Review of Resist to Vampire Attack using Wireless Ad-hoc Sensor Network

Trupti A Borgamwar[1] , Kanchan Dhote [2]

[1]P.G Student, Department of Electronics Communication Engineering/ TGPCET/ NAGPUR, INDIA.
[1] truptiborgamwar@yahoo.co.in
[2] Head of Department of Electronics Communication Engineering / TGPCET/ NAGPUR, INDIA.
[2] kanchan.dhote@rediffmail.com

ABSTRACT

An ad-hoc sensor and data routing in them is a most significant research direction in sensing. It is found that all examined protocols are susceptible to vampire attack, which is difficult to detect. In this project we explore resources exhausting attack at the routing protocol layer, which disables network permanently by quickly draining nodes battery power. In this project we discuss the method to reduce the vampire attack using PLGP-a identifying malicious attack. 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.

Keywords— Denial of service, security, routing, PLGP-a (parno ,luk, gausted and perrig wih attstations) ad-hoc networks, sensor networks, wireless networks.

1. INTRODUCTION

An ad-hoc sensor network is a decentralized collection of wireless mobile nodes forming a temporary network without the aid of any established structure. It will promise to present new application in the future as like, instantly deployable communication for first responder and military, on-demand computing power and continuous connectivity In WSN's ,act as router to relay every other node's packets to enhance performance and deployment i.e., the traffic originating from a node is usually passed through other nodes to the destination.

In this paper we consider the how routing protocol, to be secures its lack of protection from vampire attack. Vampire attack are not protocol specific in that they do not depend on design properties or implementation faults of specific routing protocols, but rather utilize common properties of protocol classes such as link-state, source routing, geographic, distance vector, and beacon routing. Neither do these attacks depend on flooding the network with huge amounts of data, but somewhat try to transmit as little data as possible to attain the biggest energy drain, preventing a rate limiting solution. These attacks are very hard to detect and prevent because Vampires use protocol compliant messages. Evaluate the vulnerabilities of existing protocols to routing layer battery reduction attacks. Existing work on secure routing attempts to confirm that intruder cannot cause path discovery to return an invalid network path, but Vampires do not modify discovered paths instead of that it uses existing valid network paths and protocol compliant messages. The process of routing a packet in an ad hoc wireless network. Hence, we define Vampire attacks as the composition and transmission of a message that causes an increase in the cumulative energy consumption by a network than if an honest node transmitted a message of identical size to the same destination.

2. LITRETURE REVIEW

Gowthami. M [1] Form this paper. The vampire attack is a resource depletion attacks at the routing protocol layer, which permanently disconnect the networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but rather depend on the characteristics of many popular classes of routing protocols. 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-ofconcept attacks against representative examples of existing routing protocols using a small number of weak adversaries. We proposed against some of the forwarding-phase attacks and against some of the forwarding-phase attacks and described PLGPa,. Derivation of damage bounds and defenses for topology discovery, as well as handling mobile networks, is left for future work.

G. Vijayanand [2] In this paper the security work in this area is priority and primarily focusing on denial of communication at the routing or medium access control levels. Finding of vampire attacks in the network is not a easy one. It's very difficult to detect, devastating .A simple vampire presenting in the network can increasing network wide energy usage. The proposed technique routing protocol are provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations and reduce the reimbursement.

Lina R Deshmukh [3] At the time of sensing and pervasive computing ad-hoc low-power wireless networks are an exciting research. First security work has first focused on denial of communication at the routing or levels of media access control. We find that all examined protocols are affected to Vampire attacks ,which are destructing, hard to detect, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages. In case of worst case, a single Vampire can increase network-wide energy usage by a factor of O (N), where N in the number of nodes of network. The methods we discuss to reduce the types of attacks which include a new proof-of- concept protocol that bounds the damage caused by Vampires during the packet forwarding phase. Depending on the location of the attacker, network energy expenditure during the forwarding phase increases. Authors proposed defences against some of the forwarding-phase attacks and PLGP-a.

