

Intelligent Two-Tier Malware and Intrusion Detection System for Secure WSNs

Ashok Kumar R¹, Dharani Kumar S V², Pasupuleti Saritha³, Mohan Kumar C E⁴,

1,2,3,4 Grt Institute of Engineering & Technology, Tiruttani

HOW TO CITE:

Ashok Kumar R, Dharani Kumar S V, Pasupuleti Saritha, Mohan Kumar C E, (2026). Intelligent Two-Tier Malware and Intrusion Detection System for Secure WSNs. International Journal of Special Education, 41(17s), 673-680

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

ABSTRACT:

Protecting Wireless Sensor Networks (WSNs) from malicious nodes is a major challenge due to its dynamic and resource-constrained nature. To address this problem, we propose a Two-Tier Security Model for Node Verification. The first tier identifies trustworthy nodes and isolates dangerous actors by computing trust ratios. To confirm valid nodes and stop unauthorized access, the second tier employs an asymmetric random key generator. This two-pronged approach maintains effective communication while significantly lowering security risks. Experiments confirm the model's advantages in terms of packet delivery rate, assault resistance, and key-matching accuracy.

Keywords: Trust computation, Hub Contact Rate, Random key generator, Node Authenticity, Sign verification..

1. Introduction

Wireless Sensor Networks (WSNs) are widely deployed for infrastructure monitoring, where sensor nodes collect and relay data via single or multi-hop communication. However, ensuring network security remains challenging, as adversaries can inject false data to disrupt operations. Node authentication is critical to verify data sources and maintain confidentiality, integrity, and authenticity. Existing approaches like Active Trust [1] mitigate black-hole attacks by dynamically assessing nodal trust values, while the Binomial Principle System (BPS) [2] enhances security by generating fake paths to obscure real node identities from malicious eavesdroppers. This paper proposes a two-tier security mechanism combining trust-based authentication and dynamic path obfuscation to detect and

isolate malignant nodes efficiently. Experimental results demonstrate improved resilience against data breaches and adversarial attacks compared to conventional methods.

2. Methodology

Wireless Sensor Networks (WSNs) face significant security challenges due to their decentralized nature and resource limitations. While numerous authentication-based security schemes have been proposed, this work highlights critical protocols, including Authentication and Key Establishment (AKE) for dynamic key management—where sensor nodes utilize a key cache verified via base station (BS) pairing—and Secure Data Aggregation (S_DA) to balance security and network performance. Attacks in WSNs are classified

across protocol stack layers [3], with eleven common attack types analyzed alongside detection methods.

Further, secret key-based user confirmation [6] and lightweight verification schemes [7] are reviewed, emphasizing hash-based security analysis and session key agreement. Hybrid approaches like Hybrid Secure Data Transmission (HSDTS) [9] integrate reputation-based node validation with improved SHA encryption, while Physical-Layered Secure Key Generation (PL-SKG) [13] reduces key material overhead via ECC. Despite advancements, trade-offs persist in latency (e.g., CASR's onion routing delays [11]) and scalability. This survey underscores the need for adaptive two-tier security mechanisms combining lightweight authentication with real-time malignant node detection, paving the way for future work on energy-efficient, machine learning-enhanced solutions.

Refined Abstract Section on Security Schemes

Recent advancements in WSN security have introduced several innovative approaches. The secret key-based user confirmation scheme [6] employs a rigorous encryption process where clients must possess matching cryptographic characteristics to access data. This scheme's security is validated through deterministic hash function analysis, ensuring robust protection against unauthorized access.

For resource-constrained environments, a lightweight user verification scheme [7] implements challenge-response authentication and session key agreement. This method has been formally proven to provide:

- Data confidentiality ("mystery" in original text)
- Message integrity ("veracity")
- Mutual authentication

Secure session key generation

The Security Cooperation Collection Tree Protocol (SCCTP) [8] establishes a trusted network environment through:

- Coupled state vectors for topology control
- Weight-based time synchronization
- Malicious node isolation mechanisms

SCCTP's synchronization mechanism uses weighted calculations between neighboring nodes to:

