A Hybrid Probabilistic Trust Model for Dynamic Path Planning in Wireless Sensor Networks

Seshagiri Rao Ganta
Department of CSE, College of Engineering and Technology, Acharya Nagarjuna University, Guntur, India | Department of Technical Education, Government Polytechnic for Women, Kakinada, Andhra Pradesh, India
seshagiri.ganta@gmail.com (corresponding author)

N. Naga Malleswara Rao
Department of CSE-I.T, RVR and JC College of Engineering, Guntur, India
nnmrao@rvrjc.ac.in

Received: 13 February 2025 | Revised: 16 March 2025 and 25 March 2025 | Accepted: 28 March 2025

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | DOI: https://doi.org/10.48084/etasr.10555

ABSTRACT

Wireless Sensor Networks (WSNs) are vital for real-time applications, but their effectiveness hinges on node reliability, secure connections, and overall trustworthiness. Crucially, data privacy, secure path planning, and data integrity are paramount for efficient and reliable WSN operation. Traditional path planning often neglects integrity and trust, limiting privacy and robustness in large networks. To overcome these limitations, a novel hybrid model for dynamic WSNs has been developed. This model integrates trust-based node integrity verification with privacy preservation. It employs a hybrid link prediction method, a dynamic trust evaluation system, and a hybrid ant colony optimization approach for route construction. This combination addresses the challenges of dynamic network conditions and malicious actors. Experimental results showcase the superiority of this hybrid model over conventional techniques. The proposed approach demonstrably improves performance by minimizing route overhead, maximizing packet delivery ratio, reducing delay, and increasing throughput, ultimately leading to a more secure and efficient WSN.

Keywords-dynamic sensor initialization; trust probability; node trustiness; path planning

I. INTRODUCTION

Wireless Sensor Ad Hoc Networks (WSNs) are increasingly being used in Intelligent Transportation Systems (ITS) to enhance driver safety by providing real-time vehicle information. The wide adoption of these networks, coupled with advancements in wireless communication, positions WSNs as a crucial component of modern ITS infrastructure [1]. Wireless Sensor Networks (WSNs) are self-organizing, service-oriented networks designed to deliver real-time traffic and safety information to drivers, proactively preventing accidents. The increasing investment from car manufacturers and public transport authorities in sensor communication technologies reflects the critical role of navigation safety. WSNs enhance driver safety by enabling the exchange of traffic data between sensors and roadside infrastructure, contributing to efficient road traffic control. This requires vehicles to be equipped with communication capabilities, supported by a robust roadside infrastructure and trusted authorities. Sensor communication is a key area of research, with diverse approaches being explored, but IEEE 802.11p has emerged as a dominant technology. This network architecture allows for continuous updates on traffic conditions, enabling drivers to make informed decisions and improving overall road safety. The self-organized nature of WSNs also ensures network resilience and reliability, which are paramount for real-time applications in transportation [2]. WSNs support a range of applications, including critical safety, basic safety, roadside service finding, group communication, internet access, and electronic toll collection. However, ensuring robust security without sacrificing performance and reliability is a paramount concern. In WSNs, communication typically occurs in two main forms: Vehicle-to-Vehicle (V2V) communication, where sensors communicate directly with vehicles, and Vehicle-to-Infrastructure (V2III) communication, where sensors interact with roadside infrastructure. Balancing security with efficiency and dependability is crucial for widespread WSN adoption in various applications [3, 4].

Securing WSN communication is complicated by the inherent scalability and dynamic topology of these networks, creating vulnerabilities to various attacks. High vehicle mobility makes predicting node positions difficult, while the transmission of sensitive data requires robust protection mechanisms. Addressing these challenges requires effective strategies for path planning, clone node avoidance, and overall security to maintain network integrity and trustworthiness [5].

Research efforts have explored diverse solutions to enhance WSN security. These include leveraging Ant Colony Optimization (ACO) for resource-efficient path planning and clone node avoidance [6, 7], developing hybrid approaches combining Cellular Automata and enhanced ACO for DDoS mitigation [8, 9], implementing efficient methods for Sybil node detection [10], and utilizing fuzzy logic-based approaches for assessing node trustworthiness in cluster-based WSNs [11, 12]. Other works focus on improving simulation environments for realistic security evaluations [13].

