Security Cooperation Model Based on Topology Control and Time Synchronization for Wireless Sensor Networks

Zhaobin Liu, Wenzhi Liu, Qiang Ma, Gang Liu, Liang Zhang, Ligang Fang, and Victor S. Sheng

Abstract: **To address malicious attacks generated from wireless sensor networks (WSNs), in this paper, we study the difficulty of detecting uncoordinated behavior by using a model that is unreliable and has uncontrollable accuracy, trustless control, and an inextensible protocol. A security collaboration model involving coupled state vectors associated with topology control and time synchronization is proposed. The networks achieve synchronization using weights and by controlling the number of goals. The simple calculation of time synchronization values between neighboring nodes serves as the basis for judging the behavior of the node topology control. The coupling state vector calculation is the core of the model. The topology coupling strength rate, signal intensity reduction, clock drift, and clock delay are combined to form a comprehensive model. The network energy consumption is reduced by updating the coupling state vector regularly. The coupling cooperation threshold is set to make security decisions and effectively distinguish between attack nodes and dead nodes. Thus, to ensure the security and reliability of the network, we present a security cooperation collection tree protocol (SC-CTP) scheme that maintains a trusted environment and isolates misbehaving nodes. The simulation results show that the model can detect malicious nodes effectively, has a high detection rate, and greatly reduces the energy consumption of the whole network. In order to verify the effectiveness of the proposed model, a large-scale wireless sensor network with 200 nodes was deployed on a campus. The proposed model was applied to optimize the deployment of key nodes on the campus. Furthermore, a candidate set of these nodes were selected to achieve coupling cooperation of key goals. This test verified the reliability of the model, its customizable accuracy, and the reliability of the control.**

Index Terms: **Security cooperation model, time synchronization, topology control, WSNs.**

Manuscript received March 5, 2019.

This research is partially supported by NSFC under Grant No. 61672372 and No. 61472211, and Outstanding Science-technology Innovation Team Program of Colleges and Universities in Jiangsu. We thank all the reviewers and shepherds for their valuable comments and helpful suggestions.

Z.-B. Liu, W.-Z. Liu, G. Liu, L. Zhang, and L.-G. Fang are with School of Computer Engineering, Suzhou Vocational University, email: {zbliusz, lwzsz}@126.com and {liugang, zhangl, fanglg}@jssvc.edu.cn.

Q. Ma is with School of Software, Tsinghua University, email: tsinghuamq@gmail.com.

V. S. Sheng is with Department of Computer Science, University of Central Arkansas, email: ssheng@uca.edu.

W.-Z. Liu is the corresponding author.

Digital Object Identifier: 10.1109/JCN.2019.000041

I. INTRODUCTION

WITH the wide application of the Internet of things (IoT), the reliability and safety of data transmission over wireless sensor networks (WSNs) have become increasingly important issues [1], [2]. Reliability refers to random packet losses or error packets in a wireless link caused by topological changes, time synchronization attacks, human disturbance, or packet collisions. These results in failure to ensure the reliability and efficiency of data transmission [3]–[5]. Safety refers to safety threats like latent invasions and attacks, including threats and attacks caused by passive wiretapping, data tampering and retransmission, falsification of identity, denial of service, node capture, and so on, which may affect the integrity, confidentiality, authentication, and serviceability of data. Traditional cryptographic- and authentication-based security schemes cannot be adopted due to associated costs and inability to counter node misbehavior attacks. Furthermore, existing trust based on topology control and time synchronization protocols incurs high control overheads in trust estimation and dissemination, leading to a high number of dead nodes arising from the topology control route discovery mechanism and high route instability [6]–[8].

The reliability relations between nodes are dynamic and uncertain in complex WSNs and change over time [9]–[11]. In the real world, as time passes, some entities that were previously reliable before become unreliable. The hostile behaviors of unreliable entities may threat normal operations of a system if changes are ignored. In addition, because of the importance of time synchronization in WSNs data transmission, the collaboration of time synchronization and topology control has become a general approach to test whether a WSNs has been attacked. Existing time synchronization methods are mostly subject to a great number of data packet exchanges, which may cause problems such as higher cost of node calculation and lower safety.

It is possible to determine whether a network has received a security threat by analyzing the degree of collaboration between topology control and time synchronization. Factors that affect the accuracy of time synchronization belong to three main categories [12]:

First, drift in the hardware clock. Its frequency can be affected by the environment, humidity, battery voltage, and so on.

Second, synchronization methods based on an external signal source rely on wireless communication to exchange the synchronization information. Uncertainty in delays can occur due to the behavior of the packets' replay attack, the presence of abnormal packets, and forgery attacks derived from malicious nodes.

Third, the depth and breadth of the network being attacked

is related to topology discovery. Network size is a key factor affecting the accuracy of time synchronization. The marginal value of time synchronization is $\Omega(DT/2)$ [13], in which D is the network diameter and T is the transmission delay.

In this paper, a dynamic security collaboration model based on topology control and time synchronization with multiple factors is proposed. The model improves the reliability degree between WSNs nodes and ensures the safety of node data transmission through a multi-angle reliability model that combines communication, data, and energy [14].

The rest of the article is organized as follows. Section II introduces the related work. Section III describes the security model. Section IV presents details of the model design. Section V analyzes the delay produced with unknown random coupling intensity information and known coupling matrix information. Section VI evaluates the performance of the model communication protocols. We demonstrate the implementation, data collection, and experimental results, and present a discussion in Section VI. The conclusions are presented in Section VII.

II. RELATED WORK

Current goals of sensor network topology control [15] largely include ensuring the connectivity of the network, optimizing the reliability of network transmission, and reducing link interference. However, with regard to improving accuracy of time synchronization, most existing topology control mechanisms lower the node degree [16] or network sparsity instead of focusing on the time synchronization accuracy and self-adaption of dynamic topological structures as their direct optimization goal. This is because they assume that the sparser the network topology and the lower the node degree, the lower the inference between shared channel links. However, this is not the case.

He and others [17] firstly proposed and verified the issues of minimization for the maximum node of the maximum independent set and load-balanced virtual backbone network [18]. They further put forward the Load-Balanced Virtual Backbone (LBVB) algorithm, which uses nonlinear integer programming and linear programming relaxation techniques to achieve the approximate best-connected dominating set.

The A3 algorithm proposed by Wightman and others [7] aims to set up a suboptimal connected dominating set. It establishes a spanning tree in the network through mutual broadcasting, reply, and confirmation of information between nodes. However, unnecessary message transmission and energy loss are present in its unique secondary wake-up process. Torkestani and others [20] presented an energy balance connection dominating set algorithm to solve the network energy and delay issues based on the theory of learning automata. This algorithm determines the optimal degree of network constraint through the interaction of the environment and automata by the continuous behavior set learning automata method, which minimizes the network delay and maximizes the life-cycle of the network.

Pratyay K [21] and others have proposed a clustering method based on the load balance of the genetic algorithm. This method matches the number of sensor nodes to the number of chromosomes in the algorithm and distributes the relevant chromosomes across gateway nodes. Next, it judges if the load of the node is balanced according to the standard deviation of the load on the gateway node when a balanced load is reached in the network. Liu and others put forward a fully distributed topology control algorithm based on the lossy link network model in which the reliability of links between nodes and the reliability of the overall network is calculated based on reliability theory to judge whether the network set up meets the threshold requirements.

Though the algorithm and the protocols proposed in the documents above solve the issue of node energy consumption within a certain range, and are able to reasonably set up the network topology and prolong the survival time of the network, there are still many problems. For instance, the information that needs to be exchanged to wake up the sleeping node is used in the process of setting up the spanning tree, which may cause unnecessary energy consumption. The link reliability and the node packet loss rate are not taken into account in the selection of cluster heads, and the distances between cluster heads are not considered, so when there are more members in the cluster the cluster head may run out of energy very quickly due to overload. Finally, link performance is not evaluated to avoid unnecessary energy consumption.