Maintain network temporal coherence

Evaluate node behavior through topology control metrics

Dynamically adjust synchronization parameters based on network objectives

Enhanced Security Mechanisms in WSNs

To ensure secure communication between nodes, mutual authentication (two-way confirmation) is implemented. The Certified Anonymous Secure Routing (CASR) scheme [11] effectively mitigates active attacks through:

- Key-encrypted onion routing for end-to-end anonymity
- Secure verification messages to validate node authenticity
- High confidentiality guarantees through layered encryption
- While CASR provides robust security, it introduces significant transmission delays due to its multi-layered encryption process. To address this, the scheme incorporates:
- Sensor-generated reports to identify malicious nodes
- Attack severity assessment algorithms for threat prioritization

Further security enhancements include:

1. Entropy-based Trust Model [12]:

- Dynamically evaluates node trustworthiness using information-theoretic metrics

- Implements adaptive acknowledgment protocols for reliable data forwarding
2. **Physical Layer Secure Key Generation (PL-SKG) [13]:**
- Reduces key material requirements through Elliptic Curve Cryptography (ECC)
 - Prevents data leakage among local nodes via lightweight key management
 - Maintains security while optimizing resource-constrained sensor operations

Proposed Work

We present a Two-tier Security Model for Node Verification (TSMNV), a novel hierarchical security framework designed to enhance network communication protection. This dual-phase security architecture significantly strengthens information confidentiality across the entire wireless sensor network.

The first tier implements a trust-based node selection mechanism, where each node's reliability is quantitatively assessed through a computed trust ratio metric. This process actively identifies and excludes potentially malicious nodes from participating in network communications.

The second tier employs an asymmetric cryptographic protocol, generating unique cryptographic keys through a randomized key generation algorithm exclusively for verified trustworthy nodes. This phase performs final validation, ensuring complete removal of any remaining unauthorized nodes from the network communication processes.

Level 1 – Trust Node Selection

Trustworthy nodes in the network are determined by evaluating the Hub Reliability Score (HRS). The HRS is derived from the exchange of Route Discovery Packets (RD-Pkts) and Route Confirmation Packets (RC-Pkts) between nodes, which helps identify reliable hubs within the communication range.

The score is computed based on the ratio of RD-Pkts received from a specific node to the number of unacknowledged RC-Pkts relative to the total

RD-Pkts received. The HRS is formulated using Equation (1) and Equation (2).

$$HCR = \left(\frac{\text{Total } R_{qrecv} - \text{Unsent } P_{ptotal}}{R_{qrecv}} \right) \times 100$$

R_{qrecv} = Number of Route Request (Rq) messages received from the node.

Unsent Rptotal = Number of Route Reply (Rp) messages not sent in response.

Hubs or sensor nodes typically transmit collected data within their designated transmission range. Nodes within this communication radius are organized into clusters for efficient data management. A cluster head is elected based on residual energy and a Link Quality Indicator (LQI). The selection process involves evaluating each node's energy reserves, and the node with the highest energy, along with an LQI exceeding 90%, is designated as the leader. This ensures reliable data routing from the source node to the sink node with minimal packet loss.

(ii) Level 2 – Generating Secured Key

After identifying the trustworthy nodes within the clusters, private keys are generated for each selected hub. The Base Station (BS) employs a secure hash-based keying algorithm to create a randomized 4-digit coded number, A_n , which is then used to compute a unique private key for every node based on their respective IDs. This process ensures node authenticity (N_{ai}). If the generated key were made public, any node in the system could gain unauthorized access to sensitive data. To prevent this, the system verifies the node's legitimacy by matching its private key before granting access. Only after successful authentication (N_{ai} , Sid (key)) can two nodes establish secure communication.

For data encryption, a random key generator produces a coded key, $M_{a,b}(k)$, using a Message Authentication Code (MAC). This key encrypts the sensed data before transmission. Each data packet includes a standard MAC-encoded authentication key, K , embedded in its header field. This security measure safeguards the information against eavesdropping attempts by

malicious nodes. Figure 1 illustrates the workflow of the proposed TSMNV mechanism.

