Efficient Utilization of Node Energy by Detecting and Preventing Denial of Sleep Attack

Usha C. Khake[1], Prof. Narendra Gawai[2]
[1]Student, [2]Guide, Department of Computer Science, UMIT, S.N.D.T University, Mumbai.

Abstract: A Wireless Sensor Network is a self-configuring network of small sensor nodes communicating among themselves using radio signals, and deployed in quantity to sense, monitor and understand the physical world. WSN provide a bridge between the real physical and virtual worlds.WSNs have a wide range of potential applications to industry, science, transportation, civil infrastructure, and security.WSNs are particularly exposed to several kinds of attacks. Due to energy constrained property in WSN, Denial-Of-Sleep attacks are recognized as a serious attack. Attack of this type exhaust the energy of sensor nodes and reduce the sensor lifetime within few days compared to other attacks on WSN. In this paper we propose a challenge and response method to detect denial of sleep attack for efficient utilization of node energy. Simulation reveals that our proposal is energy efficient and able to achieve significant performance in preventing network nodes from Denial-Of-Sleep attack.

*****

I. Introduction:

Recent trends used in modern wireless sensor networks needs to offer confidentiality, data integrity and availability of service to the user. It consists of huge number of nodes where each node is connected to one or more sensors. Due to energy constraints wireless sensor networks are vulnerable to attacks. Sensor networks typically works in different modes to conserve the energy. Various nodes are in active mode and in sleep mode. In active mode WSN node is ready to transmit and receive the data whereas in sleep mode it is not ready to do any activity. Energy Consumption WSNs are typically characterized by restricted power suppliers, low bandwidth, small memory size and limited energy. Due to these characteristics, several severe constraints exist in WSN compared to the conventional desktop computers. Sensor networks are vulnerable to several malicious attacks. Various attacks on sensor networks are:

- Wormhole attack
- Hello attack
- Sybil attacks
- Denial Of Sleep attacks
- Selective forwarding
- Acknowledgement spoofing

Among all these attacks denial of sleep attack is most dangerous energy consumption attack. In that 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.

II. Literature Survey:

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 as follows:

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

Manju.V.C,SenthilLekha.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.

Network organization.
Selective level authentication.

a) **Network organization**.

Sensor Network was built in tree like structure and organizes the nodes. Sink node is at the root of the tree. The following network organization algorithm was used to build the network in the way it is desired for our objective.

- First sink node will broadcast a Hello Packet with its ID.
- The node which receives this Hello packet which is one hop away will take ID in the Hello Packet as its parent and sends Hello Response to the ID also its broadcast a new Hello Packet with its ID.
- The node which receives the Hello Packet will check if it does not have a parent yet and it will add the ID in Hello packets as its parent and send Hello Response to its parent.
- On the arrival of Hello response, node will update its child list.

b) **Selective Local authentication**. In this part proposed method have provided three levels of security against attack and two different formats of SYNC packet were used. 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.

B) 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. Other than single period and synchronization message, it has two contention period and different networks for sending the message within the clusters and outside the cluster through the gateway node. The MAC protocol Performance Results show that G-MAC performs significantly better than other protocols in every traffic situations. The empty network case shows the protocol overhead and idle listening effects determined by the effective duty cycle-MAC has .95% duty cycle is weighted average 2 of duty cycle of gateway node and other nodes. Attacker can gain access to network through gateway node. But attacker can only affect one node at a time because nodes alternate the gate way responsibilities based upon incremental increase in battery levels.

C) 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). Implementations of selected attacks on MAC, T-MAC, and B-MAC are described and analyzed in detail to validate their effectiveness and analyze their efficiency. And it shows that the most efficient attack on S-MAC can keep a cluster of nodes awake 100% of the time by an attacker that sleeps 99% of the time. Attacks on T-MAC can keep victims awake 100% of the time while the attacker sleeps 92% of the time. With knowledge of protocol because of differences exist in packet structure and timing between WSN MAC protocols, and even without ability to penetrate encryption; all wireless sensor network MAC protocols are susceptible to a full domination attack, which reduces the network lifetime to the minimum possible by maximizing the power consumption of the nodes radio subsystem. Even without the ability to penetrate encryption, subtle attacks can be launched, which reduce the network lifetime by orders of magnitude. If sensor networks are to meet current expectations, they must be robust in the face of network attacks to include denial-of-sleep. This approach also increases the network overhead.

D) Sleep deprivation Attack Detection in Wireless Sensor network

TapalinaBhattasali [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. Here if leaf nodes are directly affected by intruder, node cannot detect it. As a result battery of affected node may be low or exhausted completely. This can affect data transmission for network due to which it is done in authenticated way.

E) Analysis of Dead Node in Wireless Sensor Network Denial of Sleep Attack

Sunita Devi, AnshulAnand[5] proposed a new clustered network with three stages, the work in the first stage performed by analyzing the number of communication and the time constraints to analyze the energy reduction rate. In second stage it tries to handle the node at the cluster level by blocking the node. In the third stage re-clustering is performed by considering that al nodes will not again form the same cluster. Merits of this method are high energy consumption and therefore high network life time. But with this method an infected nodes are identified based on energy reduction rate of sensor node only. Authors analysed the dead nodes of wireless sensor networks to prevent the occurrence of Denial of Sleep Attack. The presented work consists of three steps. Investigation within the cluster will be performed in the first step, which is computed by determining the count of communication and the time constraint to analyze the energy reduction rate of a node. The infected nodes are identified when the energy reduction rate is abnormal. In second stage, it tries to handle the node at the cluster level by blocking the node. In third step, re-clustering will be computed by considering that all nodes will not again form the same cluster. An introduced system is used to improve the network life.

