Math. Appl. 15(2)2026, 82–89

An efficient Framework for Reliable Data Transmission in Wireless Sensor Networks

Waseem Ahmad[1], Pawan Kumar[2]

Abstract: *Wireless Sensor Networks (WSNs) are widely used in environmental monitoring, healthcare, agriculture, industrial automation, and smart city applications. These networks consist of numerous sensor nodes that collect and transmit data to a central base station. However, limited energy resources, processing capabilities, memory, and bandwidth create significant challenges for reliable communication. In densely deployed networks, uneven traffic distribution and network congestion can increase packet loss, transmission delays, and energy consumption, ultimately reducing network performance and reliability. Therefore, developing an efficient communication mechanism is essential to ensure reliable data transmission and improve the overall performance of WSNs. To address these challenges, this study proposes an algorithm designed to minimize packet loss and enhance communication reliability in wireless sensor networks. The proposed algorithm is implemented and evaluated using the Network Simulator 2 (NS-2). Its performance is assessed using key parameters, including packet delivery ratio, packet loss ratio, throughput, end-to-end delay, and energy consumption. The evaluation focuses on analyzing the effectiveness of the proposed approach in maintaining stable communication under different network conditions. The study aims to improve data transmission efficiency, reduce communication overhead, and support reliable network operation. The proposed approach is expected to contribute to the development of efficient and robust communication mechanisms for resource-constrained wireless sensor networks.*

Introduction

Wireless Sensor Networks (WSNs) have emerged as a pivotal technology, enabling pervasive monitoring and data collection across diverse domains ranging from environmental monitoring to industrial automation. In the past, the deployment of WSNs has been impeded by challenges inherent in their operational environment, characterized by constrained computational resources and energy limitations. These constraints have often led to unreliable data transmission, particularly in densely populated sensor areas where nodes contend with heavy traffic loads, resulting in packet loss and network degradation. Forecasts indicate that in the near future, these networks will encompass thousands of inexpensive nodes, each endowed with sensing capabilities but constrained by limited computational and communication power. This proliferation of nodes promises the deployment of large-scale sensor networks, facilitating unprecedented data collection and analysis capabilities [1-2].

[1]Research Scholar (Computer Science), Department of Computer Science and Engineering, Shri Venkateshwara University, Gajraula, UP, India
Email: waseem82siddiqui@gmail.com
[2]Research Guide (Computer Science), Department of Computer Science and Engineering, Shri Venkateshwara University, Gajraula, UP, India

Keywords: WSNs, Sensors, Data Loss, Aggregation, QoS, Network Simulator 2

The genesis of wireless sensor nodes can be traced to recent breakthroughs in low-power digital and analog circuitry, alongside advancements in low-power RF design and sensor technology. Unlike traditional computing domains, sensor networks are designed to operate within common environments rather than dedicated ones. This inherent design philosophy necessitates the development of robust communication mechanisms among nodes, enabling them to collaborate in transmitting data to centralized collection points [3].

As these sensor devices are deployed masse, their efficacy hinges on their ability to cooperate and assist one another in data communication tasks. A pivotal milestone toward realizing this cooperative paradigm lies in the design of a sophisticated software architecture. Such an architecture serves as the linchpin bridging the chasm between the raw hardware capabilities of individual sensor nodes and the realization of a cohesive, functional system. Thus, the development of an efficient software framework represents a critical stride toward harnessing the full potential of wireless sensor networks in diverse real-world applications [4].

In the present landscape, as the demand for real-time data analytics and decision-making continues to surge, the need for reliable data transmission in WSNs becomes ever more pressing. Existing solutions, while offering partial mitigation of packet loss, often fall short of providing a comprehensive framework for ensuring data integrity across diverse deployment scenarios. Consequently, there is a critical imperative to develop efficient frameworks that not only address the challenges of packet loss but also optimize network performance and energy utilization [5-6]. Looking toward the future, advancements in WSN technology hold immense promise for revolutionizing various industries and societal sectors. However, realizing this potential hinge upon overcoming the fundamental obstacle of unreliable data transmission. By developing and implementing efficient frameworks tailored to the unique characteristics of WSNs, researchers can pave the way for a future where ubiquitous sensing and data-driven decision-making are not just aspirations but tangible realities, driving innovation and progress across myriad domains [7].

