IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 21 September 2023, accepted 17 October 2023, date of publication 25 October 2023, date of current version 3 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3327446

RESEARCH ARTICLE

AINL: Network Topology Identification of Multiple Communication Modes via Active Intercepting and Node Locating

RENHAI FENG, (Member, IEEE), AND JIAXU CUI, (Member, IEEE)
School of Electrical and Information Engineering, Tianjin University, Tianjin 300000, China
Corresponding author: Renhai Feng (fengrenhai@tju.edu.cn)

ABSTRACT Recent advance in the technologies of the tactical communication network has provided great opportunities for the new network-centric combat mode. Efficient modern communication wars are appealing for facilely mastering the key nodes and topological structure of non-cooperative networks at low computational cost. Accurate network topology identification becomes particularly relevant during the process of multiple communication situations. This paper proposes a novel method called active interception and node location (AINL) to achieve topology identification of multiple communication modes via active intercepting and node locating. Specially, active interception aims to use interfering nodes to interfere with the nodes in communication until frequency hopping occurs to obtain the corresponding power information and then calculate the location of communication nodes and their connection relationship. Node location adopts the positioning technology based on Received Signal Strength (RSS) and second-order cone programming relaxation to determine the location of communication nodes. The node location mechanism is automatically invoked to facilitate the accuracy of topology identification when there is a significant error in the estimated position of active interception. Experimental simulation results indicate that AINL can outperform competing passive interception methods as well as location methods significantly with a higher accuracy, lower power consumption and more stable recognition.

INDEX TERMS Active intercepting, node locating, topological identification, wireless communication.

I. INTRODUCTION

The booming development in tactical internet and communication system has gradually made the mode of modern warfare evolve into network information warfare. Tactical Internet is an important product of the application of Internet technology on the battlefield in the information age. Tactical internet confrontation is the key to winning the war. This confrontation aims to use advanced means to destroy the enemy's network system, master the battlefield initiative, and lay the foundation for victory in the war. In network confrontation, we not only hope to optimize our own network configuration, but also to use the least offensive means to quickly and accurately cause significant damage to the enemy's communication network. To achieve this goal, topology identification in communication networks is particularly important. If the enemy's network topology can be obtained, the key nodes in the network can be found, which will cause maximum damage to the enemy's military system while reducing consumption and improving attack efficiency. Research works on the recognition of network topological structure can provide important technical support for network countermeasure equipment. Existing methods to obtain the unknown topology of the communication network mainly apply the routing information or other address information in the data packet to determine the connected link [1], [2]. Since the data packets of non-cooperative networks are difficult to crack, how to actively identify the network topology without cracking the data packets is an urgent problem to be solved. Network topology identification generally involves the establishment of the topology model and the effective identification of the nodes in the model.

The associate editor coordinating the review of this manuscript and approving it for publication was Syed Mohammad Zafaruddin.

The network Topology model can be regarded as the physical layout of devices connected by transport media. Most works on information networks under operational conditions tend to learn different network structure model based on traditional graph theory. In graph theory, information networks are composed of simple 'points' and 'edges' between two points, and the network topology is depicted based on the statistical physical feature measures. In this modeling method, the importance of each node in the network is the same, and the edge is also a single relationship between nodes. For non-cooperative work in information networks, this theory cannot accurately reflect the differences between nodes in real network, nor can it reflect the diversity of transmission links between nodes. Since then, many works have pointed out that wireless network topology can well explain the actual military information network structure. For example, Wei and Fu [3] elaborately analyzed the characteristics of the network topology of tactical communication system and built a communication network model based on the graph theory. In the joint exercise between the British and American fleets, the U.S. army focused on analyzing the relevant nodes in the command and control system by studying the military email system, and abstracted the e-mail interaction during the entire exercise as a network topology, which showed that its military e-mail system had scale-free characteristics [4]. Various complex properties of the network displayed in the dynamic change process of the topology are conducive to building an efficient military information network. Yang et al. [5] reviewed the identification of dynamic parameters and the topology of complex networks, and provided a novel method to identify the parameters and network topology through the information conveyed in the dynamic changes of complex networks. In order to build a qualified and efficient military network, Van Waarde et al. [6] studied the necessary and sufficient topological conditions for dynamic network identifiability, which provided a prerequisite for identifiability and propelled the clear judgment of our non-cooperative networks.

Efficient node identification of topology modal is of great significance in network information warfare. Destroying 10% of the key nodes is enough to destroy the opponent's information network, since the topological structure of the network contains such information value that cannot be ignored. Without cooperation, the lack of prior knowledge about the network's topology would greatly limit our ability to characterize and analyze its communication behavior. The analysis of communication behavior is inseparable from the mutual transmission of signals, and the communication media will affect the effective transmission of signals. However, the communication medium of the wireless network makes that reciprocal transmission of information inevitably generate electromagnetic signals. This physical information can be monitored, which is difficult to encrypt and tamper with during transmission. The information potentially reflects the communication relationship and even the organizational structure in the target network, so analyzing and reasoning about this physical information presents broad prospects and great application value. Xu et al. [7] first proposed that full-duplex technology can be applied to the listener to interfere with the signal reception of the suspicious receiver while monitoring suspicious information, so as to improve the average interception rate. The technology verified that interference-assisted interception performs significantly better than passive interception. Following this groundbreaking work, a great deal of research has been conducted on active interception. Mukherjee and Swindlehurst [8] studied the design of a full duplex active eavesdropper in a three-user MIMOME monitoring channel, in which all nodes were equipped with multiple antennas. The MIMO secrecy ratio of the main channel can be minimized by optimizing the transmission and reception of sub-arrays and interference signal parameters. The design also described that the worst case interference covariance of arbitrary and Gaussian input signals was described and a numerical algorithm was developed to calculate the covariance, which showed the effectiveness of the countermeasure optimization algorithm and attackers can also block and listen in half duplex mode. Amariucai and Wei [9] studied the problem of half duplex active interception in fast fading channels, which divided the active interception into two functional modes: eavesdropping on transmissions between legitimate parties and interfering transmissions. In the classic scenario of fast fading AWGN channels with eavesdroppers, active eavesdroppers can seriously reduce the achievable confidentiality rate of signals. Ari et al. [10] studied the efficient transmission of data packets when active interception was performed in wireless networks. Through the comparisons with passive interception, it deeply demonstrated how that active interception affected the confidentiality throughput of data packet communication.