F) A Solution of Sleep Deprivation Attack in Clustered Network

GurjeetKaur, SimarjeetKaur[6] proposed a new sleep deprivation attack method in which a Hierarchal Cluster Architecture was used. The proposed method was helpful to increase the sensor networks lifetime and the algorithm used prevented the sleep deprivation attack efficiently as well. But this method is not suitable to non-clustered networks.Authors introduced a Solution of Sleep Deprivation Attack in Clustered Network. In order to extend the sensor nodes lifetime the Energy effi- cient sensor networks continuously place nodes to sleep. There are different attacks which affect the energy of sensor node. The sleep deprivation attacks are detected by using detection algorithm. The message is send to leaf nods in clustered sector. The leaf node is forward the message the sector node. Sink node check it is leaf nodes sleep. If it is true check location of malicious node. Otherwise it forwards the packet to network. In malicious node detection condition, all leaf nodes will send messages to malicious node and deactivate it. In this research work sleep deprivation attacks detection mechanism is only implemented in clustered network. It does 3 not efficiently detect the sleep deprivation attacks in nonclustered network.

The algorithm used to Prevent Denial of Sleep Attack is as follows:

1. Leaf node receive message and send to sector node

2. Sector node forward message to sector in-charge.

3. Sector in-charge checks if message coming from leaf node is in its wake mode or sleep mode.

4. If message time==sleep time Tag=invalid. Otherwise, Tag =valid.

5. Sector in-charge forwards message to sink gateway after applying tags from step 4.

6. Sink gateway checks for tags

7. If tag==valid message in the network as it is a valid message. Otherwise,

- Check location of malicious node and send the same message to all leaf nodes which malicious node send message.
- All leaf nodes will send messages to malicious node and make it deactivated.

III. Proposed System:

Proposed method to defend denial of sleep attack consists of challenge and response method in which attack is detected using Key Generation procedure and signature concept. This method will facilitate the execution of denial of sleep and its detection using authentication mechanism. KeyGen Algorithm is used for key generation mechanism.This mechanism will involve attachment of a hashed signature with the data transmitted will be distributed using an Authentication Node.

CHALLENGE AND RESPONSE SYSTEM USING KeyGen ALGORITHML:

1. It consists of 11nodes network.
2. Node 7 will act as an attacker for executing flood packet to victim node. Node 10 will act as a Main Station; node 11 will be Certification Authority.
3. Identify impact of denial of sleep attack by tracing the depletion of energy parameter at victim node (In Our case Node 9).
4. Prevention of denial of sleep attack by challenge and response mechanism
    - Verifier node (Main Station) generates challenge security key using KeyGenAlgorithm as follows:

```
Select any three prime numbers p, q, and r
N= p*q
Pi= (p-1)*(q-1)
ForI = 1 to10000 incr i
{
Mod_d = (I*r) % pi
If {mod_d == 1}
Key=I
}
```

- During communication valid node requests for challenge parameter.
- Calculate response at destination node 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.

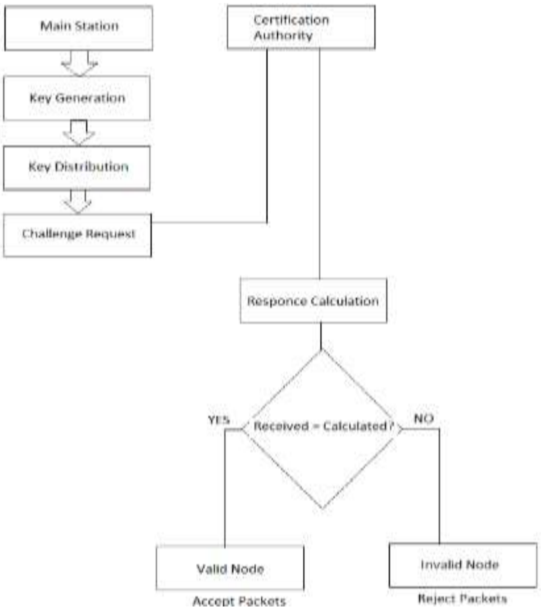
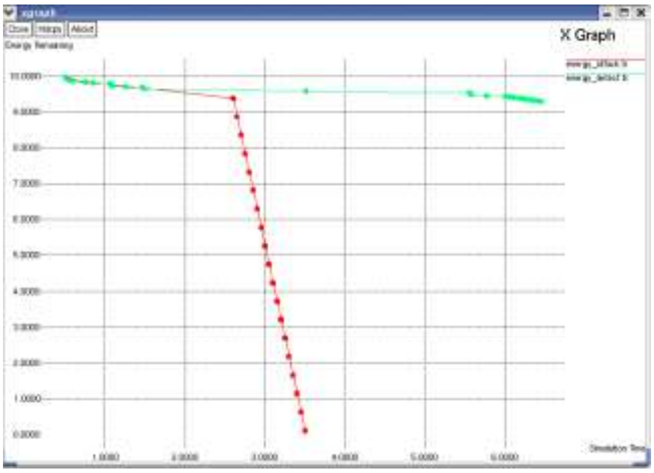


Fig. Flow Chart

IV. Analysis:

This module will facilitate the generation of analysis of transmission time of the above executions and get an overall view of the performance of the network on the basis of transmission time (i.e avg. residual energy in terms of time). For result analysis we have generated a graph wherein x-axis shows simulation time and y-axis shows battery energy.



V. Conclusion:

Building high performance WSN network systems requires an understanding of the behavior 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 analyze the output from the simulation. After the simulation we obtain the trace file from the simulation.

VI. References:

[1] Manju.V.C, SenthilLekha.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] SwapnaNaik, DrNarendraShekokar,“Conservation of energy in wireless sensor network by preventing denial of sleep attack,” in International Conference on Advanced Computing Technologies and Applications (ICACTA- 2015).