# DENIAL OF SLEEP ATTACK DETECTION USING MOBILE AGENT IN WIRELESS SENSOR NETWORKS

**G. Mahalakshmi[1], Dr. P. Subathra[2]**

[1]Assistant Professor, Department of Computer Science &Engineering , PTR College of Engineering and Technology, Tamil Nadu 624001, India.

[2]Professor, Department of Information Technology, Kamaraj College of Engineering & Technology, Tamil Nadu, India.

***ABSTRACT*: Maintenance of security is an imperative element in Wireless sensor Networks. Wireless sensor Networks contain the gathering of dispersed portable hubs with the ability of detecting the natural conditions. At the point when the extent of the WSN expands, then the activity over the sensor organize additionally increments.It will cause the network congestion and also the packet loss in the network. This category of network congestion and packet loss will occur in the sensor network due to the launching of various attacks in the wireless sensor networks. The most important attack in wireless sensor network is the Denial of Sleep (DoSL) Attack. This attack belongs to the category of the Denial of Service Attack (DoS). The motive of Denial of Sleep (DoSL) attack is to drain the energy level of the sensor network by making the sensor nodes always in processing mode and does not allow them to enter into the sleeping mode. This will also reduce the lifetime of the network from years to months. In this paper, an algorithm called Sleep attack Detection Algorithm (SLDA) is proposed to detect and prevent the Denial of attack in the WSNs. This proposed SLDA algorithm is dynamic and accurate in detecting the Sleep attack that uses Mobile agent, trust value, random key pre-distribution & random password generation. We are using a password which is generated randomly and trust value to distinguish and then for the confirmation of a normal node and an attacker node. Moreover, this algorithm helps in the transmission of data in a more secured way by avoiding the Denial of sleep attacks and also reduces the power consumption. We have simulated the proposed algorithm in NS2. We have verified the detection performance of SLDA and also checked the throughput and packet delivery ratio in wireless sensor network.***

***Keywords*: Wireless Sensor Networks, Mobile Agent, Denial of attack Detection Algorithm, Intrusion Detection.**

## 1. INTRODUCTION

### 1.1 Wireless Sensor Network

Wireless Sensor Network contains a collection of sensor nodes that work in a collaborative manner in order to sense the environmental condition. The applications of sensor networks, including surveillance systems, battlefield monitoring, etc. [1]. Sensors are typically self-possessed, portable, battery-powered and low price devices used to sense the physical parameters like light, temperature, or pressure in a particular application area. The main task of sensor networks is to sense the events, gather the sensed data's and transmit them to their corresponding destination [2]. In a wireless sensor network, the sensors communicate with each other by using wireless transceivers. The excellent features of the Wireless sensor networks like flexibility, fault tolerance, Scalability, high sensing capabilities, cheap in cost, and immediate deployment of the sensor networks enable the WSNs for many exciting applications.

However, its inflexible constraints such as limited resources of sensor nodes, insecure, short ranged radio communication, node and link failures, mobility of nodes and network topology change, broadcast network and data redundancy, power consumption, etc. causes many new challenges.

Many researchers have tried to solve these issues and challenges. In the current scenario, the security issues and the energy efficient the routing strategies are getting much preference.

### 1.2 Intrusion Detection System

An intrusion-detection system (IDS) can be defined as a set of tools, methods and resources aimed to identify assess and reports unauthorized or unapproved network activity. The main purpose of intrusion detection is to serve as an alarm mechanism for a computer system or a network [3]. The intrusion detection systems act as a second line of defense in a wireless sensor network. It also monitors the network activity, analyze data integrity, and audit network and system configurations for vulnerabilities.

### 1.3 Intrusion Detection Policies

In general, the intrusion detection policies are categorized into two types:

i) Misuse detection

ii) Anomaly detection.

*1.3.1 Rule-Based/Signature-based IDS*

Misuse detection algorithms are used to detect attacks based on the known attack signatures. They are effective in detecting only the known attacks with low errors. However, they cannot able to detect new attacks that have the different properties compared to the known attacks [5].

*1.3.2 Anomaly-based IDS*

The anomaly based IDS are based on the principle of the attacker behavior differs from the behavior of a normal user. They categorize the traffic as an attack if the characteristics of the traffic are differing from those of normal traffic patterns. Anomaly detection algorithms can be useful for the detection of new attack patterns, but they are not as effective as rule based detection methods in the detection rate of known attacks [5].

