Journal of Computer Networks, 2024, Vol. 12, No. 1, 7-14
Available online at http://pubs.sciepub.com/jcn/12/1/2
Published by Science and Education Publishing
DOI:10.12691/jcn-12-1-2

Trust Attributes in Multi-Path Congestion Avoidance Techniques to Curb Wormhole Attacks in Wireless Sensor Networks

Fortine Mwihaki Mata[1,*], Geoffrey Muchiri Muketha[1], Gabriel Ndung'u Kamau[2]

[1]Department of Computer Science, Murang'a University of Technology, Murang'a, Kenya
[2]Department of Information Technology, Murang'a University of Technology, Murang'a, Kenya
*Corresponding author: matafortine36@gmail.com

Received November 07, 2024; Revised December 09, 2024; Accepted December 16, 2024

Abstract Wireless sensor networks (WSNs) have become widespread in recent years due to their uses in healthcare, infrastructure monitoring, environmental sensing, tactical surveillance, and defense. However, their inherent vulnerabilities pose significant security threats and performance challenges. WSNs are highly exposed to wormhole attacks and congestion which affects the reliability and efficiency of a network. Current routing protocols often lack comprehensive trust mechanisms to address these challenges effectively. This study aims to evaluate trust-based multi-path routing protocols to counter wormhole attacks and minimize congestion, enhancing security and performance in Wireless Sensor Networks (WSNs). It focuses on six key trust attributes to identify the most impactful factors. A survey of 29 network security experts of various experience levels examined six key trust attributes: encryption, authentication, route disjointedness, observation similarity, packet delivery, and end-to-end latency. Statistical techniques including descriptive statistics, correlation analysis, and principal component analysis were used to assess each attribute's impact. The similarity of observation and route disjointedness were identified as the most crucial factors, with mean scores of 55.52 and 53.31. While authentication was valued, opinions varied, suggesting it should be part of a broader security framework. No differences were found in trust attribute evaluations based on qualifications or experience, indicating consensus among experts. The study shows that trust-based multi-path routing can curb wormhole attacks and detect congestion in WSNs.

Keywords: *Wireless sensor networks, trust attributes, wormhole attacks, congestion avoidance, WSNs*

Cite This Article: Fortine Mwihaki Mata, Geoffrey Muchiri Muketha, and Gabriel Ndung'u Kamau, "Trust Attributes in Multi-Path Congestion Avoidance Techniques to Curb Wormhole Attacks in Wireless Sensor Networks." *Journal of Computer Networks*, vol. 12, no. 1 (2024): 7-14. doi: 10.12691/jcn-12-1-2.

1. Introduction

Wireless Sensor Networks (WSNs) have emerged as pivotal components of contemporary technology due to their extensive applications across diverse domains, including environmental monitoring, healthcare, industrial automation, and tactical surveillance. The inherent flexibility, cost-effectiveness, and scalability of WSNs facilitate efficient data collection in remote, hazardous, or dynamic environments [1]. Notwithstanding these advantages, WSNs encounter considerable challenges in security and performance, which impede their effective utilization in mission-critical applications [2]. Among these challenges, wormhole attacks and network congestion are particularly detrimental, as they can significantly undermine network reliability and efficiency.

Wormhole attacks are recognized as one of the most critical threats to WSN security. In such an attack, malicious nodes establish a direct tunnel that circumvents regular network paths, creating a deceptive scenario in which distant nodes appear to be in closer proximity, thereby manipulating the network's topology [3]. This fabricated topology not only results in routing errors and packet losses but also facilitates subsequent attacks, such as eavesdropping or selective forwarding, wherein critical data may be intercepted or altered [4]. The ramifications of such attacks are particularly severe in WSNs due to their decentralized and ad-hoc nature, rendering them highly susceptible to such disruptions [5]. Moreover, wormhole attacks are challenging to detect using conventional security measures, as they exploit the legitimate functionalities of routing protocols [6].

Concurrently, network congestion remains a significant performance issue within WSNs. Congestion often arises from limited bandwidth, high traffic loads, or inefficient routing, resulting in packet delays, increased energy consumption, and potential packet loss [7]. This congestion can be exacerbated by malicious attacks, such as wormhole attacks, which redirect traffic through specific paths, thereby creating network bottlenecks [8]. WSNs are typically deployed in environments characterized by stringent energy and resource constraints, and congestion can substantially diminish network lifetime and compromise data integrity [9]. Therefore, it is imperative to develop solutions that concurrently address security and performance to maintain the quality of service (QoS) in WSNs [10].

