International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/218510 Volume 10, Issue 1, January – February (2023)

RESEARCH ARTICLE

Resilient Consensus-Based Time Synchronization with Distributed Sybil Attack Detection Strategy for Wireless Sensor Networks: A Graph Theoretic Approach

Suresh Kumar Jha
Department of Computer Science and Engineering, MBM University, Jodhpur, Rajasthan, India.
suresh.jha84@gmail.com

Anil Gupta
Department of Computer Science and Engineering, MBM University, Jodhpur, Rajasthan, India.
anilgupta@jnvu.edu.in

Niranjan Panigrahi
Department of Computer Science and Engineering, PMEC, Berhampur, Odisha, India
niranjan.cse@pmec.ac.in

Received: 20 November 2022 / Revised: 03 January 2023 / Accepted: 06 January 2023 / Published: 26 February 2023

Abstract – Security attacks on time synchronization services prevent the Wireless Sensor Networks (WSNs) from operating consistently and possibly cause the system to go down entirely. One of the most vulnerable attack types where a node falsely assumes many identities is the Sybil attack. Despite receiving a lot of attention for their simplicity and distributed nature, consensus-based time synchronization (CTS) algorithms in WSN do not exhibit robust behavior when subjected to a Sybil attack. In this context, a message-level Sybil detection mechanism, the Sybil resilient consensus time synchronization protocol (SRCTS), is proposed using a graph-theoretic approach. A novel distributed mechanism based on connected component theory is proposed to detect and filter Sybil messages. The comparison has been shown with Robust and secure Time Synchronization Protocol (RTSP) and Node-identification-based secure time synchronization protocols (NiSTS) for detection and convergence speed. The Sybil message detection rate is improved by 6% as compared to SRCTS vs RTSP and by 14% as compared to SRCTS vs NiSTS. Simulation results exhibit that the SRCTS algorithm is 62% more effective as compared to NiSTS and 45% more efficient than RTSP in terms of convergence rate. An in-depth mathematical analysis is presented to prove the correctness of the algorithms, and the message complexity is proven to be $O(n^2)$. The algorithm is validated through extensive simulation results.

Index Terms – Connected Components, Consensus-Based Time Synchronization (CTS), Graph Theory, Sybil Attack, Wireless Sensor Network, Message Graph, Conformance Property.

1. INTRODUCTION

The WSNs are major backbones for many recent technologies, viz., the Internet of Things (IoT) and Cyber-Physical Systems (CPS). A critical need for the smooth working of the underlying WSN backbone is time synchronization. All nodes must have synchronized clocks to run several applications. A plethora of research on this issue has been carried out for the last decade because the wireless network, poses additional challenges with time synchronization [1].

There are two basic categories in which the literature on time synchronization for WSN can be divided: (i) centralized, and (ii) distributed. The centralized approach uses a tree-based mechanism for time synchronization, where one root node is connected to many leaf nodes hierarchically, and each node performs single or multi-hop communication to synchronize with the root node. This method has a major drawback: if the root node fails or becomes corrupt, a new root-election operation must be started, which causes a delay in network synchronization [2]. The distributed approach for time synchronization is solely dependent on consensus theory [3] for time synchronization and has many advantages in fault tolerance, location determination and proximity of deployed sensor networks, scheduling of sleep periods to increase

RESEARCH ARTICLE

energy efficiency, and coordination of the network among various nodes [4].

Recently, distributed consensus-based time synchronization (CTS) protocols have gained attention in which each node communicates with its neighbors, applies some averaging principle, and converges to one value or the consensus value, which is also called the consensus-based approach [5][6]. Though CTS algorithms are robust to any type of security attack, their behavior under a Sybil attack is not resilient, and detecting a Sybil attack at the synchronization message level is an NP-hard problem. To this end, the followings are the major contributions of this work:

- Proposes a novel graph-theoretic-based approach using the connected component principle on time synchronization messages for the detection of Sybil messages, based on conformance property.
- A thorough & precise mathematical analysis is presented to prove the correctness and message complexity of the algorithm.
- An extensive simulation is carried out to validate the algorithm.

The remaining section of this paper is presented as follows: The related work is explored in Section 2. Section 3 highlights system models and problem formulation. We propose the SRCTS algorithm under the proposed strategy in Section 4. The detailed mathematical analysis is done in Section 5. Section 6 presents the simulation's findings. The paper is finally concluded in Section 7.

2. RELATED WORK

This section contains a systematic description of some major works on secure consensus-based time synchronization algorithms. In centralized synchronization, all sensor nodes synchronize their clocks to a reference source [7]-[8]. The author proposed two durable clock synchronization techniques: level and diffusion. The techniques tackle various attacks by using the median value of differences in numerous referred clocks as the base of clock deviation [9]. However, it is unable to defend against delay and wormhole attacks.

A more secure and optimal method of synchronization for sensor networks of heterogeneous type was demonstrated by using PKC (public-key cryptography) is used to protect against a variety of attacks. The strategy necessitates additional communication and storage overhead as every node is required to store the other node's keys [10]-[11].

The authors in [12] developed a series of methods for secure pair-wise and group-based synchronization to counter the delay attack. To minimize the overhead of each node, the authors have used a cryptographic method using a pairing mechanism to make the time synchronization secure, considering both homogeneous and heterogeneous type WSNs. Each node in distributed synchronization uses the clock information of its neighbor to accomplish synchronization with one another in the absence of a specific topology [13].

There have also been several proposals for secure distributed synchronization protocols. To build attack-tolerant time synchronization, Hu et al. have used a correlation mechanism on the temporal domain among nearby nodes, i.e., the hardware clock's linearity. The skew parameter on the other hand is not adjusted [14].

He et al. [15] developed secure average-consensus-based time synchronization against message manipulation attacks to take into account clock offset and skew. The hardware clock-checking procedure and the logical clock-checking process are two parts of the checking mechanism. To prevent Sybil attacks, Dong et al. [16] developed a consistent and secure time synchronization technique. The basic concept is to detect abnormalities at the message level using a graph-theoretical method. Instead of isolating problematic nodes, Wang et al. [17] analyzed the timestamp correlation between nodes and the distinctiveness of a node's clock skew to detect inaccurate information.

Each node uses the relative skew regarding its public neighbor as the basis for determining the accuracy of the information and filtering out false messages during the detection phase. Zheng et al. [18] suggested a new attack model based on the Sybil nodes' features. To locate and disable Sybil nodes in the network, a transmission mechanism based on quantized data was also created. The next step was to create an attack-resistant consensus mechanism where each normal node provides quantitative data information to its neighbors along with a distinct label created from shorter data gathered by sampling from the common distribution.