## 2 ATTACKS

A human who has the motive to exploit vulnerability perpetrates an attack on the system [17]. Vulnerability is defined as a weakness in the security system. The attack is an activity aimed to make harmful to the network performance.

Wireless Sensor networks are prone to different types of attacks such as sinkhole attack, black hole attack, DoS attack, Wormhole attack, etc. We are mainly dealing with the Denial of Sleep attack.

### 2.1 Denial of Sleep Attack

Wireless sensor network contains a set of spatially distributed sensor nodes without any wired infrastructure. This type of networks uses the wireless communication for transferring the sensed data among the sensor nodes and the users. [1]. The sensor nodes in the WSN are energized using the batteries. But, one of the major issues of WSN is the loss of energy. It is caused due to the following reasons [2],

- Collisions
- Overhearing
- Idle listening
- Control packet overhead

In the collision loss, the collision of data packets in the wireless medium causes the energy loss. In the overhearing loss, the maintenance of radios in the receive mode during data packet transmission causes the energy loss.

The idle hearing loss is created by a node's radio in just monitoring the channel. When all the nodes in the transmission range, may have to receive the control packets, then the control packet overhead is introduced. Generally, the WSN is vulnerable to two types of attacks such as invasive attack and non-invasive attack. The non-invasive 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 aim of denial-of-service attack makes the system or service inaccessible. The important properties of the DoS attacks are,

- Malicious
- Disruptive
- Remote

When the denial-of-service attack is performed purposely, it is termed as malicious. When the DoS attack is successful, the capability or service in WSN is getting damaged. Thus, disrupting the system or affected service is not the only goal of the attacker. As the attacker aims to launch multiple types of DOS attacks from a remote place. One of the special kind of denial-of-service attack is DoSL attack.

An example of the DoSL attack is shown in Fig.1. In this attack, the energy consumption of the sensor nodes is increased by preventing them to enter into sleeping mode. 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 legitimate source, it will process the data received from the attacker nodes. This makes the receiver node to be awake till the data transmission gets completed thus draining the battery power of the sensor nodes. Further, the attacker nodes can transmit a false acknowledgment and make the source node to transmit all the services thus increasing the power consumption.

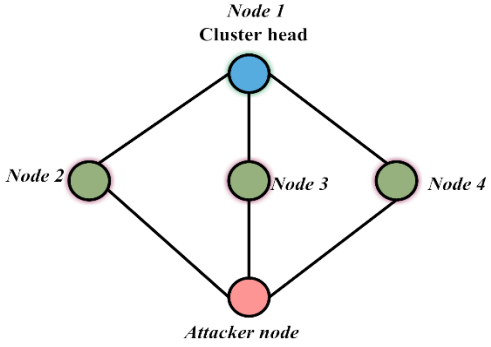


Fig.1. Denial-of-Sleep attack [4]

## 3 RELATED WORK

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

### 3.1 Detection of DoSL attacks in WSN

Mansouri, et al [5] proposed a clustering technique for addressing the DoS attacks. The suggested technique exploited the energy consumption of the nodes. Mansouri, et al [6] 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 verified that the suggested technique achieved optimal energy balance, throughput, detection coverage and delay between the packet transmissions. Chen, et al [7] proposed a time-division secret key protocol for detecting the DoS attack. The simulation results proved that the cipher function was optimized for WSN. Further, the detection jamming scheme increased the network lifetime of the WSN. He, et al [8] suggested a distributed code dissemination protocol, namely, DiCode for detecting the DoS attacks. The demerits of the suggested protocol were non-optimal security properties and consequences on the network availability. Han, et al [9] proposed an Intrusion Detection System based Energy Prediction (IDSEP) for the cluster-based WSN. The suggested scheme reduces the energy consumption of the sensor nodes by detecting the malicious nodes. Further, based on the energy consumption trusts, the types of the DoS attacks were determined. Simulation results showed that the suggested IDSEP efficiently detected the malicious nodes.

Ram Pradheep Manohar [10] proposed the technique named as Slowly Increasing and Decreasing under the 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 [11] suggested a Deluge based multi-hop code dissemination protocol for enhancing the confidentiality of the WSN. Experimental results verified that the suggested approach provided optimal latency, dissemination rate, and energy consumption.