Over the years, researchers have proposed various strategies to alleviate the dual challenges of wormhole attacks and congestion in WSNs. A promising approach is trust-based multi-path routing. This method calculates trust scores for each node based on performance metrics, including packet delivery rates, latency, encryption, and authentication [11,12]. Nodes with higher trust scores are preferentially selected for routing, enhancing network reliability and mitigating the likelihood of malicious nodes disrupting traffic [12]. Trust-based routing presents a flexible solution that safeguards against wormhole attacks but also assists in balancing traffic loads to avert congestion. Furthermore, it integrates seamlessly with existing routing protocols, rendering it a viable option for practical deployment [13,14].

2. Related Works

2.1. Wireless Sensor Networks

WSNs have become integral to many applications, allowing them to be used ubiquitously. Environmental monitoring, healthcare, and even domestic tasks have seen the employment of WSNs [32]. The efficiency with which these applications can carry out their tasks largely depends on WSNs. This helps in sending out data from sensor nodes in a secure manner. However, there are a few built-in vulnerabilities that pose serious challenges in ensuring the network's reliability and security.

2.2. Wormhole Attacks in Wireless Sensor Networks

In a wormhole attack, a set of nodes is configured in pairs within the network to eavesdrop on the information flow. One pair is set up in a location close to the data source (for example, a user). The other pair is configured to be near the data destination (for example, the Internet). A wormhole link, in effect a tunnel, is created between the two network pairs [30,31]. Information originating from the user is sent first to the eavesdropping pair, which then passes it through the wormhole to the network pair just outside the destination. This use of a network pair as a transmission path enables the attackers to fake the appearance of the data source while letting them eavesdrop and access sensitive information. Indeed, any attack that can compromise the integrity (or duplicate appearance) of the data is a dangerous one, and it raises questions about what kind of countermeasures can effectively prevent such an attack.

A wormhole attack occurs when an attacker sets up a location within the network to monitor information flow and access sensitive data from users by creating a tunnel or wormhole link between the source and destination [30,31]. The nodes are configured in pairs, allowing information to be transmitted and received between them in the direction indicated by the antenna. This method can effectively identify the wormhole through observable fluctuations in the network related to the antenna [37].

2.3. Security Approaches for Wormhole Attacks in WSNs

The Geographic and Temporal Leashes utilize GPS for loose node synchronization making it possible to identify certain kinds of wormholes. However, not all sensor networks can use GPS [33].

The LITEWORP approach is a lightweight scheme that is loosely based on the lemma that if a packet gets to its destination, then it doesn't go through a wormhole. It has unique features that allow it to do its task with very little overhead. They also help us understand just what a wormhole attack is and how it might be implemented [34].

Secure Localization and Wormhole-Resistant hybrid techniques are used to detect wormhole attacks. These methods have been used to give an overarching view of wormhole attack detection in multi-path routing environments [35,36].

The Radio Fingerprinting approach is used to obtain data from devices that use fingerprinting, converting those signals into digital forms to identify possible adversaries [36]. The Directional Antenna method identifies wormhole attacks by using pairs of nodes that communicate in a very specific direction, thus isolating fluctuations within the network [37].

2.4. Trust Computation Models in Multi-path Routing Schemes

Central to trust-based routing is the computation of trust scores for each node, derived from multiple performance indicators including packet delivery rate, data consistency, encryption, authentication, and end-to-end latency [14]. Nodes with higher trust scores are preferentially selected for routing, thereby enhancing the security and performance of the network. In recent years, various trust computation models have been proposed, including weighted summation, machine learning, fuzzy logic, block-chain, game theory-based, and evolutionary optimization models [12] [38-47].

The weighted summation model is widely utilized due to its simplicity. This model aggregates diverse trust attributes to create a composite trust score [22]. However, the rigidity of this approach often limits its adaptability, particularly in dynamic environments where node behavior evolves rapidly, such as during a wormhole attack [23]. More advanced techniques, such as machine learning-based trust computation, have demonstrated promise in addressing this limitation by dynamically adjusting trust scores based on patterns in node behavior. Although these methods are more computationally intensive, they offer enhanced detection accuracy in identifying compromised nodes [24].

Integrating trust-based multi-path routing with anomaly detection further enhances the security of WSNs. By distributing traffic across multiple trusted paths, the network reduces reliance on a single path, thereby diminishing the risk of wormhole attacks and alleviating congestion [17]. This approach is particularly effective when combined with hybrid detection mechanisms, which employ both trust metrics and cryptographic techniques to ensure data integrity and network reliability [18]. Nevertheless, the effectiveness of these techniques in real-world environments requires thorough validation [19].

2.5. Gaps, Contradictions and Inconsistencies

While significant progress has been made in the development of trust-based routing protocols, several gaps and inconsistencies persist. The absence of context-aware trust metrics constrains the effectiveness of current protocols in the dynamically evolving environments of WSNs [25]. Most protocols depend on generic trust attributes, which may not accurately reflect real-time alterations within the network or account for transient anomalies, such as wormhole attacks [26].

