NISA: Node Identification and Spoofing Attack Detection Based on Clock Features and Radio Information for Wireless Sensor Networks

Xintao Huan, *Student Member, IEEE*, Kyeong Soo Kim, *Senior Member, IEEE*, and Junqing Zhang

***Abstract*—Node identification based on unique hardware features like clock skews has been considered an efficient technique in wireless sensor networks (WSNs). Spoofing attacks imitating unique hardware features, however, could significantly impair or break down conventional clock-skew-based node identification due to exposed clock information through broadcasting. To defend against Spoofing attacks, we propose a new node identification scheme called *node identification against Spoofing attack* (NISA). It utilizes the reverse time synchronization framework, where sensor nodes' clock skews are estimated at the head of a WSN, and the spatially-correlated radio link information to achieve simultaneous node identification and attack detection. We further provide centralized and distributed NISA for covering both single-hop and multi-hop scenarios, the former of which employs a single-input and multiple-output convolutional neural network. With a real WSN testbed consisting of TelosB sensor nodes running TinyOS, we investigate the identifiability of clock skews under temperature and voltage variations and evaluate the performance of both centralized and distributed NISA. Experimental results demonstrate that both centralized and distributed NISA could provide accurate node identification and Spoofing attack detection.**

***Index Terms*—Node identification, Spoofing attack, clock skew, received signal strength, link quality indicator, wireless sensor network, convolutional neural network.**

I. Introduction

THE thriving technologies of wireless communications and networking expedite the reliance of our daily lives on smart devices such as laptops, smartphones, and nowadays Internet of Things (IoT) devices [1]. The security of those devices, therefore, becomes a serious concern. An efficient security measure for wireless networks is node identification, i.e., the identification of legitimate devices often in the presence of attackers. Conventional techniques based on pre-defined identifiers (IDs) or media access control (MAC) addresses have been widely used for node identification. Malicious devices, however, could impersonate legitimate ones so that attackers join a network, intercept data exchanged, and even launch attacks—like denial of service (DoS)—on the network [2], [3].

Device fingerprinting (DF) techniques utilizing hardware features as device-specific fingerprints are considered a promising technique that could alleviate the vulnerability of the conventional node identification techniques [4]. Of many hardware features, radio frequency (RF) and clock features—i.e., related with wireless modules and crystal oscillators (COs) of devices, respectively—attract much attention for a variety of application scenarios from wireless local area networks (WLANs) [5] to cloud [6] and controller area networks (CANs) [7] to IoT [8]. The RF features, however, often require additional equipment [8]—e.g., universal software radio peripheral (USRP)—for their measurement, so they couldn't be employed in normal gateway nodes (also called cluster heads) in multi-hop wireless networks. The clock features such as clock skews, on the other hand, are readily available as part of the time synchronization service for wireless communication and networking. Therefore, clock-skew-based node identification (CSNI) becomes an attractive option, especially for large-scale, multi-hop wireless sensor networks (WSNs).

In the literature, clock skews as device-specific fingerprints could be estimated by various methods from simple ratio-based one [9] to complex linear regression [10], and node identification could be achieved through simple thresholding [11] to advanced machine learning (ML) techniques [8], [12]. Depending on the location of clock skew estimation and node identification, CSNI schemes can be categorized as centralized (i.e., at the head[1]) or distributed (i.e., at gateway and/or sensor nodes) ones. In [11], a preliminary investigation of differentiating sensor nodes based on clock skews was studied using the flooding time synchronization protocol (FTSP) [13] as a skew estimator; sensor nodes locally estimate their clock skews and transmit them back to the head for centralized node identification by employing a simple thresholding method. In [14], the authors experimentally verified that different sensor nodes—i.e., MICAz [15] and TelosB [16]—have different and unique clock skews, which can be easily distinguished at a centralized monitoring station even in a multi-hop WSN. They also identified and discussed the issue of exposing the estimated clock skews through a *non-covert* channel from the security perspective; the transmission of clock skews over the network as in [11] is vulnerable to security attack [14]. The utilization of CSNI for defending some common attacks such as Sybil [17], Replication [18], and Wormhole [19] has also been studied: The combination of the continuity of clock skews and node IDs can be used to detect Sybil and Replication attacks [11], while the immutable characteristics of clock skews can be employed to defend Wormhole and Sybil attacks [20].

However, CSNI fails when malicious nodes can imitate the

X. Huan is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool L69 3GJ, U.K., and also with the Department of Communications and Networking, Xi'an Jiaotong-Liverpool University, Suzhou 215123, P. R. China (e-mail: Xintao.Huan@liverpool.ac.uk).

K. S. Kim is with the Department of Communications and Networking, Xi'an Jiaotong-Liverpool University, Suzhou 215123, P. R. China (e-mail: Kyeongsoo.Kim@xjtlu.edu.cn).

J. Zhang is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool L69 3GJ, U.K. (e-mail: Junqing.Zhang@liverpool.ac.uk).

[1]A head is typically an ensemble of a head/sink node and a monitoring station such as a PC or a server connected to it.

clock skews of legitimate ones to the point that fake and true clock skews cannot be differentiated from one another, which we call *Spoofing attack*[2] throughout the paper. The Spoofing attacker described in [22] could pretend itself as a legitimate sensor node by estimating the clock skew and offset based on the timestamps intercepted from the legitimate sensor node. To defend CSNI against Spoofing attack, therefore, we propose an approach called Node Identification against Spoofing Attack (NISA) based on the *reverse asymmetric time synchronization framework* [10], [23], [24]. Through unilaterally collecting the spatially-correlated radio information of received signal strength (RSS) and link quality indicator (LQI)[3] together with clock features extracted from the reverse time synchronization, NISA could simultaneously detect Spoofing attacks and achieve node identification. Note that radio information such as RSS is available as part of the transmission services for wireless communication and networking, which does not require additional equipment for its measurement; the spatial correlation of radio information has been widely employed for various applications such as indoor localization [25], [26], key generation [27], and attack detection and localization [28], [29]. To the best of the authors' knowledge, this is the first CSNI scheme simultaneously addressing the node identification and spoofing attack detection for both single-hop and multi-hop WSNs.

Our major contributions in this paper are summarized as follows:

- We propose centralized NISA that lays its foundation on BATS—i.e., the state-of-the-art reverse asymmetric time synchronization scheme—which can significantly improve the secrecy and identifiability of sensor nodes' clock skews. A single-input and multiple-output (SIMO) convolutional neural network (CNN) is employed in centralized NISA for simultaneous node identification and attack detection by taking the time series of clock features and radio information as its input.
- We also propose distributed NISA which can run at normal gateway nodes cover multi-hop scenarios, which most conventional RF fingerprint-based identification schemes [8], [30], [31] couldn't be applied to. As node identification and attack detection are done locally at gateway nodes in distributed NISA without the involvement of the head, it could immediately filter out attacks nearby and remove unnecessary packet transmissions upstream from the gateways to the head.
- We carry out a systematic investigation of the identifiability of sensor nodes' clock skews based on the high-precision centralized NISA. Unlike the existing investigations [32], [33], ours demonstrates the concurrent behaviors of the clock skews of a group of sensor nodes under temperature and voltage variations, which result from the drifts of digitally-controlled oscillators (DCOs) calibrated by COs.
- We present the design, implementation, and practical evaluation of the performance of both centralized and distributed NISA on a real WSN testbed consisting of TelosB [16] sensor nodes running TinyOS [34]. Experimental results demonstrate the effectiveness of both centralized and distributed NISA in node identification while defending against Spoofing attacks.

The rest of the paper is organized as follows: The overview of NISA is provided in Section II. The centralized and distributed realizations of NISA are presented in Sections III and IV. Our investigations on clock skews and experimental evaluation of the performance of both centralized and distributed NISA are discussed in Section V. Section VI reviews the related work in comparison to ours. Concluding remarks with future work are given in Section VII.

II. NISA: Node Identification and Spoofing Attack Detection Based on Clock Features and Radio Information

In this section, we first discuss the acquisition of the clock features for node identification and the characteristics of radio information for spoofing attack detection. Based on these foundations, then we provide an overview of the proposed NISA system.

A. Clock Features for Node Identification

Clock skew and offset represent the fundamental relationship between two hardware clocks in time synchronization. The accurate estimation and update of them are essential not only for high synchronization accuracy but also for reliable node identification based on the uniqueness of hardware clocks. Due to the imperfect manufacturing of the low-cost COs in common WSN devices, the clock frequencies of any two sensor nodes are hardly identical to each other [14]. Hence a different and unique clock frequency specific to each sensor node.

