frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 04 April 2025
DOI 10.3389/fphy.2025.1584958

OPEN ACCESS

EDITED BY
Dun Han,
Jiangsu University, China

REVIEWED BY
Jianrong Wang,
Shanxi University, China
Jingjing Yao,
Jiangsu University, China

*CORRESPONDENCE
Rongcheng Dong,
dongrch1995@outlook.com

RECEIVED 28 February 2025
ACCEPTED 20 March 2025
PUBLISHED 04 April 2025

CITATION
Huang J, Dong R, Niu Z, Peng C and Chen J (2025) Non-cooperative inference method for the IoBT topology based on flow rate estimation.
Front. Phys. 13:1584958.
doi: 10.3389/fphy.2025.1584958

Non-cooperative inference method for the IoBT topology based on flow rate estimation

Jun Huang, Rongcheng Dong*, Zhao Niu, Chao Peng and Jie Chen

College of Electronic Engineering, National University of Defense Technology, Hefei, China

The widespread integration of Internet of Things (IoT) technology in the military domain has brought significant attention to the security concerns surrounding the Internet of Battlefield Things (IoBT). Given the limited communication resources within IoBT, there is a growing focus on detecting network security without interrupting normal network operations. Topology serves as a crucial foundation for the detection of network security in IoBT, facilitating the discovery of abnormal devices and the detection of unauthorized access. Security detection based on topology can effectively enhance the information security and operational levels of IoBT. This paper utilizes matching analysis of time series for information exchanged between neighboring nodes and implements IoBT topology inference based on flow rate estimation, and a threshold parameter adaptive adjustment strategy is innovatively proposed to improve the accuracy of topology inference. The non-cooperative inference method proposed in this paper enables network topology inference without network access and information parsing, exhibiting strong generality and independence from the discovery of acknowledgment frames during information exchange processes. The simulation results demonstrate the feasibility and superiority of this method.

KEYWORDS

internet of battlefield things (IoBT), non-cooperative, topology inference, flow rate estimation, network security

1 Introduction

With the continuous evolution of military technology, the demands placed on information transmission efficiency and security during battlefield operations have escalated Wen et al. [1]. Traditional military systems encounter several limitations, including high costs, extended deployment times, constrained communication resources, and low information transmission efficacy Conradie [2]. In order to effectively improve the efficiency of battlefield communication, the construction of a distributed battlefield network has become the development direction for military communication networks worldwide Chen et al. [3]. Compared to traditional military systems, large-scale distributed networks composed of various military systems can achieve faster, cheaper, and more flexible battlefield deployment and information transmission. As a crucial component of the distributed battlefield network, IoBT is receiving increasing attention globally Abuzainab and Saad [4]. IoBT connects various combat elements through information sensing, linking them to the military information network. This integration bridges the gap between the

network domain and the physical domain, providing new perspectives for constructing a novel military communication network system Akter et al. [5]. Within the IoBT framework, real-time perception and rapid response to the status information and dynamics of weapon systems, combat units, and battlefield environments are facilitated through network communication. Despite the introduction of security measures, IoBT remains challenging to effectively counter attacks such as man-in-the-middle attacks, communication node impersonation, and information tampering Li et al. [6]. When impersonating nodes gain access to the network, the attackers can launch denial-of-service attacks by sending a large volume of useless information, leading to network congestion Islam et al. [7]. Additionally, they can disrupt normal information transmission by forging information, affecting the regular operations of military forces, such as altering commands or fabricating false situational information Rutravigneshwaran et al. [8]. To detect hidden abnormal nodes in the network and enhance the security performance of IoBT, topology discovery proves to be an effective means. Topology inference methods can be broadly classified into cooperative and non-cooperative categories, depending on network accessibility assumptions. Cooperative methods rely on network accessibility and parseable messages as their fundamental premise. They are further divided into methods based on protocol analysis Yan [9]; Yong et al. [10] and methods based on network tomography Chen et al. [11]; Zhang and Phillips [12]; Jin et al. [13]. Some methods necessitate the transmission of numerous probing packets to finalize the inference, rendering them impractical for scenarios with restricted information acquisition and inaccessible networks. Moreover, the traffic generated by the detection devices upon access can escalate the network load, exacerbating the strain, especially in environments with limited communication resources. Consequently, this can impede the efficiency of information transmission within the network. Currently, research on non-cooperative topology inference methods is relatively scarce. Relevant research outcomes mainly focus on inferring network topology based on the correlation between data frames and acknowledgment frames Niu et al. [14]. Common methods include granger causality Tilghman and Rosenbluth [15], transfer entropy Sharma et al. [16], clusteringLiu et al. [17], neural network Testi and Giorgetti [18] etc. The aforementioned methods strictly rely on the confirmation information sent from the receiving node to the sending node after data frames are transmitted. In cases where the protocol lacks a confirmation mechanism, these methods cannot infer the communication relationships between nodes. Additionally, due to the typically short length of acknowledgment frames, there is a risk of undetectable situations during the monitoring process, increasing the probability of false negatives and false positives to some extent.

To address the shortcomings of the aforementioned methods, this paper proposes a non-cooperative topology inference method based on flow rate estimation. In this method, for the monitored communication signals, the transmission times of information from different nodes are extracted. Subsequently, the close correlation between the relay nodes and the sending nodes in terms of flow rates is utilized to determine the communication relationships. In order to improve the accuracy of communication relationship inference, a threshold parameter adaptive method is also proposed. Finally, the results of communication relationship determination are integrated to achieve the inference of network topology.

The remaining sections of the paper are organized as follows. In Section 2, the related models adopted are presented. In Section 3, the non-cooperative topology inference method based on flow rate estimation is presented in detail. In Section 4, the simulation experiments and results are shown, followed by conclusions in Section 5.

2 Related model

The schematic diagram of the topology inference scenario is shown in Figure 1. The green objects represent IoBT communication equipments. Security detection devices are deployed in proximity to each IoBT communication equipment, enabling them to monitor signals within the deployment area effectively. The red line represents that two communication equipments are close enough to send signals to each other. While detection devices can detect the location information and capture all communication signals in the area, they lack the capability to parse the content of transmitted information. Therefore, the challenge at hand is: How can we infer the network topology of IoBT without directly accessing the network or parsing the transmitted information?

2.1 Network model

The topology diagram of the IoBT in Figure 1 is shown in Figure 2. In Figure 2, $G = (V, E)$ is used to represent the network topology of IoBT, where V represents the set of nodes, with each node representing a communication device, and E represents the set of edges, with each edge representing a link. Each node is capable of receiving, storing, and sending information with its communication range. When nodes are within each other's communication range, a physical link capable of information transmission exists between the two nodes. However, the existence of communication relationships between nodes is only determined when information transmission occurs between the nodes. We assume a static network, which means that the topology of the network does not change when executing algorithms.

The topology inference results are represented using an adjacency matrix $\mathbf{A} = [a_{ij}] \in \mathbb{R}^{n \times n}$, where $a_{ij} = 1$ indicates that there is a communication relationship between the ith communication device and the jth communication device during the monitoring period, while $a_{ij} = 0$ indicates that there is no communication relationship between the ith and jth communication devices during the monitoring period.

Due to the impact of communication device transmission power and environmental attenuation, each communication device in IoBT has limitations on its communication range Ganesh and Venkataraman [19]. To ensure effective information transmission, communication networks often employ multi-hop methods to achieve long-distance information transmission Singh and Shrivastava [20]. In IoBT, devices can act as both sending nodes and receiving nodes, and they can also serve as relay nodes to forward information. When the sending node (source node)

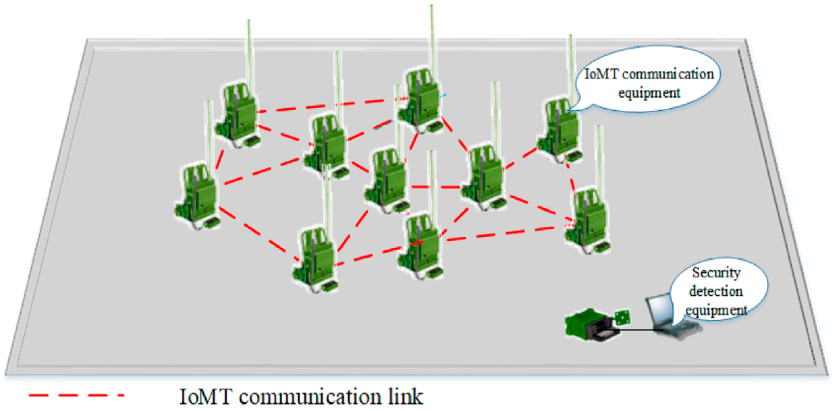

FIGURE 1
The schematic diagram of the topology inference scenario.