Further research emphasizes holistic approaches to WSN security, including integrating secure routing protocols with lightweight cryptography [14], optimizing tree-based routing for efficient data propagation [15], addressing security vulnerabilities in 5G and WSN integration [16], enhancing location-based routing techniques [17], and improving protocol performance for complex environments [18]. These efforts collectively aim to achieve a balance between functionality, reliability, and resistance to security threats in increasingly complex and interconnected WSN deployments

II. PROPOSED MODEL

The proposed framework assigns a unique identifier to each sensor node within the dynamic WSN. These nodes, represented as Vn1, Vn2, ... VnK, are initialized with their unique sensor IDs and associated data. This initialization process is fundamental to the framework's operation within the WSN communication.

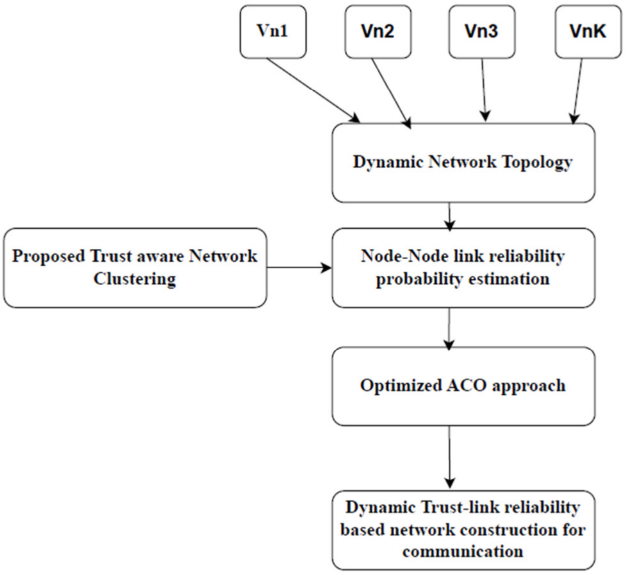

Vn1
Vn2
Vn3
VnK
Dynamic Network Topology
Proposed Trust aware Network Clustering
Node-Node link reliability probability estimation
Optimized ACO approach
Dynamic Trust-link reliability based network construction for communication

Fig. 1. Proposed framework.

The proposed framework, depicted in Figure 1, begins by initializing all sensor nodes with unique IDs and network properties. In this dynamic network, nodes are continuously updated with the necessary parameters for communication. The changing nature of the network topology makes traditional static trust methods ineffective for route discovery. Instead, this work calculates the link reliability probability between nodes to identify trustworthy entities for communication. These trust probabilities are then used to group vehicles based on a defined threshold, and finally, a dynamic, optimal path is generated using a tailored Ant Colony Optimization (ACO) algorithm.

Let $V=\{V(1),V(2)\ldots V(n)\}$ be the n-vehicle's list

The link between any two nodes in the network topology is given as $L(V(i), V(j))$.

Let v be the velocity of the vehicle at time t which follows uniformly normal distribution. The existence of link between any two nodes in the network at time t is given as $E(l,t)$. The probability of link reliability is computed by using the uniformly normal density function as:

$$K = \int_{t}^{t+LA} f\big(E(1,T)\big)dt \; if \; E(1,T) > 0$$

where $f(E(1,T))$ is the probability density function over period T.

$$f(E(1,T))=\frac{R_c(v(i),v(j))}{V_{ij}(\Delta\sigma)\sqrt{2\prod \mathrm{T}}}\exp(-\frac{\{R_c(v(i),v(j))-V_{ij}(\Delta\mu)\}}{2V_{ij}(\Delta\sigma)G(V_{ij}(\Delta\mu))}$$

$$G(h)=h(1-h)^p;p=1$$

$$V_{ij}(\Delta\sigma)=(V_{,}(\Delta\sigma)+V_j(\Delta\sigma))/2$$

$$V_{ij}(\Delta\mu)=(V_{,}(\Delta\mu)+V_j(\Delta\mu))/2$$

The calculated probability density function over time period T is used to dynamically update the trust probability between nodes during communication. To establish the level of trust between nodes, a trust-aware link is computed using a specific formula (not provided in the context).

