Received: 21 August 2019 | Revised: 18 October 2019 | Accepted: 14 November 2019

DOI: 10.4218/etrij.2019-0388

ORIGINAL ARTICLE

ETRI Journal WILEY

Sequential fusion to defend against sensing data falsification attack for cognitive Internet of Things

Jun Wu[1] | **Cong Wang**[2] | **Yue Yu**[2] | **Tiecheng Song**[2] | **Jing Hu**[2]

[1]School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China

[2]School of Information Science and Engineering, Southeast University, Nanjing, China

Correspondence
Jun Wu, School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China.
Email: wojames2011@163.com

Funding information
This work was supported by the National Natural Science Foundation of China (No. 61771126, 61801155 and 61901152) and the Key Research & Development Plan of Jiangsu Province (No. BE2018108).

Internet of Things (IoT) is considered the future network to support wireless communications. To realize an IoT network, sufficient spectrum should be allocated for the rapidly increasing IoT devices. Through cognitive radio, unlicensed IoT devices exploit cooperative spectrum sensing (CSS) to opportunistically access a licensed spectrum without causing harmful interference to licensed primary users (PUs), thereby effectively improving the spectrum utilization. However, an open access cognitive IoT allows abnormal IoT devices to undermine the CSS process. Herein, we first establish a hard-combining attack model according to the malicious behavior of falsifying sensing data. Subsequently, we propose a weighted sequential hypothesis test (WSHT) to increase the PU detection accuracy and decrease the sampling number, which comprises the data transmission status-trust evaluation mechanism, sensing data availability, and sequential hypothesis test. Finally, simulation results show that when various attacks are encountered, the requirements of the WSHT are less than those of the conventional WSHT for a better detection performance.

KEYWORDS
cognitive internet of things, cognitive radio, Internet of Things, sensing data falsification attack, weighted sequential hypothesis test

1 | INTRODUCTION

The Internet of Things (IoT), first proposed by Ashton [1], describes the future scenario where daily physical objects will be connected to the Internet and be able to identify themselves to other devices. The IoT is a new revolution of the Internet and things or objects, such as radio frequency identification tags, sensors, actuators, and mobile phones, which through unique addressing schemes can interact with each other and cooperate with their neighbors to reach typical goals [2]. To realize the IoT network paradigm, a large number of IoT devices must be deployed. However, with the increasing number of IoT devices, the amount of spectra for these devices is insufficient. Moreover, owing to the interference owing to spectrum overuse by IoT devices, the transmission performance will be degenerated significantly. Therefore, it is highly import to improve the spectrum utilization in an IoT network [3].

1.1 | Related studies

M. Zhang and others presented the concept of cognitive IoT (CIoT) by integrating intelligent thoughts into the IoT to address the lack of intelligence, modeled the CIoT network topology, and designed cognition process–related technologies

[4]. Inspired by the human cognition process, Wu and others [5] presented an operational framework for CIoT, which characterized fundamental cognitive tasks and empowered the current IoT with a "brain" for high-level intelligence. Ploennigs and others proposed a CIoT architecture [6] that combined the strength in scalability provided by a recently developed IoT architecture with self-learning and self-adaptation capabilities obtained from cognitive systems.

Furthermore, [4–6] considered cognitive capability to gradually enrich the definition of the IoT and developed a brain-empowered CIoT paradigm involving key enabling techniques. However, the spectrum shortage problem has yet to be solved in the previous IoT network. Hence, cognitive radio (CR) is envisaged as a promising solution to improve spectrum utilization by sharing a licensed spectrum. CR has been defined by Mitola and later by Haykin as an intelligent wireless communication system that is aware of its surrounding environment and uses the methodology of understanding by building to learn from the environment and adapts its internal states based on new statistical variations [7]. Integrating CR technology with the IoT network allows IoT devices to sense spectrum resources that are underutilized by primary users (PUs), which is considered as complementary to existing efforts [3].

The main goal of [8] and [9] is to discuss how CR technology can be useful for the IoT paradigm. Kim proposed using CR techniques for IoT-based systems to manage the shortage of spectrum for IoT devices [10]. Zaheer and others provided a survey of the existing decision theoretic models and their usage for CIoT [11]; furthermore, an architectural CIoT framework was proposed to discuss the open issues and solution for potential challenges emerging in the CIoT research. Considering that spectrum decision by unlicensed users of CR is important in CR-based IoT in 5G and beyond networks, Akhtar described a scientific supported spectrum decision support framework for CR networks [12], in which the goal is the same as that reported in [8] and [9].

Although a comprehensive study on recent advances in CR technology for IoT has been provided [8–12], many questions are yet to be explored, such as the attack and defense involved in CIoT. In [13], Chen and others investigated the vulnerability of the IoT infrastructure under intentional attacks by relating network resilience to percolation-based connectivity. They proposed a fusion-based defense mechanism to mitigate the damage caused by such attacks and applied the results of game equilibrium (the attack and defense strategy as a zero-sum game) to evaluate the effectiveness of the proposed mechanism. Unfortunately, only a general theoretic framework for network robustness analysis and enhancement is provided and defense against specific attacks failed [13]. In [14], Zhang and others surveyed the Sybil attack and defense schemes in the IoT. They suggested several research issues regarding Sybil defense and mentioned that further research and development related to IoT is still challenging. In [15], Li and others addressed the physical layer security issue in CIoT networks by employing cooperative jamming. They proposed a novel cooperative jamming scheme, in which a secondary user is arbitrarily assigned as the helper to confound the eavesdropper by sending jamming signals. However, if the helper is a malicious node, the system security will be severely threatened. Therefore, the untrusted helper node should be considered thoroughly. In [16], Salameh and others presented a probabilistic-based channel assignment algorithm for IoT-based cognitive radio networks (CRNs) with time-sensitive traffic under jamming attacks. In [17], Lin and others proposed a protocol and a method of spectrum management that can guard against typical types of security threats despite the limitations of local processing. With a hierarchical CIoT architecture, they incorporated the strengths of CR and the physical properties of a device to improve the performance of a CRSN and resolved the primary user emulation attack (PUEA) problem. However, using a large number of IoT devices worsens the spectrum scarcity problem significantly. The usable spectrum resources are almost entirely occupied; therefore, the increasing demands of radio access from IoT devices cannot be satisfied. Both [16] and [17] primarily focused on the resource allocation algorithm to defend against Sybil attacks, jamming or PUEAs for CIoT, and subsequently ignored the spectrum sensing problem; in fact, spectrum sensing is critical to solve the spectrum scarcity problem.

Additionally, extensive research has been performed to provide a structured and comprehensive overview on the security of IoT from different aspects, such as, [18–31] and the references therein.

