_t = v_k | i_t = q_j), 1 \leq k \leq M, 1 \leq j \leq N \tag{13}$$

The initial channel state probability matrix $\pi = \{\pi_0, \pi_1\}$, where $\pi_i = P(i_1 = q_i)$, $1 \leq i, j \leq N$, represents the probability of being in state q_i at the initial moment.

Hidden Markov Model is determined by π, A and B, so HMM can be expressed as $\lambda = (\pi, A, B)$. The HMM models of honest users and three SSDF attackers are λ_H,λ_{RY},λ_{RN} and λ_{RF}, respectively.The abnormal perception behavior of users will cause the difference between B in each model, but the parameters π and A of these four HMMs are the same because all users are perceiving the same frequency spectrum. Therefore, the four HMM models can be expressed as $\lambda_H = \{\pi, A, B_H\}$,$\lambda_{RY} = \{\pi, A, B_{RY}\}$,$\lambda_{RN} = \{\pi, A, B_{RN}\}$ and $\lambda_{RF} = \{\pi, A, B_{RF}\}$. Figure 2 and Figure 3 show the HMM model of NIDs and "random yes" attackers, respectively.

The MIDs in the CRIoT will tamper with the spectrum sensing data, so the data obtained by the final FC may have been tampered with by the MIDs. These data are quite different from the data sensed by NIDs.A priori data can be obtained through spectrum sensing, and the result of spectrum sensing is used as the observation sequence $O = (o_1, o_2, ..., o_T)$ of the HMM. Based on these known observation sequences, FC uses the forward algorithm to calculate the different probabilities of each IoT device $P(O|\lambda_H)$, $p(O|\lambda_{RY})$, $P(O|\lambda_{RN})$ and $P(O|\lambda_H)$.If FC calculates that the device's $P(O|\lambda_H)$ is higher than other probabilities, the device is more likely to be NID. Conversely, if the probability of $p(O|\lambda_{RY})$ is the highest, then the device is likely to be an "random yes" attacker. The forward algorithm is expressed as follows.

Define the forward variable as

$$\alpha_t(i) = P(o_1, o_2, ..., o_t, i_t = q_i | \lambda) \tag{14}$$

Among them,$\alpha_t(i)$ is the probability that the model observation sequence is $o_1, o_2, ..., o_t$ and the state of time slot t is q_i under the premise that the model parameter λ is determined.

The recursive process of the forward algorithm is as follows.

• Initialize the parameters.

$$\alpha_1(i) = \pi_i b_i(o_1), 1 \leq i \leq N \tag{15}$$

• Recursion.

$$\alpha_{t+1}(j) = \left[\sum_{i=1}^{N} \alpha_t(i) a_{ij}\right] b_j(o_{t+1}), \quad 1 \leq t \leq T-1, 1 \leq j \leq N \tag{16}$$

• Termination.

$$P(O|\lambda) = \sum_{i=1}^{N} \alpha_T(i) \tag{17}$$

4.2 Detection algorithm based on Weighted Combining in FC

In FC, we can get the perception report of each IoT device and use the above Hidden Markov Mmodel to calculate that a certain IoT device may be NID or MID.The FC can make the following judgments. The device reports to the FC that the PU exists. If it detects that the device may be NID, it may correctly detect the presence of the PU. The probability is p_d^H. It may also be detected incorrectly. The actual PU does not exist. The probability is p_f^H. If it is detected that the device

may be a "random yes" attacker, it may correctly detect the presence of the PU, with a probability of p_d^{RY}, or may incorrectly detect the presence of the PU, but the actual PU does not exist, with the probability p_f^{RY}. Conversely, if the device reports to the FC that the PU does not exist, if it detects that the device may be NID, it may correctly detect that the PU does not exist, the probability is $1-p_f^H$, or it may incorrectly detect that the PU does not exist, and the PU actually exists, the probability is $1-p_f^H$. If it is detected that the device may be a "random yes" attacker, it may correctly detect that the PU does not exist, with a probability of $1-p_d^{RY}$, or it may incorrectly detect that the PU does not exist, and the PU actually exists, with a probability of $1-p_f^{RY}$.

