Trust Calculation Models for Wireless Sensor Networks: A Survey

Abdul Rasheed, M R Rajesh, R Prema, K Thangavel

Department of Electronics and Communication, Hindusthan College of Arts and Science, Coimbatore, India

DOI: 10.29322/IJSRP.16.05.2026.p17326
https://dx.doi.org/10.29322/IJSRP.16.05.2026.p17326

Paper Received Date: 24th April 2026
Paper Acceptance Date: 25th May 2026
Paper Publication Date: 31st May 2026

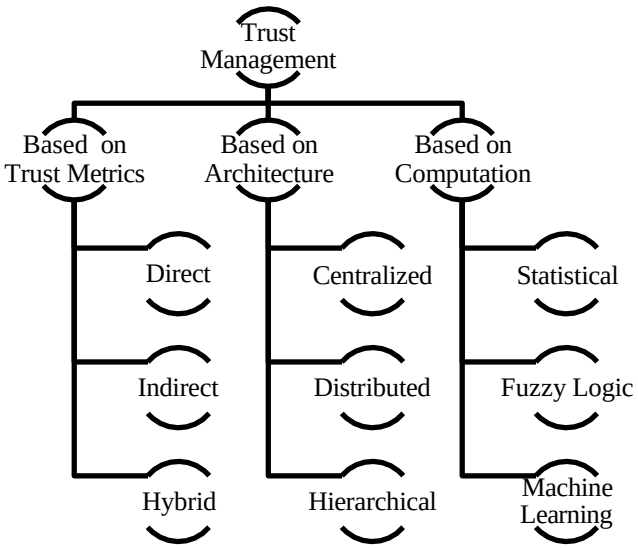
Abstract- Wireless sensor networks (WSNs) consists of resource constrained, distributed sensor nodes that are highly vulnerable to various internal and external attacks. The conventional cryptographic methods for security are inadequate due to heavy computational requirements. Trust based security emerged as an effective approach for mitigating internal attacks. Different trust computation models such as statistical, fuzzy logic, machine learning approaches are evolved over time. The method used for modelling, along with the network architecture, metrics such as communication, data used for trust calculation, significantly influences computational overhead, communication efficiency, attack detection accuracy and isolation of malicious nodes. This paper presents a survey of trust calculation models and analyze their impact on security and Quality of Service (QoS) in WSNs.

Index Terms- Wireless Sensor Networks, Trust Management, Trust Calculation Models, Intrusion Detection, Energy Efficiency, Quality of Service

I. Introduction

Wireless sensor networks (WSNs) are infrastructure-less networks having spatially distributed sensor nodes for real time monitoring of industrial, healthcare, military surveillance and environmental data [1], [2]. The sensor nodes collaboratively sense, process, and transmit data. The network management, energy conservation, and secure communication are critical design considerations in WSNs due to their resource constrains such as limited processing capacity, low memory, low bandwidth, and limited battery power [1], [3].

Factors such as open transmission medium, lack of central control, unattended operation, deployment in hostile and remote environments make the WSNs prone to internal and external security threats [4], [5], [6]. External attacks are done by nodes that are not part of the network and disturb or destroy the normal functioning of the network. While internal attacks are performed by compromised nodes that are part of the network and can cause selective forwarding, sinkhole, or Sybil attacks. Important security requirements of a WSNs are data confidentiality, data integrity, availability, data freshness, self-organization, secure localization, time synchronization and authentication. There are the most common type of security threat in WSN which adversely affect the network availability. DoS is any event that diminishes or eliminates a network's capacity to perform its expected function. Hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors can cause a DoS [8]. Asymmetric and symmetric cryptography are the effective for many threats in wireless networks but implementing them and key management are not practical due to the intensive computational requirements and the resource constraints of WSN [1], [11] and are not suitable for defending internal attacks. Trust based approaches have emerged as an alternative to these conventional cryptographic approaches and effectively defend internal attacks [12], [13].



three broad types of security vulnerabilities in WSNs [7].

i. Attacks on secrecy and authentication
ii. Attacks on network availability
iii. Stealthy attack against service integrity

Node replication attack, eavesdropping, traffic analysis, camouflage and passive monitoring are the major attacks on secrecy and

authentication. The Denial of Service (DoS) attack is

Fig. 1. Classification of Trust Management Schemes

The computational and communication overhead introduced for security and trust can cause negative impact on the energy efficiency and Quality of Service (QoS) [12], [14]. A trade-off is required between security, energy efficiency and QoS in resource constrained wireless networks.

