ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Securable Routing And Elimination Of Adversary Attack From Manet

Sureka.N[1], Prof. S. Chandra Sekaran, M.E., [2]

M.E-CSE, Department of computer science, .S.V. College of engineering & technology, Krishnagiri, Tamilnadu, India[1]

Assistant Professor, Department of computer science, .S.V. College of engineering & technology, Krishnagiri, Tamilnadu, India[2]

Abstract: The wireless Adhoc sensor network and routing data in them is vulnumarable to certain attacks. So we must ensure a secure and authenticated data transmission process. There are a lot of protocols developed to protect from DOS attack, but it is not completely possible. One such DOS attack is Vampire attack draining of node life from wireless adhoc sensor networks. 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 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

Adhoc 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 businesses 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. 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. 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.

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.

Three primary contributions.

1. 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 [29], SAODV [78], and SEAD [28] 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.

2. We show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire (insider adversary).

3. We modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

II. OVERVIEW

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 OðNÞ 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.

III. LITERATURE REVIEW

Denial of Service Resilience in Ad Hoc Networks

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.

In this paper, we studied a novel DoS attack perpetrated by JellyFish relay nodes that stealthily misorder, delay, or periodically drop packets that they are expected to forward, in a way that leads astray end-to-end congestion control protocols. This attack is protocol compliant and yet has a devastating impact on the throughput of closed-loop flows, such as TCP flows and congestion-controlled UDP flows. For completeness, we have also considered a well known attack, the Black Hole attack, as its impact on open-loop flows is similar to the effect of JellyFish on closed-loop flows. We studied these attacks in a variety of settings and have provided a quantification of the damage they can inflict. We showed that, perhaps surprisingly, such attacks can actually increase the capacity of ad hoc networks as they will starve all multihop flows and provide all resources to one-hop flows that cannot be intercepted by JellyFish or Black Holes. As such a partitioned system is clearly undesirable; we also consider fairness measures and the mean number of hops for a received packet, as critical performance measures for a system under attack. We assessed the effects of various performance factors on the above metrics via a simple analytical model and a substantial number of simulation experiments. In this way, we provide a quantitative study of the performance impact and scalability of DoS attacks in ad hoc networks. Our objective is to provide guidelines for protocol designers who are developing DoS-resilience mechanisms: with a better understanding of the key attack factors and how to evaluate the impact of an attack, protocol designers can better determine if the overhead of deploying a counter-strategy is merited given the damage that an attack can inflict.

Provably secure On-demand Source Routing in Mobile Ad Hoc Networks

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 analyzed rigorously. 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 end airA, and we demonstrate the usage of our framework by proving that it is secure in our model. The main message of this paper is that attacks against ad hoc routing protocols can be subtle and difficult to discover by informal reasoning about the properties of the protocol. We demonstrated this by presenting a novel attack on Ariadne. Another message is that it is possible to adopt rigorous techniques developed for the security analysis of cryptographic algorithms and protocols, and apply them in the context of ad hoc routing protocols in order to gain more assurances about their security.

We demonstrated this by proposing a simulation based framework for the security analysis of on demand source routing protocols. The proposed framework allows us to give a precise definition of security, to model the operation of a given routing protocol in the presence of an adversary, and to prove (or fail to prove) that the protocol is secure. We also proposed a new on-demand source routing protocol, endairA, and we demonstrated the usage of the proposed framework by proving that it is secure in our model. Originally, we developed endairA for purely illustrative purposes; however, it has some noteworthy features that may inspire designers of future protocols.

