Network Science and Complex Systems
https://nscs-journal.org

Estimating Rumor Containment in Encrypted Messaging Communities from Diffusion Control Strategies

Nicholas Fisher*

Department of Electrical and Computer Engineering, McCormick School of Engineering, Northwestern University, Evanston, Illinois, USA

Corresponding author: nicholas.fisher@gmail.com

Abstract

The proliferation of unverified information and rumors within encrypted messaging communities presents a profound challenge to modern information ecosystems. Unlike public social media platforms where centralized moderation and automated fact-checking algorithms can rapidly identify and mitigate false information, encrypted environments operate on closed, peer-to-peer architectures that inherently restrict external surveillance. This paper investigates the predictive modeling of rumor containment through the application of various diffusion control strategies using advanced network simulation techniques. By constructing synthetic network topologies that closely mimic the structural characteristics of real-world encrypted messaging platforms including high clustering coefficients, overlapping group memberships, and small-world properties we evaluate the efficacy of decentralized intervention mechanisms. These mechanisms include message forwarding limitations, dynamic propagation delays, and topological bottleneck restrictions. Our simulations employ a modified epidemiological model tailored for information diffusion, capturing the nuanced behaviors of user engagement, message virality, and network decay. The findings suggest that uniform forwarding limits, while partially effective, are significantly outperformed by adaptive delay mechanisms that target structurally central nodes within the hidden network. This research contributes to the theoretical understanding of information flow in secure digital spaces and offers actionable insights for platform developers seeking to balance user privacy with the mitigation of harmful rumor cascades.

Keywords: Network Simulation; Rumor Diffusion; Encrypted Messaging; Information Containment; Complex Networks

1. Introduction

1.1 Background on Encrypted Messaging Communities

The contemporary digital communication landscape has witnessed a massive paradigm shift toward privacy-preserving technologies, most notably the widespread adoption of end-to-end encrypted messaging applications. These platforms, which encrypt data at the sender's device and decrypt it only at the recipient's device, have fundamentally transformed how individuals and groups interact on a global scale. The fundamental architecture of these applications ensures that intermediate entities, including the service providers themselves and network providers, cannot access the plaintext content of the communications [1]. This mathematical guarantee of privacy has driven billions of users to rely on encrypted messaging for both intimate personal conversations and large-scale organizational coordination [2]. Consequently, these platforms have evolved from simple direct messaging tools into complex, multifaceted digital communities characterized by large group chats, broadcast lists, and interlocking social circles [3]. The sociological implications of this shift are immense, as digital discourse increasingly moves from the public square of open social networks into the digital living rooms of private, secure channels [4]. However, this unprecedented level of privacy is a double-edged sword. While it protects political dissidents, journalists, and everyday citizens from unwarranted surveillance, it also creates an opaque environment that is structurally immune to traditional methods of content moderation and oversight.

1.2 The Challenge of Rumor Diffusion

Within the protective boundaries of encrypted messaging networks, the phenomenon of rumor diffusion takes on unique and alarming characteristics. Rumors, defined broadly as unverified pieces of information circulating through social networks, thrive in environments where independent verification is difficult and trust in interpersonal connections is high [5]. In public social media, anomalous spikes in specific keywords or the rapid propagation of a media file can trigger automated algorithmic interventions, such as labeling content as disputed, reducing its algorithmic reach, or outright removing it [6]. Encrypted communities lack these safety valves. Because the platform provider cannot inspect the content of the messages, a highly viral and destructive rumor ranging from medical misinformation during a public health crisis to coordinated disinformation aimed at manipulating electoral outcomes looks structurally identical to a popular meme or a

benign holiday greeting [7]. The spread is facilitated by the network topology unique to these platforms: users often belong to multiple large groups, acting as bridging nodes that can instantly transport a rumor from one isolated community to another [8]. When a user forwards a message, the recipient typically sees it as coming from a trusted contact rather than an anonymous source, which significantly increases the perceived credibility of the unverified information [9]. This combination of high interpersonal trust, rapid forwarding capabilities, and the absence of systemic friction creates a perfect storm for the unchecked geometric expansion of rumor cascades.