Review of Literature

The literature on Wireless Sensor Networks (WSNs) provides a comprehensive exploration of critical aspects essential to their design and deployment. In [8], a detailed analysis of WSN hardware and software platforms is conducted, accompanied by insights into networking intricacies and future applications. Authors in [9] further delves into fundamental WSN aspects, elucidating architecture, node design, power considerations, and real-world applications, laying a robust foundation for understanding WSN potential across domains. Additionally, in [10] explores conceptual underpinnings of sensor networks, highlighting technology convergence and outlining crucial communication architectures and protocols. In [11] introduces a dynamic routing method tailored for WSNs, prioritizing fault tolerance and minimal routing overhead to ensure robust communication resilience. Security considerations are addressed in [12], proposing location-based keys to safeguard sensors in hostile environments. further, in [13] explores localized sensor localization schemes, enhancing connectivity and accuracy through controlled mobility, promising more efficient data collection and processing in WSNs (Table 1).

Table 1: Review of literature

Author	Key Contribution
S. Roy et al. (2012) [1]	Proposed Pedigree provenance scheme to append every packet with provenance information. Tagger added at each host to include provenance details.
I. Foster et al. (2002) [2]	Identified the need for securing provenance data and introduced Secure Network Provenance. This scheme provides evidence of provenance information's state, aiding network operators in identifying faulty nodes and determining network failures.
K. Muniswamy-Reddy et al. (2006) [3]	Addressed the necessity of identifying source data transmitted over the internet and introduced a scheme ensuring effective confidentiality and integrity of provenance data. Proposed scheme ensures the visibility and integrity of provenance data, safeguarding against unauthorized alterations through encryption.
Y. Simmhan et al. (2005) [4]	Introduced mechanisms for rapidly aggregating sensor data with provenance data. Notably, provenance data is embedded into actual sensor data. However, the system lacks security measures for the provenance data, leaving it vulnerable to unauthorized access or tampering.
R. Hasan et al. (2009) [5]	Narrated the design and efficiency of the Bloom Filter (BF) data structure, focusing on its encoding capabilities and network applications. Bloom Filter utilization involves hashing information and checking element subscriptions, demonstrating potential network uses.
S. Madden et al. (2002) [6]	For network management and failure analysis, introduced the Ex-SPAN provenance system in a distributed environment. Ex-SPAN leverages provenance data to validate network states, showcasing generality and extensibility. However, the system lacks considerations for provenance data safety.
A. Kirsch et al. (2006) [7]	Proposed a method for securing a directed acyclic graph of data provenance. By verifying signatures, integrity of provenance information and its graph structure is ensured, enhancing data provenance reliability.

Challenges Factors in WSNs

The design of Wireless Sensor Networks (WSNs) is intricately shaped by a myriad of challenging factors. These factors encompass diverse aspects ranging from node deployment strategies, energy consumption optimization, and data aggregation techniques to considerations of quality of service, node/link heterogeneity, and fault tolerance mechanisms. Additionally, the dynamic nature of network topology, transmission media constraints, and the imperative of achieving comprehensive coverage further compound the complexity of WSN design [14-15]. Addressing these challenges necessitates a holistic approach that balances various trade-offs to ensure efficient and reliable operation of WSNs across a spectrum of real-world applications (Table 2)

