ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Detecting and Preventing Denial of Sleep Attack using KeyGen (Key Generation) Algorithm

Usha C. Khake, Pooja L. Chelani, Vandana S. Lokhande

Lecturer, Dept. of Computer, Government Polytechnic, Mumbai, India

Lecturer, Dept. of Computer, Government Polytechnic, Mumbai, India

Lecturer, Dept. of Computer, Government Polytechnic, Mumbai, India

ABSTRACT: Wireless sensor network is a self-configured, infrastructure less wireless network consisting of a large number of sensor nodes equipped with specialized sensors that can monitor various physical attributes such as temperature, pressure, vibration and sound. The Security and energy efficiency is the most important concerns in wireless sensor networks (WSNs) design. WSN relies on hardware simplicity to make sensor field deployments both affordable and long lasting without any maintenance support. The Sensor nodes are powered up with batteries. Due to unattended nature of deployment, the sensor nodes cannot be recharged again. In this condition, the nodes must optimally consume power. An Energy constrained sensor networks periodically place nodes to sleep in order to extend the network lifetime. Various protocols are designed to reduce the energy consumption of sensor nodes by keeping the antenna in sleep mode 90% of time, so that power is saved. MAC protocols are designed to vary the sleep time based on the communication need. However, attackers use their knowledge of their underlying MAC protocol, to reduce the sleep time of the node, so that life time of the node reduces. This problem we refer it as Denial of sleep attack and in this Project we propose effective solution to defend against this attack on a sensor network. The existing system is based on Packet threshold analysis mechanism used for detection of attack here. The proposed system is based on Challenge response security using KeyGen algorithm activated to ensure the validity of the sender here and prevent unwanted communication.

KEYWORDS: Wireless sensor network, Denial of Sleep attack

1. Introduction

Wireless Sensor Networks are vulnerable to many attacks. Each attack may lead to a different problem. There are two types of attacks that are popular with the Wireless Sensor Networks. They are Physical attacks and logical attacks. Physical attacks include capturing of the nodes and tampering the nodes which will lead to loss of data. On the other hand, Logical attacks include attacks like sinkhole attack, wormhole attack, hello flood attack, selective forwarding attack, Sybil attack, Denial of sleep attack. Among all these attacks denial of sleep attack is most dangerous energy consumption attack. In this type of attack, an attacker consumes the sensor nodes energy by making the node awake even when there is no traffic to hold. For this activity an attacker consumes the sensor node energy totally and node gets die. Due to this the lifetime of wireless sensor network decreases by causing the radio of the receiver ON, draining the battery in only few days. Now it can be understood that security of WSN against denial of sleep attack is very important part. Recently, there have been several existing solutions to solve the Denial of sleep attacks problem by adding security to WSN in order to prevent/detect attacker. However, most of them have some critical drawbacks. They are described below in compact form with their strengths and limitations

II. RELATED WORK

2.1 Wireless sensor network denial of sleep attack

Brownfield [2] proposed new MAC protocol which mitigates many of the effects of denial of sleep attacks by centralizing cluster management. MAC has several energy saving features which not only extend the network lifetime, but the centralized architecture makes the network lifetime more resistant to denial of sleep attacks.

DOI: 10.15680/IJIRCCE.2017. 0505223

2.2 Effect of Denial of sleep attacks on wireless sensor network MAC protocols

David R. Raymond [3] classifies sensor network denial-of-sleep attacks in terms of an attackers knowledge of the medium access control (MAC) layer protocol and ability to bypass authentication and encryption protocols. Attacks from each classification are then modeled to show the impacts on four sensor network MAC protocols, i.e., Sensor MAC (SMAC), Timeout MAC (T-MAC), Berkeley MAC (B-MAC), and Gateway MAC (G-MAC).

2.3 Sleep deprivation Attack Detection in Wireless Sensor network

Tapalina Bhattasali [4] proposed a hierarchical framework based on distributed collaborative mechanism for detecting sleep deprivation torture in wireless sensor network efficiently. In heterogeneous sensor field, sensor nodes are categorized into various roles such as sink gateway (SG), sector monitor(SM), Sector-in charge (SIC) and leaf node (LN) depending on their battery capacity. Here leaf node is used to sense the data, SIC is used to collect the data and SM detect the data as valid data and invalid data. Sink Gateway is used to access other networks.