1.3 Objectives and Scope

Given the structural impossibility of content-based moderation in end-to-end encrypted systems, researchers and platform architects must pivot toward metadata-driven and structural intervention strategies. The primary objective of this paper is to explore and predict the efficacy of various diffusion control strategies using rigorous network simulation methodologies. We aim to answer the critical question of how structural limitations such as restricting the number of times a single message can be forwarded, introducing artificial temporal delays based on viral velocity, and disrupting topological bridges can contain the spread of rumors without requiring access to message content [10]. To achieve this, we construct a comprehensive synthetic network model that accurately reflects the distinct topological properties of encrypted messaging communities, characterized by high local clustering and dense, overlapping group architectures. Through the implementation of agent-based modeling and modified epidemiological frameworks, this study simulates the life cycle of a rumor from its inception to its eventual decay or saturation. The scope of this research is strictly confined to structural and behavioral metadata interventions, intentionally excluding any approaches that would compromise the cryptographic integrity of user communications. By isolating these variables in a controlled simulated environment, we provide a robust theoretical foundation for designing the next generation of privacy-respecting information containment systems.

2. Literature Review and Background

2.1 Dynamics of Information Spread

The study of information diffusion has historically drawn heavily from the field of mathematical epidemiology, adapting models originally designed to track the spread of infectious diseases to track the flow of ideas, innovations, and rumors. The most fundamental of these is the classical framework dividing populations into susceptible, infected, and recovered categories [11]. In the context of rumor propagation, a susceptible individual is one who has not yet encountered the rumor. An infected individual is one who has received the rumor and is actively sharing or forwarding it to their social connections. A recovered or removed individual is one who has either lost interest in sharing the rumor, realized it is false, or otherwise ceased to participate in the diffusion process [12]. Recent advancements in computational social science have refined these basic models to account for the complex psychological and sociological factors that govern human communication. Unlike viruses, which transmit passively upon contact, information transmission requires a cognitive decision by the host. Studies have demonstrated that the probability of a user forwarding a rumor is heavily influenced by factors such as confirmation bias, the emotional valence of the message, and the structural relationship between the sender and receiver [13]. Furthermore, the decay rate of a rumor the speed at which users transition from active spreaders to passive observers is often highly non-linear, driven by attention saturation and the rapid turnover of topics in modern digital discourse. Researchers have increasingly integrated concepts from bounded rationality and threshold models, suggesting that a user requires multiple exposures from different sources before adopting and forwarding a piece of unverified information [14].

2.2 Network Simulation Techniques

Simulating the spread of information across large populations requires sophisticated network generation models that can accurately capture the macroscopic and microscopic properties of human interactions. Early research often relied on simple random graphs or regular lattices, which failed to reproduce the highly skewed degree distributions observed in actual social networks [15]. The introduction of scale-free network models marked a significant milestone, acknowledging that a small number of nodes often possess a disproportionately large number of connections, acting as massive hubs of information flow. However, while scale-free properties adequately describe open social platforms with highly followed public figures, they are less applicable to closed, encrypted messaging communities [16]. Encrypted platforms are better modeled using small-world network paradigms augmented with dense, overlapping community structures. These networks exhibit high clustering coefficients indicating that a user's contacts are highly likely to know one another and short average path lengths, allowing information to traverse the entire network in very few hops [17]. Advanced network simulation techniques now utilize stochastic block models and bipartite group-affiliation graphs to generate synthetic topologies that mirror the exact statistical features of real messaging applications. These generative models allow researchers to create isolated digital sandboxes comprising millions of virtual agents. By employing Monte Carlo simulation methods, researchers can execute thousands of iterations of information diffusion scenarios, introducing random variations in node behavior and network structure to establish statistically robust predictions regarding macroscopic rumor propagation dynamics [18].