Table 2: Challenging factor for WSNs design

Challenging Factor	Description
Node Deployment	Node deployment in WSN is influenced by the application's requirements and affects routing protocol performance. Deterministic deployment involves manual sensor placement, routing data through predetermined paths. Conversely, random deployment scatters nodes ad hoc, creating an infrastructure without predefined paths.
Energy Consumption	In multi-hop WSNs, nodes act as both data senders and routers, leading to power consumption concerns. Malfunctioning nodes due to power failure can prompt topological changes, requiring packet rerouting and network reorganization.
Data Aggregation	To reduce transmission overhead, similar data from multiple nodes can be aggregated using aggregation functions. This process combines data from various sources, diminishing the number of transmissions.
Quality of Service	Time-constrained applications necessitate bounded latency for data delivery. Data must be delivered within specific timeframes from the moment it's sensed; otherwise, it loses its utility. Ensuring timely data delivery is imperative for applications with strict quality of service requirements.
Data Reporting Model	Data reporting in WSNs varies based on application and time criticality. Reporting can be continuous (time-driven), triggered by events, or initiated by queries. The chosen reporting model significantly influences energy consumption and route stability in the routing protocol.
Node/Link Heterogeneity	While many studies assume homogeneous sensor nodes, some applications necessitate nodes with varied roles or capabilities. Heterogeneous sensor sets pose challenges in data routing, requiring consideration of differing node capacities in computation, communication, and power.
Fault Tolerance	Nodes may fail due to power loss or physical damage, necessitating adjustments in transmit powers and packet rerouting through regions with available energy. Implementing fault-tolerant mechanisms is crucial for maintaining network functionality in the face of node failures.
Network Dynamics	Routing messages involving moving nodes presents challenges, particularly in ensuring route stability alongside energy and bandwidth considerations. Coping with network dynamics becomes paramount when nodes are mobile, requiring adaptive routing strategies to maintain effective communication.
Transmission Media	Wireless sensor networks rely on wireless medium for communication between nodes. Challenges associated with traditional wireless channels, such as fading and high error rates, also impact sensor network operation. Addressing transmission media constraints is essential for ensuring reliable communication within the network.
Coverage	Each sensor node in a WSN provides a specific view of the environment. Thus, achieving adequate area coverage is critical for effective network operation. Coverage considerations influence deployment strategies to ensure comprehensive monitoring and data collection across the target area.

Existing System

The present research underscores the pivotal role of provenance in systems, particularly in contexts where reliance on unreliable information could result in catastrophic failures, as seen in Supervisory Control and Data Acquisition (SCADA) systems. Despite extensive studies on provenance modeling, collection, and querying in workflows and curated databases, the application of provenance in Sensor Networks remains largely unexplored [16-17]. This gap in research highlights the need for a concerted effort to address the integration of provenance mechanisms in Sensor Networks to enhance data reliability and system robustness.

However, several disadvantages hinder the widespread adoption of provenance solutions in sensor networks. These include the intensive use of cryptography and digital signatures in traditional provenance security solutions, which can lead to resource-intensive processes. Additionally, the use of append-based data structures for storing provenance incurs prohibitive costs, limiting their practical implementation. Moreover, existing research often employs separate transmission channels for data and provenance, introducing complexity and potentially compromising efficiency in network communication [18-19]. Addressing these challenges is essential for advancing the integration of provenance in Sensor Networks and realizing its full potential in enhancing data reliability and system security.

Proposed Framework

Ensuring reliable data transfer in Wireless Sensor Networks (WSNs) is a critical challenge due to the inherent constraints of sensor nodes, such as limited power and computational resources. In our proposed system, we address this challenge by focusing on identifying and managing low-power nodes within the sensor network. This approach is particularly vital in large-scale sensor deployments where constant monitoring of all nodes is impractical (Figure 1).

The first step in our system involves the development of algorithms capable of identifying low-power nodes autonomously. These algorithms leverage various metrics, including battery voltage levels, communication latency, and data transmission success rates, to detect nodes experiencing power constraints. By continuously monitoring these metrics, our system can dynamically identify and flag nodes at risk of power depletion.

Once low-power nodes are identified, our system implements strategies to mitigate their impact on data transfer reliability. This may involve redistributing data routing paths to bypass low-power nodes, prioritizing communication with higher-power nodes, or adjusting transmission parameters to optimize energy efficiency. Additionally, our system may trigger proactive measures such as load balancing or node recharging to alleviate power constraints in critical network areas.