As a clock skew is one of the two parameters in modeling the relationship between the hardware clocks in the first-order affine *hardware clock* model that most time synchronization schemes rely on (e.g., [24], [35]), the clock skew between the hardware clock T_i of a sensor node i and the reference clock t of the head node can be defined as follows: For $i \in [0, 1, \ldots, N-1]$,

$$T_i(t) = (1 + \epsilon_i)t + \theta_i \rightarrow \epsilon_i = \frac{T_i(t) - \theta_i}{t} - 1, \tag{1}$$

where N denotes the number of sensor nodes, $\epsilon_i \in \mathbb{R}$ and $\theta_i \in \mathbb{R}$ respectively represent the clock skew and offset between the sensor node i's hardware clock and the reference clock.

For convenience, we often use clock frequency ratio R_i—also called *slope*—instead of the clock skew ϵ_i, which is given by:

$$R_i = 1 + \epsilon_i = \frac{T_i(t) - \theta_i}{t}. \tag{2}$$

The clock frequency ratio is calculated based on the clock time acquired from the internal DCO calibrated by the external CO, which represents the behaviors of both internal DCO and external CO. Note that, since DCO has up to ten times larger

[2]This attack is also called *clock skew replication attack* in [21].

[3]LQI is a vendor-specific value which is currently available in IEEE 802.15.4 standard.

ppm than CO [36], our investigation is conceptually different from those based only on external CO as in [32], [33].

The clock offset θ_i, also called *intercept*, represents the hardware clock at t=0 (i.e., $T_i(0)$). Unlike clock skew, it cannot be used as a device-specific fingerprint because its value does not depend on hardware features and changes whenever power cycling any of the two nodes. During the normal operation, however, its value is fixed & likely unique and rather stable for a short period of time, so it can be used as *an auxiliary variable* for CSNI, especially when fine-grained node identification is needed in large-scale WSNs as we will discuss in Section III.

The clock parameters are estimated based on the linear regression in BATS [10]: During the kth synchronization ($k \geq m$), the clock parameters of the sensor node i are estimated based on the latest m timestamp pairs in a sliding window as follows:

$$\mathbf{\Phi}_i(k) = \left\{\mathbf{t}(k)^\top \mathbf{t}(k)\right\}^{-1} \mathbf{t}(k)^\top \mathbf{T}_i(k), \tag{3}$$

where

$$\begin{aligned} \mathbf{\Phi}_i(k) &= \left[\hat{R}_i(k), \hat{\theta}_i(k)\right], \\ \mathbf{t}(k) &= [t_{k-m+1}, \ldots, t_k], \\ \mathbf{T}_i(k) &= [T_i(t_{k-m+1}), \ldots, T_i(t_k)], \end{aligned}$$

and $\hat{R}_i(k)$ and $\hat{\theta}_i(k)$ are the clock parameters of frequency ratio and offset, $(\cdot)^\top$ and $(\cdot)^{-1}$ denote vector transpose and matrix inverse, respectively. Note that the estimation of clock skew can be obtained from $\hat{R}_i(k)$, i.e., $\hat{\epsilon}_i(k)$=$\hat{R}_i(k)$−1.

It is worthwhile to mention the advantages of the clock parameter estimation of BATS when applied to CSNI. First, the reverse one-way time synchronization framework of BATS estimates the clock parameters of sensor nodes at the head and, thereby, does not expose estimated clock skews to other nodes in the network unlike conventional schemes where the clock skews estimated at sensor nodes have to be transmitted back to the head for node identification. Second, the sliding window size of the linear regression (i.e., m) can be adjusted for the operation environment of a WSN; a larger window size can improve the accuracy of the estimation for a static environment, while a smaller one can adapt to a dynamic environment more quickly at the expense of the estimation accuracy. Third, the high-precision estimation of clock parameters based on 64-bit double-precision floating-point at the head—providing up to 16 significant digits after a decimal point [37]—enables finer-grained CSNI which is critical for large-scale WSNs [14].

B. Radio Information for Spoofing Attack Detection

There are existing measures for CSNI against the Spoofing attack such as actively altering the synchronization interval [21]. In contrast to those measures, we novelly adopt the radio information in defending against Spoofing attacks, which could be passively measured to be consistent with the *passive nature* of the CSNI method.

Radio information such as RSS and LQI from a received packet indicates the signal strength and the quality of packet transmission. Specifically, RSS is correlated in space and, therefore, varies with location, which has been well exploited in many techniques such as indoor localization and key generation. For instance, the spatial variation of the RSS has been extensively studied in the key generation [27], [38], where they revealed that an attacker located more than one half-wavelength away from any existing legitimate device faces uncorrelated multipath fading in most scenarios. Note that RSS is not the instantaneous power of the received signal, which is not available at typical receivers, but its time average. In common WSN platforms, the average power of the received signal is referred to as the received signal strength indicator (RSSI).

LQI is another parameter on the radio information. In [39], it is suggested that LQI should be employed as an indicator for intermediate quality links after averaging over multiple readings due to its high variance over time; time-averaged LQI could be a better indicator for packet receive ratio (PRR) than RSSI. In contrast, when the link quality is good whereby the LQI is insensitive, RSSI could be a better indicator for distinguishing attackers. Note that LQI is platform-specific; LQI is highly correlated in space and can be used for key generation like RSS on some platforms [40] but not on other platforms. As such, LQI at least could be used for node identification for distinguishing attackers from legitimate devices when intermediate quality links are available [39]. Because the ensemble of RSSI and LQI is less sensitive to instantaneous link fluctuations, it can better represent the link status [41].

Note that, due to its spatial correlation, radio information is hard to be impersonated by attackers and, thereby, could complement clock features which are vulnerable to the Spoofing attack. In the following, we provide an overview of NISA which leverages both radio information and clock features to reinforce CSNI against Spoofing attacks.

C. Overview of NISA System

Two distinctive aspects of our design of NISA systems are *a covert channel* [14] and *passive nature*. For the former, the transmission of estimated clock features and radio information over a network, which is vulnerable to eavesdropping, cannot be allowed; for the latter, the system should be able to perform node identification and attack detection without the modification of standard procedures requiring the active involvement of sensor nodes like the frequent changes of synchronization time period suggested in [21]. For these reasons, we found that BATS, i.e., the reverse one-way time synchronization scheme whose estimations of clock features are all done at the head, is a perfect candidate for CSNI part of NISA; unlike conventional CSNI schemes relying on transmissions of clock features from sensor nodes to the head (or gateway nodes in the case of multi-hop WSNs) for node identification (e.g., [11]), BATS enables the clock features to be estimated and used for node identification at the same place (i.e., the head or gateway nodes) without exposing it over a network. Likewise, the head or gateway nodes can directly measure the spatially-correlated radio information for attack detection without exposing it over a network. Therefore, NISA could passively achieve node identification and attack detection through a covert channel.

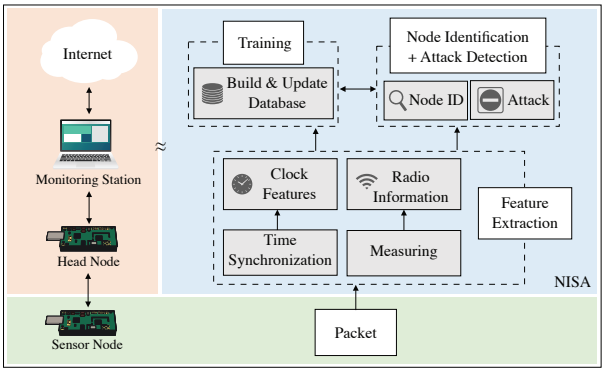
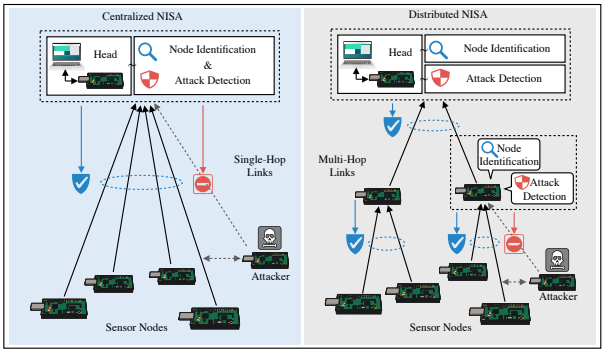


Fig. 1. Overview of NISA system.



(a) (b)

Fig. 2. NISA system designs: (a) Centralized NISA for single-hop WSNs; (b) distributed NISA for multi-hop WSNs.