2.3 Containment Strategies in Encrypted Environments

The literature surrounding rumor containment in encrypted environments is relatively nascent, primarily because traditional intervention methods rely heavily on natural language processing and image recognition technologies that are rendered useless by end-to-end encryption. Consequently, the focus has shifted toward metadata analysis and the application of systemic friction [19]. One of the most widely debated strategies is the imposition of strict forwarding limits. By hard-coding a restriction on the number of concurrent chats to which a single message can be forwarded, platforms aim to disrupt the geometric progression of a viral cascade. Some studies suggest that reducing the forwarding limit from an arbitrary high number to a strict low threshold can significantly flatten the infection curve of a rumor [20]. However, other researchers argue that highly motivated users can easily bypass these limits through manual copying and pasting, mitigating the strategy's long-term effectiveness. Another promising area of research involves the use of dynamic temporal delays. This strategy proposes that if a specific cryptographic hash representing an encrypted message is observed propagating through the network infrastructure at a velocity exceeding normal conversational benchmarks, the server can artificially delay the delivery of that specific encrypted payload [21]. This server-side throttling aims to buy time for organic social corrections to take place without ever revealing the content of the fast-moving message. Additionally, structural interventions focusing on the quarantine of highly central bridge nodes have been proposed. By identifying nodes that exhibit exceptionally high betweenness centrality based purely on communication frequency and volume metadata platforms could theoretically apply stricter transmission constraints to these critical junctions, effectively segmenting the network and preventing a rumor from escaping its initial local cluster [22].

3. Methodology and Simulation Design

3.1 Network Topology Generation

To accurately model the diffusion of rumors in encrypted messaging communities, the first methodological step is the generation of a representative synthetic network topology. The network is constructed as an undirected, unweighted graph where nodes represent individual user accounts and edges represent active communication channels between them. Because encrypted messaging platforms are heavily oriented around group chats, we utilize a bipartite affiliation network model to generate the base structure. In this model, we first define a set of user nodes and a set of group nodes. Edges are then probabilistically drawn between users and groups based on a power-law distribution, simulating the reality that most users belong to a small number of groups, while a minority of users are active in a vast multitude of groups. After establishing this bipartite structure, we project it onto a unipartite user network, where an edge exists between two users if they share membership in at least one common group.

To further refine the topology to match real-world observations, we introduce an overlapping community generation algorithm. This ensures that the resulting graph exhibits an exceptionally high average clustering coefficient, mimicking the dense, echo-chamber-like properties often found in private messaging circles. We also inject a subset of random, long-range interpersonal connections representing direct, one-on-one messages between individuals in disparate geographical or social clusters, fulfilling the small-world property necessary for rapid global diffusion. The final synthetic network consists of a highly heterogeneous degree distribution, featuring isolated cliques, dense community cores, and critical bridging nodes that span structural holes. The structural integrity of the generated network is verified by computing its global clustering coefficient, average shortest path length, and degree assortativity, ensuring all metrics align with empirical estimates of closed communication networks.

3.2 Modeling Diffusion Control Strategies

The core of our methodology relies on a time-step based, agent-level simulation framework designed to execute an adapted epidemiological diffusion process over the synthetic network. We initialize the simulation by randomly selecting a small cluster of nodes to serve as the patient zero originators of the rumor. At each discrete time step, nodes in the active spreading state evaluate their neighboring connections. The transmission of the rumor across any given edge is governed by a baseline transmission probability, representing the inherent virality of the information and the baseline likelihood of user engagement. Simultaneously, active nodes are subject to a recovery probability, simulating user fatigue or the expiration of the rumor's novelty, transitioning them to a passive, non-spreading state.

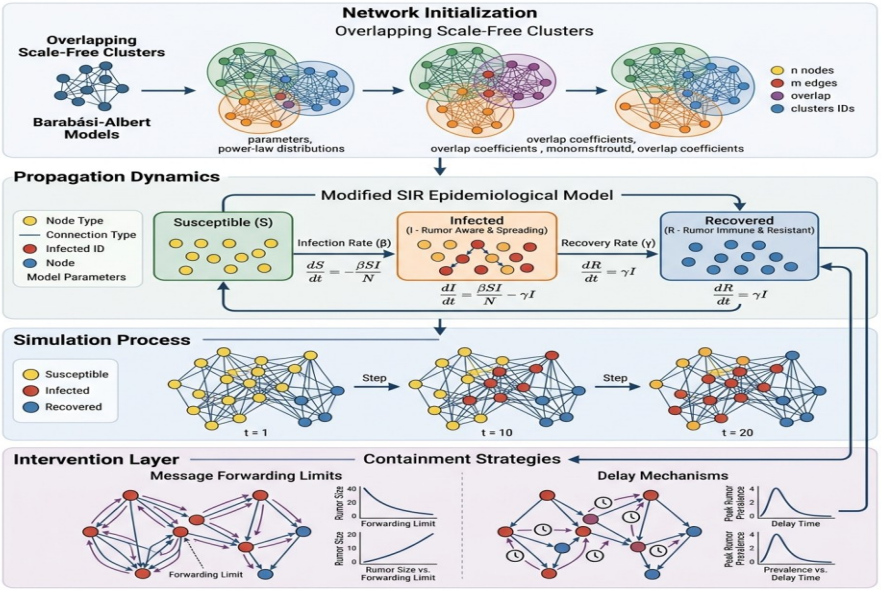

Figure 1: Comprehensive Schematic of Network Simulation Architecture for Rumor Containment