802.11Denial-of-ServiceAttacksReal vulnerabilities and Practical Solutions

The convenience of 802.11-based wireless access networks has led to widespread deployment in the consumer, industrial and military sectors. However, this use is predicated on an implicit assumption of confidentiality and availability. While the security flaws in 802.11's basic confidentially mechanisms have been widely publicized, the threats to network availability are far less widely appreciated. In fact, it has been suggested that 802.11 is highly susceptible to malicious denial-of-service (DoS) attacks targeting its management and media access protocols. This paper provides an experimental analysis of such 802.11-specific attacks – their practicality, their efficacy and potential low-overhead implementation changes to mitigate the underlying vulnerabilities.802.11-based networks have seen widespread deployment across many fields, mainly due to the physical conveniences of radio-based communication.

This deployment, however, was predicated in part on the user expectation of confidentiality and availability. This paper addressed the availability aspect of that equation. We examined the 802.11 MAC layer and identified a number of vulnerabilities that could be exploited to deny service to legitimate users. We described software infrastructure for generating arbitrary 802.11 frames using commodity hardware and then used this platform to implement versions of the deauthentication and virtual carrier sense attacks. We found that the former attack was highly effective in practice, while the latter is only a theoretical vulnerability due to implementation deficiencies in commodity 802.11 gear. In addition to demonstrating the attacks, we described and analyzed potential countermeasures. These countermeasures represent a stopgap measure, one that can be implemented with low overhead on existing hard ware, but not a long term substitute for appropriate per-packet authentication mechanisms. Overall, we believe this paper helps to underscore the care that must be taken when deploying 802.11 networks in mission critical applications.

Optimized Link State Routing Protocol

Denial of service (DoS) attacks can cause serious damage in resource constrained, wireless sensor networks (WSNs). This paper addresses an especially damaging form of DoS attack, called PDoS. In a PDoS attack, an adversary overwhelms sensor nodes a long distance away by flooding a multihop end-to-end communication path with either replayed packets or injected spurious packets. This paper proposes a solution using one-way hash chains to protect end-to-end communications in WSNs against PDoS attacks. The proposed solution is lightweight, tolerates bursty packet losses, and can easily be implemented in modern WSNs. The paper reports on performance measured from a prototype implementation.

In WSNs, an adversary can launch with little effort a path-based denial of service (PDoS) attack that will have a severe widespread effect on the WSN, disabling nodes on all branches downstream of the path, due to the tree-structured topology of WSNs. In this paper, we have proposed a lightweight and efficient mechanism using one way hash chains that allows intermediate nodes to defend against PDoS attacks by detecting replayed and spurious packets. We have proposed a novel and robust set of mechanisms to maintain one way hash chains given packet loss and topology changes. Our implementations show that our scheme is feasible in current sensor network platforms, and incurs modest overhead.

IV. PROBLEMS IDENTIFIED AND CONFIRMED

If vampire attack exist in the network, it will affect one node and drain its full energy and the particular node will goes to dead state and then the vampire attack concentrates on next node and so on it affects all nodes in the network, as a result all nodes goes to dead state. The vampire attack permanently disables or destroys the network.

V. OBJECTIVE AND SCOPE OF THE PROJECT

Our proposed project concentrates on securing the network from the malicious attack. Our implementation results in the efficient detection and elimination of vampire attack from the network. In order to detect and eliminating the vampire attack we going to implement certain intrusion detection system based on the energy level constraints. Our simulation result shows the improved network authentication rate and efficient detection of malicious node from the network, so that our proposed system forms a secure network with high throughput rate.

VI. ASSUMPTIONS, CONSTRAINTS AND LIMITATIONS

In order to show the performance metrics we locate 30 to 50 sensor nodes in the network, let number of sensor nodes be N. Then the routing is performed between sensor nodes, let the data packets be 512 bytes and the initial energy level of nodes be 10 joules. Let us use the wireless channel type for data routing among the N number of nodes. The routing is dine through link layer if link state routing protocol like aodv dsr dsdv. The graphical constraints like throughput, packet delivery ratio, delay are used to evaluate the performance of network. Mac 802.11 and Omni antenna is used for data communication and covering the transmission range.