In Fig. 1, we provide an overview of the proposed NISA system. When the packets from sensor nodes arrive, the head extracts the clock features—i.e., skew and offset—using the reverse time synchronization and measures the radio information of RSSI and LQI. Then a database is constructed based on them for node identification and attack detection later. However, as WSNs often require multi-hop configurations to cover vast areas, we provide two variations in NISA system design, namely *centralized NISA* and *distributed NISA*, for respectively addressing single-hop and multi-hop scenarios. As illustrated in Fig. 2 (a), the node identification and attack detection are done at the head consisting of a head node and a powerful monitoring station in centralized NISA, which makes it possible to employ advanced techniques for better performance. Because it would be impractical to implement a rather heavy centralized NISA system at gateway nodes, however, we propose distributed NISA in order to cover multi-hop scenarios as shown in Fig. 2 (b). Note that the system design is intentionally simplified in this case so that it can be easily implemented at gateway nodes that are often normal battery-powered sensor nodes.

The two system designs provide different options in performance and computational complexity tradeoff: Simple classification or thresholding schemes could suffice for distributed NISA but at the expense of relatively lower performance, which we discuss in Section V. Centralized NISA, on the other hand, could provide better performance through advanced

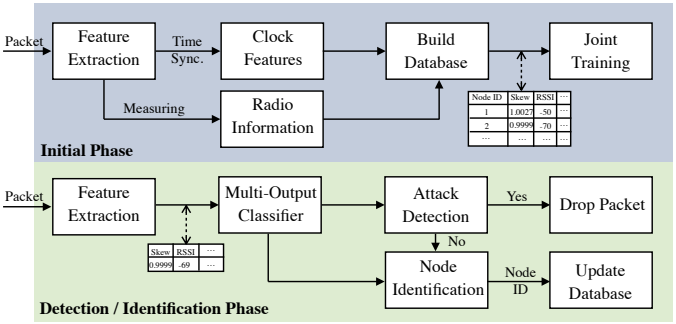


Fig. 3. Workflow of centralized NISA.

classification/detection methods like those based on neural networks [8], which can take all parameters into account and run node identification and attack detection in an integrated manner, at the expense of computational complexity.

III. Centralized NISA

As we discussed in Section II-C, centralized NISA is designed to provide better performance based on the integrated processing of clock features and radio information for single-hop WSNs. Here we provide more details of centralized NISA, including its workflow and implementation example.

A. Workflow of Centralized NISA

As shown in Fig. 3, there are two phases in the workflow of centralized NISA, i.e., the initial phase and detection/identification phase. From the packets received from sensor nodes, centralized NISA extracts clock features through time synchronization and collects radio information during the initial phase. The clock features and the radio information are then combined and fed into a database. After gathering enough data for all the sensor nodes in the network, a training process is performed based on the database for classification. The system switches to the detection/identification phase when the training process is completed.

During the detection/identification phase, a common functional block—i.e., the "Multi-Output Classifier" shown in Fig. 3—carries out both node identification and attack detection simultaneously. When an attack is detected, the corresponding packet is dropped; otherwise, the identified node ID is reported as a final result of CSNI. This group of data—i.e., a node ID and its corresponding clock features and radio information—is used to continuously update the database.

The major challenge in the workflow of centralized NISA is the implementation of the common functional block that should be able to process the clock features and the radio information as a whole for simultaneous node identification and attack detection through time-series classification (TSC); solutions based on advanced neural networks like CNN, recurrent neural network (RNN), and their many variations (e.g., long short-term memory (LSTM) and gated recurrent unit (GRU)) could be employed for TSC. Among them, CNN is rather popular for node identification (i.e., device fingerprinting) due to its capability of not only classifying

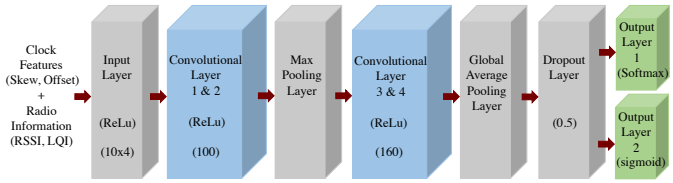


Fig. 4. SIMO CNN architecture employed as the multi-output classifier of centralized NISA.

nodes' fingerprints as image data [8], [42] but also solving the TSC problem as demonstrated in [43] and [44], which is why we choose it for our sample implementation described in the next subsection.

B. Implementation of Centralized NISA Based on SIMO CNN

Here we provide the details of our sample implementation of centralized NISA based on SIMO CNN. As discussed in Section II-A, BATS—the reverse one-way time synchronization scheme—is used for time synchronization and CSNI due to its capability of providing fine-grained identifiability of clock skews and offsets. At sensor nodes, no processes are running for NISA except MAC-layer timestamping required by BATS for achieving time synchronization. At the head node, it measures RSSI and LQI of each received packet and forwards them—together with the associated timestamps from MAC-layer timestamping—to a monitoring station which not only estimates clock skew and offset based on BATS but also performs NISA based on SIMO CNN. The details of the procedures at the head node for centralized NISA are given in the pseudocode in Appendix A.

Fig. 4 shows the architecture of SIMO CNN working as the multi-output classifier in the implementation of centralized NISA. The input layer of SIMO CNN takes time series of combined clock features and radio information—i.e., clock skew, clock offset, RSSI, and LQI—as its input. Convolutional layers 1 & 2 connecting the input layer are followed by a max pooling layer preventing overfitting, convolutional layers 3 & 4, and a global average pooling layer again preventing overfitting by using the average value. The output from the global average pooling layer goes through a dropout layer with dropout rate of 0.5, which is connected to output layers 1 and 2. All the convolutional layers use the rectified linear unit (ReLu) as their activation function. The output layer 1 for node identification uses softmax as its activation function for multiclass classification, while the output layer 2 for attack detection uses sigmoid as its activation function for binary classification. We use ADAM optimizer [45] for training and loss functions of categorical cross-entropy and binary cross-entropy for multi-class classification (node identification) and binary classification (attack detection). The batch size and the number of epochs are set to 10 and 100, respectively.

The proposed SIMO CNN is implemented in Python with Keras [46] and TensorFlow [47]. The subsystems at the head and the sensor nodes are implemented in nesC on TinyOS, and those in the monitoring station in Java and Python on macOS.

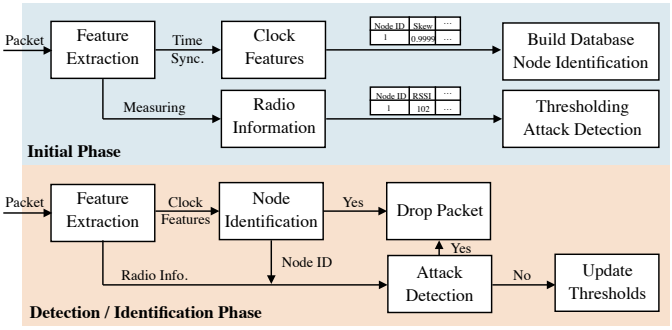


Fig. 5. Workflow of distributed NISA.

IV. Distributed NISA

Centralized NISA can provide better performance based on the integrated processing of clock features and radio information, but it would be impractical to implement a rather heavy centralized NISA system at gateway nodes in multi-hop WSNs. To support multi-hop WSNs, therefore, we separate the processing of node identification and that of attack detection in the design of distributed NISA, which not only lowers the computational complexity but also enables further simplification of each of the processing. In this section, we discuss the details of the workflow and the implementation of distributed NISA.

A. Workflow of Distributed NISA

Fig. 5 shows the workflow of distributed NISA. Using the packets received from sensor nodes, distributed NISA extracts clock features through time synchronization and collects radio information during the initial phase. Unlike centralized NISA, however, the clock features and the radio information are used separately for building a clock database for node identification and a radio database for attack detection, respectively.

During the detection/identification phase, the clock features are fed into a classifier for node identification, which operates on the built clock database consisting of pairs of node ID and clock features. The classifier could be implemented based on a simple thresholding method with upper and lower bounds for a clock skew [11] or a relatively complex classification algorithm like k-nearest neighbors (KNN) [48]. If the node identification is successful, the resulting node ID is used in further processing of attack detection; otherwise, the received packet is dropped.

Then, the radio information, together with the node ID, is provided as an input to the attack detection block, where potential Spoofing attacks are detected based on the node ID by comparing the received radio information with that already in the radio database; multiple data points are used for the processing in order to mitigate the effects of instantaneous fluctuations in the radio information like RSSI. It turns out that the anomaly detection based on RSSI with methods like thresholding is a well-studied problem [49]; there are various thresholding solutions with different complexities. Finally, if a Spoofing attack is detected, the received packet is dropped; otherwise, distributed NISA returns the node ID as a final

result and updates the databases based on the new legitimate data samples.

B. Implementation of Distributed NISA at Gateway Nodes

Based on the above workflow, we implement distributed NISA on gateway nodes which are ordinary sensor nodes in this work as discussed in Section I; our implementation of distributed NISA on an ordinary sensor node as a gateway node could demonstrate its practicality for multi-hop scenarios.