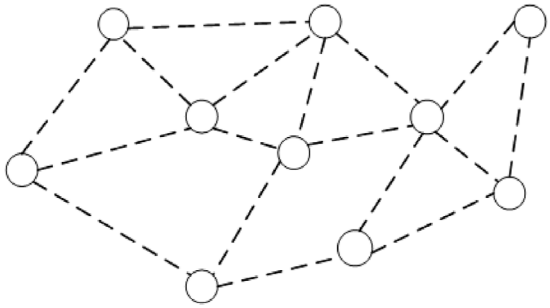

FIGURE 2
Network topology diagram.

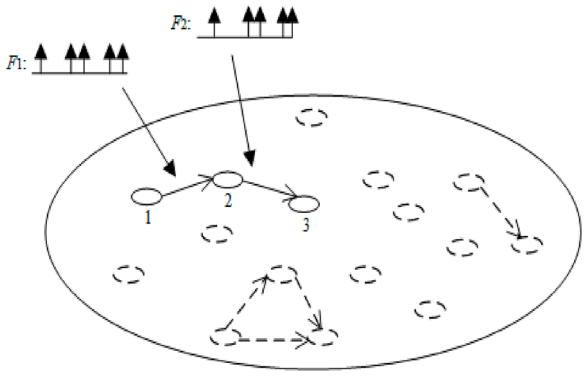

FIGURE 3
Schematic diagram of a single information flow passing through adjacent nodes.

and the receiving node (destination node) cannot be reached in a single hop, multiple data packets will be successively relayed among intermediate nodes Chai et al. [21]. The term "information flow" refers to the flow created by the relayed data packets between intermediate nodes.

2.2 Information flow model

Assuming that only one information flow passes between two adjacent nodes within a certain period, as shown in Figure 3. From Figure 3, it can be observed that the sending moments of network node data are represented as points on the real axis, described using a one-dimensional point process $F = \{F_1, F_2, \ldots, F_i, \ldots, F_n\}, 1 \le i \le n$. The sending time sequences of data between node 1 and node 2 are denoted as F_1 and F_2, where $F_1 = \{f_1(1), f_1(2), \ldots, f_1(k), \ldots, f_1(L_1)\}, 1 \le k \le L_1$, L_1 is denoted as the number of time points in F_1. For every time point in F_1, if there exists a time point in F_2 corresponding to it, such that the time difference between the two time points is less than a certain threshold, then an information flow is formed from F_1 to F_2.

Examining the forwarding process of an individual data packet within the information flow as the subject of observation, the reliable transmission of the same packet along adjacent links in the information flow path is subject to a delay, referred to here as the packet single-hop forwarding delay t_s. This delay mainly consists of two parts. First, the MAC delay, including the transmission delay t_t, and the wait-to-access medium delay t_w, where t_t is the time for data transmission when accessing the medium, which is necessary, and t_w is caused by access conflicts, determined by conflict resolution solutions Roy et al. [22]. The estimation of the wait-to-access medium delay needs to be based on a specific understanding of the content of conflict resolution solutions. Second, the queuing delay t_q of the packet in the node buffer. If the network node adopts a FIFO (First-In-First-Out) queuing mechanism, the queuing delay of the n-th packet in the queue is the sum of the single-hop forwarding delays of the preceding $(n-1)$ packets. The formula for calculating the single-hop forwarding delay of a packet is given in Equation 1:

$$t_s = t_t + t_w + t_q \tag{1}$$

where t_t is relatively small, t_s is mainly determined by the sizes of t_w and t_q. Under general circumstances, there is a maximum value for both t_w and t_q in the wireless network's packet transmission. Therefore, t_s also has a maximum value Δ_m. However, in practical networks, there is more than one information flow forwarded by a wireless node. Assume S_i represents the transmission time of

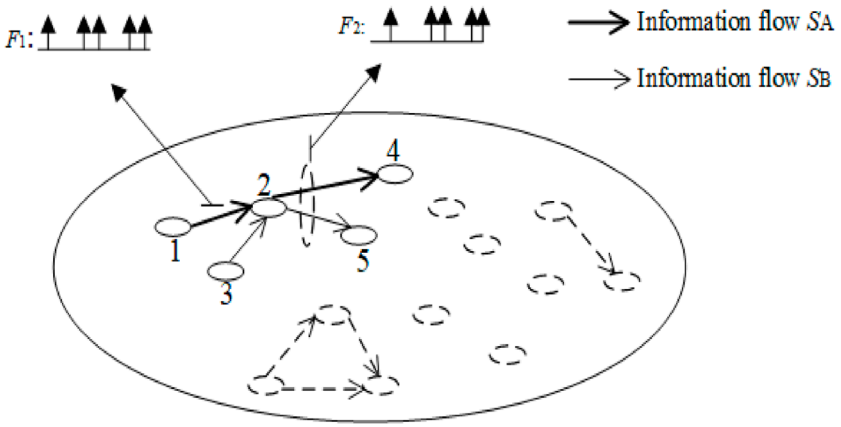

FIGURE 4
Schematic diagram of a node forwarding two information flows.

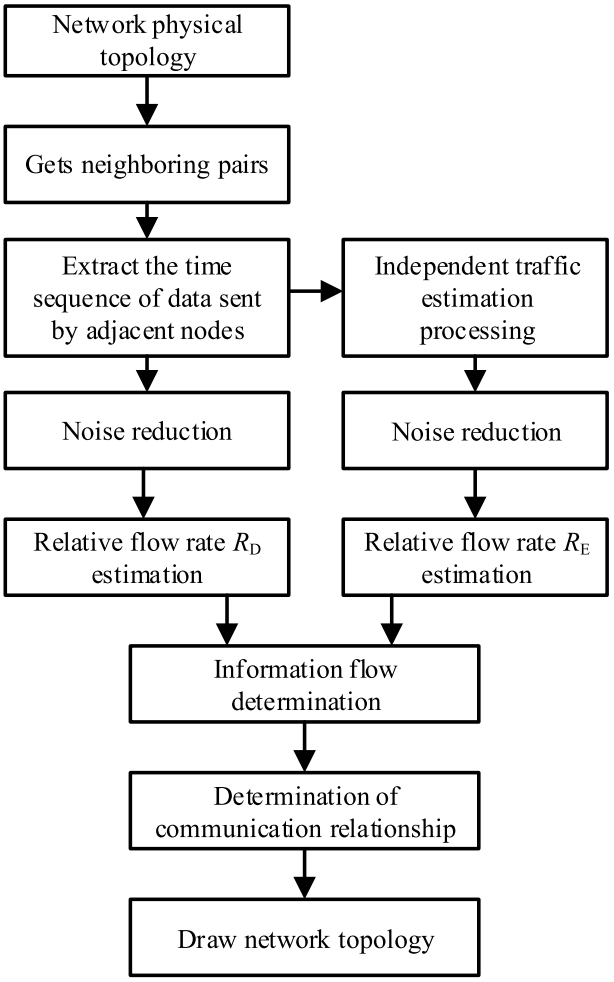

FIGURE 5
Non-cooperative topology inference process flowchart based on flow rate estimation.

data from the ith node, F_i represents the time when a particular information flow passes through the ith node, and W_i represents the times when other information flows pass through the ith node. The relationship among them can be expressed as Equation 2:

$$S_i = F_i \oplus W_i \tag{2}$$

where $\oplus$ means: for the three sequency $(a_1, a_2, \cdots)$, $(b_1, b_2, \ldots)$, and $(c_1, c_2, \ldots)$, if $(a_k)_{k=1}^{\infty} \oplus (b_k)_{k=1}^{\infty} = (c_k)_{k=1}^{\infty}$, when and only when $\{a_k\}_{k=1}^{\infty} \cup \{b_k\}_{k=1}^{\infty} = \{c_k\}_{k=1}^{\infty}$, where $a_1 < a_2 < \ldots, b_1 < b_2 < \ldots, c_1 < c_2 < \ldots$.

