A Survey On: Detection & Prevention of Energy Draining Attacks (Vampire Attacks)

Mrunal R. Arjunkar
M. Tech
Department of CSE
P.I.E.T.
Nagpur, India
tushar443@gmail.com

A. S. Sambare
H.O.D
Department of C.Tech.
P.I.E.T.
Nagpur, India
ashishsambare@hotmail.com

S. R. Jain
Assistant Professor
Department of CSE
P.I.E.T.
Nagpur, India
sachinjain98440@rediffmail.com

Abstract:- **Survivability of network is its ability of being connected even under failures and attacks. Deployment procedure of a sensor network in the hostile environment leads it to battery drainage attacks, as it's impossible to recharge and even replace sensor node's battery power. The motivation provided for the research efforts has been given by an idea maximization of network lifetime, where the lifetime of network is measure of the instant of deployment to the point. When any of the nodes has exhausted its limited power source and becomes in-operational commonly referred as first node failure. Even a novel approach for routing protocols, affect from attacks those are designed to be protected, are unable to provide protection from these attacks, which call Vampire attacks. This is a class of resource consuming attacks which permanently disable the whole network by quickly draining battery of nodes. These attacks are not specific to any specific routing protocol, are disturbing, difficult to detect, and are very easy to carry out using as few as one malicious insider sending only protocol compliant messages. In this paper, we present the overview of work done by various researchers in their literature towards various attacks on wireless sensor networks and mainly focused on energy draining attacks (Vampire Attacks).**

Index Terms:- **Ad-hoc Sensor networks, Denial of service, Energy consumption, Routing, Vampire Attacks.**

I. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors. Which are used to monitor physical or even environmental conditions. The Conditions are temperature, sound, pressure, etc. They also cooperatively pass their data through the network to a main location. The modern networks are bidirectional, which also enabling control of sensory activities. The design and development of wireless sensor networks were motivated by military applications such as battlefield surveillance. Now, these networks are used in many industries and consumer applications, like industrial process monitoring and control, achine health monitoring, and many more. The WSN is made of "nodes" - from a couple of to many lots of or perhaps thousands, wherever every node is connected to 1 (or typically several) sensors. Every such sensing element network node has generally many parts: a radio transceiver with an interior associate degreetenna or association to an external antenna, a microcontroller, and associate degree electronic circuit for interfacing with the sensors associate degreed an energy supply, typically electric battery or associate degree embedded type of energy gathering.

A wireless ad hoc network could be a localized kind of wireless network. The network is ad hoc as a result of it doesn't trust a pre-existing infrastructure, just like routers are present in wired networks or access points are present in managed (infrastructure) wireless networks. Instead of tht every node participates in routing by forwarding knowledge for alternative nodes, that the determination of that nodes forward knowledge is formed dynamically on the idea of network property. Additionally to the classic routing, ad hoc networks will use flooding for forwarding knowledge. an ad hoc network usually refers to any set of networks wherever all devices have equal standing on a network and are liberal to come with the other ad hoc network device in link vary.

Due to the decentralized (ad hoc) nature, wireless ad-hoc networks are vulnerable to denial of service attacks (DoS) or distributed denial of service attacks (DDoS), which is an attempt to make a machine or network resource unavailable to its intended user. Researchers have researched in this field to a great extends, and provided a long stream of solutions. These solutions can prevent attacks on short-term network availability, but they are not effective in case of attacks that affect long-term network availability. Complete depletion of nodes' batteries is the most permanent DoS attacks, which is instance of *resource depletion attack* where battery power is interested resource. These attacks are known as *Vampire attacks.* These attacks are different from those of DoS, reduction of quality (RoQ) and routing infrastructure attacks. They do not disrupt immediate availability but work over time to shutdown network completely.

Vampire attack is defined as the composition and transmission of message that causes a lot of energy to be consumed by the network than if an honest node(unaffected node) transmitted a message of identiscal size to identical destination, though mistreatment totally different packet headers. The strength of attack can be measured by the ratio

of network energy used in the normal case to the energy used in malicious case. In the secure and safe case of vampire attack, the ratio is 1. Energy consumption of malicious node is not considered, as they can always drain their own batteries unilaterally.