Susan Sharon George [4] This paper focuses on a more devastating, difficult to prevent, and easy to carry out attack called Vampire attacks, which quickly drain nodes' battery power leading to the permanent disabling of nodes. In this we discusses methods to mitigate these types of attacks, by introducing a new protocol that limits the damage caused by Vampire attacks. This paper discusses a more devastating form of DoS attacks called Vampire attacks. Vampire attacks targets on depleting a nodes' battery power, leading to the permanent disabling of the node, and gradually the network.

A Vincy [5] In this project 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 ad-hoc sensor networks. The The data verification process is provided at both the server and client side. It provides comparatively high security. It reduced the intruder spoofing. In this we concentrate on the energy efficient protocols they divide the network to efficiently maintain the energy consumption of sensor nodes and perform data aggregation and fusion in order to decrease the number of transmitted messages to the sink. that have been developed for WSNs.

Eugene Y.Vasserman [6] In this paper explores resource depletion attacks at the routing protocol layer, which permanently damage the 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. Vampire 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. A source composes and transmits the packet to the next hop node, which in turn relays the packet further, until the packet reaches its destination. However, this multihop relaying can consume the resources at each node. So, the process of routing a packet itself leads to resource exhaustion. Further, a malicious node within the path traced by the packet can cause an increase in the energy consumption while sending the same number of messages as an honest node.

Vidya M. [7] This project explores resource exhausting attacks at the routing protocol layer, which disable networks permanently by quickly draining node's battery power. These attacks are not protocol specific, but rather rely on the class properties of routing protocols.. Here we discuss methods to alleviate these types of attacks, including a new concept protocol assured with proofs that provably bounds the damage caused by vampire attacks on nodes during packet forwarding phase. I have dedicated large part of my phases to explain Vampire Attacks, a new class of resource consumption attacks These vampire attacks are not protocol specific but rather expose their vulnerabilities to classes of protocols. Here I have explained about PLGP protocol which is mainly based on No-Backtracking property for depletion of vampire attacks.

Soram Rakesh Singh [8] The objective of this paper is to examine resource depletion attacks at the routing protocol layer, which attempts to permanently disable network nodes by quickly draining their battery power. Vampire can increase network-wide energy usage by a factor of O (N), where N is the number of network nodes. Methods to detect and secure data packets from vampires during the packet forwarding phase is discussed. PLGP with attestations (PLGP-a) is used for identifying malicious attack. M-DSDV routing protocol is used to detect and eliminate the resource depletion attack from the network. Defenses against some of the forwarding-phase attacks has been proposed and PLGP-a, The routing protocol has been used at the time of routing to make efficient energy utilization during the packet forwarding phase's-DSDV, routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently is proposed in this paper. Prevention of data packets from entering into a malicious node is left for future work.

Ambili M.A [9] In this we define that a Network survivability is the ability of a network keeping connected under failures and attacks, which is the most important issue in the design and performance of wireless ad hoc sensor networks. The paper projects its focus on the way in which the attack can be overcome in the best possible manner. The proposed system describes some methods and alternative routing protocols solution that help to detect and eliminate vampire attack and thus make the network live.An energy constraint intrusion detection scheme is introduced along with clean state secure routing protocol.

K.Vanitha [10] An ad hoc network is a group of wireless nodes, in which each node can communicate over multihop paths to any other node without the help of any pre-existing infrastructure such as base station or access points. So as an attempt to eliminate vampire attacks, three primary contributions has been introduced. i. Evaluation of the vulnerabilities of existing protocols. ii. Quantization of performance of various protocols in the existence of solitary vampire. iii. Modification of existing protocol to deplete vampire attacks. A new class of energy draining attacks that use routing protocols to permanently halt ad hoc wireless sensor networks by depleting nodes' battery power. Vulnerabilities exposed in existing protocols are evaluated. Performance of existing protocols is quantified using small number of adversaries in a randomly generated 30 node topology.

SHARNEE KAUL [11] In Wireless Sensor Networks the limitations of system are resources like battery power, communication range and processing capabilities. One of the major challenges in Wireless Sensor Networks is the security concerns. The attacks affecting these systems are increasing as they progress. One of the resource depletion attacks called vampire attacks are the major concern. They not only affect a single node but they bring down the entire system draining the power i.e. Battery power. In this paper, the system proposed overcomes this challenge by using the Energy Weight Monitoring Algorithm (EWMA) and the energy consumption is reduced to a great-extend. In this paper the Vampire attacks, a new class of resource consumption attacks that drain the battery power by using more energy were detected and mitigated. These attacks do not depend on any specific type of protocol or condition.

