Hindawi
Security and Communication Networks
Volume 2017, Article ID 9863032, 10 pages
https://doi.org/10.1155/2017/9863032

WILEY | Hindawi

Research Article

GA-DoSLD: Genetic Algorithm Based Denial-of-Sleep Attack Detection in WSN

Mahalakshmi Gunasekaran[1] and Subathra Periakaruppan[2]

[1]*Department of Computer Science and Engineering, NPR College of Engineering and Technology, Tamil Nadu 624001, India*
[2]*Department of Information Technology, Kamaraj College of Engineering & Technology, Tamil Nadu, India*

Correspondence should be addressed to Mahalakshmi Gunasekaran; mahalakshmiit15@hotmail.com

Received 23 July 2016; Accepted 17 November 2016; Published 17 January 2017

Academic Editor: Qing Yang

Denial-of-sleep (DoSL) attack is a special category of denial-of-service attack that prevents the battery powered sensor nodes from going into the sleep mode, thus affecting the network performance. The existing schemes used for the DoSL attack detection do not provide an optimal energy conservation and key pairing operation. Hence, in this paper, an efficient Genetic Algorithm (GA) based denial-of-sleep attack detection (GA-DoSLD) algorithm is suggested for analyzing the misbehaviors of the nodes. The suggested algorithm implements a Modified-RSA (MRSA) algorithm in the base station (BS) for generating and distributing the key pair among the sensor nodes. Before sending/receiving the packets, the sensor nodes determine the optimal route using Ad Hoc On-Demand Distance Vector Routing (AODV) protocol and then ensure the trustworthiness of the relay node using the fitness calculation. The crossover and mutation operations detect and analyze the methods that the attackers use for implementing the attack. On determining an attacker node, the BS broadcasts the blocked information to all the other sensor nodes in the network. Simulation results prove that the suggested algorithm is optimal compared to the existing algorithms such as X-MAC, ZKP, and TE_2P schemes.

1. Introduction

Wireless Sensor Network (WSN) contains a collection of self-governing sensors that monitors the conditions such as sound, temperature, pressure, and vibration [1]. The sensor nodes in the WSN are energized using the batteries. But, one of the major issues of WSN is energy loss. It is caused due to the following reasons [2]:

(i) Collisions
(ii) Overhearing
(iii) Idle listening
(iv) Control packet overhead

In the collision loss, the collision of data packets in the wireless medium introduces the energy loss. In the overhearing loss, the maintenance of radios in the receiving mode during data packet transmission introduces the energy loss. The idle listening loss is created by a node's radio in just monitoring the channel. As the control packets may have to be received by all the nodes in the transmission range, the control packet overhead is introduced. Generally, the WSN is prone to two types of attacks such as invasive attack and noninvasive attack. The noninvasive attacks affect the power, frequency, and timing of the channel, whereas the invasive attacks affect the information transmission, routing process, and service availability [3]. Among the attacks of WSN, the denial-of-service attacks make the system or service inaccessible. The important properties of the DoSL attacks are

(i) malicious,
(ii) disruptive,
(iii) remote.

When the denial-of-service attack is performed intentionally, it is termed as malicious. When the DoSL attack is successful, the capability or service in WSN is affected. Thus, disrupting the affected service is not the only goal of the attacker.

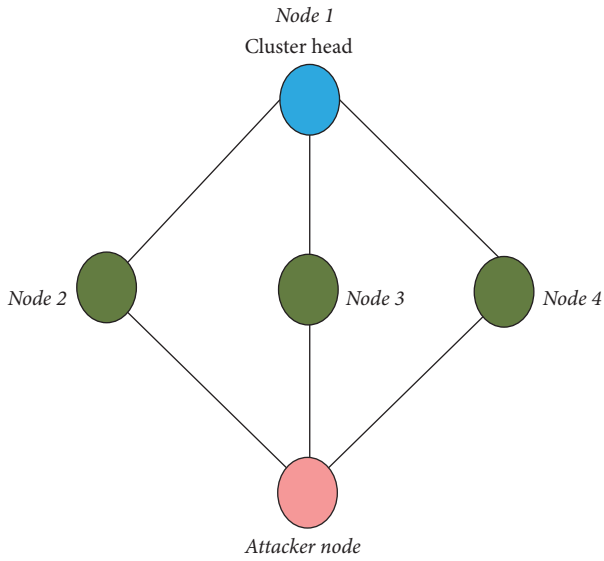

Figure 1: Denial-of-sleep attack [2].

As the physical presence of the attacker is uncomfortable for launching multiple types of DoSL attacks, the attack is performed from a remote place. One of the special categories of denial-of-service attack is DoSL attack.

An example of the DoSL attack is represented in Figure 1. In this attack, the energy consumption of the sensor nodes is increased by preventing them from sleeping. The attacker node can forward the fake data packets to the authorized nodes, thus resulting in unnecessary transmissions. On receiving the data packets, if the receiver could not identify the source, it will process the data obtained from the attacker nodes.

This makes the receiver node to be awake till the data transmission gets completed, thus exhausting the battery power of the nodes. Further, the attacker nodes can transmit a false acknowledgment and make the source node transmit all the services, thus maximizing the power consumption. The existing components used for defending the DoSL attack are as follows [2]:

(i) Strong link-layer authentication

(ii) Antireplay protection

(iii) Jamming identification

(iv) Broadcast attack protection

The strong layer authentication is a key component of the DoSL defense. On integrating this component to the WSN, the DoSL attacks can be prevented efficiently. The antireplay protection component is used for preventing the replay attacks that force the nodes to forward the old traffic information. The jamming identification component is used for preventing the jamming attack that prevents the sensor nodes from accessing the wireless medium. This component integrates the sensor nodes with the simple radios. Generally, the MAC protocols are prone to unauthenticated broadcast attacks. The broadcast attack protection technique differentiates the legitimate traffic from the malicious traffic for minimizing the energy consumption. But, the demerits of the existing DoSL defense mechanisms are nonoptimal energy conservation and lack of key pairing operations for preventing the attacker from implementing the attack. Thus, to address the issues in the existing DoSL defense schemes, an efficient GA-DoSLD algorithm is suggested.