### 3.2 Energy draining attacks

Su Man, et al [12] suggested a Statistical En-route Filtering (SEF) scheme for detecting the false reports in the intermediate nodes. Further, the false report injection attack was protected by 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 improved 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 verified that the suggested method was optimized for defending the attacker from performing the task. Swapna Naik [13] addressed the denial-of-sleep attack detection by using a zero knowledge protocol and interlock protocol. Experimental results proved that the suggested protocols prevented the replay attack, man-in-the-middle attack and also minimized the resource consumption. Hsueh, et al [14] suggested a cross-layer design of secure scheme with MAC protocol for minimizing the energy consumption of the sensor nodes. Analysis results showed that the suggested protocol efficiently defended the replay attacks and forge attacks. Further, the security requirements and energy conservation were coordinated. Kaur and Ataullah [15] 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 [16] proposed a cross-layer design of secure scheme integrated with MAC protocol for defending against the replay attack and forge attack. Experimental results verified that the suggested protocol coordinated the energy conservation and security requirements.

### 3.3 Soft computing algorithms used for detecting the energy draining attack

Shamshirband, et al [17] proposed a Density-based Fuzzy Imperialist Competitive Clustering Algorithm (D-FICCA) for identifying 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 [18] suggested a cooperative Game-based Fuzzy Q-Learning (G-FQL) approach for detecting the intrusions in the WSN. The suggested model implemented the cooperative defense counter-attack phenomenon 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, counter-defense, 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 [19] suggested an Ant Colony Optimization Attack Detection (ACO-AD) algorithm for detecting the sinkhole attacks in WSN.

The keys were disseminated 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 reduced the false positives and also minimized the storage in the sensor nodes. Keerthana and Padmavathi [20] suggested an Enhanced Particle Swarm Optimization (EPSO) technique for detecting the sink hole 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 [21] suggested a Random Neural Network based IDS for detecting the attackers.

Experimental results verified 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 recommended for preventing the DoSL attacks are unrealistic. Thus, to address the issues in the existing techniques, an efficient SLDA algorithm is proposed.

## 4 PROPOSED WORK

We have proposed a Sleep Detection Algorithm (SLDA) to detect attacker nodes, i.e. nodes having misbehavior in wireless sensor network (WSN). Through this technique we are resolving the problem of draining the energy source of sensor nodes. In the proposed work we detect the malicious nodes based on Mobile Agent and using random key pre-distribution, random password and thrust value taking together.

### 4.1 Components

#### *4.1.1 Mobile Agent*

Mobile Agent is an independent computer program that executes continuously in cross-platforms. It has the abilities of self-control moving, imitating human behavior and relationships, and providing certain types of Artificial Intelligent services.
It can autonomously travel in heterogeneous network according to certain rules and searching for suitable computing resources, information resources or software resources [7]. A mobile agent is defined as a program segment, which is self-controlling in nature. They traverse in the network from node to node not only transmitting data, but also doing some computation. They are an effective paradigm for distributed applications, and especially useful in a dynamic network environment. The mobile agent does not require more energy for processing.

The mobile agent provides the various advantages, including the space savings, network traffic reduction, asynchronous autonomous interaction, real-time systems interaction, robustness and fault tolerance, provide efficient support for heterogeneous environments, on-line extensibility of services, convenient development paradigm and client customization etc [8]. Mobile agents are useful in various applications. The intrusion detection process is our main concern. A lot of problems such as centralized or partial distribution, static reconfiguration, vulnerability to direct attacks and limited response capabilities etc. are associated with the traditional intrusion systems (IDSs). But mobile agent technology offers the potential to mitigate a number of boundaries intrinsic to existing Intrusion Detection Systems (IDSs).

Defining and collecting data which is used as input to the intrusion detection engine is a main issue in IDSs. Using a mobile agent, information retrieval and monitoring intrusion by IDSs becomes easy [18]. After intrusion detection, the intrusion must be either brought to the notification of the system administrator or to an automatic response system to take some action i.e. blocks the detected intrusion packets [8]. Mobile agents can help in IDSs by accomplishing the tasks like monitoring the WSNs, decision-making, notification as well as reaction to attempted intrusions.