2.4 Mechanisms for Detecting and Preventing Denial of Sleep Attacks on Wireless Sensor Networks

Manju.V.C,Senthil Lekha.S. L.,Dr.Sasi Kumar M. [1] proposed new algorithm to detect and prevent denial of sleep attack. Proposed method to defend denial of sleep attack consists of two parts.

1. **Network organization**. Sensor Network was built in tree like structure and organizes the nodes. Sink node is at the root of the tree. Each node must know its parent node to which it needs to send packets to reach to sink. Also the parent node must know the child node from which it can receive SYNC packets.

2. **Selective level authentication**: There are two different formats for SYNC packet. One is without authentication and other one is with authentication Token. During normal operation if the SYNC is under threshold SYNC without authentication is used. If there is a threshold cross over there is a chance of denial of sleep attack and enforces SYNC with authentication token for authentication.

III. PROPOSED ALGORITHM

The Proposed System identifies denial of sleep attack for preventing continuous depletion of energy of the proposed destination in a particular network structure. We propose an effective solution to defend against this attack on a sensor network. The detection process will include generation of public key at authority node and utilization of hash signature for detection of the same at the destination node using secret key at destination node. Thereby, preventing depletion of energy during transmission.

3.1 Assumptions

Assumptions are necessary to define both the boundaries of this research and the scope of the problem that is to be addressed. The following assumptions apply to the design of WSN denial-of-sleep attack detection mechanisms.

3.1.1 Secrete Key and Public Key: In this simulation the term secrete key and public key are used which will act as secrete code during the communication to validate node without the concept of cryptography.

3.1.2 Certification Authority: In this simulation node 11 will act as the certification authority which will generate the hash value to validate nodes.

3.1.3 Main Station: Node 10 will act as Main Station which will be responsible to generate and distribute the keys (secrete, public) to nodes and to Certification authority. These keys are generated by using KeyGen algorithm.

3.1.4 Source Node and Destination Node: Node 0 and Node 9 will act as source and destination nodes respectively.

3.1.5 Attacker Node: Node 7 will act as attacker node.

This proposed method is executed in four distinct modules. Module I involve network creation. In Module II, mechanisms are designed to execute denial-of-sleep attacks targeting the victim node. Module III involve the generation of hash. Finally, in Module IV, the mechanisms developed in Module II are tested and analyzed for detection of denial-of-sleep attack and to validate source node as well as the Main Station using the hash generated in module III.

3.2 Modules:

3.2.1. Network Configuration and Creation: This module will involve designing the network structure to be used for transmission.

3.2.2. Attack Execution: This module will demonstrate execution of attack wherein the node energy will be lost due to existence of an invalid node. Due to this loss of energy, the overall performance of the network will be affected and therefore, improper transmission executes. It will involve transmission of data from source to destination node and its analysis to track the details of nodes.

3.2.3. Attack Detection using hash analysis: This module will facilitate the execution of attack and its detection using authentication mechanism. This mechanism will involve attachment of a hash analysis with the data transmitted will be distributed using an Authentication Node.

3.2.4. Analysis Module: This module will facilitate the generation of analysis of simulation time of the above executions and get an overall view of the current energy of the network at a particular time.

IV. ARCHITECTURE

The main goal of this architectural process is to detect the denial-of-sleep attack, analyse energy consumed and calculate the Packet Delivery Ratio with detection and without detection of attack. This architectural process is divided into two stages;