Objectives. The key objectives of the suggested GA-DoSLD are as follows:

(i) To analyze the neighbor information for creating the population

(ii) To perform the key pairing using MRSA algorithm

(iii) To deploy the AODV protocol for determining the optimal route

(iv) To determine the behavior of the already existing attacker by estimating the fitness value

(v) To provide an alert message to the base station regarding the behavior of the neighbor node

(vi) To broadcast the blocked information to other sensor nodes in the network

The rest of the paper is organized as follows. Section 2 discusses the existing techniques used for detecting the DoSL attacks, energy draining attacks, and soft computing algorithms exploited for addressing the energy draining attacks. Section 3 provides a detailed description of the proposed GA-DoSLD algorithm. Section 4 discusses the experimental analysis of the proposed method and the study is concluded in Section 5.

2. Related Works

This section illustrates the existing techniques used for DoS attack detection, energy draining attacks, and soft computing algorithms used for addressing the energy draining attacks.

2.1. Detection of DoS Attacks in WSN. Mansouri et al. [4] proposed a clustering technique for addressing the DoS attacks. The suggested technique exploited the energy consumption of the nodes. Mansouri et al. [5] detected the compromised nodes in WSN using energy-preserving solution. The suggested algorithm detected the controlled nodes (Cnode) using a hierarchical clustering technique. Experimental results proved that the suggested technique achieved optimal energy balance, throughput, detection coverage, and delay between the packet transmissions. Chen et al. [6] proposed a time-division secret key protocol for detecting the DoS attack. The simulation results proved that the cipher function was optimal for WSN. Further, the detection jamming scheme increased the network lifetime of the WSN. He et al. [7] suggested a distributed code dissemination protocol, namely, DiCode, for detecting the DoS attacks. The demerits of the suggested protocol were nonoptimal security properties and consequences on the network availability. Han et al. [8] proposed an Intrusion Detection System based Energy Prediction (IDSEP) for the cluster-based WSN. The

suggested scheme exploited the energy consumption of the sensor nodes for detecting the malicious nodes. Further, based on the energy consumption thresholds, the categories of the DoS attacks were determined. Simulation results proved that the suggested IDSEP efficiently detected the malicious nodes. Ram Pradheep Manohar [9] proposed the Slowly Increasing and Decreasing under Constraint DoS Attack Strategy (SIDCAS) for detecting the Stealthy DoS (S-DoS) attacks in WSN. In addition to providing security, the suggested approach also decreased the resource maintenance cost. Tan et al. [10] suggested a Deluge based multihop code dissemination protocol for enhancing the confidentiality of the WSN. Experimental results proved that the suggested approach provided optimal latency, dissemination rate, and energy consumption.

2.2. Energy Draining Attacks. Nam and Cho [11] suggested a Statistical En-Route Filtering (SEF) scheme for detecting the false reports in the intermediate nodes. Further, the false report injection attack was defended using three types of keys such as individual key, pairwise key, and cluster key. The comparison of SEF with the suggested method proved that the proposed method enhanced the energy savings than the SEF in sensor networks. Manju et al. [1] suggested three steps such as network organization, malicious node detection, and selective authentication for detecting the denial-of-sleep attack in WSN. Experimental results proved that the suggested method was optimal for defending the attacker from performing the task. Naik and Shekokar [12] addressed the denial-of-sleep attack using zero knowledge protocol and interlock protocol. Experimental results proved that the suggested protocols prevented the replay attack and man-in-the-middle attack and also minimized the resource consumption. Hsueh et al. [13] suggested a cross-layer design of secure scheme with MAC protocol for minimizing the energy consumption of the sensor nodes. Analysis results proved that the suggested protocol efficiently defended the replay attacks and forge attacks. Further, the security requirements and energy conservation were coordinated. Kaur and Ataullah [14] suggested a hierarchical clustering based isolation of nodes for addressing the denial-of-sleep attack. The suggested approach enhanced the network lifetime, but the idle listening problem was unaddressed. Hsueh et al. [13] proposed a cross-layer design of secure scheme integrated with MAC protocol for defending against the replay attack and forge attack. Experimental results proved that the suggested protocol coordinated the energy conservation and security requirements.

2.3. Soft Computing Algorithms Used for Addressing the Energy Draining Attack. Shamshirband et al. [15] proposed a Density-Based Fuzzy Imperialist Competitive Clustering Algorithm (D-FICCA) for detecting the intruders in WSN. When compared to the existing algorithms, the proposed algorithm produced 87% detection accuracy and 0.99 clustering quality. Shamshirband et al. [16] suggested a cooperative Game-Based Fuzzy Q-Learning (G-FQL) approach for detecting the intrusions in the WSN. The suggested model deployed the cooperative defense counterattack scenario for the sink node and game theory strategy for the base station nodes. When compared to the Low Energy Adaptive Clustering Hierarchy (LEACH), the suggested model produced optimal detection accuracy, counterdefense, energy consumption, and network lifetime. Further, when compared to the existing machine learning methods, the suggested model provided enhanced detection and defense accuracy. Sreelaja and Vijayalakshmi Pai [17] suggested an Ant Colony Optimization Attack Detection (ACO-AD) algorithm for detecting the sinkhole attacks in WSN. The keys were distributed among the alerted nodes using Ant Colony Optimization Boolean Expression Evolver Sign Generation (ABXES) algorithm. Experimental results proved that when compared to the existing LIDeA architecture, the suggested architecture minimized the false positives and also minimized the storage in the sensor nodes. Keerthana and Padmavathi [18] suggested an Enhanced Particle Swarm Optimization (EPSO) technique for detecting the sinkhole attacks in WSN. When compared to the existing ACO and PSO algorithms, the suggested algorithm provided optimal packet delivery ratio, message drop, average delay, and false alarm rate. Saeed et al. [19] suggested a Random Neural Network based IDS for detecting the attackers. Experimental results proved that the suggested IDS provided higher accuracy and reduced performance overhead.