Upon receiving the request message, the Base Station (BS) initiates the authentication process using a digital signature verification system to validate the node's legitimacy. Once the certificate is verified for authorized nodes, the message encryption procedure is executed. The

sender node encrypts the message using a secure hashing algorithm combined with a private authentication key. Subsequently, the encoded data $Mk(A,B)$ is transmitted to the recipient node, appended with a valid signature $\{Nai, Id(Ki)\}$ at the end of the encrypted payload, as defined in Equation 3.

$$MA \rightarrow B = \text{Enc}(K_{\text{mig}}, \text{Data}) || \{Nai, \text{SigId}(K_{\text{priv}})\}$$

Algorithm

```

Start
Build 'N' nodes in network
Get registered to BS
→ Level 1 to be processed
Compute HCR
Select Trustable nodes using EL & HCR
Cluster formation is done
→ Level 2 to be processed
Generate coded keys 'An'
Set node 'A' → sender and 'B' → receiver
Verify nodes with 'Sid'
Do node validation {Nai, Sid(key)}
If coded key "Sid(key)" gets matched
Pass secured info to receiver
End

```

3. Results

Performance Evaluation

The performance of the TSMNV system is evaluated using Network Simulator-3 (NS3), a widely used simulation tool for network analysis. For this study, 200 nodes are deployed to compare the proposed TSMNV scheme with the

conventional SCCTP method. The simulation environment is set up in a 1500x2000 m² area to model a large-scale network scenario. Key performance metrics include Packet Delivery Ratio (PDR), Residual Energy, End-to-End Delay, and Key Matching Efficiency.

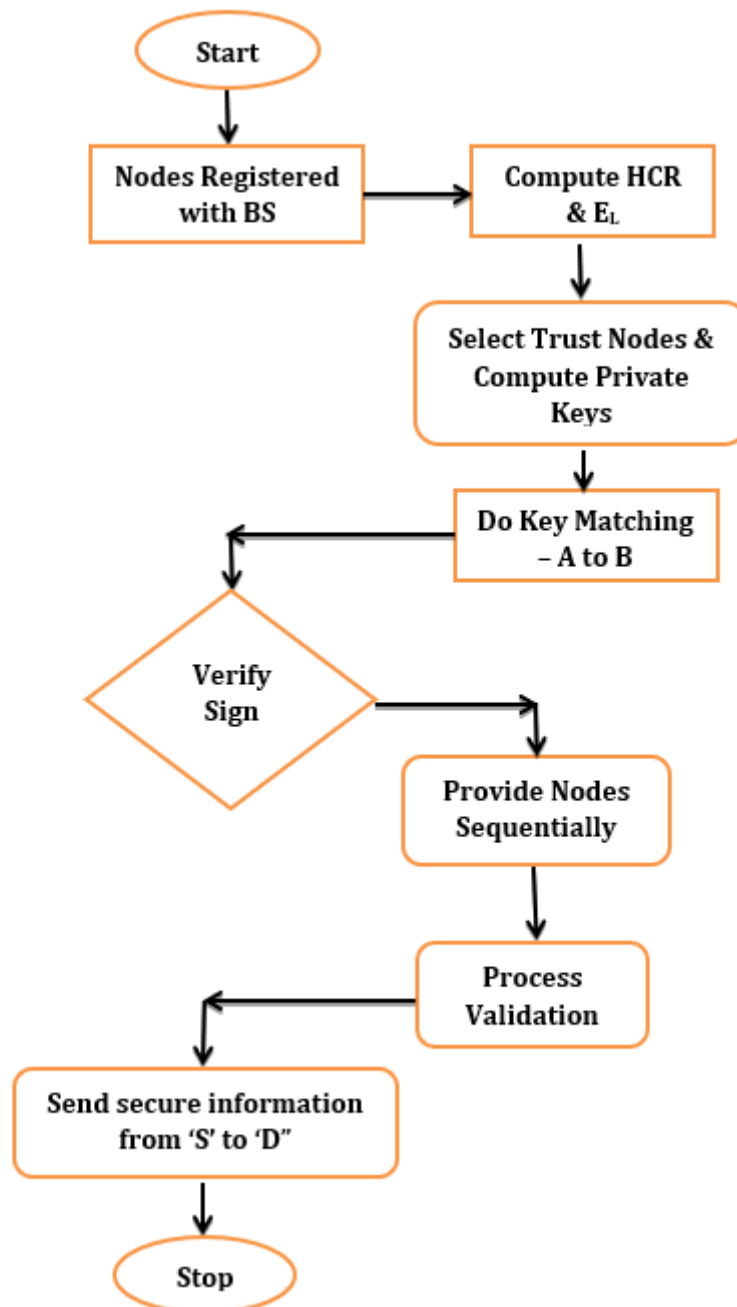


Fig:1 Flowchart of TSMNV Scheme

Packet Delivery Ratio (PDR): This metric represents the percentage of data packets successfully delivered to the destination, generated by Constant Bit Rate (CBR) traffic sources. A higher PDR indicates better network reliability and transmission efficiency. The PDR is calculated using Equation 4, where T denotes the simulation time and n represents the node density.