1.2 | Motivation and contributions

Although the security of IoT has been extensively discussed and addressed, some of which pertain to the current state of research and future directions of IoT security requirements, strong scalability concerns still exist, especially in spectrum sensing security. Most of the previously conducted research failed to consider the peculiarities of such services, such as spectrum sensing; therefore, the high bandwidth demand to serve massive numbers of IoT devices may result in spectrum scarcity for IoT applications. Such limitations fuel the motivation for providing a broader and more complete view of CIoT security challenges in spectrum sensing.

To the best of our knowledge, a sequential probability ratio test design for spectrum sensing in CIoT networks had not been studied. Local spectrum sensing by a single IoT device is often inaccurate as the channel often experiences fading and shadowing effects; therefore, cooperative

spectrum sensing (CSS) has been proposed to overcome this problem. Although CSS performed by several IoT devices can provide a more reliable decision regarding the PUs, abnormal IoT devices (AIDs) may appear, which is disadvantageous. During spectrum sensing, AIDs alter the cooperative decision by transmitting false signals, thereby resulting in the incorrect prediction of PU presence. Such attacks are known as sensing data falsification attacks (SDFAs). During SDFAs, the traditional encryption method (such as symmetric and asymmetric ciphers) may not be suitable for CIoT networks, as these networks are composed of low-profile devices.

Hence, we design a weighted sequential hypothesis test (WSHT) for CIoT to secure CSS and decrease the number of samples required at the fusion center (FC). By analyzing the malicious behavior occurring during CSS, we formulate a hard-combining SDFA model. According to the periodic spectrum sensing frame structure, we formulate a data transmission status-based trust evaluation mechanism instead of the global decision-based trust evaluation mechanism to evaluate the sensing data availability. Furthermore, we integrate the sensing data availability into the weight of the sequential hypothesis test, and propose a WSHT to defend against SDFAs in CIoT.

The remainder of the paper is structured as follows. Section 2 provides the system model including the spectrum sensing and SDFA models. Section 3 formulates the WSHT, including the data transmission status-based trust evaluation mechanism, sensing data availability, and sequential hypothesis test. Performance evaluation is presented in Section 4. Finally, conclusions and future work are presented in Section 5.

2 | SYSTEM MODEL

A generic CIoT is typically structured into four layers: application, transport, perception, and sensing layers, as shown in Figure 1. The application layer employs intelligent computing technologies (eg, data mining and cloud computing) to extract valuable information from processing voluminous data and provides an interface between users and other applications. The transport layer manages network operations, whereas the perception layer collects information [26]. The three layers above constitute a basic IoT architecture; however, because a spectrum bandwidth is not available, an IoT network cannot be realized. Hence, combined with CR technology, the sensing layer is proposed to provide an empty spectrum bandwidth for data delivery in three layers of the IoT architecture.

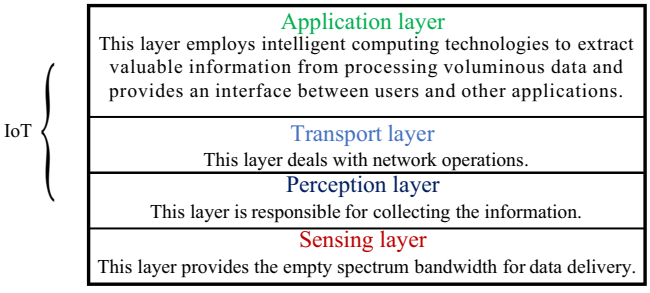

FIGURE 1 A generic CIoT architecture

As shown from the four-layered CIoT architecture above, CIoT security should include the security of the entire system crossing all four layers mentioned previously. Because the sensing layer is the fundamental brick of the upper three layers, the focus of this study is to solve the security of the sensing layer. In this section, we present the spectrum sensing and SDFA models in the sensing layer.

2.1 | Spectrum sensing model

In the sensing layer, strict requirements regarding the spectrum sensing accuracy are set to avoid collisions with the PU. However, it is extremely difficult to attain such an accuracy by individual spectrum sensing owing to shadowing and multipath fading encountered by IoT devices. Once the PU signal experiences deep fading or blocked by obstacles, the power of the received PU signal at the IoT devices may be too weak to be detected. Hence, CSS is proposed; the CSS performance will be improved by utilizing independent fading and multiple-user diversity. In the CSS architecture, all the participating IoT devices forward their observations regarding the presence or absence of the PU to the FC, which makes the global decision regarding whether the PU is transmitting. The channel between IoT devices and the FC is an error-free communication channel.

Based on the CSS process, we consider an infrastructure-based CIoT network comprising a PU, FC, and N IoT devices, wherein the AID ratio is α. Figure 2 illustrates an example of time slot assignment for IoT devices, where H_0 and H_1 represent the hypothesis regarding the absence and presence of the PU, respectively. In each sensing frame, N IoT devices independently sense the usage status of a particular spectrum channel in the sensing slot and send individual sensing results to the FC. In the processing slot, the FC makes the global decision regarding the channel status based on all received reports and subsequently sends its decision results to IoT devices. Subsequently, the FC makes the global decision via a specific rule and broadcasts a message (the

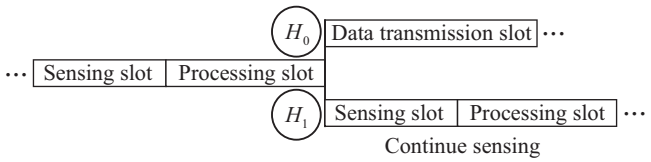

FIGURE 2 Periodic spectrum sensing frame structure

presence or absence of the PU) to the IoT devices; if the FC declares the presence of a PU, one of N IoT devices may start to transmit data in the transmission period over this channel. When the FC declares the absence of a PU, the IoT devices must be switched to sense the availability of another channel in the next sensing frame.

2.2 | Sensing data falsification attack model

The most vigorous and open facet of CIoT is that CRs are pregnable to multifarious malevolent attacks in the sensing layer. In CSS, the nature of aggregating data allows AIDs to launch SDFAs by sending false spectrum sensing data. For convenience, spectrum sensing data are abbreviated as sensing data hereinafter. The AIDs attempt to manipulate the FC into producing a global decision regarding the spectrum occupancy. This not only renders the spectrum scarcity problem more serious, but also creates security risks to the network. The reliable detection of the PU is important in CIoT. However, it becomes challenging when the AIDs share false sensing data in CSS, as shown in Figure 3.

