ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Provable Security Against Incubus Attacks & DOS Attacks Securing From Wireless AD HOC Sensor Networks

P.Avaniketh
Assistant Professor,
Department of Computer Science & Engineering,
Christu Jyothi Institute of Technology & Science.

K.Rajashekar
Assistant Professor,
Department of Computer Science & Engineering,
Christu Jyothi Institute of Technology & Science.

ABSTRACT:

As WSNs become more and more crucial to the everyday functioning of people and organizations, availability faults become less tolerable. Ad-hoc low-power wireless networks are an exciting research direction in sensing and pervasive computing. Due to their ad hoc organization, 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.The most permanent denial of service attack is to entirely deplete node's batteries. This is an instance of a resource depletion attack, with battery power as the resource of interest.

These "Incubus" 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 Incubus 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. Evaluating the vulnerabilities of existing protocols to routing layer battery depletion attacks. Modifys an existing sensor network routing protocol to provably bound the damage from Incubus attacks during packet forwarding.

INDEX TERMS:

security, routing, ad hoc networks, sensor networks, wireless networks, resource depletion nodes,denial of sevice.

I.INTROCUCTION:

Routing is one of the most basic networking functions in mobile ad hoc networks. Hence, an adversary can easily paralyze the operation of the network by attacking the routing protocol. This has been realized by many researchers and several "secure" routing protocols have been proposed for ad hoc networks. However, the security of those protocols has mainly been analyzed by informal means only. In this paper, we argue that flaws in ad hoc routing protocols can be very subtle, and we advocate a more systematic way of analysis. We propose a mathematical framework in which security can be precisely defined and routing protocols for mobile ad hoc networks can be proved to be secure in a rigorous manner. Our framework is tailored for on-demand source routing protocols, but the general principles are applicable to other types of protocols too.

Our approach is based on the simulation paradigm, which has already been used extensively for the analysis of key establishment protocols, but, to the best of our knowledge, it has not been applied in the context of ad hoc routing so far. We also propose a new on-demand source routing protocol, called endairA, and we demonstrate the use of our framework by proving that it is secure in our model. Significant progress has been made towards making ad hoc networks secure and DoS resilient. However, little attention has been focused on quantifying DoS resilience:
Do ad hoc networks have sufficiently redundant paths and counter-DoS mechanisms to make DoS attacks largely ineffective? Or are there attack and system factors that can lead to devastating effects? In this paper, we design and study DoS attacks in order to assess the damage that difficult-to-detect attackers can cause. The first attack we study, called the JellyFish attack, is targeted against closed-loop flows such as TCP; although protocol compliant, it has devastating effects. . The second is the Black Hole attack, which has effects similar to the JellyFish, but on open-loop flows. We quantify via simulations and analytical modeling the scalability of DoS attacks as a function of key performance parameters such as mobility, system size, node density, and counter-DoS strategy.

One perhaps surprising result is that such DoS attacks can increase the capacity of ad hoc networks, as they starve multi-hop flows and only allow one-hop communication, a capacity-maximizing, yet clearly undesirable situation. Abstract. This paper presents new speed records for AES software, taking advantage of (1) architecture-dependent reduction of instructions used to compute AES and (2) microarchitecture-dependent reduction of cycles used for those instructions. A wide variety of common CPU architectures—amd64, ppc32, sparcv9, and x86—are discussed in detail, along with several specific microarchitectures. Denial of service by server resource exhaustion has become a major security threat in open communications networks.

Public-key authentication does not completely protect against the attacks because the authentication protocols often leave ways for an unauthenticated client to consume a server's memory space and computational resources by initiating a large number of protocol runs and inducing the server to perform expensive cryptographic computations. We show how stateless authentication protocols and the client puzzles of Juels and Brainard can be used to prevent such attacks. Sensor networks offer economically viable solutions for a variety of applications. For example, current implementations monitor factory instrumentation, pollution levels, freeway traffic, and the structural integrity of buildings.

Other applications include climate sensing and control in office buildings and home environmental sensing systems for temperature, light, moisture, and motion. Sensor networks are key to the creation of smart spaces, which embed information technology in everyday home and work environments. The miniature wireless sensor nodes, or motes, developed from low-cost off-the-shelf components at the University of California, Berkeley, as part of its smart dust projects, establish a self-organizing sensor network when dispersed into an environment.

