A Survey in Energy Drain Attacks and Their Countermeasures in Wireless Sensor Networks

Akhil Dubey, Vaishali Jain
M.Tech. Scholars, Dept. of Computer Science & Engg.
IEC-College of Engineering & Technology
Greater Noida, U.P., INDIA

Ashwani Kumar
Assistant Professor, Dept. of Information Technology
IEC-College of Engineering & Technology
Greater Noida, U.P., INDIA

***Abstract*--Now a day, wireless sensor networks is a prime field for the research. Its security issues attracts the scholars much more because its sensitivity and interactivity in terms of easy movable data in the adverse environment. In this field the main work is focused on different attacks which are related to nodes and deployment of the networks. Energy is the much costlier resource for these networks, so in this paper we are focusing on those attacks which are on power resources of the node by the advisory. Our prior motive is to explore the knowledge about the energy drain attacks. These types of attacks do not occur on the particular protocol stack but all existing protocols are easily affected with these classes of attacks which are ruining, plundering and not easy to detect. These attacks drain the energy of the node, reduce the life of the node and invite the other types of attacks. In this paper we survey different types of energy drain attacks and we discuss the methods to mitigate these types of attacks and holistic security approach for energy drain attacks.**

Keywords—Wireless Sensor Networks, Vampire Attacks, Denial of Sleep Attacks, Holistic Security

I. INTRODUCTION

In a human life wireless sensor networks is an important factor and a very use full technology. It becomes more and more decisive to the everyday functioning of people and organizations. Wireless sensor networks [1] are the combination of sensors nodes in which every node is depend on the battery power energy. In another word Wireless networks of numerous of thrifty miniature devices capable of communication, sensing and computation is called wireless sensor network. It Provide a link between the virtual worlds and real physical world. In wireless sensor network sensors are the soul of it and play an important role for gathering the data so it is also called as 'mote'. The sensors in a node provide the facility to get the data and the main goal of the applications is achieved by the cooperation of all sensor nodes in the network. The main application of the sensor networks are the Medical Application and the military applications of sensor nodes include monitoring, surveillance and battlefield guiding systems of intelligent missiles and detection of attack by weapons of mass destruction, applications to industry, science, transportation, civil infrastructure environmental monitoring, industrial applications, infrastructure protection application etc [2]. If we see the structure of the sensor node we find that there are six types of hardware memory, sensing device, processor, GPS, radio transceiver and power resources. If we see internally then we find that without power these sensors are become dead so energy and energy drain are the main constraint in wireless sensor networks. When sensor networks are randomly deployed in a hostile environment, security becomes extremely important factor. Because sensed data of sensor nodes is prone to different types of attacks which is done on the different layer of protocol stack like denial of services attack, selective forwarding attack, wormhole attack, sinkhole attack, Sybil attack, hello flood attack etc [3]. We have to provide the best security mechanism for all above these attacks. These security mechanisms take more resources and decrease the energy efficiency of network. So this condition provide favorable environment for the advisory, this time they do not attack on the protocol stack but they attack on the energy resources of the sensor so that security mechanism provides for the protocols attacks become less strong and network is again vulnerable for other different attacks. So in this paper we present the attacks on the energy resources.

So this paper is divided in five sections in 2nd we define the energy drain attacks and its defense schemes is presented in 3rd section, holistic security approach is in 4th section at last we conclude our paper in 5th section.

II. ENERGY DRAIN ATTACKS

As we told earlier sensor nodes are based on the battery resources, it is very difficult to change or recharge sensor node batteries. So the advisory provide the attacking environment or directly attack on the energy sources. The name 'energy drain' show the wasting of energy and making dead the node. Attackers may use malicious nodes to inject forgery or corrupt reports or data into the network or generate large amount of traffic in the network. So that this consume the energy of the node because Forgery reports will cause false alarms that waste real world response efforts, and drain the heavy amount of energy in a battery based network. The main goal of these types of attacks is to degrade the performance of the networks and destroying the networks. [4] There are two types of energy drain attacks.

