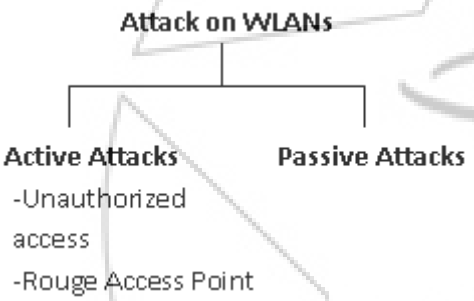
broadcast the schedule switch sync message to all the nodes but don't really change their schedule and RSSI (Received signal Strength Indication) is used to protect the switch scheme being revealed, this scheme is used to find the malicious node in the cluster.

In "Sleep deprivation Attack Detection in Wireless Sensor network" [5] proposed a hierarchical framework based on distributed collaborative mechanism for detecting sleep deprivation torture in wireless sensor network efficiently. The 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. Leaf node have the role of sensing the data, sector in-charge collecting the data and sector monitor have role of detecting the data, and this node is responsible for detecting the malicious and attackers data and sink gateway has the role of communicating with the sink node.

In "A Strategic deployment and cluster head selection for wireless sensor networks" [9] in this a paper, it proposed a cluster head selection scheme by designing the network with multiple-sized fixed grids while taking into account the arbitrary-shaped area sensed by the sensor nodes.



This cluster-based scheme considers the fact that

1) The sensor nodes are not always distributed on the square shaped field.
2) Each sensor node can have a different amount of initial energy. That is, some of the sensor nodes have more power and they also can be strategically located in other places.
3) The remaining energy of the sensor nodes is different at any given time depending on their particular position and functionality.

The drawback of this scheme is that it cannot be used for military purposes as the network is deployed in this scheme manually.

In "Distributed Wake-Up scheduling for Data collection in tree-based wireless sensor networks" [10] stated a scheme known as distributed wake-up scheduling scheme for data collection in a sensor networks that achieves both low reporting latency and energy conservation, i.e. in a wireless network which is special type of network known as multihop wireless network, a simple and efficient way of defining interference neighbors is to prohibit a node from using the same slot 0 code as those of its 1-hop and 2-hop. Power saving and latency are improved to prolong network lifetime and freshness of data.

Attack

An attack is a action performed by attacker to compromise the security of any information belonging to an organization.

Attackers

Attackers are any person or software that strongly attempts to destroy security services and violates the security policy of networked system. Such persons or computer attempts to gain unauthorized access to information resources.

3.1 Two types of attacks are

- **Active attacks**: Active attacks involve the attacker changing the information /content or even sometimes generating fraudulent information into the network. These types of attacks are malicious in nature and can result in severe losses for the victims.
- **Passive attacks**: Passive attacks are those in which the attacker obtains information being transmitted /received by the network. These types of attacks are usually difficult to detect as there is no modification of the contents by the attacker.

3.2 The Principle of Active attacks:

In the active attack scenario, a malevolent third party manipulates a response within a legitimate session in a way that tricks the client into issuing an unwanted request (unknown to the user) which discloses sensitive information. On this information the attacker can then apply a regular passive attack. So, according to it we can say that this is made possible by a design flaw, not an implementation error or bug. We describe this type of attack as "active" rather than "passive" because of two essential differences in the nature of the attack:

- Attacker initiates the attack, rather than the victim
- Attacker control the target, rather than being limited by the extent of the victim's browsing activity.

Sleep Attack

Wireless sensor nodes have schedule time for transmission, reception of data and for idle listening. Some system set the sensor nodes schedule for sending and receiving the data and the time when the system will idle for energy conservation. To understand sleep attack we need to understand the two different modes of the schedule time:

1 **Active mode**: When the system is available for sending and receiving the messages, the sensor nodes are in active mode. Consumption of energy in active mode is more.
2 **Sleep Mode**: When the system is not available for sending and receiving the messages, the sensor nodes are in sleep mode. Energy consumption is less during sleep mode.

In case of sleep deprivation attack the attacking node doesn't allow the node to go under sleep mode. It will send data during sleep mode of a sensor node which keeps sleep mode in active mode and thus energy consumption increases and hampers the life time of network.

