Prevention of Energy Drain Attacksin Wireless Sensor Networks- A survey

Hetal Patel,
Student, masters of computer engineering, SCET, Gujarat, India
patelhetal2208@gmail.com

Professor Jayesh Chaudhary,
Assistant Professor, Computer engineering, SCET, Gujarat, India
jayesh.chaudhary@scet.ac.in

---***---

Abstract-Wireless Sensor Network (WSN) is a group of sensor nodes with limited battery power and limited storage capacity. WSN have many applications areas such as military, healthcare, agriculture, home security etc. There is a need for secure communication against the various attacks. Resource depletion is the main issue in wireless sensor network which permanently disable sensor node by draining nodes battery power[1]. Vampire attacks can cause serious damage in resource constrained, wireless sensor networks (WSNs). In this paper we survey different techniques Sensor network encryption protocol (SNEP), PLGPa, Energy Weight Monitoring Algorithm (EWMA), Interior Gateway Routing Protocol (IGRP) to prevent Energy Drain Attack (Vampire attacks)[2][5]. We find that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol-compliant messages.

IndexTerms—Wireless Sensor Network, denial of service, Vampire Attacks.

1. INTRODUCTION

Wireless Sensor Network (WSN) consists of several nodes where each node is connected to one or more sensor. WSN have many applications in important areas, such as the environmental monitoring, child education, military and warfare, homeland security, healthcare, agriculture, and manufacturing. Providing security for sensor networks is not an easy task. When compared to simple desktop computers or wireless devices, severe constraints exist since sensor nodes have limited storage, processing capability, and energy, and wireless links have limited bandwidth capacity.Low-power wireless networks are an exciting research direction in the sensing and pervasive computing. Prior security work has focused primarily on denial of communication at the routing or medium access control levels.

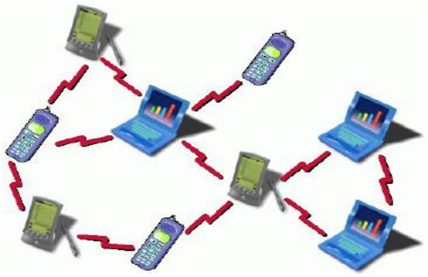

Fig.1 Wireless Sensor Ad-hoc Network (WSN)[4]

Due to distributed nature of these wireless Ad-Hoc networks and their deployment in the remote areas, these networks are exposed to many security threats that can seriously affect their proper functioning. Simple nature in Wireless Ad-Hoc networks with resource constrained nodes makes the network expose to different types of attacks. The attackersdisturb the flow of data by injecting extra bits in the channel, by eavesdropping on its communication channel, sending previously stored packets, sending false data and much more.

The only way to secure the WSN is to design the network in such a way that it supports all the security properties likeauthenticity, confidentiality, integrity, and availability.

Denial of Service (DoS) attacksand big deal of research is done to enhance survivability. These schemes can avoid attacks on short-term availability of network they do not target the attacks that affect long-term availability- the permanent DoS attack is to completely deplete nodes battery power. This is an example of resource depletion attack, with battery power of a node as the resource of interest. In this paper we have considered how the routing protocols designed to be secure, lack protection from these types of attacks, which we call as Vampire attacks, since they deplete the life of network nodes. These attacks are different from previously-studied Reduction of Quality (RoQ), DoS and routing infrastructure attacks as they do not disrupt immediate availability, but they work over time to entirely vanish a network.

Here we define a Vampire attack as the transmission and composition of messages that lead to more energy consumption by the network than honest node transmitted a message of same size to the same destination by using different packet headers. Vampire attacks do not depend on any protocol, design properties or implementation failures of particular routing protocols, but rather they exploit simple properties of protocol classes like distancevector,link-state, geographic and beacon routing and source routing. These attacks try to drain largest part of energy by transmitting as little data as possible data, preventing rate limiting solution. These attacks are difficult to detect or prevent because Vampires use protocol-compliant messages.