A. Vampire Attack

In the wireless sensors networks vampires' attacks is the first class of attacks which is based on the routing in the sensor networks. In wireless sensor networks data is transmit node to node by a defined routing protocol. This attack is done on these routing protocols of the sensor networks by either continuous repeating the corrupt data or by choosing the long rout for sending the data [5]. This class of attack has two types which is given below

1) Carousel Attack

This is the first type of vampires attack class in which the attacking node transmit the forgery report in to the network and this transmit in circled way and create the routing loops. This attack aims the source routing protocols by utilizing the limited verification of message headers at forwarding nodes and allowing a single corrupt packet to repeatedly traverse the same set of nodes in a loop [6]. As we show in the figure 1. According to the figure we clearly see that source send the data packet which marked as 1to node A. Node A send it to node B. later on data packet transmit to other nodes in the network. But instead of transmitting the data to source from node E it transmits to node F and again transmits to node A. This is done due to the corruptness nature of the data packet which is transmitting by compromised source. After three circles data send to sink after 18th round. Due to this heavy wastage of energy occur. As we show in the figure.

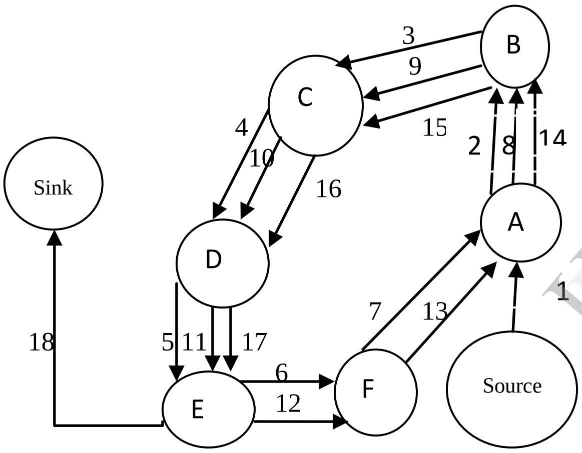

Fig 1. Malicious route construction attacks on source routing: carousel attack [6]

In this attack the routing of corrupt packet is fixed, it is predefine that how many circles are completed by data packet. It is done by the advisory. Now the next type of vampires attack class is stretch attack.

2) Stretch Attack

In this type of attack corrupt data packet choose the longest routing path instead of shortest path. In this attack an attacker define long routes artificially, potentially lying across every node in the network. We call it the stretch attack, since it increases data packet path lengths, causing data packets to be processed by a number of nodes that is independent of hop count along the shortest path between the source adversary and packet destination [7]. In the figure 2 we illustrated the working of the stretch attack by the given example. In this example we show the network of eight nodes in this figure we show the honest route by dotted line and malicious route by dashed line, link node E to sink is same for both routing. In this attack those node waste its energy that do not belong to the honest routing path.

Research [5] shows that in a randomly-generated topology, a single attacker can use a carousel attack to increase energy consumption by as much as a factor of 4, while stretch attacks increase energy usage by up to an order of magnitude, depending on the position of the malicious node.

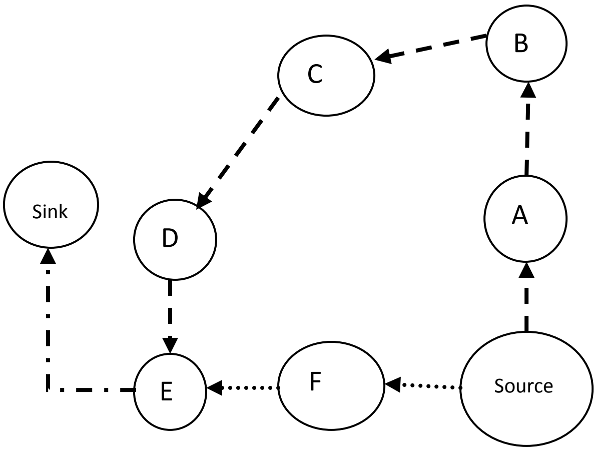

Fig 2. Malicious route construction attacks on source routing: stretch attack [7]

The impact of these attacks can be further increased by combining these two attacks, increasing the number of attacker nodes in the network, or simply sending more corrupt data packets.

