Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 10s (2025)

HAMTR: A Hybrid Authentication and Multi-Dimensional Trust-Based Routing Model for Secure Wireless Sensor Networks

Jatin Gupta[1], Vishal Goyal[2]

[1,2]Department of Computer Science, Punjabi University, Patiala, 147001, India

**Corresponding Author Email: jatin.gupta.1988@ieee.org*

Article History:

Received: 12-01-2025

Revised: 15-03-2025

Accepted: 12-05-2025

Abstract: Wireless Sensor Networks (WSNs) face increasing challenges related to security, trust, and energy efficiency, especially in dynamic and hostile environments. This paper proposes a Hybrid Authentication and Multi-dimensional Trust-based Routing (HAMTR) model, designed to enhance secure communication in WSNs. The HAMTR framework combines MAC-layer authentication with behavioral and data trust evaluations to detect and isolate malicious nodes. It incorporates dynamic trust updates, secure path selection, and lightweight communication protocols to support efficient routing with minimal energy consumption. The proposed model aims to provide a scalable and adaptive solution for mitigating internal and external security threats while ensuring reliable data transmission. This work outlines the design and operational logic of HAMTR, laying the groundwork for future implementation and performance validation in real-world scenarios.

Keywords: Wireless Sensor Networks (WSNs), Trust Management, Hybrid Authentication, Secure Routing, Energy Efficiency, MAC Protocol, IoT Security, Intrusion Detection.

1. Introduction

Networks are deployed to achieve communication, data transfer and collecting sensitive information crucial to many applications. Networks can be implemented in various flavours like Mobile ad-hoc networks, peer to peer networks, wireless sensor networks etc. depending upon their mode of deployment, nature of nodes and network links, presence of central authority etc. Irrespective of their nature of implementation, all networks are vulnerable to attacks from internal entities and external unauthorised users that can ultimately subvert the system. Security is the major concern which not only involves activating the counteract measures to identify the malicious users present inside and outside the network but also protecting the critical data on a timely basis. Of all the networks, wireless sensor networks (WSNs) have been employed in critical applications like military testing [1], environmental monitoring [2] and targeting applications [3]. These networks consist of nodes randomly deployed in a particular area, which collaboratively sense and aggregate the data from their neighbouring nodes through dynamic self-organizing and then relay it to the base station. Base Station is also called sink which collects the information and then processed it according to the specific application domain [4]. The network can become prone to various security threats [5] in case of unattended and harsh deployment of nodes. There is always an aggravating risk of the security of the wireless sensor nodes being compromised. Once security breach occurs even in a single node in the network, the integrity and availability of whole network is at stake. The adversaries who compromise the node security may acquire the encryption keys and pose as the regular nodes in the network eventually rupturing the entire network. Asymmetric cryptographic techniques [6] are widely used to ensure security in the networks like ad-hoc networks, peer to peer networks etc. But in case of wireless networks, these techniques are

futile because it can protect the network only from external attacks [7]. The wireless networks suffer from the serious consequences of the internal authenticated nodes which are constrained by the energy consumption, computing capability of the embedded processor etc and deny the service to the service requester on the grounds of limited energy resource. On the other hand, Peer-to-peer networks have their own share of challenges. The open and anonymous nature of these networks devoid of any central authority to regulate the data opens the door to malevolent users to circulate the inauthentic and malicious files ultimately succumbing the whole network to halt. Clearly, there is a dire need to adopt some security mechanisms to address these problems.

Trust and reputation management system is a concept to attain a minimum level of security between the two interacting entities in a system. Trust is basically a confidence that one node has in the other node that it will provide the level of service it has expected. Trust is a probability that the node will perform the required action while reputation is a quantity to measure accountability and credibility of a node in a network based on its past behaviour of transactions. The basic idea behind this is to quantify the rapport and competence, a node has in the network subjectively in order to achieve the secure interactions in the network. Several state-of-the-art trust and reputation models have been developed so far. Undoubtedly, these models have contributed tremendously in ensuring the security of the network. But still they suffer several shortcomings that need to be addressed like subjective evaluation of trust values, failure to distinguish between the reputed nodes in the system and novice nodes while calculating trust values etc. This paper attempts to discuss several trust and reputation models, their striking features as well as the shortcomings in detail. Apart from these, their applications in networks like WSNs, P2P networks are also discussed.

