ISSN 2348 - 2249
Volume-2, Issue-2, June-2014
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

Detection of Sleep Deprivation Attack In Sensor Networks: A Review

Gurjeet Kaur
Research Scholar, Department of Computer Engineering
SGGSWU, Fatehgarh Sahib
India
cec.it.3025@gmail.com

Simarjeet Kaur
Department of Computer Engineering
SGGSWU, Fatehgarh sahib
India
er.simarjeet@yahoo.in

Abstract **-** Development of sensor network is in hostile environment make it mainly vulnerable to battery drainage attack. So nodes battery is impossible to recharge or replace the power of the battery. Nodes battery power is easily affected by attacks cause of random drainage of the energy level of the sensor. The sleep deprivation attack is very dangerous. The main goal of the interrupter is to reduce the battery power of the sensor nodes and reduce the lifetime of the nodes. This attack is decrease the throughput. The present need of the day is to detect the interrupter for saving energy of nodes. In this paper we are discuss about detection of sleep deprivation techniques.

Keywords **-** Sleep and Wake up Strategies, Sensor Network, Energy Efficiency, Medium Access Control (MAC), wireless network.

I. INTRODUCTION

Wireless sensor network consist of several nodes where nodes are connected to one or more sensor nodes. The sensor nodes are based on the battery powered and having very limited amount of energy capacity. The sensor node having a limited processing and storage capacity, and thus can only perform limited computational functionalities. We present two attacks: barrage attack, sleep deprivation attack. Barrage attack is attack on the victim node with the valid request. The purpose of this request is to waste the node power by cause it to stay out of sleep mode and perform the energy intensive operation. In sleep deprivation attack the malicious node attack on the victim node to forcefully awake the victim node. When victim nodes are kept awake but are not made the energy intensive operation. Barrage attack is spending more energy it is easily detected. Now we focused on the sleep deprivation attack. This attack is difficult to detect, in network maximum security can be achieved by designing an effective detection model whose purpose is to provide alert about possible attack, idently in time to stop the attack. We have our survey of recent IDS in sensor network [1] stand alone IDS each nodes independent on the instruction. The distributed ID mechanism can be implemented in sensor network because of load distributed which reduce the single node overhead and gives the better performance in term of important parameter such as energy consumption response time, detection accuracy. But IDS is not efficient to found the sleep deprivation attack. For this purpose a distributed collaborative detection model is based on layered architecture.

II. RELATED WORK

Pirretti M. et al. [5]. It is discussed that attacker node must become cluster head to dispatch the sleep deprivation attack. It can allow the nodes to enter in the sleep mode to saving the energy of nodes. We have three different methods to reduce this attack Random vote scheme, round robin scheme and hash based scheme. There is ability to reduce the attacker attack. The amount of time is required for cluster head and the amount of time is required to perform these three methods.

Raymond D. R et al. [6] adoptive rate limiting approach network traffic is limited only when the malicious node is attack. It can be used to maintain the network lifetime and throughput when it is fae of sleep deprivation attack.

Chen C. et al. [7] RSSI measurement aid is the fake schedule switch scheme. The sensor node can reduce and weaken the harm from exhaustion attack and on the opposite make the attacker loss their energy quickly then die.

S.Bandyopadhyay et al.[9,10] cluster algorithm a node that have not received a request of cluster, after certain amount of time then declare itself to be a cluster head. Cluster head then start request to the neighboring nodes to join its cluster. To maintain the cluster we predict two vulnerabilities with this approach. In first during cluster formation attacker could select a cluster head by immediately request to the other nodes to join this cluster. Second once an attacker node has been selected as cluster head it can remain cluster head indefinitely by never selection a sensor.

There are different amount of initial energy. That is some of the sensor nodes have more power and they also can be strategically located in other place. The remaining energy of the sensor nodes is different at any given time depending on their particular position and functionality.

III. DETECTION TECHNIQUES

A. *Round Robin Scheme*

The cluster formation then used the round robin scheme. This scheme is used because lack of scalability in random vote scheme. This scheme were maintained the cluster for long period of time and single node maintain more state and get more scalable result. The cluster head could be chose round robin model. The round robin scheme is work in two part. First part is bootstrapping part, in which initialize the cluster and second is maintenance part in which updating of cluster and addition of new nodes and removal of the nodes.

ISSN 2348 - 2249
Volume-2, Issue-2, June-2014
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

Analytical Model: Consider an average of attacker node C and valid node n in each cluster. In proportion of time the sleep deprivation attack is launched by attacker node C in a cluster.

$$Pc,rr = C/C+n$$

In round robin scheme it required only one emphasis to select a cluster head. However in this scheme each node is maintained a list which node is in cluster or not. For maintaining this list each node required a very large amount of storage space and large cluster [6].

B. ***S-MAC*** *(Sensor MAC)*

It is designed to extend wireless sensor network lifetime. In S-MAC the time frame is divided into two parts one is listening and other is sleep mode. The listening period is further divided into a synchronization period and transfer period. The synchronization period allows nodes to periodically announce their sleep schedule to correct network time drift. Synchronization their sleep time to form virtual cluster with the same active listen and sleep period. It is used fixed duty cycle with a default 10%. In this time the traffic is exchange between nodes. The network life time is extended with throughput and latency trade off.