If the equation intends to calculate the average PDR per node/time, consider:

$$PDS = \frac{1}{n} \sum_{i=0}^n \frac{P_{delivered,i}}{T}$$

Average Delay: This metric represents the total time taken for a data packet to travel from one node to another, including processing and queuing delays. It measures the efficiency of the TSMNV system's routing protocol. The delay is calculated using Equation 5, where n denotes the node density.

$$Delay = \frac{\sum_0^n Pkt_{recvd\ time} - Pkt_{sent\ time}}{n}$$

Mismatch Key Ratio (MKR):

The Mismatch Key Ratio (MKR) is a critical metric used to identify false private keys generated by malicious nodes, which fail to authenticate when paired with the Base Station (BS). It is calculated as the ratio of mismatched bits in the secret keys to the total number of key bits generated for signature verification.

Residual Energy:

Residual energy refers to the remaining energy level in a node at a given time. It is computed by subtracting the total energy consumed by the node from its initial maximum energy capacity.

4. Discussion

Performance Analysis:

Figures 2 and 3 compare the Data Delivery Rate and Residual Energy between the proposed TSMNV scheme and the conventional SCCTP method. The results demonstrate that TSMNV outperforms SCCTP, achieving higher delivery rates and more efficient energy utilization.

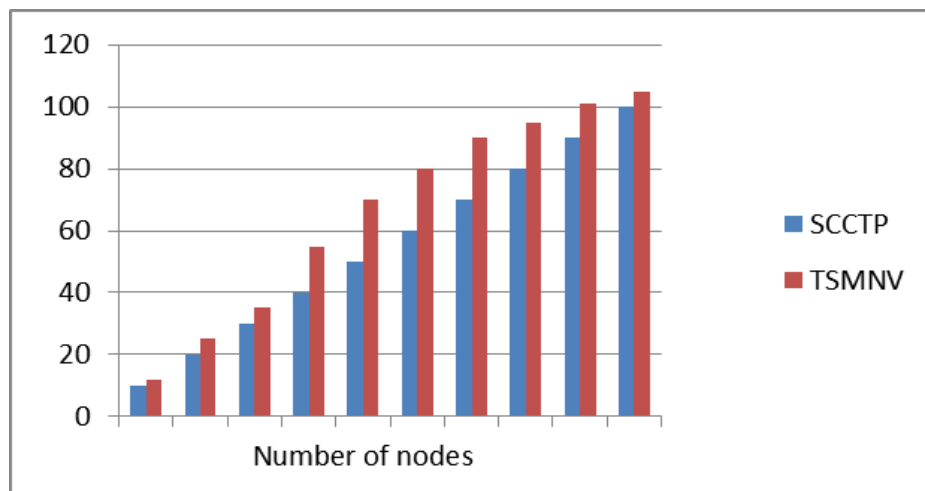


Figure 2: Data delivered rate

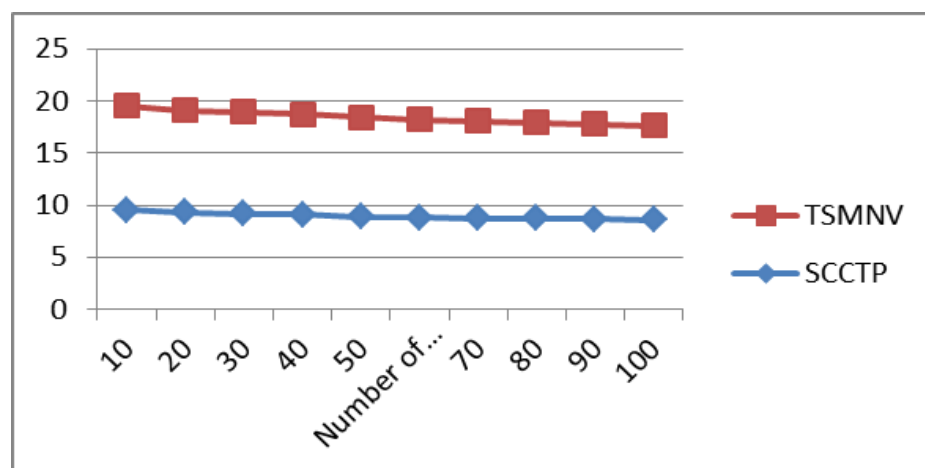


Figure 3: Leftover Energy level in nodes

Initially 10J is set for both the schemes and the energy level gets gradually reduced for each set of transmission. Leftover energy proves that the

nodes in the proposed scheme TSMNV consumes less amount of energy compared to the conventional SCCTP.

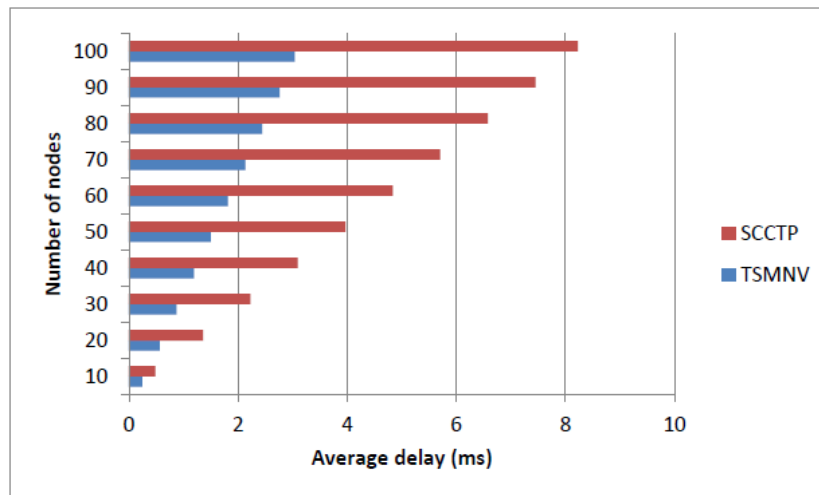


Figure 4: Delay

Average transmission delay is shown in the figure 4 for both proposed and conventional schemes. Proposed TSMNV scheme performs better in

terms of packet delivery latency in comparison with existing SCCTP.

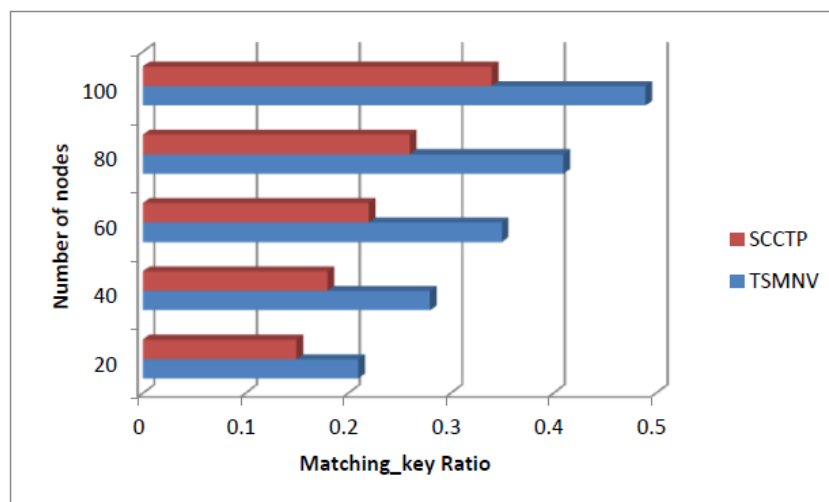


Figure 5: Matching-Key Ratio

"Figure 5 illustrates the Mismatch Key Ratio (MKR) for both the TSMNV and SCCTP schemes. The analysis reveals that the proposed TSMNV achieves a higher matching key ratio compared to the conventional SCCTP method."