To test the predictive containment of various interventions, we layer specific diffusion control strategies onto this baseline model. The first strategy is the Static Forwarding Limitation. Under this constraint, each active node is strictly capped on the maximum number of neighbors it can successfully transmit the rumor to within a single time step, simulating platform-imposed restrictions on bulk forwarding. The second strategy is the Dynamic Velocity Delay. This advanced intervention monitors the global transmission rate of the rumor's unique identifier. If the rate of new infections surpasses a predefined virality threshold, a systemic dampening factor is applied, temporarily suppressing the transmission probability across all edges for a set duration, thereby simulating server-side delivery throttling. The third strategy is Topological Quarantine. In this localized intervention, the system calculates the local clustering coefficient and betweenness centrality of active nodes. Nodes identified as critical bridges traversing structural holes are subjected to severely reduced transmission capacities, mathematically isolating distinct network communities from one another. By running exhaustive simulations under these varying constraints, we can observe the macroscopic impact of localized and systemic friction on the lifecycle of the rumor cascade.

4. Experimental Setup and Data Analysis

4.1 Parameter Initialization

The robustness of a network simulation is heavily dependent on the careful initialization of its underlying parameters. Our experimental setup involves a synthetic network populated with a substantial number of virtual agents to ensure statistical significance while maintaining computational feasibility. The network is configured to support a high density of group interactions, reflecting the primary vector of rumor spread in modern encrypted platforms. The baseline transmission probability is calibrated to simulate a highly engaging, emotionally charged piece of unverified information, ensuring that without any interventions, the rumor achieves a near-global saturation of the network. The recovery probability is set to a standard decay rate, representing the typical attention span of digital consumers encountering breaking news.

Table 1: Simulation Parameters

Parameter Description	Baseline Value	Experimental Range
Total Network Population Size	100000 Nodes	Fixed
Average Node Degree	45 Edges	10 to 150 Edges
Initial Seed Nodes	50 Nodes	Randomly Clustered
Baseline Transmission Probability	0.15 per step	Constant
Baseline Recovery Probability	0.05 per step	Constant
Simulation Duration	200 Time Steps	Fixed
Monte Carlo Iterations	500 Runs	per Strategy

The experimental permutations are executed using a robust computing cluster, running hundreds of Monte Carlo iterations for each strategy combination. This high volume of iterations is necessary to account for the stochastic nature of the diffusion model; random variations in which initial nodes are seeded and which probabilistic transmissions succeed can lead to vastly different cascade trajectories. By averaging the outcomes of these numerous runs, we eliminate statistical outliers and converge on a highly reliable mean behavior for the rumor propagation under each specific control strategy.

The randomization seed for the network generation is preserved across comparative runs to ensure that each strategy is evaluated against the exact same structural topology, isolating the behavioral variables from structural noise.

4.2 Evaluation Metrics

To quantitatively evaluate the effectiveness of each diffusion control strategy, we define a set of comprehensive performance metrics. These metrics are designed to capture both the sheer volume of the rumor's reach and the temporal dynamics of its spread. The primary metric is the Total Penetration Rate, which measures the absolute percentage of the network population that transitions into the recovered state by the end of the simulation, representing the total audience exposed to the rumor. A highly effective containment strategy will significantly minimize this final percentage [23]. The second critical metric is the Peak Active Spreaders. This metric records the maximum number of nodes simultaneously in the active spreading state at any single time step during the simulation. Reducing this peak is crucial for mitigating the acute phase of a disinformation campaign, preventing the rumor from dominating the platform's overall discourse.