Time synchronization technology is currently a focus of research [22], [23]. Studies are being carried out on energy consumption reduction and improving adaptability of changes in the topological structure, but while maintaining the accuracy of synchronization. As the time synchronization accuracy of a single-hop network is sufficient in most cases, researchers have begun to pay attention to requirements of the time synchronization algorithm in terms of energy consumption, extensibility, and adaptability. This work has expanded into multihop networks.

The reference broadcast synchronization (RBS) proposed by Elson and others [24], and R4Syn proposed by Djenouri [25] make use of broadcasting characteristics of wireless communication channels. RBS calculates the difference in mean information arrival time between receiving nodes by broadcasting more time synchronization information, and also linearly fits the clock deviation using a least-squares linear regression method. This further improves the accuracy of time synchronization. However, in a single-hop network with n nodes, this algorithm needs to exchange $O(n^2)$ information. Thus, for large-scale sensor networks, the large amount of information exchange required may cause a long convergence time and a higher energy cost for time synchronization. Therefore, this method fails to consider the space complexity.

The timing protocol for sensor network (TPSN), proposed by Ganeriwal and others [26], is similar to the traditional time synchronization network, tree structure reference time synchronization (TSRT) [27]. It was developed into a time synchronization algorithm for the overall network using the C/S model. For large-scale WSNs, the synchronization accuracy of TPSN does not decrease as the number of nodes increases. Compared to RBS, TPSN offers synchronization accuracy that is twice that of RBS. However, as the network topological structure changes, the hierarchical discovery phase needs to be initiated, which causes additional energy consumption.

Flooding time synchronization (FTSP), first put forward by Marti and others [28], is customized for wireless platforms and has higher accuracy requirements and limited energy. This al-

gorithm has a high degree of robustness as it periodically floods the network with synchronization information and conducts latent dynamic topological updates. It reaches high levels of time synchronization accuracy by comprehensive error compensation, including clock deviation and time stamp techniques on the MAC layer. The target is to achieve time synchronization for the network as a whole. However, the algorithm itself has some key issues, including a long time required for flooding and error accumulation, so there is still room for further improvement in time synchronization accuracy and energy consumption. Currently, research into optimization of the FTSP method is focused on synchronization accuracy and energy consumption.

Shannon and others [29] have proposed dynamic flooding time synchronization (D-FTSP), which dynamically changes the transmission distance of nodes according to the requirements of time synchronization by the WSNs application and the stability of the neighbor node clock. This eliminates the need to identify and preset suitable node transmission time intervals for FTSP under certain circumstances. In this case, it is not necessary to know the operation environment that the algorithm needs in advance; thus, the WSNs can be deployed quickly with remarkable energy saving effects, which prolongs the service life of nodes.

In recently reported research, Preetha and others [30] studied the low energy and self-adaptive cluster head routing area clustering topology algorithm. This algorithm reaches a balance between energy consumption and efficiency by controlling the residual energy of nodes, maintaining a continuous communication network topological structure, and freely adjustable parameters. Qian and others [31] have studied the phenomena of the inhomogeneous energy hole (caused by energy consumption) by looking at energy efficiency and fault-tolerant topological structure. They proposed energy hole aware efficient communication (EHAEC), a communication and routing algorithm of energy hole perception and energy efficiency, which achieved favorable results. Xing and others [32] have studied the uncertainty of clock drift and information transmission delay by setting up a self-adaptive WSNs time synchronization model with linear prediction. This model has a lower cost and higher accuracy than RBS and TPSN. Amulya and others [33] have studied the multihop time synchronization protocol by designing an iterative method that responds to topology changes and offers a new gradient descent time synchronization protocol with extendable multihop synchronization. They marked out basic steps to improve these algorithms. Wu and others [34] proposed a WSNs consistency time synchronization algorithm based on a colony, in which they updated the network simulation clock compensation parameter by allocating relevant weights to the virtual clock compensation parameters within each cluster head. This reduced the communication load and improved the convergence speed.

Current time synchronization protocols based on topology control in single-hop WSNs are reasonably mature, but they still have some disadvantages in multihop WSNs, detailed in the following.

Unreliable model: There is no formal definition sufficient to describe the relation between topology control and time synchronization of WSNs. For large-scale sensor networks, the large amount of information exchange leads to longer convergence time, causing them to be unable to self-adapt to the accuracy requirements of different applications to set up the connected dominating set of the virtual subnetwork.

Adjustable accuracy: The hierarchy referencing time synchronization (HRTS), FTSP, and EHAEC protocols can only ensure that time synchronization is evaluated under specific circumstances. They cannot determine whether the time synchronization accuracy is related to the topological structure path and are not able to satisfy the customized accuracy requirements of applications.

Trustless control: The load-balanced virtual backbone (LBVB), TPSN, TSRT, and D-FTSP protocols cannot accurately judge their own degree of trust. They analyze time synchronization based on mean degree constraint and edge convergence theory, while ensuring sparse network coverage and lowering the node degree. However, this analysis process has defects that could adversely affect the effectiveness of the results.

Inextensible protocol: The EHAEC and D-FTSP methods require the node to store an information table or the results of computation. When the scale of the system becomes larger, the extra time taken for this cannot be neglected.

In conclusion, the operational efficiency of existing time synchronization protocols for WSNs is low and the topology control protocol for WSNs is unable to offer reliable control of time synchronization. Thus, in view of the above deficiencies, this paper proposes a model with topology control and time synchronization accuracy that is sublinear, has self-adaptive accuracy, and has reliable control.

In order to solve the above challenges, we propose a novel scheme that takes full advantage of coupling features in the synchronization tracing process. The parameters associated with the network topology and time synchronization are the coupling state vector and mathematical models associated with the topology coupling strength rate, the signal intensity, clock drift, and clock delay. A model with topology control and time synchronization for use in a dynamic and complex sensor networks is established.

III. SECURITY COOPERATION MODEL

A. WSNs System Structure

Most classic synchronization algorithms are based on the single-hop synchronization mechanism. For large-scale networks, it is impossible to complete time synchronization within the broadcast range of one hop, and time synchronization information must be forwarded to the peripheral nodes through multiple nodes. Thus, in a multihop network, the accuracy of time synchronization is severely affected by cumulative error [35]. Therefore, a protocol that repeatedly forwards time synchronization information is clearly not suitable for large-scale, multihop networks.

FTSP and TPSN can effectively reduce the cumulative error of a multihop network by establishing a hierarchical topology for nodes. However, these protocols still have certain defects. They can not select the optimal parent node, as the arrival time is the only indicator used for selection. As a result, the accuracy of time synchronization is reduced.

In order to filter synchronization information in the dynamic

topology structure for large-scale networks, a certain number of monitoring nodes need to be deployed for each cluster, and these detection nodes are used to select the optimal parent node, which has a clock offset and frequency drift that are closer to those of the reference clock. This can effectively improve the time synchronization accuracy of the network.

Definition 1 The WSNs system is the original connected undirected graph $G = (V, E)$, where V represents all the nodes in the network and E represents a communication link between any of the two nodes. Let $V = \{V_1, \cdots, V_k\}$ be a partition of the index set $1, 2, \cdots, N$ into k non-empty subsets, $V_l \neq \phi$ and $U_{l=1}^{k} V_l = V$, where $V_1 = \{1, 2, \cdots, m_1\}$, $V_2 = \{m_1 + 1, \cdots, m_1 + m_2\}, \cdots$, and $V_k = \{m_1 + \cdots + m_{k-1} + 1, \cdots, m_1 + \cdots + m_k\}$,$1 < m_l < N, \sum_{l=1}^{k} m_l = N$. Let G_l denote the underlying topology of cluster V_l,$l \in (1, k)$, i.e.,$V_l = V(G_l)$. In order to supervise the goal, let $s_{ij} = V_i \bigcap V_j, i, j \in 1, 2, \cdots, k$ be a sensor set of the monitoring partition V_l. For $u_i \in V$, let i denote the subscript of the subset to which the integer u_i belongs, i.e., $u_i \in V_i$. The area for deployment is circular, and uses the goal node $u_i \in \{1, m_1 + 1, \cdots, m_1 + \cdots + m_{k-1} + 1\}$ as the center and $\varphi_i * \in R_G$ as the diameter. This is also referred to as the u_i node deployment area. In this area, R_G is the perceived distance of the node. $0 < \varphi_i < 1$ is the self-adaptive parameter of the node deployment area. The formula of φ_i is

$$\varphi_i = (\tau)^{\Gamma_i}. \tag{1}$$

$0 < \tau < 1$ is the parameter related to the topology coupling intensity. $\Gamma_i \geq 1$ is the weight of target u_i and the synchronization controller, the more important the target is, the larger the weight and the closer the topology control passes to the deployment path of the area, that is, the smaller the diameter of the node deployment area. Conversely, the lower the importance of the goal, the larger the diameter of node deployment area.