#### *4.1.2 Trust Value*

The cluster head calculates the trust values of all the memeber nodes by applying the following steps,
Step 1: Initially the trust value of the member nodes are
initialized with zero.
Step 2: If the packets are correctly transmitted from one
node to another node:
(a) If the correctly transmitted number of packets is between 1 to 10, then trust values of the respective nodes will be incremented by one time.
Updated trust value = old trust value + 1;
(b) If the correctly transmitted number of packets are greater than 10, then the updated trust value will be:
Updated trust value = old trust value +
(correctly transmitted packets / 10);

#### *4.1.3 Random Key Pre-distribution*

Random key pre-distribution for WSNs was first proposed by Eschenauer and Gligor [19]. In a random key pre-distribution scheme, each node is assigned a set of keys which is drawn from a much larger key pool. In our proposed model, we use the random password generator in random key pre-distribution process.

#### *4.1.4 Random Password Generator*

Every time when the sensor node starts the sensing process, a random password generator generates a new password which is a random value.The RPG Algorithm generates a random password. When a source node wants to communicate with the destination node, the mobile agent, compare the id of the source node, the random password and the trust value of the source node in order to verify its trustworthiness. If the node id, corresponding to the trust value along with the password is matched, the source node is considered as a normal node and is allowed to send data otherwise the node is considered as a malicious node and that node id is blocked. The information regarding that malicious node is transmitted to the base station via a corresponding cluster head.

*4.1.5 Random Password Generation (RPG)Algorithm* Random Password Generation (RPG) Algorithm describes the process of generating the random password by following the steps given below.

**Step 1**

Record the packet sensing time of a particular node in 00:00 format.

**Step 2**

Generate ten random values in the respective column of the particular node staring from 0 to 9 in pwd_table in Table 3.

**Step 3**

Note the each and every digit sequentially from left to right of the above described format of recorded time.

**Step 4**

Pick the random value from the respective row of pwd_table for individual digits.

**Step 5**

Using the chosen random value, generate a pre-random password.

**Step 6**

Generate a random password using pre-random password along with the random key.

*4.1.6 Random Password Generation Process*

Here the random password is generated along with the help of the following some components. Those are
i) Time of packet sensing
ii) Random password generator.

The pwd_table of cluster head contains the node_id and a sequence of 0-9 in a row as shown in table3. When the sensing process starts, a random value is generated for the particular sensing node. Ten values from 0 to 9 is generated and saved. The time of packet sensing of the particular node is recorded. Suppose the time is 12.30 then all the individual numbers, i.e. 1, 2, 3, 0 are considered, which we call "pick value".

**4.2 The Database Tables**

In dealing with attacker node detection we are using few database tables at the mobile agent, cluster head, base station and sensor nodes. Those are namely ptable, btable, ctable and pwd_table.

*4.2.1 ptable*

This ptable is present in the mobile agent and the cluster head. This table contains the following data as shown in table 1.
**Table 1. ptable**

| Node_id | Trust Value | Random Passwod |
|---|---|---|
| N1 | 7 | RACD |
| N2 | 11 | KINS |
| …… | …… | …… |

*4.2.2 ctable*

This ctable is the table of mobile agents. This table contains the following data as shown in table 2.

**Table 2. ctable**

| Node_id(Attacker node) |
|---|
| N6 |
| N3 |
| …… |

*4.2.3 pwd_table*

This pwd_table is present in the cluster head and the sensor node. These are the following data as shown in table 3.

**Table 3. pwd_table**

| Node_id / Position | Node_id 1 | Node_id 2 | …… | Node_id n |
|---|---|---|---|---|
| 0 | B | A | …….. | I |
| 1 | R | F | ……. | N |
| 2 | A | P | …….. | D |
| 3 | C | Z | …… | E |
| ……. | ……. | ……. | ……. | V |
| 9 | K | I | …… | R |

The pwd_table of cluster head contains the node_id and a sequence of 0-9 in a row as shown in table3.

A random value is generated for the particular sensing node when the sensing process starts. Ten values from 0 to 9 is generated and saved.

The time of packet sensing of the particular node is recorded. Suppose the time is 12.30 then all the individual numbers, i.e. 1, 2, 3, 0 are considered, which we call "pick value". The values from the respective node_id column will be chosen for each pick value. So the values are R, A, C, B for node_id1. Using all the above values a pre-random password is created. Finally the pre-random password along with the random key will generate a random password.

The random value in the pwd_table of a particular node will reset again for next sensing process.

*4.2.4 btable*

This btable is the table of the base station. This table obtains the data from the ctable and keeps the record of the attacker nodes in the network. The data is as shown in the following in table 4.