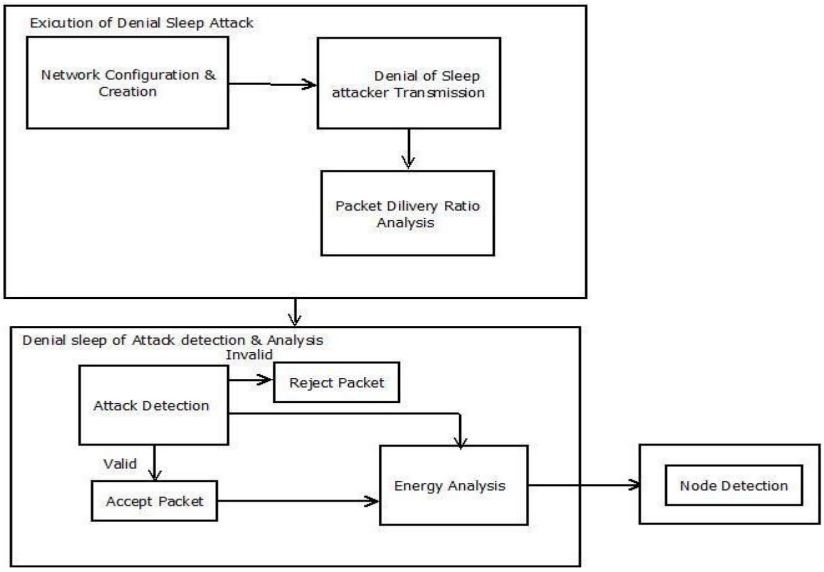

Exicution of Denial Sleep Attack
Network Configuration & Creation
Denial of Sleep attacker Transmission
Packet Dilivery Ratio Analysis
Denial sleep of Attack detection & Analysis
Invalid
Reject Packet
Attack Detection
Valid
Accept Packet
Energy Analysis
Node Detection

Fig1. Architecture of challenge and response method

4.1. Execution of Denial-Of-Sleep Attack: Initially in this stage network is created and configured. Then demonstration of execution of attack will be done wherein the node energy will be lost due to existence of an invalid node. Due to this loss of energy, the overall performance of the network will be affected and therefore, improper transmission executes. It will involve transmission of data from source to destination node and its analysis to track the details of nodes.

4.2. Denial-Of-Sleep Attack Detection Analysis: This stage executes and detects the attack using authentication mechanism. This mechanism will involve attachment of a hash analysis with the data transmitted. Attack detection will be done by comparing the response calculated by the destination node with the response received from the main station. If the received response matches the calculated response then the node is valid node. Also this stage is responsible to analyse the energy remaining at the destination node after the detecting the attack.

V. ALGORITHM

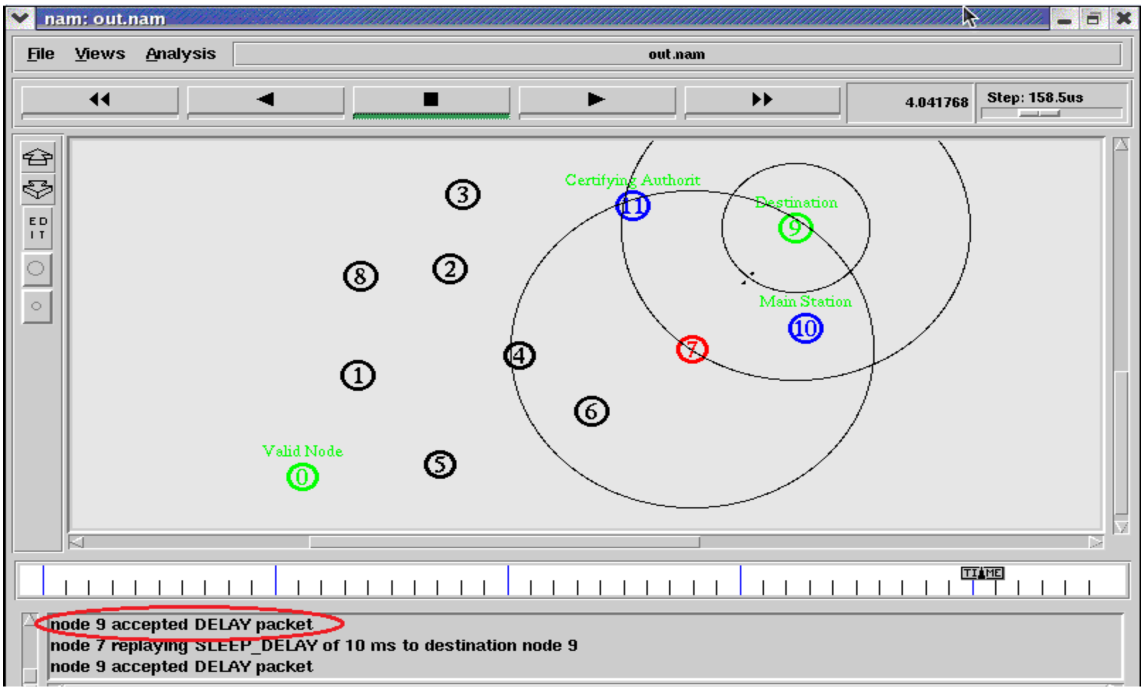
1. It consist of 11 nodes network wherein node 10 will act as a Main Station, node 11 will be Certifying Authority and Node 7 will act as an attacker for executing flood packet to victim node.
2. Identify impact of denial of sleep attack by tracing the depletion of energy parameter at victim node.
3. Prevention of denial of sleep attack by challenge and response mechanism

