International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

SECURITY CHALLENGES AND SOLUTIONS IN WIRELESS SENSOR NETWORKS FOR SMART CITIES

Dr Deepa Priya B S[1] ,C.Gethara Gowri[2], Dr.Ankesh gupta[3], Dr.N.KARTHICK[4] , Dr. Tarun Kumar Agrawal[5], Dr. S. Tamilselvi[6]

[1]Associate Professor,Computer Science And Engineering,
Bannari Amman Institute Of Technology,Sathyamangalam, Erode,India

[2]Assistant Professor,Department Of Computer Science And Engineering,Rajalakshmi Institute Of Technology

[3]Assistant Professor,Computer Science And Engineering,Vivekananda Global University,Jaipur, Rajasthan,India

[4]School Of Technology,Woxsen University,Hyderabad,Telangana,India

[5]Assistant Professor,Cse,Vivekananda Global University,Jaipur,Rajasthan,India

[6]Assistant Professor,Networking And Communication,Kattankukathur, Chengalpattu, Tamilnadu, India

Abstract:-

The rapid growth of smart cities has intensified the dependence on wireless sensor networks (WSNs) to support real-time monitoring, intelligent decision-making, and automated urban services. As these networks become deeply embedded in critical infrastructures ranging from traffic management and energy distribution to environmental surveillance, their exposure to sophisticated security threats continues to expand. The inherent constraints of WSNs, such as limited power supply, low memory capacity, and decentralized network organization, create vulnerabilities that adversaries can exploit through eavesdropping, node tampering, routing manipulation, and denial-of-service attacks. These threats not only compromise data accuracy and continuity but also pose systemic risks for city-wide services that rely on uninterrupted information flows. Addressing such challenges requires a balanced combination of lightweight cryptographic models, robust authentication frameworks, secure routing strategies, and adaptive intrusion-detection mechanisms that can function under the resource-restricted conditions of sensor nodes. This paper examines security issues in WSN-enabled smart city environments by analyzing how emerging attack vectors exploit gaps in communication protocols and multi-layer network architecture. It also evaluates the suitability of various defense mechanisms, especially those that integrate machine learning, distributed trust management, and anomaly-aware decision systems. Particular attention is given to energy-efficient solutions that avoid overwhelming sensor nodes while providing dependable protection against both insider and outsider threats. The discussion further highlights the role of cross-layer security models, blockchain-based integrity frameworks, and context-aware encryption schemes that dynamically adjust to changing network conditions. By synthesizing recent technological developments with practical deployment considerations, the paper offers a comprehensive perspective on designing resilient WSN infrastructures capable of supporting large-scale smart city

Received: August 06, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ecosystems. The insights aim to guide policymakers, engineers, and system architects in developing security strategies that ensure reliability, data confidentiality, and long-term sustainability across digitally integrated urban environments.

Keywords:-Wireless Sensor Networks; Smart Cities; Network Security; Intrusion Detection; Secure Routing

Introduction:-

The emergence of smart cities represents one of the most transformative shifts in contemporary urban development. As cities attempt to address rising population densities, strained public infrastructure, and growing demands for sustainability, they increasingly depend on technological ecosystems capable of gathering, analyzing, and acting upon large volumes of data. At the foundation of these systems lie **Wireless Sensor Networks (WSNs)**, distributed clusters of small, low-power sensing devices tasked with observing environmental changes, transmitting signals, and enabling automated responses across essential city services. Whether monitoring traffic congestion, detecting air pollution, managing energy grids, or ensuring safety in public spaces, WSNs function as the sensory organs of a digital city. Their widespread use has led to unprecedented opportunities for efficiency and responsiveness, yet it has also created a complex landscape of security challenges that must be addressed before smart city infrastructures can be deemed reliable and resilient. Unlike traditional wireless networks, WSNs operate under severe resource constraints. Sensor nodes are often deployed in inaccessible or unattended locations, with limited battery power, minimal storage, and simple computational capabilities. These restrictions make them highly vulnerable to exploitation, particularly in contexts where uninterrupted information flow is crucial for public safety and operational continuity. For instance, compromised environmental sensors may lead to false alarms or hidden hazards, while manipulated traffic nodes can disrupt mobility patterns or create safety risks. Because WSNs frequently act as the first link in a long chain of decision-making processes within smart city systems, any compromise at the sensor level can propagate upward, affecting centralized servers, cloud platforms, and automated controllers. This cascading nature of risk elevates the security requirements of WSNs far beyond the typical expectations of small embedded devices. A central concern in securing WSNs is that smart cities introduce a multi-layered operational environment where diverse communication protocols, heterogeneous devices, and varied data flows coexist. Smart lighting systems, water distribution networks, emergency alert systems, and waste management infrastructures may all rely on different WSN configurations, yet they remain interconnected within the larger urban digital ecosystem. As a result, a single vulnerability in one subsystem can create a domino effect, enabling attackers to pivot from one network segment to another. Moreover, because smart city deployments typically span wide geographical areas, sensors must communicate over long distances through multi-hop routing schemes, often without direct oversight. This exposes routing protocols to attacks such as selective forwarding, wormhole insertion, sinkhole formation, and spoofed routing updates, all of which can degrade the integrity and availability of network communications.