An SDFA on the CIoT infrastructure can be categorized into two types according to its purpose: (a) *mis-detection attack and* (b) *false alarm attack*, as shown in Figure 4. A mis-detection attack exploits a cooperative opportunity to increase the mis-detection probability (falsifying the sensing result 1 into 0); therefore, the AIDs allure other IoT devices to access the channels in use and cause an excessive interference to the PU. In contrast to causing a harmful interference to the primary network, a mis-detection attack aims to prevent other normal IoT devices (NIDs) from using the existing

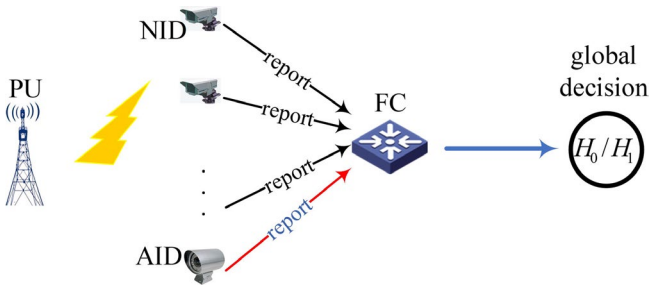

FIGURE 3 Cooperative spectrum sensing in the presence of AIDs

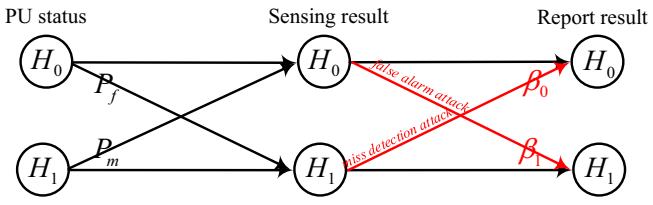

FIGURE 4 Sensing data falsification attack model

white space by increasing the false alarm probability (falsifying the sensing result 0 into 1) such that the AIDs can exclusively occupy the idle spectrum.

To evaluate the effect of the SDFA on CIoT, we adopt both the mis-detection and false alarm probabilities as the local performance metric. Furthermore, the mis-detection probability $P_{m,i}$ which represents the IoT device, outputs the sensing result that the PU is absent when the PU is present, and the false alarm probability $P_{f,i}$, which represents the IoT device, outputs the sensing result that the PU is present when the PU is absent are assumed to be the same for every IoT device irrespective of whether they are normal or abnormal, that is, $P_{m,i} = P_m$ and $P_{f,i} = P_f$, $i = 1, 2, \ldots, N$. Otherwise, the probability of the false alarm attack and the mis-detection attack are denoted as β_1 and β_0, respectively. Subsequently, the mis-detection probability P_m^A and the false alarm probability P_f^A of the j th AID ($P_{m,j}^A = P_m^A$ and $P_{f,j}^A = P_f^A$, $j = 1, 2, \ldots, \alpha N$) are given by

$$P_m^A = P_m(1-\beta_0) + (1-P_m)\beta_0 \tag{1}$$

and

$$P_f^A = P_f(1-\beta_1) + (1-P_f)\beta_1. \tag{2}$$

As shown in (1) and (2), when $\beta_0 = 1$ or $\beta_1 = 1$, the SDFA model naturally degenerates into two simple types of attack: always-no attack and always-yes attack; when $\beta_0 = 1$ and $\beta_1 = 1$, another special attack type appears, that is, always-false attack. In detail, the always-no, always-yes, and always-false attacks represent the AID always reporting the absence of the PU, the presence of the PU, and the PU status, respectively, as opposed to the sensing result to the FC regardless of the true sensing result. If those AIDs launch a simple attack characteristic, they can be easily identified by the decision fusion criteria at the FC. In fact, such a type of always attack has been extensively studied in [32–38]; the defense schemes in these references have shown satisfactory performance in some settings; however, when confronting the sophisticated attack probability (ie, a pair of attack probability β_1 and β_0 varying from 0 to 1), most of them are bound to fail.

3 | WEIGHTED SEQUENTIAL HYPOTHESIS TEST

AIDs can render the FC incapable of making a decision by completely blinding the system. In this case, the FC will be unable to decide on a particular decision regarding the presence of the phenomenon, and the performance of the FC cannot be better than a random guess of the state of channel. A critical value of 50% of the AIDs can completely blind the FC; more details regarding the blind scenario are available in [39]. In fact, a high AID ratio case has been ignored in most previous studies; however, this is a fundamental issue

involved in CSS. Therefore, we consider a sequential probability ratio test-based decision fusion criterion comprising the data transmission status-based trust evaluation mechanism, sensing data availability, and sequential hypothesis test that is robust against various SDFAs.

3.1 | Data transmission status-based trust evaluation mechanism

The trust concept is used in various contexts and with different meanings [24]. When a number of devices communicate in an uncertain network environment, trust is important for establishing a secure communication between things. Trust in the system from the devices' perspective should be considered in CIoT. To gain device trust, an effective mechanism should be established for defining trust in a dynamic and collaborative CIoT environment [21].

In the spectrum sensing behavior, the main objectives of trust research are as follows: first, the conception of a new trust evaluation mechanism for spectrum sensing behavior; next, the implementation of the trust evaluation mechanism. A good policy framework is desired to incorporate the evaluated trust level and current threat level prior to decision making [21]. Before proceeding with the description of our trust evaluation mechanism, a brief introduction to the global decision-based trust evaluation mechanism is provided, as shown in Figure 5.

Each IoT device is assigned with a trust value; the FC utilizes the global decision to verify the consistency of the local decision results from the IoT devices in each time slot; subsequently, the trust value is renewed. When the local decision is consistent with the global decision, the trust value will be increased by one; otherwise, it will be decreased by one. Therefore, according to the global decision-trust evaluate mechanism, the trust value of the ith IoT device at the kth time slot is described as follows:

$$\mathcal{T}_i(k) = \mathcal{T}_i(k-1) + (-1)^{l_i(k)+g(k)} \tag{3}$$

where $l_i(k)$ is the local decision; $g(k)$ is the global decision.

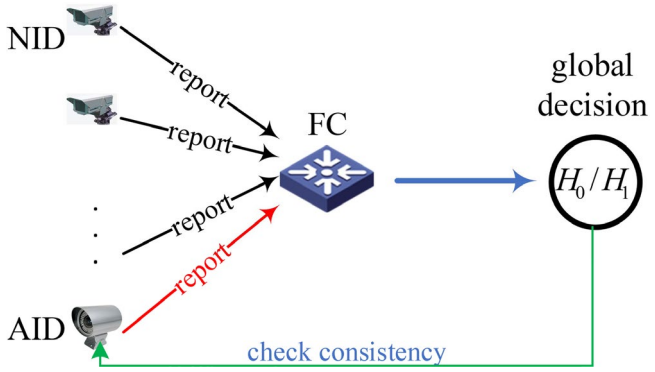

FIGURE 5 Global decision-based trust evaluation mechanism

The global decision-based trust evaluation mechanism has been adopted extensively in previous studies. In fact, this trust evaluation mechanism can cope with a few AIDs; however, when a large number of AIDs exist in CIoT, it becomes unreliable if the global decision is still used as a benchmark to verify the consistent of the local decision, because the global decision made by the FC may be compromised. Hence, it is indispensable to devise a robust trust evaluation mechanism that can verify the consistency.

Unlike the global decision-based trust evaluation mechanism, the main idea of our proposed trust evaluation mechanism is inspired by the periodic spectrum sensing frame structure, we utilize the data transmission status of an IoT device to determine whether the local decision is correct. Next, we introduce this trust evaluation mechanism in two cases.