From the analysis of the existing techniques, it is clear that they do not address the idle listening problem. Further, the solutions suggested for preventing the DoSL attacks are unrealistic. Thus, to address the issues in the existing techniques, an efficient GA-DoSLD algorithm is proposed.

3. Proposed Method

This section describes the proposed GA-DoSLD algorithm for analyzing the misbehaviors of the sensor nodes in WSN. The overall flow of the suggested algorithm is represented in Figure 2.

From the figure, it is clear that the key steps involved in the suggested algorithm are as follows:

(i) WSN initialization
(ii) Population generation
(iii) Generation and distribution of key pair
(iv) Route discovery
(v) Behavior monitoring

A detailed description of every step is provided in the following sections.

3.1. WSN Initialization. The initial step involved in the suggested approach is WSN initialization. By exploiting the NS2 tool, the WSN is initialized with 100 numbers of sensor nodes that have random waypoint mobility model. The transmission range of the WSN is 250 meters. Further, the initialized WSN poses the specifications listed in Table 1.

3.2. Population Generation and BS Configuration. Once the WSN environment is initialized, the suggested GA-DoSLD

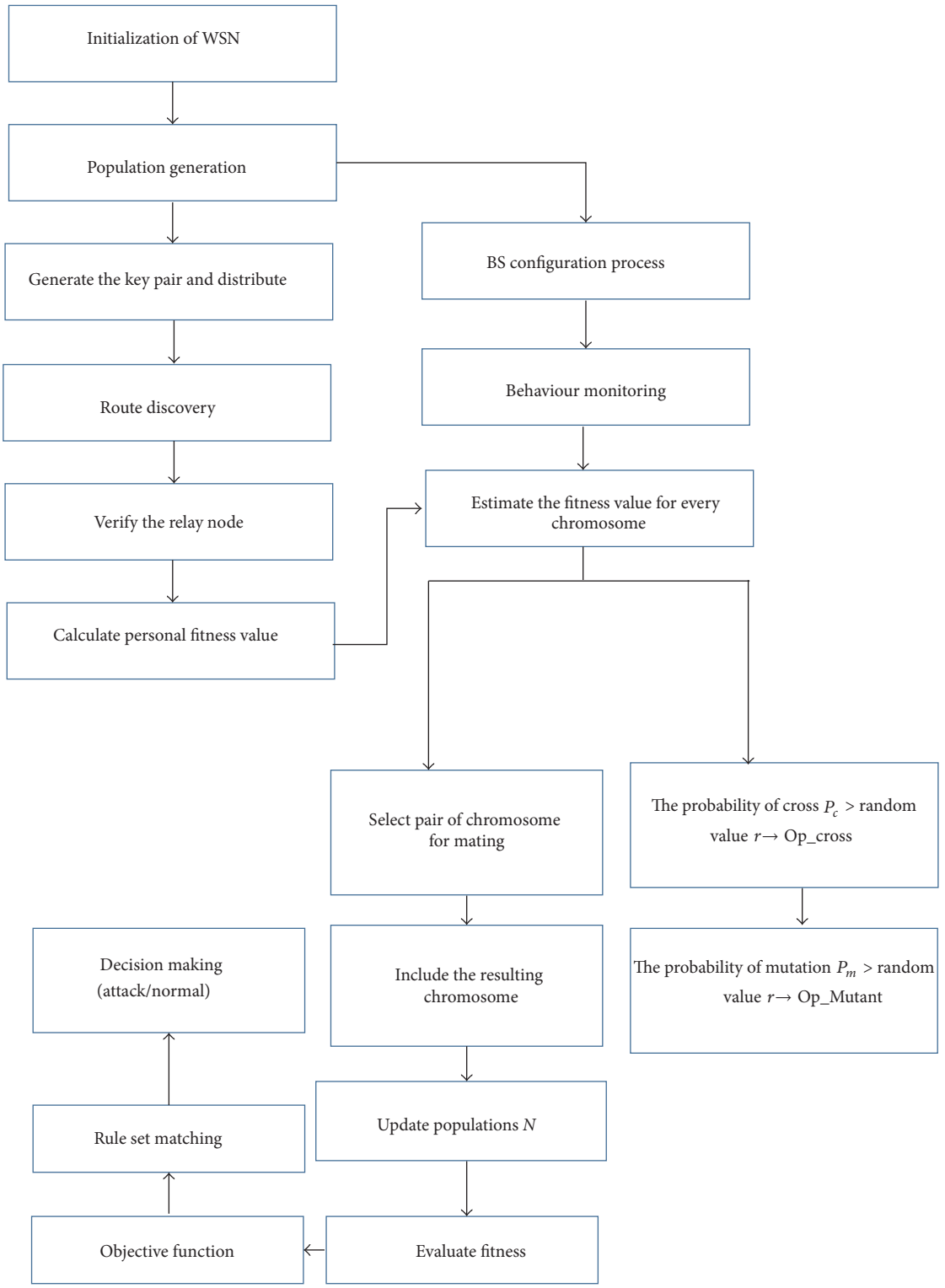

Figure 2: Overall flow of the proposed GA-DoSLD algorithm.