B. Denial of Sleep Attacks (DS)

This is the second class of energy drain attack in this attack advisory used the legitimate data for wasting the energy by sending it either continuously or sending in a wrong way. Denial of sleep attacks (DS attack) is recognized as one of the most serious attack. The DS attack [8] is that targets a battery powered device's power supply in an effort to wear out this embarrassment resource and degrade the network life time. Denial of sleep attacks divided into six categories: sleep deprivation attack, barrage attack, synchronization attack, replay attack, broadcast attack and collision attack [9]. As we show in the figure 3.

1) Sleep Deprivation Attack

In the network every node send a request to send the data to its neighbor node after receiving the request receiver node check from its routing table if requesting node in its table the n it clear to send otherwise discard it and go to in sleep mode. As per the name of this attack malicious node continuously send the data, so that node does not go in the sleep mode and waste its energy [10].

2) Barrage Attack

In this attack attacker creates bombarding by the genuine requests to the victim node and waste the energy. The main difference between the sleep deprivation attack and barrage attack is in first attack attacker is in idle mode but in second attacker is in active mode [8].

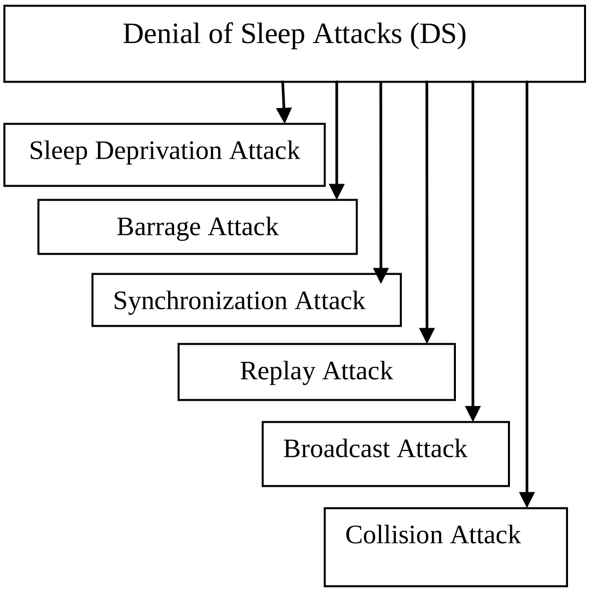

Fig 3. Classification of denial of sleep attack (DS)

3) Synchronization Attack

In this attack [11] attacker creates the disturbance in the synchronization of packet receiving and packet sending due to this the synchronization problems occur at the MAC layer and due to this node drain its battery power.

4) Replay Attack

In this attack all information which is in stored or recorded manner can be transmit again and again without any logical mean and waste the energy of the node.

5) Broadcast Attack

In this attack [12], malicious node broadcasts unauthenticated traffic into the network and reduce sensor nodes lifetime. In this attack long massage can be transmit in to the network to create the artificial traffic due to more drain of energy.

6) Collision Attack

This attack [13] can be easily attempt by an advisory through a malicious node. The malicious node does not follow medium access control protocol due to this collision occur with the neighbor node packet. After collision data packet has been lost and node has to send the data again due to this energy is wasted.

III. DEFENSE STRATEGIES FOR ENERGY DRAIN ATTACKS

In the last section we define the types of energy drain attack. In this section we will tell about the security schemes for the different types. First of all we discuss about the security against vampire attack.

A. Defense Schemes for Vampire Attack

One perfect security scheme proposed in [5] is PLGP. This scheme is based on fixed routing in which the moving of the data packet is pre define. Every node maintains a routing table in which there is an entry of data sending node so that only legitimate data move through the node. Now we see the defense scheme for the carousel attack and stretch attack.