Wu et al. [19] created a deception attack strategy by creating an event-triggered update rule that can minimize computation and communication utilization while minimizing the impact of attackers. By determining whether or not its neighbor set fulfills a particular cardinality-dependent function, each node selects the instances to update its state information.

Wang et al. [20] address the robust consensus problem in multi-agent systems that are under attack, where the attacker can eavesdrop on initial information from the system's agents and change the values in the communication connections to impede the consensus process. To safeguard the privacy of node values, they use homomorphism encryption cryptography to encrypt each agent's initial integer state without revealing the network's true value to other agents. A variant of the so-called ratio consensus technique was proposed to deal with malicious attacks once the communication network satisfies the required connectivity

RESEARCH ARTICLE

with malicious attacks once the communication network satisfies the required connectivity.

Jamshidi et al. [21] proposed detecting Sybil nodes using neighbor information and observer nodes over the network lifetime. First, certain observer nodes traverse the network and collect the data about other nodes required by the suggested approach. The acquired information is then used by each observer node to discover Sybil nodes. The suggested algorithm is compared to other algorithms using memory, communication, and compute overhead as criteria. A secure consensus challenge for nonlinear multi-agent systems with attackers and bounded communication delays was researched by Wu et al. [22].

The literature survey mentioned above shows that the majority of works have focused on security issues in centralized time synchronization protocols for WSNs. Though recent time synchronization approaches are based on consensus theory and are proven to be robust to many types of security attacks due to their distributed nature, the CTS protocols are still vulnerable to Sybil attacks. As far as we are aware, relatively few works have taken into account the Sybil attack in CTS protocols and Sybil attack detection at the time synchronization message level is still an intractable problem.

The purpose of this review is to examine the composition studies of state-of-the-art CTS algorithms and research trends with security being a key concern for WSN. Regarding potential security risks in wireless sensor network time synchronization, the following findings are made:

1. The fundamental problem with wireless sensor networks is synchronization because they are distributed systems without a centralized physical clock.
2. The energy and storage capabilities of sensor nodes are constrained. As a result, the standard cryptography approach is inadequate because it involves greater overhead in the computing process. To tackle security concerns, straightforward and lightweight strategies should be developed.
3. Message manipulation and Sybil attacks are more vulnerable attacks for time synchronization.
4. While SATS exhibits exponential convergence and corrects both skew and offset, the ATS protocol is susceptible to a message manipulation attack.
5. Message manipulation attacks are also possible against the MTS protocol.
6. The SMTS shows that possible message manipulation attacks are to be supported and refuted.
7. The RTSP protocol attempts to identify the Sybil attack using dynamic programming by locating the maximum clique in the graph, but the issue is NP-complete and has a high time complexity of $O(n^2)$.
8. The NiSTS protocol protects against attacks like Sybil and message tampering.

3. SYSTEM MODEL AND PROBLEM FORMULATION

3.1. Block Diagram

This section proposed a block Diagram for Message level Sybil attack detection and Consensus Synchronization methods.

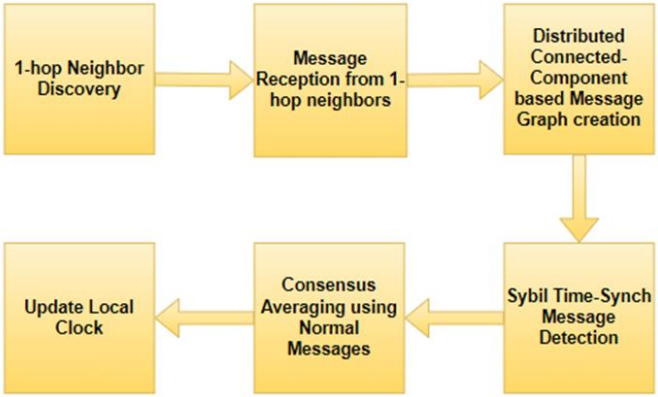


Figure 1 Proposed Block Diagram of SRCTS

The overall block diagram of SRCTS is depicted in Figure 1, which comprises six blocks. The neighbor discovery phase identifies its 1-hop neighbors. The message reception is to be done from each 1-hop neighbor, which can be seen clearly in Figure 5. The message graph is to be created by using a distributed connected component strategy, and the Sybil time sync message has been detected and discarded from the graph as a filtered isolated vertex. The consensus averaging is applied to normal messages, and clock updating is done for convergence analysis.

3.2. Clock Model

A crystal oscillator with a set frequency can estimate the clock with good accuracy over a long period. A sensor node's local hardware clock is approximated is defined as in equation 1.

$$C(t) = \alpha * t + \eta \quad (1)$$

Where t is the reference clock, α is the clock drift and η is the clock offset. The logical clock value represents the synchronized time of a node by modifying the function's coefficients, α, and η.

3.3. Network Model

A distributed WSN can be represented by a weighted graph $G = (V, E)$ where V is the set of nodes, and edge $(i, j) \in$

RESEARCH ARTICLE

E shows that node i and node j have communication [18]. The connectivity of the complete WSN can be demonstrated as an adjacency matrix A of the graph which is defined as in equation 2.

$$a_{ij} = \begin{cases} 1 \text{ if } e_{ij} \in E \\ 0 \text{ otherwise} \end{cases} \quad (2)$$

Using the above adjacency matrix, the weight matrix W can be defined in equation 3.

$$w_{ij} = \begin{cases} d_{ij} \text{ if a ij} = 1 \\ 0 \text{ otherwise} \end{cases} \quad (3)$$

d_{ij} is the distance between two sensor nodes i and j which is computed as described in Algorithm 2.

3.4. Attack Model

In a WSN, a Sybil attack scenario can be modeled as shown in Figure 2. The network has one Sybil node s and other nodes that are safe node. The Sybil node may keep the identity of nodes {g, e, b, d} and share the information among their neighbors.

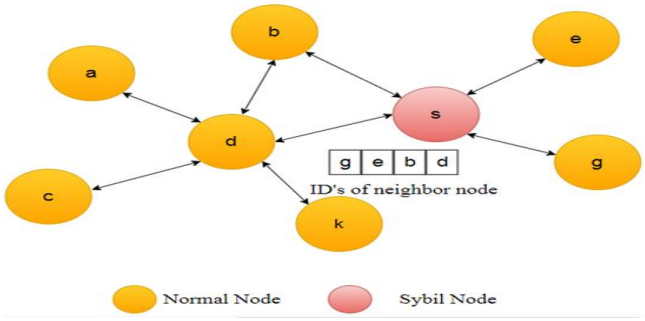


Figure 2 Sybil Attack Model

3.5. Problem Formulation

The objective for the focused problem is to design a distributed mechanism that can differentiate normal time-stamped synchronization messages (Mn) and Sybil messages (Ms) in CTS and each node in the network can filter the attacker's messages to achieve a consensus clock state in the presence of the Sybil attacker nodes. The conformance property [23] is used to design the mechanism. The proposed algorithms, flowchart, and state-transition diagram are presented in the next section.

