IJDCST @Sep-Oct, Issue- V-2, I-8, SW-26
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Vampire Attacks: Improvised Mechanism For Controlling Strenuous Life From Wireless Ad-Hoc Sensor Networks

Santhi Babu Devarapalli, Thirumala Reddy
M-tech Student Scholar, Department of Computer Science Engineering, VRS & YRN College of Engineering & Technology, Chirala; Prakasam (Dt); Andhra Pradesh, India.
Assistant Professor, Department of Computer Science Engineering,VRS & YRN College of Engineering &Technology, Chirala; Prakasam (Dt), Andhra Pradesh, India.

Abstract — Ad-hoc low-power wireless networks are an exciting research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. This paper explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes' battery power. 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. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O(N), where N in the number of network nodes. We discuss methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.

The augmentation for this project aims to increase the security of the system by adding dynamic key while logging in for more security. This dynamic key will be auto generated. As security is a prime factor in vampire attacks scenario and in wireless adhoc sensor networks, privacy preserving mechanisms should be incorporated inorder to increase the reliability. Hence we can generate a trusted wireless adhoc sensor network in the scenario of vampire attacks. Earlier research has underwent on packet distribution techniques in a wide range which increases the reliable data communication in the domain of adhoc wireless sensor networks. But in this along with reliable data communication of packeted data, we are focused to improvise the trusted and secure data communication and retrieval

and primely focusing on vampire attacks.

Index Terms— Denial of service, security, routing, ad-hoc net-works, sensor networks, wireless networks.

I. INTRODUCTION

Ad-hoc wireless sensor networks (WSNs) promise excit-ing new applications in the near future, such as ubiqui-tous on-demand computing power, continuous connectivity, and instantly-deployable communication for military and first responders. Such networks already monitor environmental conditions, factory performance, and troop deployment, to name a few applications. As WSNs become more and more crucial to the everyday functioning of people and organi-zations, 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. Due to their ad-hoc organization, wireless ad-hoc networks particularly vulnerable to denial of service (DoS) attacks , and a great deal of research has been done to enhance survivability [1, 3, 7, 8].

While these schemes can prevent attacks on the short-term availability of a network, they do not address attacks that affect long-term availability — the most permanent denial of service attack is to entirely deplete nodes' batteries. This is an instance of a resource depletion attack, with battery power as the resource of interest. In this paper we consider how routing protocols, even those designed to be

secure, lack protection from these attacks, which we call Vampire attacks [16], 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.

Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance-vector, source routing, and geographic and beacon routing. 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 Contributions. This paper makes three primary contri-butions. First, we thoroughly evaluate the vulnerabilities of existing protocols to routing layer battery depletion attacks. We observe that security measures to prevent Vampire attacks [16] are orthogonal to those used to protect routing infrastructure, and so existing secure routing protocols such as Ariadne , SAODV, and SEAD do not protect against Vampire attacks. Existing work on secure routing attempts to ensure that adversaries cannot cause path discovery to return an invalid network path, but 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 node behavior and cannot optimize out malicious action. Second, we show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire (insider adversary). Third, we modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

In the present system, the focus is on packet distribution techniques in a wide range in the domain of adhoc wireless sensor networks. To increase reliable data communication of packeted data, we are focused to improvise the trusted and secure data communication and retrieval and primely focusing on vampire attacks. To increase the security of the system, we add a dynamic key while logging in for more security. This dynamic key will be auto generated. The privacy preserving mechanisms are incorporated so as to improvise the reliability of communication between various nodes in the wireless sensor network. Thus auto generating the dynamic key will result in trusted and secure data communication and retrieval and primarily focusing on vampire attacks.

II. RELATED WORK

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, as “sleep deprivation torture.” As per the name, the proposed attack prevents nodes from entering a low-power sleep cycle, and thus deplete their batteries faster. Newer research on “denial-of-sleep” only considers attacks at the medium access control (MAC) layer. Additional work mentions resource exhaus-tion at the MAC and transport layers,but only offers rate limiting and elimination of insider adversaries as potential solutions. Malicious cycles (routing loops) have been briefly mentioned [5], but no effective defenses 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 adversary, 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 [4], which offload the initial connection state onto the client, or cryptographic puzzles [2]). 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.

III.

There is also significant past literature on attacks and defenses against quality of service (QoS) degradation, or reduction of quality (RoQ) attacks, that produce long-term degradation in network performance [11,14,41,42,44]. The focus of this work is on the transport layer rather than routing protocols, so these defenses 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 pack-ets [8]. 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) [6, 9, 10], 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 [12]. 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 defenses in [7], 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 pro-tect 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. It allows two non-neighboring malicious nodes with either a physical or virtual private connection to emulate a neighbor relationship, even in secure routing systems. 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

Mobile Computing

Mobile Computing offers such smartphones that have rich Internet media experience and require less processing, less power. In term of Mobile Cloud Computing, processing is done in cloud, data is stored in cloud. And the mobile devices serve as a media for display.

Today smartphones are employed with rich cloud services by integrating applications that consume web services. These web services are deployed in cloud.