Table 1: System specifications.

Simulation parameters	Values
Packet size	1024 Kbps
Packet rate	Random packets/sec
Routing protocol	AODV
Channel bit rate	10 MB/s
Initial power	25 J
Sensor node sensing power	5×10^{-8} J
Transmission range	150–250 meters
Duty cycle	20-time slots

algorithm generates the population using population generation algorithm. The suggested algorithm initially loads the two-hop neighbor information to the base station; then for every member in the neighbor list, the next-of-neighbor is initialized as the population. The steps involved in the suggested algorithm are illustrated as follows.

Algorithm 1 (population generation algorithm).

Step 1. Load the two-hop neighbor information with the base station.

Step 2

```
for (member in the neighbor list)
    {
        Population ← Load_Individual (new
        neighbor (next-of-neighbor))
    }
```

During the implementation of the population generation algorithm, the BS configuration process is performed in parallel for analyzing the behavior of the nodes in the WSN.

3.3. Generation and Distribution of Key Pair. After the generation of the population, the BS deploys the MRSA algorithm for generating a public key and private key pair. Among the keys, the public key is used for the BS and the private key is used for the sensor nodes. The main objective of this step is to prevent the attacker from implementing the DoSL attack. By deploying this step, the attacker node is blocked at the initial level before sending or receiving the packet, thus saving the energy of the sensor nodes. The steps involved in the suggested algorithm are illustrated as follows [20].

Algorithm 2 (MRSA algorithm).

Step 1. Choose the large prime numbers "n" and "r."

Step 2. Compute the modulus totient using

$$\Phi(a) = (n-1) * (r-1). \quad (1)$$

Step 3. Choose the public exponent "i" such that $1 < i < \Phi(n)$ and $\mathrm{GCD}(i, \Phi(a)) = 1$.

Step 4. Estimate the private exponent "m" such that $m = i^{-1} \bmod \Phi(a)$.

Step 5. Estimate the private key as (m, a).

Step 6. Estimate the public key as (i, a).

The suggested MRSA algorithm has a key size of 512 bits. Among the total number of bits, 256 bits are used as the public key in the base station and the remaining 256 bits are used as the private key in the sensor nodes. The minimal key size provides the following advantages:

(i) Minimal computational complexity

(ii) Achieving memory optimization

3.4. Route Discovery and Relay Node Validation. Before initiating the packet transmission, the sensor nodes determine the optimal route using Ad Hoc On-Demand Distance Vector (AODV) routing protocol. An example of the route discovery process is represented in Figure 3. The suggested protocol has two key operations such as route discovery and route maintenance. When the source node demands a route to the destination node or when the lifetime of the existing route to the destination node has expired, the route discovery operation is initiated with the broadcast of the RREQ messages. On receiving the RREQ messages, the intermediate nodes provide an optimal route to the destination node. When the intermediate node is the destination node, the RREP packets are directly transferred to the source node.

The steps involved in the suggested AODV based route discovery are described as follows.

Algorithm 3 (AODV routing protocol).

Step 1. When a sensor node seeks a route, the RREQ packet is propagated through the entire network till the packet reaches the destination node.

Step 2. When the source node and destination nodes are placed at the corners of the network, the RREQ packets have to travel a maximum number of hops.

Step 3. On receiving the RREQ packets, the relay nodes broadcast it ahead till it reaches the destination.

Step 4. The overhead created due to the route request process is represented as follows:

$$R_{\mathrm{RREQ}} = \sum_{a-1}^{N} (H)\, E^{N-1} \sum_{b=2}^{H} \left[(a-1-b) - \sum_{c=1}^{N-1} R_c \right] PC_b. \quad (2)$$

Step 5. Once the RREQ packet reaches the destination node, it replies back to the source node as RREP packet through the same sequence for reaching the source node.

Step 6. According to [21], the overhead created for the RREP packets is represented as follows:

$$R_{\mathrm{RREP}} = N + \frac{N}{2} (a-h-2)\, p. \quad (3)$$

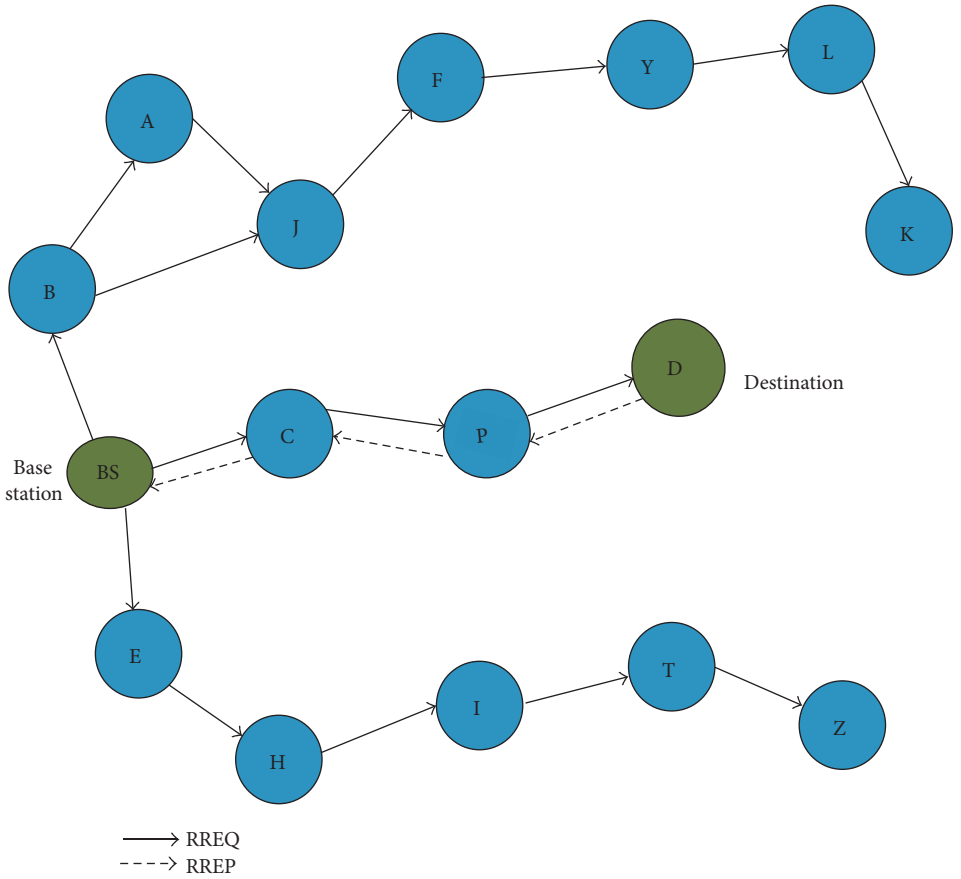

Figure 3: Example for the route discovery process using AODV.

Step 7. The overall overhead introduced for the route discovery process is

$$R_{\text{Overall}} = \text{RREQ} + \text{RREP},$$

$$R_{\text{Overall}} = \sum_{a-1}^{N} (H)\, E^{N-1} \sum_{b=2}^{H} \left[(a - 1 - b) - \sum_{c=1}^{N-1} R_c \right] PC_b + N + \frac{N}{2} (a - h - 2)\, p. \quad (4)$$

The merits of using the AODV routing protocol for the route discovery process are as follows:

(i) Loop-free routes

(ii) Faster response to link breakage

(iii) Minimal demand for the broadcast

After establishing an optimal route, the sensor nodes estimate the trustworthiness of the neighbor nodes using fitness evaluation function.

3.5. Behavior Monitoring. After ensuring the trustworthiness of the neighbor nodes, the sensor nodes forward the packets. During the transmission, if the sensor node suspects any malicious behaviors as follows, it estimates the fitness value based on the information provided by the BS:

(i) Flooding of data packets

(ii) Transmission of large sized data packets that exceed the data capacity of the sensor nodes

By estimating the fitness value based on attacker ID, the chromosome of the already existing attacker is determined. After estimating the fitness value, the sensor nodes provide alert messages about the neighbor node behavior to the BS. On receiving the alert message, the BS performs the crossover and mutation operations on the chromosomes for identifying and analyzing the method that is used by the attacker for implementing the attack. The resultant chromosomes obtained from the crossover and mutation operation are added to the existing population. Finally, the BS confirms whether the particular neighbor node is a normal node or an attacker node. If the BS determines the neighbor node as an attacker node, then the BS broadcasts the blocked information to all the other sensor nodes in the WSN. By exploiting the suggested GA-DoSLD algorithm, the attacker nodes that introduce the DoSL attacks are eliminated from the communication, thus saving the energy of the sensor nodes. Notations describe the symbols used in Algorithm 4

for the proposed GA-DoSLD. The steps involved in the suggested GA-DoSLD algorithm are illustrated below.

Algorithm 4 (GA-DoSLD algorithm).

Input. Population.

Output. Optimal population with fitness value.

Step 1. Compute the index of individuals:

Individual ← Random member (population)
Initialize the array of fittest as empty
For (node in population)
{
If (Fittest.getFitness() = getIndividual(node).getFitness())
{

$$\text{Fittest} = \text{getIndividual}(\text{node}); \quad (5)$$

}
}
Individuals [index] = Fittest;

Step 2. Compute fitness function:

Load member, population
Compute the weight accuracy (W_{ac}) and relative accuracy (R_{ac})
Compute the occurrences of weight (W_{oc}) and relative weight (R_{oc})

$$\text{Fitness} = W_{ac} * \text{accuracy of } m \text{ hop} + W_{oc} * \text{occurrence of } m \text{ hop}, \quad (6)$$
$$\text{Fitness} = (W_1 + W_2) * \text{af} + (-W_2) * R_{oc}.$$

Step 3. Execute reproduction:

Initialize the new_pop as an empty set
//select the random member in the input population based on fitness function
For ($i = 1$; $i \leq$ maximum size of population; $i + +$)
{
$X \leftarrow$ Random selected member in population based on fitness function
$Y \leftarrow$ Random selected member in population based on fitness function
Find the parent profiles of (X, Y)
Len. $X \leftarrow$ length (X)
Len. $Y \leftarrow$ length (Y)
c = Select random number between 1 and Len. X

$$\text{new\_chromosome} = (\text{substring}(X, 1, c), \ \text{substring}(Y, 1, c)) \quad (7)$$

Set offspring as new_chromosome

Step 4. Population Update:

If (random probability to mutate ≥ threshold)

$$\text{off spring} \longleftarrow \text{Mutates}(\text{off spring}) \quad (8)$$
$$\text{Set new population} \longleftarrow \text{Union}(\text{new population}, \{\text{offspring}\})$$

End do
Population ← Union (new population, new_pop)
Return Best (Population, Fitness)

4. Performance Analysis

This section describes the performance results of the proposed GA-DoSLD algorithm for the following metrics:

(i) Normalized energy consumption
(ii) Effective packet number
(iii) End-to-end delay
(iv) Average energy consumption
(v) Packet delivery ratio
(vi) Throughput ratio versus packet rate

To prove the superiority of the proposed GA-DoSLD algorithm, it is compared with the existing algorithms such as zero knowledge protocol (ZKP) [22], X-MAC, and Two-Tier Energy-Efficient Secure (TE_2S) scheme [23] and their results are discussed in the following sections.