2. Related Work

Model	Application	Advantages	Drawbacks
Eigen Trust [8]	Peer-to-peer network	Calculates global trust values by considering the entire system's history with each single peer Prevents downloading of inauthentic files	A priori notions of trust Inactive peers Malicious Collectives
Bayesian –based trust management scheme (BTMS) [9]	Wireless Sensor Networks	Calculates direct and indirect trust values Recommendations from highly reputed nodes are given more weights Prevents from Bad mouthing attack and Ballot stuffing attack	Increased energy consumption
Enhanced Bio-Inspired trust and reputation model(EBTRM) [10]	Wireless Sensor Networks	Combines Bio-inspired trust and reputation model(BTRM) and Peer Trust System to find trustworthy sensors	It is not accurate when the percentage of malicious sensors is not high Consumes considerable amount of energy under highly secured environment

Beta-based trust and reputation evaluation system(BTRES) [13]	Wireless Sensor Networks	Performs better than BRSN Defends against Slander attack and Selective Forwarding	Increased energy consumption
Work-based reputation evaluation secure routing algorithm(Work-based GEAR) [17]	Wireless Sensor Networks	Sink recognition mechanism helps in capturing real time node data Effective in tackling selective forwarding and data tempering	Increases energy consumption Fail to tackle other attacks like SYBIL attack
Trust based secure routing model [18]	Wireless multimedia sensor networks	Complex way of assigning trust values identifies malicious nodes. Direct and indirect trust values ensure security check of the nodes	Packet loss parameter to identify malicious nodes leads to the loss of data No real time capturing of node data
A Trust and Reputation management system for cloud and sensor networks integration [19]	Cloud Computing(CC) and Wireless Sensor Networks(WSNs) Integration	Novel system for CC and WSNs integration networks Helps Cloud service users(CSU) choose CSP(cloud service provider) and assist CSP in choosing SNP(sensor network provider)	Complex Increased cost
GoNe(Good Network) [20]	Wireless Sensor Network(WSNs)	Machine learning technique SOM(self-organizing maps) makes it faster and inexpensive Suited for hostile environments which present a huge amount of data Multiple attacks detection Periodic assessment of nodes Power consumption of nodes and packet's arrival delay reduced	Not suitable for real network scenarios Doesn't work with the communication technologies other than WSNs

3. Trust and Reputation Models

A trust and reputation management system comprises of five components:

(a) **Collecting information:** Information about the node is collected prior to the transaction. There are various sources of information [22]. It can be based on direct experience or can also be collected from the other peer nodes.

(b) **Scoring and ranking:** After accumulating all the information, score is assigned called reputation to the node using some algorithm. The basic idea is to provide a measurable quantity to establish the trustworthiness of the node and to decide whether to communicate or not.
(c) **Choosing entities:** After computing the reputation score, the node with the highest score is chosen for interaction.
(d) **Performing Transaction:** After ensuring the node's trustworthiness, the actual transaction occurs.
(e) **Giving Rewards or punishment:** If the transaction is successful and the receiving node is satisfied with the service, the node which provides the service achieves high reputation in the network. If the transaction was unsuccessful, its reputation score will drop considerably.

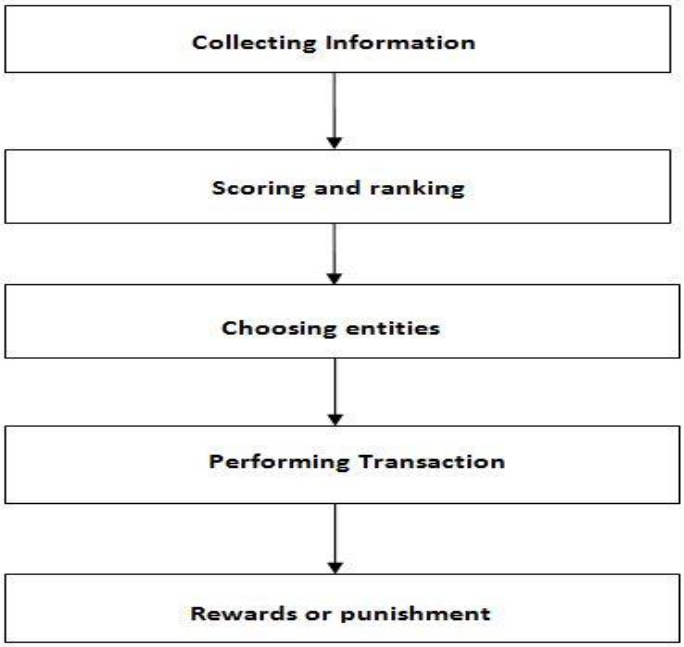

Figure 1: Basic components of a Trust and Reputation model

4. Research Gap

1. Insufficient protection against novel WSN-specific attacks
Traditional cryptographic techniques are not enough in environments where nodes can be physically compromised. Trust models often lack robustness against WSN-specific attacks such as on-the-fly key exposure, collusion, and node capture [1], [3], [19].
2. Most models still focus only on binary events
Many models evaluate node behavior only in terms of success/failure routing decisions, ignoring continuous sensing data, which is critical in WSN applications like environmental monitoring [4], [5], [13].
3. High energy consumption and communication overhead
Trust and reputation computation often leads to significant energy and bandwidth overhead, limiting their scalability in dense or mobile networks [10], [14], [18].
4. Limited resilience to collusion and insider attacks
Existing trust systems perform poorly when multiple malicious nodes coordinate. Many models