Figure 4 illustrates a scenario where the same node forwards two information flows. It can be observed that when utilizing the sending time sequences F_1 and F_2 of data from nodes 1 and 2 to detect the information flow S_A transmitted from node 1 and forwarded by node 2, the sending time sequence of information flow S_B sent by node 3 and forwarded by node 2 are also mixed in F_2. For the detection analysis of the information flow from node 1 to node 2, the sending time sequence of information flow from node 3 to node 2 is considered useless time records. Additionally, information flows initiated directly by node 2, apart from those forwarded by node 2, will also generate useless time records for the detection analysis of information flow S_A.

3 Non-cooperative topology inference based on flow rate estimation

The process of topology inference of the IoBT is depicted in Figure 5. It involves analyzing and inferring the network topology based on the timestamp sequence of packet data transmission during the node's sending process. If it can be determined that there is information forwarding between some nodes in the network, especially between two adjacent wireless nodes, and directional information flow is detected between them,

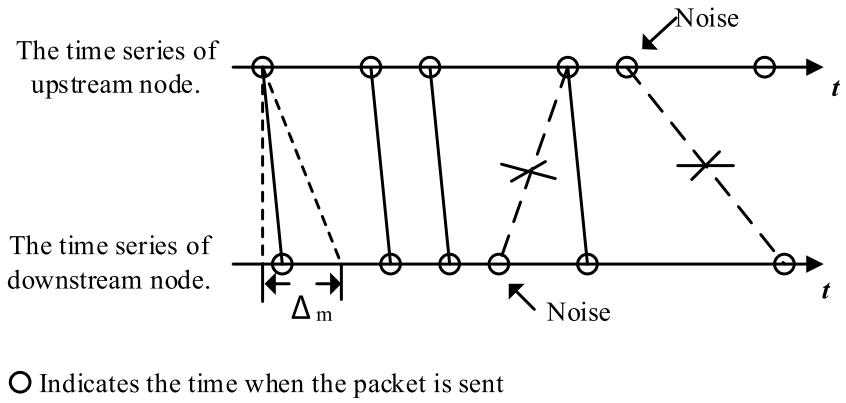

FIGURE 6
Noise reduction process diagram using the matching method for adjacent node data transmission times.

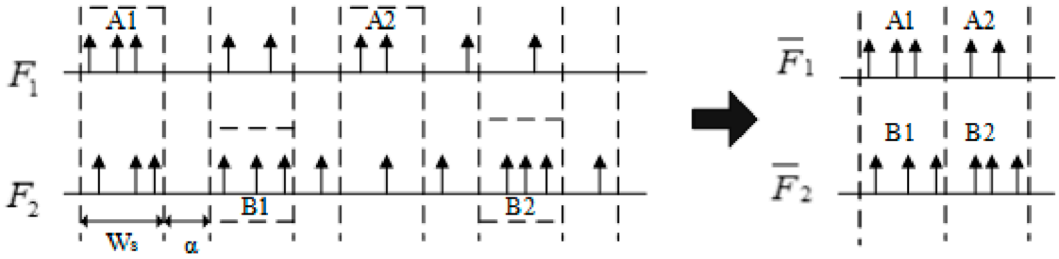

FIGURE 7
Denoising process diagram using ITA for adjacent node data transmission time sequence.

then these two wireless nodes and the corresponding directional edges can be considered as part of the entire network topology. Through prolonged accumulation and observation, the complete topology of the network can be inferred. This method does not rely on parsing the content of packet data, making it highly suitable for topology inference in IoBT.

Based on obtaining the physical topology of the IoBT and identifying pairs of adjacent nodes in the target network, the sending time sequence of data from adjacent nodes is extracted. By comparing the length differences between data frames and link control frames, the frames containing data are identified and arranged in chronological order on the time axis. Subsequently, the denoising method is applied to remove data that does not meet the criteria. The relative flow rate R_D is calculated based on the remaining data. Independent flow rate estimation is performed on the extracted data from adjacent nodes, followed by denoising and calculation of the relative flow rate of independent flows (R_E). If $R_D \geq R_E$, it is determined that there is an information transmission link between the two nodes; otherwise, it is considered that there is no information transmission link between the two nodes during the monitoring period. Finally, the determination results of communication relationships between different adjacent nodes are aggregated to draw the topology of the IoBT.

3.1 Noise reduction processing

Utilizing the characteristic that the single-hop forwarding delay of packets has a maximum value, matching is conducted between the time sequences of data transmission from adjacent nodes. Data transmission times within a certain time range difference are grouped as the same packet data, while unmatched data is deemed noise and promptly removed. The objective of denoising is to identify potential packet data for the information flow.

Addressing the two types of useless time records mixed in the information flow, one caused by the relay node forwarding other information flows and those caused by the relay node itself sending information flows, the maximum delay Δ_m requirements during the packet forwarding process can be used. This involves cross-referencing and locating packet data of the same information flow on adjacent links. Figure 6 illustrates the concept of using the interval time between data packet transmissions from adjacent nodes to match the transmitted data packets from neighboring nodes.

From the diagram, it can be seen that when the time difference between the downstream node's packet transmission time and the upstream node's packet transmission time is less than Δ_m, it is preliminarily considered that the packets sent by the two adjacent nodes belong to the same information flow; otherwise, the packets do not belong to the same information flow. In the matching process,

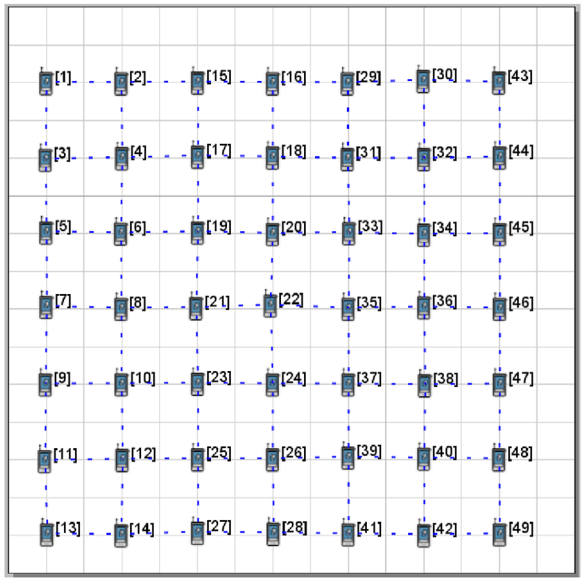

FIGURE 8
The scenario diagram.

TABLE 1 Parameter settings in the EXata simulation environment.

Parameter	Value
Simulation Area	1.5 km*1.5 km
Simulation Time	300s
Nodes Number	49
Location Distribution	grid
Interval Distance	200 m
Communication Distance	250 m
Physical Protocol	802.11
MAC Protocol	TDMA or CSMA
Routing Protocol	Bellmanford
Business Type	CBR

a greedy algorithm approach is applied, attempting to match the packets from adjacent upstream nodes with those from adjacent downstream nodes that have not yet been paired. The remaining unmatched packets are then classified as noise data.