Compared to active interception, passive interception presents numerous advantages, each with its own distinctive benefits. Active interception involves the proactive transmission of specific probe packets or requests in order to gather information pertaining to network topology. This approach yields prompt and precise results in identifying the topology. Active interception can be tailored according to the specific identification requirements and objectives, enabling users to select appropriate interception strategies and craft packet designs in accordance with the unique characteristics of the network environment and topological structure. What's more, active interception can be meticulously controlled and scheduled within specified time periods to ensure the avoidance of excessive network load or interference. In contrast, passive interception dispenses with the necessity of transmitting specific packets or requests to the network. Instead, it relies on the comprehensive analysis and interception of pre-existing network traffic, thereby circumventing any supplementary burden or interference that might compromise the network's performance. Passive interception diligently monitors and analyzes network traffic in real-time, ultimately supplying

real-time topology information. Viani et al. [11] used sensor technology and WiFi network to detect passive targets and applied passive interception to target localization. The wireless network is a system composed of specific entities and their intrinsic interactions. Different types of networks will show different characteristics, but even for the same type of network, its different topology will lead to the evolution of different dynamic behaviors and system functions in the network. Mateos et al. [12] believed that the observation results were generated by the operation of the network with potential underlying structure, and emphasized that network topology reasoning was a prominent problem in the network science. But in reality, we can easily acquire the performance data of the network, but the structure of network and its dynamics are difficult to obtain directly by observation. Moreover, Zhang et al. [13] also pointed out that it was an important and arduous task to recover the potential network structure and dynamic laws according to the observed time series data. This is a typical network reconfiguration problem in the field of network science [14]: inferring which nodes in the network are connected by edges based on the operating performance without knowing the evolution dynamics of the system. Existing solutions to the problem are diverse, ranging from correlation based method [15], information-theory based method [16], Granger-causality-test based method [17], compression-sensing based method [18], drive-response based method [19], to graph-based neural network method [20]. The aforementioned literature illustrates that passive interception is subject to limitations in non-cooperative networks. In such scenarios, active interception can compensate for the shortcomings of passive interception by actively engaging and transmitting specific requests. Through active interaction with the target network, active interception can attain a greater abundance of information, making it the preferred approach for acquiring network topology. In addition to the intercepting technology in networks, there are also location algorithms for node identification. Most of the location algorithms can be divided into range-dependent location algorithm [21], [22], [23] and range-independent location algorithm [24], [25]. In most distance-related location algorithms, ranging can usually be achieved by time of arrival [26], time difference of arrival [27] and angle of arrival [28] is a common method, which requires additional hardware support. The cost of these ranging methods is very high in large-scale wireless networks. However, RSS [29] is considered to be a relatively simple method for the ranging problem. It aims to convert the received signal strength into distance through theoretical and empirical models. This method is widely used in many fields because it is easy to implement and does not need additional hardware.

This paper proposes a novel method for general network topology identification, which incorporates the active intercepting and node locating to accurately obtain the structure of information network. Different from previous active interception methods, the proposed method uses the interfering nodes to interfere with the communication between communicating nodes until frequency hopping. The accuracy of our topology identification can be effectively improved when enabling the node location strategy to assist the location of the communicating nodes. The main contribution of this paper lies in the following three folds:

1) A novel original active interception scheme is proposed, which avoids the lack of information in non-cooperative networks.
2) The interfering nodes in the active interception tend to apply dichotomy to transmit interference signals, which effectively reduces the power consumption of the wireless network and improves the network life.
3) The proposed AINL appropriately integrates the node location mechanism to supplement the active interception, which greatly facilitates the precise location of communication nodes and improves the accuracy of topology identification.

The rest of this paper is organized as follows: In Section II, we introduce the proposed AINL method, which detailedly describes the active interception and node location. The simulation results are given in Section III and the conclusion for the work is provided in Section IV.

II. THE PROPOSED AINL METHOD

A. METHOD OVERVIEW

We provide a method to identify the network topology compatible with multiple communication nodes. The unknown wireless network is also termed the target network. It presents a preset topology with N nodes, where 80% of the nodes are transmitters and the rest are receivers. Without loss of generality, we do not consider packet forwarding, that is, two nodes can communicate directly. The preset communication modes in wireless network contain Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA) and Orthogonal Frequency Division Multiplexing (OFDM). Because FDMA, TDMA CDMA and OFDM are the most basic communication modes, other communication modes are improved on this basis. Moreover, active interception and passive interception are parallel comparison and analysis in communication modes, so we adopt the most primitive and simple communication modes.

In our wireless network, we define the console as the control center responsible for allocating channels and frequency bands to communication nodes. The console also caches and records the communication process. As communication nodes are full-duplex, the console is able to obtain and record the node ID and communication status when two communication nodes are transmitting. In the case of frequency hopping communication, the console redistributes channels and frequency bands to re-establish communication between the nodes. It also assumes that there is no aliasing between signals. Although the topology may change over time in practice, but we can assume that the topology is constant in a small observation period. So frequency hopping is relatively stable in the observation period.

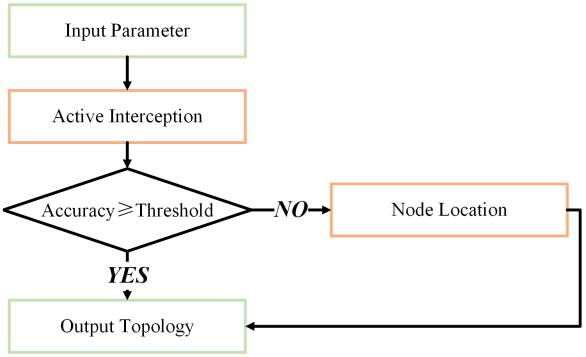


FIGURE 1. Overall framework of AINL.

Fig.1 illustrates the overall framework of our proposed AINL method, which directly depicts the main workflow for the network topology identification. The goal of this paper is to infer and obtain accurate target network topology in wartime network conditions. Since it is very difficult to get and decode data packets, we first choose an active interception way to obtain the specific location of network nodes, if some of the nodes information obtained is not accurate enough to reach an accuracy of 80%, the positioning technique will be invoked to correct the node location. To identify the network topology, we need to intercept the nodes that are communicating. As only two nodes can communicate in a frequency band, interfering node (also known as EVE [30]) can intercept to different frequency bands in turn. Half-duplex EVE can store the distance between itself and the communication node, and when we want to use the distance, we can read it and calculate it. In our method, the correct ID of nodes as well as their connection relationship can be obtained by matching the calculated information of nodes with that information stored in the console, and then the location information of nodes can be obtained based on this information. Specially, we extract the connectivity between different nodes by actively interfering with the communication between nodes to obtain the adjacency matrix of the network. If the identification accuracy of the node is less than 80%, node location strategy will be enabled to improve the identification accuracy.

B. ACTIVE INTERCEPTION

General graphs can be classified into the following four categories: weighted directed graph, weighted undirected graph, unweighted directed graph and unweighted undirected graph. The wireless network can be described as a directed graph $\mathbf{G}(\mathbf{S_t}, \mathbf{S_r}, \mathbf{L})$, where $\mathbf{S_t} = \{1, 2, \ldots, M\}$ is the set of transmitting nodes, $\mathbf{S_r} = \{M+1, M+2, \ldots, N\}, N > M$ is the set of receiving nodes, and $\mathbf{L} = l_{i,j} : i \in \mathbf{S_t}, j \in \mathbf{S_r}$ is the set of edges between the ith transmitting node and the jth receiving node. When employing graph signal analysis to examine data structure, the fundamental concept entails expressing the data through a graph formulated by means of an adjacency matrix. This matrix serves to define the interconnectedness of all graph nodes, with its elements, such as 0 and 1, indicating whether vertices are linked or not. The network topology, encapsulated within an unknown adjacency matrix $\mathbf{H} \in R^{N \times N}$, assigns each element $h_{i,j}$ in $\mathbf{H}$ a value that signifies the connection between the transmitting node i and the receiving node j. If the ith transmitting node and the jth receiving node are linked, $h_{i,j}$ assumes a value of 1; otherwise, it is assigned a value of 0.