- Verifier node generates challenge security key using KeyGen Algorithm as follows:
- Select two large primes at random: p, q
- Compute their system modulus n=p*q
- Note (n) = (p-1) (q-1)
- Select at random the encryption key e where 1<e<(n), gcd(e,(n))=1
- Following equation is used to find decryption key d e*d=1 mod (n) and 0dn
- Publish their public encryption key: PU={e,n} keep secret private decryption key: PR= {d,n}
- During communication valid node requests for challenge parameter.
- Calculate response using challenge & secure function using security key.
- Invalid node will use random security key and then transmit calculated response to verifier.
- Verifier will calculate actual response for valid node.
- If calculated response = received response then the node is valid.

VI. SIMULATION RESULTS

Test Case 1:

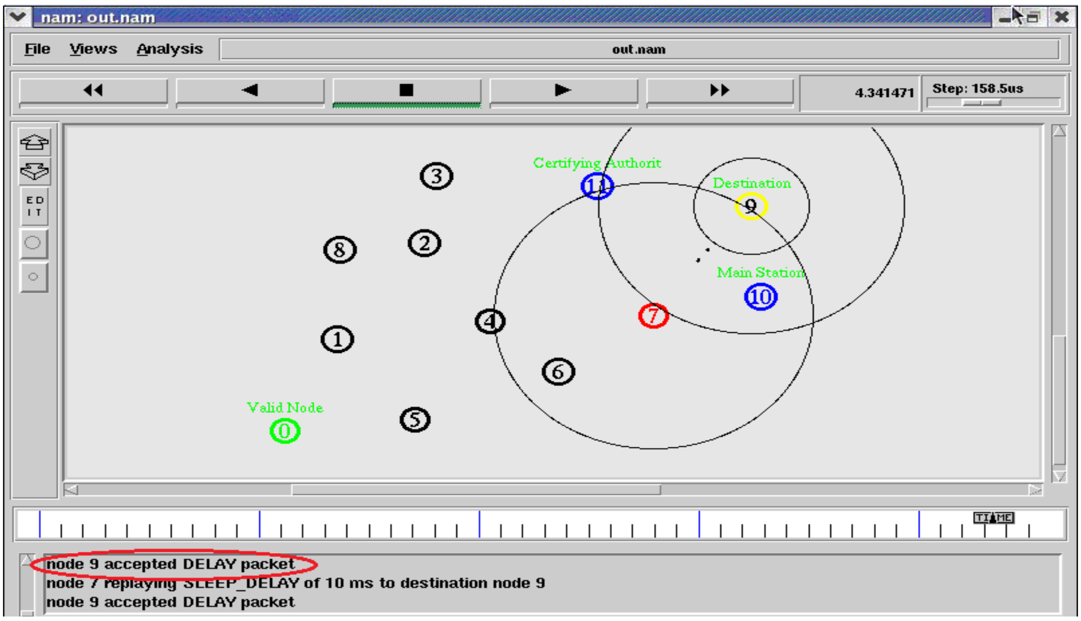
The attacker node attempt an attack on the destination node: In this case the attacker node will send the packets continuously to the destination node and drain node battery which in turn causes the node get die



```
node 9 accepted DELAY packet
node 7 replaying SLEEP_DELAY of 10 ms to destination node 9
node 9 accepted DELAY packet
```

