International Journal of Advance Research in Science and Engineering
Volume No. 13, Issue No. 03, March 2024
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Adaptive Anomaly Detection for Securing Full Duplex Wireless Sensor Networks with Physical Layer Parameters

Mrs. Sana Amin[1], Prof. Dr. A. D. Jadhav[2]

[1,2]*Department of Electronics Engineering ,Shivaji University*

Abstract: Wireless Sensor Networks (WSNs) are vulnerable to various types of attacks due to their distributed and resource-constrained nature. This research presents an innovative approach for securing WSNs using the BLSF (Behavioral Learning for Security Framework) protocol. The proposed algorithm focuses on detecting anomalies in the behavior of network nodes to identify potential attackers. By leveraging behavioral patterns, the algorithm dynamically adjusts to evolving threats, making it adaptive and robust against sophisticated attacks. The detection process involves monitoring communication patterns, route requests, and received signal strengths to distinguish between normal and malicious behavior. Additionally, the algorithm incorporates neighbor-based analysis to detect anomalies originating from nearby nodes. Through extensive simulations and experiments, the effectiveness and efficiency of the proposed method are validated, demonstrating its ability to accurately detect and mitigate attacks while minimizing overhead. This research contributes to enhancing the security of WSNs, providing a proactive defense mechanism against various forms of attacks, thereby ensuring the reliability and integrity of data transmission in critical applications.

Key words : Physical layer Security , Full Duplex Wireless Network , Wireless Network Security , Secrecy Capacity

I. Introduction:

Wireless Sensor Networks (WSNs) play a crucial role in various applications, including environmental monitoring, healthcare systems, and infrastructure management. However, the distributed and resource-constrained nature of WSNs makes them vulnerable to a wide range of security threats, posing significant challenges to the reliability and integrity of data transmission. Attacks such as node replication, selective forwarding, and sinkhole attacks can compromise the network's functionality, leading to data manipulation, eavesdropping, or even network collapse.

Previous research has proposed various security mechanisms to mitigate these threats, including encryption, authentication, and intrusion detection systems (IDS). However, many existing approaches either suffer from high computational overhead, are not adaptive to dynamic network conditions, or lack effectiveness in detecting sophisticated attacks.

In this context, this paper introduces a novel approach for securing WSNs using the Behavioral Learning for Security Framework (BLSF) protocol. The BLSF protocol focuses on detecting anomalies in node behavior to identify potential attackers, thereby providing a proactive defense mechanism against various forms of attacks. Unlike traditional signature-based IDS, BLSF leverages behavioral patterns to dynamically adapt to evolving threats, making it robust and efficient in detecting both known and unknown attacks.

The primary contribution of this paper lies in the development and evaluation of the BLSF protocol for securing WSNs. By incorporating neighbor-based analysis and behavioral learning techniques, the protocol enhances the network's resilience to attacks while minimizing computational overhead. Through extensive simulations and experiments, the effectiveness and efficiency of the proposed approach are demonstrated, highlighting its potential for real-world deployment in critical WSN applications. This paper aims to address the pressing need for robust and adaptive security mechanisms in WSNs and contributes to advancing the state-of-the-art in securing these networks against emerging threats.

II. Related Work :

This Paper presented work of Bin Van (2017)et .al and Saman atapattu et al(2019) which Securing Full Duplex Wireless Sensor Networks with Physical Layer Parameters techniques to detect Anomaly inside network. Bin Van (2017) et .al proposes a source-based jamming scheme to improve the secrecy performance of cooperative systems with an untrusted FD relay. This scheme exploits the physical characteristics of the wireless channels to protect against eavesdropping attacks. [1]. In physical layer security (PLS) schemes, the secrecy rate is determined by the characteristics of the wireless channels, such as signal-to-noise ratio (SNR), fading, and interference. The PLS schemes exploit these channel characteristics to enhance the secrecy performance of the system.[1] The calculation of the secrecy rate takes into account the transmission power, channel gains, and noise levels at the legitimate receiver and the eavesdropper. calculating these parameter helps to check behavior of network nodes to identify potential attackers along with optimizing these parameters, the secrecy rate can be maximized to ensure secure communication.[1].