The review aims to provide an analysis of trust calculation methods adapted for secure routing in WSNs with a focus on their energy efficiency, attack resistance and QoS performance. The paper classifies the existing trust models based on their trust computation technique, architecture, energy efficiency and QoS considerations. It also identifies research gaps, challenges and

Table. 1. Comparison of protocols using statistical models for trust computation

Protocol	Architecture	Information Source	Evaluation Method	Defended Attacks	Fault Detection	Energy Efficiency	Computational overhead	QoS Performance Improvement	Simulation Tools
ESRT [13]	Distributed	Hybrid	Beta probability density function	Packet forwarding misbehavior	Yes	Yes	Light	Throughput, delay, Normalized Routing Load (NRL) and Network lifetime	NS-2
TERP [16]	Distributed	Hybrid	Weighted probabilistic trust estimation with Bernoulli model	Packet forwarding misbehavior	Yes	Yes	Light	Throughput, delay, Normalized Routing Load (NRL) and Network lifetime	NS-2
LEACH-T [17]	Hierarchical	Direct	Game Theory + beta probability density function	Selective Forwarding Attack	Yes	Yes	Moderate	Network lifetime, Data forwarding, Energy consumption, Packet drop	MATLAB
TRPM[18]	Hierarchical	Hybrid	Beta Distribution with trust weighting	Blackhole, Grayhole, Selfish, On-off, Collusion	Yes	Yes	Moderate	Throughput, delay, routing overhead, and lifetime	NS-2
ECLRM [19]	Distributed	Hybrid	Weight based Probabilistic	Stealth Jamming Attack, False Route Breakage	Yes	Yes	Light	Throughput, delay, Normalized Routing Load (NRL) and Route lifetime	NS-2
TMSRS [20]	Distributed	Hybrid	Gaussian Distribution + Grey Decision Making	On–Off, Bad Mouthing, Selective Forwarding	Yes	Yes	Moderate	Throughput, Energy Efficiency, Load Balance, Latency	MATLAB, NS-2
AODV with RREQ [21]	Hierarchical	Hybrid	Correlation Coefficient + KS Test	LDoS	Yes	Yes	Moderate	Detection precision, packet loss ratio, reliability	MATLAB
TBSIOP [22]	Distributed	Direct	Beta Distribution	Black-hole attacks, Grey-hole attacks	Yes	Yes	Moderate	PDR, End-to-End Delay, Energy Consumption, and Network Lifetime	MATLAB
TSS[23]	Hierarchical	Hybrid	Binomial Distribution	On–Off, Bad-Mouthing, Collusion	Yes	Yes	Moderate	Throughput, Energy Efficiency, PDR, Security	MATLAB, NS-2
BSTrust-AODV [24]	Hierarchical	Hybrid	Markov Chain + Bayesian Model	Selfish node, packet dropping, Malicious Node	Yes	Yes	Moderate	Packet Delivery Ratio, End-to-End Delay, Routing Overhead	NS-2
LPTM[25]	Distributed	Hybrid	Beta Probability and Bayesian	DoS attacks	Yes	Yes	Moderate	Load balancing percentage	MATALAB
CESMA-MTRS [26]	Distributed	Hybrid	Beta Distribution + Slime Mould Algorithm	Black hole and Gray hole Attacks	Yes	Yes	Moderate	Delay, packet loss rate, and energy consumption	MATLAB

future directions. The paper is organized as follows: section 2 discusses the trust management schemes in WSN; section 3 discusses the trust calculation methods; section 4 analyses the trade-off between trust, energy efficiency and QoS performance based on trust calculation approach; section 5 concludes with future directions.

II. TRUST MANAGEMENT IN WSN

Trust based security in WSNs has gained appreciation in identification of malicious node and mitigating internal attacks, compared to computationally intensive cryptography method [13]. Trust is the level of confidence that a node has in the behaviour of other nodes in the network. The value of trust typically ranging between 0 and 1. The trust value calculated directly from the observation of past interactions, indirectly from recommendations of other nodes, or weighted combination of both. Direct trust has more influence than indirect trust. Based on the position where calculation, storage and updating of trust value, trust management can be Centralized, Distributed, and Hierarchical approaches [14]. The taxonomy of trust management scheme is presented in fig. 1.

