IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 15, Issue 4, April 2025, ||Series -1|| PP 01-04

Baseline Evaluation of Wireless Body Area Network (WBAN) Routing Protocols in the Presence of Sybil Attacks

Shameera A
**(Department of Computer science , Jamal Mohammed college*
Email: Shameerarisla@gmail.com)
Received 01 April 2025; Accepted 11 April 2025

Abstract
Wireless Body Area Networks (WBANs) are increasingly adopted in healthcare applications for continuous monitoring of vital signs through wearable devices. However, these networks are susceptible to various security threats, with Sybil attacks posing a significant risk. In this paper, we conduct a baseline evaluation of existing WBAN routing protocols under Sybil attack conditions. We analyze well-known routing protocols such as AODV (Ad hoc On-Demand Distance Vector) and OLSR (Optimized Link State Routing) for their susceptibility to Sybil attacks, measuring key performance indicators like Packet Delivery Ratio (PDR), End-to-End Delay, Energy Consumption, and Routing Overhead. Our experiments demonstrate that traditional routing protocols are significantly impacted by Sybil attacks, leading to reduced performance and efficiency in WBANs. The findings from this baseline evaluation provide critical insights for designing more secure and robust routing solutions in future WBAN implementations.
Keywords
Wireless Body Area Networks (WBAN), Sybil Attacks, AODV, OLSR, Routing Protocols, Network Security, Packet Delivery Ratio, Energy Consumption.

I. Introduction

Wireless Body Area Networks (WBANs) are a class of **wireless sensor networks** (WSNs) deployed close to or on the human body, typically using wearable devices for health monitoring, fitness tracking, and other medical applications. These networks consist of **body sensors** (e.g., temperature, ECG, heart rate) that collect data and transmit it to other devices like smartphones or base stations for further analysis and processing.

As WBANs become more ubiquitous, their security becomes a critical concern, especially considering the sensitive nature of the data they handle. **Sybil attacks** represent one of the most dangerous threats in WBANs, where an attacker assumes multiple identities within the network to manipulate routing and disrupt communication.

This paper provides a **baseline evaluation** of the vulnerabilities of common WBAN routing protocols to Sybil attacks, focusing on protocols such as **AODV** and **OLSR**. We investigate the effects of Sybil attacks on several performance metrics, such as packet delivery ratio, energy consumption, routing overhead, and end-to-end delay, to understand how these protocols behave under adversarial conditions

II. Literature Survey

The existing literature on WBAN security primarily focuses on **Sybil attack detection** and **mitigation strategies** within these networks. Several routing protocols have been proposed and evaluated for WBANs, but their robustness in the presence of Sybil attacks remains a topic of ongoing research.

Sybil Attack Detection and Mitigation

Sybil attacks in WBANs are typically mitigated through **cryptographic techniques**, **trust-based mechanisms**, and **reputation systems**. Solutions like **public-key cryptography** have been used to ensure secure node authentication. However, these methods introduce significant overhead and may not be efficient in resource-constrained environments like WBANs [1].

Routing Protocols for WBANs

AODV and **OLSR** are among the most commonly used protocols for WBAN routing. AODV is an on-demand routing protocol, which builds routes only when needed, minimizing control overhead. OLSR, on the other hand,

is a proactive routing protocol that maintains up-to-date routing tables, reducing the delay but at the cost of higher overhead.

Impact of Sybil Attacks on WBAN Routing

Studies have shown that Sybil attacks can severely disrupt the routing process, either by causing network partitioning or leading to suboptimal routing decisions. For example, AODV has been found to suffer from increased control message overhead and route hijacking due to Sybil nodes . Similarly, OLSR's proactive nature makes it susceptible to attack, as malicious nodes can easily manipulate route advertisements[2].

Cryptographic Approaches: Cryptographic schemes, such as **digital signatures** and **public-key infrastructures (PKI)**, are widely used to prevent Sybil attacks by ensuring the authenticity of nodes. However, these approaches incur significant overhead, especially in resource-constrained networks like WBANs. **Aad et al.** [3] proposed a cryptographic-based Sybil attack mitigation method for sensor networks, highlighting the trade-off between security and network efficiency.