We can use the different detection probabilities to determine the different weights of each device to distinguish MIDs and NIDs in the Internet of Things.

$$w_t^H = \frac{p_d^H}{2N} - \frac{p_f^H}{2N} \tag{18}$$

$$w_f^H = \frac{1-p_d^H}{2N} - \frac{1-p_f^H}{2N} \tag{19}$$

w_t^H and w_f^H respectively represent the weights of the NID perceiving the existence of the PU and perceiving the absence of the PU.

If you calculate that an Iot device might be a"random yes"attacker, you can determine the weights in the same way.

$$w_t^N = \frac{p_d^{RY}}{2N} - \frac{p_f^{RY}}{2N} \tag{20}$$

$$w_f^N = \frac{1-p_d^{RY}}{2N} - \frac{1-p_f^{RY}}{2N} \tag{21}$$

w_t^N and w_f^N respectively represent the weights of perceiving the existence of the PU and perceiving the non-existence of the PU in the case of "random yes" the attacker.

The "random no" attacker and the "random false" attacker are the same as the above situation, and will not be explained again. We will get different weights for each IoT device, and add these weights, and the result is positive means that the PU exists, and negative means that the PU does not exist. The final decision $F(\omega)$ can be expressed as follows

$$F(\omega) = \begin{cases} \sum_{i=1}^{N} \omega_i > 0, & H_1 \\ \sum_{i=1}^{N} \omega_i < 0, & H_0 \end{cases} \tag{22}$$

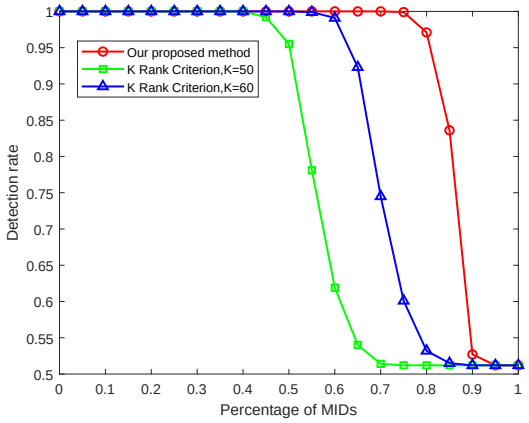


Fig. 4 The relationship between detection rate and MIDs under "random yes" attack

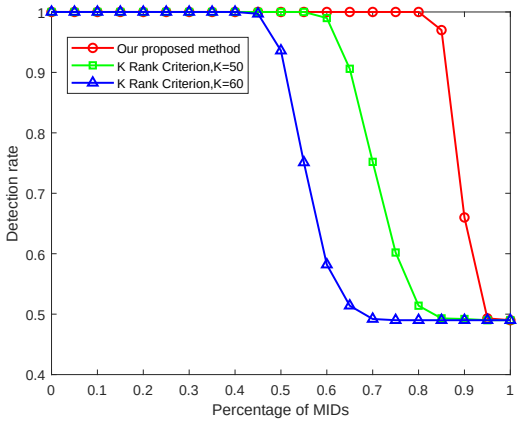


Fig. 5 The relationship between detection rate and MIDs under "random no" attack

5 Experimental simulation and analysis

In this section, we performed simulations to illustrate the effectiveness of the method. In this simulation experiment, we mainly use the MATLAB platform to set the total number of IoT devices N=100, the number of time slots T=1000, and set different p_d to simulate different noise interference in the channel, and all cooperative sensor nodes transmit their sensing data to FC through ideal control channel. Initialize the four modelsλ_H, λ_{RY},λ_{RN}, and λ_{RF}, initialize and A, set $p_d = 0.9$, $p_f = 0.1$ to get B_H, B_{RY}, B_{RN}, and B_{RF}. The detection rate can be expressed as the rate at which the channel state is correctly detected in a certain time slot.

Figure 4 and Figure 5 show the changes in the detection rate as the number of MIDs continues to increase in the case of "random yes" and "random no" attacks. We compare our proposed method with the K rank criterion. The K rank criterion is the fusion strategy

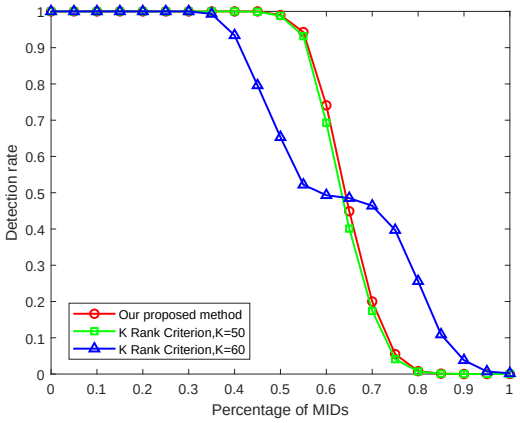


Fig. 6 The relationship between detection rate and MIDs under "random false" attacks