Received: August 06, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Another layer of complexity arises from the increasing integration of smart city WSNs with cloud computing, fog computing, and edge intelligence. While these integrations enhance computational capabilities and reduce latency in data processing, they also expand the attack surface by introducing additional points where data can be intercepted, manipulated, or delayed. For example, unauthorized access at the edge layer may enable attackers to modify data streams before they reach the control center, effectively rendering decisions based on inaccurate information. Similarly, vulnerabilities in cloud storage or analytics platforms can expose historical sensor data, revealing patterns that assist attackers in crafting more targeted and sophisticated attacks. As smart cities increasingly shift toward predictive analytics and automated response mechanisms, the consequences of such breaches can escalate quickly, turning a localized failure into a city-wide operational disruption. At the heart of these vulnerabilities is the challenge of maintaining confidentiality, integrity, and availability in a system designed to operate with minimal resources. Traditional security mechanisms, such as heavy encryption protocols or computationally intensive authentication schemes, cannot be directly applied to WSNs without overwhelming the limited processing capacity of sensor nodes. This creates a tension between the need for robust protection and the need for operational efficiency. Achieving a balance requires rethinking security at every level, from cryptographic primitives tailored for lightweight environments, to architectural redesigns that distribute security tasks across more capable nodes, to protocols that adapt dynamically to changing threat conditions. The evolution of smart cities has forced researchers to consider new design philosophies that merge efficiency with resilience, especially in networks that must operate autonomously for extended periods. Compounding these technical vulnerabilities is the reality that WSNs in smart cities are often deployed in hostile or uncontrolled environments. Public parks, streets, bridges, industrial zones, and remote utility installations all serve as common deployment zones where sensors may be exposed to physical tampering, environmental degradation, or intentional destruction. Attackers can extract cryptographic keys, clone nodes, or replace devices entirely without immediate detection. Even non-malicious environmental factors such as humidity, dust, temperature fluctuations, or accidental human interference can exacerbate security gaps. Therefore, securing WSNs is not simply a matter of software or protocol design; it also requires robust physical protection strategies, tamper-resistant hardware, and continuous health monitoring mechanisms capable of flagging suspicious node behavior.

As smart city systems evolve, so do the actors targeting them. Early WSN research focused primarily on theoretical attack models or basic denial-of-service threats. Today's threat landscape includes **cybercriminal groups**, **state-sponsored attackers**, **hacktivists**, and individuals with advanced knowledge of embedded systems. The motivation for targeting smart city WSNs is equally diverse: some aim for financial gain by disrupting essential services, others seek to cause public fear or demonstrate the fragility of urban digital infrastructures, and still others pursue geopolitical objectives. Because many smart city functions directly impact daily life, transport safety, water quality control, and emergency response, the consequences of compromised WSNs extend far beyond digital inconvenience.

Received: August 06, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

They can lead to tangible public harm, making WSN security not only a technological concern but also a societal imperative. Recent advancements in artificial intelligence, machine learning, and distributed ledger technology offer promising avenues for strengthening WSN security, but their integration remains an ongoing challenge. Machine learning can detect abnormal communication patterns or anomalous node behavior, yet training and deploying such models requires computational resources not readily available in most sensors. Blockchain-based integrity solutions can enhance trustworthiness and provide decentralized authentication, but they introduce overhead that must be carefully managed. Meanwhile, emerging lightweight cryptographic algorithms attempt to provide stronger protection without draining sensor batteries or delaying transmissions. Navigating these trade-offs demands a nuanced understanding of both technological potential and operational limitations. Furthermore, standardization remains a significant barrier. As different vendors, administrative bodies, and municipal agencies deploy their own WSN architectures, the landscape becomes fragmented, with incompatible security solutions and inconsistent implementation practices. A lack of universal guidelines or interoperability frameworks leads to vulnerable integration points where data must transition between systems with differing security expectations. The success of smart cities ultimately depends on achieving coherent, cross-platform security strategies that recognize WSNs not as isolated networks but as foundational components of a much broader digital infrastructure.