B. Time Synchronization Security Model

Synchronization refers to many dynamic systems that have the same or similar characteristics. These systems finally reach the same dynamic characteristics by mutual information exchange and interactions under different original conditions. The state equation for the dynamic cooperation status of a sensor network with N nodes is

$$\begin{aligned} \dot{X}_i(t) &= f(t, X_i(t)) \\ &\quad + \tau_1(t) \sum_{j=1}^{N} ((\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t) b_{ij} X_j(t))) \\ &\quad i = 1, 2, \cdots, N, \end{aligned} \tag{2}$$

where $X_i(t) = (x_{i1}, x_{i2}, \cdots, x_{in} \in R^n$ is the status vector of the time synchronization network node. $f : R^n \to R^n$ is a continuous, differentiable vector function, α_i and β_i are the normalized weight vectors, and $\tau(t)$ is the random coupling intensity of the time synchronization network. $B = (b_{ij}) \in R^{N \times N}$ is a constant coupling configuration matrix. They meet the following conditions: if the connection is $j (i \neq j)$, then $b_{ij} > 0$, otherwise, $b_{ij} = 0$. The diagonal elements are

$$b_{ii} = -\sum_{\substack{j=1 \\ j \neq i}}^{N} b_{ij} = -\sum_{\substack{j=1 \\ j \neq i}}^{N} b_{ji}, \quad i = 1, 2, \cdots, N. \tag{3}$$

Π_{ij} is the ratio for the clock drift value between sensor network target node u_i and deployment node s_j when the clock drifts in and out of the value of node u_i. Λ_{ij} is the ratio of the clock delay between the target node u_i and the deployment node s_j, for the total clock delay of node u_i. Thus,

$$\Pi_{ij} = \frac{\xi_{ij}}{\sum_f^{k_i} \xi_{if}} \quad \Lambda_{ij} = \frac{\Delta_{ij}}{\sum_f^{k_i} \Delta \xi_{if}}. \tag{4}$$

ξ_{ij} is the clock drift between the target node u_i and the deployment node s_j, and the clock delay between target node u_i and deployment node s_j. The degree of coupling between neighbor nodes is positively correlated with Π_{ij} and Λ_{ij}.

C. Topology Control Reliability Model

$$\begin{cases} \dot{Y}_i(t) &= f(t, Y_i(t)) \\ &\quad + \tau_2(t) \sum_{j=1}^{N} \frac{\gamma_i}{V_{ij}(t)} \psi_i(t) H_{C_{ij}} Y_j(t) + \Gamma_i(t) \\ \Gamma_i(t) &= -\eta(t) Y_i(t) \\ &\quad i = 1, 2, \cdots, m \\ \dot{Y}_i(t) &= f(t, Y_i(t)) + \tau_2(t) \sum_{j=1}^{N} \frac{\gamma_i}{V_{ij}(t)} \psi_i(t) H_{C_{ij}} Y_j(t) \\ &\quad i = m+1, m+2, \cdots, N \end{cases}, \tag{5}$$

where $Y_i = (y_{i1}, y_{i2}, \cdots, y_{iN}) \in R^n$ represents the node status vector in the topology control network, and m is the number of synchronization controllers. The vector element of the state vector in the sensor network can be the residual battery volume, channel interference, channel congestion, or the transmission speed. $\tau_2(t)$ is the topological coupling strength between network nodes. H is the coupling matrix between state variations of the goal nodes. $H = diag(\omega_1, \omega_2, \cdots, \omega_n)$ is the diagonal matrix. If any of the two goal nodes achieve coupling through the j^{th} deployment node, then $\omega_j = 1$, otherwise $\omega_j = 0 (j \neq i)$. $C = (c_{ij}) \in R^{N \times N}$ is the constant coupling configuration matrix in the topology network. If there is a direct and stable linkage between the goal node and deployment node u_i and deployment node s_j (being neighboring nodes in the topological structure with directly connected sides), then $c_{ij} = c_{ji} = 1$, otherwise, $c_{ij} = c_{ji} = 0$. The diagonal element is

$$c_{ii} = -\sum_{\substack{j=1 \\ j \neq i}}^{N} c_{ij} = -\sum_{\substack{j=1 \\ j \neq i}}^{N} c_{ji} = -k_i, \quad i = 1, 2, \cdots, N, \tag{6}$$

where k_i is the degree of node u_i , matrix c is the adjacency matrix of the sensor network, which represents the network topological structure. It is also referred to as the external coupling matrix and the Laplacian operator, and reflects certain topological structure characteristics of the network and the coupling

relations between nodes [36]. $\psi(t)$ is the communication signal strength between links (u_i, s_j), $\Gamma_i(t)$ is the synchronization controller that needs to be designed, and $\eta(t)$ is the control gain variable.

$V_{ij}(t)$ is the replaceable coefficient if each node is selected to be the deployment node according to load balance status of its neighbours within two-hops. $V_{ij}(t) = v_{ij}(t) + v_{ji}(t)$, in which $v_{ij}(t)$ is the number of other deployment nodes that can be found by u_j in the deployment coverage area and can replace s_i. $v_{ji}(t)$ is the number of other deployment nodes that can be found by u_i in the deployment coverage area and can replace s_j. The coupling degree between neighbor nodes has a negative correlation with $V_{ij}(t)$. $(\alpha_i, \beta_i, \gamma_i)$ is the normalized weight vector. Here, $\alpha_i < \beta_i < \gamma_i$, which means that the substitutability of an intermediate node that connects its 2-hop neighbors in the sensor network has a greater impact on the synchronization degree than the clock delay between them. Additionally, the clock drift between them has less impact on the topology degree than the clock delay between them.

IV. SECURITY COLLABORATIVE CONFIGURATION OF TIME SYNCHRONIZATION AND TOPOLOGY CONTROL

Definition 2

$$h_i(t) = Y_i(t) - X_i(t). \tag{7}$$

We design a suitable nonlinear synchronization controller $\Gamma_i(t)$ and achieve mean square synchronization between the drive network (time synchronization) and the response network (topology control) with a random coupling intensity, that is, the mean square deviation synchronization of formulas (2) and (5): $\lim_{t\to\infty} H\{h_i(t)\} = 0, i, j = 1, 2, \cdots, N$.

Assumption 1: When synchronization is realized when all times tend to the same value, i.e., $h_1(t) \to h_2(t) \to \cdots \to h_N(t) \to D(t)$, in which $D(t) \in R^N$; this is referred to as the synchronization status. Then, the mathematical degree and variance of the coupling degree is $\tau_i(t)(i = 1, 2)$: $H\{\tau_i(t)\} = \delta_i$, $H\{(\tau_i(t) - \delta_i)^2\} = \sigma_i^2$, where δ_i and σ_i are non-negative constants. It can be said that state (7) can gradually become stable as $h_i(t) \to D(t)$.

