A Survey of Resource Draining Attacks and Mitigation in Wireless Ad-Hoc Sensor Networks

Ms. Rashmi Jangre[1] , Mrs. R.R. Welekar[2] .

[1]*M. Tech Scholar, CSE Department, S.R.C.O.E.M, Nagpur, India*

[2]*Assistant Professor, CSE Department, S.R.C.O.E.M, Nagpur, India*

Abstract-- **Wireless ad-hoc sensor networks has become crucial for everyday functioning of people and organizations. Due to their ad-hoc organization they are vulnerable to denial-of-service attacks. The most permanent DoS attack is to entirely exhaust nodes' batteries, called "Vampire" Attacks. These vampire attacks are not impacting any specific kind of protocols. Detection of vampire attacks in the network is not easy. A single Vampire may even increase network energy usage by a factor of O(N),where N is the number of network nodes. We discuss existing routing protocols to mitigate resource draining attacks.**

Keywords--**ad-hoc, denial-of-service, sensor networks, wireless.**

I. INTRODUCTION

Wireless sensor networks are emerging as a widely used technology with evidence of their deployment in space ,educational, agriculture, domestic, commercial, military environments. WSNs are characterized with low power ,limited computational capabilities and limited memory nodes. Nodes battery is an important resource regarding ad-hoc networks.

Due to their ad-hoc organization, WSN is particularly vulnerable to Denial of Service attacks. The most permanent DoS attack is to entirely exhaust a node's battery .This is an example of Resource Depletion Attack, with battery power as a resource of interest. We call it "Vampire" attack since they drain the life from sensor nodes. These attacks are difficult to find`, prevent and can be easily carried out. They don't depend on design properties of particular routing protocols. These attacks are different from previously studied DoS attacks. They aim to transmit as little data as possible to entirely disable a network.

II.EXISTING SYSTEM

A. Routing Packets

The process of routing is initialized and done by the source node itself. The source node composes the route for transmitting the packet, The packet is forwarded hop-by-hop towards the destination. A vampire attacks as a composition and transmission of message this impact causes more energy to be consumed by the network that as well as the honest node transmitted a message of the identical amount to the same destination. The energy wasted during transmitting and receiving packets in the network while the malicious node present is much higher compared to all honest nodes forwarding the packets to the appropriate destination.

III. PROBLEM DESCRIPTION

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 .Vampire attack happens to be in the network with the help of malicious nodes. These malicious nodes affect the functioning of normal behaving nodes which causes the network energy to change abruptly. The malicious nodes has been placed in the network uniquely. First in between the routing nodes and the second placed in the Source node itself. The main problem is that these attacks are not easily identified , it takes some time to identify and make ensure that it is present in the network. They are mainly classified into two types: Carousel attack and Stretch Attack.

A. Carousel Attack

In this type of attack, attackers introduce some packet within a route tranquil as a sequence of loops, such that the packets repeatedly traverse the same set of nodes. The attack increases the routing length and delay very much in the network. It targets source routing protocols by exploiting limited verification of message headers at forwarding nodes.

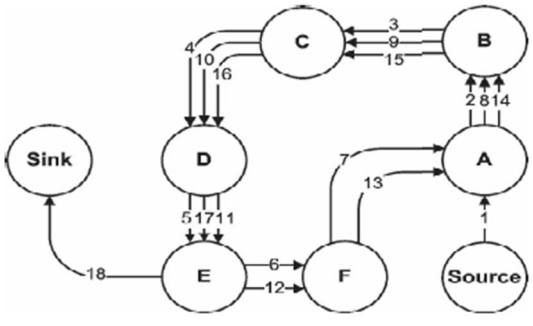

Fig. 1 Shows the carousel attack same node appears in the route many times

B. Stretch Attack

This attack also targets source routing protocols , attackers construct falsely long paths, potentially traversing every node in the network. We call it stretch attack because it increases packet path lengths. The honest route is very less distant but the malicious path is very long to make more energy consumption

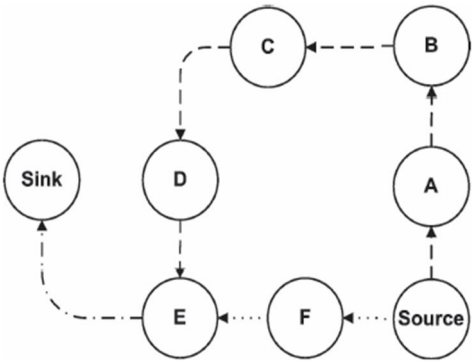

Fig. 2 Shows Stretch attack with two different paths from source to destination.(Source-A-B-C-D-E-Sink—long route)

IV.RELATED WORK

Prior work in this area has focused mainly on denial of communication at the routing or medium access control levels. Energy depletion attacks have not been addressed rigorously at the routing layer.

David et al .in [11] proposed Clustered Adaptive Rate Limiting(CARL) , a rate limiting approach which is based on current host-based intrusion detection techniques that is designed to defeat DoS attacks .Under CARL, network traffic is restricted only when malicious packets have been sensed at a rate sufficient to suspect that the network is under attack and take action to reduce the adverse affects on network lifetime imposed by these attacks.

Sonali et al. in [12] proposed a traffic filtering mechanism to curb Distributed denial of service attacks which aims to flood the network with ample packets to cause congestion .In this method, two components mitigation and compensation are adopted. When the traffic changes haphazardly within a shot time span, the rate is decreased by observing intensity of flow. When the rate of traffic drops below a certain point, compensation occurs where they get a chance to transmit the traffic in a normal manner, means their traffic rate is increased.