4.1. Normalized Energy Consumption. Normalized energy consumption is the amount of energy consumed for transferring 3 packets per second. The normalized energy consumption of the existing X-MAC algorithm, ZKP, TE_2P scheme, and the proposed GA-DoSLD algorithm is validated for multiple intervals of attack. The comparison result represented in Figure 4 depicts that, for all the attack intervals, the suggested GA-DoSLD algorithm consumes minimal energy.

4.2. Effective Packet Number. The effective packet number of the existing X-MAC algorithm, ZKP, TE_2S scheme, and the proposed GA-DoSLD algorithm is validated for the variable attack intervals. The comparison considers the packet sending rate as 1 packet every 3 seconds. The comparison result represented in Figure 5 shows that the suggested GA-DoSLD algorithm provides higher scores on effective packet number than the existing schemes.

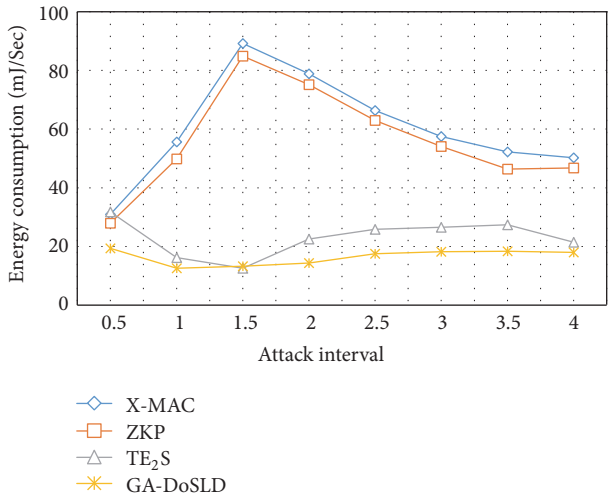

Figure 4: Comparison of normalized energy consumption for the existing and the proposed methods.

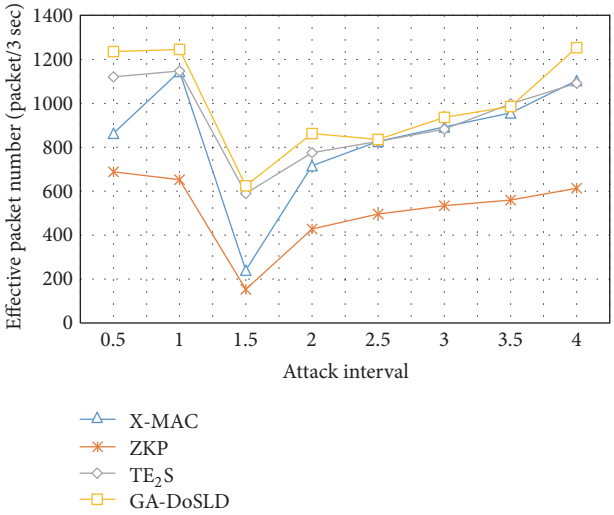

Figure 5: Comparison of packet number versus attack interval.

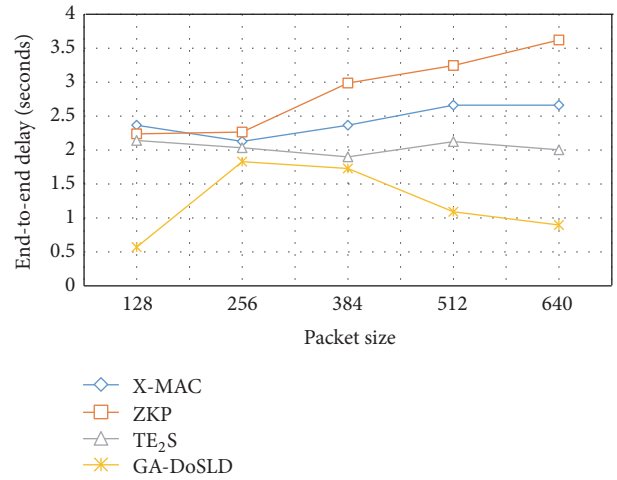

Figure 6: Comparison of end-to-end delay versus packet size for the existing and the proposed methods.

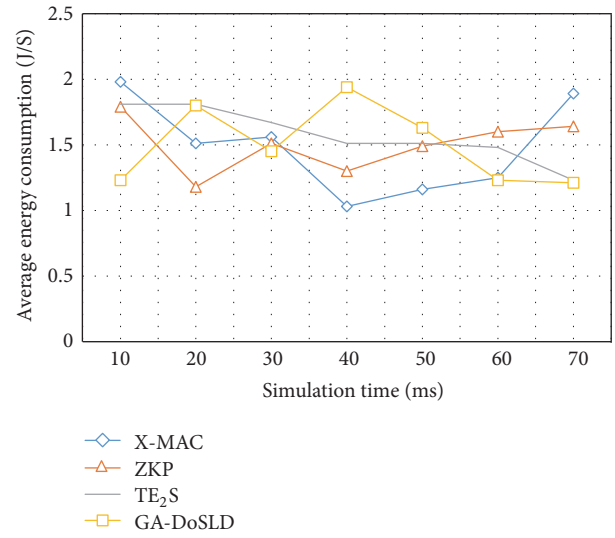

Figure 7: Analysis of average energy consumption versus simulation time for the existing and the proposed methods.

4.3. End-to-End Delay. The end-to-end delay is defined as the average time consumed for transmitting the packets. The analysis of end-to-end delay with respect to the packet size is represented in Figure 6. From the figure, it is clear that, when compared to existing X-MAC, ZKP, and TE_2S algorithms, the suggested GA-DoSLD algorithm provides a minimal end-to-end delay for the variable packet sizes.