4. Flowchart Showing Technique to Prevent Denial of Sleep Attack

Algorithmic form of above flowchart is as follow:

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

Forward message in the network as it is a valid message.
Otherwise,

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

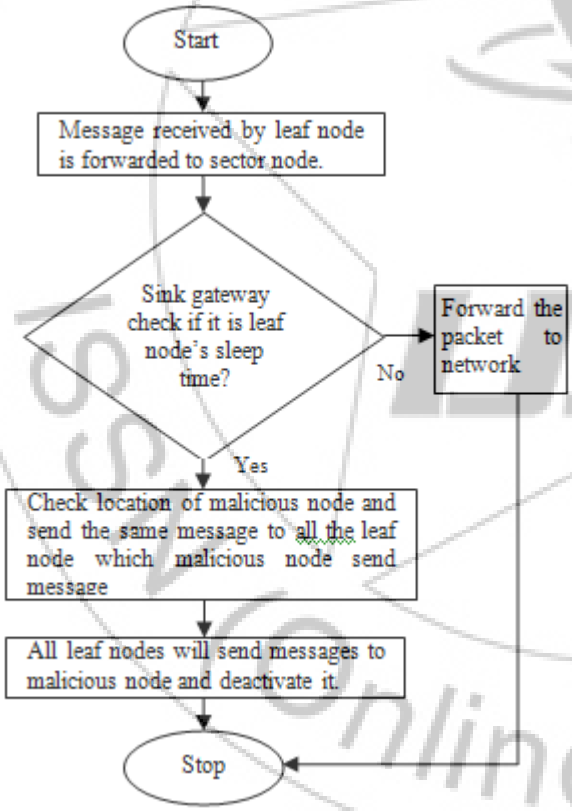


Figure 2: Flowchart of technique to prevent sleep deprivation attack

5. Results and Experiment

In figure 3 node number 6 is victim node and node number 11 is attacking node. When packet is arrived from attacking node, node 6 becomes active despite of its sleep mode schedule and packet is forwarded to sector in charge node which will check the time schedule of leaf node 6 and mark packet as invalid and send to sink. Sink node will detect attacking node and send information of its location to nearby leaf nodes. Leaf node will send packets to attacking node and make it deactivate. The scenario of implementation is shown in fig. 3.

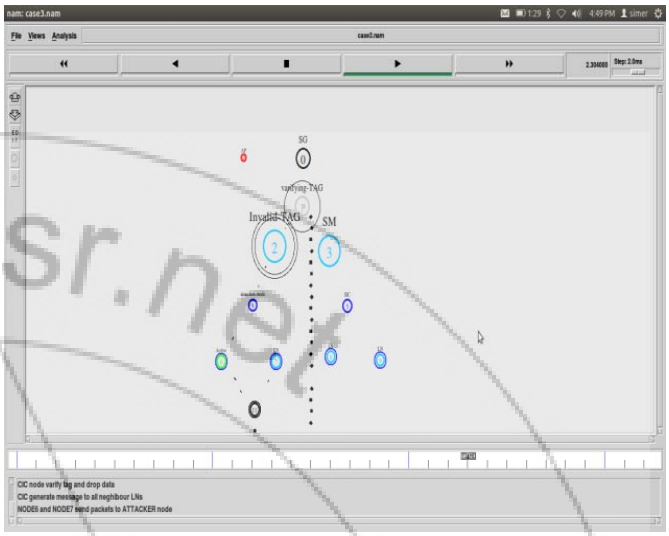


Figure 3: Implementation scenario of sleep attack's prevention.

When attack occurs all other leaf nodes will get notification from sector in charge. Then all leaf nodes will start to send packets to attacking node so that this attacking node becomes dead. The scenario showing attacking node as dead is shown in Figure 4.