For time synchronization, we implement a simplified version of BATS based on simple linear regression for the estimation of clock parameters as in [13], which is also used for extracting clock features. We apply the reverse one-way synchronization framework of BATS to the time synchronization between a gateway node and its offspring sensor nodes in a multi-hop WSN, which was originally proposed for the time synchronization between the head and sensor nodes in a single-hop WSN [10]. For node identification, we compare the clock skew of a received packet with the average clock skews of legitimate nodes in the database and find the ID of a legitimate node that matches best; during the comparison, we use a threshold-based prefiltering of the clock skew from a fake node as suggested in [11]. We use a similar approach for attack detection using RSSI for comparison.

Note that the gateway nodes in distributed NISA can decide whether to accept or drop received packets based on the results of node identification and attack detection locally without transmitting the clock skews and the radio information for the processing at the head, which prevents attackers from eavesdropping them.

V. Experimental Results

In this section, we present the experimental results for the investigation on the identifiability of clock skews under various operating conditions and the performance evaluation of centralized and distributed NISA with single-hop and multi-hop WSNs.

A. Experimental Setup

Unlike conventional node identification schemes (e.g., [8]), the proposed NISA can be implemented and evaluated on a common WSN testbed without special hardware like USRP or modification of the existing infrastructure. The WSN testbed for our investigation of clock skews and evaluation of the performance of NISA systems, therefore, consists of ordinary head, gateway, and sensor nodes, all of which are based on TelosB motes running TinyOS. We use a single-hop star topology with 1 head and 10 sensor nodes for the investigation on clock skews & the evaluations of the performance of centralized NISA and a multi-hop tree topology with 1 head, 2 gateway, and 6 sensor nodes for the evaluation of the performance of distributed NISA, which are shown in Fig. 6 (a) and (b), respectively.

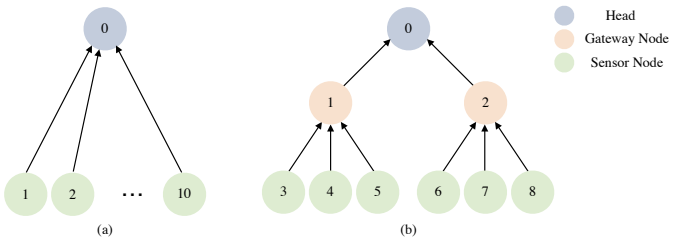


Fig. 6. Network topologies for (a) a single-hop WSN and (b) a multi-hop WSN.

B. Investigation on Clock Skew Identifiability

We carry out a series of experiments with the single-hop WSN shown in Fig. 6 (a) to investigate the fine-grained identifiability of clock skews provided by BATS under various operating environments, where we set the time synchronization interval and the sliding window size to 1 s and 19, respectively, as in [10].

1) Under Fixed Temperature and Voltage: We recorded the clock skews of each sensor node with respect to the head node for an hour in a controlled environment where the effect of temperature and voltage variations on the clock skews can be ignored. Fig. 7 (a) shows the clock frequency ratios of 10 sensor nodes, where we can observe that the frequency ratios of the sensor nodes are quite stable for the whole period and that most frequency ratios are distinguishable even in the low-precision view except those of sensor nodes 1 & 8 and 3 & 6. Thanks to the high-precision estimation of the clock parameters of BATS, we can zoom in those indistinguishable frequency ratios with higher precision as shown in Fig. 7 (b) and (c), which reveals that they can be clearly identified, too.

2) Under Temperature and Voltage Variations: It has been demonstrated by many (e.g., [14], [32], [33]) that hardware clocks, unless equipped with compensation circuits, are affected by temperature and voltage variations, resulting in time-varying clock skews; this is the case for the hardware clocks of most WSN devices, which are based on low-cost COs [33]. However, the concurrent behaviors of the clock skews of a group of sensor nodes resulting from the drifts of both DCOs and COs under temperature and voltage variations are yet to be investigated, which, in fact, is the main focus of the experiments described in this subsection.

According to the empirical study in [32], the effect of temperature and voltage variations on the clock skew could be modeled as a linear function for a period of time during which the amount of changes in temperature and voltage is rather small: Given the initial time t_0, the skew for $t>t_0$ is given by

$$\epsilon_i(t) = \epsilon_i(t_0) + \Delta\epsilon_i(t_0, t), \tag{4}$$

$$\Delta\epsilon_i(t_0, t) = \alpha(t)(\mathcal{T}(t) - \mathcal{T}(t_0)) + \beta(t)(\mathcal{V}(t) - \mathcal{V}(t_0)), \tag{5}$$

where $\Delta\epsilon_i(t_0, t)$ is the difference of the skew value between time t_0 and t, $\mathcal{T}(t)$ and $\mathcal{V}(t)$ are the temperature and the voltage at time t, and $\alpha(t)$ and $\beta(t)$ are the temperature-skew sensitivity factor and the voltage-skew sensitivity factor at time t; the sensitivity factors are to be estimated through

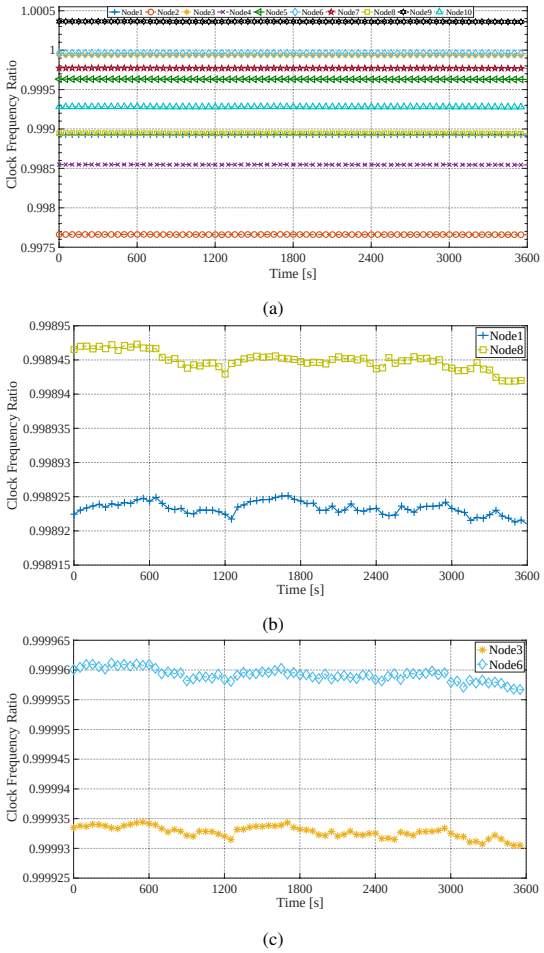


Fig. 7. Estimated clock frequency ratios of (a) all 10 sensor nodes and zoomed-in (b) sensor nodes 1 & 8 and (c) sensor nodes 3 & 6 over 3600 s.

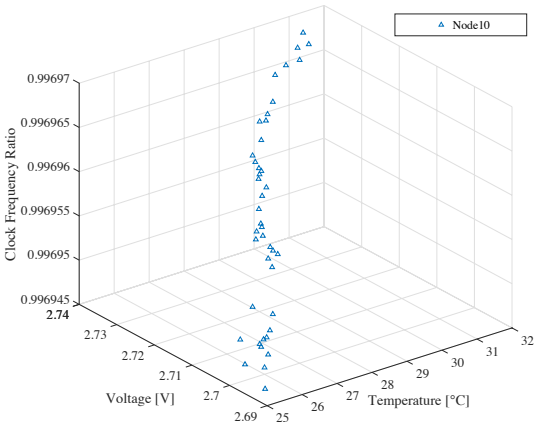


Fig. 8. Clock frequency ratio of sensor node 10 under temperature and voltage variations over 3600 s.