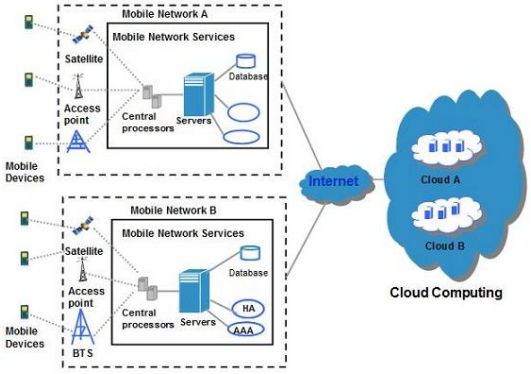
There are several Smartphone operating systems available such as **Google's Android, Apple's iOS, RIM BlackBerry, Symbian,** and **Windows Mobile Phone**. Each of these platforms support third-party applications that are deployed in cloud.

Architecture

MCC includes four types of cloud resources:

- Distant mobile cloud
- Distant immobile cloud
- Proximate mobile computing entities
- Proximate immobile computing entities
- Hybrid

The following diagram shows the framework for mobile cloud computing architecture:



From the concept of MCC, the general architecture of MCC can be shown in Figure, mobile devices are connected to the mobile networks via base stations (e.g., base transceiver station, access point, or satellite) that establish and control the connections (air links) and functional interfaces between the networks and mobile devices. Mobile users' requests and information (e.g., ID and location) are transmitted to the central processors that are connected to servers providing mobile network services. Here, mobile network operators can provide services to mobile users as authentication, authorization, and accounting based on the home agent and subscribers' data stored in databases. After that, the subscribers' requests are delivered to a cloud through the Internet. In the cloud, cloud controllers process the requests to provide mobile users with the corresponding cloud services. These services are developed with the concepts of utility computing, virtualization, and service-oriented architecture (e.g., web, application, and database servers).

IV. EXISTING SYSTEM

Existing work on secure routing attempts to ensure that adversaries cannot cause path discovery to return an invalid network path, but 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 node behavior and cannot optimize out malicious action.

V. PROPOSED SYSTEM

In proposed system we show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire. Then, we modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

VI. CONCLUSION

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 defenses 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 defenses for topology discovery, as well as handling mobile networks, is left for future work.

By implementing the above discussed, enhanced security mechanism, we are able to provide for trusted and secure data communication and retrieval in wireless adhoc networks.

REFERENCES

[1] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004.

[2] Tuomas Aura, Dos-resistant authentication with client puzzles, Interna-tional workshop on security protocols, 2001.

[3] John Bellardo and Stefan Savage, 802.11 denial-of-service attacks: real vulnerabilities and practical solutions, USENIX security, 2003.

[4] Daniel J. Bernstein, Syn cookies, 1996. http://cr.yp.to/syncookies.html.

[5] Haowen Chan and Adrian Perrig, Security and privacy in sensor net-works, Computer 36 (2003), no. 10.

[6] Jae-Hwan Chang and Leandros Tassiulas, Maximum lifetime routing in wireless sensor networks, IEEE/ACM Transactions on Networking 12 (2004), no. 4.

[7] 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.

[8] , INSENS: Intrusion-tolerant routing for wireless sensor net-works, Computer Communications 29 (2006), no. 2.

[9] Sheetalkumar Doshi, Shweta Bhandare, and Timothy X. Brown, An on-demand minimum energy routing protocol for a wireless ad hoc network, ACM SIGMOBILE Mobile Computing and Communications Review 6 (2002), no. 3.

[10] Laura M. Feeney, An energy consumption model for performance anal-ysis of routing protocols for mobile ad hoc networks, Mobile Networks and

Applications 6 (2001), no. 3.

[11] Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, and Jennifer Rexford, Path-quality monitoring in the presence of adversaries, SIG-METRICS, 2008.

[12] Andrea J. Goldsmith and Stephen B. Wicker, Design challenges for energy-constrained ad hoc wireless networks, IEEE Wireless Communi-cations 9 (2002), no. 4.

[13] R. Govindan and A. Reddy, An analysis of internet inter-domain topology and route stability, INFOCOM, 1997.

[14] Mina Guirguis, Azer Bestavros, Ibrahim Matta, and Yuting Zhang,
Reduction of quality (RoQ) attacks on Internet end-systems, INFOCOM, 2005.

[15] J.L. Hill and D.E. Culler, Mica: a wireless platform for deeply embedded networks, IEEE Micro 22 (2002), no. 6.

[16] Ieee Transactions On Mobile Computing Vol.12 No.2 Year 201

AUTHOR'S PROFILE

SANTHI BABU.D received B.Tech degree from Chirala College of Engineering &Technology, Chirala, Prakasam, Andhra Pradesh. and currently pursuing M.Tech in Computer Science Engineering at VRS & YRN College of Engineering &Technology, Chirala, Prakasam (Dt), Andhra Pradesh. His areas of interest include Mobile Computing.

Mr. K. TIRUMALA REDDY is presently working as Associate professor in VRS & YRN College of Engineering & Technology, Chirala, AP, India. He did his B.Tech. degree in Computer Science and Engineering from Andhra University, Visakhapatnam .And then completed his M.Tech. in Computer Science and Engineering as his specialization from Andhra University, Visakhapatnam. He has a teaching experience of 4.5 years.