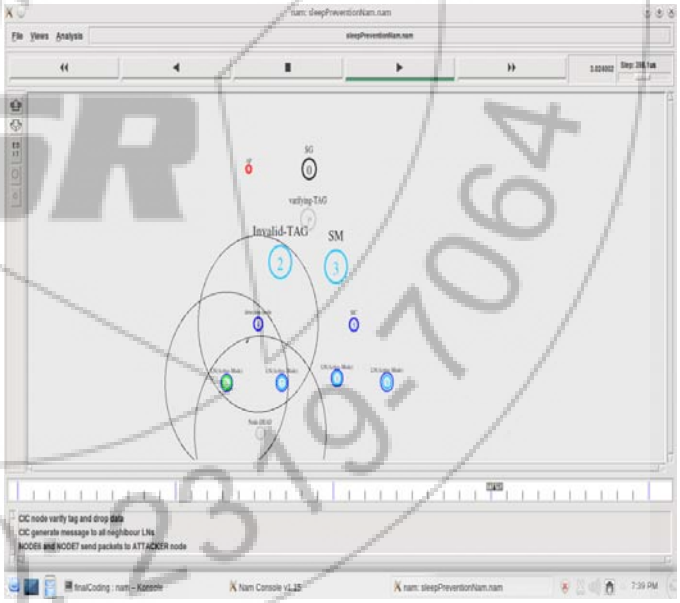


Figure 4: Scenario showing dead mlacious nodes

In figure 4 we can see that malicious node which was represented by node 11 is in gray color which represent that this malicious node is dead now as its energy has been consumed.

The energy at each moment of time of leaf node 6 is calculated for both scenarios sleep attacking scenario and prevention scenario shown in graph shown below. The red line in following graph is for sleep attacking scenario and

green line is for sleep prevention scenario. As we can clearly see that energy of leaf node 6 in sleep prevention scenario is long lasting as compared to energy of leaf node in sleep attack scenario.

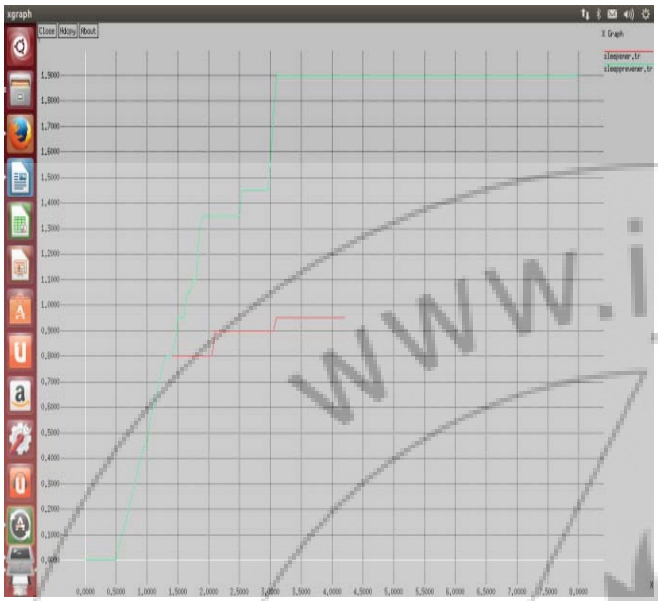


Figure 5: Comparison of energy of victim node in sleep attack and its prevention

6. Conclusion

Energy-constrained sensor networks periodically place nodes to sleep in order to extend the network Lifetime. Denial of sleep attacks is a great threat to the lifetime of sensor networks as it prevents the nodes from going into sleep mode, due to which it hampers the networks life time. So a step has been taken to prevent sleep deprivation attack. Also the comparisons of energy in both cases is done which clearly shows the prevention steps taken are helping in long lasting of network.

In future, we can work on following points:

1) More work can be done on some new techniques so as to save more energy in sleep deprivation attack.
2) The more attacks can be studied and different prevention measures can be taken upon them also.
3) Moreover as we have worked on sleep attack in cluster based network, but in future sleep attack and its prevention can done on non-clustered network.
4) Also impact of this attack can be seen on mobile ad-hoc network models using different mobility models.