**Table 4. btable**

| Attacker node_id | Cluster_id |
|---|---|
| N1 | C3 |
| N2 | C6 |

**4.3 Sleep attack Detection Algorithm (SLDA)**

In our proposed model (Fig.2) we are using the three main components in wireless sensor network (WSN). Those are sensor nodes, cluster head nodes and base station. The cluster head nodes have two tables, namely ctable and ptable and base station have btable. The mobile agent has a table named as ptable. The algorithm goes through the following steps.

**Step 1**

Generate random_key as well as node_id.

**Step 2**

Assign the node_id and random_key to each node.

**Step 3:**
Calculate the trust value of each node. Store it in the ptable.

**Step 4:**
A random password is generated in reference to the random_key.

**Step 4**

The sensor node sends data through the mobile agent, to the cluster node along with random_password.

**Step 5**
Mobile agents check the node_id in its stored database (ptable).

**Step 5.1**

If node_id matches Check for random_password as well as trust value.

**Step 5.1.1**

if random_password and trust value matches The legitimate node is confirmed. Data received by respective cluster head from legitimate node securely.

**Step 5.1.2 else**

The malicious node is detected and blocked by Mobile agent.C_table data are sent to base node. Store the data in b table.

We also represent the steps of the Sleep attack detection algorithm for the implementation point of view.

**Pseudocode**

```
Set Node_ID=n(n1,n2,n3.....),
Random_Key=R_K(R_K1,R_K2,R_K3.....),
Calculate trust value of each node.Store it in the ptable.
Generate                                Random_Password
psw(psw1,psw2,psw3.....).
mobile_agent(n,psw,n_tr)
{
  if(n==n')   / /n'=node_id stored in ptable of mobile
              agents
{
if (p==rp && n_tr==trust_value)
{

Data sent to the destination.

}
else
{

"Detect malicious node" and Store n in ctable.
Send ctable data to   btable

}} }
```

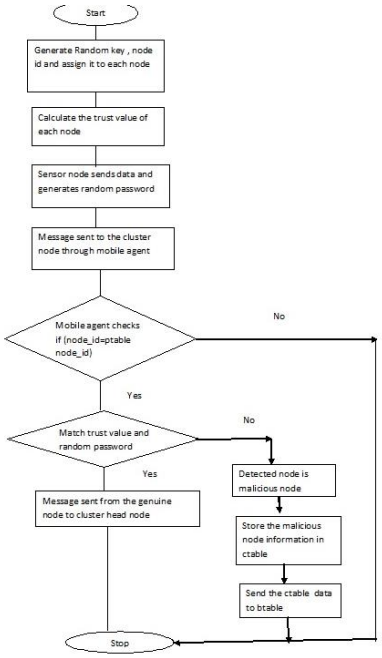


**Fig 2:Flow Diagram of SLDA**

### 4.4 Procedure

When the data packet travels in the network to the destination (Base station), mobile agent tracks it and checks node_id for the verification of node identity.If the node_id matches then the random_password and the trust value for that node is checked. The trust value stored in the database of mobile agent is compared, if the value matches, then that node is considered as the legitimate node otherwise it is considered as an attacker node. The detected malicious node is stored in ctable of cluster head. The attacker node information from the ctable is transmitted to the btable of the base station, so that on further communication with the compromised node can be easily detected and attacker nodes are blocked. The data from legitimate node is sent through the respective cluster head to base station. The base station, then keeps the record of the malicious nodes and informs the same to other nodes to alert.

## 5 SIMULATION

The proposed Sleep attack Detection algorithm is implemented in NS2. The process of attacker node detection in wireless sensor network is simulated. The performance of the algorithm is compared in terms of the packet delivery ratio before and after the attack.

The parameters used in our simulation are shown in Table 5.

**Table 5. Simulation parameter**

| | |
|---|---|
| Area | 10000m X 10000m |
| Nodes | 50 |
| Packet size | 512bits |
| Transmission protocol | UDP |
| Propagation | Two Ray Ground |
| Application Traffic | CBR |
| Queue type | Drop tail |
| Antenna Model | Omni directional area |
| Routing Protocol | AODV |
| Initial energy | 100joules |

### 5.1 Simulation Results

Fig.4 and Fig.5 shows the network deployment and malicious(attacker) node detection respectively. The number of nodes created is 50 and node 0 is the base station. After the assignment of node_id and random_key to each node the data packet was sent to

cluster head. Through mobile agent the node_id, random_password and trust_value is checked to detect the attacker node. The attacker nodes detected are 8, 16,27,35 and 43.