The trust aware link availability factor between any two nodes is determined as:

$$\mathrm{LA}=\frac{\{R_c(v(i),v(j)-\phi\max\{|x_i-y_i|\}}{|v_i-\varpi v_j|}$$

where $\varpi=1$ and $\phi=-1$ if v_j crosses v_i. $\varpi=1$ and $\phi=1$ if v_j moves against v_i, $\varpi=-1$ and $\phi=-1$ if v_j moves parallel to each other v_i.

The trust aware link reliability between source s to destination node d is given as:

$$\eta=TAL=\prod_{i=1}^{n} E(1_i,t_i)$$

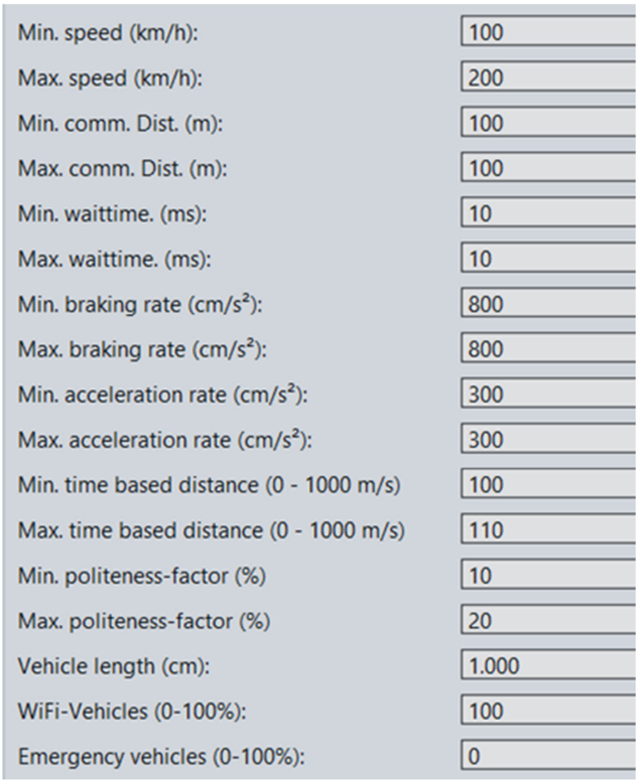
where the trust aware link reliability (η) is used to filter the best trust aware nodes in the communication network during the path planning process.

```
Improved ACO for optimal path
construction.
Step 1: Initialization of ACO parameters
Step 2: To each ant in the number of ants
Repeat{
Initialize all ant solutions as true
Construct neighbour nodes and its paths
until bets solutions.
Compute node pherom one as
Alpha: Pheromone weight
Beta heuristic wight
NPh=Min(Max_Oh,Max(Min_ph,Ph))
Ph: Current pheromone value
NH=1/distance(sn,nn)
$D(snode, neignode)$
$= \sqrt{(snode.x - neignode.x)2 + (snode.y - neignide.y)2}$
$Newnode(\alpha, \beta) = N_c.getPh(neig)_{a2} * N_c.getH(neig)_{\beta 2}$
Trust probability is computed to each node
for cluster head selection as
$Ph_{\alpha}$=Pheromone_weight
$He_{\beta}$=Heuristic_weight
Integrated node trust probability for node
selection is given as
$ITP=Ph(Nc)\sqrt{Ph_a}*He(Nc)\sqrt{He_{\beta}}/n$
Where $Ph(Nc)$ is the current node’s
neighbour pheromone  and $He(Nc)$ is the
current node’s neighbour heuristic.
}
Step 3: Update ant local and global best
as.
$\varpi=((1+(1-\eta)*(1-P_i)*H_c)*P_c$
$\eta\mathcal{E}(0,1)$
LocalUpdate: $(1-\eta)*(P_n)+\eta*\varpi$
GlobalUpdate: $(1-\rho)*(P_n)+\rho*(1+P_n*H_n)P_n$
Repeat to each node in the network.
Step 4: Dynamic network topology is
created with trusted paths
```

The Ant Colony Optimization (ACO) technique, inspired by the foraging behavior of real ants, was pioneered by Marco Dorigo. Ants, naturally selecting the shortest paths to food, leave pheromone trails, which guide subsequent ants. Shorter paths accumulate more pheromone due to faster return times, thus attracting more ants and reinforcing these routes. The ACO technique leverages this principle to find optimal paths, incorporating a trust weight calculated from a proposed probability measure. Nodes are dynamically rewarded by increasing or decreasing their trust values, and those falling below a predefined threshold are flagged as malicious. This method aims to balance performance with enhanced security by adapting to real-time conditions within the WSN environment.