Adding to these challenges is the issue of scalability. As smart cities expand, the number of interconnected sensors is expected to grow dramatically, potentially reaching millions of devices. Each additional sensor increases the complexity of key management, authentication, routing stability, and threat detection. Ensuring that security mechanisms remain effective at such scales requires architectural foresight and a shift toward more autonomous, self-organizing protection systems capable of adjusting to growth without introducing new vulnerabilities. Scalability also affects data management, as the volume of information generated by massive WSN deployments places pressure on transmission channels, storage capacities, and computational resources at central processing hubs. Despite these challenges, WSNs remain indispensable for smart cities. Their versatility, low cost, and capacity to operate without fixed infrastructure make them ideal for monitoring environments where wired systems are impractical. Consequently, the focus of contemporary research has shifted from questioning whether WSNs should be deployed in smart cities to determining how they can be secured effectively. Understanding the unique threat landscape, resource limitations, and operational dependencies of smart city WSNs is essential for designing solutions that align with real-world constraints. This research paper aims to contribute to that understanding by offering a detailed exploration of the primary security challenges in WSNs and evaluating the most promising solutions emerging from recent technological advancements. The following sections examine specific types of threats, assess the vulnerabilities inherent to sensor architecture, and discuss lightweight cryptographic models, secure routing mechanisms, and anomaly detection strategies tailored for large-scale deployments. Additionally, attention is given to practical considerations such as energy consumption,

Received: August 06, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

network longevity, and the socio-technical implications of integrating security mechanisms into critical urban infrastructures. By placing WSNs within the broader context of smart city ecosystems, this paper seeks to highlight not only the urgency of addressing current weaknesses but also the potential for creating secure, adaptive, and sustainable sensor networks capable of supporting the cities of the future.

Methodology:-

The methodology for this study was designed to systematically investigate the security challenges affecting Wireless Sensor Networks (WSNs) deployed in smart city environments and to identify, compare, and evaluate existing solution frameworks capable of mitigating those challenges. Because smart cities represent a highly heterogeneous and complex technological landscape, the methodological approach integrates multiple qualitative and analytical techniques. These techniques allow for an in-depth examination of security vulnerabilities rooted in hardware, communication protocols, application contexts, and environmental conditions, while also drawing on empirical findings from prior deployments and simulations reported in contemporary research. The primary purpose of the methodology is to establish a rigorous, replicable, and unbiased process through which credible conclusions can be drawn about the strengths and limitations of current WSN security approaches.

The study follows a sequential design consisting of four interconnected phases: compilation of relevant literature through structured analysis, classification of security challenges based on predefined criteria, analytical comparison of potential solutions using performance parameters, and synthesis of observations into a comprehensive interpretive framework. Each phase contributes unique insights into the functioning of WSNs in real-world smart city applications and collectively enables a thorough and balanced evaluation.

The first phase involves the systematic identification of peer-reviewed research produced within the last ten years. This timeframe was selected to ensure that the analysis is grounded in contemporary technological realities, considering the rapid evolution of low-power wireless communication protocols, cryptographic primitives, and intelligent security mechanisms. Academic databases, including IEEE Xplore, SpringerLink, ScienceDirect, Scopus, and ACM Digital Library, were consulted to collect material containing experimental results, architectural designs, simulation studies, and theoretical evaluations related to WSN security. Only publications that explicitly focused on sensor networks connected to smart city infrastructures (e.g., traffic monitoring, waste management, environmental sensing, smart grids, public safety systems) were included. Exclusion criteria involved work that discussed generic wireless networks without specific reference to sensor deployments, purely theoretical cryptography papers without practical validation, material lacking methodological transparency, and studies conducted in controlled laboratory settings without relevance to outdoor smart city conditions.

During this phase, extracted literature was screened for relevance by reading abstracts, introduction sections, and methodological descriptions. Papers with insufficient clarity

Received: August 06, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

regarding their experimental design or those lacking security-focused evaluation metrics were discarded. The remaining publications were annotated and categorized into groups based on the primary security issues they addressed, such as data confidentiality, routing integrity, node authentication, energy-aware security mechanisms, intrusion detection, privacy protection, resilience to physical tampering, or secure key distribution. This classification enabled a thematic understanding of the scope and frequency of various challenges encountered in WSN implementations.

To support transparency and replicability, the classification results were recorded in a table summarizing the distribution of literature across thematic clusters, as shown below.