Existing studies predominantly rely on simulation-based evaluations, which often do not capture the complexities inherent in real-world WSN deployments. These simulations typically presuppose static network topologies and predictable traffic patterns, which may indicate actual conditions in mobile or ad-hoc WSNs [11,13,27]. Furthermore, there is a notable scarcity of empirical studies that validate the long-term performance of trust-based routing protocols under varying environmental conditions, such as harsh weather, physical tampering, or network congestion [12].

Although hybrid models that integrate cryptography and trust-based routing offer enhanced security, their substantial computational requirements often render them unsuitable for deployment in energy-constrained WSNs. These models require further optimization to achieve security, performance, and resource efficiency [18,20].

Addressing these gaps necessitates several future research directions. Developing context-aware trust metrics that can adapt to real-time changes in network behavior is essential for enhancing the accuracy of trust-based routing protocols [25,26]. Such metrics must be sensitive to dynamic factors, including node mobility, fluctuating traffic loads, and environmental interference. Furthermore, the integration of machine learning algorithms into trust computation models has the potential to improve adaptability, enabling the network to learn from historical behavior and predict potential security threats [24,28,29].

3. Methodology

3.1. Research Design

This study used a descriptive survey methodology to collect expert opinions on trust-based attributes essential for mitigating wormhole attacks and congestion in WSNs. The study involved carrying out an expert opinion to establish whether cyber security experts can adopt the trust attributes identified from the Systematic Literature Review for practice in the industry. The target population selected for this research were network security experts in cyber security within Kenya.

The snowballing sampling method was employed to get a sample size of 29 experts to validate trust attributes. The expert opinion survey questionnaire was pretested by involving 5 network security experts. The pretest was carried out to help the researcher improve the questionnaire's reliability. These experts participated in a survey that assessed their evaluations of six critical trust attributes: encryption, authentication, route disjointedness, similarity of observation, packet delivery, and end-to-end latency as identified from the literature.

Data analysis was conducted utilizing descriptive statistics, correlation analysis, and Kruskal-Wallis tests to assess differences in trust attribute ratings. Cronbach's alpha test was administered to evaluate the internal consistency of the survey items, and Principal Component Analysis (PCA) was employed to identify potential underlying factors that account for the variance in trust-based evaluations.

3.2. Research Questions

This study was guided by the research question, what trust-based attributes can be used to design a multipath routing technique in WSNs? It was further broken down into four specific research questions to ease data collection and analysis. The specific research questions are as follows:

RQ1. Which trust attributes are currently leveraged by existing protocols to evaluate and select candidate paths for multi-path routing?

RQ2. What models are adopted for trust computation in multi-path routing schemes?

RQ3. How effective are current techniques for detecting wormhole attacks within WSNs?

RQ4. To what extent are existing methods successful in avoiding network congestion in multi-path routing scenarios?

4. Results

4.1. Analysis of Real-World Scenarios

In agriculture, wireless sensor networks monitor soil moisture, temperature, and humidity. The authentication attribute ensures nodes are assigned trust scores based on their history of transmitting accurate data. Data from critical sensors is routed through multiple paths, cross-checking for security sensors using similarity of observation. Consistency checks among data received via different paths help detect malicious nodes by use of encryption mechanisms. Route disjointedness attribute prevents single data dependency for sensor data. The end-to-end latency ensures data real-time updates for irrigation systems. Packet delivery checks the reliability of farming decisions.

WSNs deployed for battlefield surveillance collect sensitive data such as troop movements or environmental conditions. Trust-based routing ensures that only authenticated nodes participate in data transmission. Abnormal delays introduced by wormholes are detected using trust metrics tied to route latency. Route disjointedness ensures safe communication in hostile areas as packet delivery delivers data quickly for mission success. The similarity of observation ensures that observations are correlated with surveillance systems. Encryption attribute safeguards classified communication.

Wearable devices and health sensors transmit critical patient data to healthcare providers. A wormhole attack could delay or alter life-saving information. Malicious nodes often consume more energy while rerouting data. Monitoring node energy patterns helps identify suspicious activity. Critical health data is routed through redundant trusted paths for accuracy verification. The route disjointedness trust attribute prevents redundancy for patients' essential data. Authentication and encryption trust attributes help to protect the network from rogue and secure sensitive health information respectively. Packet delivery guarantees vital data delivery to its destination.

4.2. Empirical Results

Respondents were asked to state their highest level of education. Findings show that the respondents had obtained a bachelor's degree possessed over five years of industry experience and had completed network security studies at the bachelor's level, with a similar proportion having undertaken three to four professional courses in the discipline (36.4%). Most respondents rated their knowledge of network security between 6 and 10 on a 10-point scale, reflecting moderate to high levels of expertise. The respondents' network security qualifications and expertise are presented in Table 1, highlighting their study levels and professional courses in the field.