1) Security Schemes for Carousel Attack

In [5] authors proposed no backtracking scheme. In this scheme authors design an algorithm which stops the repetition of data packet from the same node and same path. According to this algorithm node discard those data packet that is come more than one times.

2) Security Schemes for Stretch Attack

This attack is mainly performed on on-demand routing or optimal routing for the mitigation of this attack we use strict routing but it is not optimal and flexible. Most of networks use optimal routing so it is difficult to defend this attack.

B. Defense Schemes for Denial of Sleep Attack

This type of attack is mainly done through create artificial traffic in the networks so in [14] author proposed encrypted authentication scheme. In this scheme data packet can be send in the encrypted form and node transmit the data by secret key only. But this scheme create extra load on the processor

In [15] author gave the fake schedule switch scheme. To perform the denial of sleep attack attacker must know about the schedule of the victim node. To avoid the energy drain node transmit the fake schedule in the network so that attacker node has been confused and not performing its task. In addition to generation and the transmission of the fake schedule can bring more extra overhead to the network and reduce the energy efficiency [16].

One another technique proposed in [17] have four components: anti-replay protection, broadcast attack defense, strong link-layer authentication and jamming identification and mitigation.

A defense scheme proposed by Rainer Falk in [18] is secure wake-up scheme. According to this scheme only legitimate and authenticated data packet has the wake up token, node will only clear those request that has this token.

In [20] author proposed Artificial Immune System (AIS) approach and multiple-target tracking techniques. These schemes are used for find the intruder and the malicious nodes.

As we told first this attack is divided into six categories. So now we present the defense scheme for those six types.

1) Security Schemes for Sleep Deprivation Attack

One technique proposed in [9] for defend this attack states that all node must check the identity of the received data and the transmitter node. If it belongs to the routing table then clear it to send else discards it and enters in the sleep mode. In [10] author presented random vote scheme for cluster head topology.

2) Security Schemes for Barrage Attack

Defense scheme for this attack is proposed in [9]. This scheme is performed by rejecting the sending request that is come from the attacker node. We have identified the attacker node after the prevention of sleep deprivation attack. This scheme is like above scheme because both attacks have very miner difference. In [10] author presented the round robin scheme, and the hash-based scheme for cluster head topology.

3) *Security Schemes for Synchronization Attack*

Every synchronized massage has the identity of the sender. To prevent the synchronization attack if the sender doesn't exist in the neighborhood routing table that means it is an attacker so node ignores and rejects the corrupted synchronization messages come form that sender. In [11] authors introduced the threshold-based defense scheme. According to this scheme node reject those synchronized massage that has more relative time to sleep than expected clock drift threshold.

4) *Security Schemes for Replay Attack*

For the replay attack we compute RSSI (Received Signal Strength Indication) of received packets, then by combining RSSI value with neighborhood routing table we defend this attack. Form the RSSI value we can easily find out that which node transmit the data in a very high signal strength, that node is the malicious node and we can easily over come on the attack [9].

5) *Security Schemes for Broadcast Attack*

Due to the broadcast nature of wireless sensor network it is very hard to prevent this attack. In [9] author said that targeted node accept only the first data fragment and ignore remaining fragment if it entering in the sleep mode. Because every long massage has the identity in the first fragment of the node. If the node is malicious then victim node discards the massage.

6) *Security Schemes for Collision Attack*

This attack is done by creating the error in the coding of the nodes. So in [19] author present the error correcting code scheme for defending it.

IV. HOLISTIC APPROACH FOR SECURITY

Before we present holistic security approach for energy drain attacks first we see the meaning and definition of holistic approach. The purpose of holistic approach [21] is to improve the performance of wireless sensor networks with respect to longevity, security and connectivity under changing and hostile environmental conditions. The word holistic is present first time in 1810 by the father of homoeopathy Dr. Christian Friedrich Sumuel Hahnemann in his book Organon of Medicine. The basic mean of this word holistic is to provide one security mechanism for all types of attacks. In above section we present different security schemes for different types of attacks. In this section we present the one security scheme for all types of attacks.