There are two types of Vampire attacks. In first attack, an attacker composes packets with purposefully introduced routing loops. This attack is called as Carousal attack. The second attack is also targeting source routing attacks, an attacker constructs artificially long routes, potentially traversing every node in the network, by increasing packet path lengths, causing packets to travel all the nodes which are independent of hop count along the shortest path between the attacker and packet destination. This attack is called as Stretch attack.

2. CLASSIFICATION OF ENERGY DRAIN ATTACKS (VAMPIRE ATTACKS)

Vampire attacks mainly divided in two category-(1)Attacks on Stateless Protocols and Attacks on Stateful Protocols.

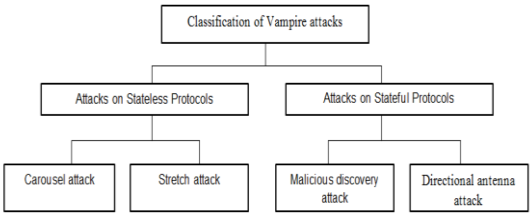
Classification of Vampire attacks
Attacks on Stateless Protocols
Attacks on Stateful Protocols
Carousel attack
Stretch attack
Malicious discovery attack
Directional antenna attack

Fig 2.Classification of vampire attacks

A.Carousel attack

In Carousel attack, adversary composes packets with purposely introduced routing loops. It sends packets in circles.

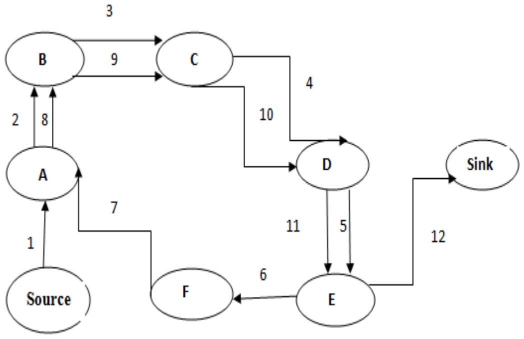

Fig 3.Stretch Attack [2]

Targets source routing protocols exploit the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes.

An adversary composes packets with purposely introduced routing loops. We call it the carousel attack, since it sends packets in circles. It targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes.

B. Stretch attack

In Stretch attack, an adversary constructs artificially long routes, potentially traversing every node in the network. It increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination.It alsotargeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network.We call this the stretch attack, since it increases packetpath lengths, causing packets to be processed by a numberof nodes that is independent of hop count along the shortestpath between the adversary and packet destination.

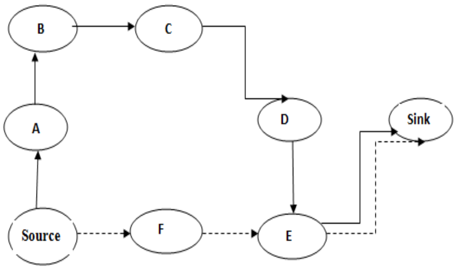

Fig4.Stretch Attack [2]

Stretch attacks increase energy usage depending on the position of the malicious node. The impact of these attacks can be further increased by combining them, increasingthe number of adversarial nodes in the network, or simply sending more packets. Although in networks that do not employ authentication or only use end-to-end authentication, adversaries are free to replace routes in any overheard packets, we assume that onlymessages originated by adversaries may have maliciously composed routes.

A 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. Few kinds of attacks are carousal and stretch attack. Carousal attack is one in which malicious node introduces loop in the path of packet travel purposely to drain the energy of honest nodes. Stretch attack is attack in which adversary causes packet to travel long distance than the needed to reach the destination leading to energy wastage. Thus both lead to consumption of energy unnecessarily.

