A MASC-Based Approach for Sybil Attack Detection in Wireless Multimedia Sensor Networks

Basavaraj Patil [1], Amiya Bhaumik[2], Raja Sarath Kumar Boddu[3]

[1]R V University, Bengaluru, [2]Lincoln University College, Malaysia; [3]Raghu Engineering College Visakhapatnam, India

[1]bbpatilcs@gmail.com, [2]amiya@lincoln.edu.my, [3]rajaboddu@lincoln.edu.my

Abstract:

Sensor-based applications generate rich data streams, including images and audio. The distributed architecture and resource constraints of sensors make them particularly pathway vulnerable to advanced security threats, such as Sybil attacks. The malicious node creates numerous false individual identities, gaining disproportionate influence and severely compromising network functionality in Sybil attack. A Sybil attack model is proposed within a Wireless Multimedia Sensor Network (WMSN) simulation environment by introducing a novel Multi-faceted Anomaly and Spatial Consistency (MASC) Sybil Detection Algorithm. It is specifically designed for WMSNs, leveraging both radio resource anomalies and the spatial consistency of multimedia features. Experimental results, presented graphically and in tabular form, demonstrate the devastating impact of the Sybil attack on network performance (e.g., data delivery ratio and network lifetime) and validate the efficiency of the proposed MASC algorithm in mitigating these impacts compared to scenarios without detection.

Keywords: Attacks, Anomaly Detection, Sybil attack, MASC, Wireless Multimedia Sensor Networks

Introduction

WSNs have revolutionized data collection in diverse environments, from environmental monitoring to industrial automation. The evolution of WSNs into Wireless Multimedia Sensor Networks (WMSNs) has further expanded their capabilities, enabling the capture and transmission of richer data types such as images, audio, and video. WMSNs [1] are deployed in challenging, often unattended, environments, making them highly susceptible to various security threats. Among these, the Sybil attack [2] stands out as a particularly insidious form of assault.

A Sybil attack involves a single malicious entity fabricating multiple false identities (Sybil IDs) to masquerade as numerous distinct nodes within the network. This allows the attacker to subvert security mechanisms, disrupt routing protocols, corrupt data aggregation, and monopolize network resources. The unique characteristics of WMSNs – particularly the higher bandwidth requirements and the semantic content of multimedia data – introduce both new vulnerabilities and potential new avenues for detection. Traditional Sybil detection methods, often focused on radio fingerprints or basic resource testing, may not be fully adequate or optimally efficient for WMSNs.

This paper addresses these challenges by:

- Designing and implementing a realistic Sybil attack model within a simulated WMSN environment, showcasing its detrimental effects on network performance.

- Proposing and implementing a novel Multi-faceted Anomaly and Spatial Consistency (MASC) Sybil Detection Algorithm. MASC integrates checks for radio resource overload with an innovative use of multimedia feature consistency, along with a dynamic trust management scheme, to identify and isolate Sybil nodes.
- Conducting comprehensive experimental simulations to evaluate the impact of the Sybil attack and demonstrate the efficacy of the MASC algorithm in mitigating these attacks, providing a direct comparison against scenarios without any detection mechanism.
- Comparing the MASC algorithm's performance metrics with reported results from several reputable existing Sybil detection methods found in peer-reviewed literature.

Related Study:

In the study of sybil attack detection, many researchers have worked on the design on efficient model to predict the vulnerabilities in the network, caused by various types of attacks. In table 1, highlights the recent work carried out for the detection of sybil attack along with results and identified limitations.

Table 1: Comparison of few important existing work

Authors & Year	Title	Attack Focused	Key Results	Limitations
Platt & McBurneyv [2] 2023	Sybil in the Haystack	Sybil resistance	PoW and PoS are most effective	Reputation-based weak against Sybil
Doğan-Tusha [3] 2024	Doppler-Shift-Based Detection	Sybil in mobile IoT	90% detection in mobility	Hardware dependency
Tulay & Koksal [4] 2024	Signal Clustering in Vehicular Networks	Identity spoofing	>98% detection rate	Testbed limited
Navinkumar & Somasundaram [5] 2024	Optimized Routing for Sybil Detection	Sybil in VANETs	Higher delivery ratio, lower delay	Simulated with lesser number of nodes.