The privacy and security issues posed by sensor networks represent a rich field of research problems. Improving network hardware and software may address many of the issues, but others will require new supporting technologies. A routing problem in static wireless ad hoc networks is considered as it arises in a rapidly deployed, sensor based, monitoring system known as the wireless sensor network. Information obtained by the monitoring nodes needs to be routed to a set of designated gateway nodes. In these networks, every node is capable of sensing, data processing, and communication, and operates on its limited amount of battery energy consumed mostly in transmission and reception at its radio transceiver. If we assume that the transmitter power level can be adjusted to use the minimum energy required to reach the intended next hop receiver then the energy consumption rate per unit information transmission depends on the choice of the next hop node, i.e., the routing decision.

We formulate the routing problem as a linear programming problem, where the objective is to maximize the network lifetime, which is equivalent to the time until the network partition due to battery outage. Two different models are considered for the information-generation processes. One assumes constant rates and the other assumes an arbitrary process.

A shortest cost path routing algorithm is proposed which uses link costs that reflect both the communication energy consumption rates and the residual energy levels at the two end nodes. The algorithm is amenable to distributed implementation. Simulation results with both information-generation process models show that the proposed algorithm can achieve network lifetime that is very close to the optimal network lifetime obtained by solving the linear programming problem.

II.IMPLEMENTATION:

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.

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.

III.SYSTEM PRELIMINARIES:

A.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.

B.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.

C.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.

D.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.CONCLUSION:

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.

REFERENCES:

[1] "The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns, 2012.

[2] I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom, 2004.

[3] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

[4] T. Aura, "Dos-Resistant Authentication with Client Puzzles," Proc. Int'l Workshop Security Protocols, 2001.

[5] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.

[6] D. Bernstein and P. Schwabe, "New AES Software Speed Records," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), 2008.

[7] D.J. Bernstein, "Syn Cookies," http://cr.yp.to/syncookies.html, 1996.

[8] I.F. Blaked, G. Seroussi, and N.P. Smart, Elliptic Curves in Cryptography, vol. 265. Cambridge Univ. , 1999.

[9] J.W. Bos, D.A. Osvik, and D. Stefan, "Fast Implementations of AES on Various Platforms," Cryptology ePrint Archive, Report 2009/ 501, http://eprint.iacr.org, 2009.

[10] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[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] T.H. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, 2003. 330 IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2, FEBRUARY 2013.

[13] 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.

[14] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks," Computer Comm., vol. 29, no. 2, pp. 216-230, 2006.

[15] S. Doshi, S. Bhandare, and T.X. Brown, "An On-Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002.

[16] J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop Peer-to-Peer Systems, 2002.

[17] H. Eberle, A. Wander, N. Gura, C.-S. Sheueling, and V. Gupta, "Architectural Extensions for Elliptic Curve Cryptography over GF(2m) on 8-bit Microprocessors," Proc. IEEE Int'l Conf' Application- Specific Systems, Architecture Processors (ASAP), 2005.

[18] T. English, M. Keller, K.L. Man, E. Popovici, M. Schellekens, and W. Marnane, "A Low-Power Pairing-Based Cryptographic Accelerator for Embedded Security Applications," Proc. IEEE Int'l SOC Conf. , 2009.

[19] 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.

[20] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," Proc. Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES), 2004.

[21] R. Fonseca, S. Ratnasamy, J. Zhao, C.T. Ee, D. Culler, S. Shenker, and I. Stoica, "Beacon Vector Routing: Scalable Point-to-Point Routing in Wireless Sensornets," Proc. Second Conf. Symp. Networked Systems Design & Implementation (NSDI), 2005.

[22] S. Galbraith, K. Harrison, and D. Soldera, "Implementing the Tate Pairing," Proc. Int'l Symp. Algorithmic Number Theory, 2002.

[23] S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford, "Path- Quality Monitoring in the Presence of Adversaries," Proc. ACM SIGMETRICS Int'l Conf. Measurement and Modeling of Compute Systems, 2008.

AUTHOR PROFILES:

P.Avanike

th received M.Tech from JNTU Hyderabad. He is currently working as a Assistant.Professor in Computer Science Engineering Department, Christu Jyothi Institute of Technology, Jangaon, Warangal,Telangana, India-506167.

K.Rajashekar

received M.Tech from Kakatiya University Warangal. He is currently working as a Assistant.Professor in Computer Science & Engineering Department, Christu Jyothi Institute of Technology,Jangaon,Warangal,Telangana,
India-506167.