Assumption 2: $f(\cdot)$ meets the following inequality:

$$\|f(t, Y_i(t)) - f(t, X_i(t))\| \le \rho \|Y_i(t) - X_i(t)\|, \tag{8}$$

where ρ is a known positive constant, and $\| \bullet \|$ represents the Euclidean norm, $Y_i, X_i \in R^N$. Based on definition 2 and its two assumptions, when the coupling matrixes B and C are known, to achieve network-based synchronization between (2) and (5), the following formula is used:

$$\begin{cases} \dot{h}_i(t) = f(t, Y_i(t)) - f(t, X_i(t)) \\ \quad + \tau_2(t) \sum_{j=1}^{N} \frac{\gamma_i}{V_{ij}(t)} \psi_i(t) H_{c_{ij}} Y_j(t) \\ \quad - \tau_1(t) \sum_{j=1}^{N} ((\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t) b_{ij} X_j(t))) \\ \quad + \Gamma_i(t) \\ \quad i = 1, 2, \cdots, m \\ \dot{h}_i(t) = f(t, Y_i(t)) - f(t, X_i(t)) \\ \quad + \tau_2(t) \sum_{j=1}^{N} \frac{\gamma_i}{V_{ij}(t)} \psi_i(t) H_{c_{ij}} Y_j(t) \\ \quad - \tau_1(t) \sum_{j=1}^{N} ((\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t) b_{ij} X_j(t))) \\ \quad i = m+1, m+2, \cdots, N \end{cases}, \tag{9}$$

Formula (9) can be converted into (10):

$$\begin{cases} \dot{h}_i(t) = f(t, Y_i(t)) - f(t, X_i(t)) \\ \quad + \tau_2(t) \sum_{j=1}^{N} \frac{\gamma_i}{V_{ij}(t)} \psi_i(t) H_{c_{ij}} Y_j(t) \\ \quad - \tau_1(t) \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} Y_j(t) \\ \quad + \delta_1 \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} h_i(t) \\ \quad + (\tau_1(t) - \delta_1) \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} h_i(t) \\ \quad + \Gamma_i(t) \\ \quad i = 1, 2, \cdots, m \\ \dot{h}_i(t) = f(t, Y_i(t)) - f(t, X_i(t)) \\ \quad + \tau_2(t) \sum_{j=1}^{N} \frac{\gamma_i}{V_{ij}(t)} \psi_i(t) H_{c_{ij}} Y_j(t) \\ \quad - \tau_1(t) \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} Y_j(t) \\ \quad + \delta_1 \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} h_i(t) \\ \quad + (\tau_1(t) - \delta_1) \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} h_i(t) \\ \quad i = m+1, m+2, \cdots, N. \end{cases} \tag{10}$$

The assumption coupling matrixes in formulas (2) and (5) are known, and the network coupling intensity $\tau_i(t)(i = 1, 2)$ is unknown. In order to achieve external synchronization of the network, the weight of the goal node can be designated as

$$\begin{aligned} \Gamma_i(t) &= -d_i h_i(t) \\ &\quad + \dot{\delta}_1 \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} Y_i(t) \\ &\quad - \dot{\delta}_2 \sum_{j=1}^{N} \frac{\gamma_i}{V_{ij}(t)} \psi_i(t) H_{c_{ij}} Y_j(t) \\ &\quad i = 1, 2, \cdots, m, \end{aligned} \tag{11}$$

$$\dot{\delta}_1 = -\sum_{i=1}^{m} h_i^T(t) \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} Y_i(t), \tag{12}$$

$$\dot{\delta}_2 = -\sum_{i=1}^{m} h_i^T(t) \sum_{j=1}^{N} \frac{\gamma_i}{V_{ij}(t)} \psi_i(t) H_{c_{ij}} Y_j(t), \tag{13}$$

$$\dot{d_i^T} = q_i h_i^T(t) h_i(t), \tag{14}$$

where q_i is any positive constant, $1 \le i \le m$, if $d_i > 0$. Then, the gain $\eta_i(t)$ greater than $\tau_i(t)$. This means that the weight gain is larger than the coupling intensity of the network system. Using the above action, (10) can be revised as

$$\begin{cases} \dot{h_i}(t) & = f(t, Y_i(t)) - f(t, X_i(t)) \\ & + (\dot{\breve{\delta}}_1 - \delta_1) \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} Y_j(t) \\ & - (\delta_1 - \tau_1(t)) \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} Y_j(t) \\ & - (\dot{\breve{\delta}}_2 - \delta_2) \sum_{j=1}^{N} \frac{\gamma_i}{V_{ij}(t)} \psi_i(t) H_{c_{ij}} Y_j(t) \\ & - (\delta_2 - \tau_2(t)) \sum_{j=1}^{N} \frac{\gamma_i}{V_{ij}(t)} \psi_i(t) H_{c_{ij}} Y_j(t) \\ & + \delta_1 \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} h_i(t) \\ & - (\tau_1(t) - \delta_1) \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} h_i(t) \\ & - d_i h_j(t) \\ & i = 1, 2, \cdots, m \\ \dot{h_i}(t) & = f(t, Y_i(t)) - f(t, X_i(t)) \\ & + \tau_2(t) \sum_{j=1}^{N} \frac{\gamma_i}{V_{ij}(t)} \psi_i(t) H_{c_{ij}} Y_j(t) \\ & - \tau_1(t) \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} Y_j(t) \\ & + \delta_1 \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} h_i(t) \\ & + (\tau_1(t) - \delta_1) \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} h_i(t) \\ & i = m+1, m+2, \cdots, N. \end{cases} \tag{15}$$

Next, we set up a Lyapunoy function $V(t, h(t))$:

$$\begin{aligned} V(t, h(t)) = & \frac{1}{2} \sum_{i=1}^{N} h_i^T(t) h_i(t) + \sum_{i=1}^{N} \frac{1}{2 q_i} (d_i - d)^2 \\ & + \frac{1}{2} (\breve{\delta}_1 - \delta_1)^2 + \frac{1}{2} (\breve{\delta}_2 - \delta_2)^2, \end{aligned} \tag{16}$$

where d is an undetermined positive constant. Taking the derivative of $V(t, h(t))$, based on (16) d exists and is large enough to satisfy $E\{\dot{V}(t, h(t))\} \le 0$. This means that synchronization between the drive network and the response network is achieved:

$$\begin{aligned} E\{\dot{V}(t, h(t))\} = & \sum_{i=1}^{N} h_i^T(t) [f(t, Y_i(t)) - f(t, X_i(t)) \\ & + \delta_1 \sum_{j=1}^{N} (\alpha_i \Pi_{ij} + \beta_i \Lambda_{ij}(t)) b_{ij} h_i(t) \\ & - (\breve{\delta}_1 - \delta_1) \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \beta_i \Lambda_{ij}(t)) b_{ij} Y_j(t) \\ & - (\breve{\delta}_2 - \delta_2) \sum_{j=1}^{N} \frac{\gamma_i}{V_{ij}(t)} \psi_i(t) H_{c_{ij}} Y_j(t)] \\ & - \sum_{i=1}^{N} d_i h_i^T(t) h_i(t) + \sum_{i=1}^{N} (d_i - d) h_i^T(t) h_i(t) \\ & - \sum_{i=1}^{N} (\breve{\delta}_1 - \delta_1) h_i^T(t) \sum_{j=1}^{N} (\alpha_i \Pi_{ij}(t) + \\ & \beta_i \Lambda_{ij}(t)) b_{ij} Y_j(t) \\ & + \sum_{i=1}^{N} (\breve{\delta}_2 - \delta_2) h_i^T(t) \sum_{j=1}^{N} \frac{\gamma_i}{V_{ij}(t)} \psi_i(t) H_{c_{ij}} Y_j(t). \end{aligned} \tag{17}$$

V. FEASIBILITY ANALYSIS

We use the random validation method to examine the model's inference accuracy. Each time, we randomly take a subset of M nodes from N nodes as the target and use the rest of the $N - M$ nodes as sources. In order to verify the effectiveness of our approach, we implemented our method on a testbed.

