Vampire Attacks: Draining Life From Wireless Ad Hoc Sensor Networks

H.Bharani I
Assistant Professor
Department of Information Technology
Karpaga Vinayaga College of Engineering Technology, Chinna Kolambakkam, Madurantakam Taluk, Kanchipuram-603308, Tamilnadu, India

M.Kanchana
Assistant Professor
Department of Information Technology
Karpaga Vinayaga College of Engineering Technology, Chinna Kolambakkam, Madurantakam Taluk, Kanchipuram-603308, Tamilnadu, India

S.B.Dhivya
Assistant Professor
Department of Information Technology
Karpaga Vinayaga College of Engineering Technology, Chinna Kolambakkam, Madurantakam Taluk, Kanchipuram-603308, Tamilnadu, India

V.Kavitha
Assistant Professor
Department of Information Technology
Karpaga Vinayaga College of Engineering Technology, Chinna Kolambakkam, Madurantakam Taluk, Kanchipuram-603308, Tamilnadu, India

I.Vinnarasi Tharania
Assistant Professor
Department of Information Technology
Karpaga Vinayaga College of Engineering Technology, Chinna Kolambakkam, Madurantakam Taluk, Kanchipuram-603308, Tamilnadu, India

Abstract

Ubiquitous on-demand computing power, continuous connectivity, and instantly deployable communication for military and first responders are some of the exciting applications for future technology which securely works in wireless ad hoc Networks. Direction in sensing and pervasive computing is the basic process in which wireless networks works. Wireless ad hoc networks are particularly vulnerable to denial of service (DoS) attacks, and a great deal of research has been done to enhance survivability. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. We consider how routing protocols, even those designed to be secure, lack protection from these attacks, which we call Vampire attacks, since they drain the life from networks nodes. These "Vampire" attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. 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. Mitigating these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase is introduced in this work.

Keywords: Vampire attacks, denial of service, draining life.

I. INTRODUCTION

Ad-hoc sensor network and routing data in them is a significant research area. There are a lot of protocols developed to protect from DOS attack, but it is not completely possible. As WSNs become more and more crucial to the everyday functioning of people and organizations, availability faults become less tolerable lack of availability can make the difference between business as usual and lost productivity, power outages, environmental disasters, and even lost lives; thus high availability of these networks is a critical property, and should hold even under malicious conditions. One such DOS attack is Vampire attack-Draining of node life from wireless ad-hoc sensor networks.

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. This attack is not specific to any protocol. Few kinds of attacks are carousal and stretch attack, since they drain the life from networks nodes. These attacks are distinct from previously studied DoS, reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but rather work over time to entirely disable a network. While some of the individual attacks are simple, and power draining and resource exhaustion attacks have been discussed before, prior work has been mostly confined to other levels of the protocol stack, e.g., medium access control (MAC) or application layers, and to our knowledge there is little discussion, and no thorough analysis or mitigation, of routing-layer resource exhaustion attacks.

Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these

attacks are very difficult to detect and prevent. We observe that security measures to prevent Vampire attacks are orthogonal to those used to protect routing Infrastructure. Vampires do not disrupt or alter discovered paths, instead using existing valid network paths and protocol-compliant messages. Protocols that maximize power efficiency are also inappropriate, since they rely on cooperative.