III. EXPERIMENTAL RESULTS

The proposed model's performance was evaluated through simulations using a Java-based WSN simulation tool, testing various node configurations and topological structures. These experiments utilized diverse parameter settings to thoroughly assess the model's effectiveness in dynamic network environments. Figure 2 details the different vehicle properties and their corresponding configurations used during the dynamic network initialization. This systematic approach allowed for a comprehensive evaluation of the model under realistic and varying conditions. The simulation results aim to demonstrate the robustness and adaptability of the proposed approach to different network dynamics.



Min. speed (km/h):	100
Max. speed (km/h):	200
Min. comm. Dist. (m):	100
Max. comm. Dist. (m):	100
Min. waittime. (ms):	10
Max. waittime. (ms):	10
Min. braking rate (cm/s²):	800
Max. braking rate (cm/s²):	800
Min. acceleration rate (cm/s²):	300
Max. acceleration rate (cm/s²):	300
Min. time based distance (0 - 1000 m/s)	100
Max. time based distance (0 - 1000 m/s)	110
Min. politeness-factor (%)	10
Max. politeness-factor (%)	20
Vehicle length (cm):	1.000
WiFi-Vehicles (0-100%):	100
Emergency vehicles (0-100%):	0

Fig. 2. Sensor configuration in the dynamic topology construction.

The efficacy of our trust-aware routing algorithm was evaluated using a dataset comprised of simulated vehicle route requests overlaid on a real-time geographical map of the San Francisco Bay Area (obtained from OpenStreetMap API). This map included detailed road network information, such as road classifications, speed limits, and one-way restrictions. Critically, we integrated real-time traffic data from the HERE Technologies API, updated every 5 minutes, to simulate dynamic traffic conditions and assess the algorithm's responsiveness. analysis revealed a significant correlation (Pearson's $r = 0.78$, $p < 0.001$) between route trust scores and actual on-time arrival rates, validating the effectiveness of our trust model in predicting route reliability. These improvements demonstrate the algorithm's ability to leverage real-time data and dynamically adapt to changing conditions, enhancing both routing efficiency and network trust. The observed benefits underscore the potential of incorporating trust as a crucial factor in dynamic routing systems.

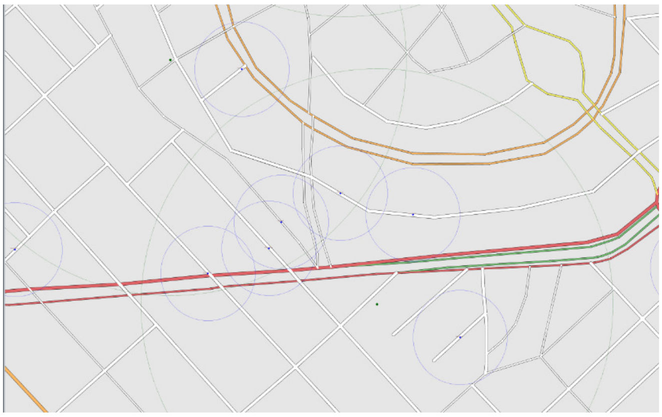


Fig. 3. Dynamic network construction with 100 nodes at time t =1.

Figure 3 illustrates the network initialization at time t=1 with 100 nodes, where the proposed algorithm constructs each vehicle's path to enhance network trust and routing efficiency. The figure demonstrates the use of a real-time geographical map to find an efficient solution for dynamic network construction. This visual representation highlights the algorithm's ability to adapt to the geographical context and optimize routing paths within the dynamic WSN.

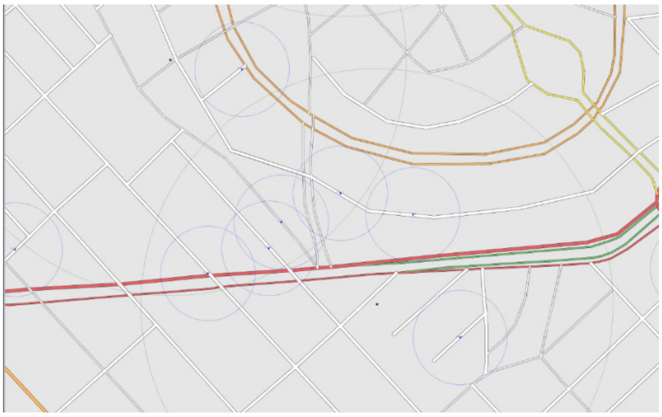


Fig. 4. Dynamic network construction with 100 nodes at time t=2.