Sybil attack detection in WMSNs has been an active area of research, with various approaches broadly categorized as:

- Resource-based Detection[6]: These methods assume that a physical node has finite resources (e.g., a single radio transceiver, limited processing power, fixed memory). If multiple identities claim to originate from the same physical location or exhibit resource consumption patterns inconsistent with distinct physical nodes, they are deemed suspicious. Newsome et al. [7] proposed an early radio resource testing method.
- Location-based Detection: This category utilizes localization techniques[8] (e.g., Received Signal Strength Indicator - RSSI, GPS, time-of-flight) to verify the physical proximity and consistency of claimed identities. If multiple identities claim widely disparate locations but are physically co-located, a Sybil attack is suspected. Jamshidi et al.[9] presented an RSSI-based scheme with high detection rates.

- Cryptographic/Authentication-based Methods[10]–[14]: These approaches rely on pre-distributed keys or a trusted authority to authenticate each node. While robust, they often incur significant overhead in terms of key management, computation, and communication, which can be prohibitive for resource constrained WSNs.
- Neighborhood/Connectivity-based Analysis [15]–[17]: These methods leverage the fact that all Sybil identities controlled by a single physical node will share an identical set of true physical neighbors. [18] proposed a method using neighboring node information for detection.
- Trust and Reputation Systems[19] [20]: Nodes build trust scores for their neighbors based on performance (e.g., packet forwarding[21], data consistency[22]). Low trust scores can lead to isolation. Recent advancements include multi-trust layered mechanisms[23] and fuzzy logic integrations[24].
- Machine Learning (ML) / Learning Automaton (LA) Approaches: These methods use ML [25] models to learn normal behavior patterns and detect deviations or employ adaptive learning mechanisms. Jamshidi et al. [26] proposed a Learning Automaton-based approach for Sybil detection.

While these methods offer solutions, WMSNs present unique challenges and opportunities due to their richer data types. Our proposed MASC algorithm aims to address these by combining a resource-based approach with a novel multimedia feature consistency check, making it particularly suitable for WMSN environments.

Sybil Attack Model in WMSN

To evaluate detection mechanisms effectively, a robust Sybil attack model is crucial. In our simulation, the Sybil attack is characterized by:

- **Attacker Capabilities**
  - Sybil Controller: A single legitimate sensor node is designated as the physical Sybil attacker. This node possesses normal WMSN node capabilities (sensing, communication, processing, energy).
  - Fake Identities: The Sybil Controller generates a predefined number of distinct, fake identities (Sybil IDs) that do not correspond to any other physical nodes in the network. These IDs are managed and controlled solely by the Sybil Controller.
  - Identity Advertising: During the neighbor discovery phase, the Sybil Controller advertises its own real node ID along with all its fabricated Sybil IDs to its direct physical neighbors. Legitimate neighboring nodes perceive these as distinct, independent nodes.
  - Packet Handling:
    - Outgoing Traffic: When the Sybil Controller needs to transmit data (either its own sensed data or relayed data), it can choose to use any of its active identities (real or fake). This can mislead legitimate nodes about traffic sources.
    - Incoming Traffic: Any data packet addressed to one of the Sybil IDs is physically received and processed by the single Sybil Controller.

    - Malicious Dropping: To actively disrupt network operations, the Sybil Controller (or any designated malicious node) has a configurable probability of arbitrarily dropping received packets, regardless of which of its IDs the packet was addressed to.