3.2 Parameter adaptive adjustment

From the above subsection, we can see that Δ_m directly affects the processing of noisy data, which in turn affects the accuracy of topological inference results. If Δ_m is set too large, it will cause misjudgment; If Δ_m is set too small, it will increase the probability of missed judgment. Therefore, this paper proposes a parameter adaptive adjustment method based on monitored data. Set node identification accuracy rate P_N as a measurement indicator, and through continuously increasing the value of Δ_m, filter the value of Δ_m when P_N reaches a stable state for subsequent topology inference. The formula for calculating P_N is shown as Equation 3:

$$P_N = \frac{|N_u|}{|N_a|} \times 100\% \tag{3}$$

where N_a is the set of nodes that send data during the monitoring time of the network, N_u is the set of upstream nodes identified in the network. In order to accelerate the speed of filtering the value of Δ_m, divide the process into two stages: coarse-grained setting and fine-grained adjustment. In the coarse-grained setting phase, set $\Delta_m = \Delta_1$, where Δ_1 is the initial value, and if the inference result is inaccurate, set $\Delta_m = 2 \times \Delta_1$, i.e., the current is doubled until the value of P_N reaches a stable state. In the fine-grained adjustment stage, it is assumed that the inference is correct when $\Delta_m = \Delta_k$, then the optimal value is found between Δ_k and Δ_{k-1}. During the optimization process, set $\Delta_m = \Delta_k + t'$, where t' is the step size, and gradually increase the value until the value of P_N reaches a stable state.

3.3 Relative flow rate estimation

Count the possible number of information flow packets, calculate the proportion of these packets among the total number of data transmissions from adjacent nodes, and obtain the magnitude of the relative flow rate value R_D. In information flow detection based on the transmission time of data packets, useless time records are analogous to noise in signal detection. Referring to the definition of signal-to-noise ratio in communication signal detection, the relative flow rate $R_f(t)$ is defined as the ratio of the number of information flow data samples to the total number of data samples transmitted by the node. The formula for calculating $R_f(t)$ is shown as

$$R_f(t)\,\Delta = \frac{\sum_{i=1}^{2} |f_i \cap [0,t]|}{\sum_{i=1}^{2} |s_i \cap [0,t]|} \tag{4}$$

where f_i represents the data transmission time of the information flow forwarded by the ith node, and S_i represents the overall data transmission time of the ith node. From Equation 4, it can be observed that $R_f(t)$ changes with time.

3.4 Independent flow rate estimation processing

The adjacent node data sending time sequences are subjected to sampling processing to generate a new time sequence reflecting the independent flow components between adjacent node pairs. Subsequently, denoising and relative flow rate estimation are applied to the new time sequence to obtain the value of the relative flow rate under the condition of mutually independent time sequences of adjacent nodes, which is denoted as R_E. Independent Traffic Approximation (ITA) is a heuristic algorithm that estimates independent traffic between node pairs by sampling data from the

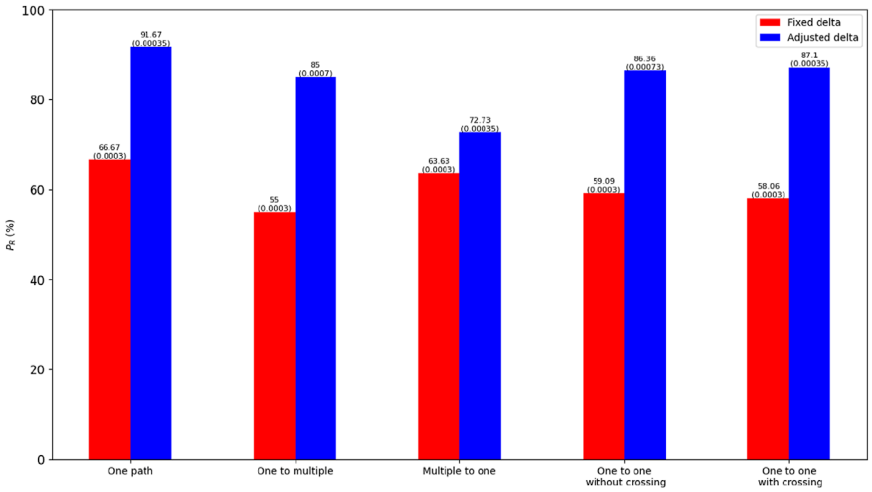

FIGURE 9
Bar chart of scene and accuracy relation with fixed delta.

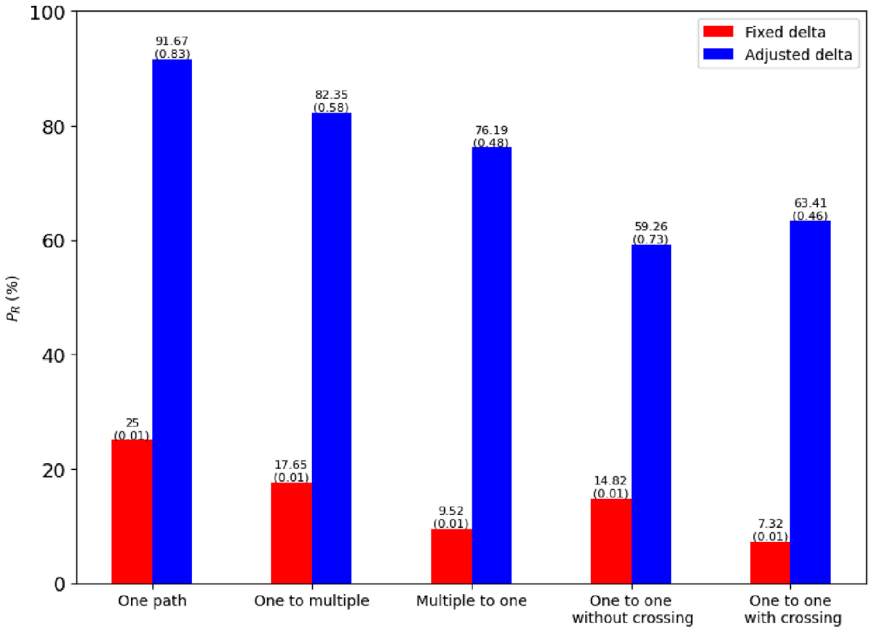

FIGURE 10
Bar chart of scene and accuracy relation with adaptive value.

node data transmission process. ITA has two parameters: one is the synchronous window size W_s, and the other is the interval between adjacent synchronous windows α. Figure 7 provides a schematic diagram of the processing of node data transmission points using the ITA method. ITA relies on the heuristic knowledge that if W_s is sufficiently large, the data transmission times of F_1 in window A_1 and F_2 in window B_1 tend to be uncorrelated, even under the condition of the existence of information flow. Then, by performing maximum matching on $\overline{F}_1$ and $\overline{F}_2$ obtained using the ITA method, the threshold value for the relative flow rate is calculated.

3.5 Determination of association relationships

Comparing R_D and R_E, if R_D is within a certain range and greater than R_E, it indicates that there is no information flow forwarding relationship between adjacent nodes. Conversely, if R_D is smaller than R_E, it suggests the presence of an information flow forwarding relationship between adjacent nodes. To assess the performance of the information flow detection algorithm, the metrics of node pairs identification accuracy rate P_R and node pairs identification false rate P_F are utilized. Assuming the set node pairs with upstream

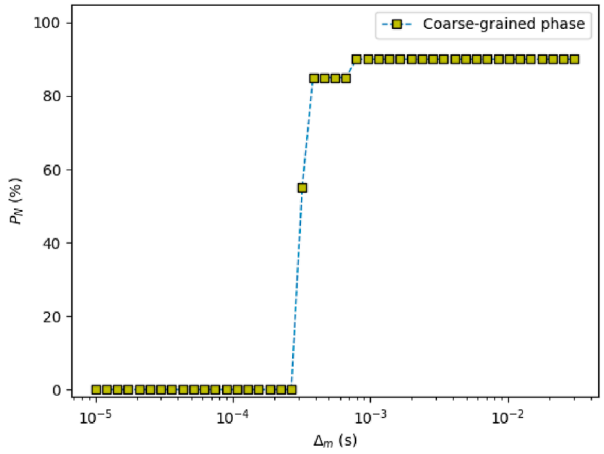

FIGURE 11
The diagram of the coarse-grained setting stage.

and downstream relationships actually exist in the network during the monitoring time is denoted as N_R, the set of node pairs with upstream and downstream relationships identified by the algorithm is denoted as N_I, the equations for calculating P_R and P_F are shown as Equations 5, 6:

$$P_R = \frac{|N_I \cap N_R|}{N_R} \times 100\% \tag{5}$$

$$P_F = \frac{|N_I - N_I \cap N_R|}{N_R} \times 100\% \tag{6}$$

Drawing the network topology based on the identified information flow transmission paths. In the topology inference process, a confirmation method based on "topological convergence" is employed. Specifically, after continuous processing of a substantial amount of link transmission activities over an extended period, if the network topology inference results no longer change, it is considered as the end of identification. The stabilized topology inference result is then considered as the final identification result. Considering the analysis of the aforementioned inference process, the pseudocode for the non-cooperative inference of IoBT topology based on flow rate estimation is presented as Algorithm 1. By lines 4, 6 and 18 in Algorithm 1, we have the run time complexity of the algorithm $\max\{O(n^2), \text{len}(F)\}$, where n is the size of the network, and F is the total sending time sequence of all nodes of the network.