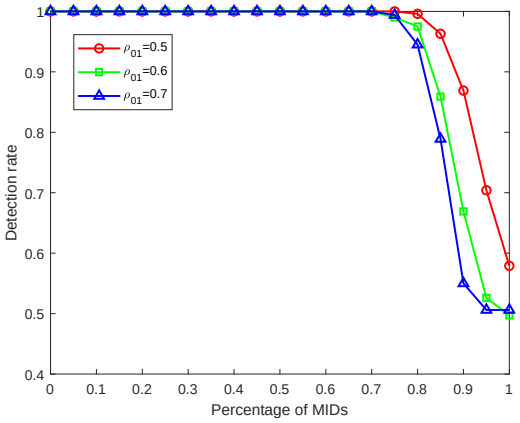


Fig. 7 The relationship between the detection rate of different attack frequencies and MIDs under "random yes" attacks

adopted by most papers at present, that is, the system can work normally when no less than K of the N devices work normally. It can be seen from the detection results that our detection method can distinguish between attackers and normal devices in IoT devices, and the weighted combining algorithm we proposed is better than the K rank criterion. The detection method is effective when MIDs account for less than 80% of the total, but as the number of MIDs continues to increase, the detection rate drops rapidly, because when the number of MIDs is too large, the result of spectrum sensing is unreliable.

Figure 6 shows that the detection rate varies with the number of MIDs under the "random false" attack. It can be seen that the detection method is effective when MIDs account for less than 50% of the total. However, as the number of MIDs continues to increase, the detection rate drops rapidly. The experimental results show that the opposite sensor data will cause greater harm to the fusion process. This is because when there are more than half of the attackers in the IoT device, the "random false" attacker will get the data flipped, which affects the judgment of FC.

Change the attack frequency of the attacker. Under the "random yes", "random no" and "random false" attacks, we set three different attack frequencies for comparison.

Figure 7, Figure 8 and Figure 9 respectively show the changes in the detection rate of different attack frequencies under the "random yes", "random no" and "random false" attacks as the number of MIDs continues to increase. It can be seen that as the frequency of attacks increases, the detection performance decreases. The increase in the frequency of attacks means that the MIDs will have a greater possibility of launching an at-

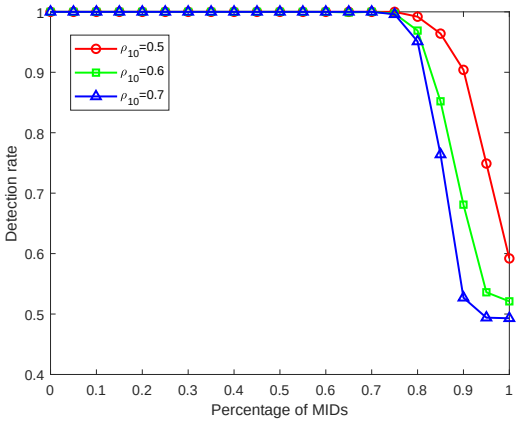


Fig. 8 The relationship between the detection rate of different attack frequencies and MIDs under the "random no" attack

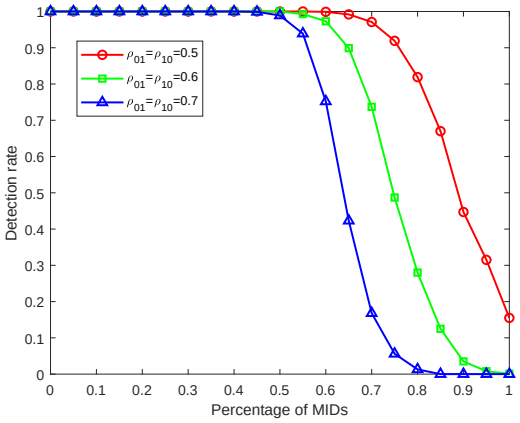


Fig. 9 The relationship between the detection rate of different attack frequencies and MIDs under "random false" attacks