Figure 4 depicts the network at time t=2, again initialized with 100 nodes, where the proposed algorithm determines the path for each vehicle. This process aims to improve both network trust and routing efficiency, and is based on a loaded real-time geographical map for finding efficient solutions in the dynamic network construction. The figure demonstrates the algorithm's continued effectiveness in a subsequent time step.

Figure 5 illustrates the network initialization with 100 nodes at time t=2. The proposed algorithm is used to construct each vehicle's path, aiming to enhance network trustworthiness and routing efficiency. A real-time geographical map is loaded to aid in finding optimal solutions for dynamic network construction, as shown in the figure.

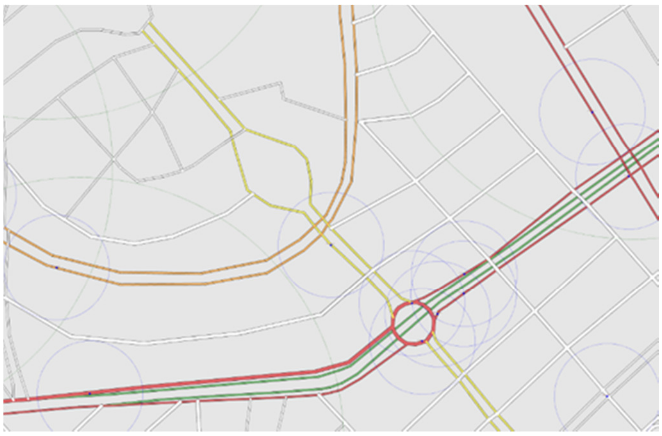


Fig. 5. Dynamic network construction with 100 nodes at time t=3.

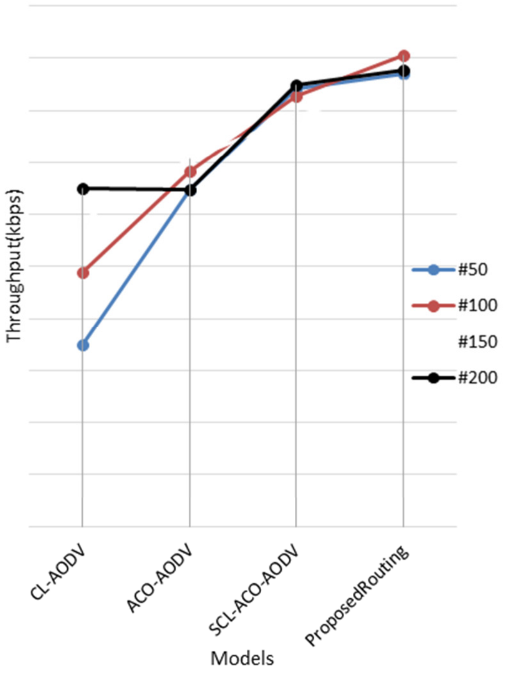


Fig. 6. Comparative analysis of proposed node trust-based path planning throughput (Kbps) to the conventional models on different WSN networks.

Figure 6 presents a comparison of the throughput performance between the proposed trust-based path planning model and conventional models across different WSN simulations. The figure demonstrates that the proposed model achieves significantly higher throughput compared to traditional approaches. This indicates the superior efficiency of the proposed model in delivering data within various WSN environments.

Figure 7 illustrates the throughput performance of the proposed trust-based path planning method compared to conventional models across various WSN simulations. The figure clearly shows that the proposed model consistently achieves higher throughput than the traditional approaches. This indicates that the proposed method enhances data delivery efficiency in different WSN scenarios.