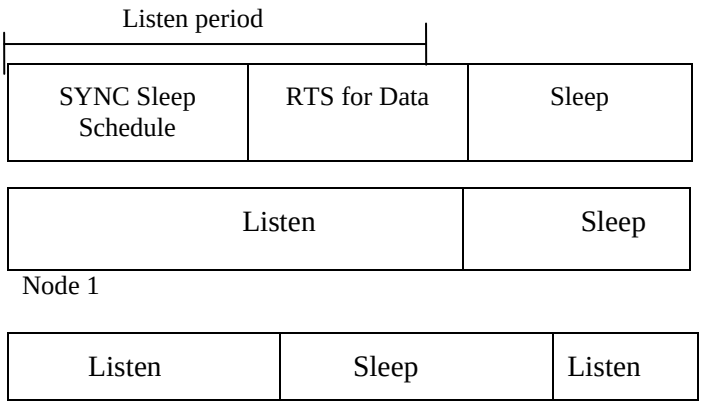

Fig. 1 S MAC Frame architecture [3]

In fig. 1 Node 1 try to transmitting to node 2 late in node 1 listen period; node 2 is in sleep period. It is not receiving the message. For all network traffic creating slotted start time the main concentration on time frame reduce, idle listening, trading latency and throughput. S MAC is reduces the energy consumption using message technique and sleep cycle is fixed. This limitation is cause of protocol to be inflexible to network traffic respond and network scaling. The fixed sleep cycle protects network life from sleep attack and nodes are only open for attack to fixed listening period [3].

$$T_{frame} = T_{listen} + T_{sleep}$$

$$D = T_{listen} / T_{frame}$$

D = duty cycle =10%

The attacker can be transmitting a message to whole network then maximum lifetime of network

S MAC is increase the tenfold of lifetime.

.

$$T_{network\ lifetime} = T_{sensor\ life} = \frac{C_{batter}}{D\ (I_{action}) + (1\text{-}D)\ (1_{sleep})}$$

C. ***T-MAC*** *(Timeout MAC)*

This is energy saving MAC protocol. It is improvement of S-MAC. It is obtained addition sleep mode to improve the throughput and latency. T-MAC used same synchronization mechanism to form the virtual cluster and message passing same as S-MAC. A node are in sleep mode TA is allows the node to transition when there are less traffic in the cluster. TA is set based on the longest time that a hidden node would have to wait before hearing the beginning of a CTS response message.

$$TA = 1.5 * (C + R + T)$$

The waiting timeout period is determined by the length of the contention interval C. The time to send RTC packet is R. The time between RTC packet and start of CTS packet is T. SIFS is the small interframe spacing. 1.5 is scaling factor to generate stable network. The arrow is shows sending and receiving message. The lifetime of this protocol is depends on how much traffic in network. It shows fivefold more lifetime the S-MAC. T MAC is more accessible to attack, if the attacker knows that this is T MAC network the nodes repeating receive transmission message. The attacker can force all node to create is 100% duty cycle [3].

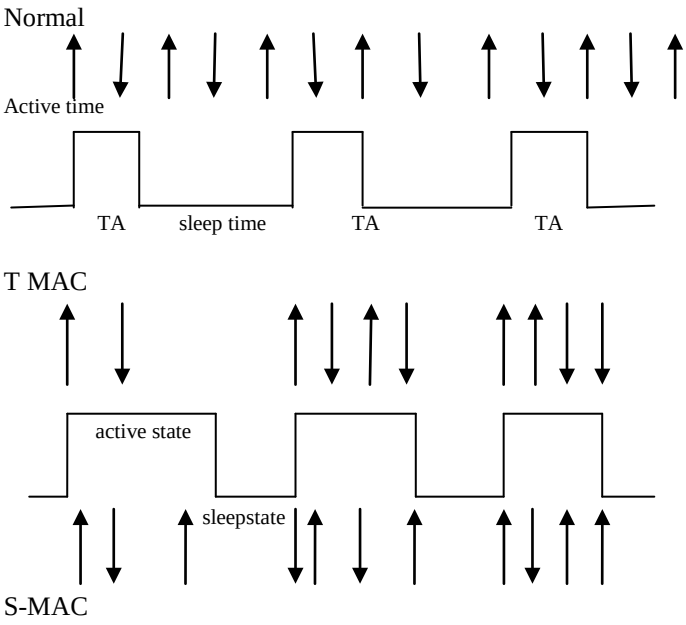

Fig. 2 T-MAC adaptive timeout [3]

D. ***B-MAC*** *(Berkeley MAC)*

B-MAC is not form the cluster of nodes like S-MAC, T-MAC. It is decentralized sleep schedule is allows the nodes to adopt any sleep schedule. It is frequently fixed. It is used the low power listening technique to reduce the consumption of energy. In LPL node is walk for fixed interval and check wireless sensor network for valid preamble byte that indicate the pending data transmission of another node. A node sends the pending data and preamble. If it is longer than interval between receiver samples to ensure that all near nodes have the opportunity to receive the preamble and subsequent data message. The interval between the channel sensing is based on the average of network node degree and traffic in the

ISSN 2348 - 2249
Volume-2, Issue-2, June-2014
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

network. B-MAC could have duty cycle as low as 1% in a low traffic network [4].