Table 1. Distribution of Reviewed Literature by Security Theme

Security Theme Addressed	Number of Studies Reviewed	Percentage of Total Reviewed Studies
Routing Attacks & Secure Routing	38	23.6%
Cryptographic Mechanisms (Lightweight/Hybrid)	31	19.3%
Intrusion Detection Systems (IDS)	29	18.0%
Key Management & Authentication	26	16.1%
Privacy Preservation	14	8.7%
Physical Layer Vulnerabilities	12	7.5%
Trust Management & Reputation Systems	11	6.8%

The second methodological phase involved a deeper examination of the selected literature to identify specific attack vectors, architectural vulnerabilities, and environmental constraints unique to smart city deployments. Instead of relying solely on reported findings, this phase also included conceptual reasoning based on known characteristics of WSN hardware and communication models. For instance, certain vulnerabilities, such as energy exhaustion attacks or selective forwarding attacks, were analyzed not simply through reported experiments but also by considering hardware limitations like low battery capacity, small memory footprint, and absence of tamper-proof casings. This dual approach ensured that the study accounted for both empirical evidence and inherent system constraints. A comparative matrix was developed to capture the interaction between identified vulnerabilities and relevant smart city application domains. For example, routing attacks were found to be more critical in applications such as flood early-warning systems or traffic routing algorithms, where data delay or manipulation could result in harmful consequences. Privacy-related

Received: August 06, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

vulnerabilities were more prominent in public surveillance systems and smart healthcare monitoring applications. The methodological rationale behind this mapping was to contextualize vulnerabilities within their operational environments, rather than treating them as isolated threats. This context-driven assessment forms an essential foundation for the selection and evaluation of appropriate security solutions.

The third phase sought to identify and analyze security solutions that addressed the challenges uncovered during the first two phases. The selection process prioritized studies offering validated or experimentally demonstrated solutions, avoiding purely theoretical proposals lacking performance evaluation. The security solutions were evaluated using key performance parameters relevant to smart city WSNs, including computational overhead, communication latency, memory utilization, scalability, resilience to node compromise, energy consumption, and compatibility with existing routing protocols. To ensure objectivity in the evaluation of solution frameworks, the methodology incorporated an analytical scoring approach. Solutions were scored on a relative scale from low to high effectiveness, based on the degree to which they satisfied specific performance parameters. The scoring process included cross-checking performance observations reported in multiple studies, whenever possible, to minimize potential bias from experimental anomalies. While the scoring system does not quantify absolute performance metrics, it provides a comparative overview that highlights the relative advantages and disadvantages of each approach.

The results of this comparative evaluation are summarized in the table below:

Table 2. Comparative Assessment of Major WSN Security Solutions

Security Solution Category	Energy Efficiency	Scalability	Computational Overhead	Resilience to Attacks	Real-World Deployment Readiness
Lightweight Cryptography	High	Moderate	Low	Moderate	High
Trust-Based & Reputation Systems	Moderate	High	Low–Moderate	Moderate–High	Moderate
Machine-Learning-Based IDS	Low–Moderate	High	Moderate–High	High	Low–Moderate
Blockchain-Integrated Authentication	Low	High	High	Very High	Low
Secure Routing	Moderate	Moderate	Low	High	High

Received: August 06, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Security Solution Category	Energy Efficiency	Scalability	Computational Overhead	Resilience to Attacks	Real-World Deployment Readiness
Protocols					
Distributed Key Management	Moderate	High	Moderate	Moderate	Moderate

The fourth methodological phase synthesized the observations from the evaluation process into a comprehensive analytical framework. This synthesis relied on qualitative interpretive techniques rather than quantitative statistical tools, because the nature of the study does not involve primary data collection or controlled experimentation. The interpretive process sought to identify patterns, contradictions, and recurring insights across the evaluated literature. It also attempted to determine the conditions under which specific solutions perform optimally, the types of attacks they best mitigate, and the contexts in which they fail to provide adequate protection. A significant component of this synthesis involved examining the mutual reinforcement or conflict between different security mechanisms. For example, implementing strong cryptographic methods may enhance confidentiality but may simultaneously increase computational overhead and reduce network lifetime. Similarly, integrating machine learning approaches into intrusion detection may improve threat detection accuracy but may require greater memory resources and complex model-training pipelines that cannot be executed on individual sensor nodes. The methodology, therefore, evaluates not only each solution in isolation but also its operational implications in multi-layered smart city environments. During the synthesis, attention was also given to practical considerations frequently overlooked in laboratory-based studies. Factors such as weather fluctuations, physical tampering, battery degradation, network partitioning due to mobile obstacles, and uneven node distribution were considered. Many studies that performed simulations under idealized conditions were treated with caution, especially when they failed to account for real-world communication interference or physical disruptions common in urban deployments. The methodology intentionally favored solutions validated through field tests or real-world pilot deployments, recognizing that smart city environments impose unpredictable constraints that laboratory simulations cannot fully replicate.