- **Impact on Network Performance**
    - Routing Disruption: Legitimate nodes, unaware of the attack, may attempt to route data through multiple "Sybil nodes," believing these offer diverse paths. However, all such paths converge to the single malicious physical node, creating bottlenecks and increasing the likelihood of packet loss if the Sybil node drops traffic. This leads to inefficient routing and decreased data delivery.
    - Data Integrity Compromise: If the network employs data aggregation or fusion, the Sybil attacker can inject multiple, potentially manipulated, data readings from its fake identities, skewing aggregated results and compromising data trustworthiness.
    - Resource Consumption: Sybil identities consume network resources such as routing table entries, bandwidth, and energy for processing non-existent traffic, leading to reduced network efficiency.
    - Trust System Subversion: If a trust system is implemented, a Sybil attacker can cycle through its fake identities, discarding compromised ones and introducing new ones, thereby attempting to evade detection and maintain a deceptive presence.

Proposed MASC Detection Algorithm

The Multi-faceted Anomaly and Spatial Consistency (MASC) Sybil Detection Algorithm is designed to leverage multiple observable characteristics, including WMSN-specific multimedia features, to detect Sybil attacks. MASC operates in a distributed manner, with each legitimate sensor node independently assessing its neighbors. MASC is based on the premise that a single physical node masquerading as multiple entities will exhibit anomalies that distinct physical nodes would not. It combines:

- **Radio Resource Overload Detection**: A single radio transceiver has physical limits on the amount of data it can simultaneously transmit and receive. If multiple identities appear to originate from the same physical point and collectively exhibit traffic patterns exceeding a plausible single-radio capacity, it's a strong indicator of a Sybil attack.
- **Multimedia Feature Consistency Check**: A key novelty for WMSNs. If multiple "distinct" sensor nodes (identities) are physically co-located and thus sensing the same physical phenomenon (e.g., an image of the same scene, a sound from the same source), their derived multimedia features (e.g., average pixel intensity, dominant color, sound frequency signature) should be highly correlated or nearly identical. Truly distinct nodes, even if close, would likely capture slightly different features due to their unique positions and sensor variations. Conversely, Sybil identities would generate identical features controlled by the same attacker.

MASC Detection Algorithm:

For each neighbor nodes Ni that L observes:

Phase 1: Observation & Feature Collection:

- L maintains traffic from neighbors[Ni], which counts packets received from Ni during a detection interval.
- L maintains observes multimedia features from neighbors, a list of multimedia feature values periodically observed from Ni. Here, a multimedia feature is a simple numeric value generated by the node.
- L notes neighbor claimed ids, the set of all IDs Ni has advertised.

Count packets: traffic[Ni] += packets_received
Record multimedia features: features[Ni].append(value)
Record claimed IDs: claimed_ids[Ni] = et(advertised_ids)

Phase 2: Anomaly Detection and Trust Score Update:

L calculates a total_anomaly_score for Ni. If Ni claims multiple identities and sufficient multimedia features have been observed from it.

1. Radio Resource Anomaly (ΔA_1)

If $|claimed\_ids[N_i]| > 1$ and $traffic[N_i] > \text{RADIO\_THRESHOLD}$:

$$\Delta A_1 = \max\left(0, \frac{traffic[N_i] - \text{RADIO\_THRESHOLD}}{\text{RADIO\_THRESHOLD}}\right)$$

2. Multimedia Feature Consistency Anomaly (ΔA_2)

If $|claimed\_ids[N_i]| > 1$ and $|features[N_i]| > 1$:

$$\text{var} = \text{Variance}(features[N_i])$$

If $\text{var} < \text{FEATURE\_THRESHOLD}$:

$$\Delta A_2 = \max\left(0, \frac{\text{FEATURE\_THRESHOLD} - \text{var}}{\text{FEATURE\_THRESHOLD}}\right)$$

Phase 3: Prevention/Mitigation:

If trust scores[Ni] falls below THRESHOLD, L actively avoids routing data through Ni and its claimed identities. This is achieved by pruning Ni from its consideration during path finding to the sink. If trust[Ni]<ISOLATION_THRESHOLD, exclude Ni and its IDs from routing paths.

$$\text{score} = w_1 \cdot \Delta A_1 + w_2 \cdot \Delta A_2 \quad (w_1 = w_2 = 0.5)$$

Update trust:

- If `score > 0`:

$$trust[N_i] = \max(0, trust[N_i] \cdot (1 - score))$$

- Else:

$$trust[N_i] = \min(1.0, trust[N_i] + \text{TRUST\_DECAY\_RATE})$$

Flag as Sybil if:

$$trust[N_i] < \text{SYBIL\_THRESHOLD}$$

Implementation

The proposed MASC based framework is used to detect the sybil attack. The process of design consists of three distinct scenarios were experimented to provide a comprehensive analysis:

- **Baseline (No Attack, No MASC)**: It represents an ideal network, with all nodes behaving legitimately and the MASC detection algorithm explicitly disabled. It serves as a benchmark for optimal performance.
- **Sybil Attack (without MASC Detection)**: Here, the designated Sybil Controller is active and performs its attack (creating fake IDs, dropping packets). However, the MASC detection algorithm is disabled, allowing the attack to run unmitigated. This highlights the severe impact of the Sybil attack.
- **Sybil Attack with MASC Detection**: The Sybil attack is present. Significantly, the MASC detection algorithm is enabled, allowing legitimate nodes to detect and mitigate the attack. This scenario demonstrates the effectiveness of the proposed MASC algorithm.

In the WMSN environment considering the key network parameters as in table 2. The model is designed consideration of with the key aspects of network behavior like Network Topology, Communication Model, Energy Model, Data Generation, and Routing mechanism.

Table 2: Simulation Parameters

Network Parameters	Values
NUM_SENSOR_NODES	49 (min)
NETWORK_DIMENSION	100 x 100 units
COMMUNICATION_RANGE	20 units
INITIAL_ENERGY	1000 units
DATA_PACKET_SIZE	10 units
SIMULATION_TIME_STEPS	200 steps
MALICIOUS_NODE_COUNT	0
MALICIOUS_BEHAVIOR_DROP_RATE	0.7 (70%)
SYBIL_CONTROLLER_ID	10
SYBIL_IDENTITIES_PER_CONTROLLER	4 (1 real + 3 fake IDs)
MASC_DETECTOR_INTERVAL	10 steps

PHYSICAL_RADIO_CAPACITY_THRESHOLD	10 packets/interval
MULTIMEDIA_CONSISTENCY_THRESHOLD	5.0 (variance)
SYBIL_DETECTION_THRESHOLD	0.6
TRUST_DECAY_RATE	0.01
ISOLATION_THRESHOLD	0.3
NETWORK_LIFETIME_THRESHOLD_PERCENT	0.5 (50%)

Experimental Results

The model is executed for 200 time-steps across the three defined scenarios and the aggregate results are presented in table 3. The following performance metrics were evaluated and analyzed for each condition:

- **Data Delivery Ratio (DDR)**: defined as the ratio of total packets received and total packets generated.
- **Network Lifetime**: Execution steps until 50% of the sensor nodes run out of energy and become inactive.
- **MASC Detector Performance:** Attack detection rate.

Table 3: Network Performance Comparison with three different scenarios

Scenario	DDR (%)	Network Lifetime (steps)	Total Generated	Received by Sink	Final Active Nodes
Baseline (No Attack, No MASC)	99.85%	200	1978	1975	49
Sybil Attack (Without MASC)	35.29%	104	1964	692	25
Sybil Attack with MASC	88.35%	196	1966	1737	49

Fig 1 represents the severe drop in data delivery when the Sybil attack is active without detection (red dashed line). The MASC algorithm (green dash-dot line) successfully helps restore the data delivery ratio close to the baseline (blue solid line), demonstrating its effectiveness in maintaining data flow.