Fig 2 Acceptance of packets by destination node from attacker node

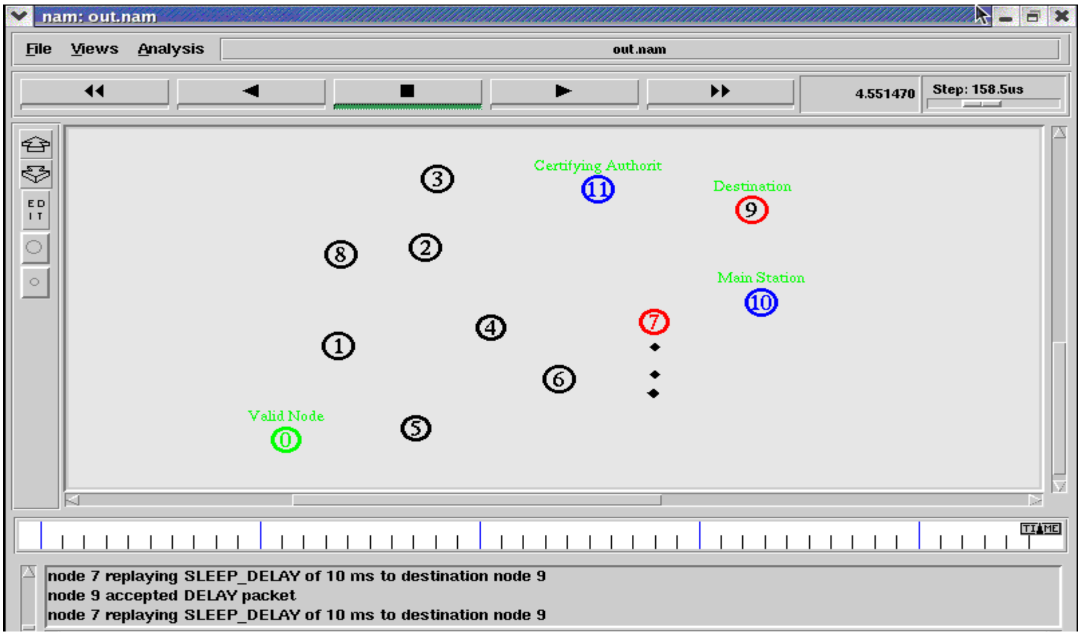
In the figure 2 the numbers of nodes created are 11. Where node 7 is an attacker node and node 9 is the destination node. Attacker node keeps on sending unwanted packets to destination node and making destination node continuously alive.



```
node 9 accepted DELAY packet
node 7 replaying SLEEP_DELAY of 10 ms to destination node 9
node 9 accepted DELAY packet
```

Fig 3: Energy Loss of destination node

In figure 3 Node 9 will accept the packets coming from attacker node as it do not have the knowledge of hash and key generated by the main station. Since destination node continuously accepting the packets there is energy loss at destination node. Yellow colour at destination node is indicating the energy loss.



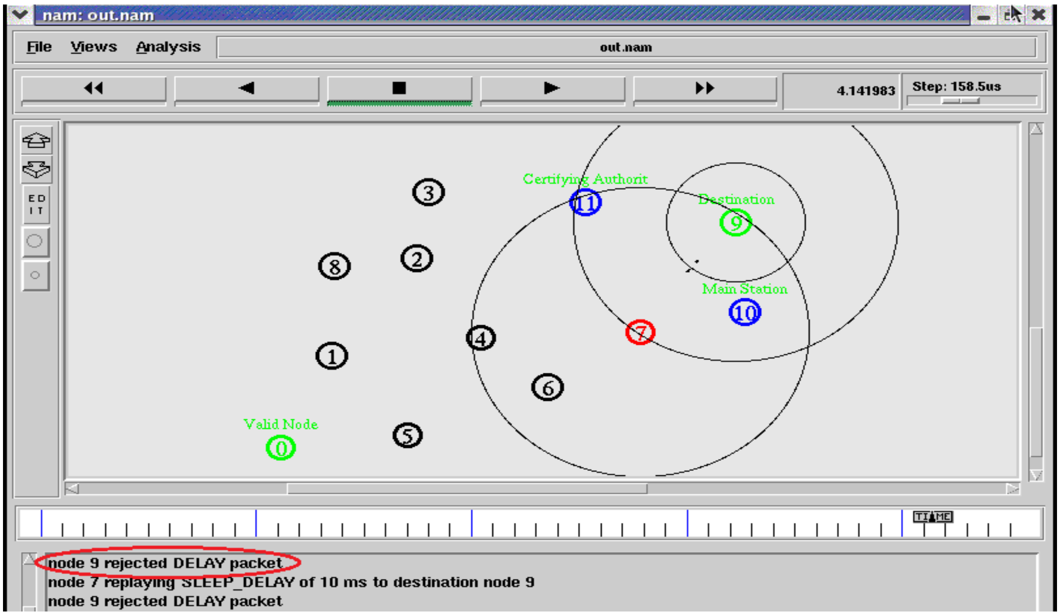
```
node 7 replaying SLEEP_DELAY of 10 ms to destination node 9
node 9 accepted DELAY packet
node 7 replaying SLEEP_DELAY of 10 ms to destination node 9
```

Fig 4: Packet Drop due to Energy Loss

Fig 4 shows the packets dropped due to energy loss at destination node by continuous acceptance of unwanted packets from attacker node.