4.4. Average Energy Consumption. The average energy consumption is the amount of energy consumed by the algorithms for transmitting the data packets. The comparison of average energy consumption for the existing X-MAC, ZKP, TE_2S schemes, and the proposed GA-DoSLD algorithm is represented in Figure 7. From the figure, it is clear that the suggested GA-DoSLD algorithm provides minimal energy consumption than the existing schemes.

4.5. Packet Delivery Ratio. The packet delivery ratio (PDR) is defined as the ratio of the number of data packets successfully delivered to the destination node to the number of data packets transmitted from the source. The estimation of the PDR is based on the following equation:

$$\text{PDR} = \frac{P_R * 100}{\sum_{a-1}^{n} P_{\text{Gen}_a}}, \tag{9}$$

where P_R represents the number of data packets received at the destination node, P_{Gen} is the total number of data packets generated by the source nodes, and n denotes the number of sensor nodes. The comparison of PDR with respect to the simulation time is represented in Figure 8.

From the figure, it is analyzed that, when compared to the existing X-MAC, ZKP, and TE_2S schemes, the proposed GA-DoSLD algorithm provides higher PDR.

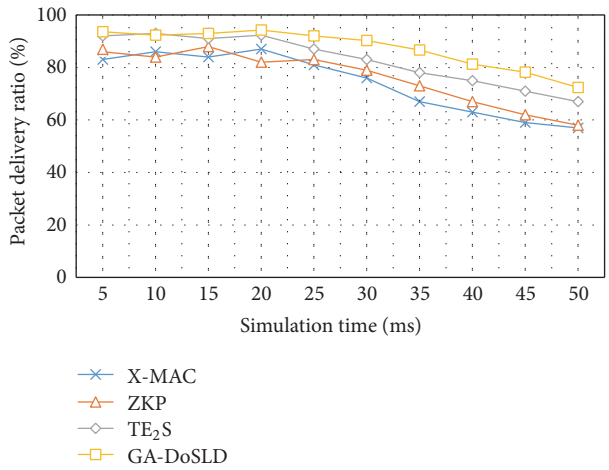

Figure 8: Comparison of packet delivery ratio versus simulation time for the existing and proposed schemes.

4.6. Throughput Performance for Various Packet Sending Rates. The effectiveness of the protocol depends on the successful reception and transmission of data packets under the various sending rates such as 1 packet/3 seconds, 1 packet/5 seconds, and 1 packet/7 seconds [22]. In this paper, the packet sending rate of 1 packet/3 seconds is taken to validate the performance of proposed work. The estimation of the throughput ratio is based on the following equation:

$$\text{Throughput ratio} = \frac{P_{\text{NS}}}{P_{\text{NT}}}, \tag{10}$$

where P_{NS} denotes the packet number under simulation scenario and P_{NT} represents the packet number delivered under the theoretical scenario. The superiority of the suggested GA-DoSLD algorithm is validated against the existing algorithms such as X-MAC, ZKP, and TE_2P for a packer rate of 1 packet per 3 seconds. Figure 9 represents the comparison of the throughput ratio with respect to the variable attack interval.

From the figure, it is clear that the suggested GA-DoSLD algorithm provides higher throughput than the existing algorithms under the packet sending rate of 1 packet/3 seconds.

5. Conclusion and Future Work

In this paper, an efficient GA-DoSLD algorithm is proposed for generating the DoSL attack profiles from multiple sensor nodes such that the attacker nodes can be prevented from the communication process. Initially, a WSN is simulated with 100 numbers of static sensor nodes; then the BS performs the operations such as key pair generation and behavior monitoring in parallel. The base station monitors the behavior of the sensor nodes and initializes every behavior as a chromosome. The MRSA algorithm is implemented in the base station for generating and distributing the key pair among the sensor nodes. Before initiating the communication between the sensor nodes, the AODV routing protocol estimates the optimal route. To validate the trustworthiness of the relay nodes in the route, the fitness value is estimated for every

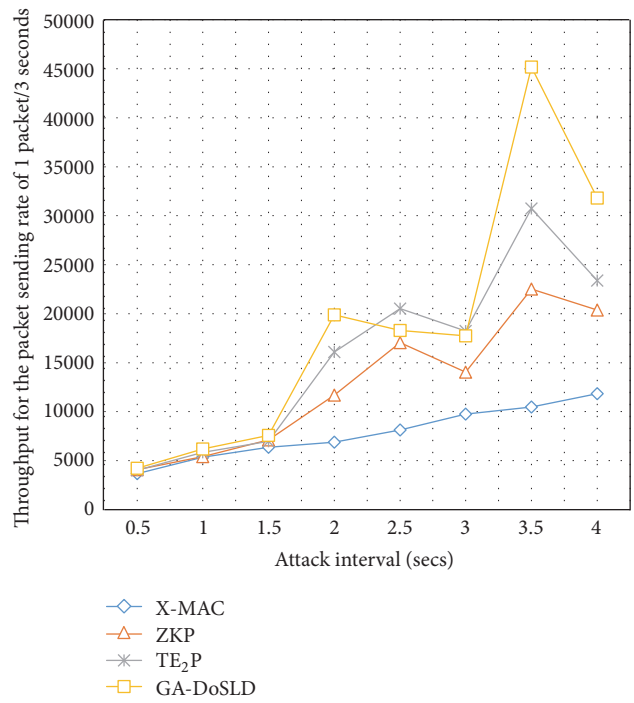

Figure 9: Comparison of throughput under packet sending rate of 1 packet/3 seconds versus attack interval.

chromosome. If the chromosome is determined as unusual, it is validated against the existing attack profiles. If there does not exist a match, the pair of chromosomes is subjected to the crossover and mutation operations. The resultant chromosomes are added to the existing chromosomes. Finally, the BS determines the attacker nodes broadcasting the blocked information to all the sensor nodes in the network. To prove the superiority of the suggested GA-DoSLD algorithm, it is compared against the existing X-MAC, ZKP, and TE_2S schemes for the metrics such as normalized energy consumption, effective packet number, end-to-end delay, average energy consumption, packet delivery ratio, and throughput ratio versus packet rate. The validation results prove that, when compared to the existing schemes, the proposed algorithm provides optimal results for all the metrics. The repeated execution of the GA-DoSLD algorithm in the sensor nodes consumes a considerable amount of energy. Thus, to achieve the energy optimization, a different soft computing algorithm other than GA can be used in future for detecting the denial-of-sleep attack in the WSN environment.