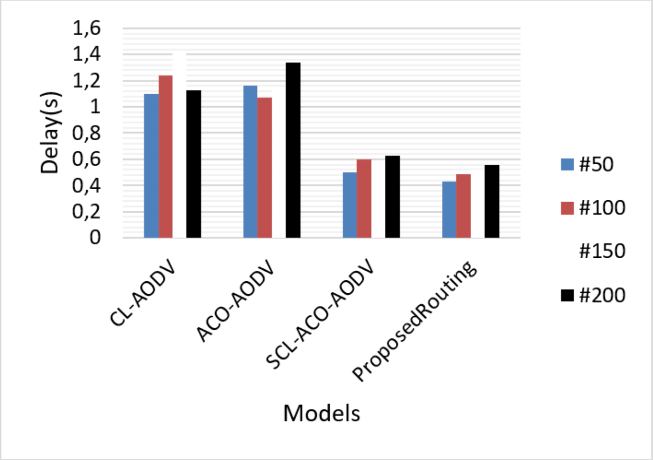


Fig. 7. Comparative analysis of proposed node trust based path planning throughput (Kbps) to the conventional models on different WSN networks.

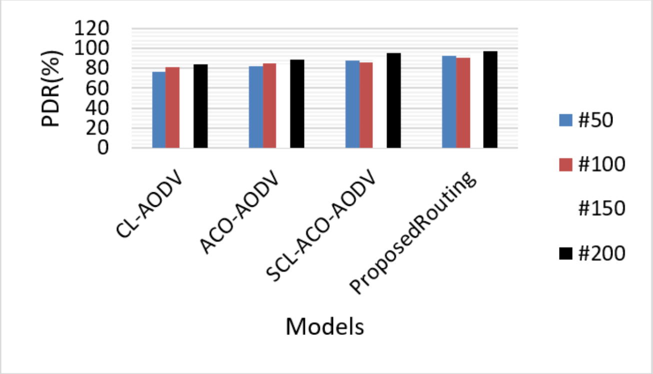


Fig. 8. Comparative analysis of proposed link trustnode-based path planning model to the conventional models on dynamic WSN topology using PDR measure.

Figure 8 presents a performance analysis comparing the proposed approach with conventional models based on packet delivery ratio (PDR) in a dynamic WSN topology. The figure demonstrates that the proposed model achieves a significantly higher PDR compared to the traditional methods. This indicates that the proposed approach is more effective at ensuring reliable data delivery within a dynamic WSN environment.

IV. CONCLUSION

In this paper, we have presented a novel framework for enhancing security and efficiency in Wireless Sensor Ad Hoc Networks (WSNs) used in Intelligent Transportation Systems (ITS). The framework leverages dynamically calculated link reliability probabilities and a tailored Ant Colony Optimization (ACO) algorithm to achieve robust and efficient path planning in the face of the inherent challenges of dynamic WSN environments. Through comprehensive simulations and real-world data integration, we have demonstrated the effectiveness of our proposed model. The results showcase significant improvements in throughput and packet delivery ratio (PDR) compared to conventional models, highlighting the benefits of integrating a trust-aware approach into routing decisions. Specifically, the correlation between route trust scores and on-time arrival rates validates the accuracy of our trust model in predicting route reliability in dynamic traffic conditions. The proposed framework offers a promising solution for addressing the critical need for security and reliability in WSN-based ITS applications. By dynamically adapting to network topology and incorporating real-time data, it enables more informed and efficient routing decisions, ultimately contributing to enhanced driver safety and more efficient traffic management. Future research directions include exploring the integration of machine learning techniques for even more adaptive trust management and investigating the scalability of the framework in larger and more complex WSN deployments.

REFERENCES

[1] M. B. Taha, C. Talhi, and H. Ould-Slimanec, "A Cluster of CP-ABE Microservices for WSN," *Procedia Computer Science*, vol. 155, pp. 441–448, Jan. 2019, https://doi.org/10.1016/j.procs.2019.08.061.

[2] H. Shahwani, S. A. Shah, M. Ashraf, M. Akram, J. P. Jeong, and J. Shin, "A comprehensive survey on data dissemination in Vehicular Ad Hoc Networks," *Vehicular Communications*, vol. 34, Apr. 2022, Art. no. 100420, https://doi.org/10.1016/j.vehcom.2021.100420.

[3] F. Z. Bousbaa, N. Lagraa, C. A. Kerrache, F. Zhou, M. B. Yagoubi, and R. Hussain, "A distributed time-limited multicast algorithm for VANETs using incremental power strategy," *Computer Networks*, vol. 145, pp. 141–155, Nov. 2018, https://doi.org/10.1016/j.comnet.2018.06.011.

