INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

REVIEW PAPER ON ENERGY DRAINING ATTACK IN WSN

MISS. APURVA KALE[1], PROF. G.D. GULHANE[2]

1. PG Research Scholar and Department of CSE, IBSS College of Engineering, Amravati.
2. Asst. Professor and Department of CSE, IBSS College of Engineering, Amravati.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

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. 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. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O (N), where N in the number of network nodes. 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.

Keywords: Denial of service, security, routing, ad hoc networks, sensor networks, wireless networks.

Corresponding Author: MISS. APURVA KALE

Access Online On:

www.ijpret.com

How to Cite This Article:

Apurva Kale, IJPRET, 2015; Volume 3 (9): 410-415

PAPER-QR CODE

INTRODUCTION

A wireless ad hoc sensor network has a wide range of application in the communication environment. It is mostly used in the remote areas, in the military communication, for finding environmental disasters etc. 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; high availability of these networks is a critical property, and should hold even under malicious conditions. The vampire attack consumes more energy from network than the original node during the transmission of message between nodes. 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 In this 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 paper 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. routing infrastructure attacks as they do not disrupt immediate availability, but rather work over time to entirely disable a network.

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 amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent.

1. Literature Review & Related Work :-

Eugene Y. Vasserman and Nicholas Hopper[1] Define 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. 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 O(N) per adversary per packet, where N is the network size. The 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 and 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. Derivation of damage bounds and defenses for topology discovery, as well as handling mobile networks, is left for future work.

G. Acs L. Buttyan, and I. Vajda [3] this paper shows attacks against ad hoc routing protocols can be subtle and difficult to discover by informal reasoning about the properties of the protocol. Demonstrated this by presenting novel attacks 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

J.-H. Chang and L. Tassiulas [3] In this paper authors had formulated the routing problem as maximizing the network lifetime. The new problem formulation has revealed that the minimum total energy (MTE) routing is not suitable for network-wise optimum utilization of transmission energy. Significant improvement can be made by the newly proposed routing algorithm in terms of maximizing the system lifetime, which can also be interpreted as maximizing the amount of information transfer between the origin and destination nodes given the limited energy.

2. Proposed Work And Objectives:-

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 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.

A. 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 node.

B. 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.

C. 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.

D. 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.

E. 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.

F. Malicious Node Elimination

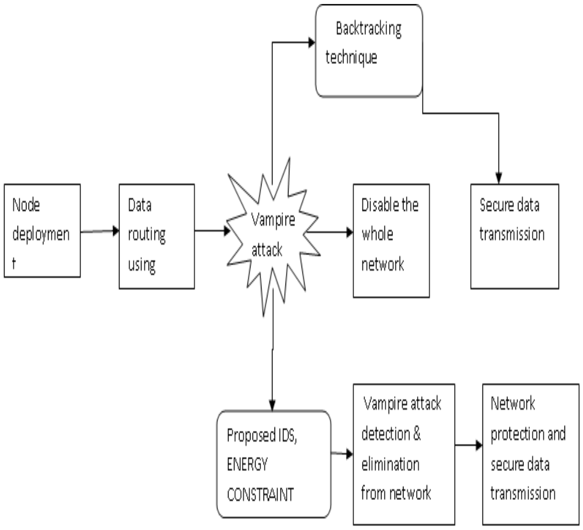
After the IDS process the malicious nodes detected. The TA trusted authority informs to all nodes in the network and eliminate the malicious node from the network. So by eliminating malicious node we can form a secure network

G. Graph Examination

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

In this proposed project concentrates on securing the network from the malicious attack. Our implementation results will efficiently detect and elimination vampire attack from the network. In order to detect and eliminating the vampire attack proposed system will going to implement certain intrusion detection system based on the energy level constraints.

3. Diagram:-


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

CONCLUSION

In this paper, 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. In wireless sensor networks where nodes operate on limited battery energy, the efficient utilization of the energy is very important. One of the main characteristics of these networks is that the transmission power consumption is closely coupled with the route selection. The energy efficiency has been considered in wireless ad hoc network routing, but the conventional routing objective was to minimize the total consumed energy in reaching the destination.

REFERENCES:-

1. Eugene Y. Vasserman and Nicholas Hopper "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks"-IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2, FEBRUARY 2013.

2. 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.

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

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

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

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

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

8. 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.

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

10. T.H. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, 2003.