Fig-6 and Fig-7 represents the packet delivery ratio before and after malicious node detection.

It has been observed that the packet drop has been decreased and hence the packet delivery ratio has been improved after the detection and blocking the attacker nodes.

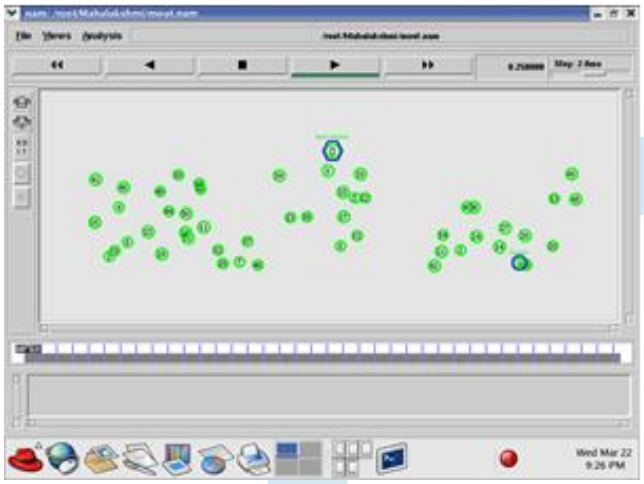

**Fig 4: Network Deployment**

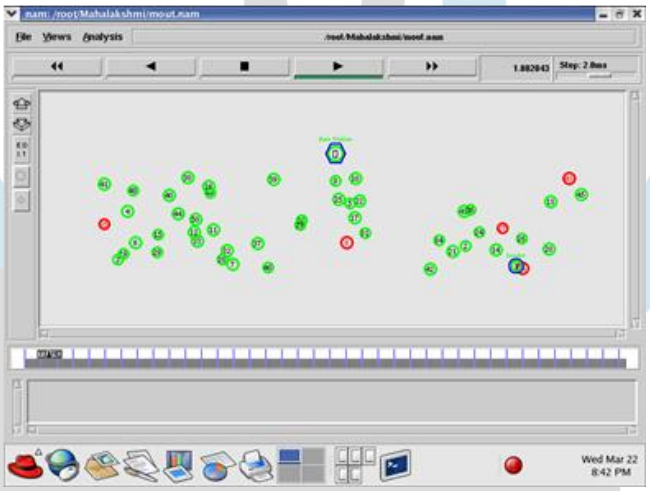

**Fig 5: Malicious node detection**

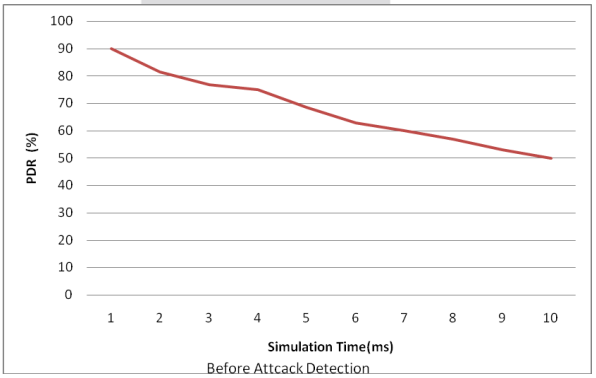


**Fig 6: Packet Delivery Ratio before attack detection**

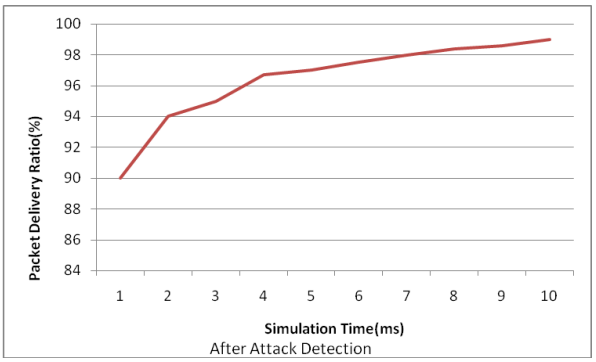


**Fig 7: Packet Delivery Ratio before attack detection**

## 6 CONCLUSION AND FUTURE WORK

Denial of sleep attack is one of the major security issues for wireless sensor network. In wireless sensor networks, the attacker node disturbs the sleeping time of the sensor node and drains the network lifetime and also degrade the network performance significantly. The network may even collapse. So, these attacks create a major challenge to the security in WSNs.
Our proposed SLDA method based on mobile agent uses three major parameters, namely, random key pre-distribution, random password and trust value to detect the attacker node. The malicious node detected is informed to the base station and the base station keeps the record of attacker nodes for security purpose and alerts the sensor nodes in the network. The network performance is evaluated in terms of the packet delivery ratio to analyze the adverse effect of Denial of Sleep attack.