Vidya.M [12] In this paper a innovative approach for routing protocols, affect from attack even those devised to be protected which is short of protection from these attacks, which we call energy debilitating attacks, which enduringly disable networks by quickly draining nodes battery power. We showed a number of proof-of-concept attacks against representative examples of existing routing protocols. We also saw how to overcome these attacks by increasing the energy of the node in the network.

R.Saranya [13] Vampire attack is draining of node life from wireless ad-hoc sensor networks. Resource depletion attack permanantly disables networks by quickly draining nodes battery power. Vampire attacks are very difficult to detect because they attack the node only by sending protocol-compliant messages. PLGP with attestations (PLGP-a) is used for identifying malicious attack. M-DSDV routing protocol is used to detect and eliminate the resource depletion attack from the network. Defenses against some of the forwarding-phase attacks has been proposed and PLGP-a, the first sensor network routing protocol that reduces the damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. The routing protocol has been used at the time of routing to make efficient energy utilization during the packet forwarding phase. But it has not offered the satisfactory solution during topology construction which is left for future work.

2.1. Propose PLGP with attestations PLGP-a (Developed by parno,luk ,gausted and perrig with attestations)

PLGP-a uses this packet history together with PLGP' s tree routing structure so every node can securely verify progress which prevents any significant adversarial influence on the path taken by any packet which traverses at least one honest node .These signatures form a chain attached to every packet and allows any node receiving it to validate its path. To ensure that the packet has never travelled away from its destination in the logical address space, every forwarding node verifies the attestation chain. PLGP-a satisfies no-backtracking- All messages are signed by their originator. Attacker can only alter packet fields that are changed en route, so only the route attestation field can be altered, shortened, or removed entirely. Use one-way signature chain construction to prevent truncation. PLGP-a never floods and its packet forwarding overhead is favourable. It demonstrates more equitable routing load distribution and path diversity. Even without hardware, the cryptographic computation required for PLGPa is tractable even on 8-bit processor.

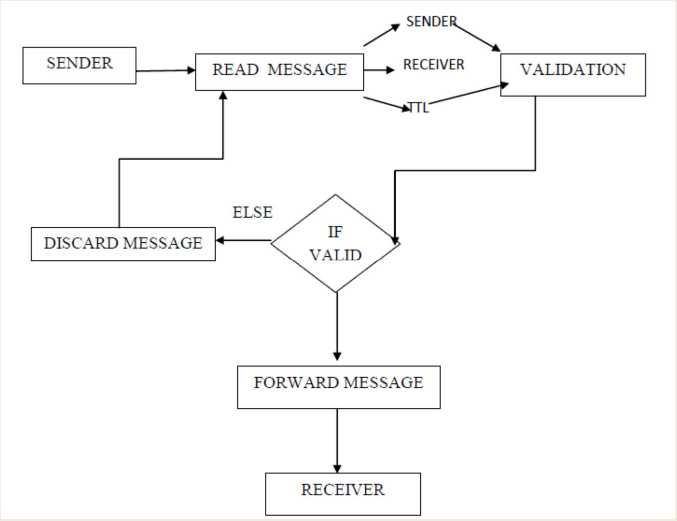

Fig:-1 Flow chart for PLGP-a.

2.2. PLGP-a satisfies no-backtracking

To show that our modified protocol preserves the no-backtracking property, we define a network as a collection of nodes, a topology, connectivity properties, and node identities, Honest nodes can broadcast and receive messages, while malicious nodes can also use directional antennas to transmit to (or receive from) any node in the network without being overheard by any other node. Honest nodes can compose, forward, accept, or drop messages, and malicious nodes can also arbitrarily transform them. Our adversary is assumed to control m nodes in an N-node network (with their corresponding identity certificates and other secret cryptographic material) and has perfect knowledge of the network topology. Finally, the adversary cannot affect connectivity between any two honest nodes. Since all messages are signed by their originator, messages from honest nodes cannot be arbitrarily modified by malicious nodes wishing to remain undetected. Rather, the adversary can only alter packet fields that are changed en route (and so are not authenticated), so only the route attestation field can be altered, shortened, or removed entirely. To prevent truncation, which allow Vampires to hide the fact that they are moving a packet away from its destination. For the purposes of Vampire attacks, we are unconcerned about packets with arbitrary hop counts that are never received by honest nodes but rather are routed between adversaries.