In centralized trust management, the collection of feedback, evaluation, maintaining and updating of trust value for all nodes held at a central node. This approach is easy to implement but leads to communication overhead and poor scalability in large-scale WSNs [15]. And compromised or failure of the central node makes the trust information unreliable.

Trust evaluation and decisions are made locally at all sensor nodes in distributed trust management. Due to distributed nature, this approach is better suited for large scale WSNs but the computational and communication requirement of each sensor node increases, more over special care has to be taken to avoid bad-mouthing. The hierarchical method takes the advantages of both centralized and distributed trust management systems.

III. TRUST COMPUTATION MODELS

This section discusses diverse trust computation models and their effect on security, energy efficiency and performance in terms of QoS parameters. The researchers employ different methodologies for trust evaluation including statistical functions, fuzzy logics, and machine learning approaches, and are often validated through simulations using NS-2, MATLAB, or COOJA.

A. Statistical Models

The routing protocols ESRT [13] and TERP [16] are enhanced versions of AODV protocol, with a multifaceted routing strategy incorporating trust, energy, and hop counts for making routing decisions. These protocols use weighted probabilistic trust estimation with beta distribution or Bernoulli distribution. While TRPM [17], a trust aware routing protocol, incorporates multi-attribute trust parameters such as communication, data, energy, and recommendation trust. The communication and data trust are estimated using beta distribution. The protocol employs an improved sliding time window mechanism that accounts for attack frequency to enhance the detection of malicious node behaviors. It has an efficient routing detection and maintenance process.

A multi-dimensional trust evaluation system based on direct trust, penalized trust, recommendation trust, cumulative trust, total trust, and optimized/best path selection is proposed in [18]. The proposed Link-based Penalized Trust Management (LPTM) scheme uses weighted probabilistic trust estimation using beta distribution. It provides a preventive measure against DoS attacks. The penalizing temporarily reduces the trust value of consistently used nodes and thereby distribute the traffic across alternate trustworthy paths and avoid the over use of highly trusted nodes.

Ahmed et al. [19] proposed an Enhanced Cross-Layer Route Maintenance (ECLRM) scheme to defend the impact of route instability due to the flooding of route discoveries caused by stealth jamming attack, which in turn improves the overall performance. This cross-layered scheme uses a Weight based Probabilistic Trust Evaluation (WPTE) and takes informed decision on route breakages to mitigate jamming attacks, and thereby improving route stability, throughput and delay performance.

A game theory-based dynamic behavior monitoring with beta probability density function is proposed in [20] for trust evaluation. The probability expectation value of beta distribution function is calculated in terms of cooperative and malicious behaviors. This dynamic behavior monitoring scheme achieved a longer network lifetime than the one based on full time behavior monitoring mechanism, without reducing successful data forwarding rate. It can also effectively defend certain routing layer attacks such as Selective forwarding, black hole, sybil, wormhole and false routing information by dynamically updating trust values and allowing only trusted nodes to become cluster heads or forwarding nodes. A comprehensive trust management system based on Gaussian distribution (GDTMS) for industrial wireless sensor network (IWSN) is proposed in [21]. Fang et al. [22] proposed a Trust Value-based Secure Routing Protocol (TV-SRP) that employs a binomial distribution-based trust model for evaluating node trustworthiness and incorporates a third-party recommendation mechanism to improve the objectivity of trust assessment. The TV-SRP able to detect and defend On-Off attack quickly and effectively, and demonstrated a trade-off between security, transmission performance and energy efficiency.

A Multi-objective Trust Routing Scheme (CESMA-MTRS) is proposed in [23], which employs beta distribution for trust calculation and Cloned Elite Slime Mould Algorithm for speed up the convergence of routing search. This heuristic trust-based approach enhances routing optimization and reduces energy consumption. It shows significant improvements in network security and quality of service.

A Low-rate Denial of Service (LDoS) attack detection algorithm based on Hilbert–Huang Transform (HHT) is proposed in [24]. The approach employs time–frequency joint analysis using HHT on the non-stationary small signal produced by such attacks. Correlation coefficient and Kolmogorov–Smirnov (KS) test approaches are united to evaluate the trustworthy of IMF components and exclude the false IMF. A trust based secure