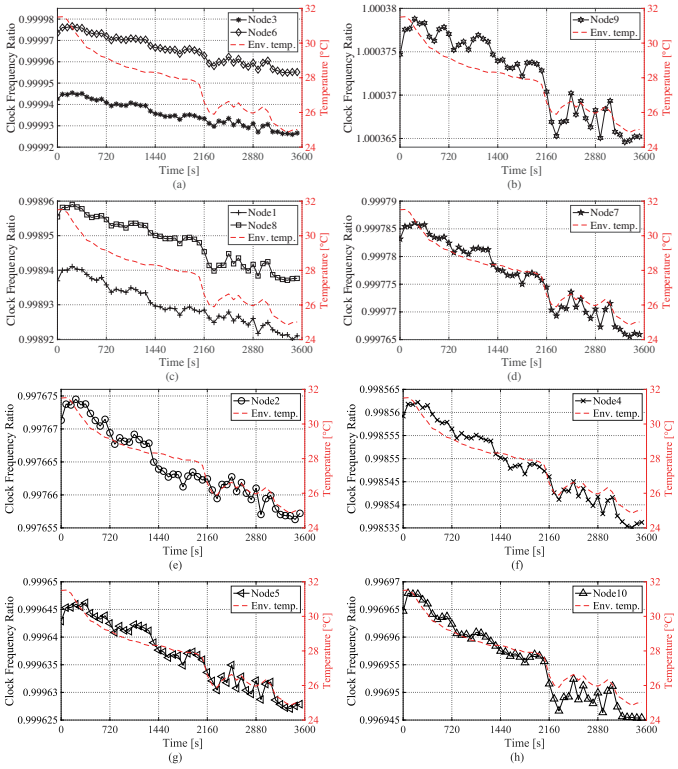


Fig. 9. Clock frequency ratios of sensor nodes under temperature variations over 3600 s: (a) Sensor nodes 3 & 6, (b) sensor node 9, (c) sensor nodes 1 & 8, (d) sensor node 7, (e) sensor node 2, (f) sensor node 4, (g) sensor node 5, and (h) sensor node 10.

experiments. Alternatively, we could feed as input data the time series of timestamps, temperatures, and voltages into a *neural network* so that it can learn the complex relationship between the clock skew and those environment variables [50].

Instead of directly modeling the effect of temperature and voltage variations on the clock skew, we could adjust the sliding window size mentioned in Section V-B so that the periodic updates of the clock skew reflect the effect, which is practical for finding the current clock skew under a dynamic environment and also sufficient for the purpose of node identification. Based on this, we experimentally investigate the identifiability of the clock skews under voltage and temperature variations in the following experiments.

We use the onboard temperature sensor to read the environment temperature which reduces gradually from 32 °C to the turn-over temperature 25 °C. We equip each sensor node with two AA batteries as in actual deployments and use the onboard voltage sensor to measure the voltage level. Since not all the batteries are brand new, their starting voltages are quite different from one another, which enables us to investigate the clock skew behavior under the same temperature change but different voltage levels. During the experiments, we observe that the voltage decrease is not significant, i.e., an average of 0.05 V decrease per each node during the 1-hour period.

Fig. 8 shows as an example the changes in the clock skew of sensor node 10 under temperature and voltage variations, where the range of the voltage level (0.05 V) is much smaller compared to that of the temperature (7 °C) as mentioned. The ranges of temperature and voltage variations in this experiment are typical for actual deployments where the batteries live for months and the temperature changes day and night.

Fig. 9 summarizes the effect of temperature variation on the clock skews of all 10 sensor nodes over 3600 s, where the left and right y-axes denote the clock frequency ratio and the

environment temperature, respectively.

Note that, though the starting voltage levels of all sensor nodes are different, their consumptions during the experiment are little and similar to one another, whose effect on the clock skews of all sensor nodes are relatively smaller compared to that of the temperature. Specifically, all the variations of the clock frequency ratios shown in Fig. 9 follow the similar trend of the varying temperature; Fig. 9 (a) and (c) in particular show that, though the clock frequency ratios of the sensor nodes are different, their changes are quite similar to each other in terms of both trend and the amount of changes. These results demonstrate that the clock skews of sensor nodes are still distinguishable as far as they are deployed under the same environment, which is of critical importance to CSNI.

C. Performance of Centralized NISA under Single-Hop Scenarios

We evaluate the performance of centralized NISA in a single-hop WSN shown in Fig. 6 (a), where each sensor node sends its packet to the head node every second as in [10]. We collect 1,000 and 500 packets for each sensor node respectively for training and validation on the first day, and another 1,000 packets for testing on the second day. Since there is no existing CSNI scheme carrying out simultaneous node identification and spoofing attack detection for WSNs, we put the focus of our evaluation on the effectiveness of the proposed centralized NISA as such using node identification accuracy and attack detection rate as performance measures. We carry out the performance evaluation in two steps: First, we focus on the effectiveness of the node identification without Spoofing attacks. Second, we evaluate the effectiveness of the attack detection under Spoofing attacks.

1) Without Spoofing Attacks: As discussed in Section III, the measurements from 10 consecutive packets are formed into time series in order to handle the variations of clock skew and offset and the fluctuations of RSS and LQI, resulting in 100 testing time series for each sensor node. Another crucial step towards TSC is the scaling of the datasets—we transform the value of our data into the range of $[0, 1]$, which is of importance for the classifier to achieve satisfactory results.

We trained the SIMO CNN of the system based on the training dataset, tuned its hyperparameters based on the validation dataset, and finally evaluated the performance of node identification based on the test dataset, whose confusion matrix is shown in Fig. 10. Labels 0 to 9 stand for sensor node IDs from 1 to 10 as shown in Fig. 6 (a). We identify each sensor node 100 times, resulting in 1,000 identifications in total, and obtain the node identification accuracy of 98.9%, which is well in line with our prior investigation on the identifiability of clock skews in Section V-B. In spite of such a high node identification accuracy, some testing segments are falsely classified to wrong labels, which results from the limited coverage of the training datasets for the clock behaviors represented by those segments. In contrast, other sensor nodes, e.g., the labels 1 and 3, are identified with 100% accuracy, which implies that their testing segments provide enough information to the system so that they can be uniquely identified based on the trained SIMO CNN model.

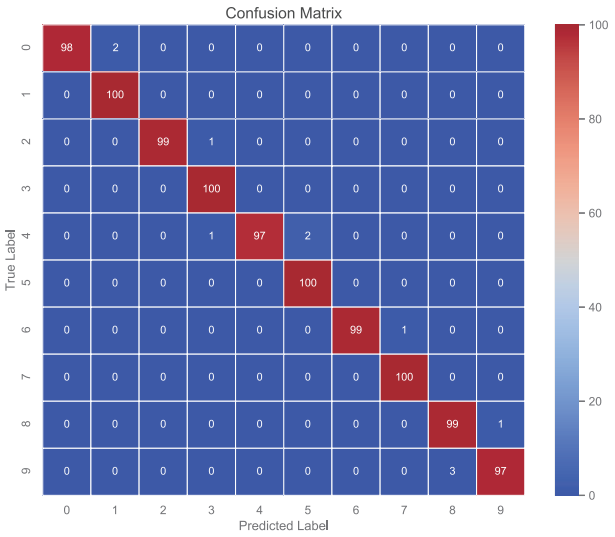


Fig. 10. Experimental results of centralized NISA for identifying 10 sensor nodes each for 100 times without Spoofing attacks.

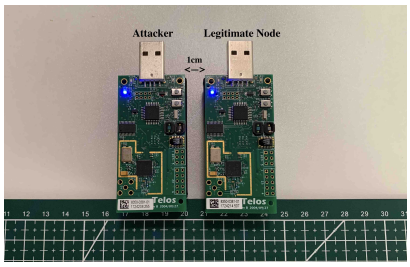


Fig. 11. Illustration of the distance between the attacker and the legitimate sensor node in our experiments.

From the experimental results discussed above, we found that the integrated system design of centralized NISA could clearly identify sensor nodes thanks to its use of combined clock features and radio information for most cases.

2) Under Spoofing Attacks: For the evaluation of the performance of centralized NISA under Spoofing attacks, we add one sensor node working as an attacker to the testbed described in Section V-A. We deploy the attacker next to a legitimate sensor with just 1-cm gap between the two as shown in Fig. 11 as a worst case scenario.

As in [14], [21], the attacker estimates the clock parameters of the legitimate sensor node—node 10 with the label 9 in our case—by eavesdropping on the time synchronization packets. The attacker then generates timestamps in its own time synchronization packets based on the legitimate sensor node's clock parameters through time synchronization so that the calculated clock skew at the head based on the received packets from the attacker would be very close to that of the legitimate sensor node. Fig. 12 (a) shows how close the attacker could imitate node 10 in its clock skew, where the attacker could very closely imitate the clock skew as investigated in [22]. Fig. 12 (b) and (c), on the other hand, show the radio information of RSSI and LQI of the attacker does not very close to that of node 10 due to its spatial correlation.

