International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 01,January-2015

Relationship between Attacks and Energy in WSN:Survey

Shweta Ghate
Department Of Information Technology
MIT College of Engineering
Pune, India.

Vivek Deshpande
Department Of Information Technology
MIT College of Engineering
Pune, India.

Anil Hiwale
Department Of Information Technology
MIT College of Engineering
Pune, India.

***Abstract*—Wireless Sensor Networks (WSN) is a collection of wireless nodes with limited energy capabilities. These nodes may be mobile or stationary and are located randomly on a dynamically changing environment. Deployment of sensor network in remote environment makes it mainly vulnerable to battery drainage attacks. It is impossible to recharge or replace the battery power of these sensor nodes. We have reviewed various papers which shows different attacks and their effects on energy consumption.We will be proposing new attack prevention method,which will be more energy efficient.**

Keywords:-Ad-hoc networks, low-power networks, routing, sensor networks, wireless networks.

I. INTRODUCTION

Ad-hoc Wireless Sensor Networks consist of sensors which are distributed in an Ad hoc manner. The sensor nodes performs the sensing tasks. These are interconnected with the wireless links. Every sensor is operational with some sensing, processing and communication components. Thus, when some event occurs (to be captured by sensor) it generates a report. This report is then forwarded to the sink; by some routing path over the network.Nowdays, WSN is part of our day to day life.

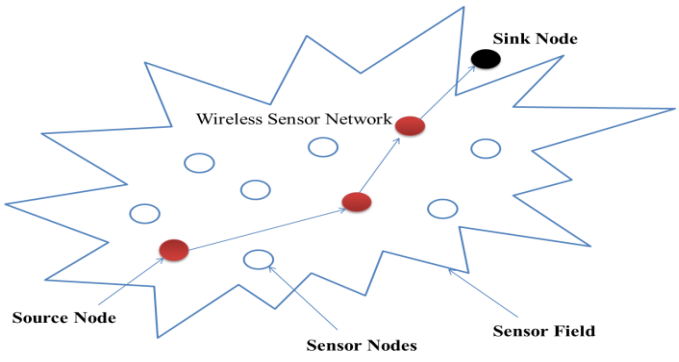

Figure 1: Wireless Sensor Network

Figure 1 shows the Wireless Sensor Network. These sensor nodes collect the data and process it under various environmental conditions such as under water in ocean,dense forest areas,desert areas and so on.WSN has some common application that includes battle field monitoring, critical asset tracking, wild-life monitoring, civic structure monitoring, forest-fire detection, home security networks, habitat monitoring, hospital or health networks, and so on.In above applications under various environmental conditions,keeping the physical location information of sensor nodes hidden from an attacker is difficult [1].The military application of sensor nodes include battlefield surveillance and monitoring, guiding systems of intelligent missiles and detection of attack by weapons of mass destruction.In these application securing the data of the sesor node is very important as such nodes contain the confidential data.Thus , security becomes a very important issue in WSNs.

Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Further they have an additional weakness because nodes are often placed in a hostile or dangerous environment where they are not physically safe.WSN are susceptible to attacks and threats such as Eavesdropping or passive information gathering, Node malfunctioning, Denial of service (DoS),[1],Directional anteena attack,Mallicious Discovery attack[2] and many more.

WSNs are highly vulnerable to the DoS attacks because of their Ad-Hoc nature [3]. Lot of research has been done to increase the survivability of these networks. These methods are useful in attacks having short-term network availability, but not so in the attacks with long term network availability. The longest DoS attack will drain the batteries of all nodes. In this type of resource depletion attack, the focus of attack is on the battery power. As battery is one of the main resource of any sensor node,such battery depletion attack is always dangerous as it drain all the power of the network.So preventing such attacks is very necessary.

