International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

IDS Range of Attack in WSN and Prevention Using PSO Fitness Measures

Annavaram Kiran Kumar*[1], Dr. R. Praveen Sam[2], Dr. K. Madhavi[3]

Submitted:11/03/2024 **Revised**: 26/04/2024 **Accepted**: 03/05/2024

Abstract: The concept of Euclidean space is used in sensor ad-hoc network routing techniques. This system's methodologies will derive the position of sensor nodes from previously used distances that measure static and dynamic sensor node placement. When the position of a node is known ahead of time, the number of security vulnerabilities increases. To put it another way, our strategy is to use PSO to detect security breaches and create an effective Intrusion Detection System. The simulation demonstrates the effectiveness of the DREAM protocol in thwarting an Intrusion Detection System attack aimed at duplicating sensor IDs within boundary areas. It's assumed that the sensor boundary maintains records of sensor nodes and their neighboring nodes, along with the distances between them, as dictated by the routing protocols. We assume that the sensor border maintains information about the sensor node and its neighboring nodes, along with the distances between them as dictated by the routing protocol. By employing PSO, we achieve a fitness value that tends to position the sensor node's neighbors within the border, thereby enhancing the secure zone for ad-hoc transmission.

Keywords: *IDS, DREAM protocol, PSO, IDS range.*

1. Introduction

The performance of the Sensor Adhoc network is harmed by including inactive sensor nodes. Consequently, an algorithm for scalability and deployability is implemented to monitor active and dormant sensor nodes within the routing table. This table serves as the basis for routing and forwarding data packets. The routine table shows active and inactive sensor node transactions, resulting in a highly adaptable and powerful network. A stabilize transaction and network setup is achieved by storing routing and forwarding data packets in parallel.

The major goal is to provide a secure routing protocol based on the Distance routing effect algorithm for mobility (DREAM) [11] (Stefano Basagni et al, 1998), in which each node uses the Link state algorithm to distribute data across intermediate nodes.

The static or dynamic nodal position serves as the foundation for focused secured nodes. GPS (S. Capkun et al, 2001) refreshes the routing information for a dynamic node within the routing table, subsequently updating the network (Chris Karlof et al, 2003). A change in one nodal update has an effect on all of the nodes that are connected to it. In this research, the alternative scenarios are depicted.

Table 1 illustrates a comparison between routing tables and their associated supporting tables. The outcomes presented in this table portray the worst-case scenarios encountered when employing different routing protocols.

PROTOCOL	RELEVANT ATTACKS
Tiny OS beaconing	False routing, sinkholes, intrusion detection systems (IDS), selective forwarding, wormholes, and HELLO floods.
Direct diffusion	False routing, sinkholes, intrusion detection systems (IDS), selective forwarding, wormholes, and HELLO floods.
Geographical routing	falsy routing, Sink Holes, IDS, , Selective Forwarding
Minimum cost forwarding	Falsy routing, Sink Holes, IDS, , Selective Forwarding wormholes, HELLO Floods
Cluster based protocol	Selective forwarding, HELLO Floods
Rumor routing	Falsy routing, Sink Holes, IDS, , Selective Forwarding, wormholes
Energy conserving topology , Maintenance	Falsy routing, IDS, HELLO Floods

Table 1. Basic attack models in proactive protocol

2. Work Outline

SSH and SSL are higher-layer protocols for sharing

[1] *Research Scholar, Dept Of CSE, JNTUA, Anantapur-515001.*
ORCID ID: 0009-0003-0698-1110
[2] *Professor And Head, Department Of CSE(AI&ML), G Pulla Reddy Engineering College (Autonomous), Kurnool – 518007.*
ORCID ID: 0000-0002-9685-1381
[3] *Professor, Dept. Of CSE, JNTUCEA, Anantapur-515002*
ORCID ID: 0000-0001-5147-1388
* *Corresponding Author Email: kiran.annavaram@gmail.com*

information, with security concerns addressed at the Link layer. Protocol use provides nodal connections but not security. In the realm of ad hoc networks, the integration of GPS, alongside the implementation of security measures utilizing PSO [10] and DREAM, is aimed at enhancing security. However, despite these efforts, the emergence of an IDS attack poses a challenge.. Our work organizations prioritize the following: (1) Addressing IDS attacks, (2) Implementing the DREAM Protocol, and (3) Utilizing PSO to mitigate attacks by adjusting fitness values, as per the literature. (L. Zhou et al, 1999) (F. Stefano et al, 1999) lists the security issues that exist in ad-hoc networks (S. Basagni et al, 2001), but it does not discuss defence strategies for device networks (S. Basagni et al, 2001).