4. PROPOSED STRATEGY

This section describes the proposed strategy in terms of a state transition diagram, flowchart, and detailed algorithms as given in algorithms 1, 2, and 3.

4.1. State Diagram

The proposed strategy is schematically represented in Figure 3 through a state-transition diagram, and the working principle is shown as a flow chart in Figure 4. In the state transition diagram, there are a total of 9 states shown as circles and labeled with the respective action performed on the messages to differentiate normal messages and Sybil messages.

Following the above scheme and flow principle, the following section describes the detailed algorithms with an explanation referring to Figure 5. Table 1 shows the notations used in the algorithm to understand.

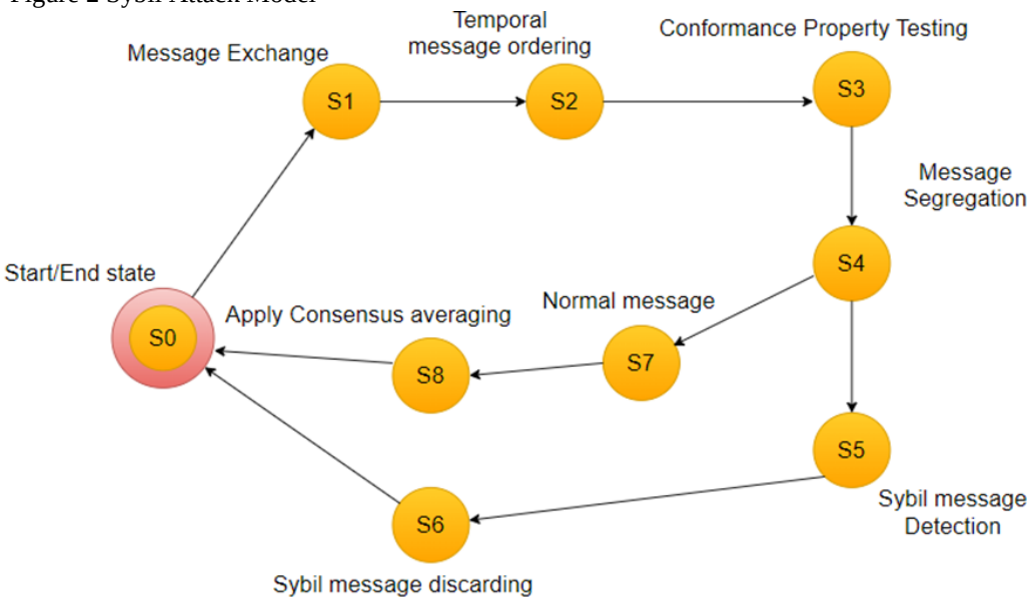


Figure 3 State Diagram of Proposed Work

RESEARCH ARTICLE

Table 1 Notation Definition

S. No	Symbol	Definition
1	NTD	Neighbor Table
2	BUFF_TAB	Buffer Table
3	MC	Message Complexity
4	Mn	Normal Message
5	Ms	Sybil Message
6	Iv	Isolated Vertex
7	d_{ij}	Distance of two nodes
8	Δts	Difference between sending a timestamp
9	Δtr	Difference between receiving a timestamp
10	a_{ij}	Adjacency Matrix
11	bm	Beacon message
12	Mc	Message Complexity

4.2. Flowchart

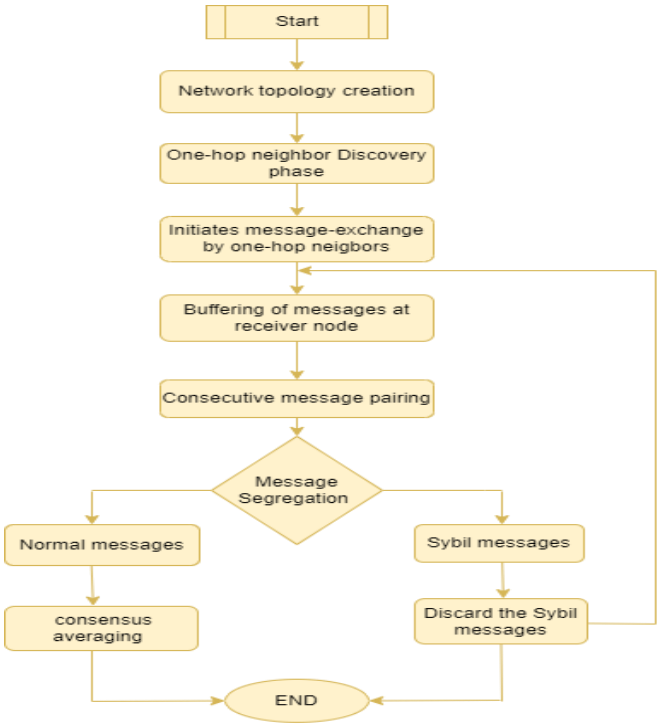


Figure 4 Flowchart of Proposed Work

The overall proposed strategy, which is given in Algorithm 1, consists of some major processes, which are diagrammatically represented as a flowchart given in Figure 4. The strategy starts with the process of discovering one-hop neighbors using Algorithm 2 at each node in the given network topology, which is generated using the network model given in figure 3. During the synchronization process, each node buffers the messages received from its one-hop neighbors. Then each node executes the proposed graph-based strategy, which is given in Algorithm 3, for Sybil message detection and filtration from the normal time synchronization messages.

4.3. Proposed Algorithms

The entire strategy is represented in the form of Algorithm 1, named SRCTS (Sybil Resilient Consensus Time Synchronization Algorithm). It calls Algorithm 2 a sub-procedure for one-hop neighbor discovery. Furthermore, it uses Algorithm 3 for differentiating the normal messages from Sybil messages at each node. Finally, it calls upon Algorithm 4 for average consensus-based time synchronization. The detailed steps of the respective phases are mentioned in the below algorithms.

