Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
May 2024 5(5), 404–408

ENHANCING RELIABILITY AND EFFICIENCY OF DETECTING MALICIOUS DATA INJECTION IN WIRELESS SENSOR NETWORKS: AN IN-DEPTH ANALYSIS

Vinay Shrivastava[1], Mukta Bhatele[2], Akhilesh A. Waoo[3]

[1, 2, 3] AKS University, SATNA, MP, India

Corresponding Author
Akhilesh A. Waoo,
akhileshwaoo@gmail.com

DOI
10.29121/shodhkosh.v5.i5.2024.1900

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Copyright: © 2024 The Author(s). This work is licensed under a Creative Commons Attribution 4.0 International License.

With the license CC-BY, authors retain the copyright, allowing anyone to download, reuse, re-print, modify, distribute, and/or copy their contribution. The work must be properly attributed to its author.

ABSTRACT

Wireless sensor networks (WSNs) have gained significant attention in recent years due to their versatile applications ranging from wildlife tracking to environmental monitoring. However, WSNs are susceptible to various challenges such as hardware failures, communication link faults, and malicious attacks, which can significantly affect their reliability and performance. In this paper, we focus on the issue of malicious data injection in WSNs and propose a survey to explore its impact on network security and performance.

Keywords: Wireless Sensor Network, Malicious Data Injection, Security, Network Performance

1. INTRODUCTION

A wireless sensor network comprises several short-sized sensor nodes that have computation features. Wireless sensor networks (WSNs) [1] have been widely used in many application areas such as infrastructure protection, environment monitoring, and habitat tracking. Wireless sensor networks consist of small sensor nodes with computational capabilities. These networks enable the collection and transmission of data from remote environments to a central sink node, facilitating real-time monitoring and control. However, the reliability of WSNs is compromised by factors such as hardware failures, communication link faults, and malicious attacks which can disrupt the entire network's communication.

The location of each sensor is planned before placement. Sensors are associated with the assigned locations by humans. The solution is scalable as much work is required for the installation. Furthermore, it is occasionally infeasible to have a manual arrangement as the location information of sensors is anonymous before actual placement. An alternative solution for localization is equipping each sensor with a GPS receiver. Sensors can find themselves independently using the GPS signals. However, connecting a GPS receiver for each sensor node significantly raises the total cost of the sensor network. In addition, the introduction of a GPS receiver increases the energy consumption [2, 16] of a node and hence restrains its lifetime. Finally, the location gained from a GPS receiver may not be precise enough for certain applications and the accuracy of GPS is affected by numerous ecological issues. Precision can be of tenths of meters for general GPS. The mistake can be lowered to less than ten meters for GPS growth systems like Differential GPS (DGPS) but with an advanced cost.

Become possible, including (a) discovering the root causes of observed indications in the network, (b) altering the routing policy for the related nodes, and (c) contributing the spare list of links for every node. In this paper, we propose a survey of malicious data injection in wireless sensor networks.
The rest of the paper is organized as follows.
Section 2 provides the background, relevant for the context. Section 3 provides the literature survey related to malicious data injection in wireless sensor networks. Section 4 concludes the paper with a summary of the main findings concluding remarks, and limitation discussion.

2. BACKGROUND

WSNs operate in diverse environments and are characterized by low-cost, low-power sensor nodes with confined resources. TA wireless sensor network is which organized itself rendering to the situation. It's a collection of nodes. The nodes are low-cost and low-battery power sensor devices. WSN can be positioned on the ground, or in the air[3]. It can be positioned in vehicles, or on bodies of the humans or animals. It can be deployed underwater and inside the houses. The main components of wireless sensor networks are a sensing unit and a wireless transceiver, these nodes collaborate to perform sensing, data communication, and processing tasks, making them suitable for deployment in challenging or inaccessible areas. However, the decentralized nature of WSNs poses threats in terms of network management, reliability, and security. Localization of sensor nodes and giving true consistent data transfer are critical considerations in WSN design. WSNs have the following individual features and limitations: Self-configurable [4]: Sensor nodes are usually arbitrarily prearranged and particularly assemble themselves into a communication range. Battery-powered sensor nodes: Sensor nodes are naturally power-driven by the battery and are prearranged in a corrective situation where it is very stimulating to change or boost the batteries.Dense sensor node situation: Sensor nodes are logically professionally situated and can be numerous orders of magnitude higher than that in a MANET.

Untrustworthy sensor nodes: Sensor nodes are prone to physical damages or letdowns due to their position in a corrective or antagonistic atmosphere.Severe energy, computation, and storage restrictions: Sensors nodes are taking largely incomplete energy, computation, and storage abilities.Data duplication: In utmost sensor network use, sensor nodes are powerfully positioned in an area of attention and group together to accomplish a shared recognizing work. Thus, the data identified by various sensor nodes naturally have a certain level of relationship or replication.