II. RELATED WORK

WSN has gain popularity in recent year and has many application in day to day life, so security is main issues that must be handeled properly.Authors Vasserman and Hopper[2] has mentioned about the resource depletion attacks in their paper.Resource depletion attacks are those that permanently disable the network by draining the battery of the sensor nodes.They have mentioned about the " Vampire Attacks" that sucks the energy from the node.Vampire attack means creating and sending messages

by malicious node which causes more energy consumption by the network leading to slow depletion of node's battery life. The Vampire attacks are different from the traditional DoS, and routing infrastructure attacks. Because the vampire attacks will slowly suck the energy from the nodes, this in turn will cause the entire failure of the network, rather than disrupting the immediate availability. Though, some individual attacks are easy to prevent. Some power draining and resource depletion attacks have been researched . All the previous work done in this field was concerned with the application layer or the other level protocol stacks, like MAC. But surprisingly, there was only a little discussion and not the complete analysis of resource depletion attacks. Vampire attacks don't belong to the protocol-specific attacks family. In simple words, these attacks are neither dependent on the implementation faults nor on the design of the protocols. Instead, they expose basic properties of protocol classes. These attacks don't even depend on the message flooding technique, but as a replacement for this, they use as less data as possible to generate lot of energy drain. These attacks are very hard to detect and prevent, due to the usage of protocol compliant messages.

Vasserman and Hopper [2] made three essential commitments. Initially, they altogether assessed the vulnerabilities of existing protocols to routing layer battery exhaustion attacks. they watched that efforts to establish safety to avoid Vampire attacks are orthogonal to those used to ensure routing foundation, thus existing secure routing protocols, for example, Ariadne [4], don't ensure against Vampire attacks. Existing work at secure routing endeavors to guarantee that enemies can't result in way disclosure to give back an invalid system path. However Vampires don't disturb or modify found paths, rather utilizing existing substantial system ways and convention consistent messages. Protocols that expand power effectiveness are additionally wrong, since they depend on helpful hub conduct and can't streamline out noxious activity. Next, they have demonstrated that reproduction results evaluating the execution of a few agent protocols in the vicinity of a solitary Vampire (insider enemy). Also, they altered a current sensor system routing convention to provably tie the harm from Vampire attacks amid bundle sending.

Vampire attacks can be categorized in three groups; namely, Attacks on stateless protocols, attacks on stateful protocol, and PLGP. In the attacks on source routing protocols, the source nodes specifies the desired route for destination in the header's of packets. Using this path, intermediate nodes follows the given path, and not chose any other path. While forwarding a message, the intermediate node only forwards it to the next hop. The source has to be sure that the decided path is valid. This approach requires very less burden on the intermediate nodes about the path logic. And also, allows all the nodes in the route to be authenticated by the sender, similar to the Ariadne [4]. The two types of attacks are included in this, Carousel Attack and Stretch attack.

In carousel attack, the attacker sends the packet in the network. The route given for destination is consisting of a series of loops. In simple words, the packets routes between the intermediate nodes few times, and then reach the destination. Hence, it drains the energy of nodes with single message even if the message is not malicious; whereas, in stretch attack, the attacker intentionally generates the longer paths. In simple words, the path to destination is extended by adding unnecessary nodes. This will in turn add the burden on network, and will drain the batteries. In Stateful routing protocols, the network topology and its state is known to the network nodes. Network nodes make forwarding decisions using the stored state. There are two important classifications of, Link State and Distance Vector. OLSR [5] is a type of Link State protocols. Here, in network, the nodes keep records of states of links. Every time a link goes down, or a new link is added, the updating is made. But these networks are built dynamically. Therefore, the carousel and stretch attack have almost no effect in these networks. Still, the Stateful protocols need to face two types of attacks, namely, wormhole attack, and spurious route discovery attack.

PLGP [6] was supposed to be a secure network protocol for the WSNs. No special hardware was required for this protocol. Even in the environment containing active adversaries, it provided message delivery. This was designed as a central design parameter with security and efficiency. But the drawback of this protocol was its inability to satisfy no-backtracking. Thus, a new protocol was developed, called PLGPa. This protocol satisfied the no-backtracking. No-backtracking is an important term to be introduced here. It means that the number of honest nodes in the path is traversed by the packet from the journey to destination is independent of the malicious node activities, for each packet in trace. Somehow, no-backtracking provide resistance to the vampire attack. Therefore, the PLGPa is used, instead of PLGP [6].

