Phoenix: International Multidisciplinary Research Journal
Vol 1, No. 2, April-June, 2023
ISSN:2583-6897

VAMPIRE ATTACK DRAINING LIFE FROM WIRELESS AD-HOC-SENSORS NETWORK

[1]***Pooja M**, Master of Computer Application BKIT-Bhalki*
[2]***Prof. Sunil Sagme,** Master of Computer Application BKIT-Bhalki*

Abstract -Exciting applications for future technology that may operate safely in wireless ad hoc networks include ubiquitous on-demand processing capacity, continuous connection, and instantaneously deployable communication for the military and first responders. These are just some of the applications that are on the horizon. The operation of wireless networks is based on a fundamental mechanism that involves direction in sensing and ubiquitous computing. Wireless ad hoc networks are especially susceptible to denial of service (DoS) attacks; thus, a significant amount of research has been conducted to improve their capacity to survive such assaults. Prior security work in this area has generally concentrated on denying communication at the routing or medium access control levels as the primary target for protection. We look at how routing protocols, even ones that are meant to be safe, do not provide any protection against these assaults, which we name "Vampire attacks" since they siphon power from the nodes that make up a network. These so-called "Vampire" attacks are not limited to a single protocol, but rather depend on the characteristics that are shared by a variety of widely used categories of routing protocols. We have come to the conclusion that every single one of the protocols that were investigated is vulnerable to Vampire assaults. These attacks are destructive, difficult to detect, and simple to execute with as little as a single hostile insider sending only protocol-compliant communications. This study introduces a novel proof-of-concept protocol that provably confines the harm produced by Vampires during the packet forwarding phase. The introduction of this protocol is part of the mitigation of these sorts of attacks.

***Key Words*:** Block chain, Security, block size, hash code

1.INTRODUCTION

Significant research is being done in the field of ad hoc sensor networks and the data routing that occurs inside them. Even though there have been many different protocols established to guard against DOS attacks, it is still not entirely practicable. A lack of availability can mean the difference between business as usual and lost productivity, power outages, environmental disasters, and even lost lives; as a result, high availability of these networks is a critical property, and it should hold even under malicious conditions. As WSNs become more and more crucial to the day-to-day functioning of people and organizations, availability faults become less tolerable. Vampire attacks are a kind of denial of service attack that include the draining of node life from wireless ad hoc sensor networks.

An assault known as a vampire attack occurs when a malicious node generates and sends messages. This results in an increase in the amount of energy that is used by the network, which eventually leads to a gradual decrease in the node's remaining battery life. This attack is not limited to a particular protocol in any way. Carousal and stretch assaults are among the most harmful forms of attacks since they deplete the energy of the nodes in a network. These assaults are unique from those that were previously examined and referred to as DoS attacks, reduction of quality (RoQ) attacks, and routing infrastructure attacks since they do not immediately interrupt availability but rather work over time to completely disable a network. Although some of the individual attacks are straightforward, and power draining and resource exhaustion attacks have been discussed in the past, previous research has been mostly limited to other levels of the protocol stack, such as the medium access control (MAC) or application layers, and to the best of our knowledge, there is very little discussion of, and no thorough analysis or mitigation of, routing-layer resource exhaustion attacks.

2. Literature survey:

Vampire Attacks: Draining life from Wireless Ad-hoc Sensor Networks

AUTHORS: Eugene Y. Vasserman, Nicholas Hopper

In the fields of sensing and ubiquitous computing, one attractive research path is the development of ad hoc low-power wireless networks. Prior security work in this area has generally concentrated on denying communication at the routing or medium access control levels as the primary target for protection. This study investigates resource depletion attacks at the routing protocol layer, which render networks useless for good by rapidly depleting the power stored in their nodes' batteries. These so-called "Vampire" attacks are not limited to a single protocol, but rather depend on the characteristics that are shared by a variety of widely used categories of routing protocols. We have come to the conclusion that every single one of the analyzed protocols is vulnerable to Vampire attacks, which are destructive, difficult to detect, and simple to execute with as little as a single malicious insider delivering only messages that comply with the protocol. In the worst case scenario, a single Vampire has the potential to raise the overall energy consumption of the network by a factor of O(N), where N refers to the total number of nodes in the network. In this paper, we describe several approaches that may be used to defend against assaults of this kind, one of which is a novel proof-of-concept protocol that demonstrably limits the harm that can be inflicted by Vampires during the packet forwarding phase.

2) Vampire attacks: exploration & consequences

AUTHORS: Virjot k, Priyanka R

The Vampire assaults, also known as the resource depletion attack, are analyzed in depth during the course of this work. It does this by rapidly depleting the power stored in the batteries of the nodes that make up the network. All of the protocols are susceptible to Vampire attacks because they are discouraging, difficult to detect, and uncomplicated to carry out. All it takes is a single hostile insider sending a single message that complies with the protocol for an attack to be successful. In this section, the examination of vampire assaults and their repercussions is reviewed, and the solutions that have been presented up to this point are investigated.