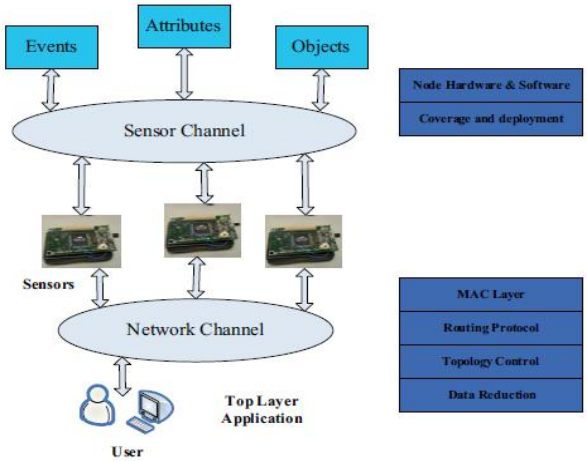


Figure 1: Proposed Wireless Sensor Network Architecture

An essential aspect of our approach is its adaptability to dynamic network conditions. As the network topology evolves or node power statuses change, our system continuously reevaluates and adjusts its strategies accordingly. This adaptability ensures robust and reliable data transfer performance even in dynamic and unpredictable sensor network environments.

Furthermore, our proposed system integrates with existing network management frameworks to facilitate seamless deployment and operation. It provides intuitive interfaces for network administrators to monitor node power statuses, configure system parameters, and analyze data transfer reliability metrics. This integration streamlines the deployment and management of reliable data transfer solutions in WSNs, making them accessible and manageable for real-world applications.

The proposed algorithm aims to mitigate the impact of low-power nodes in Wireless Sensor Networks (WSNs), thereby enhancing overall network reliability. This algorithm is designed to address the challenge of power constraints that often afflict sensor nodes in large-scale deployments. By systematically identifying and managing low-power nodes, the algorithm facilitates more efficient data transfer and prolongs network lifespan.

The Algorithm

The algorithm operates through a series of carefully crafted steps:

- Node Monitoring: The algorithm continuously monitors the power status of individual sensor nodes within the network. This monitoring process involves collecting and analyzing various metrics, including battery voltage levels, energy consumption rates, and communication performance.
- Threshold Identification: Based on the collected metrics, the algorithm establishes thresholds to classify nodes as low-power. These thresholds are determined through empirical analysis and may vary depending on network characteristics and deployment scenarios.
- Low-Power Node Detection: Using the predefined thresholds, the algorithm identifies nodes that fall below the specified power thresholds. Nodes exhibiting signs of power depletion, such as decreased transmission reliability or increased latency, are flagged as low-power nodes.
- Data Routing Optimization: Upon identifying low-power nodes, the algorithm optimizes data routing paths to mitigate their impact on network performance. This optimization process may involve rerouting data paths to bypass low-power nodes, prioritizing communication with higher-power nodes, or dynamically adjusting transmission parameters.
- Dynamic Adaptation: The algorithm continuously adapts its strategies based on real-time changes in network conditions and node power statuses. This dynamic adaptation ensures that the network remains resilient to fluctuations in node power levels and evolving environmental conditions.
- Resource Allocation: To further alleviate power constraints, the algorithm may implement resource allocation strategies, such as load balancing or energy harvesting. These strategies aim to redistribute network resources more efficiently, thereby prolonging the operational lifespan of low-power nodes.

```
Main Algorithm(S,D)
/*S is the source node and D is the destination node, the network defined is dynamic*/
{
1. Find all the nodes that occur in path between source and the destination. These nodes are representing by NodeList(1 to N ).
2. for i=1 to N
3. {
4. if(PacketLoss(NodeList(i))> MAX_THRESHOLD_VALUE)
5. {
6. find the list of compromising nodes for Node NodeList(i). This list is represented by Compromising (1 to K)
7. Select any of the compromising node from this list and use it in place of node dropping the data packet
   NodeList(i)=Rand (Compromising,1,k)
8. if K= 0 /* if there is no compromising node*/
9. {
10. NodeList(i)=Include New Node
11. }
12. }
13. }
14.     }
```

Conclusion and Future Research Scopes

In addressing the challenge of low-power nodes within Wireless Sensor Networks (WSNs), the proposed algorithm offers a significant stride towards enhancing network reliability and resilience. Through its systematic approach of identifying and managing nodes experiencing power constraints, the algorithm optimizes data routing paths, dynamically adapts to changing network conditions, and prolongs the operational lifespan of sensor networks. By prioritizing efficient data transfer and resource management, it lays a solid foundation for dependable communication in WSNs, thereby enabling diverse applications across domains. Looking ahead, future research could delve deeper into optimization techniques to refine data routing and resource management in WSNs. Exploration of energy harvesting solutions, development of fault-tolerant mechanisms, and integration with IoT platforms offer promising avenues for further advancement. By continuing to innovate and address emerging challenges, the field can unlock new opportunities for real-world applications and propel Wireless Sensor Networks towards broader adoption and impact.