II. Literature Survey

The analysis on this subject is usually turned around security solutions victimization stratified approach. Physical layer along with rest other layers named data-link, network, transport and application layer are the constituents of protocol stack within the stratified approach. The 3 planes (power management plane, mobility plane and task management plane) in conjunction with the 5 layers forms wireless stratified design. So as to boost the energy potency of wireless device networks, there's analysis physical phenomenon. A number of them are mentioned below:

A. Denial of sleep attack :

Michael Brownfield [1] discussed MAC level energy resource vulnerabilities. Denial of sleep attacks affects each sensor node's critical energy resources and rapidly drains the network's lifetime. A newly proposed G-MAC protocol controls the sleep awake pattern of sensor nodes. G-MAC has several energy saving features. In all traffic situations it performs well but deals only with MAC layer depletion attack

B. Intrusion tolerant routing :

The Jing Deng, Richard Han, Shivakanth mishra [2] proposed an Intrusion tolerant routing protocol. In INSENS each node shares a secret key only with the base station and not with any other nodes. INSENS constructs a forwarding table at each node to facilitate communication between sensor nodes and base station. Advantage in this case a node is compromised that an intruder will only have access to one secret key rather than the secret keys of neighbors and other nodes throughout the network. It provides multi path routing and minimizes the communication, at the expense of increased requirements at base station.

C. Cross layer approach :

Fatma Bouabdullah, Nizar Bouabdullah, Raouf Bouabdullah [3] has been proposed a cross layer strategy that considers MAC layers and routing jointly. Lifetime of network is time for the primary node in wireless sensor network to fail. AN economical routing protocol would drain energy slowly and uniformly among nodes resulting in the death of all nodes nearly at same time. At routing level they proposed that sending data through multiple paths instead of using a single path so can balance energy consumption. At MAC level limits the retransmission over each wireless links according to its property and the required packet delivery probability, but this scheme does not considers any attack.

D. Opportunistic routing method :

Xufei Mao, Shaojie Tang, Xiahua Xu & Huadong Ma [4] centered on opportunist technique to reduce energy consumption by all nodes however this technique doesn't contemplate any attack at routing level. Opportunist routing relies on the utilization of broadcast transmission to expand the potential forwarders that may assist within the retransmission of knowledge packets. By this technique nodes within the forwarder list are prioritized and therefore the lower priority forwarder can discard the packet if the packet has been forwarded by a better priority forwarder.

E. Optimal sleep-wake scheduling for intrusion detection :

K. Premkumar and Anurag Kumar [10] planned a protocol that uses mathematician call method models to spot the malicious nodes quickly with the utilization of smallest set of sensing element nodes in active state. By employing a smallest range of sensing element devices, it ensures that the energy expenditure for sensing, computation and communication is reduced so the life of network is maximized.

F. Sleep deprivation attack :

Tapaliana Bhattasali [5] planned a frame work supported distributive cooperative mechanism for detection sleep deprivation attack accrued energy potency however doesn't consider routing layer. Sleep deprivation torture comes within the type of causation useless management traffic and forces the node to forgo their sleep cycles so they're fully exhausted and thence shut down. Here employment is distributed among elements consistent with their capability to avoid complete exhaustion of battery power. Packet transmission overhead could high in some cases and its main advantage is it enhances energy potency and network measurability.

G. Defending against Path-based DoS Attacks in Wireless Sensor Networks :

Denial of service (DoS) attacks will cause serious damage in resource-constrained, wireless sensor networks (WSNs). This paper addresses an particularly damaging style of DoS attack, known as PDoS (Path-based Denial of Service) [11]. In an exceedingly PDoS attack, an adversary overwhelms sensor nodes a protracted distance away by flooding a multi-hop end-to-end communication path with either replayed packets or injected spurious packets. This paper proposes an answer exploitation unidirectional hash chains to safeguard end-to-end communications in WSNs against PDoS attacks. The planned solution is light-weight, tolerates bursty packet losses, and may simply be enforced in modern WSNs. The paper presents report on performance measured from a prototype implementation.