EVE actively sends the interfered signals to interfere with communication nodes to obtain the power information at frequency hopping time based on the principle that frequency hopping occurs when the communication nodes are interfered by the same frequency. While adjusting the Modulation and Coding Scheme (MCS) or transmission power can affect transmission rate and performance, these factors may not have as significant an impact as frequency hopping. Frequency hopping directly affects the communication mode and structure, whereas adjusting transmission rate and power primarily affect the performance of communication. Li et al. [31] proposed that frequency hopping sequences are generated by a specific model with regular patterns. By using a large amount of intercepted frequency hopping signal data, a long-term and short-term memory neural network model can be established for accurate frequency estimation. Unlike MCS, frequency hopping provides more direct, observable, and obvious changes that can be used for network topology identification. We acknowledge that MCS can be used as a reference factor for network topology identification, but it may provide relatively little information compared to frequency hopping. Therefore, we chose frequency hopping as the key factor in network topology identification due to its more direct and noticeable effects. The console obtains the information that exactly interferes with the frequency hopping time of the communication nodes, and then deduces the position information and communication status of the communication nodes.

The EVE interferes with the communication nodes by transmitting interference signals of different powers. General methods tend to gradually increase the transmit power of the EVE in small enough steps until it interferes with the communication nodes. These methods are relatively inefficient and they usually consume a lot of resources. Hence dichotomy is introduced in our method. Dichotomy is a method in which a function has monotonic roots in a certain domain and an approximate or exact solution is obtained by continuously bisecting the root interval. In order to interfere with the communication nodes with the least amount of resources, we improve the dichotomy by dividing the root interval with different coefficients.

We set three EVEs in this network. Set the unknown receiving node as $\mathrm{S_r}(x_r, y_r)$, the unknown transmitting node as $\mathrm{S_t}(x_t, y_t)$ and EVE as $\mathrm{E_1}(x_1, y_1)$, $\mathrm{E_2}(x_2, y_2)$ and $\mathrm{E_3}(x_3, y_3)$, respectively. The interference range of EVE can be regarded as a circle with EVE as the center and interference distance

as radius. According to the normal attenuation and distance loss model, the distance loss between EVE and nodes can be expresses as:

$$L_i = L_0 + 10\gamma \lg \frac{R_i}{d_0} + v_i \quad i = 1, 2, 3 \tag{1}$$

where $R_i = \|s - E_i\|$, γ is a path attenuation index, L_0 is the path loss between the reference distance d_0 and node. v_i represents the attenuation variable, which is generally replaced by zero mean Gaussian variable, that is $v_i \sim N(0, \sigma_i^2)$. σ_i^2 is the variance of Gaussian variable. The expression of path loss logarithm L_i is

$$L_i = 10 \lg(P_i/P) \tag{2}$$

where P represents the transmission power of EVE, and P_i represents RSS measurements value of the ith EVE at node. Based on Formula (1) and (2), we can get the relationship between the transmission power and distance of EVE.

The console changes the amount of interference power according to the improved dichotomous method, recording the transmit power P_1 at exactly the moment that causes node S_r to hop. Then the interference circle of EVE has a center of (x_1, y_1) and a radius of R_1. The relationship between R and P can be obtained from Formula (1) and Formula (2). E_1, E_2 and E_3 interfere with the communication nodes in turn and obtain the interference diagram shown in Fig. 2. Due to the fact that the node is fully duplex, the transmitting node can also receive interference signals transmitted by EVE. The distance between transmitting node and EVE can be obtained according to Formula (1) and Formula (2). Therefore, both transmitting node and receiving node can be solved by Formula (1) and Formula (2). After the interference of three EVEs, we can get

$$\begin{cases} (x_1 - x)^2 + (y_1 - y)^2 = R_1^2 \\ (x_2 - x)^2 + (y_2 - y)^2 = R_2^2 \\ (x_3 - x)^2 + (y_3 - y)^2 = R_3^2 \end{cases} \tag{3}$$

By utilizing Formula (3), the coordinates of the transmitting and receiving nodes can be derived. Furthermore, as the communication between nodes is conveyed in distinct time slots allocated by the console, even if multiple transmitters transmit simultaneously to the receiver, the communication of each pair can be computed independently.

Set the real distance from EVE to receiving node as R_{real}, the maximum transmission power of EVE as P_{max}, the maximum transmission distance as R_{max}. The root interval of R_1 is $(0, R_{\max}]$. Since EVE must send interference signals, 0 is an open interval. The dichotomy coefficient is α, and the error is δ. The active interception algorithm is shown in algorithm 1.

We use circle error probable (CEP) to describe the error of interference circle intersection. Three CEPs (that is, r) and three measured values s_{ma}, s_{mb}, s_{mc} are obtained by combining three interference circles in pairs. Take the measured value as the center of circle and r as radius to draw circles (see Fig. 3), which is established in the coordinate system

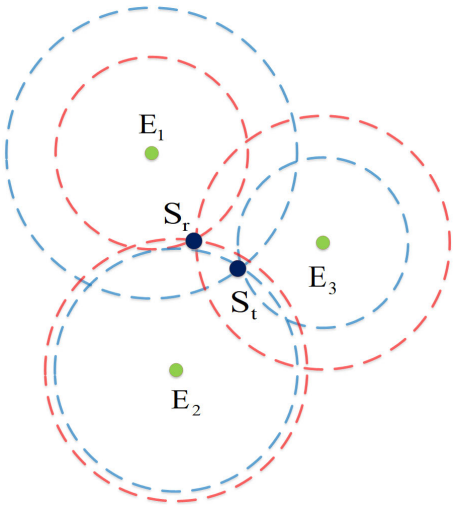


FIGURE 2. Schematic diagram of interference.

Algorithm 1 Interference Strategy of Active Interception

Input: dichotomy coefficient α**, error** δ**,** R_{real}
Initialization: $R_1^{min} = 0.0001$, $R_1^{max} = R_{max}$
Deploy transmitting node, receiving node, and EVE
EVE transmits interference signal
while $R_1^{\max} - R_1^{\min} > \delta$ **do**
    $R_1 = R_1^{\min} + \alpha(R_1^{\max} - R_1^{\min})$
    if $R_1 < R_{real}$ **then**
        set $R_1^{\min} = R_1$
    else
        set $R_1^{\max} = R_1$
    end if
end while
Calculate node coordinate with Formula (3)
Output: (x, y)

with s_{ma} as the origin. Where the distances between s_{ma}, s_{mb} and s_{mc} are d_1, d_2 and d_3, respectively. The area of overlapping part is indicated by shadow, and the vertices are A, B and C, respectively. According to Fig. 3, we can calculate the area of the shaded part S_{shadow}. The error of S_{shadow} is actually very small. For the convenience of illustration, we enlarge it and mark it, so the power consumed by increasing the shadow area can be ignored compared with the interference power.

$$\begin{aligned} S_{shadow} = {} & r_1^2(\theta_B - \theta_A) + x_1 r_1(\sin\theta_B - \sin\theta_A) \\ & - y_1 r_1(\cos\theta_B - \cos\theta_A) \\ & + r_2^2(\theta_C - \theta_B) + x_3 r_2(\sin\theta_C - \sin\theta_A) \\ & - y_3 r_2(\cos\theta_C - \cos\theta_B) \\ & + r_3^2(\theta_A - \theta_C) + x_2 r_3(\sin\theta_A - \sin\theta_C) \\ & - y_2 r_3(\cos\theta_A - \cos\theta_C) \end{aligned} \tag{4}$$