II. RELATED WORKS

We do not imply that power draining itself is novel, but rather that these attacks have not been rigorously defined, evaluated, or mitigated at the routing layer. A very early mention of power exhaustion can be found in [16], as "sleep deprivation torture." As per the name, the proposed attack prevents nodes from entering a low-power sleep cycle, and thus depletes their batteries faster. Newer research on "denial- of-sleep" only considers attacks at the medium access control (MAC) layer [14]. Additional work mentions resource exhaust- tion at the MAC and transport layers [15,17], but only offers rate limiting and elimination of insider adversaries as potential solutions. Malicious cycles (routing loops) have been briefly mentioned [4, 13], but no effective defences are discussed other than increasing efficiency of the underlying MAC and routing protocols or switching away from source routing. Even in non-power-constrained systems, depletion of re- sources such as memory, CPU time, and bandwidth may easily cause problems. A popular example is the SYN flood attack, wherein adversaries make multiple connection requests to a server, which will allocate resources for each connection request, eventually running out of resources, while the ad- versary, who allocates minimal resources, remains operational (since he does not intend to ever complete the connection handshake). Such attacks can be defeated or attenuated by putting greater burden on the connecting entity (e.g. SYN cookies which offload the initial connection state onto the client, cryptographic puzzles [3, 12]). These solutions place minimal load on legitimate clients who only initiate a small number of connections, but deter malicious entities who will attempt a large number. Note that this is actually a form of rate limiting, and not always desirable as it punishes nodes who produce bursty traffic but may not send much total data over the lifetime of the network. Since Vampire attacks rely on amplification, such solutions may not be sufficiently effective to justify the excess load on legitimate nodes. There is also significant past literature on attacks and defences against quality of service (QoS) degradation, or reduction of quality (RoQ) attacks, that produce long-term degradation in network performance [8,10]. The focus of this work is on the transport layer rather than routing protocols, so these defences are not applicable. Moreover, since Vampires do not drop packets, the quality of the malicious path itself may remain high (although with increased latency). Other work on denial of service in ad-hoc wireless net-works has primarily dealt with adversaries who prevent route setup, disrupt communication, or preferentially establish routes through themselves to drop, manipulate, or monitor packets [7,18]. The effect of denial or degradation of service on battery life and other finite node resources has not generally been a security consideration, making our work tangential to the research mentioned above. Protocols that define security in terms of path discovery success, ensuring that only valid network paths are found, cannot protect against Vampire attacks, since Vampires do not use or return illegal routes or prevent communication in the short term. Current work in minimal-energy routing, which aims to increase the lifetime of power-constrained networks by using less energy to transmit and receive packets (e.g. by minimizing wireless transmission distance) [5] is likewise orthogonal: these protocols focus on cooperative nodes and not malicious scenarios. Additional on power-conserving medium access control (MAC), upper-layer protocols, and cross-layer cooperation [9]. However, Vampires will increase energy usage even in minimal-energy routing scenarios and when power-conserving MAC protocols are used; these attacks cannot be prevented at the MAC layer or through cross-layer feedback. Attackers will produce packets which traverse more hops than necessary, so even if nodes spend the minimum required energy to transmit packets, each packet is still more expensive to transmit in the presence of Vampires. Our work can be thought of attack-resistant minimal-energy routing, where the adversary's goal includes decreasing energy savings. Deng et al. discuss path-based DoS attacks and defences in [6], including using one-way hash chains to limit the number of packets sent by a given node, limiting the rate at which nodes can transmit packets. While this strategy may protect against traditional DoS, where the malefactor overwhelms honest nodes with large amounts of data, it does not protect against "intelligent" adversaries who use a small number of packets or do not originate packets at all. As an example of the latter, Aad et al. show how protocol-compliant malicious intermediaries using intelligent packet-dropping strategies can significantly degrade performance of TCP streams traversing those nodes [1]. Our adversaries are also protocol-compliant in the sense that they use well-formed routing protocol messages. However, they either produce messages when honest nodes would not, or send packets with protocol headers different from what an honest node would produce in the same situation. Another attack that can be thought of as path-based is the wormhole attack, first introduced in [30]. It allows two non- neighbouring malicious nodes with either a physical or virtual private connection to emulate a neighbour relationship, even in secure routing systems [2]. These links are not made visible to other network members, but can be used by the colluding nodes to privately exchange messages. Similar tricks can be played using directional antennas. These attacks deny service

III. PROPOSED METHOD

We made three primary contributions. First, we thoroughly evaluate the vulnerabilities of existing protocols to routing layer battery depletion attacks. We observe that security measures to prevent Vampire attacks are orthogonal to those used to protect routing infrastructure, and so existing secure routing protocols. We will assume that a node is permanently disabled once its battery power is exhausted, let us briefly consider nodes that recharge their batteries in the field, using either continuous charging or switching between active and recharge cycles. In the continuous charging case, power-draining attacks would be effective only if the adversary is able to consume power at least as fast as nodes can recharge. Assuming that packet processing drains at least as much energy from

the victims as from the attacker, a continuously recharging adversary can keep at least one node permanently disabled at the cost of its own functionality.