The testbed experiment contained M = 10 sensor nodes set up as multihop self-organizing WSNs. As shown in Fig. 1, nodes s_{ij} and $u_i \in V_i, u_j \in V_j$ are neighbors. In the time of t_1, after node u_i broadcasts a signal, it can be considered that all the neighbors of u_i receive the signal simultaneously, as the packet receiving time is short. In Fig. 1, the solid line arrow represents the topological structure and the dotted line arrow refers to the delay between clusters. u_i and u_j record the logical clock and the hardware clock upon receipt of the packet. These nodes can evaluate the clock of another party according to the received reports of other nodes. The coupling matrix can be obtained from Fig. 1.

$$B = \begin{bmatrix} -3 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -5 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & -3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & -5 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 \end{bmatrix}, \tag{18}$$

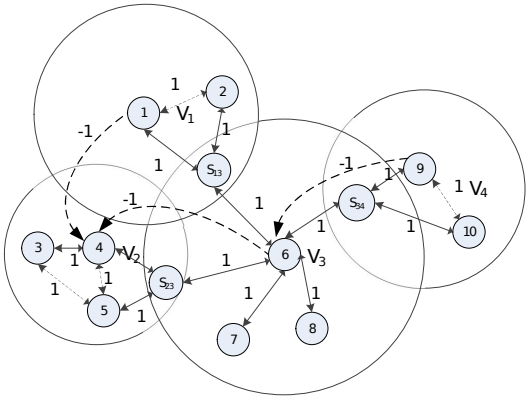


Fig. 1. Network topology analysis diagram.

$$C=\begin{bmatrix} -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 7 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & -5 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix}. \quad (19)$$

Generally, the replaceability of an intermediate node that connects its two-hop neighbors in the sensor network has a greater impact on the synchronization degree than the clock delay between them. Additionally, the clock drift between them has less impact on the topology degree than the clock delay between them. It can be taken from the state equation that

$$\Pi_{ij}(t)=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0.6 & 0.4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.9 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0.3 & 0.3 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0 \\ 0 & 0.2 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0.6 & 0 \\ 0 & 0 & 0.2 & 0.2 & 0.1 & 0 & 0 & 0 & 0.6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.1 & 0.1 & 0.1 & 0 & 0.2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0.9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad (20)$$

$$\Lambda_{ij}(t)=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0.3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.2 & 0.2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.3 & 0.2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0 & 0 \\ 0.3 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0 \\ 0 & 0.2 & 0.3 & 0 & 0 & 0 & 0 & 0 & 0.3 & 0 \\ 0 & 0 & 0.2 & 0.3 & 0.2 & 0 & 0 & 0 & 0.3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.5 & 0.3 & 0.3 & 0 & 0.1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.1 & 0 \end{bmatrix}. \quad (21)$$

Assuming that $\alpha_i = 0.2$, $\beta_i = 0.3$, and $\gamma_i = 0.5$, $i = 1, 2, \cdots, 10$, we used TPSN to test the performance of time evolution, and obtained $\Pi_{ij}(t)$, $\Lambda_{ij}(t)$ and $1/V_{ij}(t)$.

$$\frac{1}{V_{ij}(t)}=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.3 & 0.4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.6 & 0 \\ 0.2 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 \\ 0 & 0.2 & 0.3 & 0 & 0 & 0 & 0 & 0 & 0 & 0.4 \\ 0 & 0 & 0.2 & 0.2 & 0.2 & 0 & 0 & 0 & 0.4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.3 & 0.2 & 0.2 & 0 & 0.1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0 \end{bmatrix}. \quad (22)$$

By considering nodes in a complex network as a Lorenz system, the dynamic equation can be set up as

$$f(t, X_i(t))=\begin{cases} a(X_{i2}(t) - X_{i1}(t)) \\ cX_{i1}(t) - X_{i2}(t) - X_{i1}(t)X_{i3}(t) \\ -bX_{i3}(t) - X_{i1}(t)X_{i2}(t) \end{cases}, \quad (23)$$

where $a = 10$, $b = 8/3$, and $c = 28$. Assuming that the random coupling intensities of the time synchronization and topology control network, $\tau_1(t)$ and $\tau_2(t)$, are normally distributed, the relevant mathematical expectation and variance are $\delta_1 = 10$, $\delta_2 = 3$, $\sigma_1 = 0.46$, and $\sigma_2 = 0.27$. From the features of the normal distribution, we know that almost all $\tau_1(t)$ satisfied $\tau_1(t) \in (\delta_1 - 3\delta_1, \delta_1 + 3\delta_1)$, that is, $\tau_1(t) \in (8.34, 12.1)$ and $\tau_2(t) \in (1.18, 3.12)$.

The error state curves of the nodes from the time synchronization and topology control system with adaptive coupling strength are shown in Figs. 2 and 3.

The curves of the error state of the 10 nodes in the complex network of time synchronization and topology control with self-adaptive coupling intensity are shown in Figs. 2 and 3. Fig. 2 shows that the error between the first states of the corresponding nodes in the two systems is nearly 0 after t = 10. This means that the first states of the nodes in the system achieve complete synchronization. Fig. 3 shows the curves of error change for the 2nd and 3rd states of the corresponding nodes. It can be seen that when t is infinite, the corresponding nodes in the system can achieve complete synchronization. This means that the framework proposed in this paper is feasible.

VI. LARGE-SCALE DEPLOYMENT AND PERFORMANCE EVALUATION

A. Experiment Environments

In order to test the real-world effects of the coupling cooperation model of time synchronization and the topology control of WSNs, this paper applied the model to a sensor network with 200 nodes (including four clusters) on the campus of Suzhou Vocational University, as demonstrated in Fig. 5.

We examined the performance of our method in a variety of scenarios to demonstrate the efficiency of the method. The scenarios included comparisons with RBS and TPSN regarding the

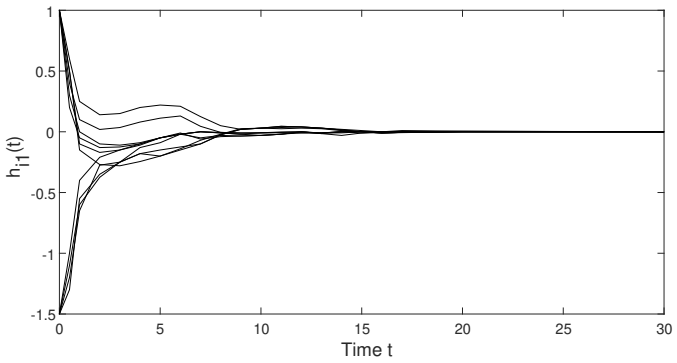


Fig. 2. Time track of $h_{i1}(t)(i = 1, 2, \cdots, 10)$ in the synchronous security controller.

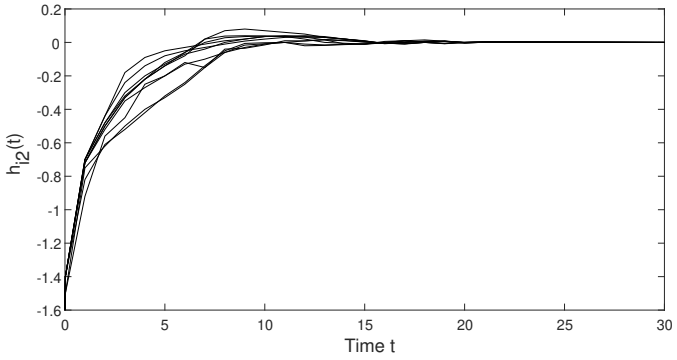


Fig. 3. Time track of $h_{i2}(t)(i = 1, 2, \cdots, 10)$ in the synchronous security controller.

Fig. 4. Real-world system graph.

depth of network topology and cost, as well as the synchronization efficiency of the number of neighbors.

B. Performance Evaluation

We evaluated the performance of our model in terms of time synchronization and topology control by testing each scenario in the experiments. For each 50-node synthetic graph, we implemented the Security Cooperation Collection Tree Protocol (SC-CTP), which is embedded into our model. Experiments with an identical setup were also performed for the RBS and TPSN algorithms. We then compared the three approaches. In order to create a general comparison, we ran the algorithms five times

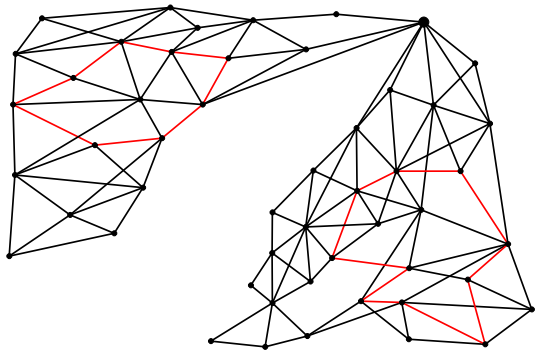


Fig. 5. Fifty node experiment.

for each cluster graph. We then used the average result of the 20 experiments as the performance indicator. During the test process, we manually entered factors from three categories: the signal intensity, the weight of the synchronization controller, and the power level. We also manually selected factors for: the attack interference, the threshold of time synchronization accuracy, and the signal intensity.A routing loop was also artificially set up. There are three incoordination scenarios in synchronization sensor nodes: nodes that cause network congestion and data loss, neighboring nodes that form routing loops, and communication resource competition nodes.