3. LITERATURE SURVEY

A. Interior Gateway Routing Protocol (IGRP)

IGRP, a network protocol, developed by Cisco Systems, designed to work on autonomous systems. Each router sends all or a portion of its routing table in a routing message update at regular intervals to each of its neighbouring routers. A router chooses the best path between a source and a destination. Since each path can comprise many links, the system needs a way to compare the links in order to find the best path. A system such as RIP uses only one criterion hops to determine the best path. IGRP uses five criteria to determine the best path: the link's speed, delay, packet size, loading and reliability. It is considered, to find the route from source to destination.

Interior Gateway Routing Protocol in medium access control level to detect and deplete the attacks made during message passing in network. Need to protect the network against attacks [10][12]. It depletes this attack by discarding the attacked filebefore passing into the nodes from the source. IGRP finds the routing information which supports the IP routing. IGRP takes faster link where the hop count is same.

IGRP has a much larger maximum hop count than otherrouting protocols.This makes IGRP best suited for larger networks. It modifies an existing sensor network routing protocol to provably bound the damage from vampire attacks during packet forwarding. Since the routing protocol information proliferates through the network, routers can identify new destinations as they are added to the network, learn of failures in the network, and, most importantly, calculate distances to all known destinations.

IGRP provides a number of features that are designed to enhance its stability. To provide additional flexibility, IGRP permits multipath routing. IGRP uses a form of distance as its metric .IGRP uses the Bellman-Ford Distance Vector algorithm to determine the best path to a particular destination.

B.PLGPa[2]

A certifiable route history must be added to eachpacket of PLGP. This packet history is used by PLGPa along with tree routing structure of PLGP so every node can safely validate progress thatavoidsany major adversarial influence on the route which is taken by any packet which passes though atleast one sincere node. These signatures create a chain connected to each packet and permit any node receiving it to verify its route. Each transmitting node validates the attestation chain, to make sure that the packet has not at all travelled, in a logical address space, away from its destination.

No-backtracking is satisfied by PLGPa- Each Originator signs all their message. Attacker canonly modify fields of packet that are altered en- route, so only the path attestation field can bechanged, shortened, or eliminated completely. To prevent truncation one-way signaturechain construction is used. PLGPa never overflows and its packet transmitting overhead is favourable. It exhibits more equitable routing load distribution and route diversity. In the absence of hardware, even on 8-bit processors the cryptographic computation needed forPLGPa is tractable.

C. sensor network encryption protocol (SNEP)[5]

In ad-hoc network, the message authentication is important for many applications. Generally, an adversary can easily inject message, in this case the receiver needs to ensure that data used in any decision making process originate from a trusted source.

This encryption protocol ensures that which allows a receiver to verify that the data really was set by claimed sender and it also determines for attack prevention such as Data integrity and data freshness in order to provide packet delivery through key authentication, easily it will identify the malicious node to detects the attack such as stretch attack and carousel attack[5]. When forwarding packet to destination through intermediate, key also should be sent with message, but unfortunately the message is lost due to network availability. Because vampire which does not allow packet to destination. Instead, the malicious packet makes its way around the loop twice or more before exiting.

However, the secure network encryption protocol prevents vampire attack to ensure that packet delivery and maintain node battery power including with boundary recognition technique by merging recursive grouping algorithm and jump point algorithm during packet forwarding phase.

SNEP provides data confidentiality, two-party data is to send the counter along with each message. But since sensors and the communicating parties share the counter and increment it after each block, the sender can save energy by sending the message without the counter. At the end of this section we describe a counter exchange protocol, which the communicating parties use to synchronize their counter values. To achieve two-party authentication and data integrity, we use a message authentication code (MAC). There are three techniques used with sensor network encryption protocol (SNEP)[6].

BOUNDARY RECOGNITION TECHNIQUE:Suppose a large number of sensor nodes are scattered in a geometric region with nearby node communicating with each other directly in this case finding that boundary nodes is difficult in Ad-hoc network so introduced that boundary recognition to find boundary nodes by using only connectivity information and merging both algorithm.

JUMP POINT ALGORITHM:In Ad-hoc network, each node should determine itsneighbour node to transmit packet when discover the pathwith going through node but it takes more time for shortestpath discovery. In order to maintain time consumptionintroduced jump point algorithm which makes shortest pathdiscovery with less than 3 seconds without going throughnodes in Ad-hoc network.