4 Simulation analysis

To validate the feasibility of the method, a simulation environment was built using simulation software. Currently, mainstream simulators include NS-2, NS-3, GloMoSim, OPNET, QualNet, EXata, etc Walia et al. [23]. In comparison to other simulators, both EXata and QualNet are developed based on GloMoSim, utilizing an efficient parallel simulation kernel. EXata and QualNet indeed showcase remarkable advantages in simulation speed, scalability, and model fidelity, making them prime choices for simulating large-scale wireless networks. Given these advantages of EXata, it was used in this paper's research to construct experimental scenarios and conduct relevant experiments.

4.1 Scene setup

In EXata, communication nodes were deployed to construct the network based on the grid model, the scenario diagram is shown in Figure 8, and relevant simulation parameters are listed in Table 1. From the diagram, it can be observed that the simulated network consists of 49 nodes positioned in a fixed manner arranged in a grid. Additionally, for simplification purposes, while maintaining the relative relationship between the network coverage area and node communication distance, the communication distance of the communication nodes and the coverage area of the network were uniformly reduced in the simulated network. The communication distance for communication nodes was set to 250 m, and the simulation area was set to 1.5km^2. The transmitted information by the communication node is generated by a constant bit rate (CBR) traffic generator in EXata.

4.2 Parameter adaptive adjustment

In order to show the necessity of Δ_m adaptive adjustment, experiments are carried out, Δ_m was set fixed value and adaptive value in different scenarios, and the accuracy rate of the algorithm was compared. The experimental results are shown in Figures 9, 10.

In Figures 9, 10, the abscissa represents the different scenarios under the CSMA and TDMA protocols, from left to right: one path mode, one-to-multiple mode, multiple-to-one mode, one-to-one without crossing mode and one-to-one with crossing mode. As can be seen from Figure 9, CSMA was used and Δ_m was set to 0.0003s, the number outside the parentheses above each bar is the accuracy, and the number in the parentheses is the value of Δ_m in the current scenario. It can be seen that when Δ_m is set to 0.0003s, the highest accuracy of the algorithm is 66.67% (one path mode), while the lowest is only 55% (multiple-to-one mode). Even under the same protocol, the accuracy of the algorithm in different scenarios is quite different. In Figure 10, TDMA was used and Δ_m was set 0.01s. In one-to-one with crossing mode, when Δ_m is fixed, the accuracy of the algorithm is only 7.32%, while the accuracy of using the adaptive adjustment reaches 63.41%. Therefore, using a fixed Δ_m value cannot be adapted to different scenarios, and it is necessary to select the appropriate values of Δ_m in combination with the scenario during the operation of the algorithm. To verify the feasibility of using the parameter adaptive adjusting method, experiments were conducted in a scenario where multiple-to-one mode was used in the network.

During the coarse-grained setting phase, Δ_m grows exponentially. It can be seen from Figure 11 that after the Δ_m is about greater than 0.0001 s, the algorithm can make node identification accuracy rate P_N stably, so we can get the appropriate range of Δ_m for fine-grained adjustment stage, which is 0.0001s–0.001 s. The reason why P_N is 0 when Δ_m is small is that, packet transmission

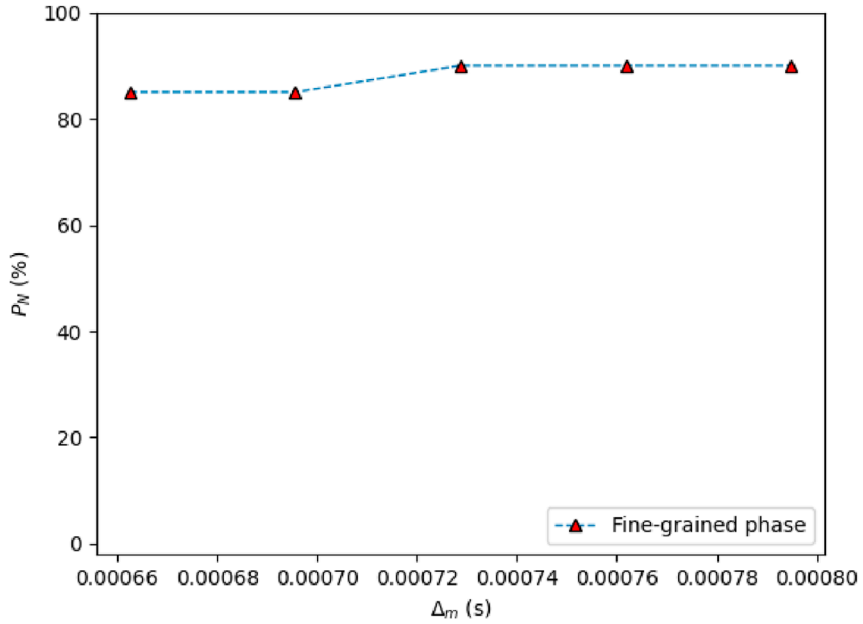

FIGURE 12
The diagram of the fine-grained adjustment stage.

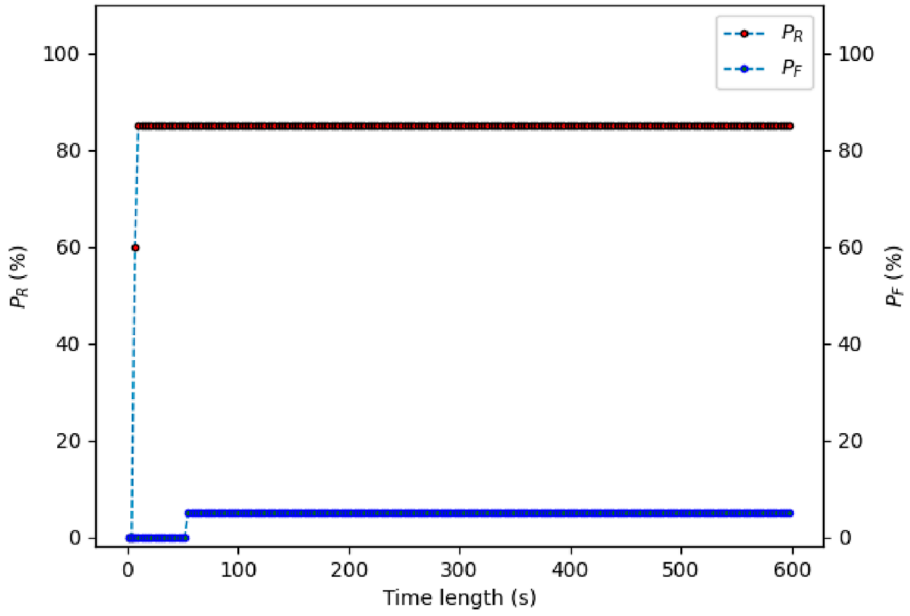

FIGURE 13
The influence of monitoring duration on inference accuracy and false rate.

between two adjacent nodes needs time. When Δ_m is too small, the algorithm will exclude any packet transmission, thus the accuracy is 0.