S. H. Jokhio et al [1] proposed a Sensor node capture attack discovery and guard (SCADD) protocol to secure the WSNs from the node capture attacks. The proposed protocol comprises of two blocks:

1. Node attack discovery (NAD) block and
2. Defense Advocating measure (DAM) block.

The principal block helps in recognizing proof of the state or seriousness of the attack on a sensor node and the last includes taking protective measures against the attack. The author accept that the correspondence inside the WSN under attention is first secured by means of utilization of condition of-workmanship cryptographic strategies. The SCADD blocks are quickly examined next.

1. Node attack detection(NAD) block.

The vulnerability of that node raise to the greatest danger; if the estimation of the sensor node's physical area is acquired by the attacker. A node capture attack may be the aftereffect of one or more attacks did on the sensor node; for instance, Dos, node blackout, along these lines on ought to likewise

be considered as conditions perhaps prompting node capture. We assess the seriousness of the attack on the sensor node with the assistance of an attack seriousness demonstrate that comprises of states and state-conditions, separately. The attack seriousness is partitioned into three states:

i. The node is not captured.
ii. The node is going to be captured.
iii. The node has been captured.

While considering such attacks severity of the attacks on the node is measured. According to the application the severity of the attack varies.If the attack is of minimum severity it broadcasts the alter beacon.Whenever there is loss of communication or false authentication the alter beacon is broadcasted.There are other kind of messages that are red beacon which informs the node about the severity of the attack in the specific region,so to avoid the node capture attack.After detecting the severity of the attack the beacon is broadcasted and the DAM block gets stimulated.

2. Defense Advocating measure (DAM) block.

WSNs are regularly sent over huge geological regions. Immediate reconnaissance of sensor nodes to keep away from node capture attacks may not be a doable arrangement concerning securing hundreds and a great many sensor nodes. Likewise planning a great many alter safe sensor nodes may not be financially feasible. The author has propose a sagacious self-dangerous protocol that at first recognizes the seriousness of the attack and afterward takes guard measures against it by deleting indispensable data from memory of the sensor node.

Here the author has done all possible simulation and find out that the method proposed by them are cost effective in terms of processing overhead,memory overhead and energy consumption.The method shows less processing and memory overhead as well as very less energy consumption by the node.

Wenjun Gu et al [7] have recommended an end to end secure correspondence protocol in arbitrarily organized WSNs. The commitments of their work are given below:

Proposed a procedure called separated key pre-distribution for end to end secure correspondences in arbitrarily organized WSNs. This protocol is focused around this philosophy. The center thought of the strategy is to pre-distribute diverse number of keys to distinctive nodes. By circulating more keys to a few nodes, the connections between those nodes have a tendency to have much higher versatility than the connection flexibility under uniform key pre-distribution.

Designed another end to end secure correspondence protocol in WSNs. In this protocol, connections with high flexibility are favored rather than connections with low versatility during directing to sink node. Also, they apply elective way steering among high flexibility connections to accomplish great harmony between end to end secure interchanges and lifetime.

After doing continuous study on the defined protocol, authors has found the minimum way to differentially pre-distribute keys into node.The performance metric mentioned in the paper is based on the possibility of receiving a message by the sink from a sensor node without it being noticed by the invader.
Authors have also shown that their work is not susceptible to the biased node capture attack.The defined protocol known as End-To-End Communication Protocol has two component.First Component is Differential Key Management and Resilience aware routing .

A. Differential Key Management.

The Differential Key Management futher compromise of two phases i.e Key pre-distribution and Pairwise Key Distribution.In the Key pre- distribution phase ,the keys are distributed uniquely.Again the number of keys chosen from each class 1 node are balanced and differs by atmost 1.There are two reasons for pre- distribution of the keys.The one reason is that the chance of a class i node shares key with a class 1 node increases. and the other reason is that the chance of class I node shares the key with the non-class 1 node decreases.Above both particulars leads to increase link flexibility

B. Resilience Aware Routing.

Author has used the location centric routing protocol and Data centric routing protocol. The simple idea is to alter the routing protocols so that they consider link flexibility as a metric during routing.To prevent the extra use of the node ,the nodes have given the authority to choose the several next hop nodes.They have used the extension of location and data centric routing protocol,so as to achieve the high end to end secure communication without negotiating network lifetime.