Since the intersection of three circles does not necessarily have intersection points, we can only minimize the error, that is, maximize the overlapping area and get the average value

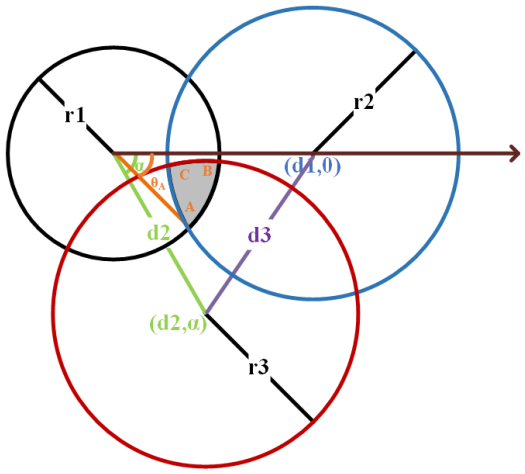


FIGURE 3. CEP schematic diagram.

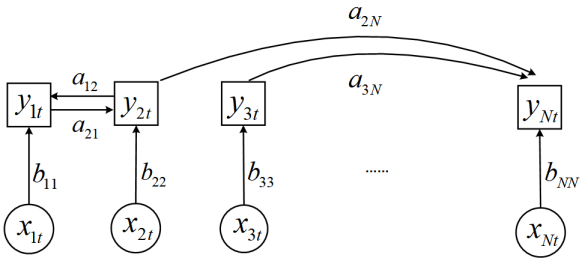


FIGURE 4. An *N*-node directed network with *t*-th samples of endogenous measurements per node.

of CEP: $\bar{r} = (r_1 + r_2 + r_3)/3$.

$$\begin{aligned} &\max_{r_1,r_2,r_3} S_{shadow} \\ &s.t. \quad r_2^2 = r_1^2 + d_1^2 - 2r_1 d_1 \cos\theta_A \\ &\qquad r_3^2 = r_1^2 + d_2^2 - 2r_1 d_2 \cos\theta_B \\ &\qquad r_2^2 = \rho^2 + d_1^2 - 2\rho d_1 \cos\theta_C \\ &\qquad r_3^2 = \rho^2 + d_2^2 - 2\rho d_2 \cos\theta_C \end{aligned} \tag{5}$$

Structural equation model (SEM) is used to identify network topology. Consider a network $\mathcal{G}(\mathcal{V}, \mathcal{E})$ that comprises N nodes, with its topology captured by an unknown adjacency matrix $\mathbf{A} \in \mathbb{R}^{N\times N}$. Let a_{np} denote entry (n, p) of $\mathbf{A}$, which is nonzero only if there is an edge between node n and p. The schematic diagram of SEM is shown in Fig. 4.

Suppose that the network abstracts a complex system with measurable inputs and observable output process. Let x_{nt} denote the input to node n at slot t, and y_{nt} the t-th observation measured at node n. In the network system in this paper, x_{nt} represents the communication node at t, and y_{nt} represents the node location.

In general, SEM assumes that y_{nt} depends on exogenous variables x_{nt} and endogenous variables y_{nt}. Most contemporary SEM approaches posit that y_{nt} depends linearly on both $\{y_{nt}\}_{p\neq n}$ and x_{nt}, during interval t; that is

$$y_{nt} = \sum_{n\neq p} a_{np} y_{pt} + b_{nn} x_{nt} \tag{6}$$

The coefficients $\{a_{np}\}$ and $\{b_{nn}\}$ are unknown, and $a_{np} \neq 0$ signifies that a directed edge from p to n is present. Collecting nodal measurements $\mathbf{y_t} = [y_{1t}, \ldots, y_{Nt}]^\top$, and $\mathbf{x_t} = [x_{1t}, \ldots, x_{Mt}]^\top M \subsetneqq N$ per slot t, (6) can be compactly described as

$$\mathbf{y_t} = \mathbf{A}\mathbf{y_t} + \mathbf{B}\mathbf{x_t} \tag{7}$$

Defining matrices $\mathbf{Y} = (y_1, \ldots, y_N)$ and $\mathbf{X} = (x_1, \ldots, x_N)$, the formula (7) can be concatenated to obtain

$$\mathbf{Y} = \mathbf{A}\mathbf{Y} + \mathbf{B}\mathbf{X} \tag{8}$$

Since it is necessary to update the position of the communication node through the relative product of $\mathbf{B}$ and x_t, the circle probability error affects $\mathbf{B}$, so $\mathbf{B} = \bar{r} \cdot r(t)$ is defined. $r(t)$ needs to be solved by SDE (stochastic differential equation). We choose a continuous-time SDE driven with Brownian motion to describe such randomness.

$$\mathrm{d}\, r(t) = \mu_1 r(t)\, \mathrm{d}\, t + \sigma_1\, \mathrm{d}\, \omega_1(t) \tag{9}$$

where $\omega_1(t)$ is the standard Brownian motion, μ_1 and σ_1 are the system parameters to be determined, take a small time step Δt, and Formula (9) can be described as

$$\Delta r(t) = \mu_1 r(t)\Delta t + \sigma_1(\omega_1(t + \Delta t) - \omega_1(t)) \tag{10}$$

where $\Delta r(t)$ represents the increment of $r(t)$. As SDE is Brownian motion, the increment follows normal distribution, that is, $\omega_1(t + \Delta t) - \omega_1(t) \sim N(0, \Delta t)$. The transfer probability $\mathrm{P}(r(t + \Delta t)|r(t))$ can be calculated. Then the maximum likelihood estimation method is used to estimate the values of μ_1 and σ_1. Suppose that there is a sample sequence set $\{r^0, r^1, \ldots, r^N\}$ of $r(t)$, and the log-likelihood function is

$$\ln(L(\mu_1, \sigma_1)) = \sum_{t=1}^{N} \ln(\mathrm{P}(r^t|r^{t-1}, \mu_1, \sigma_1)) \tag{11}$$

Find μ_1 and σ_1 that maximize $\ln(L(\mu_1, \sigma_1))$ by calculating two partial differentials equal to zero, such as formula (12).

$$\begin{cases} \dfrac{\partial \ln(L(\mu_1, \sigma_1))}{\partial \mu_1} = 0 \\ \dfrac{\partial \ln(L(\mu_1, \sigma_1))}{\partial \sigma_1} = 0 \end{cases} \tag{12}$$

The final result is shown in formula (13).

$$\begin{cases} \mu_1 = \dfrac{\sum_{t=1}^{N} (r^t - r^{t-1}) r^{t-1}}{\sum_{t=1}^{N} r^{t-1}\Delta t} \\ \sigma_1 = \sqrt{\dfrac{\sum_{t=1}^{N} (r^t - r^{t-1} - \mu_1 r^{t-1}\Delta t)^2}{\Delta t}} \end{cases} \tag{13}$$

After calculating $\mathbf{B}$, the adjacency matrix $\mathbf{A}$ is calculated according to

$$\mathbf{A} = \mathbf{I} - \mathbf{B}\mathbf{X}\mathbf{Y}^{-1} \tag{14}$$

C. THE PROPOSED AINL

Since the topology identification accuracy of active interception is not high, we propose a method via active intercepting and node locating to improve accuracy. When the position error of node identification by active intercepting is too large, the node location tactic is called.