Input: [Node_set(V_i),i=1,2,....n]
Output: Synchronized clock states ($C_i(t)$)
BEGIN
for all node_id i ∈v
    Call Neighbor_Discovery(V_i) // Algorithm 2
for k=1 to I_{max}
    Call Sybil_Detection(Vi) // Algorithm 3
    CTS(V_i) // Algorithm 4
End for
End for
END
Node i broadcast a beacon message b_m at time stamp t_s, Any node j who receives b_m will reply to a message as t_r

Algorithm 1 Sybil Resilient Consensus Time Synchronization Algorithm

Node i estimates
dij=c*(ts-tr)
if dij<r
then set NTDi[i,j]

Algorithm 2 Neighbor_Discovery(Vi,r)

Input: (NTD, Buffer_Tab)
Output: Sybil message detect at each node
for all node i∈ v_i
node i receives M={m1,m2...mn}
where Mi=t_s^i, $t_{r,}^i$ N_{id}^i
Set Buff_tab[i] ← Mi
//Creation of message graph
$\bar{G}_1 = (\bar{V}1,\bar{E}1)$
Where $\bar{V}1$ = set of messages at node i

RESEARCH ARTICLE

// Create Edge list $\bar{E}_l$ in the message graph
for i: 1 to n do
msgpair(Mi,Mi+1) //Consecutive messages
estimate
Δts= ts(Mi+1)- ts(Mi)
Δtr= tr(Mi+1)- tr(Mi)
ifΔts ≈ Δtr // conformance property satisfied as Lemma 1
$E_i \leftarrow \bar{e}(M_i, M_i + 1)$ // Inclusion of edge in the message graph
else
$I_v \leftarrow M_i + 1$ // $I_v$set of isolated vertex

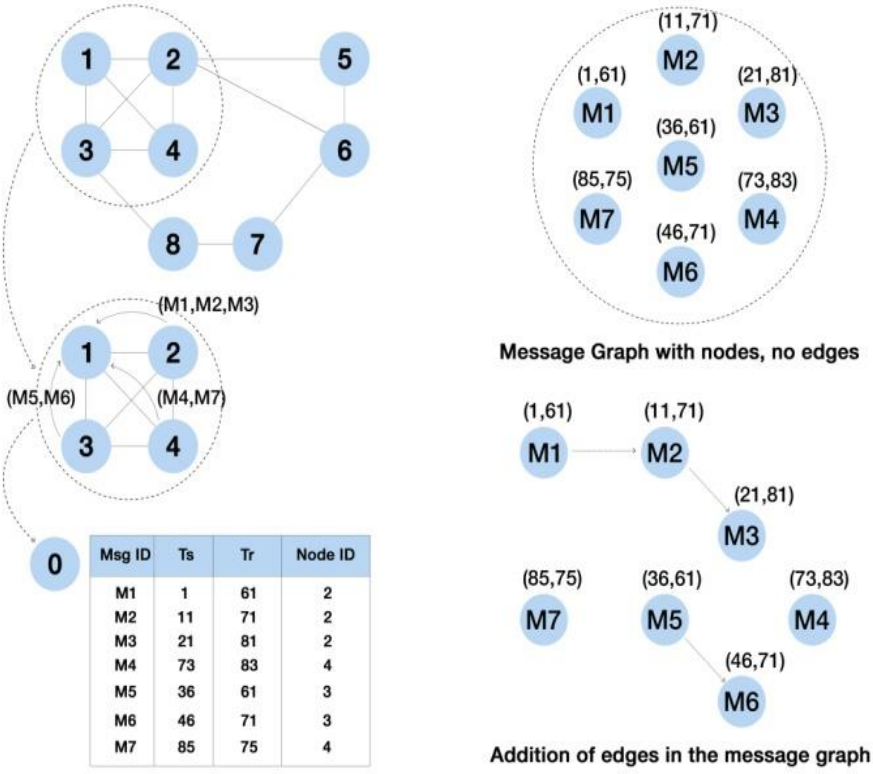
Algorithm 3 Sybil_Detection(NTD,Buffer_Tab,Vi)

BEGIN
for i: 1<i<m do
for j: 1<j<n do
if adjm((i, j))==1:
c[j]=(c[i]+c[j])/2 //pairwise averaging CTS algorithms
end for
end for
END

Algorithm 4 CTSA

4.4. Algorithms Illustration

Suppose, we have a network as shown in Figure 5. For illustrative purposes, we are taking only the part of a network of the node-{1, 2, 3, 4}, where node 4 is assumed as the Sybil node. At node 1, timestamps are received from their neighboring nodes and stored in the table as shown below.



Msg ID	Ts	Tr	Node ID
M1	1	61	2
M2	11	71	2
M3	21	81	2
M4	73	83	4
M5	36	61	3
M6	46	71	3
M7	85	75	4

Figure 5 Illustration of Proposed Work

At node 1, all the messages are stored, for message M1 sending time is 1 and receiving time is 61, similarly for message M2 sending time is 11, and receiving time is 71, and so on. After a particular iteration, the message graph at node 1 is created based on algorithm 2. The message M1 can be associated with M2, and Message M3 can be associated with M2, following the conformance property given in Lemma-1 [16]. But message M4 is kept isolated because M4 is not satisfying the conformance property. Similarly, messages M5 and M6 can be associated with each other but M7 is treated as an isolated vertex in the message graph at node 1. This process is performed at each node distributed at each iteration to filter the Sybil messages and achieve a consensus state.

5. MATHEMATICAL ANALYSIS

This section presents an in-depth mathematical analysis of the correctness of the back-bone algorithm, algorithm 3, and the overall complexity in terms of messages and space requirement for the SRCTS algorithm using graph properties.

RESEARCH ARTICLE

The following two base lemma is used for proving the correctness and complexity of the algorithms.

Lemma-1: Two time-synch messages, m_i, and m_j are said to be satisfied with the conformance property if equation 4 holds [16].

$$1 - \lambda_m \leq \frac{m_j.t_s - m_i.t_s}{m_j.t_r - m_i.t_r} \leq 1 + \lambda_m \quad (4)$$

Where $m_k.t_s$ and $m_k.t_r$ denote the sending timestamp and receiving timestamp (k = i, j) and λ_m denotes the max clock drift between two nodes.

Lemma-2: (Hand-shaking lemma) A graph's vertices' combined degrees are an even number that is equal to twice the graph's total number of edges. [24].

5.1. Correctness Proof

Theorem-1: The proposed algorithm for Sybil detection, algorithm 3, fairly differentiates Sybil message sets(Ms) and normal message sets (Mn) at every node in the network, i.e., $Ms \cap Mn = \varnothing$.

Proof: Using the graph-theoretic approach, at every node i, algorithm 3 creates a message graph $\overline{G_i} = (\overline{V}i, Ei)$ where $\overline{V}i$ contains a set of messages received at node i from its 1-hop neighbors. For any pair of consecutive messages, (Mi, Mi+1), an edge e(Mi, Mi+1) will be included in the edge set Ei if it satisfies Lemma-1. So, algorithm 3 creates a set of connected components of messages for every neighbor node of i as shown in figure 5. Any message which is a Sybil message will not be included in any connected components due to a violation of conformance property given in Lemma-1. So, Sybil message sets (Ms) will create isolated vertices in $\overline{V}i$. The intersection of the Sybil messages and normal messages sets always holds the condition shown in equation 5. Hence, using an intrinsic property of connected components i.e

$$Ms \cap Mn = \varnothing. \quad (5)$$

Hence, algorithm 3 fairly differentiates between Ms and Mn.