H. An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks :

A mobile ad hoc network (or manet) may be a cluster of mobile, wireless nodes that cooperatively form a network freelance of any fixed infrastructure or centralized administration. Especially, a manet has no base stations: a node communicates directly with nodes inside wireless range and indirectly with all alternative nodes employing a dynamically-computed, multi-hop route via the opposite nodes of the manet. Simulation and experimental results square measure combined to indicate that energy and bandwidth square measure substantively completely different metrics which resource utilization in manet routing

protocols isn't absolutely addressed by bandwidth-centric analysis. It presents a model for evaluating the energy consumption [13] behavior of a mobile ad hoc network. The model was accustomed examine the energy consumption of two well-known manet routing protocols. Energy-aware analysis of performance is shown to supply new insights into pricey protocol behaviours and suggests opportunities for improvement at the protocol and link layers.

I. Maximum Lifetime Routing In Wireless Sensor Network :
This paper show that the matter of routing messages in a very wireless sensor network therefore on maximize network lifetime [12] is NP-hard. In our model, the web model, every message should be routed while not information of future route requests. It develops conjointly an internet heuristic to maximize network lifetime. Our heuristic, that performs two shortest path computations to route every message, is superior to antecedently printed heuristics for lifespan maximization our heuristic leads to larger lifespan and its performance is a smaller amount sensitive to the choice of heuristic parameters. To boot, our heuristic is superior on the capability metrics.

J. An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks :
Attackers will render distributed denial-of- service attacks [14] tougher to defend against by bouncing their flooding traffic off of reflectors; that's, by spoofing requests from the victim to an oversized set of net servers that may inturn send their combined replies to the victim. The ensuing dilution of section within the flooding stream complicates the victim's talents each to isolate the attack traffic so as to dam it, and to use traceback techniques for locating the supply of streams of packets with spoofed supply addresses, like ITRA CE [Be00a], probabilistic packet marking [SWKA00], [SP01], and SPIE [S+01]. we have a tendency to discuss variety of potential defenses against reflector attacks, finding that the majority prove impractical, then assess the degree to that totally different kinds of reflector traffic can have characteristic signatures that the victim will use to spot and strain the attack traffic. Our analysis indicates that three varieties of reflectors cause significantly important threats: DNS and Gnutella servers, and TCP-based servers (particularly internet servers) running on TCP implementations that suffer from certain initial sequence numbers. we have a tendency to argue last in support of "reverse ITRACE" [Ba00] and for the utility of packet traceback techniques that job even for low volume flows, like SPIE.

K. Minimum Energy Mobile Wireless Networks :
This paper describes a distributed position-based network protocol optimized for minimum energy consumption in mobile wireless networks [15] that support peer-to-peer communications. Given any variety of randomly deployed nodes over a part, we tend to illustrate that a straightforward native optimization scheme executed at every node guarantees sturdy connectivity of the whole network and attains the world minimum energy solution for stationary networks. Owing to its localized nature, this proves to be self-reconfiguring and stays near the minimum energy solution once applied to mobile networks. Simulation results are wont to verify the performance of the protocol.

III. VAMPIRE ATTACKS

Vampire attack [6] represent of many attacks counting on protocol kind. They're as follows:

- Directional antenna attack. Main reason behind vampire attack is directional antenna attack. Vampires have very little management over packet progress once forwarding choices are made severally by every node; however they'll still waste energy by restarting a packet in varied parts of the network. There are 2 forms of vampire attacks supported this directional antenna attack. they're Stretch attack and carousel attack.
- Carousel attack: In carousel attack, associate degree adversary composes packets with intentionally introduced routing loops. It targets supply routing protocols by exploiting the restricted verification of message headers at forwarding nodes, permitting one packet to repeatedly traverse identical set of nodes.
- Stretch attack: In Stretch attack, associate degree resister constructs unnaturally long routes, potentially traversing each node within the network. It will increase packet path lengths; inflicting packets to be processed by form of nodes that's freelance of hop calculate the shortest path between the resister and packet destination.
- Malicious discovery attack. Another attack on all previously-mentioned routing protocols (including stateful and stateless) is spurious route discovery. In most protocols, each node can forward route discovery packets (and generally route responses as well), that means it's potential to initiate a flood by causation one message.