References

1) S. Roy, M. Conti, S. Setia, and S. Jajodia, “Secure data aggregation in wireless sensor networks,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 1040–1052, 2012.

2) I. Foster, J. Vockler, M. Wilde, and Y. Zhao, "Chimera: A virtual data system for representing, querying, and automating data derivation," in Proc.of the Conf. Scientific and Statistical Database Management, 2002, pp. 37–46.
3) K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-aware storage systems," in Proc. of the USENIX Annual TechnicalConf., 2006, pp. 4–4.
4) Y. Simmhan, B. Plale, and D. Gannon, "A survey of data provenance in e-science," SIGMOD Record, vol. 34, pp. 31–36, 2005.
5) R. Hasan, R. Sion, and M. Winslett, "The case of the fake picasso: Preventing history forgery with secure provenance," in Proc. Of FAST, 2009, pp. 1–14.
6) S. Madden, J. Franklin, J. Hellerstein, and W. Hong, "TAG: a tiny aggregation service for ad-hoc sensor networks," SIGOPS Operating Systems Review, no. SI, Dec. 2002.
7) A. Kirsch and M. Mitzenmacher, "Distance-sensitive bloom filters," in Proc. of the Workshop on Algorithm Engineering and Experiments, 2006.
8) W. Su Y. Sankarasubramaniam E. Cayirci Akyildiz, I.F. A survey on sensor-networks. IEEE Communications Magazine, pages 102{114, 2002.
9) Kumar.S.P. Chee-Yee Chong. Sensor networks: Evolution, opportunities, and challenges. Proc IEEE, August 2003.
10) Ismail H. Kasimoglui Ian .F. Akyildiz. Wireless sensor and actor: research challenges. (Elsevier) Journal, 2(38):351{367, 2004.
11) Sundeep Karthikeyan Vaidynathan, Sayantan sur and Sinha. Data aggregation techniques in sensor networks. Technical Report, OSU-CISRC-11/04-TR60, 2004.
12) D. Agrawal N. Shrivastava, C. Buragohain and S. Suri. Medians and beyond: new aggregation techniques for sensor networks. Proceedings of the 2nd international conference on Embedded networked sensor systems, pages 239{249, 2004. ACM Press.
13) Xiuli Ren and Haibin Yu1. Security mechanisms for wireless sensor networks. IJCSNS International Journal of Computer Science and Network Security, VOL.6(No.3):100{107, March 2006.
14) S. Setia S. Zhu and S. Jajodia. Leap: e±cient security mechanisms for large scale distributed sensor networks. Proceedings of the 10th ACM conference on Computer and communications security, pages 62{72, 2003. ACM Press.
15) J. Stankovic A. Perrig and D. Wagner. Security in wireless sensor networks.
16) P.Nair H.Cam, S.Ozdemir and D. Muthuavinashiappan. Espda: Energy-efficient and secure pattern-based data aggregation for wireless sensor networks. Computer Communications IEEE Sensors, 29:446{455, 2006.
17) L. Eschenauera nd V. Gligor. A key-managemensct hemef or distributed sensor networks. In Proceedings of the ACM Conference on Computer and Communication Security (CCS), Nov. 2002.
18) H. Chan, A. Perrig, and D. Song. Randomk ey predistribution schemes for sensor networks. In Proceedings of IEEE Symposium on Security and Privacy, May 2003.
19) F. Bouhafs, M. Merabti, and H. Mokhtar, A Semantic Clustering Routing Protocol for Wireless Sensor Networks, Proceedings of the 3rd IEEE Consumer Communications and Networking Conference, 2006, pp. 351-355.