Our research centers on the IDS attack [4] [5] and its countermeasures. These countermeasures involve the utilization of PSO (James Kennedy et al, 1995) and DREAM to identify secure neighboring nodes, considering a delay measure crucial in preventing the IDS [6] attack.

Won-Ik Kim et al research focuses on the stable and caution zones of sensor nodes [1], as depicted in Figure 1.

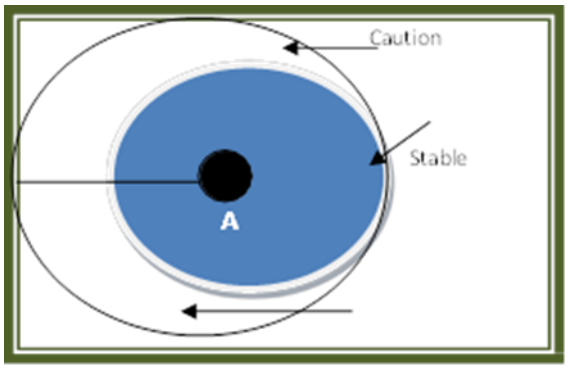

Fig. 1. Secure transmission range

The AODV avoids permanent routes by updating the routing database in real time. Packet control through flooding was managed by employing RREQ and RREP for establishing node transmission. However, the IDS attack involved creating a virtual node to orchestrate delays. The biggest amount of delay results in the greatest amount of security breach. Figure 2 depicts the proactive and reactive mechanisms implemented by DREAM. Message overhead interacts with distance effects and mobility rates, leading to flooding. DREAM resolves the problem of trajectory-based forwarding evaluation, thus eliminating the need for periodic routing table updates (TBF) (Niculescu et al., 2002).

3. Security Procedures

The AODV idea asks its route based on a time call, which prevents the sensor node from permanently storing its path. The RREQ and RREP built-in concepts were used to deploy node transmission, which started the flooding process until the control packets arrived at their destination. Because AODV uses reactive transmission and the greatest latency allows for greater security concerns, there are more security breaches. Within the wait, the IDS attack [7] builds fictitious node position co-ordinates.

Figure 2 shows node distance utilising the DREAM technique, and we believe that this strategy will function in both proactive and reactive mechanisms. The DREAM protocol is based on the distance effect (the longer the distance, the slower the transmission) and mobility rate (using the Local Positioning System (LPS)). If you use the DREAM

protocol, you can skip the periodic updates to the routing table.

Transmission between nodes utilizing DREAM focuses on Trajectory based forwarding review (TBF) to keep the choice factor in mind before sending data.

The IDS attack, which generates several co- ordinates for an instant sensor node[9], is one such assault that we've been focusing on in our research. This is due to the time it takes for a sensor node to transmit data to the farthest sensor node. The setting for our method is depicted in Figure 3.