Saman atapattu et al(2019) paper suggests two-hop relay selection schemes Optimal Relay Selection (ORS) and Suboptimal Relay Selection (SRS). Optimal Relay Selection (ORS scheme maximizes the minimum secrecy rate among all source-destination (SD) pairs by utilizing both global channel state information (CSI) and SD pair CSI. It requires knowledge of the channel state information of all nodes, including the eavesdroppers. Suboptimal Relay Selection (SRS) scheme is a more practical approach that only relies on the CSI of the main channels and statistical information of the eavesdropper channels. It aims to maximize the minimum secrecy rate among SD pairs while

considering the limited information available. The secrecy outage-intercept probability of the ORS scheme serves as a lower bound for the performance of the SRS scheme

This scheme analyzed general multi-hop networks with multiple eavesdroppers. Numerical results demonstrate the significant enhancement of secrecy performance achieved by the proposed schemes. [2]. The analysis and performance evaluation of the relay selection schemes are based on mathematical derivations and simulations. However, there may be limitations in the accuracy and generalizability of these results to practical wireless networks.[2] The paper focuses on the physical-layer security aspect of relay networks and does not consider other potential security threats or attacks, such as network-level vulnerabilities or higher-layer security protocols.[2]

Andriy Stetsko, et al (2010) paper presents a neighbor-based detection technique for wireless sensor networks, which is localized, unsupervised, and adaptable to changing network dynamics. [3] The paper contributes to the field of intrusion detection in wireless sensor networks by providing a promising and accurate detection technique that takes advantage of spatial proximity and collaboration among neighboring nodes. [3] . The neighbor-based detection technique leverages the principle that sensor nodes in close proximity tend to exhibit similar behavior. By comparing the behavior of a node with its neighboring nodes, the technique can identify malicious nodes whose behavior significantly differs from their neighbors. The technique is localized, unsupervised, and adaptable to changing network dynamics. It has been evaluated and shown to be highly accurate, especially when collaboration among neighboring nodes is utilized. The symptoms and statistics used in the neighbor-based technique enable the detection of selective forwarding, jamming, and hello flood attacks in wireless sensor networks. The paper does not provide a comprehensive analysis of the performance and efficiency of the neighbor-based detection technique in terms of resource utilization, such as energy consumption, memory usage, and computational overhead.

III. Design and Implementation:

A. Establishment of neighbor relationships

Suggested algorithm employs several mechanisms to facilitate efficient and reliable communication while mitigating potential security threats. At its core, our suggested algorithm leverages bordercasting, low-power operation, and shortest-path forwarding to optimize data transmission in resource-constrained environments. Initially, upon node initialization, essential parameters such as node index and identifier are set. The protocol establishes neighbor relationships and initializes data structures to store neighbor information and routing tables. Each node maintains a list of attackers and tracks unwanted messages received from neighboring nodes. An iterative process is employed to handle various events and messages, such as hello messages for neighbor discovery and route requests and replies for route establishment.

To ensure network robustness, BLSF incorporates a route discovery mechanism initiated by nodes when attempting to transmit data to a destination. Route requests are broadcasted to neighboring nodes, and routes are established based on received replies. This process involves hop-by-hop forwarding, with each node maintaining routing information to facilitate packet delivery.

BLSF integrates mechanisms for detecting and mitigating potential attacks within the network. Suspicious nodes are identified based on anomalous behavior, such as the reception of multiple unwanted messages. Once flagged, nodes broadcast attacker announcement packets to alert neighboring nodes, enabling collective identification and marking of suspected attackers. Additionally, the protocol implements jamming signal transmission to disrupt malicious activities and notify eavesdropping nodes of potential threats.

B. Attacker Detection: The BLSF protocol operates through several key stages to identify potential attackers from neighboring nodes and bolster the security of the wireless sensor network. Initially, upon receiving packets from neighboring nodes, the protocol scrutinizes the header information to ascertain the source node. Subsequently, it conducts behavior analysis by monitoring various aspects of neighboring nodes' packet transmission patterns, including frequency and timing. Suspicious activity detection follows, whereby nodes exhibiting unusual behavior, such as excessive packet transmission or routing manipulation attempts, are flagged as potential threats.