Table. 2. Comparison of protocols using ML models for trust computation

Protocol	Architecture	Information Source	Evaluation Method	Defended Attacks	Fault Detection	Energy Efficiency	Computational overhead	QoS Performance Improvement	Simulation Tools
ATRP [27]	Hierarchical	Hybrid	Q Learning + AHP	Packet dropping, flooding/energy drain, false recommendation	Yes	Yes	Moderate	Lifetime, Energy, Throughput, Packet Delivery Ratio, Delay, Packet Loss	MATLAB
EATSRA [28]	Distributed	Hybrid	Decision Tree	DoS, Sybil, packet dropping	Yes	Yes	Moderate	delay, PDR, detection accuracy	NS-2
ATE[29]	Hierarchical	Hybrid	AI – ANFIS	DoS	Yes	Yes	Moderate	Network lifetime, Packet Delivery Ratio, Delay, Confidential Data Forwarding	NS-2
TAGA [30]	Hierarchical	Hybrid	Adaptive Genetic Algorithm	Black hole, Hello flood, Selective forwarding, Sinkhole, On-off, Bad-mouth	Yes	Yes	Moderate	PDR, Energy efficiency, Network lifetime, Stability, Trust accuracy	MATLAB
OQR-SC [31]	Distributed	Hybrid	Chaotic Bird Swarm Optimization + Gini coefficient and neural network weighting	false trust, eavesdropping, data tampering	Yes	Yes	Moderate	Energy, Lifetime, Delay, Throughput, Node survival	NS2
GITM [32]	Distributed	Hybrid	GINI Index decision tree	Sybil, Sinkhole, Bad Mouthing	Yes	Yes	Moderate	PDR, Throughput, Delay, Energy, Lifetime, Trust Accuracy	COOJA

intelligent opportunistic routing protocol (TBSIOP) is proposed in [25]. The Trust calculation is done based on sincerity in forwarding data packets, acknowledgment and Energy Depletion. It has shown a comparatively better performance in terms of average risk level, packet delivery ratio, end-to-end delay, energy consumption, and network lifetime. Gong et al. proposed a high-reliability trust evaluation model for secure routing that employs a Markov chain prediction mechanism with states power level, traffic, response time, and network delay for evaluating the trustworthiness of routing nodes [26]. A fine-grained trust-based routing principle is developed based on Bayesian model to dynamically identify and isolate malicious nodes. This trust model effectively strengthens routing security, ensures rapid response to attacks, and enhances overall network reliability and availability.

B. Machine Learning Models

A Q-learning based Adaptive Trust-Based Routing Protocol (ATRP) proposed in [27] integrates direct, indirect, and witness trust with Analytic Hierarchy Process (AHP). It uses Q-learning to dynamically balance energy efficiency, reliability, and trustworthiness. ATRP effectively addresses the challenges in large scale, distributed sensor networks. The scheme demonstrates longer lifetime, less delay, less packet loss and low energy consumption. Later, an adaptive Neuro-Fuzzy Inference System (ANFIS)-based Trust-aware Routing framework (ATE) [28] is proposed to enhance the security and lifetime of Wireless Sensor Networks (WSNs). It combines ANFIS and Neural Network (NN)-based trust evaluation to identify malicious nodes, optimize energy utilization, and establish reliable routing paths for confidential data forwarding. The ATE protocol demonstrates improved network lifetime, secure transmission, and reduced computational complexity compared to existing schemes like TRAF and ETARP.

The protocols EASTRA [29] and TAGA [30] are energy aware trust based secure routing protocols, which leverages machine learning techniques to enhance security and energy efficiency. The EATSRA employs a Decision Tree algorithm combined with spatio-temporal constraints to determine optimal and secure routing paths. While TAGA integrates trust metrics and energy parameters within Adaptive Genetic Algorithm (AGA) framework to select optimal and secure routes dynamically. Comprehensive trust values are calculated based on direct trust considering the volatilization and adaptive penalty factors, and indirect trust with the filtering mechanisms. Both the approaches

show considerable improvements in QoS performance.

Table. 3. Comparison of protocols using fuzzy logic for trust computation

Protocol	Architecture	Information Source	Defended Attacks	Fault Detection	Energy Efficiency	Computational overhead	QoS Performance Improvement	Simulation Tools
MATM [33]	Distributed	Hybrid	Routing, Data/Address Modification, Compromised/ Selfish Nodes	Yes	Yes	Light	Delay, PDR, Detection Rate	NS-2
Fuzzy-IoT [34]	Hierarchical	Hybrid	On–Off, Con-behaviour, Bad Service Provider	Yes	Yes	Moderate	Trust accuracy, scalability, reliability	COOJA
FEBSRA [35]	Hierarchical	Hybrid	DoS, Flooding, Black Hole	Yes	Yes	Moderate	Energy, Delay, PDR, Throughput, Security, Lifetime	NS-2