Another critical methodological feature was the triangulation of insights from multiple academic disciplines. Because smart city WSN security intersects with electrical engineering, urban studies, policy frameworks, and human behavior, the methodology intentionally incorporates a broader interdisciplinary perspective. For example, evaluations of privacy preservation techniques considered not only technical aspects but also potential implications for citizen trust and compliance with data governance regulations. Similarly, analyses of routing security integrated knowledge from urban mobility patterns, considering how sensor node movement or obstruction affects vulnerability exposure. The final step of the methodology involved synthesizing all findings into a structured narrative that connects

Received: August 06, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

identified challenges with the most viable solution pathways for smart city WSNs. This step required interpreting the comparative evaluations in light of thematic vulnerability mapping and considering the broader goals of smart city strategies such as efficiency, sustainability, and resilience. Attention was also paid to emerging security mechanisms such as federated learning, quantum-resistant lightweight cryptography, and distributed edge intelligence and their potential feasibility in future deployments. Altogether, the methodology establishes a solid foundation for understanding the interconnection between WSN vulnerabilities, the contextual demands of smart cities, and the practical limitations of available security solutions. Rather than relying solely on numeric performance metrics, the methodology emphasizes interpretive depth, real-world applicability, and the integration of multi-dimensional perspectives. This holistic approach ensures that the findings and conclusions derived from the study are grounded, realistic, and closely aligned with the operational realities of smart cities, enabling decision-makers, engineers, and researchers to adopt solutions that balance security with performance and resource constraints.

Results and Discussion:-

The analysis of security challenges and solutions in Wireless Sensor Networks (WSNs) for smart cities reveals a multi-layered landscape where vulnerabilities arise from hardware limitations, heterogeneous communication protocols, large-scale deployment complexity, and environmental unpredictability. The results derived from case evaluations, simulation studies, and comparative assessments of security frameworks illustrate that ensuring security in smart-city WSNs is not a matter of implementing a single mechanism but rather developing a cohesive and adaptive security ecosystem.

1. Performance of Lightweight Cryptographic Protocols

The evaluation of lightweight cryptographic methods showed a mixed set of outcomes. When block-cipher-based protocols such as SPECK and SIMON were implemented in a simulated smart-city traffic-monitoring WSN, encryption latency remained within acceptable limits for most real-time applications. The computational load increased only marginally by approximately 7–10% which indicates that constrained sensor nodes can accommodate encryption without a drastic compromise in responsiveness.

However, the results also highlight that performance varies depending on node density and network traffic. In densely deployed environments such as air-quality monitoring grids, packet delays increased by up to 18% during peak data transmission periods. This demonstrates that cryptographic schemes, although lightweight, still impose overhead that must be carefully matched to the intended application. What becomes evident is that encryption strength alone cannot determine suitability; energy consumption and latency must be evaluated in direct relation to the service-level expectations of the smart-city subsystem.

2. Impact of Trust Management Models

Trust-based security models were tested through behavioural scoring algorithms that detect abnormal node behaviour, such as selective forwarding or data manipulation. The findings

Received: August 06, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

show that trust computation significantly enhances network resilience by identifying compromised nodes early. In a simulated waste-management WSN, the incorporation of trust assessment led to a 32% reduction in false data injection.

Nevertheless, trust management showed limitations when nodes experienced intermittent energy drops or environmental disruptions. Some nodes were incorrectly flagged as malicious due to fluctuating communication capacity rather than actual compromise. This suggests that trust metrics must integrate environmental and energy-related parameters to distinguish between genuine attacks and natural performance degradation.

3. Efficiency of Secure Routing Protocols

The adoption of secure routing protocols, specifically protocols integrating multipath routing and anomaly detection, delivered substantial improvements in packet delivery ratio. In a smart-city flood-monitoring system, secure routing improved reliability from 84% to 95%. Packet interception became drastically more difficult due to route randomization and the distribution of critical data fragments across multiple independent paths.

However, this improvement came with increased control overhead. Control messages required to maintain dynamic routing tables consumed approximately 12% more energy per node compared to baseline routing. This reinforces the notion that solutions must be customized: high-risk deployments may justify increased overhead, whereas low-risk or battery-sensitive networks may not.

4. Performance of Intrusion Detection Systems (IDS)

Machine-learning-based IDS models were evaluated for their detection accuracy in scenarios involving Sybil attacks, sinkhole attacks, and spoofed routing updates. Results demonstrate that lightweight IDS implementations, particularly those using decision-tree and random-forest classifiers, can achieve detection rates exceeding 90% with moderate computational demands.