In our experiments, we used TPSN and RBS to test the performance of both the SC-CTP and Collection Tree Protocol (CTP) algorithms. The results are shown in Figs. 6(a) and (b) and Figs. 6(c) and (d). The SC-CTP algorithm found the nodes with the shortest synchronization time and the fewest hops through TPSN, and the routing loop was broken because the link between nodes disconnected. We can observe that, using our approach, the skew of TPSN improved by almost 11 μs, while RBS was improved by almost 5 μs.

The node degree constraint in the SC-CTP was added to the optimization function. The node degree can help to balance the power consumption and reduce interference throughout the network. The node degree is inversely proportional to topological coupling intensity. As can be seen in Fig. 6(a)(b), the average node degree of the SC-CTP algorithm is smaller than that of the CTP algorithm. For CTP, the node degree has an almost linear increase with the number of nodes.

We used RBS and TPSN to test the depth-first traversal of both the SC-CTP and CTP algorithms. The results show that the global and local traversal times improved in the SC-CTP, and the depth of the network topology was also shallower than CTP. The probability of the network forming with a depth of less than 3, less than 4, and less than 5 was respectively 33%, 29%, and 8%. We can see that structure of the coupling tree in the coupling cooperation model has a greater capacity to tolerate the missing connected nodes when broadcasting the RBS protocol package. We can see that the structure of the coupling tree of the coupling cooperation model has a large deviation-tolerant capacity to broadcast the RBS protocol package to connecting nodes. The external cluster packet that switches from one node to the cluster's peripheral nodes is certainly acyclic, because they are determined by the controller of the region, this

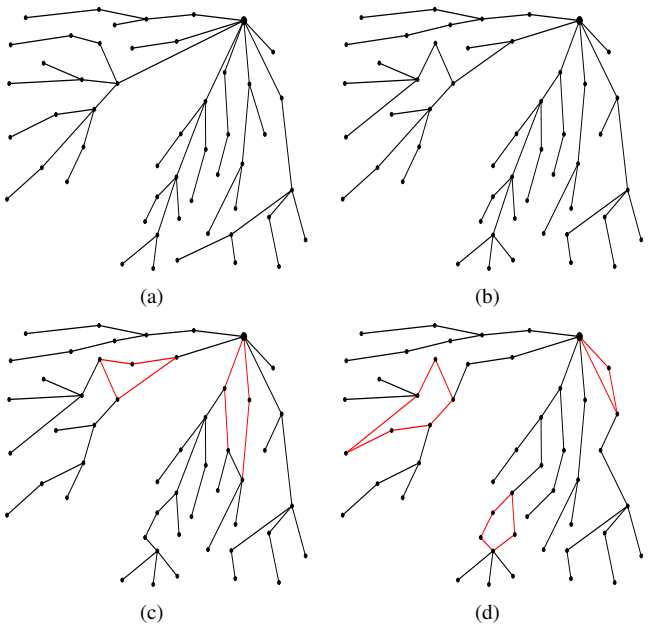


Fig. 6. Evaluation of SC-CTP and CTP in topology control, time synchronization performance: (a) TPSN test the performance of SC-CTP, (b) RBS test the performance of SC-CTP, (c) TPSN test the performance of CTP, and (d) RBS test the performance of CTP.

can be seen from the depth-first traversal of the zonal topological graph. The traversed cluster list field contains the sequence of clusters that one particular syn-route-select synchronization message has traversed. A syn-route-select message cannot be propagated within a cluster more than once. This avoids loops. In inter-cluster communication, if the synchronization controller of a cluster receives a syn-route-select message from more than one of its nodes corresponding to the same destination, then it sends a syn-route-reply to the one with the highest topological coupling intensity. The topological coupling intensity is the combination of the residual energy, channel interference, channel congestion, transmission speed, and synchronization accuracy.

As the number of neighbor nodes increases, the colony synchronization between the depth of the topological structure, the signal intensity, the clock drift, and the clock delay becomes greater. When network topology changes occur, the coupling area between neighbors changes automatically, and corresponding nodes are required to assess the time synchronization. This enables the coupling cooperation system to greatly reduce the maintenance costs of the coupling tree to avoid the impact of the network topology. This verifies that the SC-CTP method is superior to other single factor methods.

We can see from Fig. 7 that if two different protocols, CTP and SC-CTP, are operated in a test platform with more than 50 nodes, when the number of neighbor nodes is 16, CTP can only identify 59% of the neighbor nodes, while SC-CTP can identify 81% of the neighbor nodes. The synchronization efficiency of neighbor nodes increases to 22% on average and the synchronization efficiency of SC-CTP increases. As the node number increases. SC-CTP can identify and synchronize about 88% of neighbor communication resources.

Fig. 8 shows the energy consumption of CTP and that of

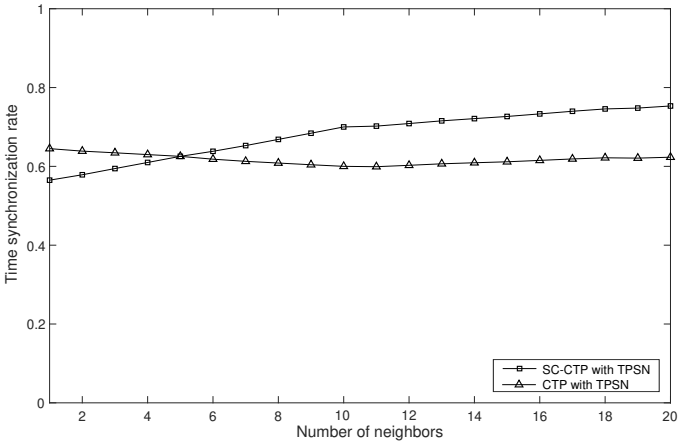


Fig. 7. Comparison of model accuracy.

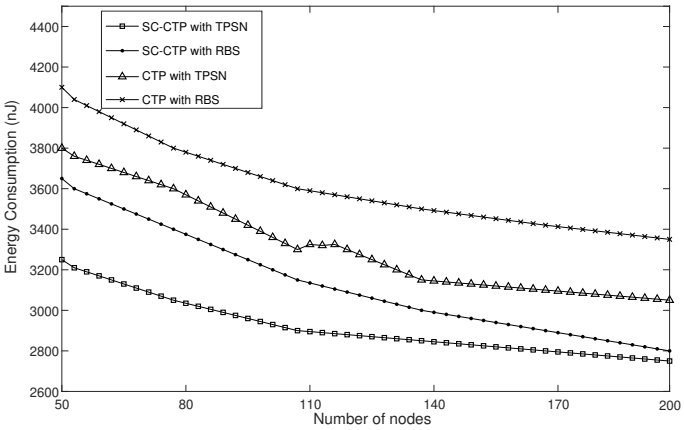


Fig. 8. Energy consumption of nodes 50 to 200.

SC-CTP with RBS and TPSN. The curves are not as smooth, because the calculation of the data load for the algorithm is achieved by a discrete method. The energy consumption in SC-CTP is not bigger than that in CTP with either RBS or TPSN, because SC-CTP and CTP use different selection mechanisms for synchronization control. As the number of nodes increases, the gap between them becomes larger. The reason for this is that the waiting time mechanism in the new algorithm chooses nodes with high coupling strength and many targets, which reduces the energy cost. Additionally, the number of common target nodes covered by different clusters decreases. Energy consumption in the intercluster decreases because the degree and depth of nodes decreases. The data load decreases in the external cluster are caused by more nodes reaching the sink immediately, due to the larger broadcast radius. Thus, nodes in the intercluster do not have to forward as much data as in CTP.