An Optimal QoS-Aware Routing technique proposed in [31] employs Chaotic Bird Swarm Optimization (CBSO) for cluster formation and Improved Differential Search (IDS) to estimate node trust. An Optimal Decision-Making (ODM) algorithm is used to determines the best route. In the fog-enabled GINI Index-based Trust Mechanism (GITM) [32], the forwarding behavior of legitimate nodes and a fog- layered architecture used to offload complex trust computations from sensor nodes, thereby reducing their energy consumption. This approach effectively defended sybil attack.

C. Fuzzy Logic Models

A Fuzzy Logic-based Multi-Attribute Trust Model (MATM) to assess the node behaviour and thereby enhance the security and reliability of WSNs is proposed in [33]. The model evaluates the trust based on message success rate, elapsed time at the node, correctness, and fairness. Simulation study demonstrate MATM detect the malicious nodes effectively and achieves superior performance than Hierarchical Trust Management Protocol (HTMP).

The cluster-based fuzzy logic trust management framework (Fuzzy-IoT) [34] employs fuzzy logic to detect and mitigate malicious activities, including on–off attacks, contradictory behavior, and bad service provisioning. The model dynamically adapts with the network size variations. The hexadecimal-based messaging system of the model ensures safe inter-node communication. The Fuzzy-IoT effectively detect malicious nodes, achieves fast trust convergence, and improves overall network stability.

In the Fuzzy Trust-Based Energy-Aware Balanced Secure Routing Algorithm (FEBSRA) [35], a dynamic trust model that calculates trust by considering both energy levels and communication delay is proposed. A fuzzy logic is employed to make multi-criteria routing decisions based on trust scores, node energy levels, and hop counts. Simulation study shows that FEBSRA significantly improves energy consumption, delay, throughput, and security performance compared to existing methods.

IV. ANALYSIS AND DISCUSSION

Over the past decade a clear transition in trust calculation models for WSNs from the deterministic mathematical to probabilistic models and fuzzy logic models and, recently to more adaptive machine learning models is clearly visible. Early research focused on dynamic trust evaluation models using hybrid trust to detect malicious nodes. Fuzzy logic models and machine learning models are proposed to assess trust level dynamically and adapt the routing decision in real time. These methods effectively detect complex attack behaviours.

The statistical models are the most widely used method for trust calculation in resource constrained sensor networks, due to its analytical simplicity and computational efficiency. Table 1 compare different protocols employing statistical methods for trust evaluation. The protocols such as ESRT, TERP, and ECLRM employed weighted probabilistic models such as beta distribution or Bernoulli to estimate the trust worthiness are efficient in network with distributed architectures, offering light computational overhead and good energy efficiency, which are very crucial in wireless sensor networks. Even though, these protocols defend only a limited type of attacks, they effectively detect packet forwarding misbehaviour, and show improvements in QoS metrics such as throughput, delay, and routing load. They are failed to defend attacks having dynamic nature. The protocols ESRT and TERP requires non-colluding nodes and promiscuous monitoring. Incorporating more advanced statistical model such as Markov chain with hierarchical architecture expands the spectrum of defended threats including collusion, selfishness, with a cost of moderate computational overhead. The penalizing trust mechanisms and heuristic approaches implemented in LPTM and CESMA-MTRS respectively, offers adaptive and pre-emptive trust management while they introduced considerable computational overhead. So, the light weight trust mechanisms based on simple probabilistic models defend against fewer attack types, while hybrid models offer high precision on detection with more computational overhead.

The fuzzy logic approaches in protocols Fuzzy-IoT, FEBSRA, and MATM effectively handles uncertainty in trust decision, and