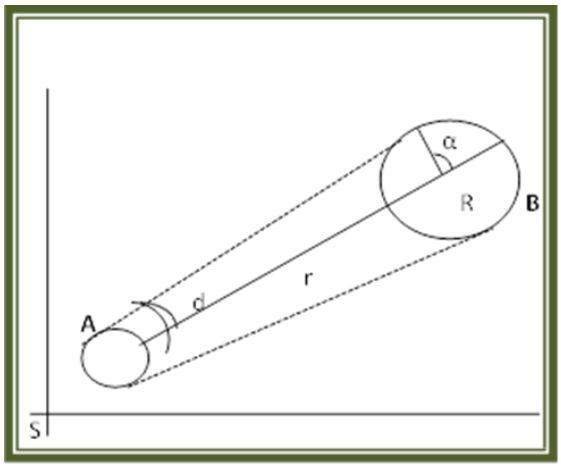

Fig. 2. Measure the distance between Node A and

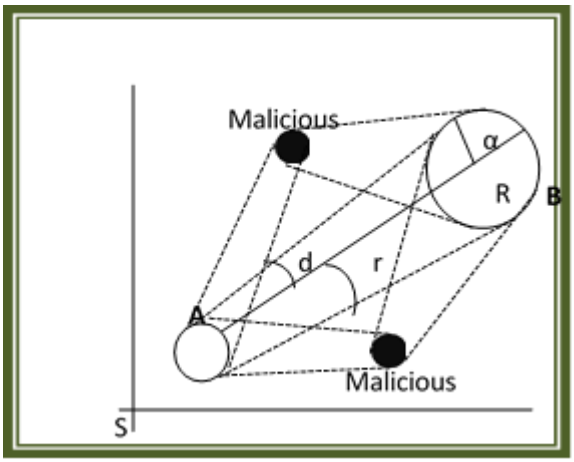

Fig. 3. IDS attack in sensor environment

The attack, which generates several co- ordinates for an

instant sensor node [2], is one such attack on which we have concentrated our efforts. This is due to the time it takes for a sensor node to transmit to the farthest sensor node. Our technique is depicted in Figure 3.

Along with LPS, PSO optimizes sensor nodes based on their location. This ensures that the co-ordinates of sensor nodes are always in the same place. As a consequence of the attack's influence, multiple coordinates of sensor nodes are generated based on the sensor delay. Duplicate sensor coordinates arise from the maximum delay.

The boundary is defined by the registration of sensor nodes.

$$B_{i,n} = \sum_{1=0}^{n} x^i b^{xy} \quad (1)$$

In this representation, B signifies the boundary set, x denotes the node, and bxy represents the movable coordinates.

The equation T^{xy} shows the trajectory formation T^{xy}.

$$T^{xy} = \sum_{1=0}^{n} x^i \; X(t) \quad (2)$$

When nodes A and B establish a connection, the trajectory set for these nodes is represented by

$$T^{AB} = \cdot \overset{n}{x}_{1=0} \quad X(t)$$

Where xA is the starting node.

Distance formulas were used to calculate the distance between two nodes (Subburaj.V et. al, 2012)

$$V_{id} = \text{w}* V_{id} + C_1 * \text{r1}(P_{id}\text{-id}) + C_1 + \text{a/r2}(\text{pgd-}X_{id}) \quad (4)$$

$$V_{id} = \begin{cases} V_{max}, & if\ V_{id} \geq V_{max} \\ -V_{max}, & if\ V_i \geq -V_{max} \end{cases} \quad (5)$$

$$X_{id} = X_{id} + V_{id} \quad (6)$$

Particle mobility is measured using equations (3) to (5).

Within the specified sensor boundary, the RREQ and RREP were used to determine the latency between nodes.

The transmission and delay were measured with the help of

$$B_{i,n} = B_{i,n-1}\ B_{i-1,n} \quad (7)$$

$$B_{i,n} = \prod_{i}^{n} B_{i-1,n}\ D_{i-1,n} \quad (8)$$

4. IDS Boundary

The boundary is represented by the variable B, while the delay distortion is represented by the variable D.