Figs. 9 and 10 show the average and maximum data loss rates for single node failures. The maximum and average data loss of the CTP method are greater than those of the SC-CTP algorithm. This is because the CTP method does not consider the depth of the tree and the transmission path problem between the node and the sink. As can be seen from Fig. 10, the key node failures of the CTP method may result in a loss of up to 40% of perceived

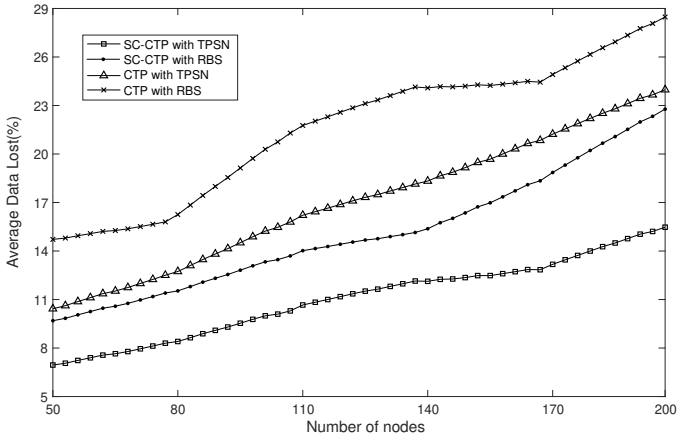


Fig. 9. Average data loss of nodes 50 to 200.

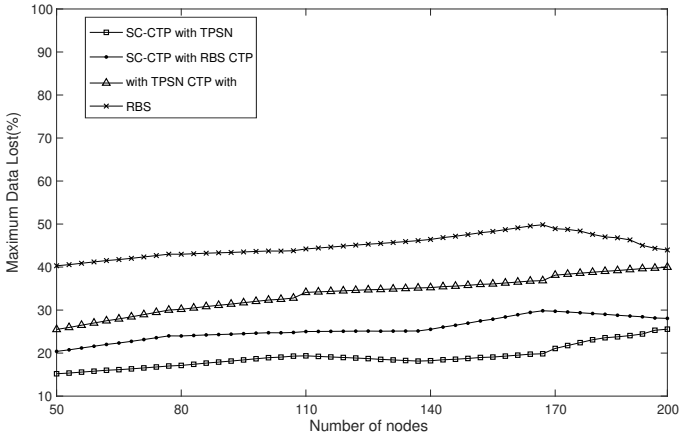


Fig. 10. Maximum data loss of nodes 50 to 200.

data.

In terms of reliability gain, more disjoint paths are needed to meet the network reliability requirements in multihop communication. SC-CTP has obvious advantages, especially for large-scale networks, which can be adapted to a network environment with a high packet loss rate. However, CTP clearly cannot meet the reliability requirements of large-scale multihop network communication. In terms of energy consumption, CTP consumes more energy.

Fig. 11 shows the impact of the network size on the time synchronization delay. SC-CTP outperforms CTP, and TPSN performs even better. The SC-CTP broadcast delay is reduced by 12.3%, because the reduction in transmission leads to a decrement in delay, and SC-CTP can provide a broadcast tree with less depth and a lower degree. The delay of both schemes is not related to the network size, because even though a high network size requires many transmissions, it also brings high transmitting parallelism.

VII. CONCLUSION

This paper presents the dynamic behavior of time synchronization and topology control cooperation of WSNs in a complex network with attack delays. The topology control and

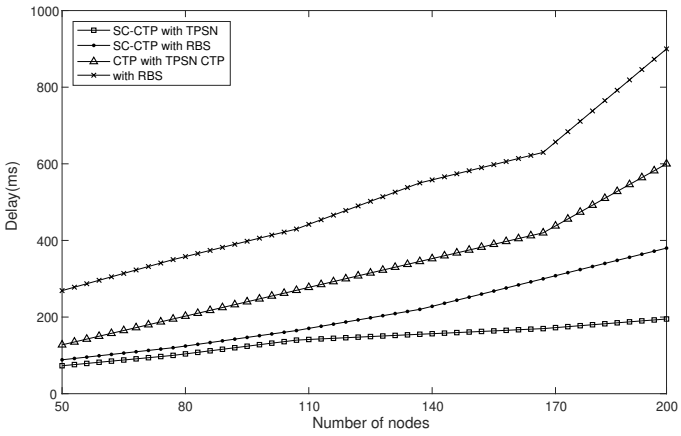


Fig. 11. The impact of the network size

time synchronization issues were studied in two different complex networks with a random coupling intensity based on the Lyapunov stability theory and Schur lemma. Sufficient conditions for partial synchronization of the complex network were acquired. The two networks were able to achieve synchronization using the weights and number of goal controllers. To overcome the difficulties caused by delay and diffusion effects, novel time-synchronization-based adaptive strategies were proposed based on coupling weights. By specifying the coupling strength, some criteria based on the coupling configuration matrix were derived to justify exponential synchronization. The coupled controller was proven to be related to the signal strength, clock drift, and clock delay during attacks. We can see from the above that the coupling time synchronization state of the topological link in large-scale WSNs is jointly determined by the dynamic system of the single nodes, $f(\cdot)$,$(\alpha_i, \beta_i, \gamma_i)$,$(\Pi_{ij}(t), \Lambda_{ij}(t), 1/V_{ij}(t))^T$; matrixes H,B, and C; and ψ. These parameters are easily affected by attack interference. The experiments performed in this study showed that for a complex network with a topology switch, the achievement of synchronization is closely related to the topological structure of each attack interference mode. The method can effectively restrict the behavior of the packets under replay attack, the abnormality of packets in forgery attacks derived from malicious nodes, and it can reduce the node trust value and increase the security and reliability of the wireless sensor network. In the future work, we will attempt to expand the method of synchronization to complex and dynamic networks with internal time delay and coupling time delay. Such dynamic network are common in the real world, especially in biological networks and neural networks. This will be challenging and interesting work.

REFERENCES

[1] D. Sikeridis, E. E. Tsiropoulou, M. Devetsikiotis, and S. Papavassiliou, "Wireless powered public safety IoT: A UAV-assisted adaptive-learning approach towards energy efficiency," *J. Netw. Comput. Applicat.*, vol. 123, pp. 69–79, Sept. 2018.

[2] F. Ahmad, A. Adnane, V. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies," *Sensors*, vol. 18, no. 11, 2018.

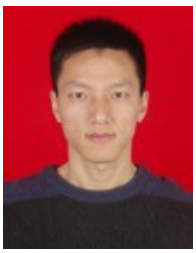
[3] M. Safkhani and M. Shariat,"Implementation of secret disclosure attack