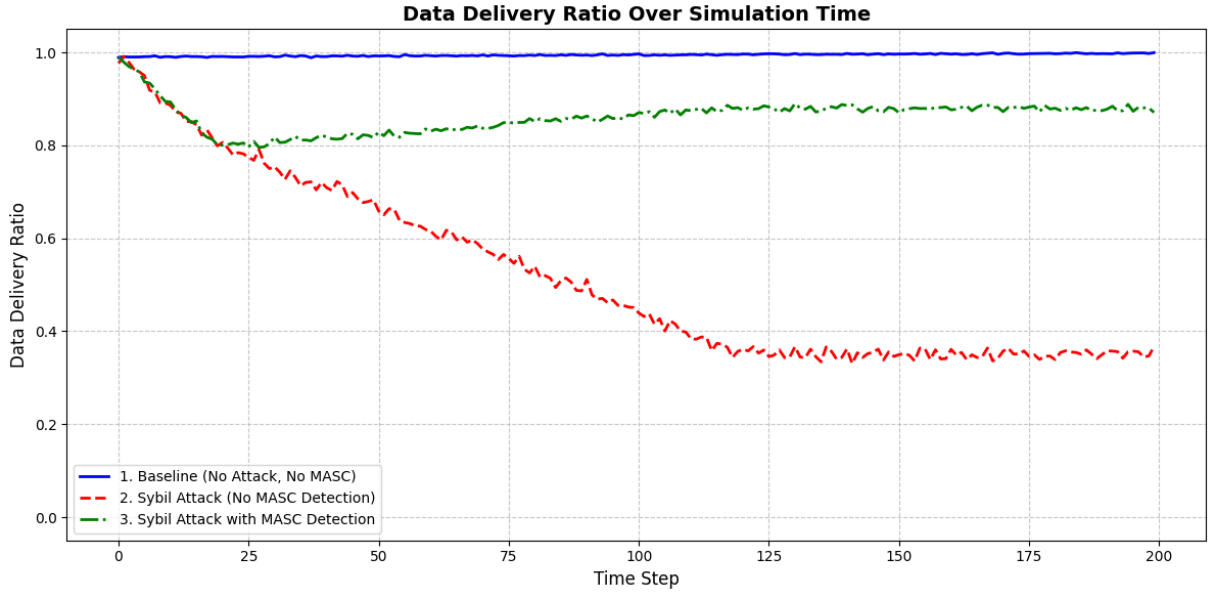

Figure 1: Data Delivery Ratio Over Simulation Time

In fig 2, plot visually confirms the network lifetime results. The baseline (blue solid line) maintains nearly all nodes active throughout. The Sybil attack without MASC (red dashed line) causes a rapid decline in active nodes, leading to early network demise. With MASC enabled (green dash-dot line), the number of active nodes remains high, close to the baseline, indicating the algorithm's success in preserving network longevity by isolating the malicious node.