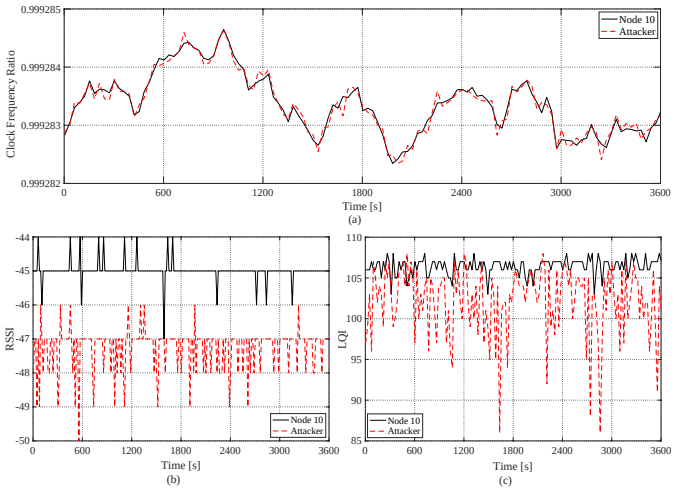


Fig. 12. Illustrations of (a) clock feature of skew, and radio information of (b) RSSI and (c) LQI between the attacker and the legitimate sensor node in our attack experiments.

The results shown in Fig. 12 demonstrate that conventional CSNI schemes may not detect the attacker solely based on the clock skews as discussed in [22]. However, the difference in RSSI between the attacker and node 10 enables centralized NISA, which takes into account both clock features and radio information during the node identification, to detect the attacks. Note that the LQI difference is not evident as that of RSSI, where there are many intersections; this suggests that LQI alone is not enough for attack detection, though it could supplement RSSI for further improvement of its performance.

The confusion matrix shown in Fig. 13 (a) summarizes the results of 1,100 trials of detecting attacks, 100 of which are true attacks originated by the attacker targeting at sensor node 10 (label 9). The x- and y-axis list the predicted and true labels where 0 and 1 indicate "no attack" and "under attack", respectively; when a predicted label matches a true label, we consider it as correct detection. The lower right corner of Fig. 13 (a) shows our detection for actual attacks, in which 99 out of 100 attacks are correctly detected (i.e., attack detection rate of 99%). The reason for this high detection rate is the high radio information difference between the attacker and the legitimate sensor node, even though the attacker is located very close to the legitimate sensor node (i.e., just 1-cm gap between them), which could demonstrate the effectiveness of the proposed system for detecting the attackers.

The confusion matrix shown in Fig. 13 (b) is for node identification which is carried out simultaneously with the attack detection. As discussed with Fig. 13 (a), there is one case where the fake data segment received from the attacker has been considered as a legitimate one due to a false attack detection. As a consequence, one additional node identification is done for node 10 of label 9 (i.e., 101 times in total unlike 100 times for other legitimate sensor nodes), while 99 out of 100 attacks are filtered out for node identification based on the results from the attack detection. Compared to the results shown in Fig. 10, we found that the effect of Spoofing attacks on node identification has been negligible thanks to the highly-

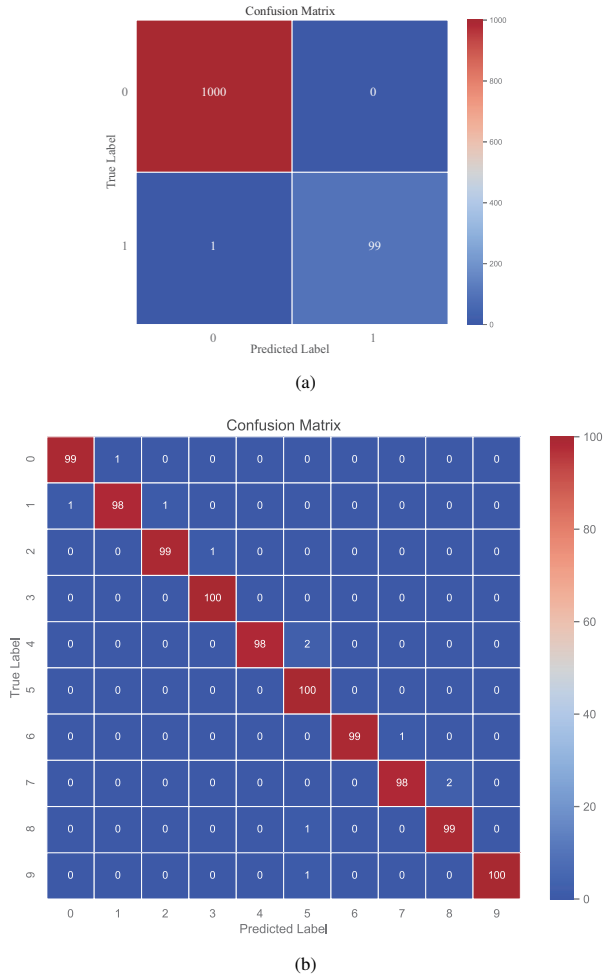


Fig. 13. Experimental results of centralized NISA for simultaneous (a) attack detection and (b) node identification for 10 sensor nodes and 1 attacker each for 100 times.

successful attack detection.

D. Performance of Distributed NISA under Multi-Hop Scenarios

For the evaluation of the performance of distributed NISA, we change the network topology to that of the multi-hop WSN shown in Fig. 6 (b). As in Section V-C, we also carry out the performance evaluation without and under Spoofing attacks.

1) Without Spoofing Attacks: We evaluate the performance of distributed NISA in the multi-hop WSN shown in Fig. 6 (b), where the NISA system is implemented at the head and gateway nodes, i.e., nodes 0, 1, and 2. The head node 0 and gateway nodes 1 and 2 are responsible for the node identification and attack detection for gateway nodes 1-2, sensor nodes 3-5, and sensor nodes 6-8, respectively.

As discussed in Section IV-A, distributed NISA drops the packet at either case of failed node identification or attack detection. A packet drop without the existence of attackers, therefore, indicates failed node identification. Fig. 14 demonstrates the evaluation results where distributed NISA could achieve the overall node identification accuracy of 96.563%. The identification of node 8 is the worst with the accuracy

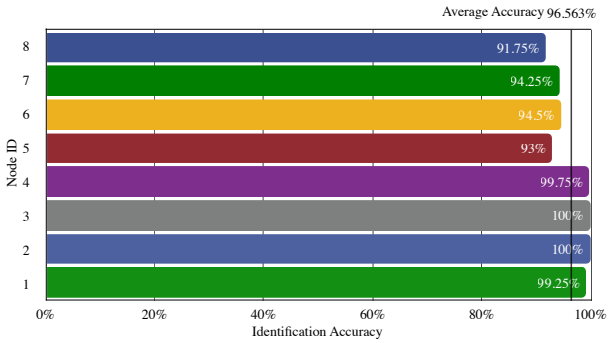


Fig. 14. Experimental results of distributed NISA for identifying 8 gateway and sensor nodes without Spoofing attacks.

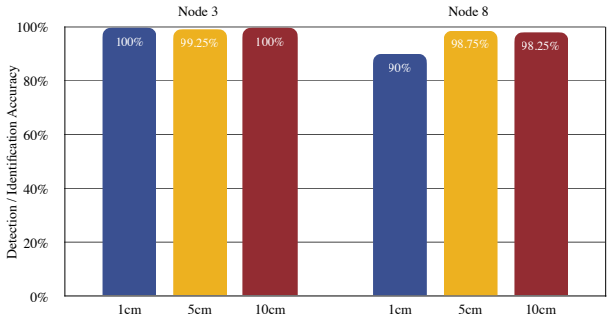


Fig. 15. Experimental results of distributed NISA running at gateway nodes: Detection/identification accuracy of node 3 and node 8 with spoofing attacks at distances of 1 cm, 5 cm, and 10 cm.

of 91.75% and that of nodes 2 and 3 are the best with the accuracy of 100%. This performance difference may result from the fluctuations in the radio information, which the simple thresholding cannot handle well.

2) Under Spoofing Attacks: To evaluate the performance of distributed NISA under Spoofing attacks, we add one sensor node working as an attacker as in Section V-C2. To comprehensively demonstrate the performance of distributed NISA under Spoofing attacks, we focus on nodes 8 and 3 in the experiments, which provide the worst and best node identification accuracy from the experiments without Spoofing attacks. In addition, we launch the attacks from different distances—i.e., 1 cm, 5 cm, and 10 cm—to the legitimate sensor nodes. Fig. 15 illustrates the combined accuracy of attack detection and node identification—called "detection/identification accuracy" in the following—of distributed NISA for nodes 8 and 3 under Spoofing attacks. For node 3, the detection/identification accuracy of above 99% is achieved for all the distances. For node 8, on the other hand, the detection/identification accuracy increases from 90% to above 98% as the attack distance increases from 1 cm to 10 cm; this is because the channel condition of the attacker differs more from that of the legitimate sensor node as the distance between the two increases.