3.1.1 | Case I

In Case I, when the FC declares the global decision as idle and broadcasts this message to the IoT devices at the processing slot, in accordance with the entire process of CSS and periodic spectrum sensing frame structure, at least one IoT device will be allocated to the channel for data transmission at the data transmission slot. At this time, if the delivery of data transmission occurs from the IoT device at the channel, then the global decision is correct; meanwhile, if collisions with the primary network occur, then the global decision is incorrect.

3.1.2 | Case II

In Case II, when the FC announces that the global decision is busy, typically, all IoT devices must switch to another channel and continue sensing; in other words, data transmission should not occur from the IoT device in the channel, and the global decision is regarded as correct. However, if data transmission occurs from the IoT device, then the global decision is incorrect.

In general, we can use the data transmission status $d(k)$ of the IoT devices instead of the global decision $g(k)$ to verify the consistency of the local decisions. The entire data transmission-based trust evaluation mechanism is illustrated in Figure 6. In addition, from the implementation of data transmission-based trust evaluation, the FC or a trusted node can be adopted to monitor the procedure above. However, it is noteworthy that the data transmission status is only used as a benchmark to verify the consistency of the local decisions and is not a substitute for the global decision as an indicator of whether the IoT device has accessed the channel (because data transmission status-based

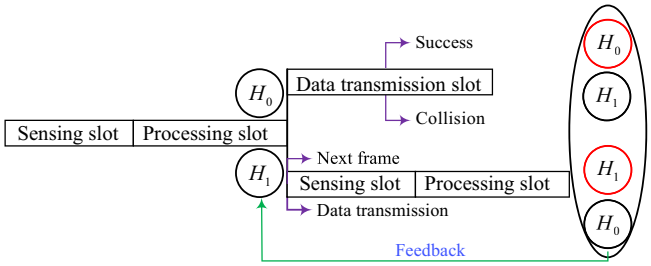

FIGURE 6 Data transmission status-based trust evaluation mechanism

trust evaluation mechanism is executed at the end of the global decision-making).

3.2 | Sensing data availability

To protect the sensing data integrity, security countermeasures are divided into two main categories: preventive and reactive. Preventive countermeasures seek to prevent intrusion attempts by directly protecting data and communications. Examples of preventive security include cryptographic protocols to authenticate the identity of devices and authorize users to access data. Authentication and authorization protocols ensure that the FC receives data streams only from trusted devices. They prevent an adversary from introducing malicious data to the FC via a rogue, unverified device [30].

Reactive countermeasures aim to mitigate failures in preventive security and ensure that the system continues to operate appropriately even when the preventive security fails. Meanwhile, preventive security protects CIoT networks by rendering it more difficult for an adversary to compromise data, and reactive security ensures that systems operate resiliently even when a number of IoT devices become hijacked. Reactive countermeasures include attack detection and identification algorithms for cyberphysical systems. The objectives of attack detection and identification are to determine if the measurements from any of the IoT devices have been altered by an adversary and to identify IoT devices that have been compromised, respectively. After detecting or identifying an attack, the system may perform a corrective action to mitigate the damage [30].

Following reactive countermeasures, we utilize the consistency verification of the local decision to evaluate the sensing data availability. After the kth sensing slot, the consistency $c_i(k)$ of the ith IoT device is empirically defined as

$$c_i(k) = \begin{cases} 0, & \mathcal{T}_i(k) \le 0, \\ \frac{\mathcal{T}_i(k)}{k}, & \mathcal{T}_i(k) > 0. \end{cases} \tag{4}$$

As shown in (4), $c_i(k)$ is measured only when $\mathcal{T}_i(k) > 0$; in other words, the IoT device correctly detects the PU status at least $\lceil k/2 \rceil$ times in k sensing frames; subsequently, its consistency can be measured. The goal is to mitigate the effect of abnormal sensing data on the global decision.

Next, the sensing data availability must be measured according to the consistency. Here, we use a new weight allocation to evaluate the sensing data availability, wherein the weight is a function with regard to the consistency and is presented as

$$w_i(k) = \begin{cases} 0, & \mathcal{T}_i(k) \le 0, \\ \sqrt{c_i(k)}, & \mathcal{T}_i(k) > 0. \end{cases} \tag{5}$$

In fact, the sensing data availability can be expressed as various functions involved in the consistency $c_i(k)$. However, it needs to comply with the basic principle, that is, the higher the consistency, the higher is the sensing data availability, except that the slope of the sensing data availability increases with increasing consistency in different functions, which affects the global performance and sample size. However, this is beyond the scope of this paper.

3.3 | Sequential hypothesis test

In the typical decision fusion criteria (ie, voting rule, Neyman–Pearson detection, and Bayesian test), the same methodology is employed for a multiple but fixed number of observation samples. In many practical situations, however, observations are collected sequentially and more information becomes available as time progresses. In such cases, we may wish to process the observations sequentially and make a global decision as soon as we are satisfied with the decision quality or detection performance. The aim is to perform additional observations only if they are necessary [40].

In the sequential hypothesis test process, after each sensing frame, the FC computes the likelihood ratio and compares it with two thresholds. Either it decides on one of the two hypotheses or it decides to take another observation. The main advantage of the sequential hypothesis test is that it requires, on the average, fewer observations to achieve the same probability of error performance as a fixed sample size test. This advantage is attained at the expense of additional computation [40].

Hence, the likelihood ratio is computed and compared with the lower threshold η_0 and the upper threshold η_1, which are determined by the specified values of $\overline{P}_f$ and $\overline{P}_m$, respectively. If the likelihood ratio is greater than or equal to η_1, the FC decides that H_1 is present. If the likelihood ratio is less than or equal to η_0, then the FC decides that H_0 is present.

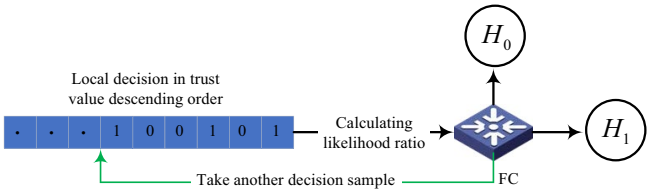

FIGURE 7 Weighted sequential hypothesis test

To secure CSS, we integrate the sensing data availability into the weight of the likelihood ratio; subsequently, the decision variable can be described as.

$$\begin{aligned}\Lambda_M(k) &= \prod_{i=1}^{M}\left[\frac{P\left(l_i(k)|H_1\right)}{P\left(l_i(k)|H_0\right)}\right]^{w_i(k)} \\ &= \prod_{i=1}^{M}\left[\frac{P\left(l_i(k)=1|H_1\right)}{P\left(l_i(k)=1|H_0\right)}\right]^{w_i(k)l_i(k)}\left[\frac{P\left(l_i(k)=0|H_1\right)}{P\left(l_i(k)=0|H_0\right)}\right]^{w_i(k)(1-l_i(k))} \\ &= \prod_{i=1}^{M}\left[\frac{1-P_m}{P_f}\right]^{w_i(k)l_i(k)}\left[\frac{P_m}{1-P_f}\right]^{w_i(k)(1-l_i(k))},\end{aligned} \tag{6}$$

where M is the required number of samples at the kth sensing frame.