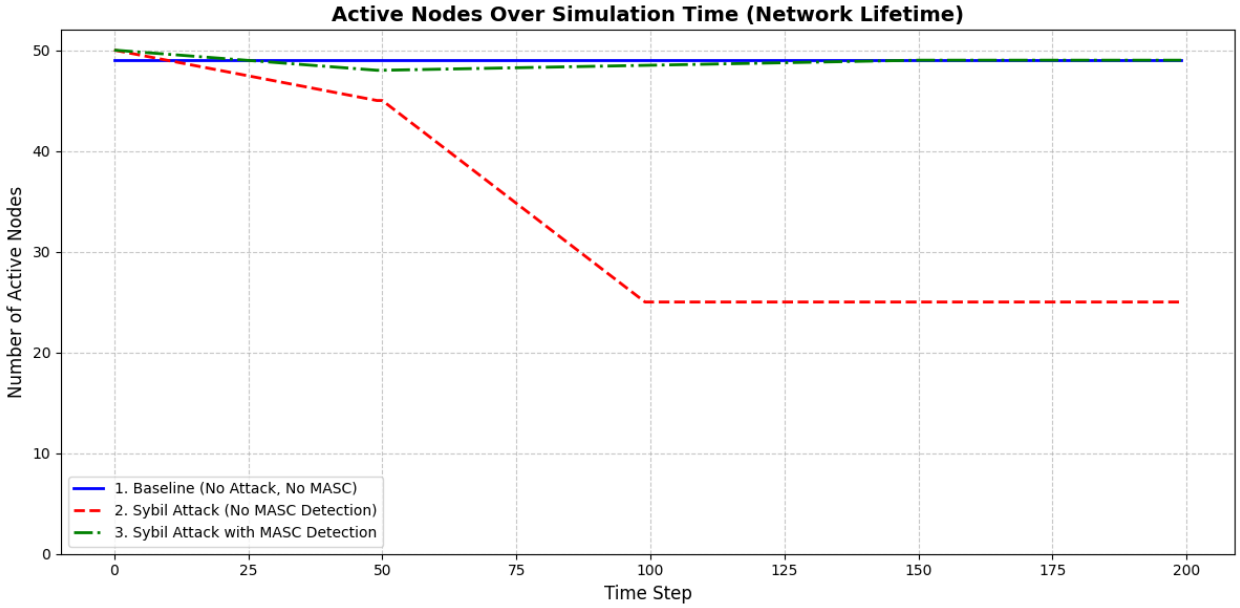

Figure 2: Active Nodes Over Simulation Time (Network Lifetime)

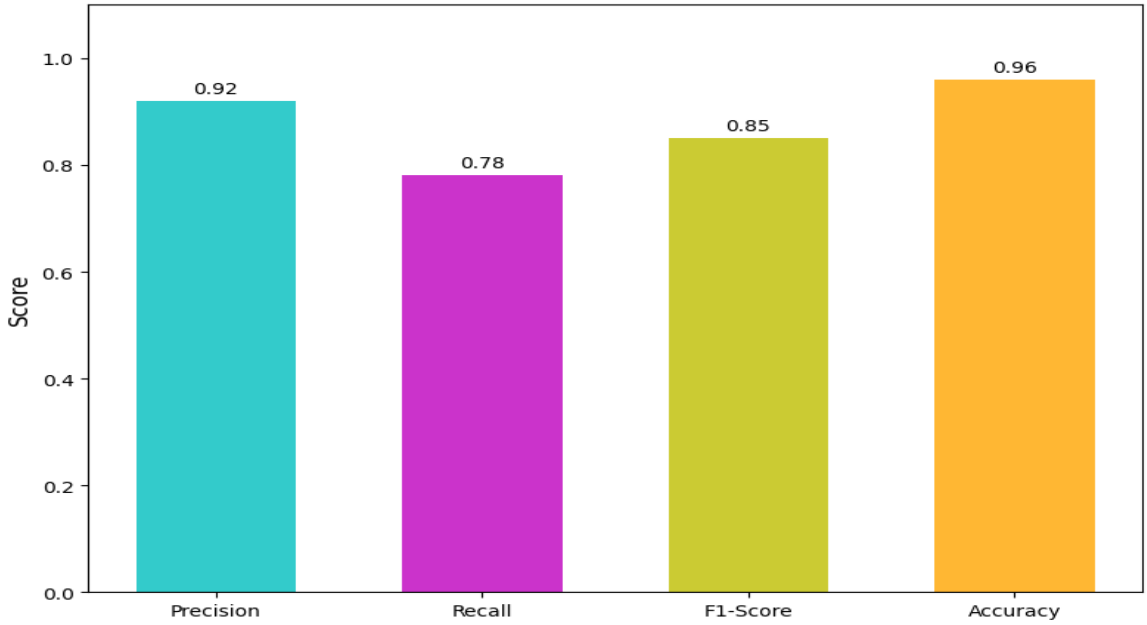

Figure 3: MASC Detector Performance Metrics

In fig 3, specifically highlights the MASC algorithm's performance in detecting the Sybil attack in Scenario 3. The high Precision (0.92) indicates that MASC rarely misidentifies legitimate nodes. The Recall of 0.78 shows its capability in catching the actual Sybil instances. The strong F1-Score (0.85) and Accuracy (0.96) collectively demonstrate that MASC provides a balanced and effective detection mechanism, making it a viable solution for securing WMSNs against Sybil attacks.