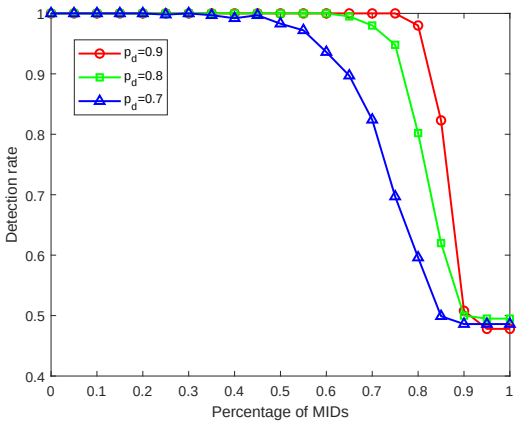


Fig. 10 The relationship between different p_d detection rates and MIDs under "random yes" attacks

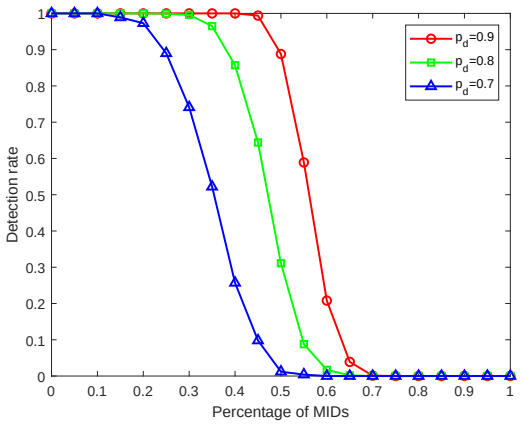


Fig. 12 The relationship between different p_d detection rates and MIDs under "random false" attacks

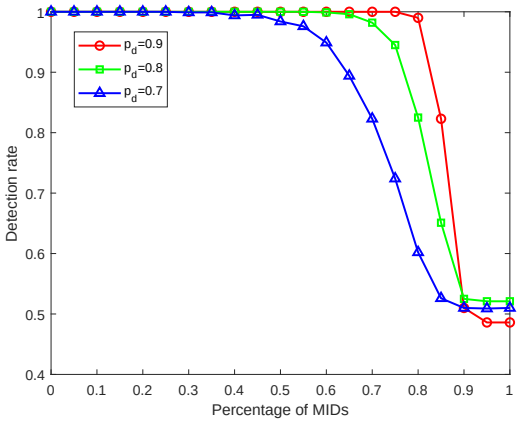


Fig. 11 The relationship between different p_d detection rates and MIDs under "random no" attacks

tack, so the probability of an attack will increase, which will affect the detection rate.

Figure 10, Figure 11 and Figure 12 respectively show the changes in the detection rate of different p_d as the number of MIDs continues to increase under the "random yes", "random no" and "random false" attacks. It can be seen that as p_d increases, the detection rate is also increasing. p_d is the probability of correctly detecting the existence of the PU. Because of the interference of the noise in the channel, we may not be completely accurate in the detection of the existence of the PU, because different signal-to-noise ratios in the channel will lead to different p_d, which further leads to a detection rate low when there is no noise.

6 conclusion

This paper proposes a cooperative spectrum sensing strategy based on the weighted combining of Hidden Markov Model to defend SSDF attacks from malicious devices in the IoT. This method uses the Hidden Markov Model to detect the probability of malicious attacks on each device node and reports it to FC. FC assigns a reasonable weight value based on the evaluation of the submitted observation results, so as to avoid FC from making wrong decisions and correctly judging the channel status.

This paper studies the performance parameters of the detection rate under three different attacks with the increase of malicious devices, and compare our algorithm with the traditional K rank criterion. Our algorithm can use Hidden Markov Model to determine the weight, so that the final decision made by FC is closer to the accurate value. In the future, we will further optimize our detection model to improve the detection rate in the case of more malicious devices. In addition, the combination of cognitive radio and IoT will be further studied to solve more security problems in CIoT.

Declarations

Funding This work was supported by the Excellent Middle-aged and Young Research and Innovation Team of Northeast Petroleum University Research on Performance Optimization of Oil and Gas Pipeline Internet of Things, China, No. KYCXTDQ201901. And, the work also is supported by National Natural Science Foundation of China, No. 61601111. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

Data Availability Data can be shared and is available on request. Data can be requested by sending an email to the main author.