As illustrated in Figure 7, the procedure of the sequential hypothesis test is described as follows:

If $\Lambda_M(k) \geq \eta_1$, the FC decides H_1;

If $\Lambda_M(k) \leq \eta_0$, the FC decides H_0;

If $\eta_0 < \Lambda_M(k) < \eta_1$, the FC takes another decision sample, where $\eta_0 = \overline{P}_m \Big/ \left(1-\overline{P}_f\right)$ and $\eta_1 = \left(1-\overline{P}_m\right) \Big/ \overline{P}_f$.

However, it is noteworthy that when sequentially calculating the likelihood ratio of the FC, the IoT device with a high trust value preferentially calculates the likelihood ratio such that the negative effect of abnormal sensing data on the global decision can be further mitigated.

After the FC decides that H_0 is present by the sequential hypothesis test, the IoT devices are allowed to access the idle channel. During resource allocation, the AID may selfishly occupy the channel for transmitting abnormal data; therefore, we should consider a fair scheduling strategy, that is, the IoT device with a high trust value has priority access to the idle channel. This is both a punishment for malicious spectrum sensing behavior and a reward for normal spectrum sensing behavior. Therefore, it is not necessary to take the same disposal as the previous secure CSS methods to remove the AIDs after they are identified, because a real AID cannot benefit from an SDFA and may not continue to launch an attack. However, for other NIDs, it can avoid being mistakenly eliminated owing to the effect of the fundamental characteristics of dynamically changed wireless channels.

4 | SIMULATION RESULTS AND DISCUSSIONS

In this section, we corroborate the effectiveness and robustness of our proposed data transmission status-based trust evaluation mechanism, as evidenced by the comparison-based simulation results. Additionally, we compare the performance of the conventional weighted sequential hypothesis test (CWSHT) and WSHT through in-depth numerical simulations under various scenarios. Here, we offer a brief overview of the CWSHT [32]. The decision variable of the CWSHT is

$$\Lambda_M(k) = \prod_{i=1}^{M}\left[\frac{P\left(l_i(k)|H_1\right)}{P\left(l_i(k)|H_0\right)}\right]^{w_i(k)}, \tag{7}$$

where

$$w_i(k) = \begin{cases} 0, & \mathcal{T}_i(k) \leq -5, \\ \dfrac{\mathcal{T}_i(k)+5}{\max\left(\mathcal{T}_i(k)\right)+5}, & \mathcal{T}_i(k) > -5. \end{cases} \tag{8}$$

Hence, it can be concluded that the CWSHT and WSHT exhibit the following differences: (a) trust evaluate mechanism—the CWSHT adopts the global decision-based trust evaluation mechanism while the WSHT adopts the data transmission status-based trust evaluation mechanism to solve the unreliability of the global decision as a benchmark for verifying local decisions; (b) the weight allocation—the CWSHT selects the threshold—5 to evaluate the sensing availability, while the WSHT utilizes the consistency verification of local decisions to evaluate the sensing data availability to filter unreliable sensing results caused by the shadowing characteristic and multipath effects; (c) the hypothesis test—each AID's likelihood ratio is randomly calculated into the decision variable when the CWSHT proceeds with the hypothesis test; however, the WSHT computes each AID's likelihood ratio in a trust value ranking order to reduce the number of samples and improve the sensing efficiency.

For comparison, we focus on the global performance: detection accuracy Q_d and average number of samples Q_s. The detection accuracy Q_d indicates the percentage of correct PU detection in 1000 sensing frames. The average number of samples refers to that the FC must collect from each neighbor to make a global decision; it measures the overhead of a particular decision fusion criterion [32]. For decision fusion and the fixed number likelihood ratio test, the number of samples is always N. The number of samples changes only for the sequential hypothesis test.

The values of important simulation parameters are as follows: the number of collaborative IoT devices N is 100, the local spectrum sensing performance P_f and P_m are set to 0.1, $\overline{P}_f = 10^{-3}$, and $\overline{P}_m = 10^{-3}$ in the sequential hypothesis test. Otherwise, all numerical results are simulated in 1000 sensing frames.

4.1 | Comparison of trust evaluation mechanism

We first simulate the (average) trust value of the NID and AID under the global decision-based trust evaluation and

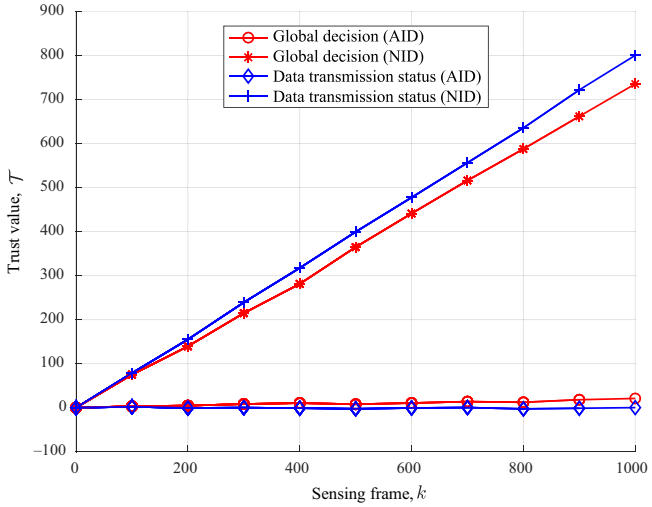

FIGURE 8 Trust value in the global decision/data transmission status-based trust evaluation mechanism when $\beta_1 = \beta_0 = 0.5$

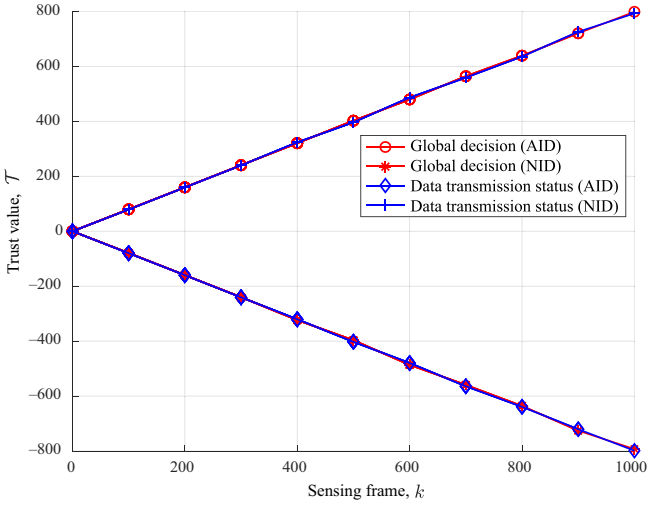

FIGURE 9 Trust value in the global decision/data transmission status-based trust evaluation mechanism when $\beta_1 = \beta_0 = 1$

data transmission status-based trust evaluation mechanisms. Considering that extensive studies have provided a satisfactory performance when the AIDs represent the minority, we assume the AID ratio α to be 0.8 and the probability of the hypothesis test H_0 to be 0.5. Figure 8 illustrates the trust value when $\beta_1 = \beta_0 = 0.5$; as shown, the trust values of the NID and AID are relatively close in two types of trust evaluation mechanisms, and that it is easy to implement AID identification by the difference in the trust value.