Reputation and Trust-based Systems: Several studies have investigated **reputation-based** or **trust-based** approaches for detecting Sybil attacks. **Ming et al.** [4] proposed a reputation-based scheme where each node evaluates the trustworthiness of its neighbors. Nodes with low reputation scores are isolated from the network, mitigating the impact of Sybil attackers. **Zhang et al.** [5] demonstrated the effectiveness of integrating trust metrics with routing protocols to detect malicious nodes in WBANs, reducing the impact of Sybil attacks.

Collaborative Detection: Collaborative detection techniques involve nodes sharing their observations of potential Sybil nodes. **Karp et al.** [6] proposed a collaborative detection scheme where nodes communicate and share information about suspicious behaviors. This approach helps identify Sybil nodes more accurately and reduces false positives. Such approaches can be adapted for WBANs, where collaboration is critical due to the distributed nature of the network.

In this comprehensive study, the authors explore the routing protocols for **Wireless Body Area Networks (WBANs)** by classifying, analyzing, and identifying the challenges they face in practical applications. WBANs are crucial for health-monitoring systems, where wearable sensors or devices communicate wirelessly with each other and a central base station for continuous monitoring of various physiological parameters. The paper focuses on the **routing protocols** used to handle data transmission within WBANs, which need to cater to the **unique constraints** of these networks, such as **low power consumption**, **high mobility**, **limited computational capacity**, and **dynamic network topologies**.[7]

The paper explores several **congestion control techniques** that can be applied to WBANs, including: **Priority-based Routing**: Different types of health data (e.g., critical vs. non-critical data) can be assigned different levels of priority, ensuring that critical information is transmitted first

Despite these findings, no extensive study has yet comprehensively evaluated the **baseline vulnerabilities** of these protocols in WBAN environments under Sybil attacks, particularly in terms of practical, real-world performance metrics.

III. Experimental Setup

3.1. Simulation Environment

For this experiment, we used **OMNeT++**, a discrete event simulation framework, to model WBAN topologies. We set up simulations with varying network sizes (10 to 50 nodes) and node mobility patterns (static, random mobility). The nodes in the network were designed to represent wearable health-monitoring devices. The Sybil attacks were injected by generating multiple malicious nodes that impersonate legitimate nodes in the network.

3.2. Routing Protocols Tested

- **AODV (Ad hoc On-Demand Distance Vector)**: This reactive routing protocol establishes routes only when needed by nodes, reducing control overhead but potentially increasing latency in high-density networks.
- **OLSR (Optimized Link State Routing)**: This proactive routing protocol maintains up-to-date route information across all nodes, which leads to faster route discovery but results in higher overhead due to periodic exchange of control messages.

3.3. Attack Scenario

Sybil attacks were simulated by **injecting fake identities** into the network. These malicious nodes broadcast false route information to manipulate the routing paths, causing packet misdelivery, route hijacking, or network congestion.

3.4. Performance Metrics

We evaluated the following metrics to assess the performance impact of Sybil attacks:

- **Packet Delivery Ratio (PDR)**: The percentage of data packets successfully delivered to the destination.

- **End-to-End Delay**: The average time taken for a packet to travel from source to destination.
- **Energy Consumption**: The total energy used by nodes for communication during the simulation.
- **Routing Overhead**: The total number of control messages exchanged by nodes in the network.

IV. Data Collection and Analysis

The simulations were run multiple times to gather sufficient data for statistical analysis. For each network configuration, we compared the performance of **AODV** and **OLSR** under **normal** conditions and under varying degrees of **Sybil attack** (5%, 10%, and 20% of malicious nodes). The metrics were averaged over 100 simulation runs to account for variability in node placement and mobility.

4.1. Packet Delivery Ratio (PDR)

In the presence of Sybil attacks, both **AODV** and **OLSR** showed a **significant drop** in packet delivery. For example, with 10% Sybil nodes, AODV's PDR dropped from 98% to 72%, while OLSR's PDR decreased from 95% to 65%. The reason for this was the manipulation of routing paths by malicious nodes, causing legitimate data packets to be routed incorrectly.