In the fine-grained adjustment phase, Δ_m grows linearly, in this experiment, the Δ_m grows by $\frac{1}{20}$ of the Δ_1 at the beginning of each fine setting phase. It can be seen from Figure 12 that the value of P_N is highest when the Δ_m is around 0.00073 s. Therefore, we can obtain the optimal Δ_m value for this experimental configuration. Set Δ_m = 0.00073 s, then we study the influence of monitoring duration and loss rate on inference accuracy and false rate.

As can be seen from Figure 13, the algorithm cannot make effective inferences when the detection duration is less than 30*s*, and when the detection duration is more than 36*s*, the algorithm can make inferences. It is because before 30*s*, the algorithm does not have

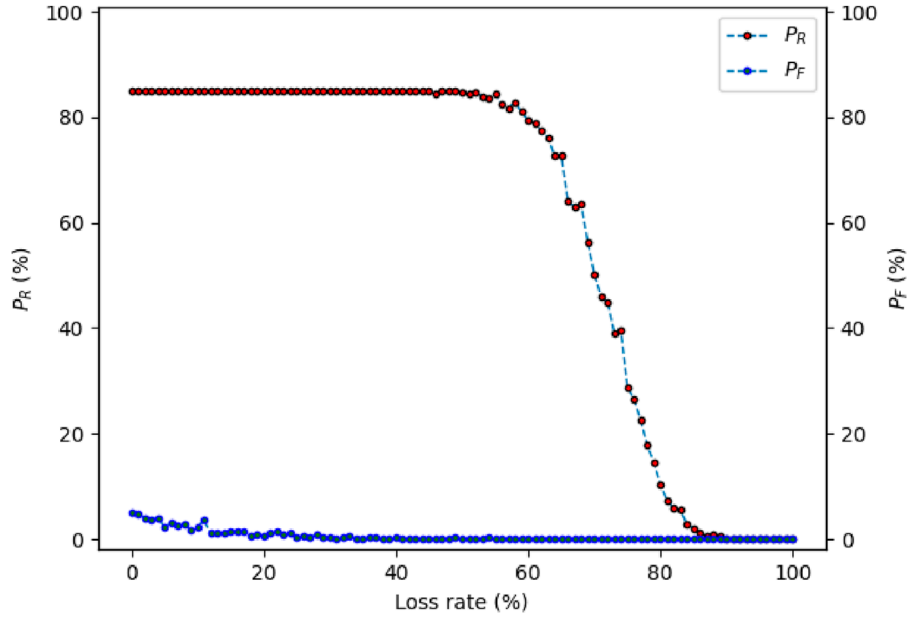

FIGURE 14
The influence of loss rate on inference accuracy and false rate.

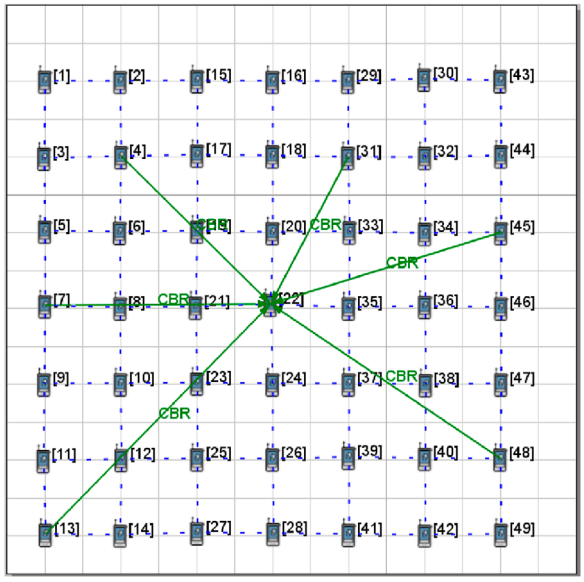

FIGURE 15
Multiple-to-one business mode scenario diagram.

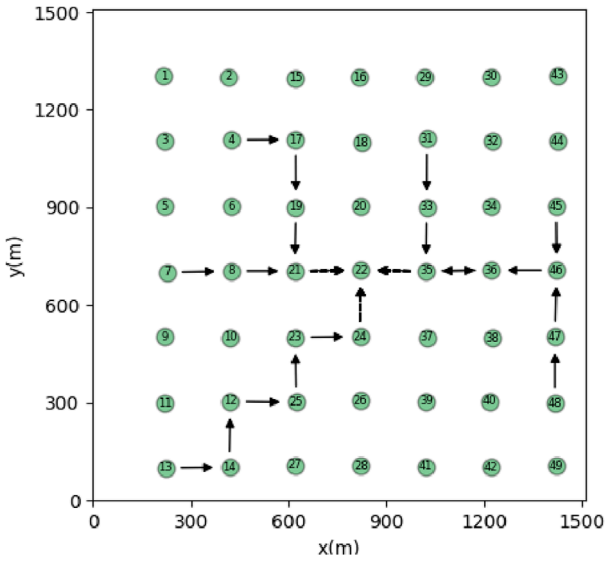

FIGURE 16
Inference result for the multiple-to-one operational mode.

enough input, thus the calculated accuracy is low; after 36*s*, the input is enough to infer the topology.

As can be seen from Figure 14, when the loss rate reaches a certain value, around 57%, the false rate will gradually decrease. It is because the amount of data is too small at this time, resulting in very few node pairs inferred by the algorithm, and thus the number of inferred wrong node pairs is gradually reduced.

4.3 Typical operational scenarios experiments

In the aforementioned simulated network environment, the algorithm's performance is validated in conjunction with different typical operational scenarios. In each scenario, the value of Δ_m is obtained through adaptive adjusting.

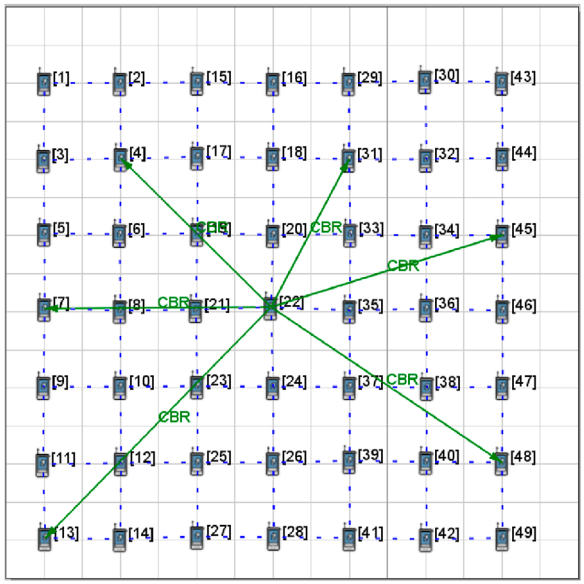

FIGURE 17
One-to-multiple business mode scenario diagram.

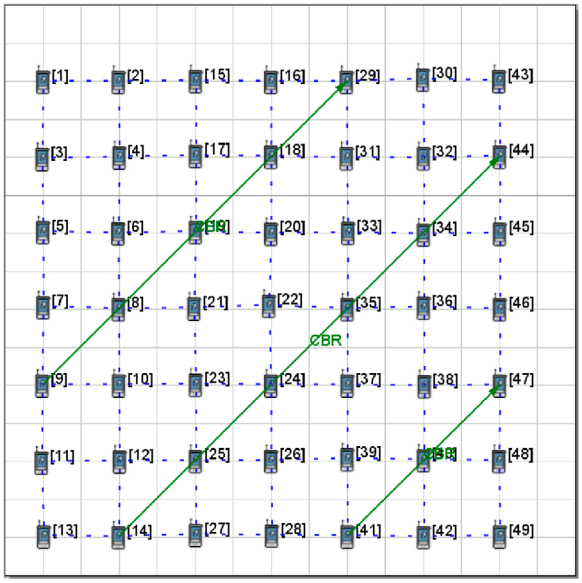

FIGURE 19
Scene diagram for the one-to-one operational mode (non-crossing).