As the attack probability increases, that is, $\beta_1 = \beta_0 = 1$, the trust value in the global decision/data transmission status-based trust evaluation mechanism changes differently, as shown in Figure 9. Evidently, in our proposed data transmission status-based trust evaluation mechanism, the significant difference in the trust between the NID and AID values remains unchanged, while it is completely reversed in the global decision-based trust evaluation mechanism. In other words, if the global decision-based trust evaluation mechanism is applied into the CSS algorithm, the NID/AID can be regarded as the AID/NID. This is because the global decision is compromised when the attack probability is sufficiently large and the attack population sufficient.

4.2 | Effect of always attack

Owing to recent advances in secure CSS methods, significant effort has been expended to combat always attacks. Before discussing sophisticated attacks in detail, we begin with an in-depth investigation on always attacks, including always-yes, always-no, and always-false attacks. To build a fair comparison framework, we integrate the previous sequential hypothesis test (represented by [32–36,38]) to establish the CWSHT and vary the AID ratio α from 0 to 0.9.

Figures 10 and 11 display the detection accuracy and average number of samples of the CWSHT and WSHT in the presence of an always attack, respectively. As shown in Figure 10, the CWSHT and WSHT can maintain a 100% detection accuracy in the presence of a relatively low AID ratio; however, as the AID ratio increases, the detection accuracy of the CWSHT decreases to varying degrees in either the always-yes, always-no, or always-false attack, while our proposed WSHT still maintains a good detection accuracy until the AID ratio reaches 80%, where the detection accuracy only slightly decreases but is still impressive.

Figure 11 shows the average number of samples required for the CWSHT and WSHT. It is clear that under three types of always attacks, the sampling number of the WSHT remains at six even with an increasing AID ratio. In contrast to the CWSHT, the number of samples at the beginning increases with the AID ratio; however, after the AID ratio has

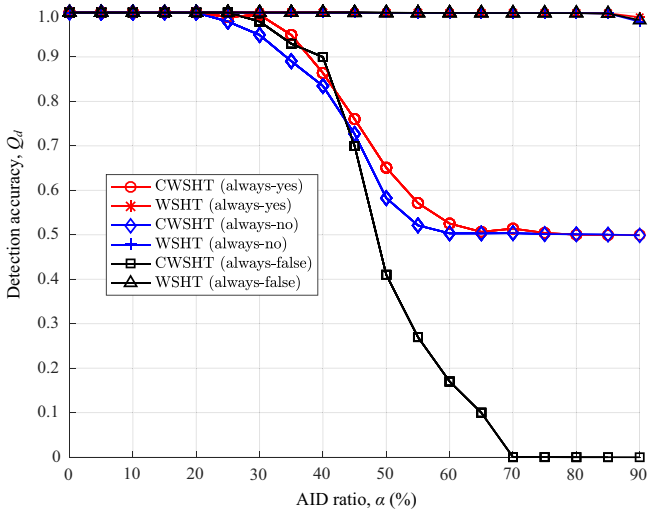

FIGURE 10 Detection accuracy of CWSHT and WSHT in the presence of always attack

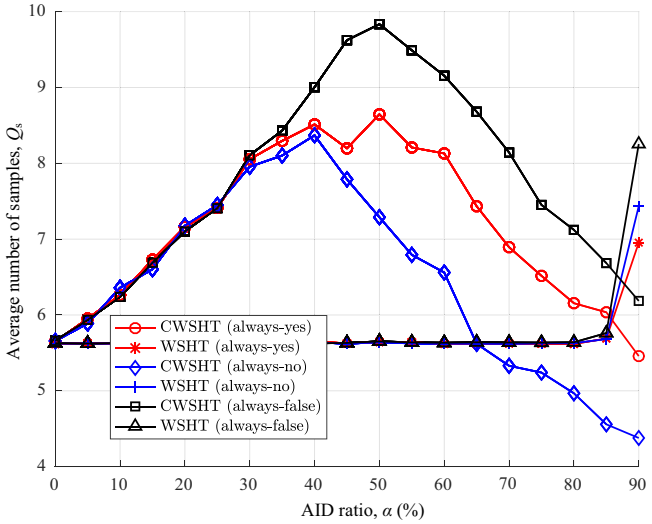

FIGURE 11 Average number of samples required for CWSHT and WSHT in the presence of always attack

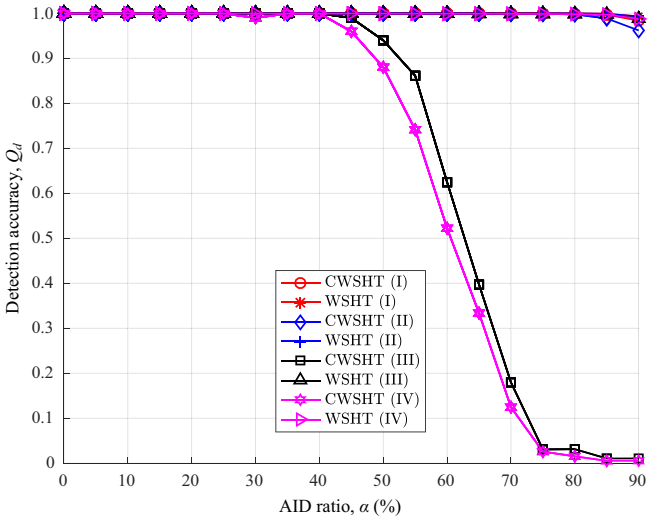

FIGURE 12 Detection accuracy of CWSHT and WSHT varies with the AID ratio when the AID launches sophisticated attacks

reached a certain level, the number of samples required starts to decline to varying degrees in the three always attacks.

In summary, the detection accuracy of the CWSHT deteriorates significantly at high AID ratios, while our proposed WSHT can guarantee a good detection accuracy with less sampling number if the AID ratio is less than 80%. In fact, typical malicious detection methods can easily cope with a few always attacks but fail to defend against a large number of always attacks. This is because the sequential hypothesis test process at the FC is compromised such that the FC requires more decision samples to make a global decision. However, when the AID ratio is sufficiently high, the global decision used as a benchmark of the local decision is no longer reliable, thereby causing a breakdown of the trust evaluation mechanism, while data transmission status as a verification for the consistency of local decisions is not affected. It is clear that the data transmission status-trust evaluation is crucial to ensure the robustness of the WSHT.

