EFFICIENCY GAIN ON WSN (WIRELESS SENSOR NETWORKS) FOR LEECH ATTACKS

[1]SHAIK REHANA , [2]P SHAKEEL AHAMED, [3]P.BABU

[1]PG SCHOLAR, CSE,QCET ,NELLORE
[2]ASSOCIATE PROFESSOR, CSE,QCET ,NELLORE
[3]ASSOCIATE PROFESSOR,CSE,QCET ,NELLORE

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.*

1.INTRODUCTION:

Ad-hoc wireless sensor networks (WSNs) promise 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, 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, 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 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, 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.

2. 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.

3.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.

4. MODULE DESCRIPTION:

4.1. 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.

4.2 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.

4.3 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.

4.4. 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

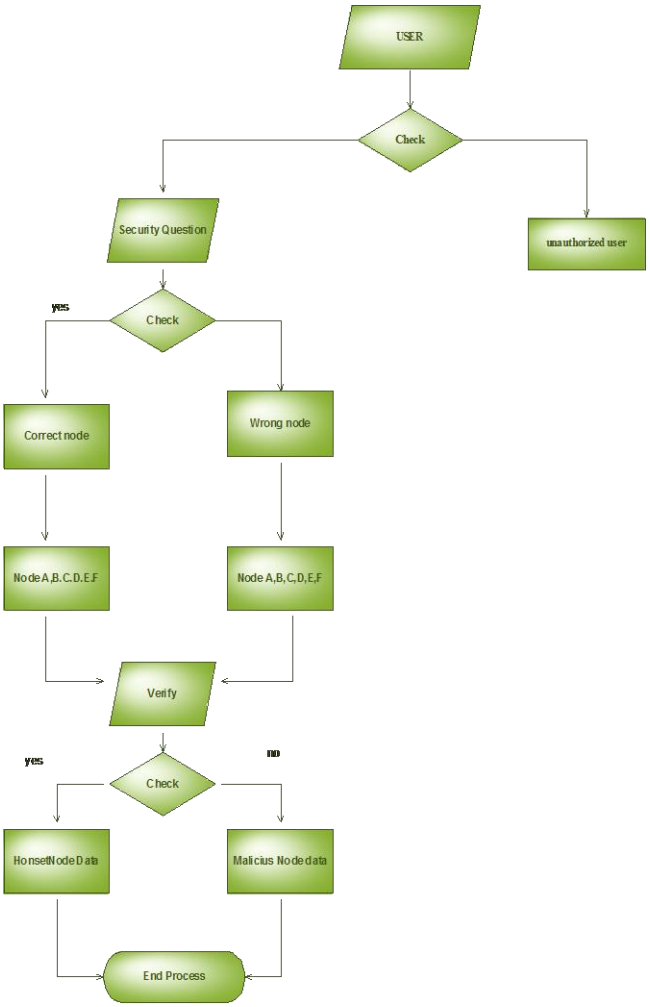
four nodes including itself, but the malicious node selects a longer route, affecting all nodes in the network. These routes cause nodes that do not lie along the honest route to consume energy by forwarding packets they would not receive in honest scenarios.

5.Data Flow Diagram :

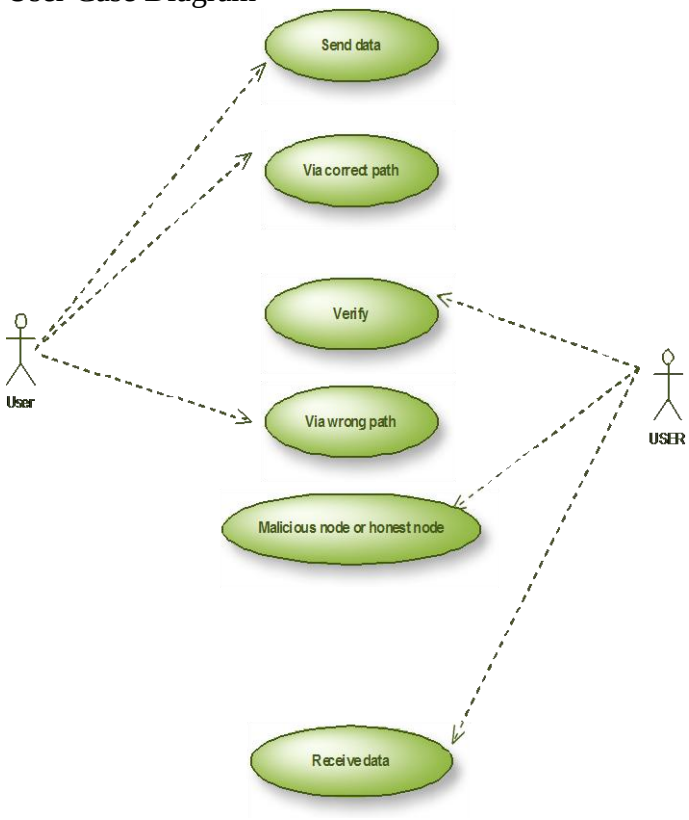
The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of the input data to the system, various processing carried out on these data, and the output data is generated by the system.