Table 1. Network Security Background

Level of Education	Frequency	Percentage
Diploma	4	13.8
Undergraduate	15	51.8
Masters	5	17.2
PhD	5	17.2
Total	29	100

An analysis of trust attributes provided insights into the significance that experts attribute to various characteristics for securing WSNs. A sample size of 29 security experts was used. The route disjointedness trust attribute emerged as the highest-rated security, with a mean score of 55.52 showing its critical role in identity verification and preventing unauthorized access. This finding suggests that experts consider route disjointedness essential for ensuring that only authorized entities can interact with the network, thereby mitigating the risk of wormhole attacks.

The end-to-end latency trust attribute exhibited the lowest variability, with a mean score of 44.40, indicating a strong consensus among experts regarding its vital role in maintaining network performance. This outcome underscores the importance of ensuring timely data transmission, as delays in a WSN could render the network susceptible to disruptions or security vulnerabilities. The emphasis on end-to-end latency highlights the necessity for efficient routing mechanisms within mobile node environments.

Regarding reliability, the encryption trust attribute attained a mean score of 45.66 reflecting divergent opinions among experts concerning the extent to which encryption alone can ensure network reliability. While encryption is essential for safeguarding data in transit, experts may perceive it as merely one of several complementary measures required to secure the network against wormhole attacks as shown in Table 2.

Table 2. Descriptive Statistics for Trust Attributes

	Trust Attributes	Min	Max	Mean	Std Dev
Existing	Encryption	1	5	45.66	30.90
	Packet Delivery Ratio	1	5	48.38	25.81
	End to End latency	1	5	44.40	23.78
New	Authentication	1	5	50.62	28.69
	Route Disjointedness	1	5	55.52	31.62
	Similarity of Observation	1	5	53.31	30.90

Findings indicate that trust attributes related to security, particularly authentication, are highly regarded in mitigating wormhole attacks. The strong consensus regarding the significance of end-to-end latency for network performance underscores that timely data transmission is essential for effectively operating WSNs, particularly in scenarios involving mobile nodes.

The moderate rating assigned to encryption implies that, while it is recognized as important, experts may perceive it as merely one component of a more comprehensive security strategy addressing wormhole attacks. A reliability analysis used Cronbach's alpha to assess the internal consistency of the six trust-based items under evaluation. The resulting Cronbach's alpha value of 0.717 indicates satisfactory internal consistency.

Furthermore, the new trust attributes were correlated with the encryption trust attribute and were analyzed using a two-tailed Spearman's rho correlation because it measures the strength and direction of a relationship between two variables. The results of this analysis are presented in Table 3.

Table 3. Correlation Analysis

	Encryption trust
Authentication	0.541, p= 0.038
Route disjointedness	0.675, p=0.024
Similarity of observation	0.129, p=0.027

A significant positive correlation was observed between encryption trust and authentication trust (correlation = 0.541, p = 0.038), suggesting that experts who value encryption also recognize the significance of authentication in enhancing network security. This implies that encryption and authentication are perceived as complementary attributes that contribute to the overall security of network systems.

The route disjointedness trust attribute (security) was positively correlated with encryption trust (correlation = 0.675, p = 0.024), the connection of these attributes in maintaining network resilience. Experts who highly rate route disjointedness are likely to emphasize encryption, indicating that these attributes collaboratively enhance secure routing.

The similarity of observation exhibited a moderate positive correlation with encryption trust (correlation = 0.129, p = 0.027). This indicates that experts who value encryption, tend to consider the similarity of observation as important for security as shown in Table 4.

Table 4. Ranks by Years in Industry

Attribute	Mean Rank
Encryption	34.46
Authentication	34.31
Route Disjointedness	34.43
Similarity of Observation	33.87
Packet Delivery	34.41
End-to-End Latency	33.87

The ranks for each trust attribute are shown in Table 4. It was observed that encryption had the highest mean value of 34.46, while route disjointedness was ranked second with a mean of 34.43. This suggests that these trust attributes highly favor security-related attributes, and Authentication, packet delivery, and end-to-end; latency highly favor performance-related attributes. Experts were grouped based on their knowledge scores to explore further the relationship between trust attributes and network security knowledge as shown in Table 5.

Table 5. Ranks by Network Security Knowledge Score

Attribute	Mean Rank
Encryption	30.97
Authentication	31.27
Route Disjointedness	31.12
Similarity of Observation	34.68
Packet Delivery	31.00
End-to-End Latency	31.82

Similarity of observation was ranked highest with a mean value of 34.68. This suggests that this trust attribute is important in security-related issues. End-to-end latency also had a mean of 31.82. This indicates that the performance of the network also highly contributes to the trust of a network.

The Kruskal-Wallis test statistics for network security knowledge scores are shown in **Table 6**. Similar to the analysis by years in industry, no statistically significant differences were found between the groups for any trust attribute, as all p-values are greater than 0.05.

