

Active Trust: Secure and Trustable Routing in Wireless Sensor Network

Anbarasi R¹, Devika G², Janani R³, Aruloli R⁴

^{1,2,3}UG Student, Computer science and engineering & Bharathiyar Institute of Engineering for women, (Autonomous), Salem, Tamilnadu, India

⁴Assistant Professor, Computer science and engineering & Bharathiyar Institute of Engineering for women (Autonomous), Salem, TamilNadu, India

ABSTRACT

Wireless Sensor Networks (WSNs) are widely used in many applications such as environmental monitoring, healthcare systems, military surveillance, and smart cities. These networks consist of a large number of sensor nodes that collect and transmit data to a base station through wireless communication. However, due to their limited resources, open wireless medium, and distributed nature, WSNs are highly vulnerable to various security threats such as packet dropping, false data injection, and malicious node attacks. Ensuring secure and reliable routing is therefore a critical challenge in WSNs.

The **ActiveTrust** mechanism is proposed to provide secure and trustable routing in Wireless Sensor Networks. The main objective of ActiveTrust is to identify trustworthy nodes and avoid malicious nodes during data transmission. In this approach, each sensor node evaluates the behavior of its neighboring nodes by monitoring packet forwarding activities. Based on this observation, trust values are calculated for each node. Nodes with higher trust values are considered reliable and are selected for routing, while nodes with low trust values are treated as suspicious or malicious and excluded from the routing path.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of a large number of small sensor nodes that are deployed in a specific environment to monitor physical or environmental conditions such as temperature, humidity, pressure, and motion. These sensor nodes collect data from the

environment and transmit it to a base station or sink node for further processing. Due to their ability to operate in remote and unattended areas,

WSNs are widely used in applications such as environmental monitoring, healthcare systems, military surveillance, disaster management, and smart agriculture.

Despite their advantages, Wireless Sensor Networks face several challenges, especially in terms of security and reliability. Sensor nodes have limited power, memory, and computational capabilities, which make them vulnerable to various security attacks. Malicious nodes in the network may drop packets, modify data, or mislead other nodes during the routing process. Such attacks can significantly affect the network performance and reduce the reliability of data transmission.

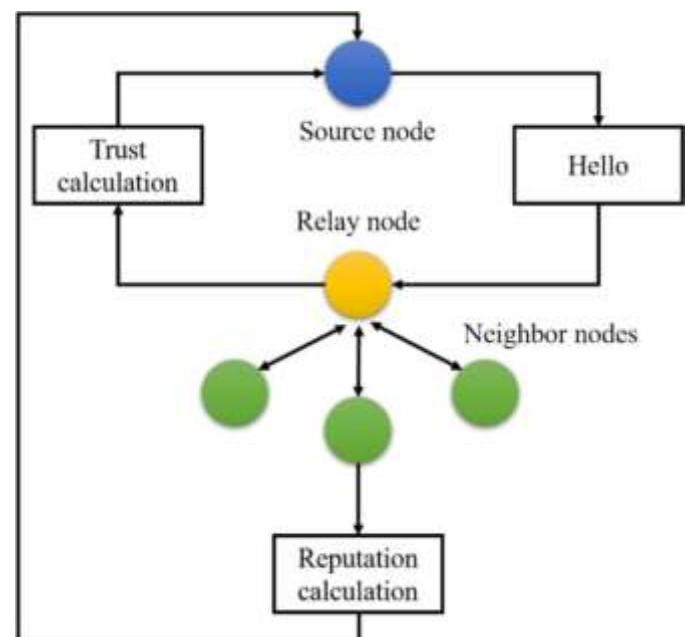


fig :1.1: Active Trust Wireless Sensor Network

The ActiveTrust mechanism improves the security, reliability, and efficiency of data communication in WSNs. By combining trust

management with secure routing strategies, it helps ensure that data packets are transmitted through trusted paths. This approach enhances the overall performance of the network and provides a robust solution for secure communication in Wireless Sensor Networks

2. LITERATURE REVIEW

Wireless Sensor Networks (WSNs) have attracted significant research interest due to their wide applications in environmental monitoring, healthcare, military surveillance, and smart cities. However, security and reliable routing remain major challenges because sensor nodes have limited energy, memory, and computational resources. Many researchers have proposed different secure routing and trust-based mechanisms to improve network reliability and protect WSNs from malicious attacks.