assume nodes are mostly honest, leading to inaccurate or delayed misbehavior detection [2], [6], [11].

5. Lack of modular or adaptable trust frameworks
Trust and reputation models are often tailored to specific WSN configurations, lacking modularity for reuse or adaptation to different topologies or threat conditions [7], [16], [20].
6. No standardized evaluation metrics or datasets comparative studies reveal inconsistent methods for evaluating trust models, making it hard to validate or benchmark new designs under common threat models and scenarios [3], [12], [17].
7. Delayed integration of trust in routing protocol decisions
Many models compute trust separately and do not embed trust in routing decisions dynamically, resulting in weaker real-time response to threats [6], [9], [15].

5. Methodology Trust-Based Routing

i. Authentication-Driven Network Access Control

The initial step of the suggested approach introduces a strong authentication procedure for blocking unauthorized or malicious nodes from joining the network. In contrast with most previous models that depend only on trust thresholds [2], [4], [6] or behavioral analysis post-node entry, the HAMTR model applies a three-factor authentication procedure based on a node's MAC address, a defined user password, and a pre-assigned unique key. The node must, therefore, pass all three validations for entry into the network. This guarantees only authenticated nodes are involved in network activities, providing a powerful first line of defense against external manipulation, e.g., Sybil and blackhole entries, often targeting weak or delayed trust establishment processes [3], [10].

The access control is proactive as well as deterministic, removing the threat of trust exploitation at an early stage. Further, incorporating the MAC address—a hardware-bound identifier—allows the model to add a layer of non-replicable identity, limiting impersonation risks. The authentication layer is synchronized with the trust module such that only the authenticated nodes advance to being assessed for trustworthiness based on their actions, comprising a two-stage defense model.

ii. Multi-Dimensional Trust Evaluation and Secure Routing

After being verified, each node continues to engage in continuous trust assessments over three fundamental axes: communication trust (for example, forwarding packets properly), data trust (for example, accuracy and consistency of the passed data), as well as energy trust (reporting one's own battery state truthfully). It monitors these indicators continuously through direct observation as well as indirect feedback from neighboring nodes. In contrast to previously proposed systems that used solely packet delivery or one-shot success probabilities [5], [11], HAMTR computes a weighted aggregate trust value through a normalized scoring scheme that adjusts itself according to current network behavior.

This trust rating is used for routing decisions. These nodes are deemed qualified for inclusion in routes when their rating is above a chosen threshold, whereas nodes consistently registering low ratings are isolated or relegated in the routing hierarchy. For additional reliability, HAMTR provides a mechanism for trust recovery, enabling temporarily deviating nodes (as a consequence of link failure, for example, or excessive load) gradually to reestablish their trust through appropriate action. This is different from past models that tend to permanently blacklist nodes for transient, low-weight, or spurious detections [1], [13].

6. Conclusion

Routing choices are thus not made only on the minimum energy, shortest path, but rather on a hybrid model based on trust, energy stability, and packet history. This considerably improves the model's resistance to internal misbehavior as well as its adaptability to the evolving dynamics of ad hoc, as well as IoT, environments, particularly where mobile nodes are integrated [14], [15].

The HAMTR model presented in this work is a novel, proposed framework aimed at strengthening the security of wireless sensor networks through hybrid authentication and multi-dimensional trust evaluation. By integrating MAC-layer control with trust-based routing and behavior analysis, the method is designed to proactively identify and isolate malicious nodes. It emphasizes adaptability, energy efficiency, and resilience against both external and internal threats. Although this is a conceptual framework at this stage, its layered architecture and comprehensive trust metrics indicate strong potential for real-time, secure, and efficient communication in IoT and wireless sensor environments. Future implementation and evaluation are expected to validate its practical effectiveness.