Table. 4. Strengths and limitations of trust calculation models

Model	Strength	Limitations
Statistical	• Energy-efficient trust management • Lightweight • Scalable • Effective malicious node detection • Dynamic route selection and load balancing • Faster convergence	• Handle only a few attacks like blackhole, DoS, or On–Off attacks, • Lack of adaptability to hybrid or evolving multi-vector threats. • Promiscuous monitoring increases energy drain • Lack of Collusion Resistance • Assume fixed topology and ideal conditions • Many models lack location or time synchronization
Fuzzy Logic	• Handles uncertainty and imprecise behaviour • Adaptive Trust Score Computation • Improved detection accuracy of malicious nodes • Balanced energy usage	• Computational overhead • Requires careful parameter and rule-base tuning • Most models focus on limited attacks such as DoS, blackhole and packet drop • Lack of adaptability to hybrid or evolving multi-vector threats. • Assume fixed topology and ideal conditions • Increased latency in large networks
Machine Learning	• Intelligent and adaptive trust prediction • High malicious node detection accuracy • Adaptive learning mechanisms identify complex attack behaviours	• High computational and storage requirements • Complexity of implementation and parameter tuning • Scalability challenges in dense networks

demonstrate effective defense against diverse threats including blackhole and on–off. The fuzzy logic models require more computational ability than statistical models. Table 3 compare different protocols employing fuzzy logic for trust evaluation.

The machine learning approaches demonstrates a more adaptive and intelligent trust evaluation. The RL, GA and LSTM models are incorporated in ATRP, TAGA and FLSTMT-LAR respectively which dynamically calculate trust value. The multi criteria trust evaluation method in ATRP-AHP prioritizes multiple trust factors including reliability and energy coverage, takes adaptive routing decisions suitable to dynamic network topology. They are not suitable for large scale network due to its layered trust estimation process and high communication overhead. The schemes TAGA and OQR-SC improves energy efficiency and QoS using differential search and genetic algorithms, but they have higher computational requirements. The AI models such as ANFIS and federated learning employed in ATE and FLSTMT-LAR offers predictive and dynamic trust evaluation. Table 2 compare different protocols employing machine learning methods for trust evaluation.

V. CONCLUSION

Existing studies demonstrate that trust calculation models play a critical role in enhancing both security and Quality of Service (QoS) in Wireless Sensor Networks (WSNs). This paper examines various models and approaches employed for trust evaluation in WSNs. The surveyed models are compared based on their impact on security, energy efficiency, and QoS performance, and are further classified according to their underlying trust computation mechanisms.

Early approaches are generally lightweight and resource-efficient; however, they are limited in their ability to defend against a wide range of attacks. To address this limitation, some methods introduce penalty mechanisms by reducing the trustworthiness of frequently utilized nodes. This approach reduces the load on trust worthy nodes and mitigate DoS attacks. The newer approaches expand the spectrum of defended attacks including more complex, dynamic behavior. But they introduce additional computational and communication overhead, leading to reduced QoS performance in large-scale networks. Most of them assumes static topology and promiscuous monitoring. These computational approaches are validated through simulation studies and are not experimentally verified on a real WSN hardware.

Future work should focus on developing light weight, scalable trust evaluation models to detect and mitigate sophisticated attacks while maintaining energy efficiency and QoS performance. Furthermore, emphasis should be placed on supporting dynamic network topologies, integrating multi-attribute and cross-layer trust evaluation mechanisms, and validating the proposed models through real-world WSN testbeds.

REFERENCES

[1] M. S. Obaidat and S. Misra, Principles of Wireless Sensor Networks, 1st ed. Cambridge University Press, 2014. doi: 10.1017/CBO9781139030960.
[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” Comput. Netw., vol. 38, no. 4, pp. 393–422, Mar. 2002, doi: 10.1016/S1389-1286(01)00302-4.
[3] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “SPINS: Security Protocols for Sensor Networks,” Wirel. Netw., vol. 8, no. 5, pp. 521–534, Sep. 2002, doi: 10.1023/A:1016598314198.
[4] R. Roman, J. Zhou, and J. Lopez, “On the Security of Wireless Sensor Networks,” in Computational Science and Its Applications – ICCSA 2005, O. Gervasi, M. L. Gavrilova, V. Kumar, A. Laganà, H. P. Lee, Y. Mun, D. Taniar,