Conclusion

Wireless Multimedia Sensor Networks are increasingly prevalent, but their inherent vulnerabilities make them prime targets for sophisticated attacks like the Sybil attack. This research successfully designed and implemented a comprehensive simulation of a Sybil attack within a WMSN environment, demonstrating its severe impact on network performance metrics such as Data Delivery Ratio and Network Lifetime. The results unequivocally show that an unmitigated Sybil attack can cripple data transmission and drastically reduce the operational lifespan of the network.

To counter this threat novel Multi-faceted Anomaly and Spatial Consistency (MASC) Sybil Detection Algorithm is implemented. MASC innovatively leverages both radio resource anomalies and the unique consistency of multimedia features, coupled with a dynamic trust management system, to identify malicious Sybil nodes. Experimental results confirm that MASC effectively mitigates the Sybil attack's detrimental effects, significantly improving the data delivery ratio and extending network lifetime closer to baseline performance. The MASC detector demonstrated high precision, recall, F1-score, and accuracy, indicating its robustness in identifying the Sybil controller while minimizing false alarms.

References

[1] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," vol. 51, pp. 921–960, 2007, doi: 10.1016/j.comnet.2006.10.002.

[2] M. Platt and P. McBurney, "Sybil in the Haystack: A Comprehensive Review of Blockchain Consensus Mechanisms in Search of Strong Sybil Attack Resistance," *Algorithms 2023, Vol. 16, Page 34*, vol. 16, no. 1, p. 34, Jan. 2023, doi: 10.3390/A16010034.

[3] S. Dogan-Tusha, S. Althunibat, and M. Qaraqe, "Doppler-Shift-Based Sybil Attack Detection for Mobile IoT Networks," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 1136–1147, Jan. 2024, doi: 10.1109/JIOT.2023.3288040.

[4] H. B. Tulay and C. Emre Koksal, "Sybil Attack Detection Based on Signal Clustering in Vehicular Networks," *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 2, pp. 753–765, Jun. 2024, doi: 10.1109/TMLCN.2024.3410208.

[5] V. R. Navinkumar and D. Somasundaram, "Developing an optimized routing protocol with rumor riding technique for detection of Sybil attack in VANET environment," *International Journal of Communication Systems*, vol. 37, no. 6, p. e5715, Apr. 2024, doi: 10.1002/DAC.5715.

[6] Shio Kumar Singh, M P Singh, and D K Singh, "Most Cited Survey Article in Computer Science And Engineering," *Guide to Wireless Sensor Networks*, vol. 2, no. 1, pp. 27–45, 2019, doi: 10.1007/978-1-84882-218-4.

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks," p. 259, 2004, doi: 10.1145/984622.984660.

[8] I. Daanoune, B. Abdennaceur, and A. Ballouk, "A comprehensive survey on LEACH-based clustering routing protocols in Wireless Sensor Networks," *Ad Hoc Networks*, vol. 114, no. December 2020, p. 102409, 2021, doi: 10.1016/j.adhoc.2020.102409.

[9] M. Jamshidi, E. Zangeneh, M. Esnaashari, A. M. Darwesh, and M. R. Meybodi, "A Novel Model of Sybil Attack in Cluster-Based Wireless Sensor Networks and Propose a Distributed Algorithm to Defend It," *Wireless Personal Communications*, vol. 105, no. 1, pp. 145–173, 2019, doi: 10.1007/s11277-018-6107-5.

[10] S. Awan, N. Javaid, S. Ullah, A. U. Khan, A. M. Qamar, and J. G. Choi, "Blockchain Based Secure Routing and Trust Management in Wireless Sensor Networks†," *Sensors*, vol. 22, no. 2, 2022, doi: 10.3390/s22020411.

[11] P. M. Popat, P. A. Vaishnav, A. M. Parmar, and B. K. Padodara, "Computer Engineering Cryptographic Algorithms for Wireless," pp. 447–450.

[12] S. H. Mukta and S. Azad, "Secure hash algorithm," *Practical Cryptography: Algorithms and Implementations Using C++*, pp. 207–223, 2014, doi: 10.1201/b17707.