Early research focused on **trust-based routing mechanisms** where nodes evaluate the behavior of neighboring nodes to determine their reliability. In trust-enabled routing systems, reputation or rating mechanisms are used to monitor node behavior and detect malicious activities. These systems help nodes make better routing decisions by selecting trustworthy nodes for packet forwarding. Such approaches improve network security and reduce the impact of malicious nodes in the network.

Another important study proposed **secure routing using trust values**. In this approach, nodes monitor the packet forwarding behavior of their neighbors and calculate trust levels based on their cooperation in forwarding packets. Routes are then selected based on both shortest path and trust value, ensuring that data is transmitted through reliable nodes. This method helps detect selfish or malicious nodes that refuse to forward packets and improves the overall reliability of the network.

Researchers have also proposed **multipath routing based on trust models** to enhance security and reliability. In this method, multiple routing paths are established between the source and destination nodes, and the trust value of each node is considered when selecting the path.

3. PROPOSEDSYSTEM

The proposed system introduces **ActiveTrust**, a secure and trustable routing mechanism for Wireless Sensor Networks (WSNs). The system evaluates node behavior using trust values and selects secure routing paths while avoiding malicious nodes.

4.1 Active Trust Model Overview

The ActiveTrust model is designed to provide secure communication between sensor nodes in the network. In this model, each node monitors the behavior of its neighboring nodes and assigns trust values based on packet forwarding performance and communication reliability. Nodes that behave properly receive higher trust values, while nodes that show suspicious behavior receive lower trust values.

4.2 Trust Evaluation Mechanism

In the proposed system, each node evaluates the trustworthiness of neighboring nodes. The trust value is calculated using parameters such as packet forwarding rate, communication reliability, and node cooperation. If a node consistently forwards packets successfully, its trust value increases.

4. METHODOLOGY

The methodology of the proposed ActiveTrust secure and trustable routing system in Wireless Sensor Networks (WSN) focuses on providing secure communication and reliable data transmission between sensor nodes. Initially, sensor nodes are deployed in the network area and each node is assigned a unique identification number. These nodes automatically discover their neighboring nodes and establish communication links. After the network initialization process, every node starts monitoring the behavior of its neighboring nodes during data transmission.

In the next stage, a trust evaluation mechanism is applied to calculate the trust value of each node. The trust value is determined based on parameters such as packet forwarding rate, communication reliability, and packet dropping behavior. Nodes that successfully forward packets and cooperate with other nodes receive higher trust values, while nodes that drop packets or behave abnormally receive lower trust values. This trust evaluation helps in identifying reliable nodes in the network

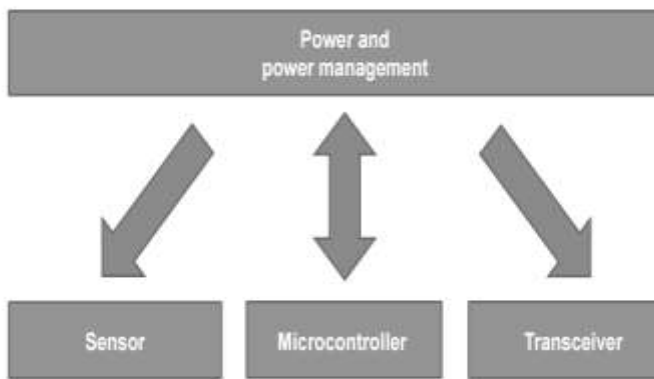


Fig 5.1: *Hardware structure of a WSN sensor node*

After calculating the trust values, the system performs **malicious node detection**. If a node repeatedly shows abnormal behavior and its trust value falls below a predefined threshold, it is identified as a malicious node. These malicious nodes are isolated from the routing process to prevent attacks and data loss in the network.

Next, the **ActiveTrust routing mechanism** selects the most secure and efficient route for data transmission. The routing path is chosen based on nodes with higher trust values, sufficient energy levels, and the shortest distance to the base station. By selecting only trusted nodes for routing, the system ensures secure and reliable communication. Finally, the data packets are transmitted from

the source node to the base station through the base station through the selected trusted path. The performance of the proposed system is evaluated using parameters such as packet delivery ratio, energy consumption, network lifetime, and malicious node detection rate. This methodology improves the security, reliability, and efficiency of data routing in wireless sensor networks.