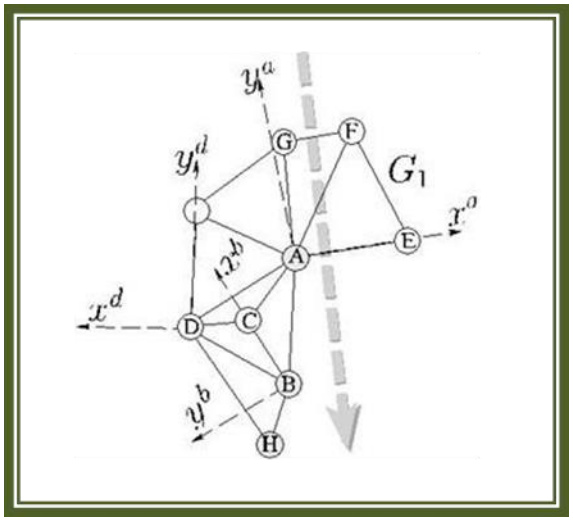

Fig. 4. LPS measures based on distance measures

$$Fitness\ (B_i) = {}^{a}/_{A} - {}^{b}/_{B} \quad (9)$$

Attack fitness to prevent duplicate co- ordinates

$$Fitness\ (B_i) = {}^{a}/_{A} \quad (10)$$

Every node's fitness value and co-ordinates are set according to the aforementioned equation. Once a node has been attacked by IDS [4], it will never be able to access any further coordinates.

Each node will undergo examination based on the following parameters:

- Transfiguration node (including its source, destination and intermediate nodes
- Boundary values
- Co-ordinate values and
- Fitness values

For sensor node authentication and IDS in every transmission, all of these values must be examined in a single stretch.

5. Results and Observations

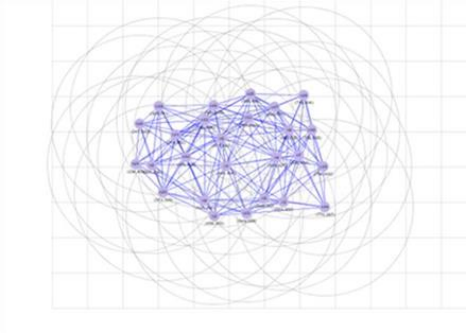

Fig. 5. NS2 mobility simulator was used to simulate a node scenario (with 25 nodes for demonstration purposes).

NS2 mobility simulator was used to simulate a node scenario (with 25 nodes for demonstration) For sensor node authentication and IDS in every transmission, all of these values must be examined in a single stretch.