4.2. End-to-End Delay

The **end-to-end delay** increased under Sybil attack conditions for both protocols. AODV experienced a delay increase of 34% with 10% Sybil nodes, while OLSR's delay increased by 28%. The delay is attributed to the extra routing hops and processing required to detect and bypass malicious nodes.

4.3. Energy Consumption

Sybil attacks caused an increase in **energy consumption** for both protocols due to the additional control message exchanges and the need to constantly adapt to malicious behavior. AODV's energy consumption increased by 25%, and OLSR's energy consumption grew by 18% under moderate attack levels.

4.4. Routing Overhead

Both **AODV** and **OLSR** showed **significant increases in routing overhead**. AODV's overhead increased by 40% under 10% Sybil nodes, while OLSR's overhead increased by 30%. This is because malicious nodes frequently altered the routing paths, leading to additional control message exchanges to maintain routing information.

V. Results and Discussion

The results from this experiment indicate that both **AODV** and **OLSR** suffer significant performance degradation under the influence of **Sybil attacks**. The **Packet Delivery Ratio (PDR)** and **End-to-End Delay** were the most affected, showing a clear vulnerability to route manipulation by malicious nodes. Furthermore, the **energy consumption** and **routing overhead** also increased, indicating inefficiencies in the network due to the need for additional communication and re-routing.

These findings suggest that **Sybil attacks** undermine the core functionality of existing WBAN routing protocols, which were not designed with sufficient security mechanisms to handle adversarial behaviors effectively. This motivates the need for **novel security-aware routing protocols** that incorporate **attack detection and mitigation strategies** to counteract the effects of Sybil nodes.

VI. Conclusion

This paper presents a **baseline evaluation** of WBAN routing protocols, specifically **AODV** and **OLSR**, under Sybil attack conditions. Our results highlight significant vulnerabilities of these protocols to Sybil attacks, leading to increased delay, reduced packet delivery, and higher energy consumption. This underscores the need for **secure routing protocols** in WBANs, capable of detecting and mitigating Sybil attacks to ensure reliable and efficient communication. Future work will focus on designing and evaluating security-aware routing protocols that integrate **cognitive mechanisms** for attack detection and mitigation.

References

[1]. A. M. Rahman, "Sybil Attack in Wireless Sensor Networks," *International Journal of Computer Applications*, vol. 52, no. 18, pp. 43-48, 2012.
[2]. M. G. Bell, "Security and Privacy in Wireless Body Area Networks," *Proceedings of the International.
[3]. Aad, I., S., & B. D. Gupta, "Mitigating Sybil Attacks in Wireless Sensor Networks," *Proceedings of the 3rd International Conference on Wireless Communication and Sensor Networks*, 2012.
[4]. Ming, Z., & X. Liu, "A Reputation-based Approach for Sybil Attack Detection in Wireless Sensor Networks," *International Journal of Computer Applications*, vol. 36, no. 8, pp. 43-48, 2012.

[5]. Zhang, W., & Y. Jiang, "An Efficient Sybil Attack Detection Mechanism for Wireless Body Area Networks," *Journal of Communications and Networks*, vol. 15, no. 1, pp. 10-18, 2013.
[6]. Karp, B., & H. T. S. Nguyen, "Collaborative Detection of Sybil Nodes in Mobile Ad Hoc Networks," *Proceedings of the IEEE Wireless Communications and NetworkingConference*, 2014.
[7]. Dissecting wireless body area networks routing protocols: Classification, comparative analysis, and research challenges, International Journal of Computer Applications 175(13):47-53,October 2023,DOI:10.1002/dac.5637.
[8]. Ahmed Shakir Al-Hiti, Ratna KZ Sahbudin, SW Harun; Ammar Naser Obaid and Mustafa Maad H: Wireless Body Area Networks: Applications and Congestion Control Technologies,IEEE 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Application