A. ADVANTAGES

- Cannot optimize out malicious action like maximize power efficiency of network, which is inappropriate.
- Ensure that the route is valid at the time of sending, and that every node in the route is a physical neighbour of the previous route hop.

B. MODULES DESCRIPTION

1) Adversaries and Honest node Module

All routing protocols employ at least one topology discovery period, since ad hoc deployment implies no prior position knowledge. Limiting ourselves to immutable but dynamically organized topologies, as in most wireless sensor networks, we further differentiate on-demand routing protocols, where topology discovery is done at transmission time, and static protocols, where topology is discovered during an initial setup phase, with periodic rediscovery to handle rare topology changes. Our adversaries are malicious insiders and have the same resources and level of network access as honest nodes. Vampire in terms of the "maliciousness" of the adversary, or the induced stretch of the optimal route in number of hops. This reduces cumulative network energy, or almost the entire lifetime of a single node. Therefore, the stretch attack increases the effectiveness of an adversary by an order of magnitude, reducing its energy expenditure to compose and transmit messages. Forwarding nodes using minimum-energy routing could replace long distance transmissions with a number of shorter distance hops, but the attack still works since the malicious path is longer. Rate limiting also potentially punishes honest nodes that may transmit large amounts of time-critical (bursty) data.

C. Loop Detection Module

One of the attractive features of source routing is that the route can it is better to simply drop the packet, especially considering that the sending node is likely malicious (honest nodes should not introduce loops). The described attacks are only valid within the network "neighborhood" of the adversarial node. An alternate solution is to alter how intermediate nodes process the source route. To forward a message, a node must determine the next hop by locating itself in the source route. If a node searches for itself from the destination backward instead from the source forward, any loop that includes the current node will be automatically truncated (the last instance of the local node will be found in the source route rather than the first). No extra processing is required for this defense, since a node must perform this check anyway, we only alter the way the check is done.

D. Loose Source Routing

We can define loose source routing, where intermediate nodes may replace part or all of the route in the packet header if they know of a better route to the destination. This makes it necessary for nodes to discover and cache optimal routes to at least some fraction of other nodes, partially defeating the as-needed discovery advantage. Caching must be done carefully lest a maliciously suboptimal route be introduced.

E. No-backtracking

Routes are dynamically composed of forwarding decisions made independently by each node. PLGP differs from other protocols in that packets paths are further bounded by a tree, forwarding packets along the shortest route through the tree that is allowed by the physical topology. No-backtracking implies that for each packet in the trace, the number of intermediate honest nodes traversed by the packet between source and destination is independent of the actions of malicious nodes. Equivalently, traces that include malicious nodes should show the same network wide energy utilization by honest nodes as traces of a network with no malicious actors.