Table 6. Kruskal-Wallis Test Statistics by Network Security Knowledge Score

Attribute	Chi-Square	df	Asymp. Sig.
Encryption	3.730	2	0.247
Authentication	2.940	2	0.230
Route Disjointedness	2.424	2	0.298
Similarity of Observation	0.870	2	0.647
Packet Delivery	2.105	2	0.349
End-to-End Latency	1.597	2	0.450

The results of the Kruskal-Wallis test indicate no statistically significant differences in the ratings of trust attributes by experts based on their years of industry experience or network security knowledge scores. This finding suggests that evaluations of trust attributes, including encryption trust, authentication trust, and packet delivery trust, were consistent among experts, irrespective of their levels of experience or knowledge.

For instance, the mean rank for the encryption trust attribute was 29 for experts was 34.46, however, this difference was not statistically significant ($\chi^2 = 1.667$, p = 0.197). Likewise, no significant differences were observed in the mean ranks of trust attributes based on network security knowledge scores. Experts rated encryption trust higher (mean rank = 30.97), but this difference also lacked statistical significance ($\chi^2 = 3.730$, p = 0.247).

These findings imply that perceptions of trust attributes were uniform across experts, regardless of their experience or knowledge levels. This consistency underscores the universal significance of these attributes for the security of WSNs indicating that trust-based strategies can be effectively applied across varying levels of expertise.

Before conducting factor analysis, the Kaiser-Meyer-Olkin (KMO) measure and Bartlett's Test of Sphericity were employed to assess the appropriateness of the data for such analysis. The KMO value was recorded at 0.743 which is acceptable. Furthermore, Bartlett’s Test of Sphericity produced a significant result ($\chi^2 = 29.837$, p = 0.013), demonstrating that the correlation matrix is not an identity matrix, thus confirming that factor analysis is warranted as shown in Table 7.

Table 7. KMO and Bartlett’s Test

Test	Result
Kaiser-Meyer-Olkin (KMO) Measure	0.743
Bartlett’s Test of Sphericity	
Approx. Chi-Square	29.837
df	15
Sig.	0.013

Communalities represent the proportion of each variable’s variance that the extracted factors can explain. As illustrated in Table 8, all trust attributes exhibited relatively high communalities following extraction, with values ranging from 0.678 for the end-to-end latency trust attribute to 0.953 for the encryption trust attribute. This indicates that the extracted factors can explain a large proportion of the variance in each trust attribute.

Table 8. Communalities of Trust Attributes

Trust Attribute	Initial	Extraction
Encryption	1.000	0.953
Authentication	1.000	0.816
Route Disjointedness	1.000	0.747
Similarity of Observation	1.000	0.678
Packet Delivery	1.000	0.828
End-to-End Latency	1.000	0.686

The Principal Component Analysis (PCA) identified two components with eigenvalues exceeding 1. Collectively, these components accounted for 79.09% of the total variance. Specifically, the first component elucidated 40.84% of the variance, whereas the second component contributed an additional 38.25% as shown in Table 9.

Table 9. Total Variance Explained

Component	Initial Eigenvalues	Percent (%) of Variance	Cumulative Percent (%)
1	2.451	40.843	40.843
2	2.295	38.249	79.092

The component matrix illustrates the loadings of each variable onto the extracted components before rotation. The variables of encryption trust, authentication trust, and packet delivery trust exhibited substantial loadings on the first component. In contrast, the route disjointedness trust and similarity of observation trust demonstrated strong loadings on the second component. This suggests that the first component encompasses security-related attributes, while the second pertains to performance-related attributes as shown in Table 10.

Table 10. Component Matrix

Trust Attribute	Component 1	Component 2
Encryption	0.597	0.771
Authentication	0.897	0.107
Route Disjointedness	-0.010	0.881
Similarity of Observation	-0.498	0.662
Packet Delivery	0.903	0.116
End-to-End Latency	0.476	-0.678

After conducting varimax rotation to optimize the loadings of variables onto one of the two components, a more discernible pattern emerged. Encryption trust, authentication trust, and packet delivery trust exhibited high loadings on Component 1. Route disjointedness trust, similarity of observation trust, and end-to-end latency trust demonstrated high loadings on Component 2 as shown in Table 12.

The trust attributes in Component 1 are more aligned with reliability and performance, while Component 2 is more tied to security aspects. These components reflect two distinct priorities in the assessment of trust attributes with one focusing on performance and reliability, the other on security and timing.

4.3. Comparison with Existing Frameworks

Different theoretical frameworks that utilize trust attributes in multipath routing to curb wormhole attacks in wireless sensor networks (WSNs) vary in methodology, trust attributes, and overall effectiveness. Table 11 compares existing frameworks based on key parameters.