Because of the threats of designing routing protocols for wireless sensor networks, we have many constraints. WSN has limitations due to resources. WSNs have low storage capacity [5], and low bandwidth. The other limitations are low central processing units and limited battery energy. The design threats of WSN are limited hardware resources, limited power capacity, sensor positions, random and big node positioning, scalability, network characteristics and unreliable environment, data aggregation, and many sensing application requirements[17-19].

In WSNs, consistency can be understood into diverse levels event or Packet dependability Level, End-to-End or Hop-by-Hop dependability Level. Nodes in WSNs are disposed to lowdown as to hardware letdown, power reduction, communication link damages, mischievous attacks, and so on. Consistency of WSN is affected by mistakes that may happen due to numerous reasons such as software poor functioning, malfunctioning hardware, dislocation, or environmental hazards. Nodes in sensor networks have very limited energy. In a temporary network battery can be replaced as and when needed. The battery condition of the WSN node is a very important factor for better communication. The hardware in quality condition is very necessary for WSN communication. The communication of WSN is not only affected by antenna angle but also weather conditions, and obstacles. It also depends on interference.

Routing in a wireless network is another type of simple ad-hoc network. Wireless sensor networks are infrastructure-less. Wireless links are not reliable. All the routing protocols of wireless sensor networks require good energy. Wireless sensor nodes may fail because of infrastructure. The wireless sensor network protocols are position-based, hierarchical protocols, data-centric protocols, multipath-based protocols, QoS-based protocols, mobility-based protocols, and heterogeneity-based protocols. Location-based protocols are GAF, TBF, SMECH, GeRaF, MECN, GEAR, Span, and BVGF. Hierarchical Protocols are APTEEN, LEACH [6], HEED, PEGASIS, TEEN.

Data-centric Protocols are Rumor Routing, ACQUIRE, Quorum-Based Information Dissemination, SPIN, EAD, Information-Directed Routing, HABID, GBR, EAR, IDR, COUGAR, DD.

Heterogeneity-based Protocols are CHR, CADR, IDSQ. Multipath-based Protocols are Braided Multipath, Sensor-Disjoint Multipath, N-to-1 Multipath Discovery. Mobility-based Protocols are TTDD, Data MULES, SEAD, Joint Mobility and Routing, and Dynamic Proxy Tree-Base Data Dissemination. QoS-based protocols are SPEED, Energy-aware routing, and SAR.

Low-energy adaptive clustering hierarchy (LEACH): LEACH is the first and most popular energy-efficient hierarchical clustering algorithm for WSNs that was devised to reduce power consumption. The operation of LEACH is divided into rounds having two phases each namely (i) a setup phase to organize the network into clusters, CH advertisement, and transmission schedule creation and (ii) a steady-state phase for data aggregation, compression, and transmission to the sink.

LEACH is completely distributed and requires no global knowledge of the network. It decreases energy consumption by (a) reducing the communication cost between sensors and their cluster heads and (b) turning off non-head nodes as much as possible. LEACH uses single-hop routing where each node can transmit directly to the cluster-head and the sink. Therefore, it does not apply to networks deployed in large regions. Furthermore, the idea of dynamic clustering brings extra overhead, e.g. head changes, advertisements, etc., which may diminish the gain in energy consumption.

3. LITERATURE SERVEY

Developed approaches for network diagnosis in WSNs include debugging tools and inference schemes. The debugging tools focus on source-level debugging of sensor nodes, inference schemes aim to infer network status based on gathered data. False data injection poses a significant threat to WSNs but affects network performance and reliability. Detection of unwanted injections is challenging, especially in multi-hop networks, due to dynamic topology structures and environmental factors. Network diagnosis has been extensively studied in recent years. Existing approaches can be broadly divided into two categories: debugging tools and inference schemes. This work belongs to the latter category. [7] is a notable tool that focuses on debugging sensor nodes at the source, and puts developers to wirelessly connect to a remote sensor and execute debugging commands. To lessen the overhead, some researchers devise established inference models by marking the data packets and then parsing the outcomes at the sink to infer the network status or conduct the diagnosis process in local areas. [8] apply Belief Network with the bipartite graph to represent dependencies among links and end-to-end joins, then the root causes can be outlined by conducting inference on the Belief Network. [9] explores the bottleneck nodes in a WSN, and enhances the network visibility by analyzing the events and status in history. Most approaches actively design their probes to fetch desired information for faulty link detection [10], especially in the managed industry WLANs and wireless mesh networks, where the monitors are easy to deploy. For each cycle, a node is required to monitor the cycle's performance. [11] develops a non-adaptive fault diagnosis through a set of probes where all the probes are employed in advance. The authors in [12] propose a failure detection scheme, in which monitors are assigned to each optical multiplexing and transmission section. These approaches usually compute the probe paths according to different network symptoms, to join the network topology to infer link status. These sensors are equipped with sensing capabilities to collect data on environmental parameters and physical quantities, which are transmitted to a central server or data center for further analysis and decision-making. WSNs are widely employed in various fields, including military affairs, agriculture, healthcare, industrial automation, and intelligent transportation [13]. Typically, the sensors in WSNs are resource-constrained devices in unprotected environments that are vulnerable to physical tampering [14-15]