In our future work, we will compute and compare the detection rates (i.e true positives and false positives) and the detection ratio and analyze the performance for a different set of simulation parameters. We will also verify the energy efficiency of the proposed SLDA method to be cost effective.

## REFERENCES

[1] Kamdeo Prasad, Chandrakant Mallick,"A Mobile Agent based Sybil Attack Detection Algorithm for Wireless Sensor Network" in *International Conference on Emergent Trends in Computing and Communication (ETCC 2015)*

[2] V. C. Manju, S. L. S. Lekha, and M. S. Kumar, "Mechanisms for detecting and preventing denial of sleep attacks on wireless sensor networks," in *IEEE Conference on Information & Communication Technologies (ICT)*, 2013, pp. 74-77.

[3] 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, pp. 343-348, 2016.

[4] 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, pp. 367-380, 2009.

[5] D. Mansouri, L. Mokddad, J. Ben-othman, and M. Ioualalen, "Preventing Denial of Service attacks in Wireless Sensor Networks," in IEEE International Conference on Communications (ICC), 2015, pp.3014-3019.

[6] D. Mansouri, L. Mokdad, J. Ben-othman, and M. Ioualalen, "Detecting DoS attacks in WSN based on clustering technique," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2013, pp. 2214-2219.

[7] J. l. Chen, Y. w. Ma, X. Wang, Y. m. Huang, and Y. f. Lai, "Time-division secret key protocol for wireless sensor networking," *IET Communications* vol. 5, pp. 1720-1726, 2011.

[8] 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, pp. 1946-1956, 2012.

[9] 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, pp. 97-105, 2013.

[10] 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.

[11] 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, 2// 2013.

[12] N. Su Man and T. H. Cho, "Energy efficient method for detection and prevention of false reports in wireless sensor networks," in *8th International Conference on Information Science and Digital Content Technology (ICIDT)*, 2012, pp. 766-769.

[13] D. N. S. Swapna Naik, "Conservation of energy in wireless sensor network by preventing denial of sleep attack," *International Conference on Advanced Computing Technologies and Applications (ICACTA)*, vol. 45, pp. 370-379, 2015.

[14] 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, pp. 3590-3602, 2015.

[15] 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, 2014.

[16] 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, pp. 3590-3602, 2015.

[17] 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, 9// 2014.

[18] 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, 6// 2014.

[19] Eschenauer and V. D. Gligor. A key management scheme for distributed sensor networks. In 9th ACM conference on Computer and communications security, pages 41–47, 2002.

[20] G. P. G.Keerthana, "Detecting Sinkhole Attack in Wireless Sensor Network using Enhanced Particle Swarm Optimization Technique," *International Journal of Security and Its Applications*, vol. 10, pp. 41-54, 2016.

[21] D.Sheela, V.R.Srividhya, Amrithavarshini and J.Jayashubha, *A Mobile Agent Based Security System of Wireless Sensor Networks against Cloning and Sink Hole Attacks*, Issues ICCTAI'2012.

[22] D. Rajesh Kumar, R. Sathish, *Mitigation of Replication Attack Detection in Clusters through a Mobile Agent in Wireless Sensor Networks*, Issue March-April 2013 (IJERA).

[23] T. N Manjunatha, M.D Sushma, K.M Shivakumar,*Security Concepts and Sybil Attack Detection in Wireless Sensor Networks*, Issue March-April 2013 (IJETTCS).

[24] Sasmita Pani, Omkar Pattnaik, *A survey on secure localization with Intrusion Detection System in WSN*, Issue October-2013 (IJRCCT).

[25] Deepika P Vinchurkar, Alpa Reshamwala, *A Review of Intrusion Detection System Using Neural Network and Machine Learning Technique*, Issue November 2012(IJESIT).

[26] Gisung Kim, Seungmin Lee , Sehun Kim,"*A novel hybrid intrusion detection method integrating anomaly detection with misuse detection",* Expert Systems with Applications,Elsevier, Pages 1690-1700.