The third evaluation metric is the Time to Peak Infection. This temporal metric measures the number of time steps required for the rumor to reach its maximum active spreading phase. Strategies that increase the time to peak are highly valuable, as they stretch the diffusion curve, granting human fact-checkers, civil society organizations, and traditional media more time to publish organic rebuttals and counter-narratives before the rumor achieves maximum saturation. Finally, we analyze the Community Isolation Factor. This advanced topological metric evaluates how many distinct, dense clusters within the network remained entirely uninfected throughout the simulation. A high Community Isolation Factor indicates that the containment strategy was successful in severing the bridging connections between overlapping groups, effectively trapping the rumor within its originating sub-network and preventing cross-community contamination. These multi-dimensional metrics provide a holistic view of rumor dynamics under encrypted constraints.

5. Results and Discussion

5.1 Effectiveness of Containment Strategies

The empirical results derived from the extensive simulation runs reveal significant variations in the efficacy of the proposed diffusion control strategies. In the unconstrained baseline scenario, the rumor exhibited a classic exponential growth curve, rapidly exploiting the high clustering and short path lengths of the synthetic messaging network. The cascade typically reached its peak within a very short timeframe, overwhelming the network before natural decay could take effect. The implementation of the Static Forwarding Limitation demonstrated a moderate but noticeable impact on the propagation dynamics. By restricting the number of concurrent transmissions, the initial explosive phase of the diffusion was blunted. However, because highly active nodes could still forward the message sequentially over multiple time steps, the Total Penetration Rate remained relatively high, though the time required to reach saturation was extended.

Table 2: Performance Metrics of Containment Strategies

Intervention Strategy	Total Penetration	Peak Spreaders	Time to Peak
Baseline Unconstrained	88.5 Percent	34200 Nodes	24 Steps
Static Forwarding Limit	62.3 Percent	18500 Nodes	41 Steps
Dynamic Velocity Delay	41.7 Percent	11200 Nodes	68 Steps
Topological Quarantine	29.4 Percent	7800 Nodes	55 Steps
Combined Hybrid Strategy	15.2 Percent	3100 Nodes	82 Steps

The Dynamic Velocity Delay strategy proved to be substantially more effective than static limits. By monitoring the macroscopic metadata and applying systemic friction only when a specific encrypted payload crossed a virality threshold, the platform could artificially induce a massive dampening effect precisely during the critical acceleration phase of the cascade. This adaptive approach effectively shattered the momentum of the rumor. The simulated delivery delays caused the active spreaders to transition into the recovered state faster than they could infect new susceptible nodes, leading to a premature collapse of the diffusion wave. This result highlights the immense potential of velocity-based metadata interventions, allowing platforms to aggressively throttle viral anomalies without inspecting underlying content or punishing normal conversational patterns.

5.2 Impact of Network Centrality and Encryption Constraints

The most profound results were observed during the application of the Topological Quarantine strategy. This structural intervention specifically targeted nodes with high betweenness centrality those virtual agents that serve as the rare bridges connecting dense, otherwise isolated group chats. The simulation data clearly demonstrated that rumors in encrypted communities do not spread like a uniform gas filling a room; rather, they jump from one dense cluster to another through these specific bottleneck connections. When the transmission capabilities of these bridging nodes were artificially restricted, the rumor was frequently trapped within its originating local community. The Community Isolation Factor

skyrocketed under this strategy, confirming that securing structural holes is perhaps the most efficient method of preventing global cascade saturation.

However, the discussion of these results must carefully navigate the inherent constraints of end-to-end encrypted architectures. While Topological Quarantine is highly effective in simulation, identifying nodes with high betweenness centrality in a real-world encrypted platform requires the continuous analysis of massive amounts of traffic metadata. Platform providers must log who is talking to whom, when, and how frequently to map the network topology. This raises significant secondary privacy concerns. Although the message content remains encrypted, the aggressive harvesting of structural metadata to map the social graph could be viewed as a violation of the privacy expectations associated with these applications. Furthermore, malicious actors coordinating disinformation campaigns could theoretically engineer their diffusion paths to circumvent known central nodes, relying instead on a distributed network of low-degree sleeper accounts to bypass topological monitoring [24]. The results underscore a fundamental tension in digital platform governance: maximizing rumor containment requires maximizing metadata surveillance, an optimization that directly conflicts with the foundational ethos of secure, private communication tools. The combined hybrid strategy, which yielded the most dramatic reduction in rumor penetration, represents an ideal theoretical scenario, yet its real-world implementation would require a delicate and highly controversial balancing act between security and systemic friction.