Corollary-1: The normal message sets {Mn} create connected components of the message graph G_i with cardinality greater than 1, i.e., |Mn| >1.

Corollary-2: The Sybil message sets {Ms} creates connected components of message graph Gi with cardinality equal to 1, i.e., |Ms| = 1.

5.2. Message Complexity

The message complexity of the SRCTS algorithm solely depends on the message exchanges during the neighbor discovery phase (algorithm 2), Sybil detection phase (algorithm 3), and consensus synchronization phase (algorithm 4). This can be analyzed and proved as given in Theorem 2.

Theorem 2: The overall asymptotic message complexity of the SRCTS algorithm is $O(n^2)$ where n = The number of sensor nodes in the randomly connected network topology.

Proof: In the neighbor discovery phase (algorithm 2), n nodes broadcast n beacon messages (bm) to their neighbors and received ideally the total number of rm messages equal to its number of neighbors. As per lemma-2, the number of neighbors of the randomly connected network topology is: $\sum_{i=1}^{n} \deg(i)$. So, for this phase, the asymptotic message complexity can be expressed by equation 6.

$$|bm| + \sum_{i=1}^{n} \deg(i) = n + 2 \quad (6)$$

As we know that

$$|E| = n + (n-1) = 2n - 1 = O(n) \quad (7)$$

For, the Sybil detection phase (algorithm 3), each node i needs at least two consecutive message transmissions from its neighbors for the detection of Sybil messages. So using equation 7, the number of messages received for the complete network can be expressed by equation 8.

$$2n \sum_{i=1}^{n} \deg(i) = 2n(n-1) = O(n^2) \quad (8)$$

For a generic CTS algorithm, each node i exchanges messages with its neighbors to apply the consensus averaging principle as given in algorithm 4. Considering a given number of maximum iterations K, the CTS will consume the number of messages as equation 9.

$$Kn \left(\sum_{i=1}^{n} \deg(i) = Kn(n-1) = O(n^2)\right) \quad (9)$$

So, By using equation 9, the overall asymptotic message complexity of SRCTS is given by equation 10.

$$Mc(n) = O(n) + O(n^2) + O(n^2) = O(n^2) \quad (10)$$

6. SIMULATION RESULTS

6.1. Experimental Setup

The behavior of CTS algorithms is modeled using Pymote Simulator [25], which provides event-based simulation and is specially designed for analyzing distributed systems. The Pymote uses the graph data structure to investigate node communication. It supports several scientific software packages, including Numpy, matplotlib, and scipy, and is mostly developed on top of the NetworkX library of Python. It also provides a GUI where we can configure different network scenarios. IPython is available on the console, and PySide is used for the GUI.

The deployment of sensors is done by the radius (r) using equation 11 to fulfill the connected topology. The typical skew range, according to the TeloSB datasheet, is between 5 PPM and 5 PPM.

$$r = L * \frac{\sqrt{2 \log n}}{n} \quad (11)$$

RESEARCH ARTICLE

To compare NiSTS, RTSP, and SRCTS, the clock offsets are generated randomly using a uniform distribution between 0 and 1. The simulation parameters and their values are displayed in Table 2 for use in the analysis.

Table 2 Simulation Setting and Parameters

S.No	Parameter	Values
1	Nodes Deployment	10 × 10 square unit
2	Network Topology	Random
3	Nodes	100-500
4	Iteration Interval	10 s
5	Connectivity radius (r)	2 unit
6	Initial Skew	Uniform (− 5,5)
7	Initial Offset	Uniform (0,1)

6.2. Performance Metrics

The state-of-the-art methods are thoroughly evaluated using the unique and generic approach of Sybil resilient consensus time synchronization (SRCTS), which is proposed. Standard performance indicators include convergence speed, Sybil message detection rate, and global synchronization error.

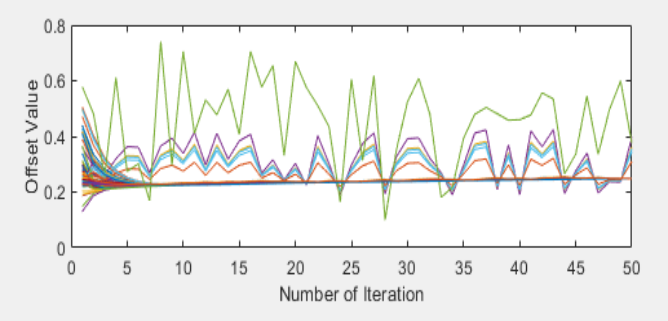


Figure 6 Convergence Distortion of Clock Offset with Sybil Attack

Figure 6 depicts the result of the Sybil attack on a network of 100 nodes, with 1% attacker nodes. It has clearly shown the convergence distortion of the network.

The Sybil message detection rate is shown in Figure 7 for the network of (100–500) nodes; as the number of attacker nodes rises, the rate of detection falls.

Figure 8 shows the Sybil message detection rate comparison of our proposed algorithms SRCTS with RTSP [16] and NiSTS [17] algorithms. Comparatively to other Sybil detection algorithms, It is noticeable that the suggested SRCTS algorithm detects Sybil messages more accurately.

Figure 9 shows the comparison of our proposed algorithms (SRCTS) with RTSP [16] and NiSTS [17] algorithms with (100-500) nodes. It can be observed that the proposed SRCTS algorithm detects Sybil messages with more accuracy.

Figure 10 shows the Global synchronization error comparison of our proposed algorithms (SRCTS) with RTSP[16] and NiSTS [17] algorithms in presence of a Sybil attack without using SRCTS.

Figure 11 shows the convergence of the network by using NiSTS [17]. It can be observed that, by using this detection process, convergence was achieved after 40 iterations, which is quite large.

It can be observed that by using this detection process, convergence was achieved at 22 iterations, which is quite average.

Figure 13 shows the convergence of the network using our proposed detection algorithm.