A. *Holistic Security Approach for Vampire Attack*

The proposed holistic security scheme for vampire attack is an algorithm which is the combination of the PLGP and no backtracking scheme. However it is difficult to generate this combination. Because PLGP follows strict routing but no backtracking follows optimal routing. But according to this approach node that want to send the data to its sink node may send the sending request to all nodes in the network and then it found the acknowledgement from all nodes. With the help of acknowledgements node can find the minimum hop towards the sink node. Then this minimum weight way will be the fixed path from node to sink node. Source node broadcast this path so all node belong to this path make entry of sender and receiver node in to it routing table. And if there create a circle in the path then we can stop circling by no backtracking techniques. So source can send data with minimum energy.

B. *Holistic Security Approach for Denial of Sleep Attack*

However we present some security scheme in the above section like encrypted authentication but now we proposed light weight holistic security scheme. In this scheme node can check the signal strength because all attacker node send the data in a high signal. So we present the authentication with puzzle identification algorithm. According to this algorithm first we set the input signal strength. If a node receives data from the source node. It checks the signal strength of data packet. If signal strength of received data is equal to fixed signal strength in radio range than source node is classified as a true node accepts data packet and perform necessary function. If not than check another condition, If Signal strength of received data packet is nearly equal to fixed signal strength in radio range then nodes request an authentication identity and send a puzzle to source node, If authentication identity is correct and reply message of correct answers comes in fixed time threshold then Node is classified as a true node and accepts the request and performs function. If not than check signal strength of received message is greater than fixed signal strength in radio range then source node is classified as stranger and rejects the further requests from it. This scheme is all useful in detection for the intruder.

C. *One Holistic Security Approach for Energy Drain Attack*

In the research of attacks in wireless sensor network we found one thing that is most of the attacks are done through malicious node by the attacker like energy drain attack. In this attack every type of attacks are through malicious node. So according to this approach first we have to find that how many victim nodes are present in the network. So in [22] authors give the formula to calculate the average number of attacked nodes.

$$A= (N-1)\, \pi\, r^2 / a \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where, a is the area of the range region, N is the number of nodes in that region and r is the intruder transmission radius. After finding the victim node we can easily detect the false or malicious node by signal strength and geographical information is proposed in [23]. In this scheme we compare the actual signal strength and calculated signal strength according to the geographical information and fine the attacker node. If we find the malicious node then we easily overcome on both vampire attack as well as denial of sleep attack by this above singe scheme.

V. CONCLUSION

Wireless sensor network plays an important role in natural calamities. It was vastly use in environmental monitoring like through it we can effectively act to prevent the consequences of floods. The sensor nodes have been deployed in the river where nodes monitor the change of water level in real time. Sensor network also use at the time of earthquake. At the time of national disaster enemy country can attack on these networks, so it provide wrong information and disaster will become more horrible. So we have to defend all types of attack on WSN, energy drain attack is one of them. So in this paper we present the energy drain attack, vampires' attack, denial of sleep attack and different defense schemes proposed by many scholars time to time and holistic security approach. In future we implement these security schemes with holistic security approach on network simulator to check effectiveness of the security schemes.

ACKNOWLEDGEMENT

We all of us would like to dedicate this paper to our parents, without their blessings we cannot write the single word. We all of us would like to thanks Madam Anusha Dubey and our head of the department of our college.