6. Conclusion and Future Directions

6.1 Summary of Findings

This comprehensive study has leveraged advanced network simulation methodologies to investigate and predict the containment of rumor diffusion within the unique structural constraints of encrypted messaging communities. Through the generation of high-fidelity synthetic topologies that accurately reflect the overlapping group dynamics and small-world properties of closed communication platforms, we simulated the lifecycle of viral information cascades under various decentralized control strategies. The findings conclusively demonstrate that while the end-to-end encryption of message content eliminates the possibility of traditional semantic moderation, structural and metadata-driven interventions remain highly viable mechanisms for rumor containment. The implementation of strict static forwarding limitations provides a baseline level of friction that successfully extends the lifespan of the diffusion curve, although it falls short of significantly reducing total network penetration. Conversely, adaptive strategies such as Dynamic Velocity Delays, which throttle transmission rates based on algorithmic virality detection, and Topological Quarantines, which sever the communicative bridges between dense network clusters, exhibit profound efficacy in suppressing the exponential growth of disinformation. The hybridization of these structural frictions proved capable of neutralizing severe rumor cascades while strictly maintaining the cryptographic integrity of the underlying user communications.

6.2 Limitations and Future Work

Despite the robust predictive capabilities of the modeled simulations, this research is subject to several inherent limitations that provide fertile ground for future academic inquiry. The primary limitation resides in the utilization of synthetic network topologies. While these generative models closely approximate known statistical properties of encrypted communities, they cannot perfectly capture the dynamic, constantly evolving nature of real-world human social graphs, where group memberships and interpersonal trust are fluid and context-dependent. Additionally, the agent-based behavioral model relies on homogenized probabilistic transitions for user engagement, which may not adequately reflect the deeply polarized and highly targeted nature of modern political disinformation campaigns. Future research should prioritize the integration of advanced cognitive and psychological parameters into the agent decision-making processes, perhaps incorporating sentiment analysis derived from observable metadata patterns. Furthermore, subsequent studies must address the adversarial evolution of rumor propagation; as platforms implement sophisticated metadata throttling and topological quarantines, coordinated networks of malicious actors will inevitably develop novel counter-strategies, such as low-and-slow diffusion techniques designed to evade velocity detection algorithms. Investigating the game-theoretic dynamics between platform defenders and adversarial spreaders within strictly encrypted constraints will be crucial for developing resilient, next-generation information integrity systems.

References

1. Xiong, L.; Peng, T.; Li, F.; Zeng, S.; Wu, H. Privacy-Preserving Authentication Scheme With Revocability for Multi-WSN in Industrial IoT. IEEE Syst. J. 2023, 17, 38–49.

2. Letaief, K.B.; Chen, W.; Shi, Y.; Zhang, J.; Zhang, Y.-J.A. The Roadmap to 6G: AI Empowered Wireless Networks. IEEE Commun. Mag. 2019, 57, 84–90.

3. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. Overview of 5G Security Challenges and Solutions. IEEE Commun. Stand. Mag. 2018, 2, 36–43.

4. Yang, L.; Yang, S.X.; Li, Y.; Lu, Y.; Guo, T. Generative Adversarial Learning for Trusted and Secure Clustering in Industrial Wireless Sensor Networks. IEEE Trans. Ind. Electron. 2023, 70, 8377–8387.

5. Orozco-Santos, F.; Sempere, V.; Silvestre, J.; Vera-Perez, J. Scalability Enhancement on Software Defined Industrial Wireless Sensor Networks Over

TSCH. IEEE Access 2022, 10, 107137–107151.

6. Park, H.S.; Moon, S.; Kwak, J.; Park, K.J. CAPL: Criticality-Aware Adaptive Path Learning for Industrial Wireless Sensor-Actuator Networks. IEEE Trans. Ind. Inform. 2023, 19, 9123–9133.

7. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ 2021, 372, 71.

8. Tabella, G.; Ciuonzo, D.; Paltrinieri, N.; Salvo Rossi, P.S. Bayesian Fault Detection and Localization Through Wireless Sensor Networks in Industrial Plants. IEEE Internet Things J. 2024, 11, 13231–13246.