Node location tactic is based on a second-order cone convex relaxation strategy and a least-square algorithm to improve the non convexity of maximum likelihood estimation. The maximum likelihood estimation of node position s can be obtained by combining Formula (1) with a non convex least square strategy.

$$\hat{s} = \arg\min_{s} \sum_{i=1}^{3} \frac{1}{\sigma_i^2}[(L_i - L_0) - 10\gamma \lg \frac{R_i}{d_0}] \tag{15}$$

To simplify the algorithm, let $\sigma_i^2 = \sigma$. If noise in wireless network environment is small enough, according to Formula (1) we can obtain

$$\alpha_i R_i \approx d_0 \tag{16}$$

where $\alpha_i = 10^{(L_0 - L_i)/10\gamma}$.

Position information s of a node is estimated based on the least square method, and the least square estimation $\hat{s}_{\min}$ of node position information s can be obtained based on Formula (16).

$$\hat{s}_{\min} = \arg\min_{s} \sum_{i=1}^{3} \frac{1}{\sigma^2}(\alpha_i R_i - d_0)^2 \tag{17}$$

Define auxiliary variable $z = [z_1, z_2, z_3]^T$, where $z_i = a_i R_i - d_0$,we can get

$$\begin{aligned} &\min_{s,R,z} imize \quad \|z\|^2 \\ &s.t. \quad R_i = \|s - E_i\| \\ &\qquad z_i = a_i R_i - d_0, i = 1, 2, 3 \end{aligned} \tag{18}$$

With the help of relaxation variable t, nonconvex constraint is released, $R_i = \|s - E_i\|$ is transformed into $R_i \geq \|s - E_i\|$, and then the mentioned problem is transformed into a second-order cone convex relaxation problem.

$$\begin{aligned} &\min_{s,R,z,t} imize \quad t \\ &s.t. \quad \|[2z; t-1]\| \leq t+1, \|s - E_i\| \leq R_i \\ &\qquad z_i = a_i R_i - d_0, i = 1, 2, 3 \end{aligned} \tag{19}$$

After transformation, the above problem can be accurately calculated with Formula (19) based on the literature [32].

We define X_{real} and X_{calc} to be the true position and the calculated position of a node, respectively. The overall workflow is demonstrated in flow is shown in Algorithm 2.

Algorithm 2 Workflow of the Proposed AINL

Input: the nodes' number N, error δ, communication mode CM, Y, X
for $i = 1{:}N$ **do**
  Calculate $\bar{r}$ with formula (5)
  Calculate $\ln(L(\mu_1, \sigma_1))$ with Formula (13)
  Calculate **A** with Formula (14)
  if $X_{real} - X_{calc} > \delta$ **then**
    Calculate R with Formula (19)
  end if
end for
Output: Identification Topology

III. SIMULATION RESULTS

A. DESIGN SCHEME

This paper provides a novel method called AINL for network topology identification of multiple communication modes by jointly active intercepting and node locating. We conduct elaborate comparisons to demonstrate the effectiveness of our method with classical competing works, including the passive interception (PI) method [33] and node location models [27], [29], [34]. The simulation experiments are performed on Matlab R2021b. Due to the impact on passive interception from different communication modes, we use four communication nodes to implement the simulation. Since the comparative location methods are independent of data packets, we compare AINL in FDMA mode with RSS [29], Time Difference of Arrival (TDOA) [27] and Weight Centroid [34]. These methods are briefly described as follows:

RSS (Received Signal Strength): The Shadowing Model uses the equation $p(d) = p(d_0) - 10n \lg(d/d_0)$, where d represents the distance between the interference node and the communication node, and $p(d)$ represents the signal strength received by the communication node at distance d (also known as the RSS value). Here, $p(d_0)$ represents the signal power received by the receiver at reference distance d_0. The reference distance, typically set as 1, is used as a baseline. The pass loss index is denoted as n. By knowing the RSS value received by the communication node, the distance between communication node and interfering node can be calculated.

TDOA (Time Difference of Arrival): This method involves three interfering nodes simultaneously transmitting wireless electromagnetic signals and ultrasonic signals with different propagation speeds. Using the arrival time difference between the two signals, the communication node utilizes the transmission speed of the signals to calculate the distances between the interfering nodes and the communication node. Subsequently, the least square method is implemented to estimate the position of the communication nodes.

Weight Centroid: For a multi-particle with each particle having a weight (m_i) and position (x_i, y_i, z_i), the centroid of the system can be calculated using the equations: $x_c = (1/N)\sum_{i=1}^{N} m_i \cdot x_i$, $y_c = (1/N)\sum_{i=1}^{N} m_i \cdot y_i$, $z_c = (1/N)\sum_{i=1}^{N} m_i \cdot z_i$. The centroid theorem is applied to the location algorithm. By treating all interfering nodes that have detected the communication node as a multi-particle system, the location of the communication node can be estimated by calculating the centroid using the above

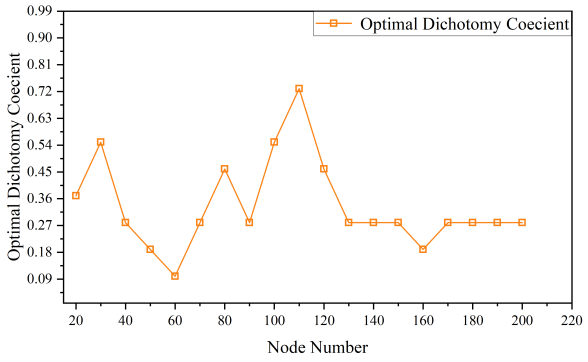


FIGURE 5. Optimal dichotomy coefficient corresponding to different number of communication nodes.

equations. The power of the interfering node varies with a dichotomy, and the dichotomy coefficient impacts the number of iterations when the interfering node interferes with the communication. Therefore, an optimal dichotomy coefficient is defined to enable the interfering node to interfere with the communication node efficiently. Different networks of distinct scales require different optimal dichotomy coefficients. Fig. 5 demonstrates the optimal dichotomy coefficients corresponding to different number of communication nodes, so we set dichotomy coefficient $\alpha = 0.19$ and distance error $\delta = 0.01$ (unit: m).

We can compare the real position with the calculated position to evaluate the quality of the algorithm in the simulation. This paper evaluates the AINL from two aspects: accuracy and power loss. The accuracy of topology identification is

$$Acc = \frac{N_{true}}{N_{all}}$$

where, N_{true} is the number of correct identified elements in the adjacency matrix, and N_{all} is the number of all elements in the adjacency matrix.

It is assumes that the power and consume time of computer iteration are equal when intercepting and locating. If the number of iterations is N, the power required for each iteration is P, and the consume time for each iteration is t, then the power consumption of the wireless network is

$$E = \sum_{i=1}^{N} P_i t_i$$

B. COMPARISON RESULTS

A network is comprised of numerous nodes and links, which establish connections between these nodes, thus representing various objects and interconnectedness. In a network, the quantity of nodes can serve as an indicator of its size. The simulation diagram in the paper employs varying numbers of nodes as abscissas to simulate networks of distinct scales.

