© 2014 IJIRT | Volume 1 Issue 5 | ISSN : 2349-6002

EXHAUSTING LIVELINESS FROM WIRELESS AD-HOC SENSOR NETWORKS

A. Nagender Babu[1], P. Amarendra Reddy[2]
[1]*M.Tech, CSE Dept, MLRIT, Hyderabad*
[2]*M.Tech, Asst. Professor, MLRIT, Hyderabad*

***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.**

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

I. INTRODUCTION

Over the last couple of years wireless communication has become of such fundamental importance that a world without it is no longer imaginable for many of us. Beyond the established technologies such as mobile phones and WLAN, new approaches to wireless communication are emerging; one of them are so called ad hoc and sensor networks. Ad hoc and sensor networks are formed by autonomous nodes communicating via radio without any additional backbone infrastructure. A Wireless Sensor Network (WSN) can be defined as a network of small embedded devices, called sensors, which communicate wirelessly following an ad hoc configuration. They are located strategically inside a physical medium and are able to interact with it in order to measure physical parameters from the environment and provide the sensed information. The nodes mainly use a broadcast communication and the network topology can change constantly due, for example, to the fact that nodes are prone to fail. Because of this, we should keep in mind that nodes should be autonomous and, frequently, they will be disregarded. This kind of device has limited power, low computational capabilities and limited memory. One of the main issues that should be studied in WSNs is their scalability feature, their connection strategy for communication and the limited energy to supply the device.

Wireless Adhoc Network

An ad hoc wireless network is a collection of wireless mobile nodes that self-configure to form a network without the aid of any established infrastructure, as shown in without an inherent infrastructure, the mobiles handle the necessary control and networking tasks by themselves, generally through the use of distributed control algorithms. Multihop connections, whereby intermediate nodes send the packets toward their final destination, are supported to allow for efficient wireless communication between parties that are relatively far apart. Ad hoc wireless networks are highly appealing for many reasons. They can be rapidly deployed and reconfigured. They can be tailored to specific applications, as implied by Oxford's definition. They are also highly robust due to their distributed nature, node redundancy, and the lack of single points of failure.

Exciting new applications in the near future, such as ubiquitous 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 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. Due to their ad-hoc organization, wireless ad-hoc networks are particularly vulnerable to denial of service (DoS) attacks [15], and a great deal of research has been done to enhance survivability.

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, 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 [13, 9, 8], 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.

II. Problem Statement

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.

This paper makes 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 such as Ariadne [9], SAODV [18], and SEAD [8] 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.

III. System Development

Data-Verification

In data verification module, receiver verifies the path. Suppose data come with malicious node means placed in malicious packet. Otherwise data placed in honest packet. This way user verifies the data's.

Denial of service

In computing, a denial-of-service attack or distributed denial-of-service attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

User Module

In user module, verify user and any time create a new path. In security purpose user give the wrong details means display wrong node path otherwise display correct node path.

Stretch Attack

Stretch attack, where a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. An honest source would select the route Source → F → E → Sink, affecting four nodes including itself, but the malicious node selects a longer route, affecting all nodes in the network. These routes cause nodes that do not lie along the honest route to consume energy by forwarding packets they would not receive in honest scenarios.

IV. Related Work

Classical models of denial of service by Gligor and Yu [6, 17], Amoroso [1], and Millen [13] concentrate the specification and design of fair multi-user operating systems. They assume that all service requests are arbitrated by a trusted computing base (TCB) that enforces the policy set by a single security officer. Their ideas do not extend well to open distributed systems like the Internet where there is no central trusted administration and no global policy or means for enforcing one, and there are too many simultaneous users to theoretically guarantee the availability of any service.

Graph-theoretical models of network reliability by Cunningham [4] and Phillips [14] assess the vulnerability of a communications network to the destruction of nodes and links. These models are useful in the design of network

topologies on the physical layer but their applicability does not easily extend to higher protocol layers. The SYN attack against the TCP connection protocol on the Internet was reported e.g. in [3]. The attack and possible remedies were analyzed in detail by Schuba et al. [15]. Cookies have been previously used in the Photuris protocol by Karn and Simpson [11] and in the Internet Key Exchange (IKE) by Harkins and Carrel [7]. Criticism of the latter [16] shows that the gradually strengthening authentication is not straightforward to design and a careful analysis of the server resource usage is needed.

Meadows [12] formalized the idea of gradually strengthening authentication. The design goals of a cryptographic protocol should specify how much resources the server may allocate at each level when its assurance of the client's identity and honest purposes step by step increases. This assurance is measured by the resources the client would need to mount a successful attack. The advantages of statelessness in the beginning of an authentication protocol were recognized by Janson & al. [9] in the KryptoKnight protocol suite. Aura and Nikander [2] generalized the cookie approach to create stateless servers that maintain connections by passing the state data to the client. The paper also gives examples of authentication protocols where the server avoids saving a state until the authentication of the client is complete. Hirose and Matsuura [8] applied these ideas to a DOS-resistant version of their KAP protocol. In addition to remaining stateless, the server in their protocol postpones expensive exponentiation operations until it has verified that the client has performed similar operations. This way, the server commits its memory and computational resources only after the client has demonstrated its sincerity.