Conflict of interest The authors declare that they have no conflict of interest.

Authors' contributions Liu Miao conceived and designed the study. Xu Di designed the study and performed experiments. Liu Miao and Xu Di wrote the paper. Zhuo-Miao Huo and Zhen-xing Sun edited the manuscript.

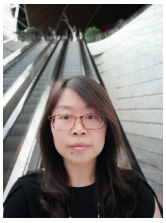
References

1. Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.
2. Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. Context aware computing for the internet of things: A survey. *IEEE communications surveys & tutorials*, 16(1):414–454, 2013.
3. Miao Liu, Zhenxing Sun, Yan-chang Liu, and Cun Zhao. The optimization algorithm for cr system based on optimal wavelet filter. *Wireless Communications and Mobile Computing*, 2019, 2019.
4. Liu Miao, Zhenxing Sun, and Zhang Jie. The parallel algorithm based on genetic algorithm for improving the performance of cognitive radio. *Wireless Communications and Mobile Computing*, 2018, 2018.
5. Weidang Lu, Su Hu, Xin Liu, Chenxin He, and Yi Gong. Incentive mechanism based cooperative spectrum sharing for ofdm cognitive iot network. *IEEE Transactions on Network Science and Engineering*, 7(2):662–672, 2019.
6. Mingchuan Zhang, Haixia Zhao, Ruijuan Zheng, Qingtao Wu, and Wangyang Wei. Cognitive internet of things: concepts and application example. *International Journal of Computer Science Issues (IJCSI)*, 9(6):151, 2012.
7. Qihui Wu, Guoru Ding, Yuhua Xu, Shuo Feng, Zhiyong Du, Jinlong Wang, and Keping Long. Cognitive internet of things: a new paradigm beyond connection. *IEEE Internet of Things journal*, 1(2):129–143, 2014.
8. Joern Ploennigs, Amadou Ba, and Michael Barry. Materializing the promises of cognitive iot: How cognitive buildings are shaping the way. *IEEE Internet of Things Journal*, 5(4):2367–2374, 2017.
9. Dina Tarek, Abderrahim Benslimane, M Darwish, and Amira M Kotb. Survey on spectrum sharing/allocation for cognitive radio networks internet of things. *Egyptian Informatics Journal*, 2020.
10. Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. Iot security: ongoing challenges and research opportunities. In *2014 IEEE 7th international conference on service-oriented computing and applications*, pages 230–234. IEEE, 2014.
11. Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan. Internet of things (iot) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 336–341. IEEE, 2015.
12. Francesca Meneghello, Matteo Calore, Daniel Zucchetto, Michele Polese, and Andrea Zanella. Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices. *IEEE Internet of Things Journal*, 6(5):8182–8201, 2019.
13. Zhen Li, Tao Jing, Liran Ma, Yan Huo, and Jin Qian. Worst-case cooperative jamming for secure communications in ciot networks. *Sensors*, 16(3):339, 2016.
14. Haythem Bany Salameh, Sufyan Almajali, Moussa Ayyash, and Hany Elgala. Security-aware channel assignment in iot-based cognitive radio networks for time-critical applications. In *2017 Fourth International Conference on Software Defined Systems (SDS)*, pages 43–47. IEEE, 2017.
15. Feten Slimeni, Zied Chtourou, Bart Scheers, Vincent Le Nir, and Rabah Attia. Cooperative q-learning based channel selection for cognitive radio networks. *Wireless Networks*, 25(7):4161–4171, 2019.
16. Pin-Yu Chen, Shin-Ming Cheng, and Kwang-Cheng Chen. Information fusion to defend intentional attack in internet of things. *IEEE Internet of Things journal*, 1(4):337–348, 2014.
17. Bilal Naqvi, Imran Rashid, Faisal Riaz, and Baber Aslam. Primary user emulation attack and their mitigation strategies: A survey. In *2013 2nd National Conference on Information Assurance (NCIA)*, pages 95–100. IEEE, 2013.
18. Jingyu Feng, Yuqing Zhang, Guangyue Lu, and Liang Zhang. Defend against collusive ssdf attack using trust in cooperative spectrum sensing environment. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pages 1656–1661. IEEE, 2013.
19. Fan Jin, Vijay Varadharajan, and Udaya Tupakula. An eclat algorithm based energy detection for cognitive radio networks. In *2017 IEEE Trustcom/BigDataSE/ICESS*, pages 1096–1102. IEEE, 2017.
20. Suchismita Bhattacharjee, Roshni Rajkumari, and Ningrinla Marchang. Effect of colluding attack in

collaborative spectrum sensing. In *2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN)*, pages 223–227. IEEE, 2015.