REFERENCES

[1] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary," Wireless Sensor Network Security: A Survey", Security in Distributed, Grid, and Pervasive Computing Yang Xiao,(Eds.) pp. – - – © 2006 Auerbach Publications, CRC Press

[2] Kalpana Sharma, M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010

[3] Akhil Dubey, Deepak Meena, Shaili Gaur," A Survey in Hello Flood Attack in Wireless Sensor Networks", International Journal of Engineering Research & Technology (IJERT),Vol. 3 Issue 1, January – 2014,ISSN: 2278-0181

[4] Dr. Yudhvir Singh, Dheer Dhwaj Barak, Vikas Siwach, Prabha Rani,"Attacks on Wireless Sensor Network: A Survey ", IJCSMS International Journal of Computer Science and Management Studies, Vol. 12, Issue 03, Sept 2012 ISSN (Online): 2231-5268

[5] Eugene Y. Vasserman and Nicholas Hopper," Vampire attacks: Draining life from wireless ad-hoc sensor networks", University of Minnesota, IEEE

[6] Haowen Chan and Adrian Perrig, Security and privacy in sensor networks, Computer 36 (2003), no. 10.

[7] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensor network routing: A clean-slate approach, CoNEXT, 2006.

[8] F. Stajano, R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," In ICISC, Springer-Verlag, 2000

[9] Djallel Eddine Boubiche and Azeddine Bilami" A Defense Strategy against Energy Exhausting Attacks in Wireless Sensor Networks" JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE, VOL. 5, NO. 1, FEBRUARY 2013

[10] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. Mcdaniel, and M. Kandemir, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense," International Journal of Distributed Sensor Networks, 2: 267–287, 2006.

[11] L. Xiaoming, M. Spear, K. Levitt, N.S. Matloff, and S.F. Wu, "A Synchronization Attack and Defense in Energy- Efficient Listen-Sleep Slotted MAC Protocols," SECURWARE '08. Second International Conference on Emerging Security Information, Systems and Technologies, pp. 403-411, 2008.

[12] M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," In Proc. 6th Annu. IEEE SMC Inf. Assurance Workshop, pp. 356–364. 2005.

[13] Y.l. Law, "Link-layer Jamming Attacks on SMAC," Technical Paper, Univ. of Twente, NL, 2005.

[14] M. Stahlberg, "Radio Jamming attacks against two popular mobile networks," In Helsinki University of Tech. Seminar on Network Security, 2000.

[15] C.C. Li, H.Q. Pei, and L. P. Ning, Qingquan, "An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks," Fifth International Conference on Information Assurance and Security. pp. 446-449. 2009.

[16] Nils Hoeller, Christoph Reinke, Jana Neumann, Sven Groppe. Dynamic Approximative Caching Scheme for Energy Conservation in Wireless. Sensor Networks. Journal of Networking Technology, 2 (1); p. 10-21.(2011).

[17] 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, No. 1, pp. 367-380, January 2009.

[18] F. Rainer, and H. Hans-Joachim, "Fighting Insomnia: A Secure Wake-Up Scheme for Wireless Sensor Networks," Third International Conference on Emerging Security Information, Systems and Technologies, pp.191-196, 2009.

[19] Chaudhari H.C. and Kadam L.U."Wireless Sensor Networks: Security, Attacks and Challenges" International Journal of Networking Volume 1, Issue 1, 2011, pp-04-16 Available online at: http://www.bioinfo.in/contents.php?id=108

[20] J. Zhao, and K.E. Nygard, "A Two-Phase Security Algorithm for Hierarchical Sensor Networks," FUTURE COMPUTING 2011: The Third International Conference on Future Computational Technologies and Applications, pp. 144-120. 2011.

[21] Avancha, S, "A Holistic Approach to Secure Sensor Networks", PhD Dissertition, University of Maryland, 2005.

[22] D. Boubiche, and A. Bilami, "HEEP (Hybrid Energy Efficiency Protocol) Based on Chain Clustering," Int. J. Sensor Networks, Volume 10 Issue 1/2, pp. 25 - 35, 2011.

[23] Waldir Ribeiro Pires J´unior Thiago H. de Paula Figueiredo Hao Chi Wong Antonio A.F. Loureiro, (2004), MaliciousNode Detection in Wireless Sensor Networks, IEEE