VI. Comparison to Related Work

Changing Time Synchronization Interval: In [21], based on their investigations on the Spoofing attack countering CSNI, the authors observe that two main factors should be considered in spoofing clock skew, namely the difference between two consecutive offsets and the synchronization interval, which we call $\Delta\theta$ and SI, respectively. Changing $\Delta\theta$ could puzzle the Spoofing attacker in predicting the correct difference in the next period; the clock skew in this circumstance, however, becomes unstable & fluctuating and thereby being unpredictable, which further causes false identification. Consequently, they shift their focus on the latter factor of SI whose value in most time synchronization schemes (e.g., [10], [13]) is fixed. Based on their observations that changing SI could cause an immediate impact on the precision of attacker's imitating approach—i.e., wrong calculation of fake timestamps induced by miscalculation of SI—while the effectiveness of identification is maintained, they employ this method for defending against Spoofing attack in CSNI. The performance is evaluated through the experiments on a real testbed based on Taroko motes [51], which demonstrates that the proposed method reduces the success rate of an attack to less than 2.4%. Note that, however, this method requires frequent changing of SI; it is in fact changed every 7 rounds of synchronizations in their underlying time synchronization scheme. This changing period method requires an empirical value that demanding experiments in advance for its acquisition. In addition, it has certain assumptions on the clock skew calculation capability of the attacker, e.g., the attacker could not resume its accuracy in estimating the clock skew in certain synchronization rounds. Note that, unlike NISA, this method requires changes in existing synchronization schemes on the resource-constrained sensor nodes.

RSS Distribution (RSSD)-Based Fingerprinting: In [22], the authors experimentally demonstrate the vulnerability of CSNI to the Spoofing attack and, as a result, change the base of node identification from clock skews to spatially-correlated RSSs instead of reinforcing CSNI itself as in [21]. Specifically, a set of RSSs measured at a sensor node for its neighboring nodes becomes a fingerprint for the sensor node. Note that, employing RSS for detecting the Spoofing attack is not new in the literature; for instance, the effectiveness of detecting and localizing the Spoofing attackers has been systematically investigated in [28], [29]. Therefore, the RSSD-based fingerprinting proposed in [22] could identify sensor nodes based on their RSS fingerprints while defending the Spoofing attack.

Note that RSSD-based fingerprinting is different from NISA in that its node identification is solely based on radio information: In NISA, on the other hand, the radio information is used only for detecting the Spoofing attack. Due to the random fluctuation of a signal, the noise from multi-path effects, and the device dependency in RSS measurements [52], the RSSD-based fingerprinting has an innate limit in its identifiability compared to CSNI. The use of radio information in NISA, on the other hand, is dedicated for attack detection, which is binary classification and, therefore, does not require fine-grained identifiability. As we discussed in Section I, the use of RSS for node identification would make the RSSD-based fingerprinting unsuitable for large-scale scenarios due to its coarse-grained identifiability.

VII. Concluding Remarks

In this paper, we have proposed a new CSNI framework called NISA where node identification is protected from Spoofing attacks based on spatially-correlated radio information. We have also provided two variations of NISA system implementation—called *centralized NISA* and *distributed NISA*, respectively—to cover both single- and multi-hop scenarios.

In distributed NISA, node identification and attack detection are done independently with a dedicated algorithm for each, which could significantly lower the implementation complexity and, thereby, enables distributed NISA to be implemented and run at gateway nodes (i.e., cluster heads) as well as the head. Centralized NISA, on the other hand, could provide higher performance through its integrated processing of node identification and attack detection using a common algorithm for both based on the time-series of combined clock features and radio information. This synergy of the two processes that are separately handled in distributed NISA, however, comes at the expense of the higher implementation complexity and would limit its application to single-hop scenarios, i.e., running only at the head.

To investigate the identifiability of clock skews under various working conditions and the performance/complexity tradeoff between centralized and distributed NISA in single-hop and multi-hop WSNs, we have carried out a series of experiments on a real WSN testbed consisting of 11 TelosB motes running TinyOS. The experimental results demonstrate the identifiability of clock skews and their concurrent behaviors under temperature and voltage variations, which are enabled by the high-precision clock parameter estimation of BATS. We could also observe from the experimental results that the feasibility and effectiveness of node identification and Spoofing attack detection of centralized and distributed NISA are proper for single-hop and multi-hop scenarios, respectively.

Although we have provided the initial design, implementation, and performance evaluation of both centralized and distributed NISA in this paper, there is still room for further improvements: Centralized NISA has the potential to use not only other neural network architectures like RNN (including its variations of LSTM and GRU) and hybrid of CNN and RNN but also conventional machine learning algorithms such as random forest, which could have different performance and computational complexity; distributed NISA, on the other hand, could be improved by adopting more advanced thresholding and parameter fusion techniques.

Appendix
Pseudocode for Procedures of Centralized NISA at The Head Node

Algorithm 1 shows pseudocode for the procedures of centralized NISA running at the head node.

Data: The head node maintains the following data and variables:
- e: Event object;
- p: Packet object;
- $T2$: MAC-layer Timestamp;
- $RSSI$: RSSI value;
- LQI: LQI value;
- Q_P: FIFO queue for packets;
- Q_{T2}: FIFO queue for timestamp $T2$.

```
1  On detecting an event e:
2  switch e.type do
3      case PACKET do
4          if p.getDestAddress()==HEAD then
5              p ← Q_P.dequeue()
6              T2 ← Q_T2.dequeue()
7              RSSI ← getRSSI(p)
8              LQI ← getLQI(p)
9              p ← Packet(p, T2, RSSI, LQI)
10             send(p)          // forward the packet to
                monitoring station
11         else
               // Packets not for the head ...
12     otherwise do
           // Process other events ...
```

Algorithm 1: Pseudocode for the procedures of centralized NISA at the head node.

Acknowledgment

This work was supported in part by Research Development Fund (under Grant RDF-16-02-39) and Key Programme Special Fund (under Grant KSF-E-25) of Xi'an Jiaotong-Liverpool University.

References

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[3] L. Xiao, G. Sheng, X. Wan, W. Su, and P. Cheng, "Learning-based phy-layer authentication for underwater sensor networks," *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 60–63, Jan. 2019.

[4] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 94–104, First Quarter 2016.

[5] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Trans. Mobile Comput.*, vol. 9, no. 3, pp. 449–462, Mar. 2010.

[6] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," *IEEE Trans. Dependable Secure Comput.*, vol. 2, no. 2, pp. 93–108, Apr. 2005.

[7] S. U. Sagong, X. Ying, A. Clark, L. Bushnell, and R. Poovendran, "Cloaking the clock: Emulating clock skew in controller area networks," in *Proc. ICCPS'18*, Apr. 2018, pp. 32–42.

[8] J. Yu, A. Hu, G. Li, and L. Peng, "A robust RF fingerprinting approach using multisampling convolutional neural network," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6786–6799, Aug. 2019.

[9] J.-P. Sheu, W.-K. Hu, and J.-C. Lin, "Ratio-based time synchronization protocol in wireless sensor networks," *Telecommunication Systems*, vol. 39, no. 1, pp. 25–35, Sep. 2008.

[10] X. Huan, K. S. Kim, S. Lee, E. G. Lim, and A. Marshall, "A beaconless asymmetric energy-efficient time synchronization scheme for resource-constrained multi-hop wireless sensor networks," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1716–1730, Mar. 2020.

[11] D. Huang, W. Teng, C. Wang, H. Huang, and J. M. Hellerstein, "Clock skew based node identification in wireless sensor networks," in *Proc. 2008 IEEE GLOBECOM*, Nov. 2008, pp. 1–5.

[12] S. V. Radhakrishnan, A. S. Uluagac, and R. Beyah, "GTID: A technique for physical device and device type fingerprinting," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 5, pp. 519–532, Sep. 2015.

[13] M. Maróti, B. Kusy, G. Simon, and Ákos Lédeczi, "The flooding time synchronization protocol," in *Proc. SenSys'04*, Baltimore, MD, USA, Nov. 2004, pp. 39–49.

[14] M. B. Uddin and C. Castelluccia, "Toward clock skew based wireless sensor node services," in *Proc. WICON 2010*, Singapore, Mar. 2010, pp. 1–9.

[15] MicaZ datasheet. Accessed: 2021-02-01. [Online]. Available: http://courses.ece.ubc.ca/494/files/MICAz_Datasheet.pdf

[16] TelosB datasheet. Accessed: 2021-02-01. [Online]. Available: http://www2.ece.ohio-state.edu/~bibyk/ee582/telosMote.pdf

[17] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proc. IPSN'04*, Berkeley, CA, USA, Apr. 2004, pp. 259–268.

[18] H. Fu, S. Kawamura, M. Zhang, and L. Zhang, "Replication attack on random key pre-distribution schemes for wireless sensor networks," in *Proc. IAW 2005*, West Point, NY, USA, Jun. 2005, pp. 134–141.

[19] Y.-C. Hu, A. Perrig, and D. Johnson, "Wormhole attacks in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 370–380, Feb. 2006.