DISADVANTAGES

The presence of vampire attack in the network will permanently disable the whole network. The energy level of nodes tends to 0 joules because of vampire attack presence. This system doesn't concentrates on eliminating the vampire attacks

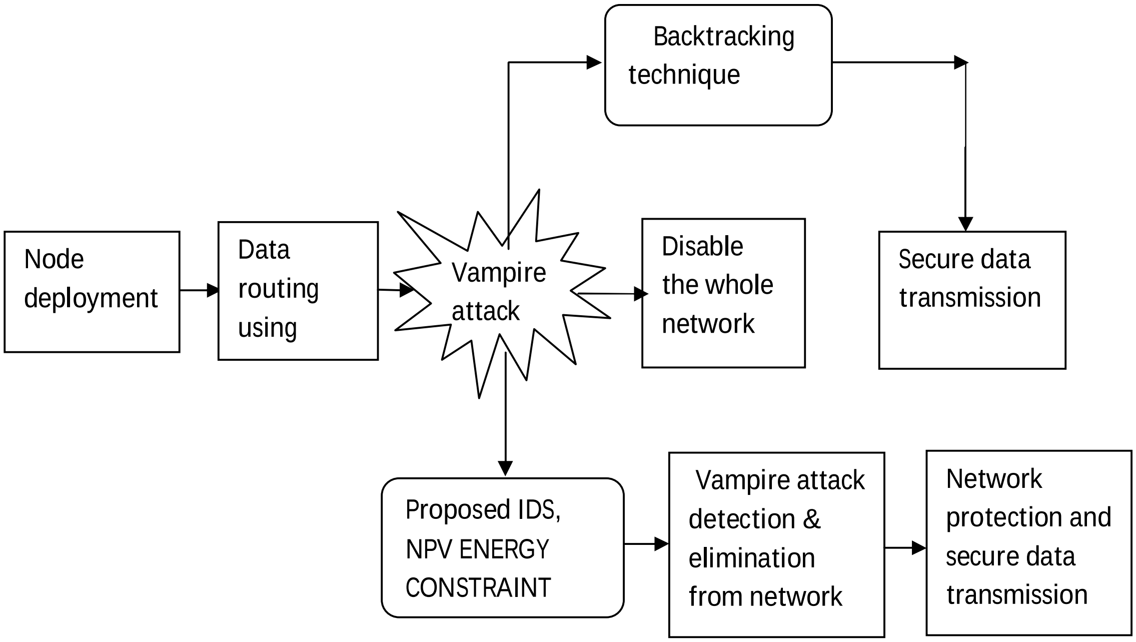
VII.PROPOSED METHOD

The proposed system concentrates on a secure data transmission from the adversary nodes in the sensor network. In order to build a secure network, the network should be an extinct to adversary nodes. So we propose a technique called nodes position verification [NPA] and node verification intrusion detection techniques [IDS]. The nodes which has the exceed threshold value other than normal nodes, then a node supposed to be a malicious nodes which will undergoes a vampire attack. By the proposed IDS system we can calculate the threshold value and energy level of malicious nodes, and also by NPA techniques the malicious nodes can be detected efficiently and detected nodes are eliminated from the network which increases the network performance and throughput rate.

ADVANTAGES

This system examines about the characteristics of vampire attack and its vulnumerable nature to the network. The stem proposes the mitagation technique to detect the vampire attack.

Fig. 1.SYSTEM ARCHITECTURE DESIGN


Backtracking technique
Node deployment
Data routing using
Vampire attack
Disable the whole network
Secure data transmission
Proposed IDS, NPV ENERGY CONSTRAINT
Vampire attack detection & elimination from network
Network protection and secure data transmission

VIII. MODULES DESCRIPTION

1. NODE CONFIGURATION SETTING

The mobile nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes.