IV. OUTPUT ANALYSIS

F. Access point connection

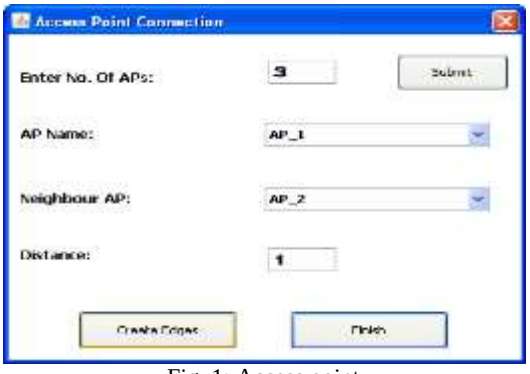


Fig. 1: Access point

Fig. 2: proxies

G. Instantiation

Fig. 3: Instantiation

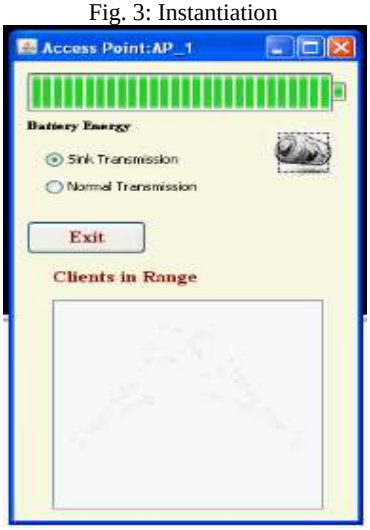


Fig. 4: Battery level

H. Login

Fig. 5: logging

I. File process

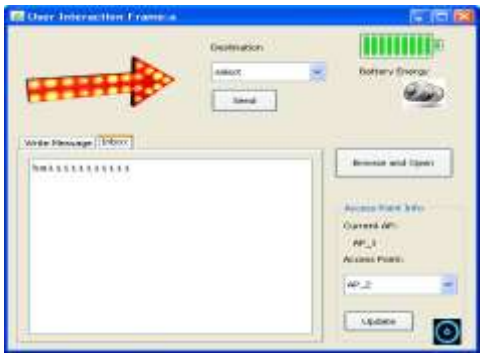


Fig. 6: File sending

J. Attacker entry

Fig. 7: attacker

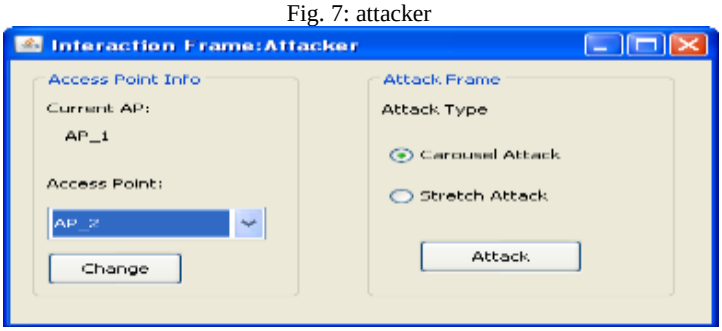


Fig. 8: attacker type

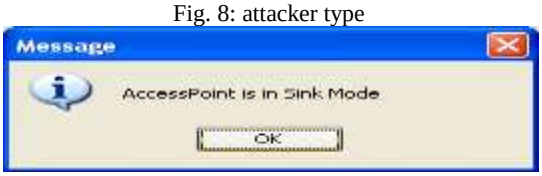


Fig. 9: access point mode

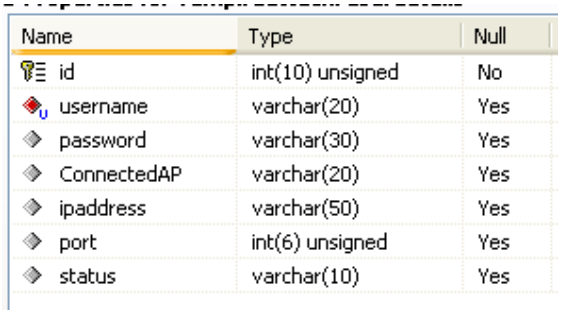
K. Back end details

Name	Type	Null
APName	varchar(20)	Yes
APindex	tinyint(3) unsigned	Yes
port	varchar(50)	Yes
ip	varchar(50)	Yes
Status	varchar(10)	Yes

Fig. 10: Access point

Name	Type	Null
APName	varchar(20)	Yes
NeighbourAP	varchar(20)	Yes
Distance	tinyint(3) unsigned	Yes