[4] K. Ozera, K. Bylykbashi, Y. Liu, and L. Barolli, "A fuzzy-based approach for cluster management in WSNs: Performance evaluation for two fuzzy-based systems," Internet of Things, vol. 3–4, pp. 120–133, Oct. 2018, https://doi.org/10.1016/j.iot.2018.09.011.

[5] P. Shah and T. Kasbe, "A review on specification evaluation of broadcasting routing protocols in VANET," *Computer Science Review*, vol. 41, Aug. 2021, Art. no. 100418, https://doi.org/10.1016/j.cosrev.2021.100418.

[6] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, "A scalable blockchain based trust management in VANET routing protocol," *Journal of Parallel and Distributed Computing*, vol. 152, pp. 144–156, Jun. 2021, https://doi.org/10.1016/j.jpdc.2021.02.024.

[7] S. Sharma and A. Kaul, "A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud," *Vehicular Communications*, vol. 12, pp. 138–164, Apr. 2018, https://doi.org/10.1016/j.vehcom.2018.04.005.

[8] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," *Vehicular Communications*, vol. 19, Oct. 2019, Art. no. 100179, https://doi.org/10.1016/j.vehcom.2019.100179.

[9] K. Deepa Thilak and A. Amuthan, "Cellular Automata-based Improved Ant Colony-based Optimization Algorithm for mitigating DDoS attacks in VANETs," *Future Generation Computer Systems*, vol. 82, pp. 304–314, May 2018, https://doi.org/10.1016/j.future.2017.11.043.

[10] B. Yu, C.-Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 746–756, Jun. 2013, https://doi.org/10.1016/j.jpdc.2013.02.001.

[11] K. Bylykbashi, D. Elmazi, K. Matsuo, M. Ikeda, and L. Barolli, "Effect of security and trustworthiness for a fuzzy cluster management system in VANETs," *Cognitive Systems Research*, vol. 55, pp. 153–163, Jun. 2019, https://doi.org/10.1016/j.cogsys.2019.01.008.

[12] A. Paranjothi, M. S. Khan, S. Zeadally, A. Pawar, and D. Hicks, "GSTR: Secure multi-hop message dissemination in connected vehicles using social trust model," *Internet of Things*, vol. 7, Sep. 2019, Art. no. 100071, https://doi.org/10.1016/j.iot.2019.100071.

[13] R. Riebl, M. Monz, S. Varga, L. Maglaras, H. Janicke, A. H. Al-Bayatti, and C. Facchi, "Improved Security Performance for VANET Simulations," *IFAC-PapersOnLine*, vol. 49, no. 30, pp. 233–238, Nov. 2016, https://doi.org/10.1016/j.ifacol.2016.11.173.

[14] S. Zhang, M. Lagutkina, K. O. Akpinar, and M. Akpinar, "Improving performance and data transmission security in VANETs," *Computer*

Communications, vol. 180, pp. 126–133, Dec. 2021, https://doi.org/10.1016/j.comcom.2021.09.005.

[15] A. Harbouche, D. Djabour, and A. Saiah, "Z-MSP: Zonal-Max Stable Protocol for Wireless Sensor Networks," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 18036–18041, Dec. 2024, https://doi.org/10.48084/etasr.8691.

[16] R. Hussain, F. Hussain, and S. Zeadally, "Integration of WSN and 5G Security: A review of design and implementation issues," *Future Generation Computer Systems*, vol. 101, pp. 843–864, Dec. 2019, https://doi.org/10.1016/j.future.2019.07.006.

[17] J. M. A. Jaleel, M. A. Khan, T. Mazhar, J. Khan, S. K. uz Zaman, U. F. Khattak, and S. Batool, "An energy-efficient hybrid LEACH protocol that enhances the lifetime of wireless sensor networks," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19364–19369, Feb. 2025, https://doi.org/10.48084/etasr.8458.

[18] M. R. Maganti and K. R. Rao, "Optimising the EPMIPv6 protocol for the analysis of advanced sensor networks," *Ingénierie des Systèmes d'Information*, vol. 29, no. 2, pp. 543–549, Apr. 2024, https://doi.org/10.18280/isi.290215.