To assess the trustworthiness of neighboring nodes, the protocol evaluates their reputation based on observed behavior, assigning higher scores to consistently normal nodes and lower scores to those displaying suspicious behavior. Employing a threshold-based approach, the protocol determines if a node's reputation score falls below a predefined threshold, signaling potential malicious activity. Upon identifying a potential attacker, the protocol takes decisive action, which may include alerting other nodes or implementing defensive measures to mitigate the threat.Dynamic adaptation is integral to the protocol, enabling it to adjust detection mechanisms in response to evolving network conditions and node behavior. This adaptive approach ensures effective identification of potential attackers in dynamic environments, thereby enhancing the overall security of the wireless sensor network.

IV: Experimentation and Result:

A. Simulation Environment: The network consists of 50 sensor nodes deployed in a grid topology of dimensions 1000m x 1000m. The simulation duration is set to 200 seconds. Each sensor node is configured with specific parameters, including the routing protocol (BLSF), energy model, initial energy level, propagation model, antenna type, and wireless channel characteristics. The physical layer parameters such as carrier sensing threshold (CST) and alpha value are also defined to configure the wireless PHY layer.The script initializes the topology, creates a god object for global

IJARSE
ISSN 2319 - 8354

operations, and configures each node according to the specified parameters. Additionally, it sets the position of each node and designates two nodes as eavesdroppers by setting the eves_drop attribute. The simulation scenario involves generating constant bit rate (CBR) traffic between pairs of nodes. A loop iterates over a range of time intervals, during which CBR traffic is initiated from a source node to a destination node. Each CBR flow is defined by its source and destination nodes, start time, and stop time.

B. Evaluation matric: Secrecy Capacity (γR and γD) [1] Secrecy capacity measures the maximum achievable secure communication rate between the source and destination while keeping the information confidential from potential eavesdroppers.

Secrecy capacity is calculated using the formulas [1]:

$$\boldsymbol{\gamma R} = \frac{\alpha \gamma sr}{((1-\alpha)\gamma sr + \gamma rr + 1)} \qquad (1)$$

$$\boldsymbol{\gamma D} = \frac{\boldsymbol{\alpha \gamma sr\ \gamma rd}}{\frac{(\boldsymbol{\gamma rd\ \gamma rr(\ \alpha \gamma sr + 1)})}{\boldsymbol{\gamma sr + 1}} + \boldsymbol{\gamma sr + \gamma rd + \gamma rr + 1})} \qquad (2)$$

where γsr, γrd, and γrr represent the received signal-to-noise ratios (SNRs) at the source-relay, relay-destination, and relay-relay links, respectively [1]. α is a parameter representing the fraction of resources allocated to the source-relay link. By calculating secrecy performance metrics like γR and γD, the BLSF protocol can assess the level of security provided by the network and make informed decisions to enhance security measures if necessary. These metrics consider factors such as received powers, channel conditions, and noise levels to evaluate the effectiveness of the communication channels in maintaining confidentiality.

C. Results: The results section of this paper presents a comprehensive analysis of the performance metrics and characteristics of the proposed protocol under various network conditions and scenarios. Through detailed experimentation and simulation, we examine key parameters such as secrecy capacity, packet delivery ratio, and throughput to evaluate the protocol's effectiveness and efficiency.