Fuzzy Logic and Machine Learning frameworks excel in adaptive and uncertain environments but are resource-heavy. Blockchain-based models offer high security but may not scale well in low-power, resource-constrained WSNs. Game Theory and Probabilistic Models are lightweight alternatives but may lack sophistication against advanced threats. A trust-based multipath congestion avoidance technique approach combining multiple attributes achieves better trade-offs between security, efficiency, and adaptability.

5. Discussion

5.1. Implications of Real-World Scenarios

In agriculture, real-world scenarios often need intuitive decision-making as farmers face complex environmental conditions such as pest outbreaks, and crop growth stages. Technology helps optimize irrigation, monitor soil conditions, and predict weather changes.

Autonomous systems like drones and satellites collect large amounts of data that can be analysed for threats or enemy movements. While technology can provide situational awareness, humans guide strategy in high-pressure situations where there may be too much noise in the data.

Machine learning and AI tools can analyse patient data, to identify patterns that suggest potential diagnoses or predict outcomes. Healthcare professionals often rely on intuition gained through years of experience.

Table 11. Comparison with existing Theoretical Frameworks

Framework Type	Attributes used	Strengths	Weaknesses
Trust Aware Routing Framework (TMRF)	Node Reliability, Packet forwarding Ratio, Energy consumption	Highly effective in identifying malicious nodes	Computationally intensive
Fuzzy Trust Based Multipath Routing (FTMR)	Latency, Energy consumption, throughput	Handles uncertainty effectively	High computational overhead
Block Chain Integrated Trust Model (BCITM)	Consensus scores	High security and fault tolerance	Resource intensive
Game Theory-Based Trust (GTBT)	Payoff functions	Promotes cooperation	Complex modelling
Machine Learning Based Model (MLBM)	Machine learning algorithms, ANN, SVM	Adaptive and accurate	High computations and data demands
Trust Based Multi- Path Congestion Avoidance Technique (TB-MPCAT)	Authentication, encryption, route disjointedness, packet delivery ratio, similarity of observation, latency	Highly effective in identifying malicious nodes, high security, and performance	High computational overhead

Table 12. Rotated Component Matrix

Trust Attribute	Component 1	Component 2
Encryption	0.824	0.522
Authentication	0.880	-0.205
Route Disjointedness	0.291	0.832
Similarity of Observation	-0.242	0.793
Packet Delivery	0.888	-0.198
End-to-End Latency	0.216	-0.800

5.2. Empirical Study Implications

The study shows that Similarity of observation and Route disjointedness were identified as the most critical attributes for mitigating wormhole attacks and ensuring optimal performance in WSNs. These findings are consistent with prevailing scholarly consensus, wherein authentication is frequently emphasized as a primary defense mechanism against unauthorized access to sensor networks.

The attribute exhibiting the lowest variability, with a mean score of 3.27 (SD = 0.467), was end-to-end latency, indicating a strong consensus regarding its significance for network performance. In WSNs, the prompt transmission of data is important, as delays may result in vulnerabilities such as data loss and network congestion, especially within mobile node environments. Kruskal-Wallis test yielded no significant differences in latency ratings based on participant qualifications or industry experience, thereby implying that the necessity for low latency is universally acknowledged among experts.

The findings also underscore the diverse perspectives concerning the adequacy of encryption in guaranteeing network reliability. Although encryption exhibited a moderate mean score of 3.36 (SD = 1.43), its relatively high loading in the PCA indicates that it is regarded as a crucial, albeit not singular, security measure.

Conversely, the analysis revealed no statistically significant differences in the assessment of trust attributes based on years of industry experience, implying that perceptions of network security remain relatively consistent across varying levels of professional experience.

The PCA test identified two components that account for 79.09% of the variance in trust attribute evaluations. The first component predominantly included security-related attributes such as encryption, authentication, and packet delivery, whereas the second component was linked to performance-related attributes, including route disjointedness and end-to-end latency. This bifurcation underscores the dual emphasis in WSN security on both the prevention of malicious attacks and the maintenance of optimal network performance.

5.3. Implications of Comparison with Existing Frameworks

Fuzzy Logic and Machine Learning frameworks excel in adaptive and uncertain environments but are resource-heavy. Blockchain-based models offer high security but may not scale well in low-power, resource-constrained WSNs. Game Theory is a lightweight alternative but may lack sophistication against advanced threats. A trust-based multipath congestion avoidance technique hybrid approach combining multiple techniques often achieves better trade-offs between security, efficiency, and adaptability.

6. Conclusion

The findings of this study provide significant insights into the trust-based attributes deemed critical for mitigating wormhole attacks and preventing congestion in WSNs. The emphasis on authentication and end-to-end latency highlights the necessity for a multi-layered security approach that effectively balances protection and performance. While encryption remains an essential tool, it must be supplemented by additional strategies, such as route disjointedness, to enhance network resilience against sophisticated threats, including wormhole attacks.