5. Conclusion

A Two-Tier Security Model for Node Verification (TSMNV) is introduced to bolster security during network communication. This model aims to improve the security level of information packet transit and ensure reliable communication. The proposed scheme requires secure communication for all nodes within the

system, achieved through the allocation of a private key to each node. The first level involves the selection of trustworthy nodes by calculating a node trust ratio, thereby excluding malicious nodes from the communication process. The second level implements a key generation process for the identified trustworthy nodes using an asymmetric random key generator, further eliminating illegitimate nodes from participation in communication. Empirical results indicate the proposed scheme's significant capability in detecting malignant nodes and its provision of enhanced network security.

References

- V. R. Doifode, R. Ashok Kumar, M. A. Stephenraj, B. Vishnu Vardhana Naidu, C. Bhatt, and D. Deepa, "Development of Smart Environmental Monitoring in Nuclear Power Station Using Data Fusion Techniques," in *Challenges in Information, Communication and Computing Technology*, V. Sharmila et al. (Eds.), London: Taylor & Francis, 2025, pp. 343–348. DOI: 10.1201/978100355673-680, Access: Open Access at Taylor & Francis.
- R. Ashok Kumar and K. Balaji, "PI and Sliding Mode Speed Control of Permanent Magnet Synchronous Motor Fed from Three Phase Four Switch VSI," *Journal of Mechanical Engineering Research and Developments*, vol. 40, no. 4, pp. 716–725, 2017.
- Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). ActiveTrust: Secure and trustable routing in wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 11(9), 673-680.
- Suresh, G., & Kumar, A. S. (2020). Secure Transmission Using Bivariate Principle System for WSN. *Helix*, 10(03), 673-680.
- Xie, H., Yan, Z., Yao, Z., & Atiquzzaman, M. (2018). Data collection for security measurement in wireless sensor networks: a survey. *IEEE Internet of Things Journal*, 6(2), 673-680.
- Liu, X., Yu, J., Li, F., Lv, W., Wang, Y., & Cheng, X. (2019). Data aggregation in wireless sensor networks: from the perspective of security. *IEEE Internet of Things Journal*.
- Y. Qiu, J. Zhou, J. Baek, and J. Lopez, "Authentication and key establishment in dynamic wireless sensor networks," *Sensors*, vol. 10, no. 4, pp. 3718–3731, 2010.
- Jokhio, S. H., Jokhio, I. A., & Kemp, A. H. (2013). Light-weight framework for security-sensitive wireless sensor networks applications. *IET Wireless Sensor Systems*, 3(4), 673-680.
- Chatterjee, S., & Das, A. K. (2015). An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks. *Security and Communication Networks*, 8(9), 673-680.
- Liu, Z., Liu, W., Ma, Q., Liu, G., Zhang, L., Fang, L., & Sheng, V. S. (2019). Security cooperation model based on topology control and time synchronization for wireless sensor networks. *Journal of Communications and Networks*, 21(5), 673-680.
- DAS Kumar (2020). Hybrid cryptography key based Secure Data Transmission Scheme for Wireless Sensor Network. In *Alochana Chakra Journal* 9 (Issue IV, April/2020), 1120 - 1127.
- Jokhio, S. H., Jokhio, I. A., & Kemp, A. H. (2013). Light-weight framework for security-sensitive wireless sensor networks applications. *IET Wireless Sensor Systems*, 3(4), 673-680.
- Ashok Kumar R, Dr. Balaji K, "Sensor Less Control of PMSM fed from Three Phase Four Switch Inverter based on Back EMF Observer and Sliding Mode Controller with Fast Reaching Law", *International Journal of Engineering and Technology*, vol. 7, no. 2, pp.673-680, 2018.

Acknowledgements (Optional)

Funding Disclosure Manuscript Title: Intelligent Two-Tier Malware and Intrusion Detection System for Secure WSNs

No Funding received internally or externally

Authors: Ashok Kumar R, Dharani Kumar S V, Pasupuleti Saritha, Mohan Kumar C E

Author Declaration

Originality of Work

We, the undersigned authors, declare that this manuscript is our original work. It has not been published previously and is not under consideration for publication elsewhere. All sources of information have been appropriately acknowledged and cited.

Conflict of Interest

We declare that there are no financial, personal, professional, or institutional conflicts of interest that could have influenced the research or the publication of this manuscript.