Fig. 11: graphs



Name	Type	Null
id	int(10) unsigned	No
username	varchar(20)	Yes
password	varchar(30)	Yes
ConnectedAP	varchar(20)	Yes
ipaddress	varchar(50)	Yes
port	int(6) unsigned	Yes
status	varchar(10)	Yes

Fig. 12: User details

V. CONCLUSIONS

In this paper we defined Vampire attacks, a new class of resource consumption attacks that use routing protocols to permanently disable ad-hoc wireless sensor networks by depleting nodes' battery power. These attacks do not depend on particular protocols or implementations, but rather ex- pose vulnerabilities in a number of popular protocol classes. We showed a number of proof-of-concept attacks against representative examples of existing routing protocols using a small number of weak adversaries, and measured their attack success on a randomly-generated topology of 30 nodes. Simulation results show that depending on the location of the adversary, network energy expenditure during the forwarding phase increases from between 50 to 1,000 percent. Theoretical worst-case energy usage can increase by as much as a factor of O(N) per adversary per packet, where N is the network size. We proposed defences against some of the forwarding-phase attacks and described PLGPa, the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. We have not offered a fully satisfactory solution for Vampire attacks during the topology discovery phase, but suggested some intuition about damage limitations possible with further modifications to PLGPa. Derivation of damage bounds and defences for topology discovery, as well as handling mobile networks, is left for future work.

REFERENCES

[1] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004.
[2] Gergely Acs, Levente Buttyan, and Istvan Vajda, Provably secure on- demand source routing in mobile ad hoc networks, IEEE Transactions on Mobile Computing 05 (2006), no. 11.
[3] Tuomas Aura, Dos-resistant authentication with client puzzles, Interna- tional workshop on securityprotocols,2001.
[4] Haowen Chan and Adrian Perrig, Security and privacy in sensor net- works, Computer 36 (2003), no.10.
[5] Jae-Hwan Chang and Leandros Tassiulas, Maximum lifetime routing in wireless sensor networks, IEEE/ACM Transactions on Networking 12 (2004), no. 4.
[6] Jing Deng, Richard Han, and Shivakant Mishra, Defending against path- based DoS attacks in wireless sensor networks, ACM workshop on security of ad hoc and sensor networks, 2005.
[7] INSENS: Intrusion-tolerant routing for wireless sensor net- works, Computer Communications 29 (2006), no. 2.
[8] Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, and Jennifer Rexford, Path-quality monitoring in the presence of adversaries, SIG- METRICS, 2008.
[9] Andrea J. Goldsmith and Stephen B. Wicker, Design challenges for energy-constrained ad hoc wireless networks, IEEE Wireless Communi- cations 9 (2002), no. 4.
[10] Mina Guirguis, Azer Bestavros, Ibrahim Matta, and Yuting Zhang, Reduction of quality (RoQ) attacks on Internet end-systems, INFOCOM, 2005.
[11] Packet leashes: A defense against wormhole attacks in wireless ad hoc networks, INFOCOM, 2003.
[12] Timothy J. McNevin, Jung-Min Park, and Randolph Marchany, pTCP: A client puzzle protocol for defending against resource exhaustion denial of service attacks, Technical Report TR-ECE-04-10, Department of Electrical and Computer Engineering, Virginia Tech, 2004.
[13] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensor network routing: A clean-slate approach, CoNEXT, 2006.
[14] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, Effects of denial-of-sleep attacks on wireless sensor network MAC protocols, IEEE Transactions on Vehicular Technology 58 (2009), no. 1.
[15] David R. Raymond and Scott F. Midkiff, Denial-of-service in wireless sensor networks: Attacks and defenses, IEEE Pervasive Computing 7 (2008), no. 1.
[16] Frank Stajano and Ross Anderson, The resurrecting duckling: security issues for ad-hoc wireless networks, International workshop on security protocols, 1999.
[17] Anthony D. Wood and John A. Stankovic, Denial of service in sensor networks, Computer 35 (2002), no. 10.
[18] Manel Guerrero Zapata and N. Asokan, Securing ad hoc routing proto- cols, WiSE, 2002.