In this review, real-world scenarios appreciate the use of the new set of trust attributes in enhancing the performance, reliability, and security of agriculture, health, and surveillance systems.

Future research should concentrate on the development of context-aware trust metrics and the empirical testing of these attributes in real-world scenarios to validate their effectiveness. Moreover, it is imperative to investigate hybrid trust computation models applying machine learning to detect patterns and predict congestion in real-time reroute packets proactively. and prevent spoofing attacks during authentication processes.

References

[1] Adu-Manu KS, Abdulai JD, Engmann F, Akazue M, Appati JK, Baiden GE, et al. WSN Architectures for Environmental Monitoring Applications. J Sens 2022; 2022.

[2] Garg R, Gulati T. Issues and Challenges of Wormhole Attack Detection for Secure Localization in WSNs. 2023 International Conference on Advancement in Computation and Computer Technologies 2023: 628–33.

[3] Ghugar U, Pradhan J. Survey of wormhole attack in wireless sensor networks. Computer Science and Information Technologies 2021; 2: 33–42.

[4] Zhang K. A wormhole attack detection method for tactical wireless sensor networks. PeerJ Comput Sci 2023; 9.

[5] Dhama P, K P. Genetic algorithm-based Wormhole attack detection in WSN. International Journal of Science and Research Archive 2023; 9: 795–802.

[6] Al-Ahmadi S, Aliady W, Alrashedy A. An Efficient Wormhole Attack Detection Method in Wireless Sensor Networks. Proceedings - 26th International Conference on Circuits, Systems, Communications and Computers, CSCC 2022 2022: 240–9.

[7] Mahajan M, Kaur S. Congestion Control Protocols in Wireless Sensor Networks: a comprehensive Survey. Proceedings of International Conference on Intelligent Engineering and Management, ICIEM 2020 2020: 160–4.

[8] Kazmi HSZ, Javaid N, Awais M, Tahir M, Shim S o., Zikria Y Bin. Congestion avoidance and fault detection in WSNs using data science techniques. Transactions on Emerging Telecommunications Technologies 2022; 33: e3756.

[9] Anil DN, Azmat A, Patil YM. Security issues in wireless sensor networks. I-Manager's Journal on Wireless Communication Networks 2023; 11: 32.

[10] Pathak A, Al-Anbagi I, Hamilton HJ. An Adaptive QoS and Trust-Based Lightweight Secure Routing Algorithm for WSNs. IEEE Internet Things J 2022; 9: 23826–40.

[11] Visumathi J, Gurusubramani S, Mouleeswaran SK, Sammeta N. Enhancing Reliability in Multi-Path Mobile Wireless Sensor Network. Proceedings of the 3rd International Conference on Artificial Intelligence and Smart Energy, ICAIS 2023 2023: 345–9.

[12] Liu J, Xu F. Research on trust-based secure routing in wireless sensor networks. Spie Digital Library 2023; 12610: 942–8.

[13] Ambekar RK, Kolekar UD. T-TOHIP: Trust-based topology-hiding multipath routing in mobile ad hoc network. Evol Intell 2019; 15: 1067–81.

[14] Khalid NA, Bai Q, Al-Anbuky A. Adaptive Trust-Based Routing Protocol for Large Scale WSNs. IEEE Access 2019; 7: 143539–49.

[15] Kaur S, Monal B. Securing the Future of Wireless Sensor Networks: Challenges, Threats, and Innovative Solutions. Int J Res Appl Sci Eng Technology 2023; 11: 719–28.

[16] Arulselvan G, Rajaram A. Hybrid trust-based secure routing protocol for detection of routing attacks in environment

monitoring over MANETs. Journal of Intelligent & Fuzzy Systems 2023; 45: 6575–90.

[17] Sun Y, Chen Y. Detection of Wormhole Attacks in Wireless Sensor Networks Based on Anomaly Detection Algorithms. 2022 2nd International Conference on Consumer Electronics and Computer Engineering, ICCECE 2022 2022: 777–82.

[18] Tripathy A, Pradhan SK, Tripathy AR, Nayak AK. A New Hybrid Cryptography Technique in Wireless Sensor Network. International Journal of Innovative Technology and Exploring Engineering (IJITEE) 2019; 8: 121–31.

[19] Ardiansyah F, Budi AS, Primananda R. Hybrid Cryptography for Data Security in Wireless Sensor Network. International Conference on Sustainable Information Engineering and Technology 2021: 221–5.

[20] Mohindru V, Singh Y, Bhatt R. Hybrid Cryptography Algorithm for Securing Wireless Sensor Networks from Node Clone Attack. Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering) 2020; 13: 251–9.

[21] Suma S, Harsoor B. An optimized routing scheme for congestion avoidance using mobile nodes in Wireless Sensor Network. Measurement: Sensors 2022; 24: 100457.