21. Jingyu Feng, Shaoping Li, Shaoqing Lv, Honggang Wang, and Anmin Fu. Securing cooperative spectrum sensing against collusive false feedback attack in cognitive radio networks. *IEEE Transactions on Vehicular Technology*, 67(9):8276–8287, 2018.
22. Tao Qin, Han Yu, Cyril Leung, Zhiqi Shen, and Chunyan Miao. Towards a trust aware cognitive radio architecture. *ACM SIGMOBILE Mobile Computing and Communications Review*, 13(2):86–95, 2009.
23. Fang Ye, Xun Zhang, and Yibing Li. Comprehensive reputation-based security mechanism against dynamic ssdf attack in cognitive radio networks. *Symmetry*, 8(12):147, 2016.
24. Ming Zhou, Jiafeng Shen, Huifang Chen, and Lei Xie. A cooperative spectrum sensing scheme based on the bayesian reputation model in cognitive radio networks. In *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 614–619. IEEE, 2013.
25. M Yu Morozov, O Yu Perfilov, NV Malyavina, RV Teryokhin, and IV Chernova. Combined approach to ssdf-attacks mitigation in cognitive radio networks. In *2020 Systems of Signals Generating and Processing in the Field of on Board Communications*, pages 1–4. IEEE, 2020.
26. Muhammad Sajjad Khan, Noor Gul, Junsu Kim, Ijaz Mansoor Qureshi, and Su Min Kim. A genetic algorithm-based soft decision fusion scheme in cognitive iot networks with malicious users. *Wireless Communications and Mobile Computing*, 2020, 2020.
27. Wangjam Niranjan Singh, Ningrinla Marchang, and Amar Taggu. Mitigating ssdf attack using distance-based outlier approach in cognitive radio networks. *International Journal of Ad Hoc and Ubiquitous Computing*, 32(2):119–132, 2019.
28. Zhixu Cheng, Jing Zhang, Tiecheng Song, Jing Hu, and Xu Bao. Interaction-based detection strategy against probabilistic ssdf attack in css network. In *2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pages 1–5. IEEE, 2020.
29. Zhixu Cheng, Jing Zhang, Tiecheng Song, Jing Hu, and Xu Bao. Interaction-based detection strategy against probabilistic ssdf attack in css network. In *2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pages 1–5. IEEE, 2020.
30. Amrapali Shivajirao Chavan and Aparna Junnarkar. Dynamic spectrum sensing method for mobile cognitive radio ad hoc networks. In *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)*, pages 92–97. IEEE, 2020.
31. Xiaofan He, Huaiyu Dai, and Peng Ning. A byzantine attack defender in cognitive radio networks: The conditional frequency check. *IEEE Transactions on Wireless Communications*, 12(5):2512–2523, 2013.
32. Roshni Rajkumari and Ningrinla Marchang. Mitigating spectrum sensing data falsification attack in ad hoc cognitive radio networks. *International Journal of Communication Systems*, 32(2):e3852, 2019.
33. Kun Zeng, QiHang Peng, and YouXi Tang. Mitigating spectrum sensing data falsification attacks in hard-decision combining cooperative spectrum sensing. *Science China Information Sciences*, 57(4):1–9, 2014.
34. Yuanhua Fu and Zhiming He. Entropy-based weighted decision combining for collaborative spectrum sensing over byzantine attack. *IEEE Wireless Communications Letters*, 8(6):1528–1532, 2019.
35. Fang Ye, Ping Bai, and Yuan Tian. An algorithm based on evidence theory and fuzzy entropy to defend against ssdf. *Journal of Systems Engineering and Electronics*, 31(2):243–251, 2020.
36. Changlong Chen, Min Song, Chunsheng Xin, and Mansoor Alam. A robust malicious user detection scheme in cooperative spectrum sensing. In *2012 IEEE Global Communications Conference (GLOBECOM)*, pages 4856–4861. IEEE, 2012.
37. Rupam Sarmah, Amar Taggu, and Ningrinla Marchang. Detecting byzantine attack in cognitive radio networks using machine learning. *Wireless Networks*, 26(8):5939–5950, 2020.
38. Yuanhua Fu and Zhiming He. Bayesian-inference-based sliding window trust model against probabilistic ssdf attack in cognitive radio networks. *IEEE Systems Journal*, 14(2):1764–1775, 2019.
39. Muhammad Sajjad Khan, Liaqat Khan, Noor Gul, Muhammad Amir, Junsu Kim, and Su Min Kim. Support vector machine-based classification of malicious users in cognitive radio networks. *Wireless Communications and Mobile Computing*, 2020, 2020.
40. Jun Wu, Cong Wang, Yue Yu, Tiecheng Song, and Jing Hu. Sequential fusion to defend against sensing data falsification attack for cognitive internet of things. *ETRI Journal*, 42(6):976–986, 2020.