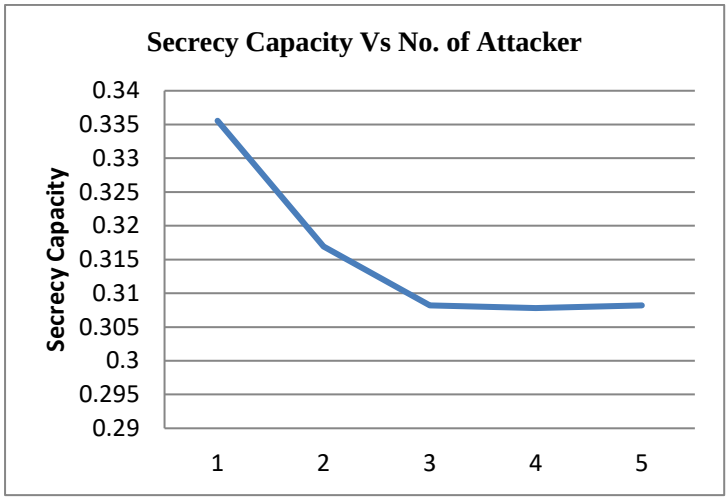

Fig:1 Graph of Secrecy Capacity Vs no.of attackers

Figure (1) shows graph of secrecy capacity versus the number of attackers showcases the protocol's capability to maintain a considerable level of secrecy even in the presence of attackers. Despite a slight decrease in secrecy capacity with an increasing number of attackers, the protocol demonstrates resilience and effectiveness in safeguarding communication against potential threats.

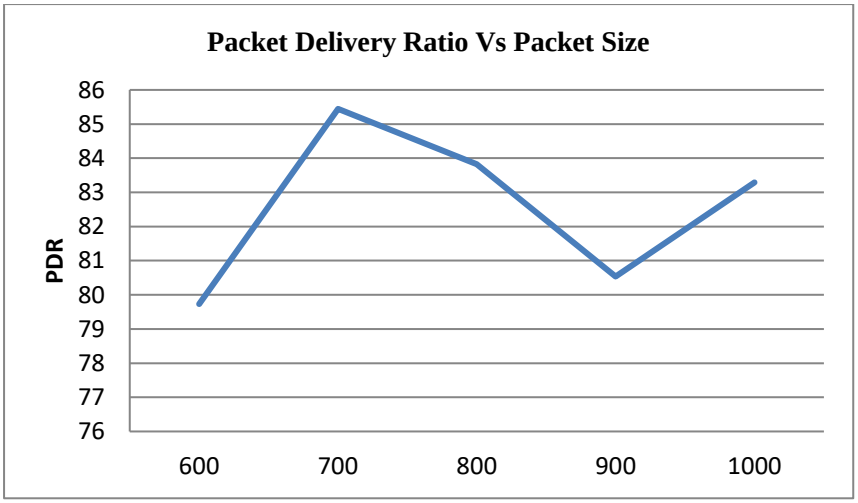

Fig:2 Graph of packet delivery ratio Vs Packet Size

Fig :2 shows graph of Packet delivery ratio Vs Packet Size .The packet delivery ratio exhibits a positive trend with increasing packet size in the protocol, showcasing its ability to handle larger data payloads efficiently. At a packet size of 600, the delivery ratio stands at a commendable 79.73%, indicating reliable transmission even with smaller data packets. As the packet size increases to 1000, the delivery ratio further improves to 83.29%, demonstrating the protocol's scalability and robustness in handling larger volumes of data.

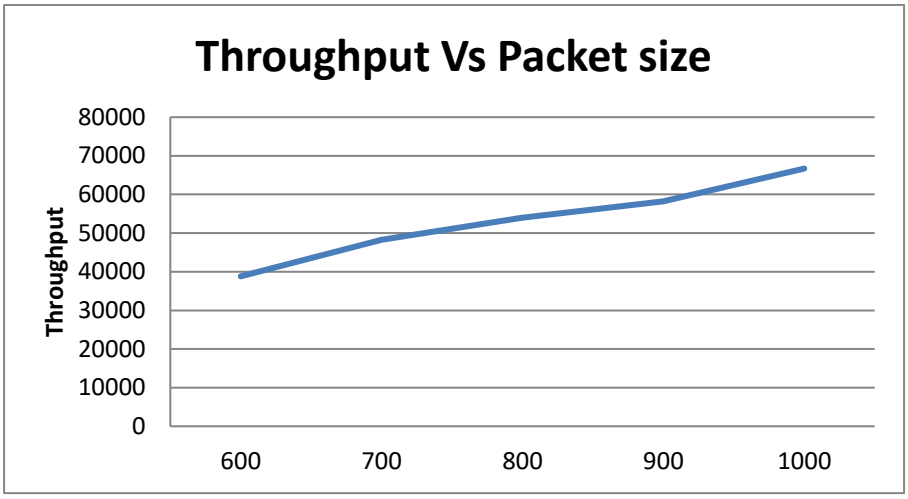

Fig:3 Graph of Throughput Vs Packet Size

Fig: 3 shows graph of Throughput ,At a packet size of 600, the throughput stands at a rate of 38,814 bytes per second, indicating efficient data transmission even with relatively smaller packet sizes. As the packet size increases to 1000, the throughput further improves to 66,704.8 bytes per second, highlighting the protocol's scalability and ability to accommodate larger data payloads. The consistent improvement in throughput with larger packet sizes indicates that the protocol effectively utilizes network resources and optimizes data transmission, contributing to enhanced overall network performance and user experience.