and C. J. K. Tan, Eds., Berlin, Heidelberg: Springer, 2005, pp. 681–690. doi: 10.1007/11424857_75.
[5] A. K. Gautam and R. Kumar, "A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks," SN Appl. Sci., vol. 3, no. 1, p. 50, Jan. 2021, doi: 10.1007/s42452-020-04089-9.
[6] S. Hudda and K. Haribabu, "A review on WSN based resource constrained smart IoT systems," Discov. Internet Things, vol. 5, no. 1, p. 56, May 2025, doi: 10.1007/s43926-025-00152-2.
[7] J. Sen, "A Survey on Wireless Sensor Network Security," Nov. 06, 2010, arXiv: arXiv:1011.1529. doi: 10.48550/arXiv.1011.1529.
[8] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, no. 10, pp. 54–62, Oct. 2002, doi: 10.1109/MC.2002.1039518.
[9] "Wireless Sensor Security Issues on Data Link Layer: A Survey," Comput. Mater. Contin., vol. 75, no. 2, pp. 4065–4084, Mar. 2023, doi: 10.32604/cmc.2023.036444.
[10] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Commun. Surv. Tutor., vol. 8, no. 2, pp. 2–23, 2006, doi: 10.1109/COMST.2006.315852.
[11] Y.-H. Lee, V. Phadke, A. Deshmukh, and J. W. Lee, "Key Management in Wireless Sensor Networks," in Security in Ad-hoc and Sensor Networks, C. Castelluccia, H. Hartenstein, C. Paar, and D. Westhoff, Eds., Berlin, Heidelberg: Springer, 2005, pp. 190–204. doi: 10.1007/978-3-540-30496-8_16.
[12] H. Hu, Y. Han, M. Yao, and X. Song, "Trust Based Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks," IEEE Access, vol. 10, pp. 10585–10596, 2022, doi: 10.1109/ACCESS.2021.3075959.
[13] A. Ahmed, K. A. Bakar, M. I. Channa, A. W. Khan, and K. Haseeb, "Energy-aware and secure routing with trust for disaster response wireless sensor network," Peer--Peer Netw. Appl., vol. 10, no. 1, pp. 216–237, Jan. 2017, doi: 10.1007/s12083-015-0421-4.
[14] A. K. Gautam and R. Kumar, "A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks," SN Appl. Sci., vol. 3, no. 1, p. 50, Jan. 2021, doi: 10.1007/s42452-020-04089-9.
[15] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," IEEE Trans. Netw. Serv. Manag., vol. 9, no. 2, pp. 169–183, Jun. 2012, doi: 10.1109/TCOMM.2012.031912.110179.
[16] A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network," IEEE Sens. J., vol. 15, no. 12, pp. 6962–6972, Dec. 2015, doi: 10.1109/JSEN.2015.2468576.
[17] B. Sun and D. Li, "A Comprehensive Trust-Aware Routing Protocol With Multi-Attributes for WSNs," IEEE Access, vol. 6, pp. 4725–4741, 2018, doi: 10.1109/ACCESS.2017.2786944.
[18] A. Ahmed, K. N. Qureshi, M. Anwar, F. Masud, J. Imtiaz, and G. Jeon, "Link-based penalized trust management scheme for preemptive measures to secure the edge-based internet of things networks," Wirel. Netw., vol. 30, no. 5, pp. 4237–4259, Jul. 2024, doi: 10.1007/s11276-022-02948-4.
[19] A. Ahmed, U. Ashraf, F. Tunio, K. Abu Bakar, and M. S. AL-Zahrani, "Stealth Jamming Attack in WSNs: Effects and Countermeasure," IEEE Sens. J., vol. 18, no. 17, pp. 7106–7113, Sep. 2018, doi: 10.1109/JSEN.2018.2852358.
[20] L. Yang, Y. Lu, S. Liu, T. Guo, and Z. Liang, "A Dynamic Behavior Monitoring Game-Based Trust Evaluation Scheme for Clustering in Wireless Sensor Networks," IEEE Access, vol. 6, pp. 71404–71412, 2018, doi: 10.1109/ACCESS.2018.2879360.
[21] W. Fang, W. Zhang, W. Chen, Y. Liu, and C. Tang, "TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing," Wirel. Netw., vol. 26, no. 5, pp. 3169–3182, Jul. 2020, doi: 10.1007/s11276-019-02129-w.
[22] W. Fang, N. Cui, W. Chen, W. Zhang, and Y. Chen, "A Trust-Based Security System for Data Collection in Smart City," IEEE Trans. Ind. Inform., vol. 17, no. 6, pp. 4131–4140, Jun. 2021, doi: 10.1109/TII.2020.3006137.