3. CONCLUSIONS AND FUTURE SCOPE

In this paper we studied that the 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 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. Authors proposed defenses against some of the forwarding-phase attacks and described PLGP-a, the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. Authors 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 PLGP-a.

As WSN's become more and more crucial to everyday life availability faults become less tolerable. Thus high availability of these nodes is critical and must hold even under malicious condition.

ACKNOWLEDGMENT

We would like to thank Eugene Gowthami. M Y.Vasserman, Lina R Deshmukh ,Susan Sharon George, Soram Rakesh Singh ,A Vincy, Ambili M.A ,,G. Vijayanand, K.Vanitha, Vidya M, SHARNEE KAUL and our anonymous reviewers for their very helpful comments on earlier drafts of this paper.

REFERENCES

[1] Gowthami.M, and Jessy Nirmal.A.G, "Mitigating Vampire Attack in Wireless Ad-Hoc Sensor Networks", IJARCST 2014 Vol. 2. Jan-Mar 2014.

[2] G. Vijayanand, R. Muralidharan, ''Overcome vampire attacks problem in wireless ad-hoc sensor network by using distance vector protocols", G. Vijayanand *et al*, International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 1, January- 2014.

[3] Lina R. Deshmukh and Amol D. Potgantwar, " Prevention of vampire attacks in WSN using Routing Loop", proceedings of IRF International conference,5th& 6th Feb 2014,Pune India.

[4] Susan Sharon George and Suma , " Attack-Resistant Routing for Wireless Ad Hoc Networks", International Journal of CS & IT, vol.5.(3),2014

[5] A.Vincy, and V.Uma Devi, "Maximizing Lifetime of Nodes in WirelessAd Hoc Sensor Network by PreventingVampire Attack", IEEE International Conference on Innovations in Engineering and Technology, 21st& 22nd Mar 2014.

[6] Eugene Y. Vasserman and Nicholas Hopper, " Vampire attacks: draning life from wireless ad-hoc sensor networks", IEEE Trans on mobile computing vol.12 no.2 year 2013.

[7] Vidya.M and Reshmi.S, "Contending Against Energy Debilitating Attacks in Wireless Ad Hoc Sensor Networks'', IJIRAE vol. 1. Mar 2014

[8] Soram Rakesh Singh and Narendra Babu C R, " Improving the Performance of Energy Attack Detection In WSN By Secure Forward Mechanism'', International Journal of Scientific and Research Publications, Vol 4, July 2014.

[9] Ambili M.A, Biju Balakrishnan, ''Vampitr attack: Detection and elimination in WSN", IJSR Vol- 3 April 2014 .

[10] K.Vanitha,V.Dhivya, ''A Valuable Secure Protocol to Prevent Vampire Attacks In Wireless Ad Hoc Sensor Networks", 2014 IEEE International Conference on Innovations in Engineering and Technology (ICIET'14) On 21st & 22nd March Organized by K.L.N. College of Engineering , Madurai, Tamil Nadu, India.

[11] SHARNEE KAUL, HELEN SAMUEL, JOSE ANAND, ''Defending against Vampire Attacks in Wireless Sensor Networks", International Journal of Communication Engineering Applications-IJCEA in March 2014.

[12] Vidya.M, Reshmi.S, ''Alleviating Energy Depletion Attacks in Wireless Sensor Networks", International

Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014.

[13] K.Abirami, R.Sarany , Dr.P.Jesu Jayarine, ‘‘Maintaining Lifetime of Wireless Ad-hoc Sensor Networks by Mitigating Resource Depletion Attack using M-DSDV”, International Journal for Research and Development in Engineering (IJRDE).