41. Jun Wu, Pei Li, Yang Chen, Jifei Tang, Chao Wei, Lanhua Xia, and Tiecheng Song. Analysis of byzantine attack strategy for cooperative spectrum sensing. *IEEE Communications Letters*, 24(8):1631–1635, 2020.
42. S Vimal, L Kalaivani, Madasamy Kaliappan, Annamalai Suresh, Xiao-Zhi Gao, and R Varatharajan. Development of secured data transmission using machine learning-based discrete-time partially observed markov model and energy optimization in cognitive radio networks. *Neural Computing and Applications*, 32(1):151–161, 2020.
43. Xiaofan He, Huaiyu Dai, and Peng Ning. Hmm-based malicious user detection for robust collaborative spectrum sensing. *IEEE Journal on Selected Areas in Communications*, 31(11):2196–2208, 2013.
44. Lawrence R Rabiner. A tutorial on hidden markov models and selected applications in speech recognition. *Proceedings of the IEEE*, 77(2):257–286, 1989.



Liu Miaoreceived B.S degree at School of Computer Science and Technology, Jilin University, China in 2002. In 2008, she obtained the M.S degree at School of Computer Science and Technology, Jilin University. She got a Ph.D. degree at College of Communication Engineering, Jilin University in 2011. In 2015, she finished postdoctoral work at China Petroleum and Natural Gas Pipeline Bureau, China

Now, she is a professor of Northeast Petroleum University, China. She has dozens of refereed international publications, including book, journals, and conferences in her research areas. In addition, she got a number of invention patents and presided over the research projects supported by the National Natural Science Foundation of China (NSFC), Postdoctoral Scientific Research Developmental Fund of China and so on.

She is the chief expert of Excellent Young and Middle-aged Research and Innovation Team of NNortheast Petroleum University (Performance Optimization Research Team of Oil and Gas Pipeline Internet of Things). Her current research interests include the performance optimization of Internet of Things, Cognitive Radio network and low energy consumption communication protocol.

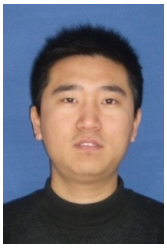
Xu Direceived the B.S. degree from the Taiyuan University, China, in 2020. From 2016 to 2020, she was an undergraduate with College of Computer Science and Technology.

Since 2020, she is currently pursuing M.S degree in Northeast Petroleum University, Heilongjiang, China. Her current research interests include Internet of Things, energy harvesting, and Cognitive Radio networks.

Zhuo-miao Huoreceived the B.S. degree from the Jinggangshan University, China, in 2019. From 2015 to 2019, was an undergraduate with College of Electronic Information Science and Technology.

Since 2020, she is currently pursuing M.S degree in Northeast Petroleum University, Heilongjiang, China. Her current research interests include Internet of Things, energy harvesting, and Cognitive Radio networks.

Since 2020, she is currently pursuing M.S degree in Northeast Petroleum University, Heilongjiang, China. Her current research interests include Internet of Things, energy harvesting, and Cognitive Radio networks.



Zhen-xing Sunreceived B.S. degree and M.S. degree from Northeast Petroleum University, Daqing, China, in 2003 and in 2011, respectively. He has been a doctoral student in Northeastern University, Shenyang, China, since 2015. Currently, he is an assistant professor at Department of Electronics and Information Engineering, Northeast Petroleum University at Qinhuangdao since 2017. His research interests include Cognitive Radio network, Internet of Things IoT, interference management technique in Ultra-Dense Networks.