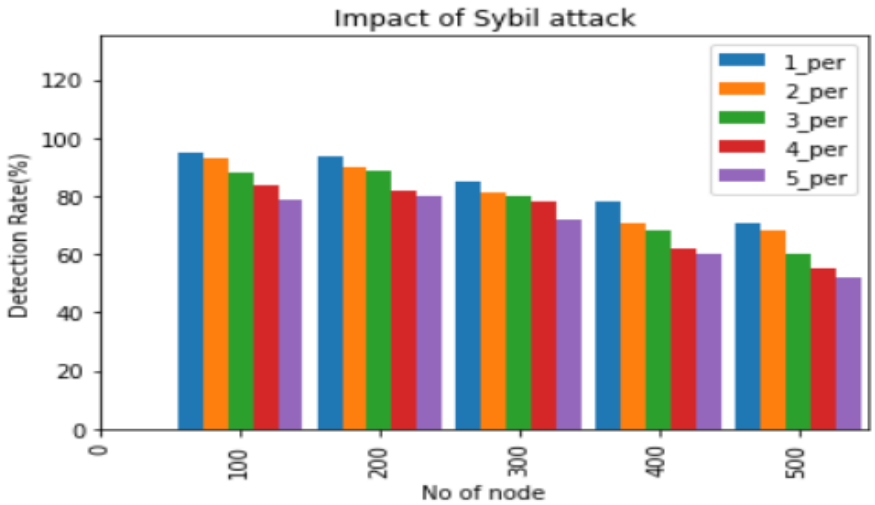


Figure 7 Sybil Message Detection Rate (in %) for (100-500) Nodes

RESEARCH ARTICLE

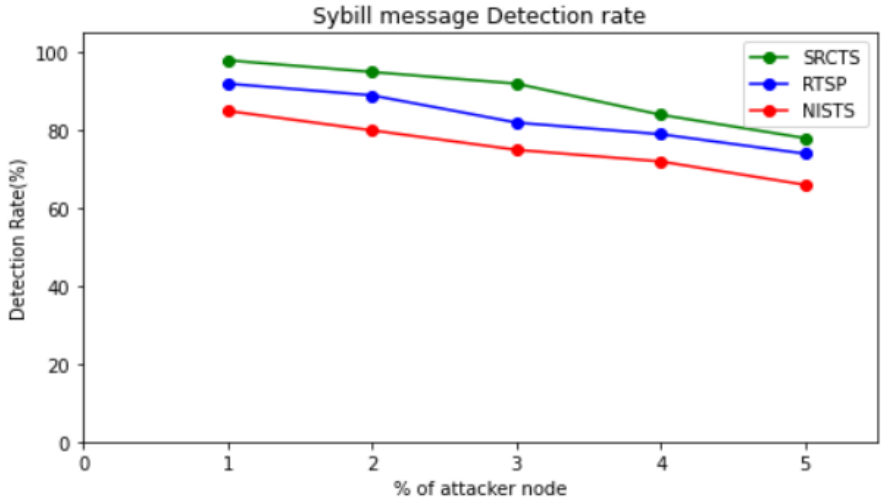


Figure 8 Sybil Message Detection Rate Comparison for Three Algorithms (in %)

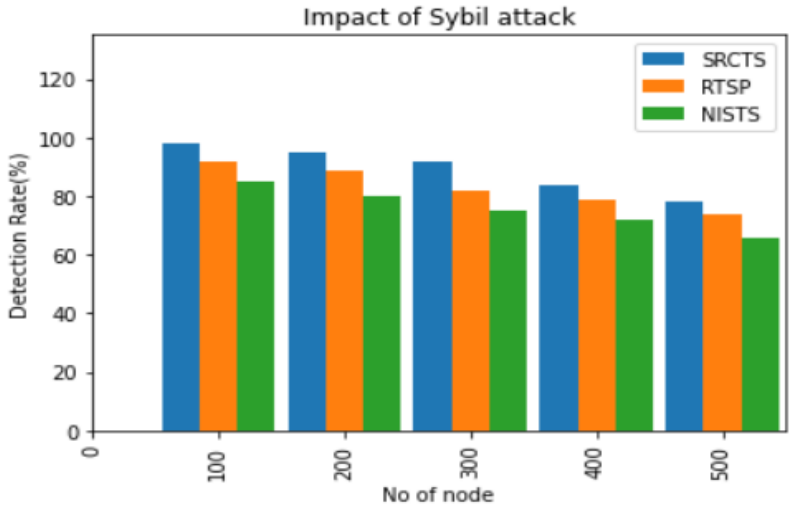


Figure 9 Comparison of Detection Rate of Individual Algorithms

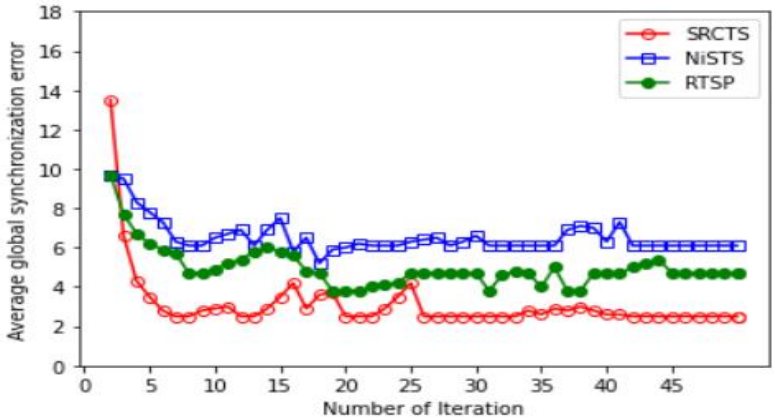


Figure 10 Global Synchronization Error Using Different Detection Algorithms in Presence of Sybil Attack