RECURSIVE GROUPING ALGORITHM:Recursive Grouping algorithm proceeds in anasynchronous, distributed fashion to correctly detect nodeson the boundaries and connects them into meaningfulboundary cycle. It ensures that node addressing and routinginformation for neighbour nodes.

D. Energy Weight Monitoring Algorithm(EWMA)

In this method energy of each node is calculated continuously and malicious node is reaches threshold level. It sends ENG_WEG message to all nodes. Neighbouring nodes reply by ENG_RES message with current energy level. Then update routing table with current energy level. Sender node computes the energy required to transmit the data and established the path with minimum energy level and data routing.

4. COMPARISION

	Pros.	Cons.
IGRP	-More scalable than RIP -Its standardized counterpart that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations -Provides multipath routing	-Derivation of damage bounds and defenses for topology Discovery is not done
PLGPa	-Packet Constantly make progress in the direction of destination that bound from vampire attacks	-At the time of topology discovery phase completely acceptable solution for vampire attacks is not offered yet
SNEP	-It verifying that packets consistently make progress toward their destinations -It provides data confidentiality	-Not offered a fully satisfactory solution for Vampire attacks
EWMA	-Established the path with minimum energy level and data routing	-Continuously updating routing table with energy calculation so it takes time and memory space

5. CONCLUSION

In this paper we described basics of wireless sensor network and defined Vampire attacks, their effects on the networks, how these attacks permanently disable ad-hoc wireless sensor networks by using node's battery power. We have shown two types of vampire attacks: (1) Carousel attack and Stretch attack, which reduce the battery power of the nodes in a network, wastes bandwidth and time by forming loops or by travelling a long path than required in an ad-hoc network[5]. We studied different Techniques to prevent vampire attacks. But there is no method which isfully prevents the vampire attacks. So we can proposea method which prevents the vampire attacks.

REFERENCES

[1] Jae-Hwan ChanG, LeandrosTassiulas," Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 12, NO. 4, AUGUST 2004,PP. 609-619.

[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] David R. Raymond, Randy C. Marchany,"Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 1, JANUARY 2009.

[4] Sunil Bhutada, Manisha.K, KranthiKumar.K," A Novel Approach for Secure Routing Protocol: To Improve Life of Network," International Conference on Contemporary Computing and Informatics, IEEE,2014.

[5] E.Mariyappan, Mr.C.Balakrishnan,"Power Draining Prevention In Ad-Hoc Sensor Networks Using Sensor Network Encryption Protocol," IEEE,2014.

[6] AshishPatil, Rahul Gaikwad,"Comparative analysis of the Prevention Techniques of Denial of Service Attacks in Wireless Sensor Network," International Conference on mobile computing, IEEE,2015.

[7] David Martins and HervéGuyennet," Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey,"13th International Conference on Network-Based Information Systems,IEEE,2010.

[8] AbhishekChunawale, SumedhaSirsikar,"Minimization of Average Energy Consumption to Prolong Lifetime of Wireless Sensor Network,"13th International Conference on Network-Based Information Systems, IEEE, 2014.

[9] A.J. Goldsmith and S.B. Wicker, "Design Challenges for Energy- Constrained Ad Hoc Wireless Networks," Wireless Comm., vol. 9, no. 4, pp. 8-27, Aug ,IEEE, 2002.

[10] 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 Trans. Vehicular Technology, vol. 58, pp. 367-380, Jan. 2009.

[11] J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol. 12, no. 4, pp. 609-619, Aug. 2004.

[12] L.M. Feeney, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 6, no. 3, pp. 239-249, 2001.

[13] D.R. Raymond and S.F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7,pp. 74-81, Mar. 2008.

[14] Ye, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," IEEE/ACM Trans. Netw., vol. 12,pp. 493–506, Jun. 2004.