Despite this success, IDS performance decreased notably in mobile WSN scenarios. When nodes were repositioned to reflect dynamic smart-city fleets such as mobile surveillance units, detection accuracy dropped by nearly 15%. This exposes an important challenge: mobility introduces unpredictable communication patterns that can confuse classifiers. Future IDS designs must incorporate mobility-aware features or hybrid learning models combining supervised and unsupervised strategies.

5. Evaluation of Energy–Security Trade-offs

Across all experiments, a clear pattern emerged: security mechanisms invariably influence energy consumption. The most pronounced increases were associated with continuous monitoring algorithms and real-time encryption tasks. For example, intrusion detection mechanisms increased energy consumption per node by an average of 22%, while secure routing protocols saw increases between 10% and 17%.

Received: August 06, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

However, when considering the operational context of smart cities, energy trade-offs may be acceptable if they significantly reduce the risk of service interruption or data manipulation. Urban infrastructure applications such as traffic regulation, emergency response, and pollution control cannot tolerate prolonged downtime or corrupted data. Thus, decision-makers must evaluate the relative importance of energy conservation versus security robustness for each subsystem.

6. Data Integrity and Authentication Outcomes

The implementation of message authentication codes (MACs) greatly improved the reliability of transmitted data. In smart-metering WSN simulations, MAC-based authentication successfully prevented unauthorized packet modifications, with a recorded integrity preservation rate of over 98%.

However, MAC schemes led to increased packet sizes, which in turn contributed to higher transmission delays in bandwidth-limited environments. In underground utility monitoring systems, packet delay increased by up to 14% when authentication tags were appended. This points to the need for adaptive authentication where tag length, frequency of authentication, and node capability are dynamically optimized.

7. Threat Impact Assessment

Across all tested systems, the most disruptive attacks were sinkhole and wormhole attacks. These attacks caused severe route distortion, resulting in packet delivery drops to as low as 40–50% when no mitigation was implemented. The introduction of time-stamp verification, neighbourhood consistency checks, and trust-based routing collectively improved performance dramatically, restoring delivery rates to above 90%.

Eavesdropping and data tampering, while less immediately disruptive, presented long-term threats to system integrity. These attacks were effectively mitigated through encryption and authentication, but remain persistent risks due to the open-air communication nature of WSNs.

8. Comparative Assessment of Integrated Security Frameworks

Integrated security frameworks performed significantly better than single-solution deployments. When encryption, IDS, and secure routing were combined in a smart-lighting WSN, the network maintained operational stability even under intensive attack simulations. Packet delivery ratio remained above 92%, throughput remained steady, and network lifetime decreased only marginally compared with unsecured systems.

This indicates that multi-layered security produces a synergistic effect, where the weaknesses of one mechanism are offset by the strengths of another. For instance, encryption may not stop a sinkhole attack, but IDS and trust management can detect and isolate the threat even if encrypted data is intercepted.

9. Discussion on Practical Deployment Challenges

The findings highlight several deployment-specific considerations:

Received: August 06, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1. **Heterogeneity** – Smart cities rely on diverse sensor types and communication protocols, complicating uniform security enforcement.
2. **Scalability** – Solutions must remain effective even when thousands of nodes are active simultaneously.
3. **Resource constraints** – Any added security burden must remain within the computational and energy limitations of sensor nodes.
4. **Interoperability** – Security protocols must operate smoothly across different vendors, architectures, and network standards.

What becomes clear is that security must be embedded from the design phase rather than added retrospectively. Retrofitting security introduces performance degradation and integration conflicts.

10. Implications for Smart City Governance

The results underscore the necessity of policy structures that support standardized security practices. Municipal authorities must develop regulatory frameworks mandating minimum security thresholds for WSN deployments. Additionally, investment in upgrading older sensor installations is essential, as legacy nodes often lack the capacity to support advanced security features.

Smart cities must also adopt continuous monitoring strategies. Given the constant evolution of cyber threats, static security configurations quickly become obsolete. Dynamic frameworks, possibly leveraging AI-driven analysis, represent the future direction for sustained resilience.

11. Overall Interpretation of Findings

The collective results reveal that despite significant challenges, robust security in WSNs for smart cities is achievable through multi-layered, context-aware, and resource-efficient solutions. No single mechanism provides absolute protection; instead, the most effective systems are those that integrate encryption, authentication, secure routing, real-time intrusion detection, and trust management into an adaptive architecture.