RESEARCH ARTICLE

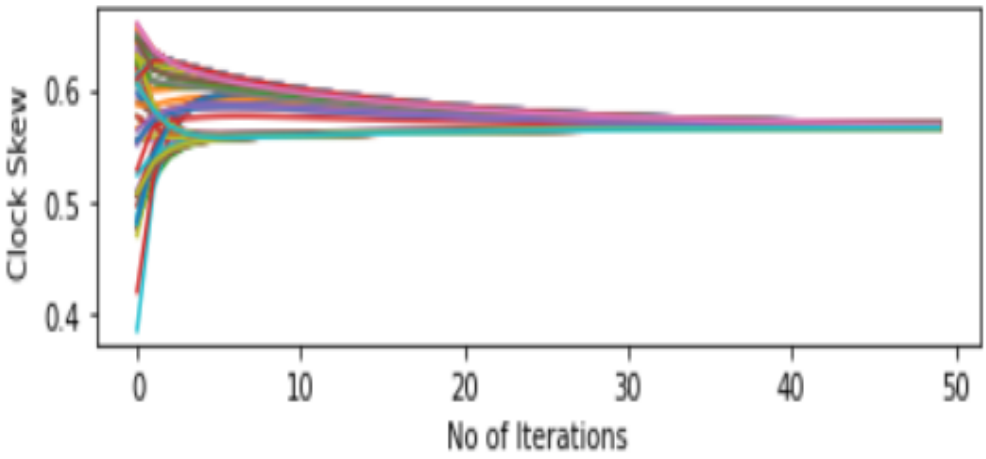


Figure 11 Convergence in the Presence of Sybil Attack Using NiSTS

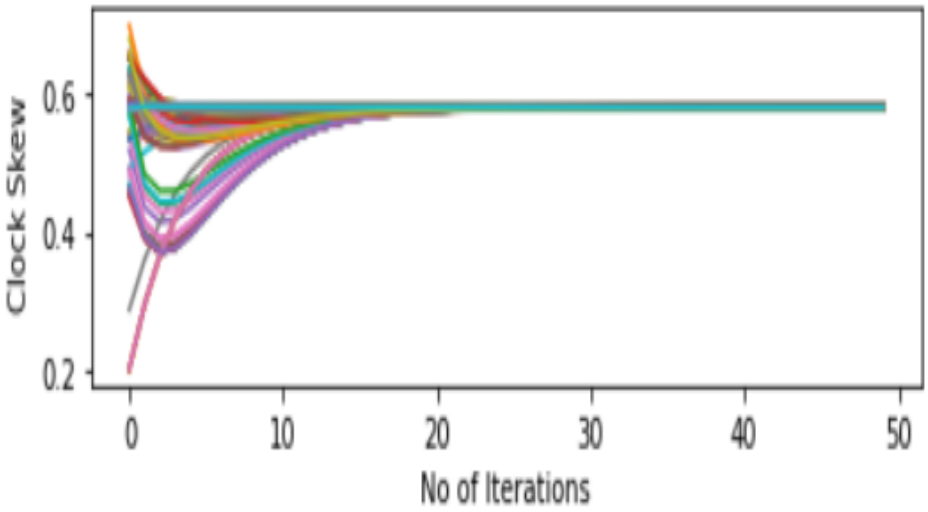


Figure 12 Shows the Convergence of the Network by Using RTSP [16]

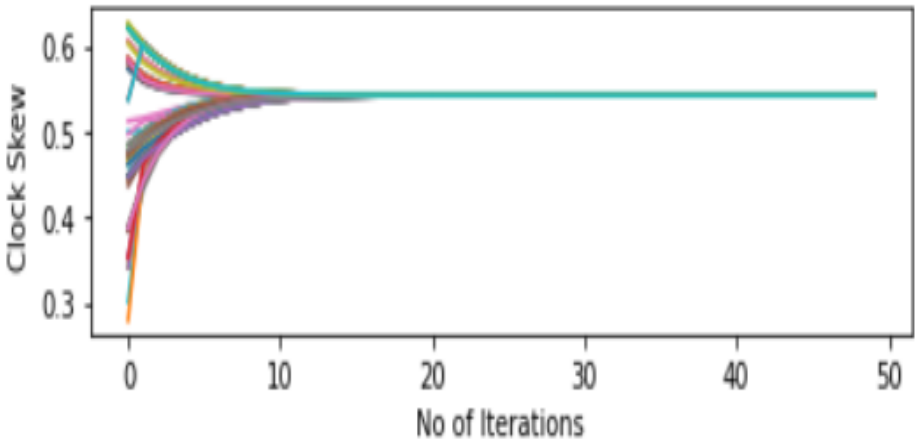


Figure 13 Convergence in the Presence of Sybil Attack Using SRCTS

RESEARCH ARTICLE

6.3. Result Discussion

It can be observed that by using the proposed detection process, convergence was achieved at 15 iterations, which is quite good compared to other detection algorithms mentioned in figure 11 and figure 12, and data are shown in Table 3. For detection and convergence speed, a comparison between the RTSP and the NiSTS has been made. When comparing SRCTS to RTSP and NiSTS, the Sybil message detection rate is increased by 6% and 14%, respectively. According to simulation studies, the SRCTS algorithm has a convergence rate that is 45% higher than RTSP and 62% higher than NiSTS. The proposed distributed, connected component based message graph creation (Algorithm-3) helps in filtering Sybil messages at every node. Hence, every node can fairly differentiate the Sybil messages and normal messages with a high overall network-wide detection accuracy as shown in Figure 7 as compared to RTSP and NiSTS. Hence, consensus convergence is faster and synchronization error is less as shown in Table 3 and Table 4. Table 4 shows a comparison of three algorithms based on global synchronization error criteria with increasing numbers of attacker nodes from 1% to 5%. The mean (μ) and variance σ^2 for each algorithm have been calculated, and it is clear that the error of the SRCTS algorithm is comparatively less than those of RTSP and SRCTS protocol.

Table 3 Convergence Speed Comparison of All Algorithms

S.No	Sybil Detection Algorithms	CTS Algorithm (Common to all)	Convergence Speed (no. of Iterations)
1	NiSTS	Pairwise averaging	40
2	RTSP	Pairwise averaging	22
3	SRCTS	Pairwise averaging	15

Table 4 Comparative Analysis of Global Synchronization Error with Increasing % of Attacker Node

Algorithms	CTS Algorithm	Error Parameter	Percentage of attacker node									
			1 %		2 %		3 %		4 %		5 %μ	
			μ	σ^2	μ	σ^2	μ	σ^2	M	σ^2	μ	σ^2
NiSTS	Pairwise Averaging	Global Synchronization Error	6.51	0.1	5.52	0.1	5.24	0.18	5.12	0.09	8.857	0.19
RTSP	Pairwise Averaging	Global Synchronization Error	3.02	0.1	4.12	0.1	4.19	0.16	4.89	0.08	7.246	0.09
SRCTS	Pairwise Averaging	Global Synchronization Error	1.12	0.3	0.07	0.1	1.46	0.03	2.57	0.11	4.289	1.05

7. CONCLUSION AND FUTURE WORK

This work has investigated the adverse effect of the Sybil attack on the CTS algorithm for distributed WSN and proposes a novel graph-theoretic-based approach using connected component theory to detect Sybil messages. The correctness of the proposed algorithm is proved via in-depth mathematical analysis and extensive simulation results. The comparison of our proposed algorithm SRCTS, with the other two algorithms RTSP and NiSTS has been shown. It is observable that SRCTS detecting Sybil messages is more accurate other than the two algorithms in terms of convergence rate and detection rate. The Global Synchronization error is also evaluated to strengthen the result. The limitation of the current work is the assumption of neglecting one-hop neighbor delay in transmitting the synchronization messages, which may hamper conformance property. Future work may include, the behavioral study of the proposed algorithms in clustered sensor networks and multi-agent networks with localization, power consumption, etc., in presence of different kinds of attacks.

REFERENCES

[1] Zhang Xuxin , Liu Yanzhang& Zhang Ya , "A Secure Clock Synchronization Scheme for Wireless Sensor Networks Against Malicious Attacks", Journal of Systems Science and Complexity volume 34,https://doi.org/10.1007/s11424-021-0002-y, pages 2125–2138, 04 February 2021.