Test Case 2:

Attack Detection using KeyGen algorithm: Attack detection will be done by comparing the response calculated by the destination node with the response received from the main station. If the received response matches the calculated response then the node is valid node. Also this stage is responsible to analyse the energy remaining at the destination node after the detecting the attack.



```
node 9 rejected DELAY packet
node 7 replaying SLEEP_DELAY of 10 ms to destination node 9
node 9 rejected DELAY packet
```

Fig 5: Rejection of Packet from Attacker Node

In this case we identify the impact of denial of sleep attack by tracing the depletion of energy parameter at victim node. Verifier node generates challenge security key. During communication, valid node requests for challenge parameter. Calculate response using challenge secure function using security key. Attacker node will use random security key and then transmit calculated response to verifier. Destination node will compare the response from attacker node and then reject the packets coming from that node. Figure 5 shows rejection of packet from attacker node.

For the result analysis we have created two graphs shown in Figure 6 and Figure 7. In these graphs the x-axis shows the simulation time the y-axis shows the energy remaining and packet delivery ratio respectively. The green line in figure 6 shows that preventing the attack improves the lifetime of the sensor network significantly the comparison of packet delivery ratio with and without the attack shows an improvement of performance when the attack is prevented.

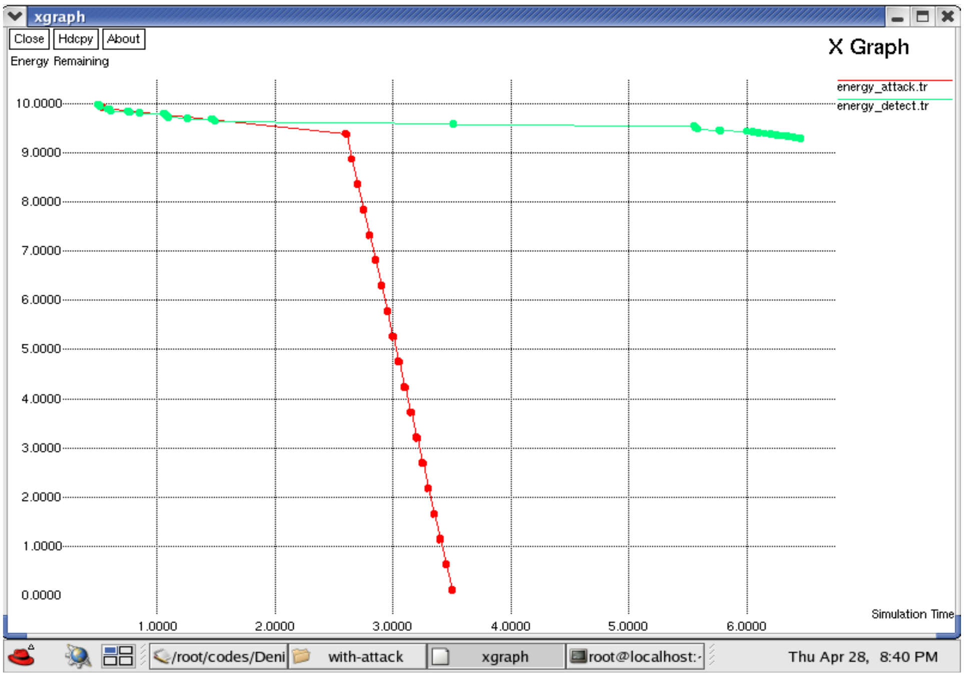


Fig 6: Energy Comparison Graph

The graph in Figure 6 shows the usage of battery power during simulation. When the attack takes place the red line shows that the battery of the node attacked quickly goes down as the replay message synchronizes the sleep cycle again and again thus depleting the battery life very fast. The battery life of the network shows vast improvement whenever the attack is prevented by carrying out the challenge and response method of authentication for nodes sending synchronization messages.