[22] Kang S, Kim T, Chung W. Hybrid RSS/AOA Localization using Approximated Weighted Least Square in Wireless Sensor Networks. Italian National Conference on Sensors 2020; 20.

[23] Verma S, Arora S, Rawat A. Wormhole Detection using Zonal Security Nodes in Wireless Sensor Networks. 2023 International Conference on Computational Intelligence, Communication Technology and Networking, CICTN 2023 2023: 353–8.

[24] Kim T, Vecchietti LF, Choi K, Lee S, Har D. Machine Learning for Advanced Wireless Sensor Networks: A Review. IEEE Sens J 2021; 21: 12379–97.

[25] Chaudhari S. A survey on multipath routing techniques in wireless sensor networks. Int J Netw Virtual Organisations 2021; 24: 267–328.

[26] Adu-Manu KS, Engmann F, Sarfo-Kantanka G, Baiden GE, Dulemordzi BA. WSN Protocols and Security Challenges for Environmental Monitoring Applications: A Survey. J Sens 2022; 2022.

[27] Shukla M, Joshi BK. A trust-based approach to mitigate wormhole attacks in mobile ad-hoc networks. Proceedings - 2021 IEEE 10th International Conference on Communication Systems and Network Technologies 2021: 776–82.

[28] Pundir M, Sandhu JK. A Systematic Review of Quality of Service in Wireless Sensor Networks using Machine Learning: Recent Trend and Future Vision. Journal of Network and Computer Applications 2021; 188.

[29] Parakh A, Subramaniam M. Network routing protocols for multi-p**hot**on quantum cryptography. Optical Engineering + Applications 2021: 10.

[30] Umashankar Ghugar1, and Jayaram Pradhan2, A Review on Wormhole Attacks in Wireless Sensor Networks, International Journal of Information Communication Technology and Digital Convergence (2019).

[31] M.G. Zapata, Secure Ad hoc On-Demand Distance Vector Routing, ACM SIGMOBILE Mobile Computing and Communications Review. Jun, (2002), vol, 6(3), pp.106-107.

[32] C. Zhu, M. J. Lee, T. Saadaw, RTT-Based Optimal Waiting Time For Best Route Selection In Ad Hoc Routing Protocols, IEEE Military Communication Conference, Vol.2 Oct, (2003), pp1054- 1059.

[33] K.U.R Khan, A.V. Reddy, R.U. Zaman, K.A Reddy, T.S Harsha, An Efficient DSDV Routing Protocol for Wireless Mobile Ad Hoc Networks and its Performance Comparison, Second UKSIM European Symposium on Computer Modeling and Simulation, India, (2008), pp. 506-511.

[34] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A Survey Of Routing Attacks In Mobile Ad Hoc Networks, IEEE Wireless Communication, vol. 14(5), October, (2007).

[35] A. Verma and N. Bhardwaj, A Review on Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) Routing Protocol. International Journal of Future Generation Communication and Networking, vol. 9(4), (2016), pp. 161-170.

[36] U. Ghugar, J. Pradhan, Intrusion Detection System in Wireless Sensor Networks for Wormhole Attack Using Trust-Based System, Handbook of Research on Information Security in Biomedical Signal Processing, IGI Global, (2018).

[37] E. Kaffashi, A. Mousavi, H. Rahvard, A new attack on a link-state database in open shortest path first routing protocol. Journal of Electrical and Electronic Engineering, (2015); vol. 3(2-1), pp. 39-45.

[38] S. Roy, M. Conti, and S. Setia, "Securing Wireless Sensor Networks Against Wormhole Attacks," IEEE Security & Privacy, 2010.

[39] K. Sun et al., "Secure Routing for Wireless Mesh Networks: A Trust Management Perspective," IEEE Transactions on Networking, 2011.

[40] A. Josang and R. Ismail, "The Beta Reputation System," International Workshop on Deception, Fraud, and Trust in Agent Societies, 2002.

[41] H. Yang et al., "Fuzzy Trust Evaluation Mechanism for Secure Routing in Wireless Sensor Networks," Springer Wireless Networks Journal, 2014.

[42] Z. Zheng et al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," IEEE International Congress on Big Data, 2017.

[43] A. Sharma et al., "Blockchain-Based Trust Management for Secure Routing in IoT Networks," IEEE Access, 2020.

[44] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol," ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2002.

[45] Z. Han and H. V. Poor, "Game Theory in Wireless and Communication Networks," Cambridge University Press, 2012.

[46] K. Zia et al., "A Trust Management Framework Using Machine Learning for IoT Networks," Springer Sensors Journal, 2018.

[47] A. Al-Makhadmeh and A. Tolba, "Trust Management in Wireless Sensor Networks Using Neural Networks," International Journal of Advanced Computer Science and Applications, 2020.