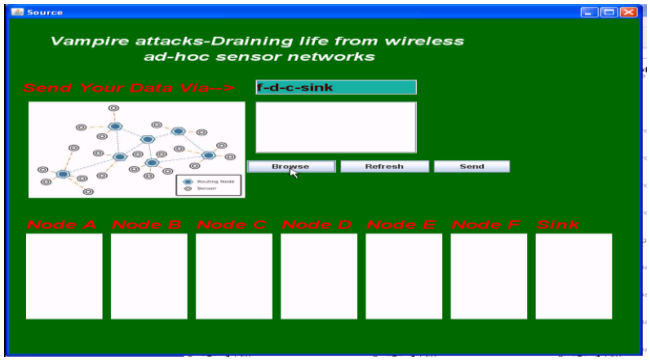
The idea of requiring the client to commit its resources first was described early by Dwork and Naor [5]. They suggested increasing the cost of electronic junk mailing by asking the sender to solve a small cryptographic puzzle for each message. The cost would be negligible for normal users but high for mass mailers. Juels and Brainard [10] recently presented a simpler puzzle that could be sent to TCP clients during a suspected SYN attack. If the server thinks it is under a denial-of-service attack, it can ask clients to compute the reverse of a secure one-way function by brute force before they are allowed to carry on with rest of the protocol. The cost of the brute force computation is parameterized by revealing some input bits to the client and letting it find the remaining ones.

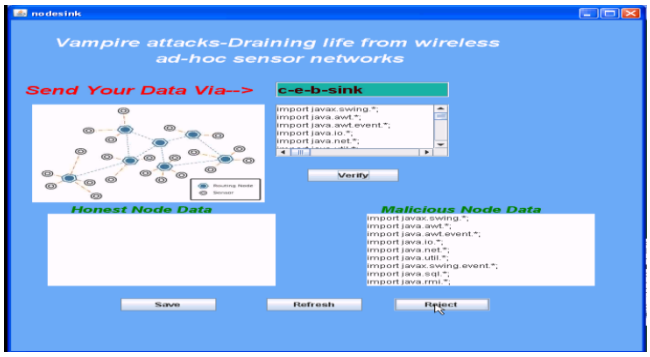
However, Juels and Brainard concentrate on the SYN attack and don't consider DOS attacks against authentication protocols. They, in fact, suggest that a certificate based client authentication solves the DOS problem and, hence, would not benefit from the puzzles. We disagree with this and use the client puzzles to generalize the design principles of the DOS-resistant KAP to any authentication protocol. We also improve the efficiency of the client puzzles by reducing the length of the puzzle and its solution, by minimizing the number of hash operations needed in the verification of the solution (at the cost of slightly coarser puzzle difficulty levels), and by observing that the puzzles can in some networks be broadcast to the potential clients.

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 [18], 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 "denialof- sleep" only considers attacks at the medium access control (MAC) layer [19]. Additional work mentions resource exhaustion at the MAC and transport layers [60, 75], but only offers rate limiting and elimination of insider adversaries as potential solutions. Malicious cycles (routing loops) have been briefly mentioned [10, 12], 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 resources 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 [7], which offload the initial connection state onto the client, or cryptographic puzzles [4, 18, 13]). 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.

V. RESULTS





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 expose 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.

REFERENCES

[1] The network simulator Ns-2. http://www.isi.edu/ nsnam/ns/.

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

[3] Gergely Acs, Levente Buttyan, and Istvan Vajda, Provably secure ondemand source routing in mobile ad hoc networks, IEEE Transactions on Mobile Computing 05 (2006), no. 11.

[4] Tuomas Aura, Dos-resistant authentication with client puzzles, International workshop on security protocols, 2001.

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

[6] Daniel Bernstein and Peter Schwabe, New AES software speed records, INDOCRYPT, 2008.

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

[8] I.F. Blake, G. Seroussi, and N.P. Smart, Elliptic curves in cryptography, Vol. 265, Cambridge University Press, 1999.

[9] Joppe W. Bos, Dag Arne Osvik, and Deian Stefan, Fast implementations of AES on various platforms, 2009.

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

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

[12] Thomas H. Clausen and Philippe Jacquet, Optimized link state routing protocol (OLSR), 2003.

[13] Jing Deng, Richard Han, and Shivakant Mishra, Defending against pathbased DoS attacks in wireless sensor networks, ACM workshop on security of ad hoc and sensor networks, 2005.

[14] , INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications 29 (2006).

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

[16] John R. Douceur, The Sybil attack, International workshop on peer-topeer systems, 2002.

[17] Hans Eberle, Arvinderpal Wander, Nils Gura, Sheueling Chang-Shantz, and Vipul Gupta, Architectural

extensions for elliptic curve cryptography over GF(2m) on 8-bit microprocessors, ASAP, 2005.
[18] T. English, M. Keller, Ka Lok Man, E. Popovici, M. Schellekens, and W. Marnane, A low-power pairing-based cryptographic accelerator for embedded security applications, SOCC, 2009.
[19] Laura M. Feeney, An energy consumption model for performance analysis of routing protocols for mobile ad hoc networks, Mobile Networks and Applications 6 (2001).
[20] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, Strong authentication for RFID systems using the AES algorithm, CHES, 2004.

AUTHOR DETAILS:

First Author: ***A. Nagender Babu*** received B.Tech Information Technology from DRK College of Engineering and Technology, Hyderabad, in the year 2012. He is currently M.Tech student in Computer Science and Engineering Department from Marri Laxman Reddy Institute of Technology. And his research interested areas are in the field of Networking, Information Security and Cloud Computing, Mobile Computing.

Second Author: ***P. Amarendra Reddy*** working as an Asst. Professor in Marri Laxman Reddy Institute of Technology, Hyderabad. He has completed his M.Tech CSE and he has 9 years of teaching experience. His research interested areas are Data Mining, Network Security and Cloud Computing.