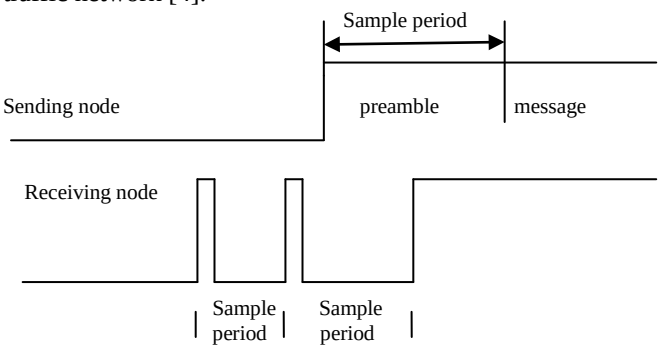

Fig. 3 B-MAC low power listening [3]

E. **G-MAC** (Gateway MAC)

GMAC is an energy efficient MAC protocol designed to equivalent transmissions within a cluster. G MAC frame structure, it is divide into two period distributions period and collection period. During the collection period nodes that have outgoing unicast traffic transmit a future RTS (FRTS) message to a Gateway. Traffic destined for other cluster is also transmitted to the gateway node during the contention period using an RTS/CTS/DATA/ACK exchange. At the end of the contention period the cluster head or gateway transmits a gateway indication message that provide a mechanism for cluster synchronization while broadcasting a schedule of message transaction between nodes than nodes exchange data during the contention free period. The gateway is elected using a periodic recourse adaptive election process in which node volunteer based on current resource level .new election is indicate by flag. Mac eliminates over heading, expect for a minimum amount of control traffic that a node might overhear while waiting to transmit an FRTS during the contention period [4].

IV. COMPARATIVE ANALYSIS OF SLEEP DEPRIVATION ATTACK DETECTION TECHNIQUES

TECHNIQUE	ADVANTAGE	DISADVANTAGE
Sensor MAC (S-MAC) [3]	It increase wireless sensor network lifetime	(a)Inflexible in responding to network scaling. (b)Fixed sleep cycle makes to unsafe to broadcast as well as unicast attack.
Timeout MAC (T-MAC)[3]	(a)Dynamic cycle make network scalable and flexible. (b)Energy saving is better.	It more unsafe to broadcast attack.
Berkley MAC (B-MAC)[3]	It is doing better work in ultra low traffic.	It performance is decreases because each passive node has to wake up and receive all message.
Gateway MAC (G-MAC)[4]	It is perform better than other in every traffic situation.	All cluster nodes depends on gateway.
Round Robin Scheme[5]	(a)In this attacker node cannot easily declare itself as cluster head. (b)It required single iteration to select cluster head.	For large cluster, each node requires an unrealistic amount of per storage, which enhances the over head.

Table: 1 Detection Techniques

V. CONCLUSION

In this paper the aim of propose model to save power consumption of the sensor node and extend lifetime of the network even in face of the sleep deprivation attack. GMAC technique is batter the other because the performance of GMAC is better in the all networks.

REFERENCES

[1]Tapalina Bhattasali, Rituparna Chaki, *"Sleep Deprivation Attack Detection in Wireless Sensor Network"*, International Journal of Computer Applications (0975 – 8887) Volume 40– No.15, February 2012.

[2] 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.

[3] Brownfield M .,Gupta Y .,Davis N., *"Wireless Sensor Network Denial of Sleep Attack"*, Proceeding of the 2005 IEEE, Workshop on information Assurance, united states Military Academy, West Point, NY , June 2005, DOI:10.1.1.133.8865.

[4] Raymond D. R., Marchany R. C., Brownfield M. I., Midkiff S. F., *"Effects of Denial-of Sleep Attacks on Wireless Sensor Network MAC Protocols"*, IEEE Transactions on Vehicular Technology, Vol. 58, Issue 1, pp. 367-380, January 2009.

[5] 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.

[6] Raymond D. R., Midkiff S. F., *"Clustered Adaptive Rate Limiting: Defeating Denial-Of-Sleep Attacks In Wireless Sensor Networks"*, Military Communications Conference, 2007, MILCOM 2007, IEEE, pp. 1-7.

[7] 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, IEEE CS, Washington DC, USA, ISBN: 978-0-7695-3744-3, DOI:10.1109/IAS.2009.33.

[8] 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.

[10] Bhattasali T., Chaki R.: "Lightweight Hierarchical Model.

[9] H.Chan and A.Perrig, *"ACE:An emergent algorithm for highly uniform cluster formation,"* in EWSN,2004.

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