2. DATA ROUTING

The source and destination are set at larger distance, the source transmits the data packets to destination through the intermediate hop nodes using UDP user data gram protocol, link state routing like PLGP act as an ad hoc routing protocol

3 VAMPIRE ATTACK

The malicious node enters the network, and affects the one of the intermediate node by sending false packets. So the malicious node drain the energy of the intermediate node, the intermediate energy level goes to 0 joules. So the data transmission is affected, the path tends to be failure between source and destination. As a result source retransmits the data in another path to destination. If the vampire attack continues it will disable the whole network.

4. BACKTRACKING TECHNIQUE

The back tracking technique is used to identify legitimate nodes in the particular path.The nodes accept the data only after the execution of back tracking technique. If source transmits the data to next neighbor node, the next node verifies the source identity using back tracking process. Through this technique the data is transmitted securely in the presence of vampire nodes.

5. INTRUSION DETECTION SYSTEM

The energy constraint IDS is used to detect the malicious nodes from the network, for that purpose the energy level for all nodes are calculated after every data iteration process. Maximum nodes have an average energy level in certain range, due to the nature of vampire nodes have a abnormal energy level like malicious node energy level is three times more than the average energy level, by this technique the malicious nodes can be identified easily.

6. MALICIOUS NODE ELIMINATION

After the IDS process the malicious nodes detected. The TA trusted authority informs to all nodes in the network and eliminate the malicious node from the network. So by eliminating malicious node we can form a secure network

7. GRAPH EXAMINATION

The performance analysis of the existing and proposed work is examined through graphical analysis.

IX. FUTURE WORK

We then present a solution towards preventing such attacks in the form of a new breakpoint framework named Galanus. Galanus also adds support for legacy I/O breakpoints in kernel-mode, an important feature required to analyze keyloggers, BIOS flashers, CMOS updaters and rootkits. We also evaluate Galanus, comparing it to VAMPIRE in the context of a few real-world malware.

X. PUBLICATION PRINCIPLES

N.SUREKA, PROF. S. CHANDRA SEKARAN, M.E, (Ph.D.,) "SECURABLE ROUTING AND EFFICIENT INTRUSION DETECTION AND ELIMINATION OF ADVERSARY ATTACK FROM MANET" National Conference on Emerging Trends in Advanced Computing and Communication held at Government College of Engineering, Bargur on 24th & 25th October 2013.

XI. ACKNOWLEDGEMENT

First and Foremost, I would like to thank my graduate advisor, Asst. prof. Anitha .M, for his guidance and encouragement throughout my graduate studies. His vast knowledge and working experience in computer science and engineering have proven invaluable in my quest to learn and grow. I would also like to thank my other professors and advisors, Prof. Sakthivel .B, for their constructive support, camaraderie, and teamwork. My studies would not have been the same without their contributions. Finally, but definitely not least, I want to thank my parents for their loving encouragement and grounding support at home which allowed me to concentrate and complete my work.

XII.CONCLUSION

As our proposed energy level constraint algorithm efficiently detects the malicious nodes from the network, by eliminating those affected nodes we can form the secure network with authenticated data transmission. The graphical results show the improved network performance with increased throughput rate and improved packet delivery ratio.

REFERENCES

[1]. M. Poturalski, P. Papadimitratos, and J.-P. Hubaux, "Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2008.

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

[3]. V.P. Nambiar, M. Khalil-Hani, and M.M.A. Zabidi, "Accelerating the AES Encryption Function in OpenSSL for Embedded Systems," Proc. Int'l Conf Electrical Design (ICED), 2008.

[4]. 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.

[5]. G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," 2006
[6]. M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of Quality (RoQ) Attacks on Internet End-Systems," Proc. IEEE INFOCOM, 2005.
[7]. 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.
[8]. I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom, 2004.
[9]. 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.
[10].Y.-C. Hu, D.B. Johnson, and A. Perrig, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom, 2002.
[11]. 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.
[12]. T.Aura, "Dos-Resistant Authentication with Client Puzzles," Proc. Int'l Workshop Security Protocols, 2001.