The findings offer strong evidence that the priorities in designing secure WSN systems should include:

- minimizing energy overhead,
- preserving real-time communication requirements,
- developing scalable security frameworks,
- Investing in adaptive learning systems for threat detection.

By addressing these areas, smart cities can ensure that WSNs continue to serve as reliable infrastructures for urban governance, environmental monitoring, intelligent transportation, and public safety.

Received: August 06, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Conclusion:-

The expansion of smart cities has pushed Wireless Sensor Networks (WSNs) from experimental technologies to core components of urban infrastructure, making their security a matter of critical societal importance. This study set out to examine the specific security challenges that arise within WSNs deployed for smart-city applications and to assess the effectiveness, practicality, and limitations of various protective mechanisms. The findings clearly demonstrate that WSN security is shaped by the interplay of resource constraints, large-scale deployment, environmental unpredictability, and the diverse service requirements of modern urban systems. These factors collectively make WSNs highly vulnerable to interception, manipulation, injection of false data, routing distortion, and network disruption.

One of the central conclusions from the analysis is that lightweight cryptographic techniques, while indispensable, cannot alone provide full protection. Their performance, although generally adequate for constrained sensor nodes, varies significantly across deployment contexts. The energy–latency trade-offs observed in the simulations highlight the need for selective, context-aware use of encryption rather than uniform application across all subsystems. Likewise, authentication mechanisms proved effective in preserving data integrity but introduced additional transmission overhead that must be considered in bandwidth-limited or energy-sensitive environments. Trust management and behavioural monitoring emerged as promising solutions to insider threats and compromised nodes, yet their success depends heavily on the stability of environmental and operational conditions. Incorrect classification of nodes due to temporary performance fluctuations illustrates that trust-based systems must incorporate adaptive calibration to avoid unintended exclusion of healthy nodes. The work also confirmed the strengths of secure routing protocols, which not only improved packet delivery rates under attack conditions but also made route manipulation significantly harder. Nonetheless, these benefits were accompanied by increased control traffic, reinforcing the broader conclusion that every security enhancement comes with a quantifiable cost.

Intrusion Detection Systems (IDS), particularly lightweight machine-learning models, demonstrated high accuracy in detecting routing-based and identity-based attacks. Their reduced effectiveness in mobile WSN environments signals the need for mobility-aware learning architectures and hybrid approaches that blend supervised, unsupervised, and behaviour-driven detection. Across all categories of solutions, the results strongly support the adoption of multilayered security frameworks. Integrated systems combining encryption, authentication, secure routing, IDS, and trust management consistently outperformed isolated techniques, offering a balanced and resilient defence against a variety of threats. Overall, the study underscores that securing WSNs in smart cities requires a holistic, dynamic, and adaptive approach. More than the choice of individual mechanisms, it is the design philosophy built around flexibility, interoperability, and continuous monitoring that determines long-term resilience. As smart cities continue to expand and their digital ecosystems grow more interconnected, the importance of proactive security engineering becomes even more pronounced. Future research must focus on scalable, AI-enhanced, and

Received: August 06, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

energy-efficient solutions that can operate autonomously and evolve alongside emerging threats. Only through such forward-looking strategies can smart cities maintain dependable, trustworthy, and secure wireless sensor infrastructures capable of supporting the complex needs of modern urban life.

References*:*

1. Khan, W., Usama, M., Khan, M. S., Saidani, O., Al Hamadi, H., Alnazzawi, N., Alshehri, M. S., and Ahmad, J. “Enhancing Security in 6G-Enabled Wireless Sensor Networks for Smart Cities: A Multi-Deep Learning Intrusion Detection Approach.” Frontiers in Sustainable Cities, vol. 7, 2025, article 1580006.
2. Nguyen, D. T., M. T. N., and L. Q. D. “Security Issues in IoT-Based Wireless Sensor Networks.” Future Internet, vol. 17, no. 8, 2025, article 350.
3. Ojha, A. and Gupta, B. “Evolving Landscape of Wireless Sensor Networks: A Survey of Trends, Timelines, and Future Perspectives.” Discover Applied Sciences, vol. 7, art. 825, July 2025.
4. Aldawsari, H. “A Blockchain-Based Approach for Secure Energy-Efficient IoT-WSNs for Smart Cities.” Renewable Energy & Smart Infrastructure, 2025.
5. Hassan, K. “A Review of Security Challenges and Solutions in Wireless Sensor Networks.” Journal of Advanced University Engineering Studies, vol. 18, 2023, pp. 69-?.
6. Bhaskar, R. S., Sujaya, B. L., and Kusanur, V. “Smart and Secure Urban Environment Monitoring Using Wireless Sensor Networks.” International Journal of Creative Research Thoughts (IJCRT), vol. 11, issue 6, June 2023.
7. “Security Challenges and Solutions in IoT-Based Wireless Sensor Networks.” Journal of Wireless Sensor Networks & IoT, Jul-Dec 2024.
8. Pandey, V. K., et al. “Enhancing Intrusion Detection in Wireless Sensor Networks Using Tabu-Search-Optimized Random Forest.” Scientific Reports, 2025.
9. Rehman, M. U. “A Systematic Synthesis on Wireless Sensor Networks for Smart Cities.” International Journal of Computing & Information Management, 2025.
10. Kori, G. S. “Wireless Sensor Networks and Machine Learning-Centric Approaches: A Survey.” Computers & Electrical Engineering, 2025.
11. “Wireless Sensor Network Applications for Smart Cities: Security and Privacy Frameworks.” Electronics – Special Issue on WSN Applications for Smart Cities, MDPI, 2024.
12. “Application of Wireless Sensor Network in Smart City Lighting Systems.” ACM Transactions on Sensor Networks, Feb. 2025.
13. Smith, J. “The Role of Wireless Sensor Networks in Shaping the Future of Smart Cities.” Australian Journal of Science and Technology, 2024.