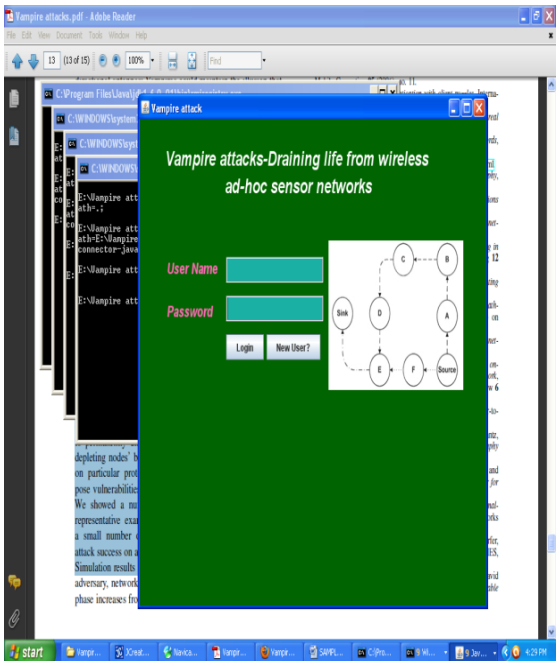
SYSTEM DESIGN

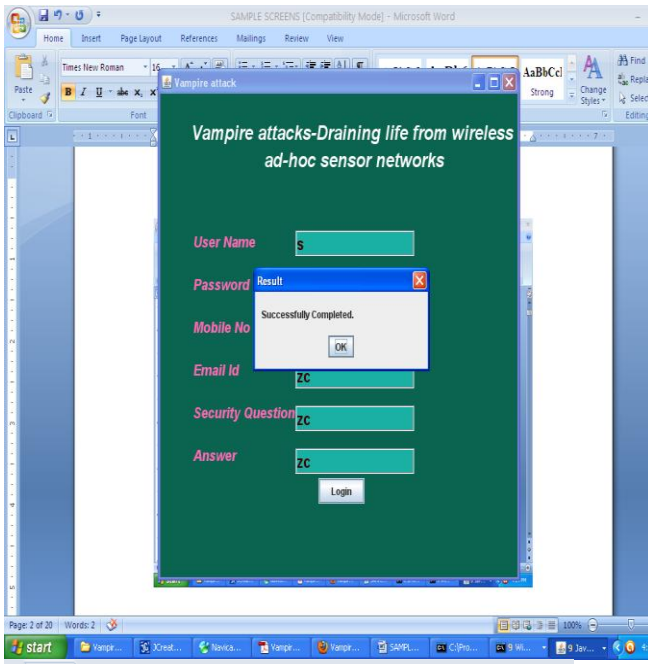
User



User Case Diagram







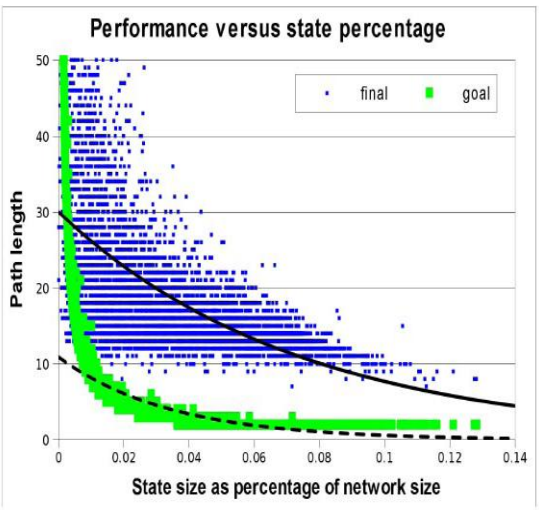


Fig:Loose source routing performance compared to optimal, in a network with diameter slightly above 10. The dashed trend line represents expected path length when nodes store logN local state, and the solid trend line shows actual observed performance.

System Configuration:-

H/W System Configuration:-

Processor - Pentium –III

Speed - 1.1 Ghz
RAM - 256 MB(min)
Hard Disk - 20 GB
Floppy Drive - 1.44 MB
Key Board - Standard Windows Keyboard
Mouse - Two or Three Button Mouse
Monitor - SVGA

S/W System Configuration:-

Operating System :Windows XP
Front End : JAVA,RMI, SWING

6. 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.
[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 Computer Systems, 2008.
[24] A.J. Goldsmith and S.B. Wicker, "Design Challenges for Energy-Constrained Ad Hoc Wireless Networks," IEEE Wireless Comm., vol. 9, no. 4, pp. 8-27, Aug. 2002.
[25] R. Govindan and A. Reddy, "An Analysis of Internet Inter- Domain Topology and Route Stability," Proc. IEEE INFOCOM, 1997.
[26] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of Quality (RoQ) Attacks on Internet End-Systems," Proc. IEEE INFOCOM, 2005.
[27] J.L. Hill and D.E. Culler, "Mica: A Wireless Platform for Deeply Embedded Networks," IEEE Micro, vol. 22, no. 6, pp. 12-24, Nov./ Dec. 2002.
[28] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications,2002.
[29] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom, 2002.
[30] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Proc. IEEE INFOCOM, 2003.
[31] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proc. Second ACM Workshop Wireless Security (WiSE), 2003.
[32] Y. Huang and S. Bhatti, "Fast-Converging Distance Vector Routing for Wireless Mesh Networks," Proc. 28th Int'l Conf. Distributed Computing Systems Workshops (ICDCSW), 2008.
[33] D. Hwang, B.-C. Lai, P. Schaumont, K. Sakiyama, Y. Fan, S. Yang, A. Hodjat, and I. Verbauwhede, "Design Flow for HW/SW Acceleration Transparency in the Thumbpod Secure Embedded System," Proc. Design Automation Conf., 2003.
[34] L. Iannone, R. Khalili, K. Salamatian, and S. Fdida, "Cross-Layer Routing in Wireless Mesh Networks," Proc. Int'l Symp. Wireless Comm. Systems, 2004.
[35] D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," Ad Hoc Networking, Addison-Wesley, 2001.