Fig. 6 describes the objective accuracy of the passive interception with different communication modes from the comparative methods. We find that the recognition accuracy of AINL is more than 95% in all the communication modes, which is greatly higher than that of passive interception method [33]. The communication mode has a great impact on passive interception, the accuracy rate fluctuates, the impact on AINL is small, and the accuracy rate is stable. AINL persists in deploying the node location algorithm as a dual safeguard and a means to enhance identification accuracy in cases where the topology identification precision of active interception is not optimal. However, passive interception solely operates on data packets, rendering it ineffective in instances where communication encounters abnormalities such as a lack of data packet generation or loss. Consequently, this can lead to significant errors and fluctuations in the passive interception process. Therefore, AINL can be applied to different communication modes and can ensure a high recognition accuracy. In networks of different scales, the recognition accuracy of AINL can reach over 90%, which shows the adaptability of AINL to networks of different scales.

In TDMA mode, the accuracy comparison between the proposed AINL and comparative positioning algorithms is shown in Figure 7. It can be seen from the figure that the accuracy of the node locating positioning strategy is more than 95%, significantly higher than comparative positioning algorithms. When the interference nodes are sparsely distributed, the Weight Centroid method tends to yield significant errors. Moreover, the RSS ranging-based location algorithm necessitates a highly favorable environment and a substantial amount of data. As ultrasonic signals attenuate rapidly and have limited propagation distance, the TDOA method proves more suitable for precise indoor positioning within a confined range. The node location algorithm employed by AINL has been improved by incorporating a second-order cone convex relaxation strategy and the least square algorithm to address the non-convex nature of maximum likelihood estimation. Simulation results demonstrate that this approach effectively enhances recognition accuracy. Comparisons with other location algorithms across network of various scales have revealed AINL's adaptability and high precision. There findings validate the effectiveness of the node locating strategy. Compared with other location algorithms in different scale networks, it can be concluded that AINL has strong adaptability and high accuracy. It shows the effectiveness of node locating strategy.

Fig. 8 depicts the power consumption comparison between proposed AINL and passive interception in different communication modes. Based on the Fig. 8, it can be observed that the power consumption of AINL and passive interception in different communication modes shows the same trend. With the growth of network scale, the growth of power consumption of AINL is relatively gentle, while the growth of passive interception power consumption is relatively rapid. When the network size is small, the power consumption of passive interception is less than that of AINL, but the difference is not significant. When the number of network nodes is about 50, the power consumption of passive interception is greater than that of AINL. Therefore, it can be demonstrated that the network of AINL size is applicable.

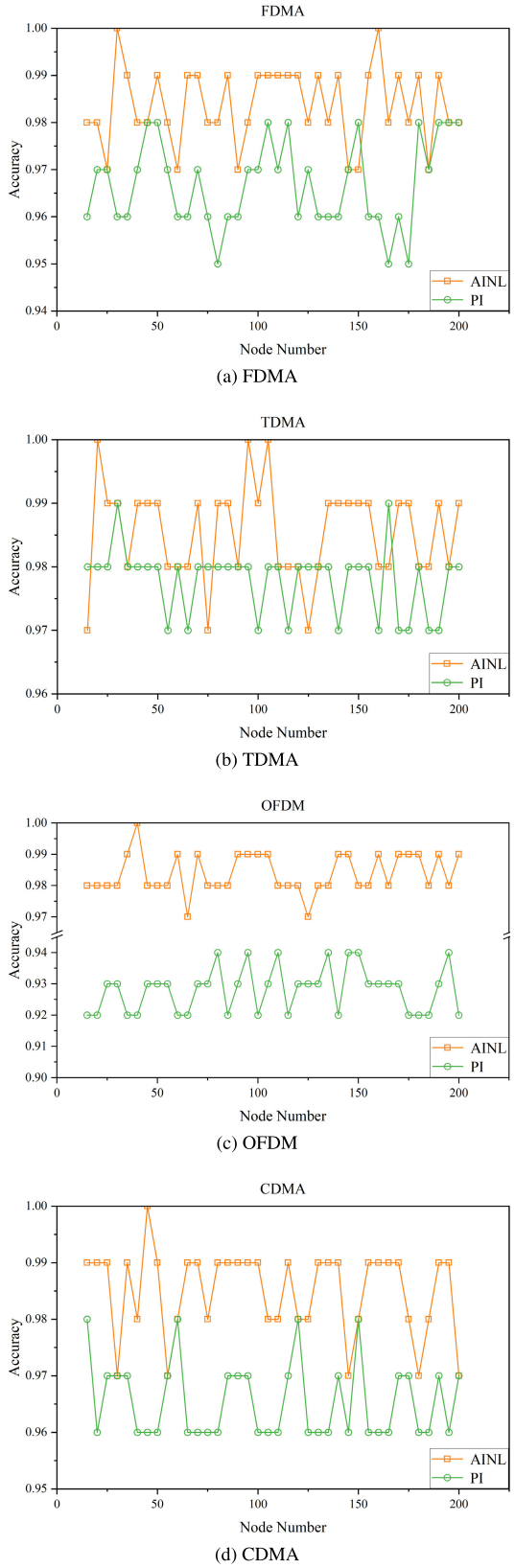


FIGURE 6. Accuracy of AINL and PI under different communication modes.

From the simulation results, we have observed that the power consumption of passive interception is higher than that of active interception. This is because passive interception does not require additional resources, such as interference nodes, and only deals with packet analysis in the network. However, a large number of packets are generated during the communication process, which results in increased power consumption. As the calculation formula for power consumption is the sum of power consumption per iteration, passive interception requires multiple iterations and a longer time to process each packet of communication. On the other hand, active interception does not involve data packet processing but relies on interference nodes to interfere with the communication. Additionally, the paper incorporates a dichotomy strategy for setting the interference power, which greatly reduces the number of iterations. Therefore, the power consumption of active interception is lower than that of passive interception in the simulation results. Furthermore, as the network scale increases and more data packets are present, the difference in power consumption between active and passive interception becomes more pronounced.

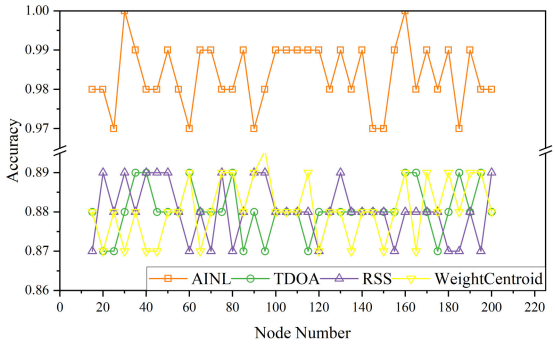


FIGURE 7. Accuracy of AINL and comparative positioning algorithms.

TABLE 1. Comparison of accuracy before and after joint model under different node numbers.