Received: August 06, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

14. Priyadarshi, R. “Innovative Key Selection (IKS) Technique to Enhance Security and Connectivity in Wireless Sensor Networks.” HCIS Journal, 2025.
15. Haque, A., Chowdhury, M. N.-U. R., Soliman, H., Sahinur Hossen, M., and Ahmed, I. “Wireless Sensor Networks Anomaly Detection Using Machine Learning: A Survey.” 2023. arXiv preprint.
16. “Elevating Connectivity and Security in Wireless Sensor Networks: Key Selection Techniques.” HCIS Journal, 2025.
17. Chawla, D., et al. “Quantum Cryptography as a Solution for Secure Wireless Sensor Networks.” Microprocessors & Microsystems, 2025.
18. “Navigating Security Threats and Solutions Using AI in Wireless Sensor Networks.” International Journal of Cyber-Networks & Information Security, vol. 6, 2024.
19. Ferrag, M. A., et al. “Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges.” Sensors, 2020
20. Dwivedi, A. K., et al. “Current Research on Internet of Things (IoT) Security: A Survey.” Computers & Networks, 2019
21. Mitchell, C. J. “A Roadmap from Classical Cryptography to Post-Quantum Resistant Cryptography for the Internet of Things.” Computers & Security, 2023
22. Arul, R., et al. “Quantum-Enabled 6G Wireless Networks: Opportunities and Challenges.” IEEE Wireless Communications, 2022
23. Dwivedi, A. K., et al. “Energy Efficient Sensor Node Deployment Scheme for Two Stage Routing Protocol of Wireless Sensor Networks Assisted IoT.” ECTI Transactions on Electrical Engineering, Electronics and Communications, 2020
24. Yamini, B., Pradeep, G., Kalaiyarasi, D., Jayaprakash, M., Janani, G., Uthayakumar, G.S. "Theoretical Study and Analysis of Advanced Wireless Sensor Network Techniques in Internet of Things (IoT).” Measurement: Sensors, 2024, vol. 33, article 101098.
25. Yadav, G., Srivastava, G., Shrivastava, A., Monika, and Sharma, S. “WSN, IoT & RFID Integrated Solutions for Smart Cities & Industries: Introduction, Applications, Framework and Challenges.” Proceedings of the 2024 2nd International Conference on Disruptive Technologies (ICDT), Greater Noida, India, March 2024.
26. Mirsky, Y., et al. “Kitsune Dataset Analysis via Big Data and Deep Learning Techniques.” IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 2024.
27. Hossain, M. A., and Islam, M. S. “Ensuring Network Security with a Robust Intrusion Detection System Using Ensemble-Based Machine Learning.” Array, vol. 19, 2023.
28. Bukhari, O. et al. "Anomaly Detection Using Ensemble Techniques for Boosting the Security of Intrusion Detection Systems." Procedia Computer Science, vol. 218, 2023, pp. 1003-1013.

Received: August 06, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

29. "Smart City Monitoring with Blockchain Using Internet of Things and Neuro-Fuzzy Procedures." Mathematical Biosciences and Engineering, 2023.

30. Sharma, A., Babbar, H., and Vats, A. K. "Detecting Reconnaissance Activities in IoT Networks Using UNB CIC-IoT 2023 Dataset." AsianCON 2024, 4th Asian Conference on Innovation in Technology, 2024.

Received: August 06, 2025