V. Conclusion and Future Scope: In conclusion, the BLSF protocol presents an effective approach to enhance the security of wireless sensor networks (WSNs) by implementing various security mechanisms and performance evaluation metrics. Through the implementation and analysis of secrecy performance metrics such as secrecy capacity (γR and γD), the protocol can effectively assess the level of security provided by the network and take proactive measures to mitigate potential threats from unauthorized access and eavesdropping. The protocol incorporates features such as neighbor behavior analysis, attacker detection, and dynamic adaptation to dynamically changing network conditions, thereby ensuring robust security in dynamic environments. By leveraging physical layer security (PLS) principles and cryptographic techniques, BLSF offers a comprehensive solution for securing wireless communication channels in WSNs. n the future, research in wireless sensor networks (WSNs) will focus on enhancing security with advanced cryptographic techniques and intrusion detection systems. Integration of machine learning and blockchain can further bolster security and data integrity. Additionally, optimization efforts will target efficient routing and energy harvesting for improved performance and scalability. Collaboration across academia, industry, and government will be pivotal in driving innovation and addressing emerging challenges in WSNs.

References:

1. Nguyen, B. V., Jung, H., & Kim, K. (2018). *Physical Layer Security Schemes for Full-Duplex Cooperative Systems: State of the Art and Beyond. IEEE Communications Magazine, 2–8.* doi:10.1109/mcom.2017.1700588
2. S. Atapattu, Y. Jing, Y He , Nathan Ross, J. Evans *" Physical-Layer Security in Full-Duplex Multi-Hop Multi-User Wireless Network with Relay Selection" IEEE Transactions on Wireless Communications DOI 10.1109/TWC.2018.2890609,*
3. *Andriy Stetsko, et al (2010) Neighbor-based Intrusion Detection for Wireless Sensor Networks Faculty of Informatics, Masaryk University, Brno, Czech Republic xstetsko@fi.muni.cz, xfolkman@mail.muni.cz, matyas@fi.muni.cz*
4. Y. Zou et al., *"A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," Proc. IEEE, vol. 104, no. 9, Sept. 2016, pp. 1727–65.*
5. M. Z. Win et al., *"Multi- Tier Network Secrecy in the Ether," IEEE Commun. Mag., June 2015, pp. 28–32.*
6. L. Mucchi et al., *"A New Metric for Measuring the Security of an Environment: The Secrecy Pressure," IEEE Trans. Wireless Commun., vol. 16, no. 5, May 2017, pp. 3416–30.*
7. F. Oggier and M. J. Mihaljević, *"An Information Theoretic Security Evaluation of a Class of Randomized Encryption Schemes," IEEE Trans. Inf. Forensics Security, vol. 9, no. 2, Feb. 2014, pp. 158–68.*
8. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, *"System architecture directions for networked sensors," in Proceedings of ACM ASPLOS, pp. 93–104, 2000.*
9. F. Liu, X. Cheng, and D. Chen, *"Insider attacker detection in wireless sensor networks," in Proceedings of IEEE INFOCOM, pp. 1937–1945, 2007.*
10. G. Li, J. He, and Y. Fu, *"A group-based intrusion detection scheme in wireless sensor networks," in Proceedings of GPS – Workshops, pp. 286–291, IEEE, 2008.*
11. A. Stetsko, L. Folkman, and V. Matyas, *"Neighbor-based intrusion detection for wireless sensor networks," Tech. Rep. FIMU-RS-2010-04, Faculty of Informatics, Masaryk University, May 2010.*
12. W. Xu, K. Ma, W. Trappe, and Y. Zhang, *"Jamming sensor networks: attack and defense strategies," Network, IEEE, vol. 20, no. 3, pp. 41–47, 2006.*