Notations

N: Expected number of hops
H: Number of hops between the source and destination
E: Number of neighbors at the higher tiers
R_c: Expected number of neighbors at cth hop
C_b: Additional coverage index of the node with b neighbors
W_{ac}: Weight accuracy

R_{ac}: Accuracy relative
W_{oc}: Occurrence
R_{oc}: Relative weight of occurrence.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] V. C. Manju, S. L. Senthil Lekha, and M. Sasi Kumar, "Mechanisms for detecting and preventing denial of sleep attacks on wireless sensor networks," in *Proceedings of the IEEE Conference on Information and Communication Technologies (ICT '13)*, pp. 74–77, Tamil Nadu, India, April 2013.

[2] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 1, pp. 367–380, 2009.

[3] R. P. Manohar and E. Baburaj, "Detection of Stealthy Denial of Service (S-DoS) attacks in wireless sensor networks," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 14, pp. 343–348, 2016.

[4] D. Mansouri, L. Mokddad, J. Ben-Othman, and M. Ioualalen, "Preventing denial of service attacks in wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '15)*, pp. 3014–3019, London, UK, June 2015.

[5] D. Mansouri, L. Mokdad, J. Ben-Othman, and M. Ioualalen, "Detecting DoS attacks in WSN based on clustering technique," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '13)*, pp. 2214–2219, Shanghai, China, April 2013.

[6] J.-L. Chen, Y.-W. Ma, X. Wang, Y.-M. Huang, and Y.-F. Lai, "Time-division secret key protocol for wireless sensor networking," *Institution of Engineering and Technology Communications*, vol. 5, no. 12, pp. 1720–1726, 2011.

[7] D. He, C. Chen, S. Chan, and J. Bu, "DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 5, pp. 1946–1956, 2012.

[8] G. Han, J. Jiang, W. Shen, L. Shu, and J. Rodrigues, "IDSEP: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks," *IET Information Security*, vol. 7, no. 2, pp. 97–105, 2013.

[9] E. B. Ram Pradheep Manohar, "Detection of stealthy denial of service (S-DoS) attacks in wireless sensor networks," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 14, 2016.

[10] H. Tan, D. Ostry, J. Zic, and S. Jha, "A confidential and DoS-resistant multi-hop code dissemination protocol for wireless sensor networks," *Computers & Security*, vol. 32, pp. 36–55, 2013.

[11] S. M. Nam and T. H. Cho, "Energy efficient method for detection and prevention of false reports in wireless sensor networks," in *Proceedings of the 8th International Conference on Information Science and Digital Content Technology (ICIDT '12)*, pp. 766–769, Jeju Island, South Korea, June 2012.

[12] S. Naik and N. Shekokar, "Conservation of energy in wireless sensor network by preventing denial of sleep attack," *Procedia Computer Science*, vol. 45, pp. 370–379, 2015.

[13] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks," *IEEE Sensors Journal*, vol. 15, no. 6, pp. 3590–3602, 2015.

[14] S. Kaur and M. Ataullah, "Securing the wireless sensor network from denial of sleep attack by isolating the nodes," *International Journal of Computer Applications*, vol. 103, no. 1, pp. 29–33, 2014.

[15] S. Shamshirband, A. Amini, N. B. Anuar, M. L. Mat Kiah, Y. W. Teh, and S. Furnell, "D-FICCA: a density-based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks," *Measurement*, vol. 55, pp. 212–226, 2014.

[16] S. Shamshirband, A. Patel, N. B. Anuar, M. L. M. Kiah, and A. Abraham, "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks," *Engineering Applications of Artificial Intelligence*, vol. 32, pp. 228–241, 2014.

[17] N. K. Sreelaja and G. A. Vijayalakshmi Pai, "Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks," *Applied Soft Computing Journal*, vol. 19, pp. 68–79, 2014.

[18] G. Keerthana and G. Padmavathi, "Detecting sinkhole attack in wireless sensor network using enhanced particle swarm optimization technique," *International Journal of Security and Its Applications*, vol. 10, no. 3, pp. 41–54, 2016.

[19] A. Saeed, A. Ahmadinia, A. Javed, and H. Larijani, "Random neural network based intelligent intrusion detection for wireless sensor networks," *Procedia Computer Science*, vol. 80, pp. 2372–2376, 2016.

[20] D. Management, "RSA Algorithm," 2016, http://www.di-mgt.com.au/rsa_alg.html.

[21] M. Zhao, Y. Li, and W. Wang, "Modeling and analytical study of link properties in multihop wireless networks," *IEEE Transactions on Communications*, vol. 60, no. 2, pp. 445–455, 2012.

[22] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks," *IEEE Sensors Journal*, vol. 15, no. 6, pp. 3590–3602, 2015.

[23] D. N. S. Swapna Naik, "Conservation of energy in wireless sensor network by preventing denial of sleep attack," in *Proceedings of the International Conference on Advanced Computing Technologies and Applications (ICACTA '15)*, pp. 370–379, Mumbai, India, March 2015.