[20] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in *Proc. 2007 IEEE INFOCOM*, Anchorage, AK, USA, May 2007, pp. 107–115.

[21] D. Huang and W. Teng, "A defense against clock skew replication attacks in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 39, pp. 26–37, Mar. 2014.

[22] X. Mei, D. Liu, K. Sun, and D. Xu, "On feasibility of fingerprinting wireless sensor nodes using physical properties," in *Proc. IPDPS 2013*, Boston, MA, USA, May 2013, pp. 1112–1121.

[23] X. Huan and K. S. Kim, "On the practical implementation of propagation delay and clock skew compensated high-precision time synchronization schemes with resource-constrained sensor nodes in multi-hop wireless sensor networks," *Computer Networks*, vol. 166, p. 106959, Jan. 2020.

[24] K. S. Kim, S. Lee, and E. G. Lim, "Energy-efficient time synchronization based on asynchronous source clock frequency recovery and reverse two-way message exchanges in wireless sensor networks," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 347–359, Jan. 2017.

[25] A. Achroufene, Y. Amirat, and A. Chibani, "RSS-based indoor localization using belief function theory," *IEEE Trans. Autom. Sci. Eng.*, vol. 16, no. 3, pp. 1163–1180, Jul. 2019.

[26] S. Tomic, M. Beko, and R. Dinis, "RSS-based localization in wireless sensor networks using convex relaxation: Noncooperative and cooperative schemes," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 2037–2050, May 2015.

[27] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, Jan. 2016.

[28] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010.

[29] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 44–58, Jan. 2013.

[30] D. A. Knox and T. Kunz, "Wireless fingerprints inside a wireless sensor network," *ACM Trans. Sen. Netw.*, vol. 11, no. 2, Mar. 2015.

[31] B. W. Ramsey, B. E. Mullins, M. A. Temple, and M. R. Grimaila, "Wireless intrusion detection and device fingerprinting through preamble manipulation," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 5, pp. 585–596, Sep. 2015.

[32] M. Jin, T. Xing, X. Chen, X. Meng, D. Fang, and Y. He, "Dualsync: Taming clock skew variation for synchronization in low-power wireless networks," in *Proc. 2016 IEEE INFOCOM*, San Francisco, CA, USA, Apr. 2016, pp. 1–9.

[33] Z. Yang, L. He, L. Cai, and J. Pan, "Temperature-assisted clock synchronization and self-calibration for sensor networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3419–3429, Jun. 2014.

[34] TinyOS. Accessed: 2019-12-16. [Online]. Available: https://github.com/tinyos/tinyos-main

[35] N. M. Freris, S. R. Graham, and P. R. Kumar, "Fundamental limits on synchronizing clocks over networks," *Proc. IEEE*, vol. 56, no. 6, pp. 1352–1364, Jun. 2011.

[36] X. Huan and K. S. Kim, "Per-hop delay compensation in time synchronization for multi-hop wireless sensor networks based on packet-relaying gateways," *IEEE Commun. Lett.*, vol. 24, no. 10, pp. 2300–2304, Oct. 2020.

[37] IEEE Computer Society, *IEEE Std 754^{TM}-2008, IEEE Standard for floating-point arithmetic*, Std., 2008.

[38] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2820–2835, Dec. 2014.

[39] N. Baccour, A. Koubâa, L. Mottola, M. A. Zúñiga, H. Youssef, C. A. Boano, and M. Alves, "Radio link quality estimation in wireless sensor networks: A survey," *ACM Trans. Sen. Netw.*, vol. 8, no. 4, Sep. 2012.

[40] N. Kuruwatti, Y. N. Nayana, N. Sarole, G. Revadigar, and C. Javali, "LQI-Key: Symmetric key generation scheme for Internet-of-Things (IoT) devices using wireless channel link quality," in *Proc. ICAECC 2018*, Feb. 2018, pp. 1–6.

[41] W. Liu, Y. Xia, R. Luo, and S. Hu, "Lightweight, fluctuation insensitive multi-parameter fusion link quality estimation for wireless sensor networks," *IEEE Access*, vol. 8, pp. 28 496–28 511, Feb. 2020.

[42] K. Sankhe, M. Belgiovine, F. Zhou, L. Angioloni, F. Restuccia, S. D'Oro, T. Melodia, S. Ioannidis, and K. Chowdhury, "No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments," *IEEE Trans. Cogn. Commun. Netw.*, vol. 6, no. 1, pp. 165–178, Mar. 2020.

[43] B. Zhao, H. Lu, S. Chen, J. Liu, and D. Wu, "Convolutional neural networks for time series classification," *J. Syst. Eng. Electron.*, vol. 28, no. 1, pp. 162–169, Feb. 2017.

[44] C. Liu, W. Hsaio, and Y. Tu, "Time series classification with multivariate convolutional neural network," *IEEE Trans. Ind. Electron*, vol. 66, no. 6, pp. 4788–4797, Jun. 2019.

[45] D. Kingma and J. Ba, "ADAM: A method for stochastic optimization," *ArXiv e-prints*, Jan. 2017.

[46] F. Chollet *et al.*, "Keras," https://keras.io, 2015.

[47] TensorFlow^{TM}. Accessed: 2021-02-01. [Online]. Available: https://www.tensorflow.org/

[48] T. M. Cover and P. E. Hart, "Nearest neighbor pattern classification," *IEEE Trans. Inf. Theory*, vol. 13, no. 1, pp. 21–27, Jan. 1967.

[49] S. Fu, M. Ceriotti, Y. Jiang, C. Shih, X. Huan, and P. J. Marron, "An approach to detect anomalous degradation in signal strength of IEEE 802.15.4 links," in *Proc. IEEE SECON 2018*, Jun. 2018, pp. 1–9.

[50] G. Cena, S. Scanzio, and A. Valenzano, "A neural network clock discipline algorithm for the RBIS clock synchronization protocol," in *Proc. WFCS 2018*, Imperia, Italy, Jun. 2018, pp. 1–10.

[51] S.-Y. Lau, T.-H. Chang, S.-Y. Hu, H.-J. Huang, L. de Shyu, C.-M. Chiu, and P. Huang, "Sensor networks for everyday use: The BL-Live experience," in *Proc. SUTC'06*, vol. 1, Taichung, Taiwan, Jun. 2006, pp. 1–7.

[52] K. S. Kim, R. Wang, Z. Zhong, Z. Tan, H. Song, J. Cha, and S. Lee, "Large-scale location-aware services in access: Hierarchical building/floor classification and location estimation using Wi-Fi fingerprinting based on deep neural networks," *Fiber and Integrated Optics*, vol. 37, no. 5, pp. 277–289, Apr. 2018.

Xintao Huan (S'00) received the B.Sc. and M.Sc. degrees in computer engineering from the University of Duisburg-Essen, Germany, in 2013 and 2017, respectively. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering and Electronics, University of Liverpool, UK, and the Department of Communications and Networking, Xi'an Jiaotong-Liverpool University, China. He was a Research Assistant with the Networked Embedded Systems Group, University of Duisburg-Essen, from 2012 to 2016. His research interests include wireless sensor networks and Internet of Things.

Kyeong Soo Kim (S'89-M'97-SM'19) received PhD degree in Electronics Engineering from Seoul National University, Korea, in 1995, and has been working as an associate professor at the Department of Communications and Networking, Xi'an Jiaotong-Liverpool University, China, since 2014. From 1996 to 1997, he was engaged in the development of multi-channel asynchronous transfer mode (ATM) switching systems as a Post-Doc researcher at Washington University in St. Louis, Missouri. From 1997 to 2000, he worked with the passive optical network (PON) Systems R&D organization of Lucent Technologies and was involved with development of ATM-PON systems, which won 1999 Bell Labs President's Silver Award. From 2001 to 2007, he was with STMicroelectronics, working as a Principal Engineer; during this period, he also took the position of STMicroelectronics Researcher-in-Residence at the Stanford Networking Research Center. From 2007 to 2014, he worked at Swansea University, U.K., as an associate professor. Dr. Kim is a senior member of IEEE and a member of IET.

Junqing Zhang received the B.Eng and M.Eng degrees in Electrical Engineering from Tianjin University, China in 2009 and 2012, respectively, and the Ph.D degree in Electronics and Electrical Engineering from Queen's University Belfast, UK in 2016. From Feb. 2016 to Jan. 2018, he was a Postdoctoral Research Fellow with Queen's University Belfast. From Feb. 2018 to May 2020, he was a Tenure Track Fellow (Assistant Professor) with University of Liverpool, UK. Since June 2020, he is a Lecturer (Assistant Professor) with University of Liverpool. His research interests include Internet of Things, wireless security, physical layer security, key generation, and radio frequency fingerprinting identification.