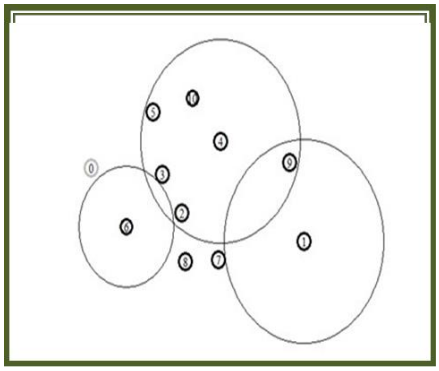

Fig. 6. Interference between nodes at various sites

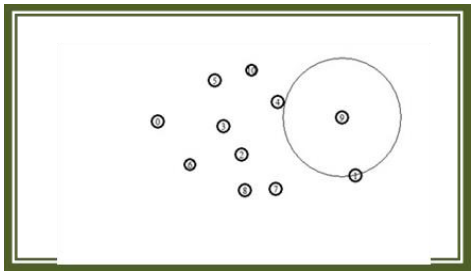

Fig. 7. Interference between nodes at various locations

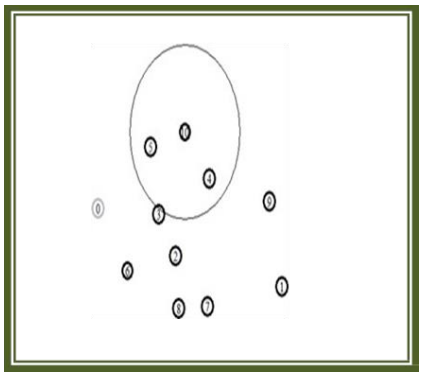

Fig. 8. Interference between nodes 5 and 6 as well as boundary setting

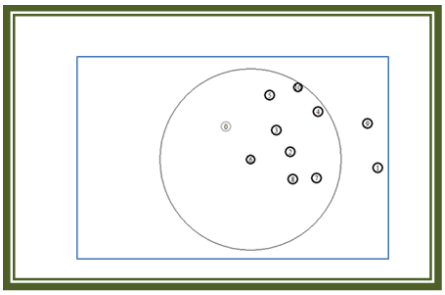

Fig. 9. Excluding nodes 9 and 1 from node interference and boundary setting

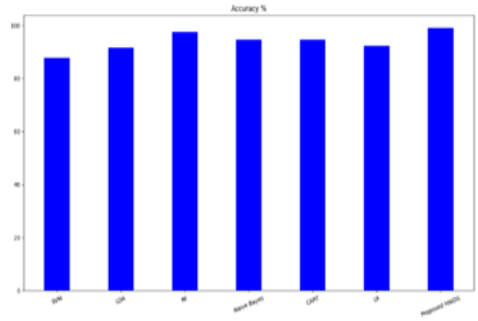

Fig. 10. The accuracy graph for the proposed HNIDS and existing ML methods for BCC, which indicates the strength of the proposed method in terms of higher accuracy %.

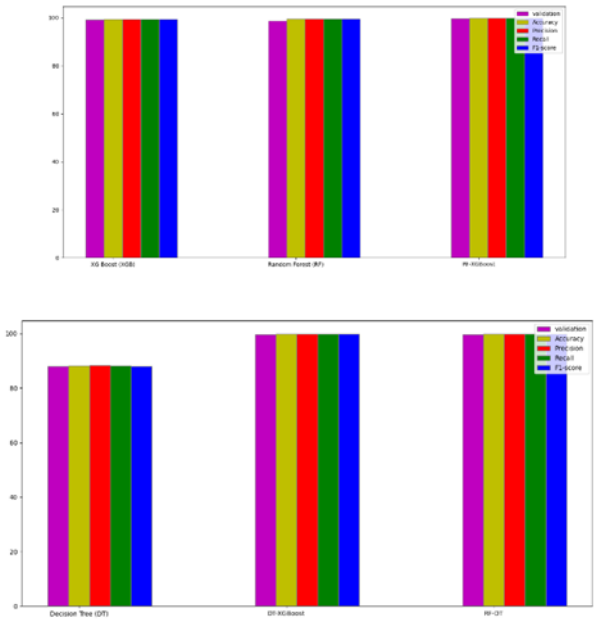

Fig. 11. Performance comparison of various machine learning models using NSL-KDD. (a) RF-based comparative analysis and (b) DT-based comparative analysis

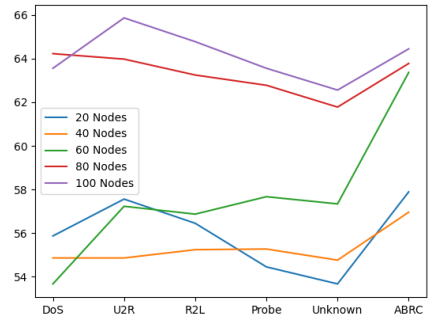

Fig. 12. Throughput comparison of varying number of nodes are presented. The performance of proposed ABRC stated that for 60 node the throughput is maximized.