References

[1] David R.Raymond and Scott F.Midkiff Virginia tech, “Denial of service in wireless sensor networks: attacks and defenses”, Pervasive Computing, IEEE vol 7 no1 pp74-81 2008.
[2] Manju.V.C, “Mechanisms for detecting and preventing denial of sleep attacks on wireless sensor networks”, IEEE Conference on Information & Communication Technologies (ICT), pp.74-77 2013.
[3] Michael Brownfield, 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, pp.356-364, 2005.
[4] David R. Raymond, Member, IEEE, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, “Effect of Denial of sleep attacks on Wireless Sensor Network MAC protocols” IEEE Transactions on Vehicular Technology, vol 58 no 1, pp. 367-380,2008.
[5] Raymond D. R., Midkiff S. F, “Clustered Adaptive Rate Limiting: Defeating Denial-Of-Sleep Attacks In Wireless Sensor Networks”, Military Communications Conference(MILCOM), IEEE, pp. 1-7,2007
[6] Chen C., Hui L., Pei Q., Ning L., Qingquan P. “An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks”, Proceedings of the 2009 Fifth International Conference on Information Assurance and Security, Vol. 02, 2009.
[7] Tapalina Bhattasali, Rituparna Chaki, Sugata sanyal, “Sleep deprivation Attack Detection in Wireless Sensor network”, International Journal of Computer Applications, vol 40 no 15 pp. 19-25,2012.
[8] Tara deep kaur, and Jinsuk Baek, “A Strategic deployment and Cluster-Header Selection for Wireless sensor networks.” IEEE Transactions on Consumer Electronics, Vol. 55, No.4, pp 1890-1897, 2009.
[9] Fang- Jing Wu and Yu-Chee Tseng “Distributed Wake-up Scheduling for Data collection in tree-based wireless sensor networks” IEEE Communications letters, Vol. 13, No.11, pp 850-852, 2009.
[10] Nok Hang Mak and Winston K.G. Seah “How long is the lifetime of a wireless sensor network?” International conference on advanced networking and application,pp 763-770, 2009.
[11] Qing Bian, Yan Zhang and Yanjuan Zhao “Research on Clustering Routing Algorithms in Wireless Sensor Networks” International conference on Intelligent Computation Technology and Automation, vol 2, pp.1110-1113,2010.
[12] Bhattasali, T. “SEGNET: Secure Geo-Sensor Network Model”. arXiv preprint arXiv:1209.6262.,2012
[13] Bhattasali, T., Chaki, R., & Sanyal, S. ,“Sleep Deprivation Attack Detection in Wireless Sensor Network”, arXiv preprint arXiv: 1203, 0231.,2012
[14] Abbasi, A. A., & Younis, M., “A survey on clustering algorithms for wireless sensor networks”, Computer communications, vol 30 no 14-15, pp. 2826-2841, 2007.
[15] Abuarqoub, A., Alfayez, F., Hammoudeh, M., Alsboui, T., & Nisbet, A. “Simulation Issues in Wireless Sensor Networks: A Survey”, In SENSOR COMM 2012, the Sixth International Conference on Sensor Technologies and Applications pp. 222-228, 2012.
[16] Pirretti M., Zhu S., Vijaykrishnan N., Mcdaniel P., Kandemir M., Brooks R., “The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense”, International Journal of Distributed Sensor Networks, Vol. 2, Issue 3, pp. 267-287, 2006.
[17] Premkumar K., Kumar A., “Optimal Sleep-Wake Scheduling for Quickest Intrusion Detection using Sensor Networks”, The 27th Conference on Computer Communications; IEEE INFOCOM 2008, 13-18 April

2008, Phoenix, AZ, USA,pp. 1400-1408, ISBN: 978-1-4244-2025-4. [10] Bhattasali T., Chaki R.: "Lightweight Hierarchical Model.

[18] S.Bandyopadhyay and E.J. coyle, "An energy-efficient hierarchical clustering algorithm for wireless sensor networks," in INFOCIM, vol. 3, 2003, pp. 1713-1723.

[19] M. Brownfield, K. Mehrjoo, A. Fayez, and N. Davis, "Wireless sensor network energy-adaptive MAC protocol," In IEEE CCNC, pp.778-782,2006.

[20] C.Rajni and G.Vrinda, "Energy Efficient Sleep Scheduled Clustering & Spanning Tree Based Data Aggregation in Wireless Sensor Network", 1st Int'l Conf. on Recent Advances in Information Technology, pp 536-541, 2012.

Author Profile

Gurjeet Kaur received the B.Tech degree in Information Technology from Chandigarh Engineering College, Landran during 2008- 2012 and M.Tech degree in Computer Science Engineering from Sri Guru Granth Sahib World University, Fatehgarh Sahib during 2012-2014 respectively.

Er. Simarjeet Kaur is working as Assistant Professor in the department of Computer Science and Engineering at Sri Guru Granth Sahib World University, Fatehgarh Sahib. Her educational qualifications are B.Tech (IT) from Guru Nanak Dev Engineering College and M.Tech in the field of Computer Science & Engineering from Punjab Agricultural University, Ludhiana. She has published a number of research papers in leading International Journals. She has experience of teaching under graduate and post graduate students.