REFERENCES

[1] Callaway, E. H. Wireless Sensor Networks: Architectures and Protocols. Boca Raton, FL: Auerbach Publications, 2004

[2] Zhao, F. and L. J. Guibas. Wireless Sensor Networks: An Information Processing Approach. Amsterdam: Morgan Kaufmann, 2004

[3] Martincic, F. and L. Schwiebert. "Introduction to Wireless Sensor Networking." Handbook of Sensor Networks: Algorithms and Architectures. Hoboken, NJ, USA: John Wiley & Sons, 2005.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” *Computer Networks*, vol.38, no. 4, pp. 393–422, 2002.

[5] F. G. M´armol and G. M. P´erez, “Security threats scenarios in trust, reputation models for distributed systems,” *Computers & Security*, vol. 28, no. 7, pp. 545–556, 2009.

[6] O. Khalid, S. U. Khan, S. A. Madani et al., “Comparative study of trust and reputation systems for wireless sensor networks, *“Security and Communication Networks*, vol. 6, no. 6, pp. 669–688, 2013.

[7] Srinivasan, A., et al. "Reputation and Trust-based Systems for Ad Hoc and Sensor Networks." On Trust Establishment in Mobile Ad-Hoc Networks. Ed. A. Boukerche. Wiley & Sons, 2007.

[8] Kamvar, S. D., Schlosser, M. T., & Garcia-Molina, H. (2003, May). The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th international conference on World Wide Web* (pp. 640-651). ACM.

[9] Feng, R., Han, X., Liu, Q., & Yu, N. (2015). A credible Bayesian-based trust management scheme for wireless sensor networks. *International Journal of Distributed Sensor Networks*, *11*(11), 678926.

[10] Marzi, H., & Li, M. (2013). An enhanced bio-inspired trust and reputation model for wireless sensor network. *Procedia Computer Science*, *19*, 1159-1166.

[11] Mármol, F. G., & Pérez, G. M. (2011). Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommunication systems*, *46*(2), 163-180.

[12] Xiong, L., & Liu, L. (2004). Peer trust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE transactions on Knowledge and Data Engineering*, *16*(7), 843-857.

[13] Fang, W., Zhang, C., Shi, Z., Zhao, Q., & Shan, L. (2016). BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks. *Journal of Network and Computer Applications*, *59*, 88- 94.

[14] Konwar, S., Paul, A. B., Nandi, S., & Biswas, S. (2011, December). MCDM based trust model for secure routing in Wireless Mesh Networks. In *Information and Communication Technologies (WICT), 2011 World Congress on* (pp. 910-915). IEEE.

[15] Sun, Y. L., Yu, W., Han, Z., & Liu, K. R. (2006). Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE Journal on Selected Areas in Communications*, *24*(2), 305-317.

[16] Das, P. (2010). In search of best alternatives: a TOPSIS driven MCDM procedure for neural network modeling. *Neural Computing and Applications*, *19*(1), 91-102.

[17] Song, Y., Zhang, J. P., Li, L. J., & Wang, Q. (2012, May). Work-based Reputation Evaluation Secure Routing Algorithm in wireless sensor networks. In *Millimeter Waves (GSMM), 2012 5th Global Symposium on* (pp. 490-493). IEEE.

[18] Nagarathna, K., Kiran, Y. B., Mallapur, J. D., & Hiremath, S. (2012, July). Trust based secured routing in wireless multimedia sensor networks. In *Computational Intelligence, Communication Systems and Networks (CICSyN), 2012 Fourth International Conference on* (pp. 53-58). IEEE.

[19] Zhu, C., Nicanfar, H., Leung, V. C., Li, W., & Yang, L. T. (2014, June). A trust and reputation management system for cloud and sensor networks integration. In *Communications (ICC), 2014 IEEE International Conference on* (pp. 557-562). IEEE

[20] S. Sicari, A. Rizzardi, L. A.Grieco, and A.Coen-Porisini, "GoNe: Dealing with node behaviour," in *Proceedings of the 5th IEEE International Conference on Consumer Electronics - Berlin, ICCE-Berlin 2015*, pp. 358–362, Berlin, Germany, September 2015.

[21] Castelluccia, C., Mykletun, E., & Tsudik, G. (2005, July). Efficient aggregation of encrypted data in wireless sensor networks. In *Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on* (pp. 109-117). IEEE.

[22] Meena, U., & Jha, M. K. (2015, March). An efficiency model for authentication approaches in WBAN. In *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on* (pp. 476-481). IEEE.

[23] Z. Bankovic, D. Fraga, J. Manuel Moya et al., "Improving security in WMNs with reputation systems and self-organizing maps," *Journal of Network and Computer Applications*, vol. 34, no. 2, pp. 455–463, 2011.