against two IoT lightweight authentication protocols," *J. Supercomputing*, vol. 74, no. 11, pp. 6220–6235, Aug. 2018.
[4] H. Zhao, L. Li, H. Peng, J. Xiao, and Y Yang, "Finite-time topology identification and stochastic synchronization of complex network with multiple time delays," *Neurocomputing*, vol. 219, pp. 39–49, Jan. 2017.
[5] H. Lin, D. Bai, D. Gao, and Y. Liu, "Maximum data collection rate routing protocol based on topology control for rechargeable wireless sensor networks," *Sensors*, vol. 16, no. 8, p. 1201, 2016.
[6] J. Almeida, C. Silvestre, and A. Pascoal, "Synchronization of multi-agent systems using event-triggered and self-triggered broadcasts," *IEEE Trans. Autom. Control*, vol. 62, no. 9, pp. 4741–4746, Sept. 2017.
[7] P. M. Wightman and M. A. Labrador, "A3: A topology construction algorithm for wireless sensor networks," in *Proc. IEEE GLOBECOM*, Nov. 2008, pp. 1–6.
[8] T. Qiu, X. Wang, C. Chen, M. Atiquzzaman, and L. Liu. "TMED: A spider web-like transmission mechanism for emergency data in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8682–8694, 2018.
[9] G. Liu and X. Xu, "Analysis on controlled synchronization ability of non-dissipate coupled complex network," *J. Electron. Informat.*, vol. 23, pp. 722–72, 2012.
[10] Y. Zhang, J. He, J. Xu, B. Zhao, and F. Cai, "Dynamic optimal planning of path of mobile nodes," *J. Beijing Univ. Technol.*, vol. 42, no. 6, pp. 851–855 ,June 2016.
[11] T. Qiu, R. Qiao, and D. O. Wu, "EABS: An event-aware backpressure scheduling scheme for emergency Internet of things," *IEEE Trans. Mobile Comput.*, vol. 17, no. 1, pp. 72–84, 2018.
[12] C. H. Yeh, "The heterogeneous hidden/exposed terminal problem for power-controlled ad hoc MAC protocols and its solutions," in *Proc. IEEE VTC*, May. 2004, pp. 2548–2554.
[13] J. He, S. Ji, R. Beyah, Y. Xie and Y Li, "Constructing load-balanced virtual backbones in probabilistic wireless sensor networks via multi-objective genetic algorithm," *Trans. Emerging Telecommun. Technol.*, vol. 26, no. 2, pp. 147–163, 2015.
[14] G. Dhand and S. S. Tyagi, "SMEER: Secure multi-tier energy efficient routing protocol for hierarchical wireless sensor networks," *Wireless Personal Commun.*, vol. 105, pp. 17–35, 2019.
[15] T. M Chiwewe and G. P. Hancke, "A distributed topology control technique for low interference and energy efficiency in wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 8, no. 1, pp. 11–19, Feb. 2012.
[16] K. Junseok, J. Shin, and Y. Kwon. "Adaptive 3-dimensional topology control for wireless ad-hoc sensor networks." *Ieice Trans. Commun.*, vol. E93.B, no. 11, PP. 2901–2911, 2010.
[17] S. He, L. Ji, Y. Pan, and S. Li, "Approximation algorithms for load-balanced virtual backbone construction in wireless sensor networks," *Theoretical Comput. Science*, vol. 507, pp. 2–16, Oct. 2013.
[18] A. N. Uwaechia, and N. M. Mahyuddin, "Collaborative framework of algorithms for sparse channel estimation in OFDM systems," *IEEE J. Commun. Netw.*, vol. 20, no. 1, pp. 9–19, Feb. 2018.
[19] J. A. Torkestani, "An adaptive backbone formation algorithm for wireless sensor networks," *Comput. Commun.*, vol. 35, no. 11, pp. 1333–1344, June 2012.
[20] K. Pratyay, K. G. Suneet, and K. J, Prasanta, "A novel evolutionary approach for load balanced clustering problem for wireless sensor networks," *Swarm and Evolutionary Comput.*, vol. 12, pp. 48–56, Oct. 2013.
[21] J. Wang, D. Wei, Z. Cao, and Y. Liu, "On the delay performance in a large-scale wireless sensor network: measurement, analysis, and implications." *IEEE/ACM Trans. Netw.*, vol. 23, no. 1, pp. 186–197, Feb. 2015.
[22] G. Brandner, U. Schilcher, and C. Bettstetter, "Firefly synchronization with phase rate equalization and its experimental analysis in wireless systems." *Comput. Netw.*, vol. 97, pp. 74–87, Mar. 2016.
[23] J. Elson, L. Girod, and D. Estrin, "Fine-grained network time synchronization using reference broadcast," in *Proc. USENIX*, Dec. 2002, pp. 147–163.
[24] D. Djenouri, "R4Syn: Relative reference receiver/receiver time synchronization in wireless sensor networks," *IEEE Signal Process. Lett.*, vol. 19, no. 4, pp. 175–178, Apr. 2012.
[25] G. Saurabh, K. Ram, and M. B. Srivastava, "Timing sync protocol for sensor networks," in *Proc. ACM SenSys*, Nov. 2003, pp. 138–149.
[26] S. Rahmatkar and A. Agarwal, "A reference based, tree structured time synchronization approach and its analysis in WSN," *Int. J. Ad Hoc Sensor Ubiquitous Comput.*, vol. 2, no. 1, pp. 20–31, Mar. 2011.
[27] M. Maróti, B. Kusy, G. Simon, and A. Ledeczi, "The flooding time synchronization protocol," in *Proc. ACM SenSys*, Nov. 2004, pp. 39–49.
[28] J. Shannon, H. Melvin, and A. G. Ruzzelli, "Dynamic flooding time synchronisation protocol for WSNs," in *Proc. IEEE GLOBECOM*, Dec. 2012, pp. 365–371.
[29] T. Preetha and A. W. Kevin, "Topology control of tactical wireless sensor networks using energy efficient zone routing," *Digital Commun. Netw.*, vol. 2, no. 1, pp. 1–14, Feb. 2016.
[30] Q. Zhao and N. Yukikazu, "Topology management for reducing energy consumption and tolerating failures in wireless sensor networks," *Int. J. Netw. Comput.*, vol. 6, no. 1, pp. 107–123, Jan. 2016.
[31] Y. L. Xing, Y. R. Chen, W. D. Yi, and C. H. Duan, "Time synchronization for wireless sensor networks using adaptive linear prediction," *Int. J. Distributed Sensor Netw.*, vol. 2015, no. 22, pp. 1–9, Jan. 2015.
[32] A. R. Swain and R. C. Hansdah, "A model for the classification and survey of clock synchronization protocols in WSNs," *Ad Hoc Netw.*, vol. 27, pp. 219–241, Apr. 2015.
[33] J. Wu, L. Zhang, Y. Bai, and Y. Sun, "Cluster based consensus time synchronization for wireless sensor networks," *IEEE Sensors J.*, vol. 15, no. 3, pp. 1404–1413, Mar. 2015.
[34] T. Qiu, H. Wang, K. Li, H. Ning, A. K. Sangaiah, and B. Chen. "SIGMM: A novel machine learning algorithm for spammer identification in industrial mobile cloud computing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2349–2359, Apr. 2019.
[35] R. L. Deng, S.B. He, P. Cheng, and Y. X. Sun, "Towards balanced energy charging and transmission collision in wireless rechargeable sensor networks," *J. Commun. Netw.*, vol. 19, no. 4, pp. 341–350, Aug. 2017.

Zhaobin Liu is a Professor of School of Computer Engineering, Suzhou Vocational University, heading the Department of IoT Technology. He received his M.S. degree in Computer Science and Technology from Xian Jiaotong University in 2005. His research interest includes pervasive computing, wireless sensor network, and network security. He is a Member of the CCF and the ACM.

Wenzhin Liu received her BS degree in Telecommunications and Information Engineering from Nanjing University of Posts and Telecommunications in 1998, and M.S. degree in Radio Physics from Lanzhou University in 2001. Her research interest includes wireless communication and wireless sensor network. She is a Member of the CCF.

Qiang Ma received his BS degree in Department of Computer Science and Technology from Tsinghua University in 2009, and Ph.D. degree in Department of Computer Science and Engineering at the Hong Kong University of Science and Technology in 2013. He is now a Assistant Researcher in Tsinghua University. His research interests include sensor networks, mobile computing, and privacy protection.



GANG LIU is a Lecturer in the School of Computer Engineering, Suzhou Vocational University. He received his Ph.D. in Computer Science and Technology from Nanjing University of Science and Technology in 2014. At present, his research interest includes wireless sensor network, software engineering and information security.

Liang Zhang received his B.S. degree in 2005 and the M.S. degree in 2008 in Computer Science both from Soochow University. He is currently a Ph.D. student in Department of Control Science and Engineering of Tongji University. His research interest includes multi-/many-objective optimization, large-scale optimization, model based evolutionary algorithms, and swarm intelligence.

Ligang Fang received his M.S. degree in 2003 in Remote Sensing and GIS and his Ph. D degree in Environmental Science in 2007 from Graduate University of Chinese Academy of Sciences, Beijing. He has been working in department of Computer Engineering, Suzhou Vocational University since August 2007 and was as a Professor in 2018. His research interest includes environmental remote sensing, sensor network and environment modeling.

Victor S. Sheng received his M.S. degree in Computer Science from the University of New Brunswick, Canada, in 2003, and his Ph.D. degree in Computer Science from Western University, Ontario, Canada, in 2007. His research interests include data mining, machine learning, and related applications. He is a Senior Member of IEEE and a Lifetime Member of ACM.