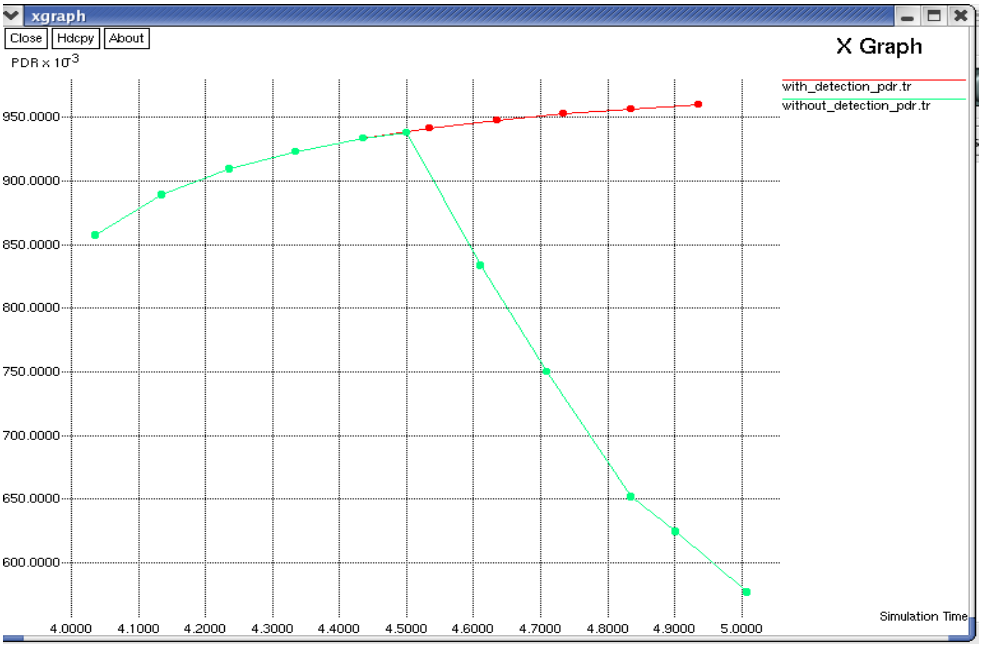


Fig 7: Packet Delivery Ratio Comparison Graph

The green line in figure 7 shows attack scenario where there is high packet delivery initially as packets are replayed repeatedly by the attacker node but once the battery is depleted sharp drop in packet delivery is seen.

VII. CONCLUSION

Building high performance WSN network systems requires an understanding of the behaviour of sensor network and what makes them fast or slow. In addition to the performance analysis, we have also evaluate the proposed technique in which denial of sleep attack between nodes will be detected and prevented with the help of new technique ,challenge response method. The final but most important step in our experiment is to analyse the output from the simulation. After the simulation we obtain the trace file from the simulation.

REFERENCES

[1] Manju.V.C, Senthil Lekha. S. L. Dr. Sasi Kumar M., “Mechanisms for Detecting and Preventing Denial of Sleep Attacks on Wireless Sensor Networks,” in Proceedings of2013 IEEE Conference on Information and Communication Technologies (ICT 2013).

[2] Brownfield, Michael, Yatharth Gupta, and Nathaniel Davis., “Wireless sensor network denial of sleep attack”,Information Assurance Workshop, 2005. IAW’ 05. Proceedings from the Sixth Annual IEEE SMC.IEEE, 2005.

[3] D. Raymond, R. Marchany, M. Brownfield, and S. Midkiff, “Effects of denial of sleep attacks on wireless sensor network MAC protocols,” in Seventh Annual
IEEE Systems, Man, and Cybernetics (SMC) Information Assurance Workshop, pp. 297304, June 2006.

[4] Bhattasali, Tapalina, RituparnaChaki, and SugataSanyal, “Sleep Deprivation Attack Detection in Wireless Sensor Network”, arXiv preprint arXiv:1203.0231 (2012).

[5] Sunita Devi, AnshulAnand, “Analysis of Dead Node in Wireless Sensor Network Denial of Sleep Attack,” in International Journal of Computer Science and Mobile Computing, Vol.3 Issue.6, June- 2014.

[6] GurjeetKaur, SimarjeetKaur, “A Solution of Sleep Deprivation Attack in Clustered Network,” in International Journal of Science and Research (IJSR), Volume 3 Issue 8, August 2014.

[7] Vidya M., “DENIAL OF SLEEP ATTACKS ON WIRELESS SENSOR NETWORKS,” in International Journal of Combined Research Development (IJCRD) Volume: 4; Issue: 4; April -2015.

[8] Swapna Naik, Dr Narendra Shekokar, “Conservation of energy in wireless sensor network by preventing denial of sleep attack,” in International Conference on Advanced Computing Technologies and Applications (ICACTA- 2015).