[2] Kobo, H.I.; Abu-Mahfouz, A.M.; Hancke, G.P,"A survey on software-defined wireless sensor networks: Challenges and design requirements". IEEE Access 2017, 5, 1872–1899

RESEARCH ARTICLE

[3] Du Shengli, Wang Y, Dong L, "Secure consensus of multiagent systems with DoS attacks via a graph-based approach", https://doi.org/10.1016/j.ins.2021.03.0540020-0255, Elsevier 2021
[4] Wang, Z.; Zeng, P.; Zhou, M.; Li, D.; Wang, J. "Cluster-based maximum consensus time synchronization for industrial wireless sensor networks". Sensors 2017, 17, 141.
[5] Hansdah, R.C.; Swain, A.R. "A model for the classification and survey of clock synchronization protocols in WSNs". Ad Hoc Network. 2015, 27, 219–241.
[6] Schenato, L.; Fiorentin, "Average TimeSynch: A consensus-based protocol for clock synchronization in wireless sensor networks". Automatica 2011, 47, 1878–1886
[7] Sarvghadi, M.A.; Wan, T.C. "Message Passing Based Time Synchronization in Wireless Sensor Networks: A Survey". Int. J. Distrib. Sens. Netw. 2016, 12, 1280904.
[8] Ganeriwal, P.; Kumar, P.; Srivastava, M.B. "Timing-sync protocol for sensor networks". In Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys), Los Angeles, CA, USA, 5–7 November 2013; pp. 138–149.
[9] Yildirim, K.S.; Kantarci, A.,"Time synchronization based on slow-flooding in wireless sensor networks".IEEE Trans. Parallel Distrib. Syst. 2014, 25, 244–253
[10] Alsaedi, N.; Hashim, F.; Sali, A.; Rokhani, F.Z., "Detecting Sybil attacks in clustered wireless sensor networks based on energy trust system (ETS)". Comput. Commun. 2017, 110, 75–82.
[11] Wu Yiming, "Secure Consensus Control for Multi-Agent Systems with Attacks and Communication Delays", CAA Journal of Automatica Sinica · January 2017, DOI: 10.1109/JAS.2016.7510010
[12] Ganeriwal, S.; Han, C.C.; Srivastava, M.B. "Secure time synchronization service for sensor networks". In Proceedings of the 4th ACM Workshop on Wireless Security, Cologne, Germany, 2 September 2005; pp. 97–106.
[13] Rahman, M.; El-Khatib, K. "Secure time synchronization for wireless sensor networks based on bilinear pairing functions". IEEE Trans. Parallel. Distrib. Syst. 2010.
[14] Hu, X.; Park, T.; Shin, K.G., "Attack-tolerant time-synchronization in wireless sensor networks". In Proceedings of the 27th Conference on Computer Communications (IEEE INFOCOM), Phoenix, AZ, USA, 13–18 April 2008; pp. 41–45.
[15] He, J.; Cheng, P.; Shi, L.; Chen, J., "SATS: Secure average-consensus-based time synchronization in wireless sensor networks". IEEE Trans. Signal Process. 2013, 61, 6387–6400.
[16] Dong, W.; Liu, X., "Robust and secure time-synchronization against Sybil attacks for sensor networks", IEEE Trans. Ind. Inform. 2015, 11, 1482–1491.
[17] Wang, Zeng, Kong, Li, Jin, "Node-Identification-Based Secure Time Synchronization in Industrial Wireless Sensor Networks", MDPI Sensors 2018, 18, 2718; doi:10.3390/s18082718
[18] Zheng, N., "Resilient Consensus for Multi-Agent Systems in the Presence of Sybil Attacks", Electronics 2022, 11, 800. https://doi.org/10.3390/ electronics1105080.
[19] Wu, Y.; Xu, M.; Zheng, N.; He, X. "Event-Triggered Resilient Consensus for Multi-Agent Networks Under Deception Attacks", IEEE Access 2020, 8, 78121–78129.
[20] Wang, D.; Zheng, N.; Xu, M.; Wu, Y.; Hu, Q.; Wang, G. "Resilient Privacy-Preserving Average Consensus for Multi-agent Systems under Attacks", In Proceedings of the 16th International Conference on Control, Automation, Robotics and Vision (ICARCV), Shenzhen, China, 13–15 December 2020; pp. 1399–1405
[21] Jamshidi, M.; Darwesh, A.M.; Lorenc, A.; Ranjbari, M.; Meybodi, M.R, "A precise algorithm for detecting malicious sybil nodes in mobile wireless sensor networks", IEIE Trans. Smart Process. Comput. 2018, 7, 457–466
[22] Wu, Y.; He, X., "Secure Consensus Control for Multi-Agent Systems with Attacks and Communication Delays", IEEE/CAA J. Autom.Sin. 2017, 4, 136–142.
[23] He J, Cheng P, Shi L, Chen J. "SATS: secure average-consensus-based time synchronization in wireless sensor networks", IEEE Trans Signal Process. 2013;61(24):6387.
[24] Panigrahi N, Khilar PM, "Optimal consensus-based clock synchronization algorithm in wireless sensor network by selective averaging", IET WirelSens Syst. 2015. https:// doi. org/ 10. 1049/ iet-wss. 2013. 0102(1stOctober 2014).
[25] Pymote documentation, <https://pymote.readthedocs.io/en/latest/> [30 December 2022].

Authors

Mr. Suresh K Jha received his B.E (CSE) from Government Engineering College, Kota, and his M.Tech (CSE) from RTU, Kota. He is pursuing a Ph.D. from MBM University, Jodhpur, Rajasthan. His area of research is a multi-agent network, Consensus theory, Graph theory, and Distributed algorithms.

Prof. (Dr.) Anil Gupta is currently working as Professor in the computer science and Engineering department, at MBM University, Jodhpur, Rajasthan. His area of research is Algorithm Design, Information security, Machine learning, and Distributed systems. He has 20 years of teaching experience. He teaches undergraduate and postgraduate courses and is supervising Ph.D.

Dr. Niranjan Panigrahi completed his M.Tech in Computer Science & Engineering from NIT, Rourkela, India in the year 2009 and his Ph.D. from NIT, Rourkela, India in the year 2017. Presently, He is working as an assistant professor in the department of CSE, Parala Maharaja Engineering College, an autonomous college of the Government of Odisha, Berhampur, India. His research area includes Wireless Sensor Networks, Applied Machine learning, Parallel Algorithm, and soft computing.

How to cite this article:

Suresh Kumar Jha, Anil Gupta, Niranjan Panigrahi, "Resilient Consensus-Based Time Synchronization with Distributed Sybil Attack Detection Strategy for Wireless Sensor Networks: A Graph Theoretic Approach", International Journal of Computer Networks and Applications (IJCNA), 10(1), PP: 39-50, 2023, DOI: 10.22247/ijcna/2023/218510.