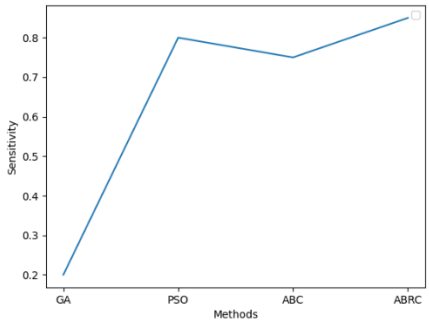

Fig. 13. Comparison of Sensitivity

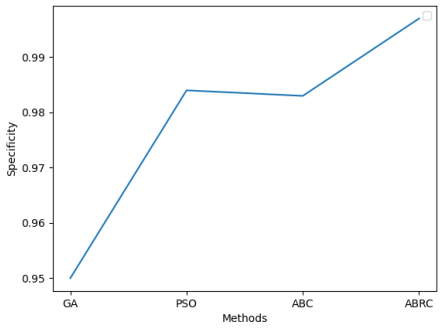

Fig. 14. Comparison of Specificity

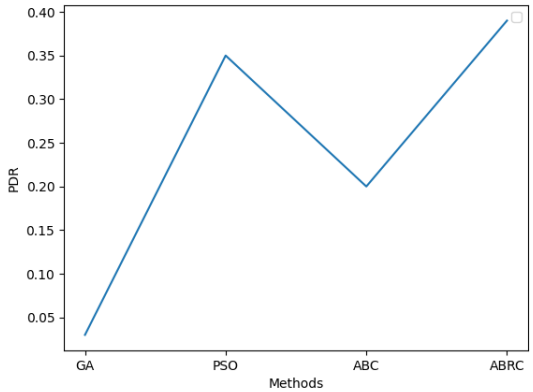

Fig. 15. Comparison of Accuracy

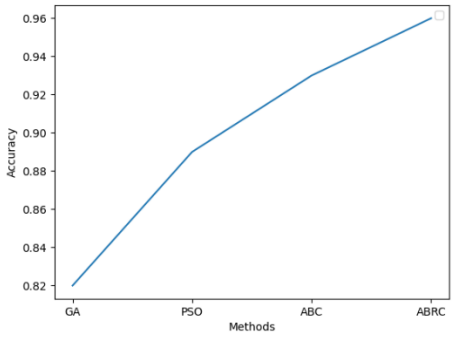

Fig. 16. Comparison of PDR

6. Findings

In this paper, an attack-fighting PSO-based optimum solution is provided. By removing repeated co-ordinate creation, the proposed fitness value of PSO reduces the impact of IDS attack [8]. Furthermore, the fitness function adjusts to a variety of environments in order to prevent attacks in the WSN environment. This work's experimental results with 500 sensor nodes showed that the attack ratio might be optimised for roughly 10 and 25 nodes. The work will be expanded to include raising the size of sensor nodes and various forms of attacks that benefit the WSN ecosystem.

References

[1] Otoum, Safa, Burak Kantarci, and Hussein T. Mouftah. "On the feasibility of deep learning in sensor network intrusion detection." IEEE Networking Letters 1.2 (2019): 68-71.

[2] Borkar, Gautam M., et al. "A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept." Sustainable Computing: Informatics and Systems 23 (2019): 120-135.

[3] Kaushik, Ila, Nikhil Sharma, and Nanhay Singh. "Intrusion detection and security system for blackhole attack." 2019 2nd International Conference on Signal Processing and Communication (ICSPC). IEEE, 2019.

[4] Sherubha, P., P. Amudhavalli, and S. P. Sasirekha. "Clone attack detection using random forest and multi objective cuckoo search classification." 2019 International Conference on Communication and Signal Processing (ICCSP). IEEE, 2019.

[5] Kfoury, Elie, et al. "A self organizing map intrusion detection system for rpl protocol attacks." International Journal of Interdisciplinary Telecommunications and Networking (IJITN) 11.1 (2019): 30-43.

[6] Mohapatra, Hitesh, et al. "Handling of man-in-the-middle attack in wsn through intrusion detection

system." International journal 8.5 (2020): 1503-1510.

[7] Dharini, N., N. Duraipandian, and Jeevaa Katiravan. "A novel IDS to detect multiple DoS attacks with network lifetime estimation based on learning-based energy prediction algorithm for hierarchical WSN." International Conference on Intelligent Computing and Applications. Springer, Singapore, 2019.

[8] Yahyaoui, Aymen, Takoua Abdellatif, and Rabah Attia. "Hierarchical anomaly based intrusion detection and localization in IoT." 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC). IEEE, 2019.

[9] Bhushan, Bharat, and G. Sahoo. "A Hybrid Secure and Energy Efficient Cluster Based Intrusion Detection system for Wireless Sensing Environment." 2019 2nd International Conference on Signal Processing and Communication (ICSPC). IEEE, 2019.

[10] Subburaj, V., K. Chitra, and S. Venkateswaran. "Secure Topology updates using PSO in MANET for Reducing Mobility Delay for Tactical Networks using TORA." i-Manager's Journal on Communication Engineering and Systems 3.2 (2014): 27.

[11] Mohseni, Shima, et al. "Comparative review study of reactive and proactive routing protocols in MANETs." 4th IEEE International Conference on Digital Ecosystems and Technologies. IEEE, 2010.