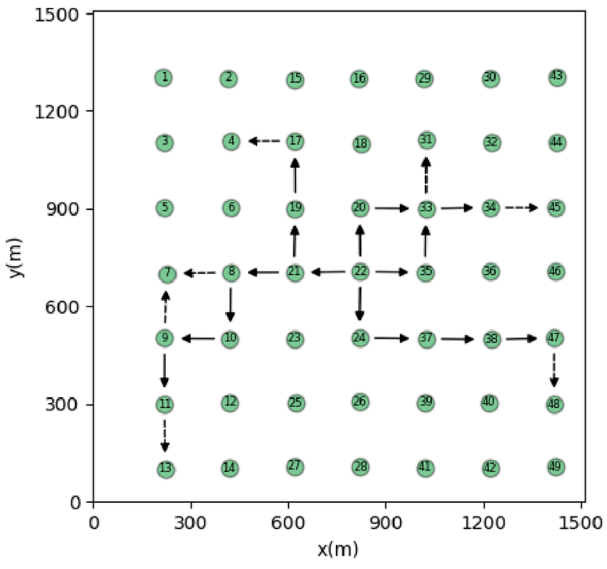

FIGURE 18
Inference result for the one-to-multiple operational mode.

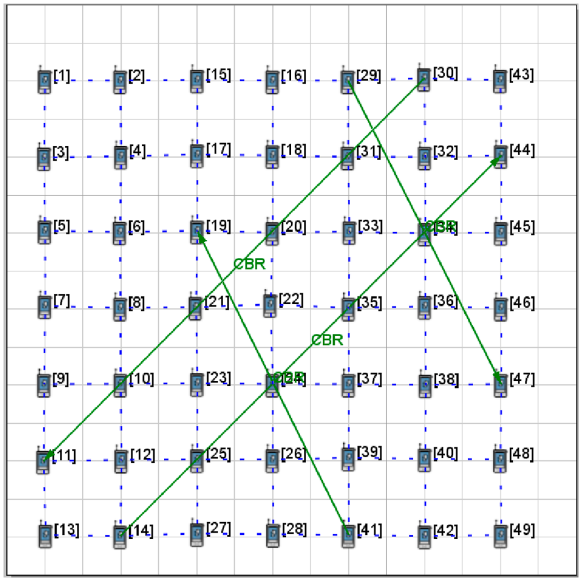

FIGURE 20
Scene diagram for the one-to-one operational mode (crossing).

4.3.1 Multiple-to-one operational mode

Multiple-to-one operational mode refers to a scenario where multiple nodes in the network communicate with a specified node during the simulation period. This operational mode often occurs in practical scenarios where lower-level units report situations to higher-level units. The simulation scenario diagram containing the business information flow is shown in Figure 15, nodes 4, 7, 13, 31, 45, and 46 transmit a CBR to node 22, respectively. The time duration of every CBR is 30s. The topology inference result is depicted in Figure 16. It can be observed that the node pairs identification accuracy rate P_R is 85%, and the node pairs identification false rate P_F is 5%. The reason for the last-hop cannot be inferred is mainly because the method in this paper depends on the forwarding behavior of the communication node, the receiving node does not forward.

4.3.2 One-to-multiple operational mode

One-to-multiple operational mode refers to a scenario where a specified node distributes information to multiple nodes in the network during the simulation period. This operational mode often

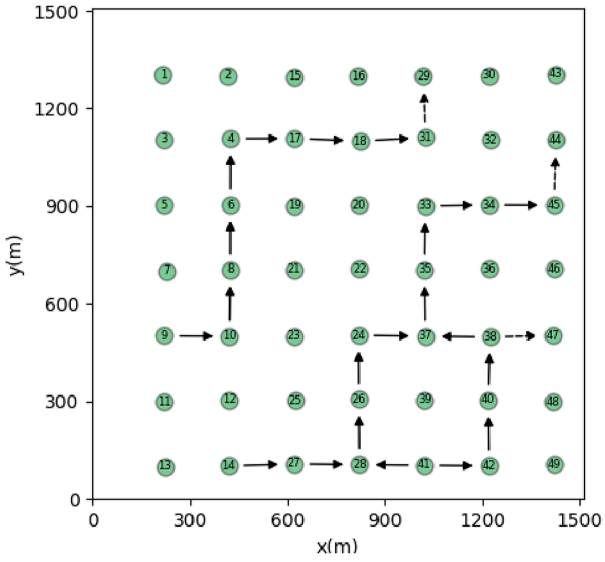

FIGURE 21
Inference result for the one-to-one operational mode (non-crossing).

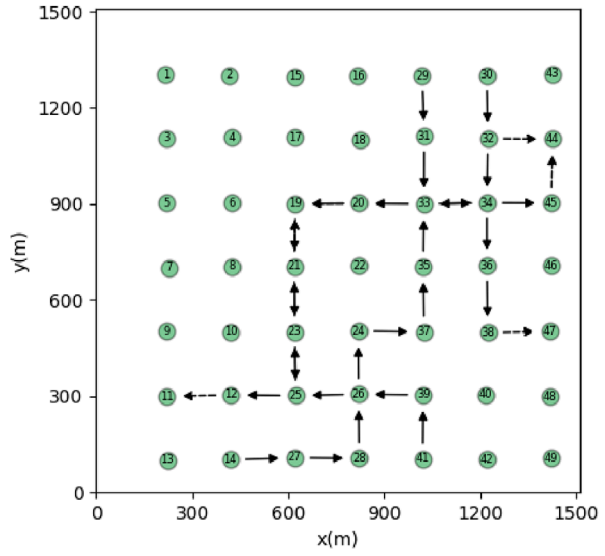

FIGURE 22
Inference result for the one-to-one operational mode (crossing).

occurs in practical scenarios where higher-level units assign tasks to lower-level units. The simulation scenario diagram is shown in Figure 17, node 22 transmits one CBR to nodes 4, 7, 13, 31, and 45, respectively. The topology inference result is depicted in Figure 18. It can be observed that the node pairs identification accuracy rate P_R is 72.73%, and the node pairs identification false rate P_F is 0%.

4.3.3 One-to-one operational mode

One-to-one operational mode refers to a scenario where a specified node in the network randomly initiates business communication with other nodes in the network. This operational

Input: $F = \{F_1, F_2, \ldots, F_n\}, F', n, t, \Delta_m$
Output: $\mathbf{A} = [a_{ij}] \in \mathbb{R}^{n \times n}$
$\mathbf{A} \leftarrow \mathbf{0}_n$
$F' \leftarrow \varnothing$
Calculate Δ_m by adaptive adjustment method based on input data
for $i = 1 : n$ **do**
  $n_i = len(F_i)$
  for $j = 1 : (n_i - 1)$ **do**
    $f_u = F_i[j]\}$
    $f_d = F_{i+1}[j]$
    if then $f_d - f_u \le \Delta_m$
      $j = j + 1$
    else
      break
    end if
  end for
  Add$\{F_i, F_{i+1}\}$ to F'
  $i = i + 1$
end for
$n' = len(F')$
for $i = 1 : n'$ **do**
  $R_D \leftarrow R_f(t)\Delta = \frac{\sum_{i}^{i+1} |F_i \cap [\emptyset, t]|}{\sum_{i+1}^{i+1} |s_i \cap [\emptyset, t]|}$
  CalculateR_E between node i and node j
  if $R_E \le R_D$ **then**
    $a_{ij} = 1$
  else
    $a_{ij} = \emptyset$
  end if
end for

Algorithm 1. Topology inference algorithm.

mode often occurs in practical scenarios where adjacent units exchange information. Two simulation scenarios were constructed based on whether there are crossings in the information flow transmission paths, as shown in Figures 19, 20. The topology inference results are depicted in Figures 21, 22. From those figures, it can be observed that in the case of non-crossing business flows, the node pairs identification accuracy rate P_R is 86.36%, and the node pairs identification false rate P_F is 9.1%. In the case of crossing business flows, the node pairs identification accuracy rate P_R is 87.1%, and the node pairs identification false rate P_F is 0%.