4.3 | Effect of sophisticated attack

Another aspect requiring further investigation is the performances of the WSHT and CWSHT in the presence of a sophisticated attack. Considering that an always attack is a special case of a probabilistic attack, when the attack probability is appropriately set from the malicious perspective, the AID can launch a stealthy attack and avoid being detected. Additionally, in the real world, the primary network may be relatively busy (ie, daytime) or idle (ie, nighttime) during a sensing observation period. Therefore, we consider four scenarios as follows:

Scenario I: the false alarm attack probability β_0 and the mis-detection attack probability β_1 are set to 0.5; the probability of the hypothesis test H_0 is 0.2.

Scenario II: the false alarm attack probability β_0 and the mis-detection attack probability β_1 are set to 0.5; the probability of the hypothesis test H_0 is 0.8.

Scenario III: the false alarm attack probability β_0 and the mis-detection attack probability β_1 are set to 0.8; the probability of the hypothesis test H_0 is 0.2.

Scenario IV: the false alarm attack probability β_0 and the mis-detection attack probability β_1 are set to 0.8; the probability of the hypothesis test H_0 is 0.8.

Based on the considerations above, Figures 12 and 13 show the detection accuracy and average number of the CWSHT and WSHT in four scenarios, respectively. As shown, the WSHT still maintains the same performance as that of the previous always attack, regardless of the attack probability and the probability of the hypothesis test H_0. Unlike the always attack case, an appropriate attack probability allows the AID devices to exhibit better attack stealthiness; therefore, in the CWSHT, both the downtrend of the detection accuracy and the uptrend of the average number of samples under sophisticated attacks are slower than those under the always attack. However, the superiority of our proposal with respect to the detection accuracy and sampling number is still evident in the presence of sophisticated attacks, which proves the high performance of the proposed WSHT, even when the AID devices represent the majority.

This can be attributed to the fact that, on the one hand, a new weight allocation related to the consistency of the local decisions is introduced to establish the sensing data availability, while, on the other hand, the sequential hypothesis test is conducted in the trust value descending order. Based on the data transmission status-based trust evaluation mechanism, the higher the trust value of the IoT device, the better is the consistency. Hence, the likelihood ratio of an IoT device with a high trust value can be preferentially calculated into the decision variable. This advantage facilitates the FC to promptly make an

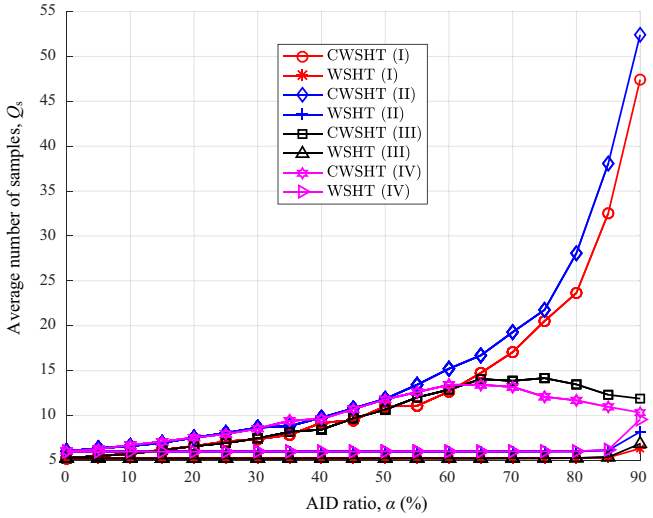

FIGURE 13 Average number of samples of CWSHT and WSHT varies with the AID ratio when the AID launches sophisticated attacks

accurate global decision. Consequently, the proposed WSHT can not only cope with different attacks, but also guarantee a high detection accuracy with a small number of samples.

5 | CONCLUSION AND FUTURE WORKS

Herein, we proposed a WSHT to defend against SDFAs in CIoT, which required a few samples for a better performance. Based on the mis-detection attack and false alarm attack models, we first developed the data transmission status-based trust evaluation mechanism from the periodic spectrum sensing frame structure to solve the unreliability of the global decision-based trust evaluation mechanism. Subsequently, we integrated the sensing data availability into the weight of the sequential hypothesis test. Moreover, we utilized the sequential characteristics to proceed with the sequential hypothesis test in descending order of the trust value. Finally, we conducted a series of numerical studies to corroborate the effectiveness and robustness of our proposed data transmission status and verify that the WSHT only required few samples compared with the CWSHT to achieve a better performance.

ACKNOWLEDGMENTS

The authors declare that they have no commercial or associative interests that represent a conflict of interest in connection with the work submitted.

ORCID

Jun Wu https://orcid.org/0000-0002-8918-3194

REFERENCES

1. K. Ashton, *That 'internet of things' thing*, RFID J. **22** (2009), no. 7, 97–114.
2. L. Atzori, A. Iera, and G. Morabito, *The internet of things: a survey*, Computer Netw. **54** (2010), no. 15, 2787–2805.
3. W. Lu et al., *Incentive mechanism based cooperative spectrum sharing for OFDM cognitive IoT network*, IEEE Trans. Netw. Sci. Engin. (2019). https://doi.org/10.1109/TNSE.2019.2917071
4. M. Zhang et al., *Cognitive internet of things: Concepts and application example*, Int. J. Comput. Sci. Issues **9** (2012), no. 6, 151.
5. Q. Wu et al., *Cognitive internet of things: a new paradigm beyond connection*, IEEE Internet Things J. **1** (2014), no. 2, 129–143.
6. J. Ploennigs, A. Ba, and M. Barry, *Materializing the promises of cognitive IoT: How cognitive buildings are shaping the way*, IEEE Internet Things J. **5** (2017), no. 4, 2367–2374.
7. K. Katzis and H. Ahmadi, *Challenges implementing Internet of Things (IoT) using cognitive radio capabilities in 5G mobile networks*, Internet of Things (IoT) in 5G Mobile Technologies. Springer, Cham, 2016, pp. 55–76.
8. A. A. Khan, M. H. Rehmani, and A. Rachedi, *When cognitive radio meets the internet of things?* in Proc. IEEE Int. Wirel. Commun. Mob. Comput. Conf. (Paphos, Cyprus), Sept. 2016, pp. 469–474.
9. A. A. Khan, M. H. Rehmani, and A. Rachedi, *Cognitive-radio-based internet of things: applications, architectures, spectrum related functionalities, and future research directions*, IEEE Wirel. Commun. **24** (2017), no. 3, 17–25.
10. S. Kim, *New game paradigm for IoT systems*, in Game Theory: Breakthroughs in Research and Practice. Hershey, PA, USA: IGI Global, 2017, p. 120.
11. K. Zaheer et al., *A Survey of decision-theoretic models for cognitive internet of things (CIoT)*, IEEE Access **6** (2018), 22489–22512.
12. A. N. Akhtar, F. Arif, and A. M. Siddique, *Spectrum decision framework to support cognitive radio based IoT in 5G*, Cognitive Radio in 4G/5G Wirel, Commun. Syst. (2018), 73.
13. P. Y. Chen, S. M. Cheng, and K. C. Chen, *Information fusion to defend intentional attack in internet of things*, IEEE Internet Things J. **1** (2014), no. 4, 337–348.
14. K. Zhang et al., *Sybil attacks and their defenses in the internet of things*, IEEE Internet Things J. **1** (2014), no. 5, 372–383.
15. Z. Li et al., *Worst-case cooperative jamming for secure communications in CIoT networks*, Sens. **16** (2016), no. 3, 339.
16. H. A. B. Salameh et al., *Spectrum assignment in cognitive radio networks for internet-of-things delay-sensitive applications under jamming attacks*, IEEE Internet Things J. **5** (2018), no. 3, 1904–1913.
17. S. C. Lin, C. Y. Wen, and W. A. Sethares, *Two-tier device-based authentication protocol against PUEA attacks for IoT applications*, IEEE Trans. Signal Inf. Process. over Netw. **4** (2017), no. 1, 33–47.
18. H. Suo et al., *Security in the internet of things: a review*, in Proc. IEEE Int. Conf. Comput. Sci. Electron. Eng. (Hangzhou, China), Mar. 2012, pp. 648–651.
19. R. Roman, J. Zhou, and J. Lopez, *On the features and challenges of security and privacy in distributed internet of things*, Comput. Netw. **57** (2013), no. 10, 2266–2279.
20. L. Da Xu, W. He, and S. Li, *Internet of things in industries: a survey*, IEEE Trans. Ind. Inform. **10** (2014), no. 4, 2233–2243.
21. M. Abomhara and G. M. Køien, *Security and privacy in the Internet of Things: Current status and open issues*, in Proc. Int. Conf. Priv. Secur. Mob. Syst. (Aalborg, Denmark), May 2014, pp. 1–8.
22. Q. Jing et al., *Security of the Internet of Things: perspectives and challenges*, Wirel. Netw. **20** (2014), no. 8, 2481–2501.
23. I. Andrea, C. Chrysostomou, and G. Hadjichristofi, *Internet of Things: Security vulnerabilities and challenges*, in Proc. IEEE Symp. Comput. Commun. (Larnaca, Cyprus), July 2015, pp. 180–187.