Methods	Accuracy				
	15 nodes	50 nodes	100 nodes	150 nodes	200 nodes
Active Interception	0.93	0.92	0.90	0.92	0.93
Node Location	0.95	0.98	0.96	0.98	0.96
AINL	0.99	0.99	0.98	0.99	0.99

In TDMA mode, the power consumption comparison between AINL and other positioning algorithms is shown in Figure 9. It can be seen from the figure that the power consumption of AINL is similar to comparative positioning algorithms when the network size is small. However, with the increase of the network size, the power consumption of AINL is significantly lower than comparative positioning algorithms. Since RSS, TDOA and Weight Centroid are easily influenced by the environment, it is necessary to collect and process more signal data to ensure the recognition accuracy. In contrast, the localization algorithm based on second-order cone programming relaxation can effectively solve the problem using fewer nodes and fewer computing resources. Additionally, this algorithm can optimize the linear combination and constraints of signals without the need to collect complete signal information from all nodes. Therefore,

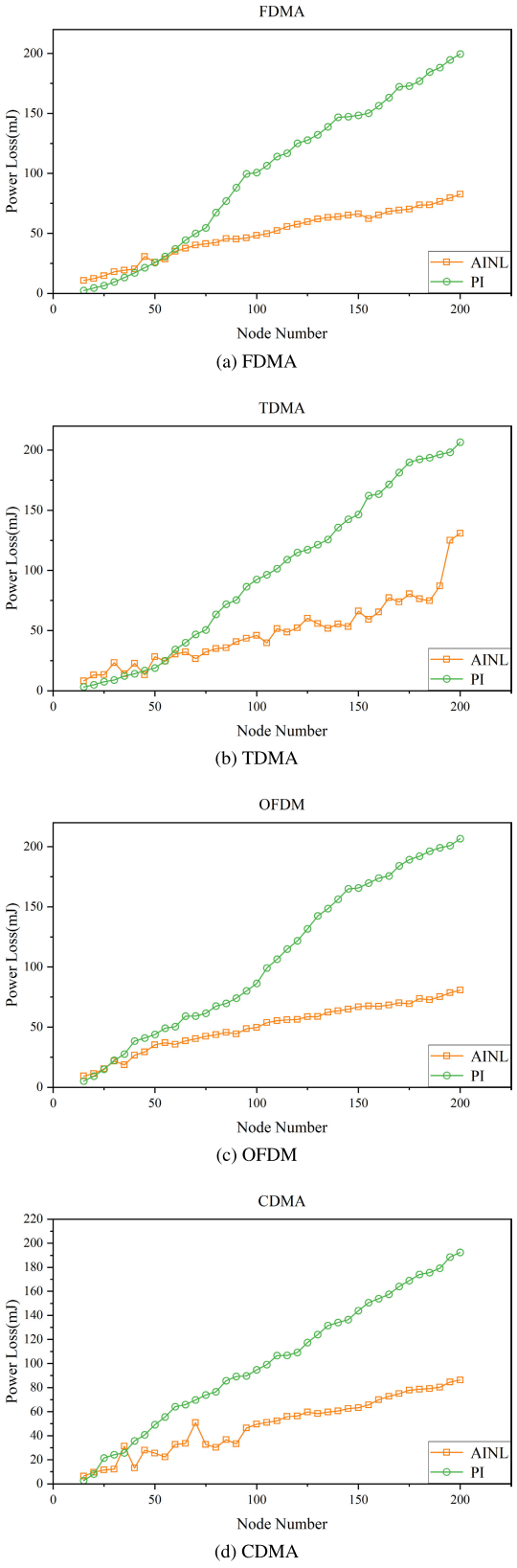


FIGURE 8. Power loss of AINL and PI under different communication modes.

AINL has strong advantages over comparative positioning algorithms.

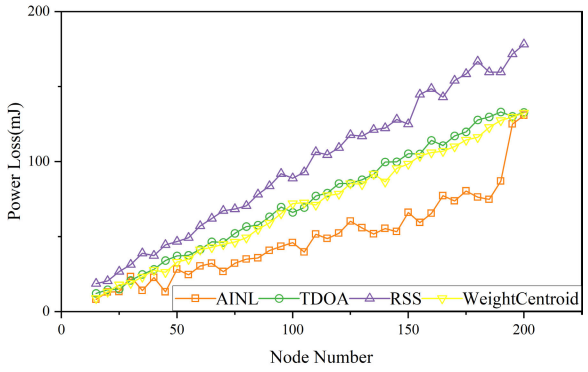


FIGURE 9. Power loss of AINL and comparative positioning algorithms.

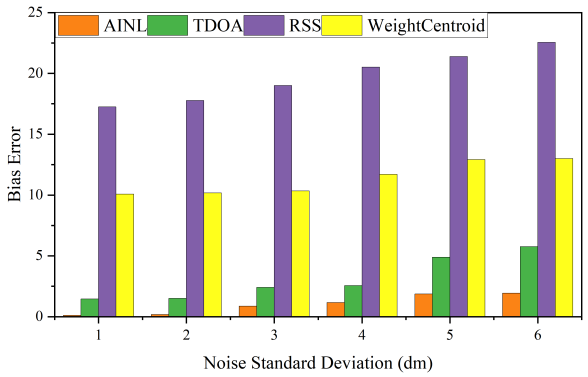


FIGURE 10. Bias error of AINL and comparative positioning algorithms under different noise errors.

Table 1 illustrates a comparison of accuracy between active interception, node location and AINL for different numbers of nodes in TDMA mode. Compared with active interception and node location, the recognition accuracy of AINL has been improved, indicating the feasibility of the joint model.

Figure 10 depicts the bias error of AINL and comparative positioning algorithms under different noise errors. It can be seen that as the noise increases, the bias error of the four algorithms gradually increases, but the bias error of AINL is always the smallest. As the noise level rises, the algorithm relying on second-order cone programming relaxation excels in optimizing a second-order cone programming problem to determine the optimal solution. This algorithm effectively mitigates bias errors by dynamically adjusting constraints and parameters in the presence of noise. In contrast, other location algorithms typically rely on measured data or signal strength for localization. However, as noise increases, measurement results are more susceptible to errors, thereby amplifying offset errors. Consequently, our algorithm yields minimal errors, as demonstrated by experimental results. This demonstrates the strong stability of the AINL algorithm.

IV. CONCLUSION

This paper proposes a method called AINL to achieve topology identification via active intercepting and node locating. The accuracy of network topology identification is more than 95%. Compared with active interception and node location,

AINL improves the accuracy of network topology identification. By comparing with passive interception and node location algorithms, AINL has the advantages of higher identification accuracy, lower power consumption and more stable identification in different communication modes. It can also be applied to large and small scale networks.

However, the network built in this paper does not consider relay routing or forwarding. How to make active interception and passive interception adapt to more complex networks needs further research.

REFERENCES

[1] R. Zhang, Y. Li, and X. Li, "Topology inference with network tomography based on t-test," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 921–924, Jun. 2014.

[2] S. Zhou, L. Cui, C. Fang, and S. Chai, "Research on network topology discovery algorithm for Internet of Things based on multi-protocol," in *Proc. 10th Int. Conf. Modeling, Identificat. Control (ICMIC)*, Jul. 2018, pp. 1–6.

[3] Y. Wei and F. Wu, "Research on network topology model of tactical communication system," in *Proc. IEEE 9th Joint Int. Inf. Technol. Artif. Intell. Conf. (ITAIC)*, vol. 9, Dec. 2020, pp. 808–811.

[4] D. A. Jarvis, "A methodology for analyzing complex military command and control (C2) networks," in *Proc. 10th Int. Command Control Res. Technol. Symp.*, 2005.

[5] Y. Wei, Y. Qing, W. Xiaohui, and Z. Hua, "Dynamic parameters and topological structure identification of complex networks with stochastic perturbations," in *Proc. Chin. Control Conf. (CCC)*, Jul. 2019, pp. 1631–1636.