3)Routing Techniques in Wireless Sensor Networks: A Survey

AUTHORS: Jamal N. Al-Karaki Ahmed E. Kamal

Small nodes that can sense their surroundings, do computations, and communicate wirelessly are the building blocks of wireless sensor networks. Numerous protocols for data transmission, power management, and routing have been developed expressly for wireless sensor networks (WSNs), for which energy awareness is a key component of the architecture. It's possible that different applications and network architectures will call for different routing techniques in WSNs. In this paper, we provide a comprehensive review of the most recent advancements in the field of WSN routing algorithms. Following an introduction to the difficulties inherent in the design of routing protocols for WSNs, a full analysis of routing strategies is presented. In general, the various routing strategies may be broken down into one of three groups that are determined by the underlying structure of the network: flit, hierarchical, and location-based routing. In addition, the operation of the protocol may be used to categorize these protocols according to multipath-based, query-based, negotiation-based, quality of service-based, and coherent-based categories respectively. In each routing paradigm, we investigate the design trade-offs that exist between reducing energy use and lowering communication overhead. In addition, we discuss the benefits and potential performance difficulties associated with each routing strategy. The paper wraps off by discussing some potential directions for further study.

4)Detection and Removal of Vampire Attack in Wireless Sensor Network

AUTHORS: Manish S., Bharat P

The wireless sensor network is a communication network that spans low-cost and low-energy sensor nodes, and its primary function is to detect and gather data on the surrounding physical environment. The sensing and ubiquitous computing properties of WSN opened the door to a wide variety of applications, which in turn boosted the number of study topics. WSN has been used in a variety of domains, including the military, forests, health care, inventory management, and others. Energy is a crucial component for sensor nodes, and a recently identified kind of assault known as a "vampire attack" is capable of rendering a network inoperable by depleting the battery life of sensor networks. In the study that has been suggested, a novel technique that is centered on energy threshold and packet broadcast threshold of network sensor nodes has been presented. The solution presented in the earlier study was restricted to the phase of packet forwarding alone and did not function with topology change. The method that has been suggested is straightforward, and it is also compatible with topology changes in the network.

4. SYSTEM ANALYSIS:

Existing System:

The Vampire attack will use any number of infected nodes to launch an assault on the service provided by the network. "Malicious node" refers to the node in a network that causes a rapid change in the behavior of the network. The energy of the nodes will be impacted as a result of the malicious nodes. The shortest route routing algorithm is used in order to establish the routing path. The route will not be altered in any way by the nodes that come in between. An assault by vampires could be possible in this scenario. The adversary nodes put together packets that had routing loops that were purposefully added.

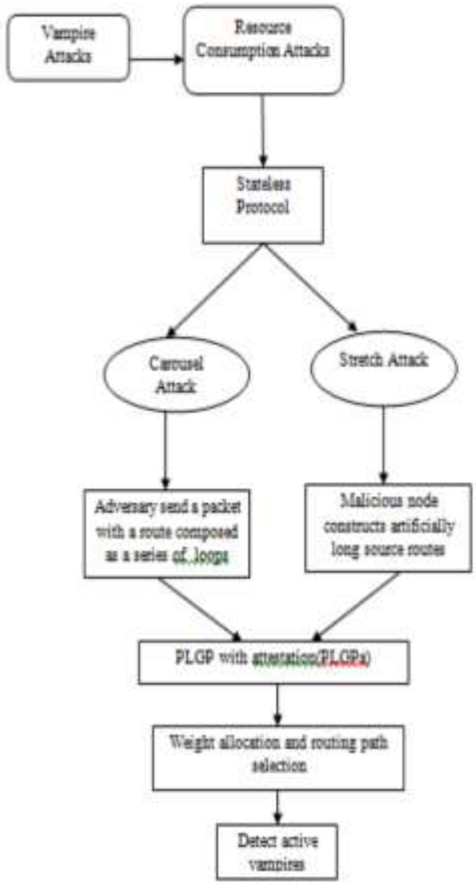
Proposed System

The newly suggested system will include all of the previously implemented system components. In addition to that, there is the operation of secure synchronization. The synchronization issue is resolved by the newly developed system, which does this by computing the transmission schedule by making use of the weight information and basing it on the suggested algorithm steps.

In addition, in order to reach a condition of stability in the network, it is necessary to synchronize all of the neighbor nodes, which may belong to a variety of clusters. Give a presentation on several methods for synchronizing the nodes that periodically broadcast content and presence updates to other nodes that are co-located across an ad hoc network. Synchronizing the periodic transmissions of nodes is the goal of the newly developed algorithms. As a result, this enables nodes to save the power of their batteries.