A clean-state secure detector network routing protocol is associate degree economical, extremely resilient to active attacks. This protocol [8] is introduced by Bryan Parno, Mark Luk, Evan Gaustad, Adrian Perrig (PLGP from here on). It's 2 phases, they're topology discovery section and packet forwarding section. the first version of the protocol, though designed for security, is susceptible to vampire attacks. Here PLGP may be changed to demonstrably resist. Vampire attacks throughout the packet forwarding phase.
PLGPa is that the protocol that bounds injury from vampire attack, however this has many drawbacks. they're outlined below PLGPa includes path attestations, increasing the dimensions of each packet, acquisition penalties in terms of information measure use, and therefore radio power. Adding additional packet verification necessities for intermediate nodes conjointly will increase processor utilization, requiring time, and extra power. Energy expenditure for cryptographical operations at intermediate hops is, abundant larger than transmit or receive overhead, and far a lot of smitten by the precise chipset accustomed construct the detector. whereas PLGPa isn't susceptible to vampire attacks throughout the forwarding section, however it doesn't

provide a satisfactory resolution throughout the topology discovery phase.

IV. REFERENCES

[1] Michael Brownfield, Yatharth Gupta, "Wireless Sensor Network Denial of Sleep Attack", Proceedings of 2005 IEEE workshop on information assurance, June 2005.

[2] Jing Deng, Richard Han, Shivakanth Mishra, "INSENS: IntrusionTolerant routing in Wireless Sensor Networks", University of Colorado, Department of computer science Technical report, June 2006 .

[3] Fatma Bouabdullah, Nizar Bouabdullah,Raouf Bouabdullah "Cross-layer Design for Energy Conservation in Wireless Sensor Networks", IEEE GLOBECOM 2008, New Orleans, USA, December 2008.

[4] Xufei Mao,Shaojie Tang, Xiahua Xu, "Energy efficient Oppurtunistic Routing in Wireless Sensor Networks", IEEE transactions on parellel and distributed systems, VOL. 12, NO. 2, February 2011

[5] Tapaliana Bhattasali,Rituparna Chaki,Sugata Sanyal "Sleep Deprivation Attack Detection in Wireless Sensor Networks", International journal of computer applications(0975-8887)vol. 40- No: 15,February 2012

[6] Eugene Y. Vasserman, Nicholas Hopper, " Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", IEEE transactions onmobile computing, VOL. 12, NO. 2, February 2013

[7] Yazeed Al-Obaisat,Robin Braun, "On Wireless Sensor Networks: Architectures, Protocols,Applications and Management", Institute of Information and Communication Technologies,May 2004

[8] B.Prano, M.Luk, E.Gustad, A.Perrig, "Secur Sensor Network Routing: A Clean-state Approach", CoNEXT:Proc.ACM CoNEXT Conf.,2006

[9] D.B. Johnson, D.A Maltz, J.Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Adhoc Networks", Adhoc Networking, Addison Wesley, 2001

[10] K. Premkumar and Anurag Kumar, "Optimal sleep-wake scheduling for quickest intrusion detection using sensor networks", IEEE explore, February, 2008

[11] J. Deng, R. Han, and S. Mishra, "Defending against Path-Based DoS Attacks in Wireless Sensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.

[12] 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.

[13] 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..

[14] Vern Paxson, An analysis of using reflectors for distributed denial-of-service attacks, SIGCOMM Comput. Commun. Rev. 31 (2001), no. 3

[15] Volkan Rodoplu and Teresa H. Meng, "Minimum energy mobile wireless networks", IEEE Journal on Selected Areas in Communications 17 (1999), no. 8.