5 Conclusion and future work

This paper investigates the topology inference of IoBT without network access and information parsing. We propose a non-cooperative topology inference method for IoBT based on flow rate estimation. In the method, the sending time sequences of data between adjacent nodes in the IoBT are extracted. According to the requirement of the maximum delay in information transmission in the network, the information flow within a certain threshold of the

information transmission time between adjacent nodes is extracted. In order to improve the accuracy of communication relationship inference, a threshold parameter adaptive method is also proposed, by adjusting the value adaptively, the negative influence of fixed value on the inference result is avoided. The relative flow rate size R_D of information transmission in the network and the relative flow rate R_E between nodes with independent information flow are calculated. If $R_D \geq R_E$, it is determined that there is a communication relationship between adjacent node pairs. Simulation experiments have demonstrated the feasibility of this method.

However, there are limitations and challenges associated with the proposed method. First, the proposed algorithm operates in a centralized manner. Since the runtime complexity of the algorithm is polynomial with respect to the input size, the execution time increases significantly as the size of the network grows. This makes the proposed method less suitable for large-scale networks, where the computational overhead and latency could become prohibitive. To address this, future work could explore distributed or parallelized versions of the algorithm, leveraging modern computing architectures such as edge computing or cloud-based solutions to improve scalability and efficiency.

Second, the proposed method is primarily designed for static networks. The input to the algorithm, which is the timestamp sequence, remains fixed during the execution of the algorithm. As a result, the inferred topology reflects only a snapshot of the network's state at the time the input was collected. If the network topology changes after the input is taken—due to node mobility, link failures, or adversarial actions—the accuracy of the inferred topology may degrade significantly. This limitation is particularly critical in IoBT environments, where network dynamics are inherent due to the mobility of combat units, environmental factors, and evolving mission requirements. To overcome such a challenge, future research should focus on developing adaptive and real-time topology inference methods capable of handling dynamic network conditions.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

JH: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Methodology, Project administration, Resources, Writing – original draft. RD: Conceptualization, Data curation, Formal Analysis, Methodology, Writing – review and editing. ZN: Formal Analysis, Investigation, Writing – review and editing. CP: Data curation, Software, Writing – review and editing. JC: Validation, Writing – review and editing.

Funding

The author(s) declare that no financial support was received for the research and/or publication of this article.

Acknowledgments

The authors would like to thank the reviewers for their valuable comments and suggestions.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Gen AI was used in the creation of this manuscript.

Publisher's note

References

1. Wen J, Yang J, Wang S. Development status and prospect of electronic warfare equipment technology. *Inf Countermeasure Technology* (2022) 1:1–10. doi:10.12399/j.issn.2097-163x.2022.01.001

2. Conradie NH. Autonomous military systems: collective responsibility and distributed burdens. *Ethics Inf Technology* (2023) 25:20. doi:10.1007/s10676-023-09696-9

3. Chen J, Zheng X, Peng L, Xu Z, Li A. Research on land battlefield situation distribution network based on brn. *J Phys Conf Ser* (2020) 1646:012048. doi:10.1088/1742-6596/1646/1/012048

4. Abuzainab N, Saad W. Dynamic connectivity game for adversarial internet of battlefield things systems. *IEEE Internet Things J* (2018) 5:378–90. doi:10.1109/JIOT.2017.2786546

5. Akter R, Golam M, Doan V-S, Lee J-M, Kim D-S. Iomt-net: blockchain-integrated unauthorized uav localization using lightweight convolution neural network for internet of military things. *IEEE Internet Things J* (2023) 10:6634–51. doi:10.1109/JIOT.2022.3176310

6. Li X, Wei P, Wei ZJ, Guosong L, Ping W. Research on security issues of military internet of things. In: *2020 17th international computer conference on wavelet active media technology and information processing (ICCWAMTIP)* (2020). p. 399–403. doi:10.1109/ICCWAMTIP51612.2020.9317401

7. Islam A, Masuduzzaman M, Akter A, Young Shin S. Mr-block: a blockchain-assisted secure content sharing scheme for multi-user mixed-reality applications in internet of military things. In: *2020 international conference on*

information and communication technology convergence (ICTC) (2020). p. 407–11. doi:10.1109/ICTC49870.2020.9289327

8. Rutravigneshwaran P, Anitha G, Prathapchandran K. Trust-based support vector regressive (tsvr) security mechanism to identify malicious nodes in the internet of battlefield things (iobt). *Int J Syst Assur Eng Management* (2024) 15:287–99. doi:10.1007/s13198-022-01719-w

9. Yan H. The study on network topology discovery algorithm based on snmp protocol and imp protocol. In: *2012 IEEE international Conference on computer Science and automation engineering (beijing: ieee)* (2012). p. 665–8.

10. Yong W, Nan P, Xiaoling T. Network topology discovery algorithm based on ospf. In: *2010 international conference on intelligent computing and integrated systems* (2010). p. 136–9. doi:10.1109/ICISS.2010.5656788

11. Chen R, Chang L, Hui Y, Cheng N, Zhang W. Noncooperative topology inference of wireless networks with monitoring sensors. *IEEE Internet Things J* (2023) 10:19282–95. doi:10.1109/JIOT.2023.3281388

12. Zhang X, Phillips C. A survey on selective routing topology inference through active probing. *IEEE Commun Surv & Tutorials* (2012) 14:1129–41. doi:10.1109/SURV.2011.081611.00040

13. Jin X, Yiu W-PK, Chan S-HG, Wang Y. Network topology inference based on end-to-end measurements. *IEEE J Selected Areas Commun* (2006) 24:2182–95. doi:10.1109/JSAC.2006.884016

14. Niu Z, Ma T, Shu N, Shan H. Interference sources localization and communication relationship inference with cognitive radio iot networks. *IEEE Access* (2020) 8:103062–72. doi:10.1109/access.2020.2998730

15. Tilghman P, Rosenbluth D. Inferring wireless communications links and network topology from externals using granger causality. In: *Milcom 2013 - 2013 IEEE military communications conference*. San Diego, CA, USA: IEEE (2013). p. 1284–9.

16. Sharma P, Bucci DJ, Brahma SK, Varshney PK. Communication network topology inference via transfer entropy. *IEEE Trans Netw Sci Eng* (2020) 7:562–75. doi:10.1109/tnse.2018.2889454

17. Liu C, Wu X, Zhu L, Yao C, Yu L, Wang L, et al. The communication relationship discovery based on the spectrum monitoring data by improved dbscan. *IEEE Access* (2019) 7:121793–804. doi:10.1109/ACCESS.2019.2938296

18. Testi E, Giorgetti A. Blind wireless network topology inference. *IEEE Trans Commun* (2021) 69:1109–20. doi:10.1109/TCOMM.2020.3036058

19. Ganesh P, Venkataraman H. Rf-based wireless communication for shallow water networks: survey and analysis. *Wireless Personal Commun* (2021) 120:3415–41. doi:10.1007/s11277-021-09068-w

20. Singh M, Shrivastava L. Multi-objective optimized multi-path and multi-hop routing based on hybrid optimization algorithm in wireless sensor networks. *Wireless Networks* (2024) 30:2715–31. doi:10.1007/s11276-024-03686-5

21. Chai Y, Zeng X, Liu Z. The future of wireless mesh network in next-generation communication: a perspective overview. *Evolving Syst* (2024) 15:1635–48. doi:10.1007/s12530-024-09583-8

22. Roy A, Pachuau JL, Saha AK. An overview of queuing delay and various delay based algorithms in networks. *Computing* (2021) 103:2361–99. doi:10.1007/s00607-021-00973-3

23. Walia AK, Chhabra A, Sharma D. Comparative analysis of contemporary network simulators. In: JS Raj, editor. *Innovative data communication technologies and application*, 96. Singapore: Springer (2022). p. 369–83. doi:10.1007/978-981-16-7167-8_27