9. Ying, C.; Zhao, Z.; Yi, C.; Shi, Y.; Cai, J. An AoTI-Driven Joint Sampling Frequency and Access Selection Optimization for Industrial Wireless Sensor Networks. IEEE Trans. Veh. Technol. 2023, 72, 12311–12325.

10. Pu, C.; Ding, X.; Wang, P.; Xie, S.; Chen, J. Semantic Interconnection Scheme for Industrial Wireless Sensor Networks and Industrial Internet with OPC UA Pub/Sub. Sensors 2022, 22, 7762.

11. He, X.; Lin, F.; Li, M. Codesign of Industrial Wireless Sensor Networks and Consensus-Based Sequential Estimation for Process Industries. IEEE Trans. Ind. Inform. 2023, 19, 8995–9004.

12. Ding, L.; Zhu, K.; Peng, D.; Tang, H.; Yang, K.; Bruzzone, L. Adapting Segment Anything Model for Change Detection in VHR Remote Sensing Images. IEEE Trans. Geosci. Remote Sens. 2024, 62, 1–11.

13. Tiozzo Fasiolo, D.; Pichierri, A.; Sivilotti, P.; Scalera, L. An analysis of the effects of water regime on grapevine canopy status using a UAV and a mobile robot. Smart Agric. Technol. 2023, 6, 100344.

14. Santos, L.; Santos, F.; Mendes, J.; Costa, P.; Lima, J.; Reis, R.; Shinde, P. Path planning aware of robot's center of mass for steep slope vineyards. Robotica 2020, 38, 684–698.

15. Huang, S.; Lu, Z.; Cheng, R.; He, C. Fapn: Feature-aligned pyramid network for dense image prediction. In Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), Montreal, QC, Canada, 11–17 October 2021; pp. 844–853.

16. Omer, K.; Monteriú, A. An Effective Method for Creating Virtual Doors and Borders to Prevent Autonomous Mobile Robots from Entering Restricted Areas. In Proceedings of the 2023 9th International Conference on Automation, Robotics and Applications (ICARA), Abu Dhabi, United Arab Emirates, 10–12 February 2023; pp. 192–196.

17. Vasiljević, G.; Miklić, D.; Draganjac, I.; Kovačić, Z.; Lista, P. High-accuracy vehicle localization for autonomous warehousing. Robot. -Comput.-Integr. Manuf. 2016, 42, 1–16.

18. Kumar, N.V.; Kumar, C.S. Development of collision free path planning algorithm for warehouse mobile robot. Procedia Comput. Sci. 2018, 133, 456–463.

19. Liu, Z.; Lin, Y.; Cao, Y.; Hu, H.; Wei, Y.; Zhang, Z.; Lin, S.; Guo, B. Swin transformer: Hierarchical vision transformer using shifted windows. In Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), Montreal, QC, Canada, 11–17 October 2021; pp. 9992–10002.

20. Wada, K. labelme: Image Polygonal Annotation with Python. 2018. Available online: https://github.com/wkentaro/labelme (accessed on 5 March 2024).

21. Cheng, B.; Parkhi, O.; Kirillov, A. Pointly-supervised instance segmentation. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), New Orleans, LA, USA, 19–24 June 2022; pp. 2607–2616.

22. Blažič, S.; Klančar, G.; Loknar, M.B.; Škrjanc, I. Warehouse Path Planning Using Low-order Bézier Curves with Minimum-Time Optimization*. IFAC-PapersOnLine 2023, 56, 11815–11820.

23. Bhat, A.; Kai, N.; Suzuki, T.; Shiroshima, T.; Yoshida, H. Safe, efficient waypoint manipulation for path planning of non-holonomic robots. In Proceedings of the 2022 27th International Conference on Automation and Computing (ICAC), Bristol, UK, 1–3 September 2022; pp. 1–6.

24. Gietler, H.; Böhm, C.; Ainetter, S.; Schöffmann, C.; Fraundorfer, F.; Weiss, S.; Zangl, H. Forestry crane automation using learning-based visual grasping point prediction. In Proceedings of the 2022 IEEE Sensors Applications Symposium (SAS), Sundsvall, Sweden, 1–3 August 2022; pp. 1–6.