6. CONCLUSION

The proposed ActiveTrust secure and trustable routing system in Wireless Sensor Networks (WSN) improves the security and reliability of data transmission in the network. In this approach, trust values are calculated for each sensor node based on its behavior during communication. Nodes that behave normally and forward packets correctly are given higher trust values, while nodes that drop packets or act abnormally are identified as malicious nodes.

By detecting and isolating malicious nodes, the system prevents them from participating in the routing process. The ActiveTrust mechanism

selects routing paths only through trusted nodes, which helps in ensuring secure and efficient communication between the source node and the base station. This method also considers energy efficiency while selecting routing paths, which helps in extending the network lifetime.

7. REFERENCES

- [1] Y. Hu, M. Dong, K. Ota, et al., "Mobile Target Detection in Wireless Sensor Networks with Adjustable Sensing Frequency," *IEEE Systems Journal*, 2014.
- [2] M. Dong, K. Ota, A. Liu, et al., "Joint Optimization of Lifetime and Transport Delay under Reliability Constraint in Wireless Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 1, pp. 225–236, 2016.
- [3] S. He, J. Chen, F. Jiang, et al., "Energy Provisioning in Wireless Rechargeable Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 10, pp. 1931–1942, 2013.
- [4] X. Liu, M. Dong, K. Ota, P. Hung, A. Liu, "Service Pricing Decision in Cyber-Physical Systems: Insights from Game Theory," *IEEE Transactions on Services Computing*, vol. 9, no. 2, pp. 186–198, 2016.
- [5] C. Zhu, H. Nicanfar, V. C. M. Leung, et al., "An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 118–131, 2015.
- [6] A. Liu, M. Dong, K. Ota, et al., "PHACK: An Efficient Scheme for Selective Forwarding Attack Detecting in WSNs," *Sensors*, vol. 15, no. 12, pp. 30942–30963, 2015.
- [7] A. Liu, X. Jin, G. Cui, Z. Chen, "Deployment Guidelines for Achieving Maximum Lifetime and Avoiding Energy Holes in Sensor Networks," *Information Sciences*, vol. 230, pp. 197–226, 2013.
- [8] Z. Zheng, A. Liu, L. Cai, et al., "Energy and Memory Efficient Clone Detection in Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 15, no. 5, pp. 1130–1143, 2016.

- [9] T. Shu, M. Krunz, S. Liu, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes," *IEEE Transactions on Mobile Computing*, vol. 9, no. 7, pp. 941–954, 2010.
- [10] P. Zhou, S. Jiang, A. Irissappane, et al., "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 613–625, 2015.
- [11] S. Shen, H. Li, R. Han, et al., "Differential Game-Based Strategies for Preventing Malware Propagation in Wireless Sensor Networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1962–1973, 2014.
- [12] O. Souihli, M. Frikha, B. H. Mahmoud, "Load-Balancing in MANET Shortest-Path Routing Protocols," *Ad Hoc Networks*, vol. 7, no. 2, pp. 431–442, 2009.
- [13] J. Long, A. Liu, M. Dong, et al., "An Energy-Efficient and Sink-Location Privacy Enhanced Scheme for WSNs Through Ring-Based Routing," *Journal of Parallel and Distributed Computing*, vol. 81, pp. 47–65, 2015.
- [14] S. He, J. Chen, X. Li, et al., "Mobility and Intruder Prior Information Improving the Barrier Coverage of Sparse Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 6, pp. 1268–1282, 2015.
- [15] S. H. Seo, J. Won, S. Sultana, et al., "Effective Key Management in Dynamic Wireless Sensor Networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 371–383, 2014.
- [16] Y. Hu, A. Liu, "An Efficient Heuristic Subtraction Deployment Strategy to Guarantee Quality of Event Detection for WSNs," *The Computer Journal*, vol. 58, no. 8, pp. 1747–1762, 2015.
- [17] S. J. Lee, M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," *IEEE ICC*, pp. 3201–3205, 2011.
- [18] Y. Zhang, S. He, J. Chen, "Data Gathering Optimization by Dynamic Sensing and Routing in Rechargeable Sensor Networks," *IEEE/ACM Transactions on Networking*, 2015.
- [19] T. P. Nghiem, T. H. Cho, "A Multi-Path Interleaved Hop-by-Hop En-Route Filtering Scheme in Wireless Sensor Networks," *Computer Communications*, vol. 33, no. 10, pp. 1202–1209, 2010.
- [20] Y. L. Yu, K. Q. Li, W. L. Zhou, P. Li, "Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.