Thus here the author has report the problem of providing end to end secure communications in arbitrarily organized WSN with the help of differential key pre-distribution ,whose idea is to distribute different number of keys to different sensors to improve the flexibility of certain links in the network. This feature is influenced during routing, where nodes make out route through links with higher flexibility.The author has presented end to end secure communication protocol based on the above approach by extending well known location centric (GPSR) and data centric (minimum hop) routing protocols.

Kwon and Hong[8] has shown that the delayed exposure of one-way chains is used as a base in µTESLA and its multilevel variants are used widely for securing the WSNs. µTESLA, is used with the parameters that are appropriate, number of future keys can be recovered by using cryptanalytic tradeoffs. Thus, to overcome this drawback, they have proposed a new eXtensible broadcast authentication technique called as X-TESLA. The base of this technology, is the cross authentication between two level chains with distinct intervals. This allows chains to work indefinitely and the chains are shorter as well. The one-way chain using the block-ciphers is also available.

This technique also proposes the commitment hopping strategies and the sleep mode management. In two levels of chains, the lower level chain basically authenticates the next upper level chain. These chains not only have the distinct intervals, but also have functionality to cross-authenticate each other. Thus, the X-TESLA overcomes the drawbacks of the previous TESLA versions. , like problems of sleep mode, network failures, and idle session etc. Also, provides the continuity indefinitely and securely. The technique can be combined with the public key techniques for more security.

Daojing He et al.[9] have discussed about code propagation in WSN in their paper.Various code propagation protocols have been proposed to broadcast new code images in WSNs.Here author have defined a new secure and distributed code dissemination protocol named DiCode.The proposed protocol has ability to resist denial-of-service attack,which is having sever costs on network accessibility.The author have proposed three important aspects in their scheme.Primarily they have measured denial-of-service attack on code propagation which have severe costs on network accessibility.Along with this they have recommended and applied two approaches to overthrow DoS attacks.Further, the recommended code propagation protocol is based on a safe and proficient proxy signature by warrant (PSW) technique,which make it stronger than the other scheme.Finally they have taken steps to avoid reprogramming conflict and support dynamic contribution.

A secure distributed code propagation protocol should fulfill the requirements like integrity of code images,freshness,Dos attack resistance,node compromise tolerance, along with this it should also satisfies the properties like distributed network, supporting different user privileges, partial reprogram capabilities, avoiding reprogramming conflicts, user tracebility,scalability and dynamic participation. For satisfying the above properties ,authors have proposed a practical secure and distributed code propagation protocol named *DiCode*, which is baised on the PSW technique.This protocol has three phases system initialization, user pre-processing, and sensor node verification. In system initialization phase the public and the private key is created by the network owner and then it delivers the proxy signature key to the authorized users. Before deployment of nodes the network owner's publick key is loaded into each node. The user pre-processing phase states that the every user must construct the code propagation packet of each new program image and then direct them to the nodes.

The nodes accepts the program image,if and only if the packet passes through the verification phase.The given protocol provide the functionality of restricting the number of reprogramming times of each certified user and more effective DoS attack resistance.

The author have implemented and evaluated the Dicode protocol on the parameters liked memory overhead,execution time and propagation delay.The method take very less ROM but take more memory space to store the public key and proxy signature.the execution time require is less for this method.There is linear increase in propagation delay,as the code image size increases.Thus the DiCode method is more efficient against the Dos attacks.

III. REVIEW

Study of various papers conclude that different authours have suggested various methods for security in WSN. The study conducted shows that there are many kinds of attack which drain the battery life of the node and degrade the quality of services of a network.These kind of attacks are really harmful and does not give reliability for transferring data in the network. Attacks like vampire attack, Node capture attack, directional antenna attack, Denial of Service attack degrade the quality of network by damaging it.