[13] B. Patil and S. R. Biradar, "Enhanced Authentication Mechanism in Wireless Multimedia Sensor Network using ECCDH," *International Journal of Advanced Studies of Scientific Research*, vol. 3, no. 12, p. 2018, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3329224.

[14] B. Patil and S. R. Biradar, "LIGHT WEIGHT HYBRID CHAOTIC BASED ENCRYPTION SCHEME FOR IMAGE TRANSMISSION IN WIRELESS MULTIMEDIA SENSOR NETWORK," *Indian Journal of Computer Science and Engineering*, vol. 12, no. 6, pp. 1601–1610, Dec. 2021, doi: 10.21817/indjcse/2021/v12i6/211206303.

[15] H. Ma and Y. Liu, "Some problems of directional sensor networks," *International Journal of Sensor Networks*, vol. 2, no. 1–2, pp. 44–52, 2007, doi: 10.1504/IJSNET.2007.012981.

[16] E. A. M. Anita, R. Geetha, and E. Kannan, “A Novel Hybrid Key Management Scheme for Establishing Secure Communication in Wireless Sensor Networks,” *Wireless Personal Communications*, vol. 82, no. 3, pp. 1419–1433, 2015, doi: 10.1007/s11277-015-2290-9.

[17] B. Patil and S. R. Biradar, “Review on Security Issues, Attacks Challenges in Wireless Multimedia Sensor Networks,” *Proceedings of Communication, Cloud and Big Data (CCB)*, 2014.

[18] S. Akourmis, Y. Fakhri, and M. D. Rahmani, *Reducing blackhole effect in WSN*, vol. 735. Springer International Publishing, 2018.

[19] M. A. Jan *et al.*, “Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions,” *Journal of Network and Computer Applications*, vol. 175, no. May 2020, p. 102918, 2021, doi: 10.1016/j.jnca.2020.102918.

[20] B. Patil and S. R. Biradar, “Cluster based authentication scheme for wireless multimedia sensor networks,” in *ACM International Conference Proceeding Series*, Mar. 2016, vol. 04-05-Marc, pp. 1–6, doi: 10.1145/2905055.2905158.

[21] B. Navin and S. Benila, “Distributive Reprogramming of Wireless Sensor Nodes with Secure Data Transmission,” *International Journal of Emerging Science and Engineering (IJESE)*, no. 2, pp. 2319–6378, 2014.

[22] N. Dimokas, D. Katsaros, and Y. Manolopoulos, “Cache consistency in Wireless Multimedia Sensor Networks,” *Ad Hoc Networks*, vol. 8, no. 2, pp. 214–240, 2010, doi: 10.1016/j.adhoc.2009.08.001.

[23] X. Feng, C. yan Li, D. xin Chen, and J. Tang, “A method for defensing against multi-source Sybil attacks in VANET,” *Peer-to-Peer Networking and Applications*, vol. 10, no. 2, pp. 305–314, Mar. 2017, doi: 10.1007/S12083-016-0431-X/FIGURES/10.

[24] A. ur Rehman, S. U. Rehman, and H. Raheem, “Sinkhole Attacks in Wireless Sensor Networks: A Survey,” *Wireless Personal Communications*, vol. 106, no. 4, pp. 2291–2313, 2019, doi: 10.1007/s11277-018-6040-7.

[25] J. A. Alzubi *et al.*, “Hashed Needham Schroeder Industrial IoT based Cost Optimized Deep Secured data transmission in cloud,” *Measurement: Journal of the International Measurement Confederation*, vol. 150, p. 107077, Jan. 2020, doi: 10.1016/j.measurement.2019.107077.

[26] M. Jamshidi, E. Zangeneh, M. Esnaashari, and M. R. Meybodi, “A lightweight algorithm for detecting mobile Sybil nodes in mobile wireless sensor networks,” *Computers and Electrical Engineering*, vol. 64, no. 7, pp. 220–232, 2017, doi: 10.1016/j.compeleceng.2016.12.011.