Su Man Nam as in [13] proposed SEF (statistical en-route filtering) scheme to detect false reports in intermediate nodes while forwarding processes. They used a black list to prepare a countermeasure against false report injection attack and three types of keys: an individual key for encrypting event information between a node and a base station, a pair wise key to maintain secure routing paths between the intermediate nodes, and a cluster key for detecting forged MACs between neighboring nodes of a cluster region. The experiment results show that the proposed method enhances energy savings more compared to the SEF in the sensor network.

Chakib et al. in [14] proposed H2BSAP that limits the effects of resource-depletion DoS attack to the one-hop neighbors of the attacker only, but introduces an acceptable extra computation and transmission overheads on the network. Unlike other time-asymmetry BSAPs, in which sensors first forward data, then later verify them, which let them susceptible to resource-draining DoS attacks, in *H2BSAP*, sensors buffer data, then later verify them, and forward them only if data is authentic.

Previous studies proposed to protect the network against denial of service attacks with the use of traffic monitoring agents on some nodes. But if the control nodes go down they leave the network unprotected. To better fight against attacks, Quentin as in [15] try to enhance this solution by introducing an energy-aware and secure method to select these monitoring nodes (called *c-Nodes*) in a clustered wireless sensor network. They suggested a workaround to designate new control nodes (named *v-Nodes*). These *v-Nodes* are responsible for monitoring the *c-Nodes* by periodically enquiring about their remaining energy and ensuring that they do not lie during the election process.

Yi Xu as in [3] proposed a new scheme for DoS mitigation which requires a node to undertake packet forwarding responsibility if it sends large amount of packets through other nodes. By placing this need, It becomes easy to differentiate normal nodes from malicious nodes, since a normal nodes is willing to undertake its responsibility while a malicious node would not. If a malicious node drops the packets , neighbors are able to detect it and then malicious node is isolated.

Eugene. Y. Vasserman as in [1] explores resource depletion attacks at routing protocol layer, which permanently breakdown networks by quickly draining nodes' battery power. This paper had not offered a fully satisfactory solution for Vampire attacks during topology discovery phase but suggested some intuition about damage limitations possible with further modifications to PLGPa.

L. Lakshmanan as in [4] proposed Modified destination Distance Vector (M-DSDV) protocol to prevent the draining of life from network nodes. In M-DSDV the data packets are temporarily stored in the nodes .When the packets are send to the neighboring node, the data stored in it will be deleted.

V. CONCLUSION

In this paper, we defined Vampire attack, a new class of resource draining attack ,that use routing protocols to permanently disable ad-hoc wireless networks by exhausting

nodes' battery power. A survey of various methods to mitigate resource draining attacks has been made but a fully satisfactorily solution to overcome Vampire attack has not been done. We can work in the direction for providing efficient algorithm to mitigate vampire attacks.

REFERENCES

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

[2] Gergely Acs, Levente Buttyan, and Istvan Vajda "Provably Secure OnDemand Source Routing in Mobile Ad Hoc Networks"-IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 5, NO. 11, NOVEMBER 2006.

[3] Yi Xu and Wenye Wang "Detecting and mitigating DOS attacks in wireless networks without affecting the normal behaving nodes"-IEEE 2007.

[4] L.Lakshmanan , Dr. D.C. Tomar "Secure Routing Protocol in wireless Sensor networks for vampire attack"-INDIAN JOURNAL OF APPLIED RESEARCH April 2014.

[5] Umakanth, J. Damodhar "Detection of Energy draining attack using EWMA in Wireless Ad Hoc Sensor Networks"-International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 8- August 2013 .

[6] G.Vijayanand, R.Muralidharan "Overcome vampire attacks problem in wireless ad-hoc sensor network by using Distance Vector Protocols"-International Journal of Computer Science and Mobile Applications,Vol.2 Issue. 1, January- 2014.

[7] Volkan Rodoplu, *Student Member, IEEE, and Teresa H. Meng, Fellow, IEEE* "Minimum Energy Mobile Wireless Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 17, NO. 8, AUGUST 1999.

[8] Jae-Hwan Chang, *Member, IEEE, and Leandros Tassiulas, Member, IEEE* "Maximum Lifetime Routing in Wireless Sensor Networks-IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 12, NO. 4, AUGUST 2004.

[9] Volkan Rodoplu, *Student Member, IEEE,* and Teresa H. Meng, *Fellow, IEEE"* Minimum Energy Mobile Wireless Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 17, NO. 8, AUGUST 1999.

[10] Tawseef Ahmad Naqishbandi and Imthyaz Sheriff C" A Resilient Strategy against Energy Attacks in Ad-Hoc WSN and Future IoT" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 2, February 2014.

[11] David .R.Raymond, Scott F. Midkiff " Clustered Adaptive Rate Limiting:Defeating Denial-Of-Sleep Attacks In Wireless Sensor Networks"-IEEE 2007.

[12] Sonali Swetapadma Sahu,,Pooja Priyadarshini,Saurabh Bilgaiyan "Curbing Distributed Denial Of Service Attack By Traffic Filtering In Wireless Sensor Network" 5th ICCCNT – 2014 July 11 - 13, 2014, Hefei, China.

[13] Su Man Nam, Tae Ho Cho "Energy Efficient Method for Detection and Prevention of False Reports in Wireless Sensor Networks"

[14] Chakib BEKARA and Maryline LAURENT-MAKNAVICIUS and Kheira BEKARA "H2BSAP: A Hop-by-Hop Broadcast Source AuthenticationProtocol for WSN to mitigate DoS Attacks" –IEEE 2008.

[15] Quentin MONNET, Lynda MOKDAD, Jalel BEN-OTHMAN "Energy-balancing method to detect denial of service attacks in wireless sensor networks" IEEE ICC 2014 - Ad-hoc and Sensor Networking Symposium.