[23] C. Li, Y. Liu, Y. Zhang, M. Xu, J. Xiao, and J. Zhou, "A Novel Nature-Inspired Routing Scheme for Improving Routing Quality of Service in Power Grid Monitoring Systems," IEEE Syst. J., vol. 17, no. 2, pp. 2616–2627, Jun. 2023, doi: 10.1109/JSYST.2022.3192856.
[24] H. Chen, C. Meng, Z. Shan, Z. Fu, and B. K. Bhargava, "A Novel Low-Rate Denial of Service Attack Detection Approach in ZigBee Wireless Sensor Network by Combining Hilbert-Huang Transformation and Trust Evaluation," IEEE Access, vol. 7, pp. 32853–32866, 2019, doi: 10.1109/ACCESS.2019.2903816.
[25] D. K. Bangotra, Y. Singh, A. Selwal, N. Kumar, and P. K. Singh, "A Trust Based Secure Intelligent Opportunistic Routing Protocol for Wireless Sensor Networks," Wirel. Pers. Commun., vol. 127, no. 2, pp. 1045–1066, Nov. 2022, doi: 10.1007/s11277-021-08564-3.
[26] L. Gong, C. Wang, H. Yang, Z. Li, and Z. Zhao, "Fine-grained Trust-based Routing Algorithm for Wireless Sensor Networks," Mob. Netw. Appl., vol. 26, no. 6, pp. 2515–2524, Dec. 2021, doi: 10.1007/s11036-018-1106-z.
[27] N. A. Khalid, Q. Bai, and A. Al-Anbuky, "Adaptive Trust-Based Routing Protocol for Large Scale WSNs," IEEE Access, vol. 7, pp. 143539–143549, 2019, doi: 10.1109/ACCESS.2019.2944648.
[28] P. N. Renjith, "Towards Secure Data Forwarding with ANFIS and Trust Evaluation in Wireless Sensor Networks," Wirel. Pers. Commun., vol. 114, no. 1, pp. 765–781, Sep. 2020, doi: 10.1007/s11277-020-07392-1.
[29] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H. Khannah Nehemiah, and A. Kannan, "An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks," Wirel. Pers. Commun., vol. 105, no. 4, pp. 1475–1490, Apr. 2019, doi: 10.1007/s11277-019-06155-x.
[30] Y. Han, H. Hu, and Y. Guo, "Energy-Aware and Trust-Based Secure Routing Protocol for Wireless Sensor Networks Using Adaptive Genetic Algorithm," IEEE Access, vol. 10, pp. 11538–11550, 2022, doi: 10.1109/ACCESS.2022.3144015.
[31] D. Karunkuzhali, B. Meenakshi, and K. Lingam, "OQR-SC: An Optimal QoS Aware Routing Technique for Smart Cities Using IoT Enabled Wireless Sensor Networks," Wirel. Pers. Commun., vol. 125, no. 4, pp. 3575–3602, Aug. 2022, doi: 10.1007/s11277-022-09725-8.
[32] M. Hassan et al., "GITM: A GINI Index-Based Trust Mechanism to Mitigate and Isolate Sybil Attack in RPL-Enabled Smart Grid Advanced Metering Infrastructures," IEEE Access, vol. 11, pp. 62697–62720, 2023, doi: 10.1109/ACCESS.2023.3286536.
[33] V. Ram Prabha and P. Latha, "Fuzzy Trust Protocol for Malicious Node Detection in Wireless Sensor Networks," Wirel. Pers. Commun., vol. 94, no. 4, pp. 2549–2559, Jun. 2017, doi: 10.1007/s11277-016-3666-1.
[34] M. D. Alshehri and F. K. Hussain, "A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT)," Computing, vol. 101, no. 7, pp. 791–818, Jul. 2019, doi: 10.1007/s00607-018-0685-7.
[35] R. Anitha, B. R. T. Bapu, P. G. Kuppusamy, N. Partheeban, and A. N. Sasikumar, "FEBSRA: Fuzzy Trust Based Energy Aware Balanced Secure Routing Algorithm for Secured Communications in WSNs," Wirel. Pers. Commun., vol. 125, no. 1, pp. 63–86, Jul. 2022, doi: 10.1007/s11277-022-09541-0.

AUTHORS

First Author – Abdul Rasheed, MSc, Hindusthan College of Arts and Science, Coimbatore, India, rasheed.mailady@gmail.com
Second Author – M R Rajesh, MSc, Hindusthan College of Arts and Science, Coimbatore, India, rajeshmrsn@gmail.com
Third Author – R Prema, PhD, Hindusthan College of Arts and Science, Coimbatore, India, prema.r@hicas.ac.in
Fourth Author – K Thangavel, PhD, Hindusthan College of Arts and Science, Coimbatore, India, thangavel@hicas.ac.in

Correspondence Author – Abdul Rasheed, rasheed.mailady@gmail.com