Every attack has a solution for its prevention and a method of defence. Many major steps are taken to detect, prevent, avoid and destroy the effect of these attacks. But these kind of attacks require considerable amount of cost. Previously many authors have defined various methods for preventing these kinds of attacks and has also made performance analysis of their methods.

Solutions given by various authors show good result, but there is still scope for improvement.So there can be different ways for improving these methods. A new approach for this kind of problem can be given by providing efficient algorithm.

IV. CONCLUSION

With rigorous survey of many papers, we can conclude that there are various attacks that drain the battery life of a node in the WSN resulting in reducing network life time.The papers shows various battery drainage attack and various methods for their prevention.For such attacks in future we can propose a method which will be more energy and cost effective.

V. REFFERENCES

[1] S.H. Jokhio ,I.A. Jokhio, A.H. Kemp, "Node capture attack detection and defence in wireless sensor networks", IET Wirel. Sens. Syst., Vol. 2, Iss. 3, 2012

[2] Eugene Y. Vasserman and Nicholas Hopper,"Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2, FEBRUARY 2013.

[3] A.D. Wood, J. A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", Dept of Computer Sc., University of Virginia, 2002.

[4] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", *Proc. MobiCom*, 2002

[5] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot, "Optimized Link State Routing Protocol for Ad-Hoc Networks", *Hipercom Project*, 2003.

[6] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure SensorNetwork Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf., 2006.

[7] Wenjun Gu, Neelanjana Dutta, Sriram Chellappan, and Xiaole Bai, "Providing End-to-End Secure Communications in Wireless Sensor Networks", IEEE transactions on network and service management, vol. 8, no. 3, september 2011.

[8] Taekyoung Kwon, Member, IEEE, and Jin Hong,"Secure and Efficient Broadcast Authentication in Wireless Sensor Networks",IEEE Transaction on Computers,VOL.59, No. 8, August 2010.

[9] Daojing He, Student Member, IEEE, Chun Chen, Member, IEEE,Sammy Chan, Member, IEEE, and Jiajun Bu, Member, IEEE," DiCode: DoS-Resistant and Distributed Code Dissemination in Wireless Sensor Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 11, NO. 5, MAY 2012

[10] H. Chan and A. Perrig, "Security and Privacy in SensorNetworks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[11] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks," Proc. Int'l WorkshopSecurity Protocols, 1999.

[12] M.G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," Proc. First ACM Workshop Wireless Security (WiSE),2002.

[13] B. Karp and H. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in Proc. ACM International Conf. Mobile Comput. *Netw.*, Aug. 2000.

[14] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of Quality (RoQ) Attacks on Internet End-Systems," *Proc. IEEE INFOCOM*, 2005.

[15] R. N. Duche, N. P. Sarwade, "Sensor Node Failure Detection Based on Round Trip Delay and Paths in WSNs", *IEEE Sensors Journal, Vol. 14, No. 2*, February 2014.

[16] S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford, "Path-Quality Monitoring in the Presence of Adversaries," *Proc. ACM SIGMETRICS Int. Conf. Measurement and Modeling of Computer Systems*, 2008.

[17] S.-H. Fang, C.-C. Chuang, C. Wang, "Attack-Resistant Wireless Localization Using an Inclusive Disjunction Model", *IEEE Transactions On Communications, Vol. 60, No. 5*, May 2012.

[18] Y.-K. Kwok, R. Tripathi, Y. Chen, and K. Hwang, "HAWK: Halting Anomalies with Weighted Choking to Rescue Well-Behaved TCP Sessions from Shrew DDoS Attacks," *Proc. Int. Conf. Networking and Mobile Computing*, 2005.

[19] Mauro Conti, Member, IEEE, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei, Member, IEEE, "Distributed Detection of Clone Attacksin Wireless Sensor Networks", IEEE Transactions On Dependable And Secure Computing, Vol. 8, No. 5, September/October 2011.

[20] Hong Huang, *Member, IEEE,* Nihal Ahmed, and Pappu Karthik," On a New Type of Denial of Service Attack in Wireless Networks:The Distributed Jammer Network", IEEE Transactions On Wireless Communications, Vol. 10, No. 7, July 2011.