[6] H. J. van Waarde, P. Tesi, and M. K. Camlibel, "Necessary and sufficient topological conditions for identifiability of dynamical networks," *IEEE Trans. Autom. Control*, vol. 65, no. 11, pp. 4525–4537, Nov. 2020.

[7] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 80–83, Feb. 2016.

[8] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. Conf. Rec. 45th Asilomar Conf. Signals, Syst. Comput. (ASILOMAR)*, Nov. 2011, pp. 265–269.

[9] G. T. Amariucai and S. Wei, "Half-duplex active eavesdropping in fast-fading channels: A block-Markov Wyner secrecy encoding scheme," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4660–4677, Jul. 2012.

[10] N. Ari, N. Thomos, and L. Musavian, "Active eavesdropping in short packet communication: Average secrecy throughput analysis," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2021, pp. 1–6.

[11] F. Viani, F. Robol, E. Giarola, P. Rocca, G. Oliveri, and A. Massa, "Passive imaging strategies for real-time wireless localization of non-cooperative targets in security applications," in *Proc. 9th Eur. Conf. Antennas Propag. (EuCAP)*, Apr. 2015, pp. 1–4.

[12] G. Mateos, S. Segarra, A. G. Marques, and A. Ribeiro, "Connecting the dots: Identifying network structure via graph signal processing," *IEEE Signal Process. Mag.*, vol. 36, no. 3, pp. 16–43, May 2019.

[13] Z. Zhang, Y. Zhao, J. Liu, S. Wang, R. Tao, R. Xin, and J. Zhang, "A general deep learning framework for network reconstruction and dynamics learning," *Appl. Netw. Sci.*, vol. 4, no. 1, pp. 1–17, Dec. 2019.

[14] G. Cimini, R. Mastrandrea, and T. Squartini, "Reconstructing networks," 2020, *arXiv:2012.02677*.

[15] L. Kullmann, J. Kertész, and K. Kaski, "Time-dependent cross-correlations between different stock returns: A directed network of influence," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 66, no. 2, Aug. 2002, Art. no. 026125.

[16] O. Stetter, D. Battaglia, J. Soriano, and T. Geisel, "Model-free reconstruction of excitatory neuronal connectivity from calcium imaging signals," *PLoS Comput. Biol.*, vol. 8, no. 8, Aug. 2012, Art. no. e1002653.

[17] J. Runge, "Inferring causation from time series in Earth system sciences," *Nature Commun.*, vol. 10, no. 1, pp. 1–13, Jun. 2019.

[18] W.-X. Wang, Y.-C. Lai, and C. Grebogi, "Data based identification and prediction of nonlinear and complex dynamical systems," *Phys. Rep.*, vol. 644, pp. 1–76, Jul. 2016.

[19] M. Nitzan, J. Casadiego, and M. Timme, "Revealing physical interaction networks from statistics of collective dynamics," *Sci. Adv.*, vol. 3, no. 2, Feb. 2017, Art. no. e1600396.

[20] P. W. Battaglia, "Relational inductive biases, deep learning, and graph networks," 2018, *arXiv:1806.01261*.

[21] Q. Luo, Y. Peng, J. Li, and X. Peng, "RSSI-based localization through uncertain data mapping for wireless sensor networks," *IEEE Sensors J.*, vol. 16, no. 9, pp. 3155–3162, May 2016.

[22] T. Wang, H. Ding, H. Xiong, and L. Zheng, "A compensated multi-anchors TOF-based localization algorithm for asynchronous wireless sensor networks," *IEEE Access*, vol. 7, pp. 64162–64176, 2019.

[23] T. Wang, H. Xiong, H. Ding, and L. Zheng, "TDOA-based joint synchronization and localization algorithm for asynchronous wireless sensor networks," *IEEE Trans. Commun.*, vol. 68, no. 5, pp. 3107–3124, May 2020.

[24] L. Gui, F. Xiao, Y. Zhou, F. Shu, and T. Val, "Connectivity based DV-hop localization for Internet of Things," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8949–8958, Aug. 2020.

[25] S. Hartung, A. Bochem, A. Zdziarstek, and D. Hogrefe, *Applied Sensor-Assisted Monte Carlo Localization for Mobile Wireless Sensor Networks*. Junction Publishing, 2016.

[26] N. Xie, Y. Chen, Z. Li, and D. O. Wu, "Lightweight secure localization approach in wireless sensor networks," *IEEE Trans. Commun.*, vol. 69, no. 10, pp. 6879–6893, Oct. 2021.

[27] J. Yin, Q. Wan, S. Yang, and K. C. Ho, "A simple and accurate TDOA-AOA localization method using two stations," *IEEE Signal Process. Lett.*, vol. 23, no. 1, pp. 144–148, Jan. 2016.

[28] W. Ding, S. Chang, and J. Li, "A novel weighted localization method in wireless sensor networks based on hybrid RSS/AoA measurements," *IEEE Access*, vol. 9, pp. 150677–150685, 2021.

[29] Y. I. Wu, H. Wang, and X. Zheng, "WSN localization using RSS in three-dimensional space—A geometric method with closed-form solution," *IEEE Sensors J.*, vol. 16, no. 11, pp. 4397–4404, Jun. 2016.

[30] N. H. Mahmood, I. S. Ansari, P. Popovski, P. Mogensen, and K. A. Qaraqe, "Physical-layer security with full-duplex transceivers and multiuser receiver at eve," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4392–4405, Oct. 2017.

[31] G. Li, W. Wang, G. Ding, Q. Wu, and Z. Liu, "Frequency-hopping frequency reconnaissance and prediction for non-cooperative communication network," *China Commun.*, vol. 18, no. 12, pp. 51–64, Dec. 2021.

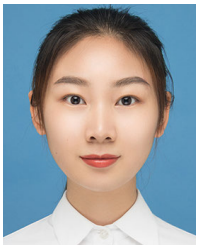
[32] M. Grant and S. Boyd. (2010). *CVX: MATLAB Software for Disciplined Convex Programming*. [Online]. Available: http://cvxr.com/cvx

[33] Z. Liu, W. Wang, G. Ding, Q. Wu, and X. Wang, "Topology sensing of non-collaborative wireless networks with conditional Granger causality," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1501–1515, May 2022.

[34] Q. D. Vo and P. De, "A survey of fingerprint-based outdoor localization," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 491–506, 1st Quart., 2016.

RENHAI FENG (Member, IEEE) received the B.S. and M.S. degrees from the School of Information Science and Technology, Sun Yat-sen University, Guangzhou, China, in 2009 and 2014, respectively.

From 2014 to 2016, he was a Postdoctoral Researcher with the School of Information Engineering, Shenzhen University, Shenzhen, China. He is currently an Associate Professor with the School of Electrical and Information Engineering, Tianjin University, Tianjin, China. His current research interests include visible light communication, convex optimization, and smart grids.



JIAXU CUI (Member, IEEE) received the B.S. degree from the College of Computer and Control Engineering, Northeast Forestry University, Harbin, China, in 2021. She is currently pursuing the M.Eng. degree with the School of Electrical and Information Engineering, Tianjin University, Tianjin, China.

Her current research interests include topology identification, convex optimization, and machine learning.