24. S. Sicari et al., *Security, privacy and trust in internet of things: The road ahead*, Comp. Netw. **76** (2015), 146–164.
25. W. Wei, A. T. Yang, and W. Shi, *Security in internet of things: Opportunities and challenges*, in Proc. Int. Conf. Identif. Inf. Knowl. Internet Things (Beijing, China), Oct. 2016, pp. 512–518.
26. I. Yaqoob et al., *Internet of things architecture: recent advances, taxonomy, requirements, and open challenges*, IEEE Wirel. Commun. **24** (2017), no. 3, 10–16.
27. F. A. Alaba et al., *Internet of things security: a survey*, J. Netw. Comput. Appl. **88** (2017), 10–28.
28. K. Sha et al., *On security challenges and open issues in internet of things*, Future Gener. Comput. Syst. **83** (2018), 326–337.
29. J. E. Siegel, S. Kumar, and S. E. Sarma, *The future internet of things: Secure, efficient, and model-based*, IEEE Internet Things J. **5** (2017), no. 4, 2386–2398.
30. Y. Chen, S. Kar, and J. M. F. Moura, *The internet of things: secure distributed inference*, IEEE Signal Process. Mag. **35** (2018), no. 5, 64–75.
31. H. A. Khattak et al., *Perception layer security in Internet of Things*, Future Gener. Comput. Syst. **100** (2019), 144–164.
32. R. Chen, J. M. J. Park, and K. Bian, *Robustness against Byzantine failures in distributed spectrum sensing*, Comput. Commun. **35** (2012), no. 17, 2115–2124.
33. C. Y. Chen et al., *Secure centralized spectrum sensing for cognitive radio networks*, Wirel. Netw. **18** (2012), no. 6, 667–677.
34. H. Wang et al. *An improved spectrum sensing data-fusion algorithm based on reputation*, in Proc. Int. Conf. Commun. Signal Process., Syst. Springer, Cham, 2015, pp. 359–364.
35. J. Lu and P. Wei, *Improved cooperative spectrum sensing based on the reputation in cognitive radio networks*, Int. J. Electron. **102** (2015), no. 5, 855–863.
36. A. A. Sharifi and J. M. Niya, *Securing collaborative spectrum sensing against malicious attackers in cognitive radio networks*, Wirel. Pers. Commun. **90** (2016), no. 1, 75–91.
37. F. Zhao and J. Feng, *Supporting trusted soft decision scheme using volatility decay in cooperative spectrum sensing*, KSII Trans. Internet and Inf. Syst. **10** (2016), no. 5, 2067–2080.
38. H. Alizadeh et al., *Attack-aware cooperative spectrum sensing in cognitive radio networks under Byzantine attack*, J. Commun. Engin. **6** (2017), no. 1, 81–98.
39. B. Kailkhuraet al.,*Distributed Bayesian detection in the presence of Byzantine data*, IEEE Trans. Signal Process. **63** (2015), no. 19, 5250–5263.
40. P. K. Varshney, Distributed detection and data fusion, Berlin, Germany: Springer-Verla, 1997.

AUTHOR BIOGRAPHIES

Jun Wu pursued the PhD degree at the National Mobile Communication Research Laboratory, School of Information Science and Engineering, Southeast University. Since 2019, he has been a lecturer at the School of Communication Engineering, Hangzhou Dianzi University. His research interests include cognitive radio networks, cooperative spectrum sensing, game theory, and related security issues. In the future, he will concentrate on solving various malicious attacks in collaborative spectrum sensing by machine learning.

Cong Wang has been pursuing the PhD degree at the National Mobile Communication Research Laboratory, Southeast University, Nanjing, China. Her research interests include spectrum resource allocation and its application to cognitive radio network.

Yue Yu has been pursuing the PhD degree at the National Mobile Communication Research Laboratory, Southeast University, Nanjing, China. His research interests include spectrum resource allocation, game theory, and network security.

Tiecheng Song received the BS and MS degrees in 1989 and 1992, respectively, from the Department of Radio Engineering, Southeast University, Nanjing, China. He received the PhD degree in 1996 from the School of Information Science and Engineering, Southeast University. In 1992, he joined the Department of Radio Engineering at Southeast University as a Research Associate, where he is currently a Professor of the School of Information Science and Engineering and National Mobile Communication Research Laboratory. He has also served as the Executive Vice President of the Nanjing Institute of Communication Technology. His research interests include 5G wireless systems, optical wireless communication technologies, and cognitive radio.

Jing Hu received the PhD degree from Southeast University in 2011 and is currently an Associate Professor and Master Instructor at the National Mobile Communication Research Laboratory, Southeast University. Her research interests include cognitive radio, wireless sensor networks, and vehicle networks.