4. CONCLUSION

WSNs offer promising opportunities for monitoring and control applications in diverse environments. However, challenges such as hardware failures, communication faults, and malicious attacks can undermine their performance and reliability. Malicious data injection poses a significant threat to WSNs, requiring robust detection and mitigation strategies. This paper provides insights into the impact of malicious data injection on WSNs and highlights the importance of addressing the security issue to ensure network integrity and performance.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Vittorio P. Illiano and Emil C. Lupu, "Detecting Malicious Data Injections in Event Detection Wireless Sensor Networks," IEEE Transactions on Network and Service Management, vol. 12, no. 3, pp. 496-512, Sep. 2015.

T. S. Rappaport et al., "Wireless Communications: Principles and Practice," Prentice-Hall, 1996.

W. Dong et al., "Measurement and analysis on the packet delivery performance in a large-scale sensor network," IEEE/ACM Transactions on Networking, vol. 22, no. 6, pp. 1952-1963, Dec. 2014.

H. Chang et al., "Spinning beacons for precise indoor localization," in Proceedings of ACM SenSys, 2008, pp. 127-140.

Qiang Ma et al., "Link Scanner: Faulty Link Detection for Wireless Sensor Networks," IEEE Transactions on Wireless Communications, vol. 14, pp. 4428-4438, Aug. 2015.

S. S. Ahuja et al., "Single-link failure detection in all-optical networks using monitoring cycles and paths," IEEE/ACM Transactions on Networking, vol. 17, no. 4, pp. 1080-1093, Aug. 2009.

Q. Cao et al., "Declarative tracepoints: A programmable and application independent debugging system for wireless sensor networks," in Proceedings of ACM SenSys, 2008, pp. 85-98.

A. Cerpa et al., "Statistical model of lossy links in wireless sensor networks," in Proceedings of IEEE IPSN, 2005, pp. 81-88.

L. Girod et al., "EmStar: A software environment for developing and deploying wireless sensor networks," in Proceedings of USENIX Annual Technical Conference, 2004, p. 24.

Y. Hamazumi et al., "Optical path fault management in layered networks," in Proceedings of IEEE GLOBECOM, 1998, pp. 2309-2314.

C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Networks, vol. 1, no. 2/3, pp. 293-315, 2003.

A. Perrig et al., "Security in wireless sensor networks," Communications Magazine, vol. 47, no. 6, pp. 53-57, Jun. 2004.

El Emary, I.M.M.; Ramakrishnan, S. (Eds.) Wireless Sensor Networks: From Theory to Applications; CRC Press: Boca Raton, FL, USA, 2013

Rani, A.; Kumar, S. A survey of security in wireless sensor networks. In Proceedings of the 3rd International Conference on CICT, Ghaziabad, India, 9–10 February 2017; pp. 1–5.

Jiamin Hu, Xiaofan Yang, Lu-Xing Yang a framework for detecting false data injection in large scale wireless sensor network. March 2024 Sensors 24(5):1643.

M. S. Beg and A. A. Waoo, “A comprehensive study in wireless sensor network (WSN) Using artificial bee colony (ABC) algorithms,” International Research Journal of Engineering and Technology (IRJET), vol. 6, no. 9, pp. 873–879, 2019.

Waoo, A., and Sanjay Sharma. "Threshold Sensitive Stable Election Multi-path Energy Aware Hierarchical Protocol for Clustered Heterogeneous Wireless Sensor Networks." International Journal of Recent Trends in Engineering & Research 3.09 (2017): 158-16.

Jain, Jay Kumar, and Akhilesh A. Waoo. "An Analytical Study of Energy Efficient Routing Approaches in Wireless Sensor Network." THEETAS 2022: Proceedings of The International Conference on Emerging Trends in Artificial Intelligence and Smart Systems, THEETAS 2022, 16-17 April 2022, Jabalpur, India. European Alliance for Innovation, 2022.

Waoo, A. A., and Sharma, S., “Analysis of Energy Efficient Coverage and Prolonging Lifetime by Comparing Homogenous and Heterogeneous Wireless Sensor Networks”, International Conference on Advanced Computation and Telecommunication (ICACAT), 2018.