4. ARCHITECTURE

The direction that the nodes will travel is determined by the Randomized future peak detection. Using the NS-2, you may get the total number of nodes by using its distinct nodes id. The most power-efficient battery that also provides a secure synchronization will be taken into consideration when choosing the routing route. The primary purpose of the content-based multicasting protocol is to gather the content of packet transfer times and node weights in order to determine the route. The architectural diagram may be seen in figure 6. Describes the steps involved in providing the service in its entirety, which are listed below.


Vampire Attacks
Resource Consumption Attacks
Stateless Protocol
Carousel Attack
Stretch Attack
Adversary send a packet with a route composed as a series of loops
Malicious node constructs artificially long source routes
PLGP with attestation(PLGPa)
Weight allocation and routing path selection
Detect active vampires

Conclusion:

In this study, we introduced Vampire attacks, a novel family of resource consumption attacks that employ routing protocols to permanently disable ad-hoc wireless sensor networks by draining the battery power of the nodes in the network. These attacks do not rely on any specific protocols or implementations; rather, they take use of weaknesses that are present in a variety of widely used protocol types. We demonstrated many proof-of-concept attacks against typical instances of current routing protocols by using a limited number of weak adversaries. We then tested the effectiveness of these attacks on a randomly constructed topology consisting of 30 nodes. The findings of the simulation indicate that the amount of network energy that must be used during the forwarding phase rises by anywhere from fifty to one thousand percent, depending on the position of the opponent. In the theoretical worst-case scenario, the amount of energy used might go up by as much as a factor of O(N) for each opponent per packet, where N is the total size of the network. We presented defenses against several of the forwarding-phase assaults and introduced PLGPa, the first routing protocol for sensor networks that provably limits damage from Vampire attacks. This is accomplished by confirming that packets constantly make progress toward their destinations. During the topology discovery process, we could not provide a solution that was completely adequate for Vampire assaults; however, we did give some ideas about damage bounds that are conceivable with additional improvements to PLGPa. The derivation of damage boundaries and defenses for topology discovery, in addition to the management of mobile networks, is work that will take place in the future.

ACKNOWLEDGEMENT

The heading should be treated as a 3rd level heading and should not be assigned a number.

REFERENCES

[1] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, "Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly," MobiCom, 2004 study on the robustness of ad hoc networks against denial of service attacks.

[2] Gergely Acs, Levente Buttyan, and Istvan Vajda, in Gergely Acs, et al., Provably safe on-demand source routing in mobile ad hoc networks, IEEE Transactions on Mobile Computing 05 (2006), no. 11 [Provably secure on-demand source routing in mobile ad hoc networks].

[3] Tuomas Aura, "Dos-resistant authentication with client puzzles," presented at the International workshop on security protocols in the year 2001.

[4] Haowen Chan and Adrian Perrig, "Security and privacy in sensor networks," Computer 36, issue 10 (2003).

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

[6] Jing Deng, Richard Han, and Shivakant Mishra, Defending against path-based Denial of Service Attacks in Wireless Sensor Networks, presented at the ACM Workshop on the Security of Ad Hoc and Sensor Networks in 2005.

[7] INSENS: Intrusion-tolerant routing for wireless sensor networks, published in Computer Communications 29 (2006), number 2.

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

[9] Andrea J. Goldsmith and Stephen B. Wicker, "Design challenges for energy-constrained ad hoc wireless networks," published in IEEE Wireless Communications, vol. 9, issue 4, in 2002.

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

[11] Packet leashes: A Defense Against Wormhole Attacks on Wireless Ad Hoc Networks, INFOCOM, 2003. [This] article was published in 2003.

[12] Timothy J. McNevin, Jung-Min Park, and Randolph Marchany, "pTCP: A Client Puzzle Protocol for Defending Against Resource Exhaustion Denial of Service Attacks," Technical Report TR-ECE-04-10, Department of Electrical and Computer Engineering, Virginia Tech, 2004. [Citation needed] pTCP: A Client Puzzle Protocol for Defending Against Resource Exhaustion Denial of Service Attacks.

[13] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig are the authors. A clean slate method to secure sensor network routing, published at CoNEXT in 2006.

[14] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols," IEEE Transactions on Vehicular Technology 58 (2009), no. 1; Effects of denial-of-sleep attacks on wireless sensor network MAC protocols.

[15] Denial-of-service in wireless sensor networks: Attacks and countermeasures, IEEE Pervasive Computing 7 (2008), no. 1. David R. Raymond and Scott F. Midkiff.

[16] The reviving duckling: security concerns for ad-hoc wireless networks was presented at the International workshop on security protocols in 1999 by Frank Stajano and Ross Anderson.

[17] Anthony D. Wood and John A. Stankovic, "Denial of service in sensor networks," Computer 35, no. 10 (2002, September).

[18] Manel Guerrero Zapata and N. Asokan, Securing Ad Hoc Routing Protocols, published in WiSE in the year 2002.