iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** VIII **Month of publication:** August 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue VIII, August 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Review on Vampire Attacks in ad hoc Wireless Networks

Divya Gautam[1], Dheeraj Pal[2]
Computer Science & Engineering, Amity University, Madhya Pradesh

Abstract: ***A new class of resource consumption attacks is Vampire Attacks. Such attacks use different routing protocols to disable the ad hoc wireless networks by depleting the battery power of the node. Devices in ad hoc wireless networks require energy as their power supply because they are not in wired network. Power limitation in the network is one of the major issue. These attacks particularly expose the protocols by highlighting the vulnerabilities. Vampire attacks reduce the power of nodes by sending the message to the nodes which cause more power to be consumed by the network which in turn permanently disable the network. This paper contains the effect of Vampire attacks on wireless ad hoc networks and thus reduction in QoS.***
Key Words: MANET, Wireless Sensor network, Qos.

I. INTRODUCTION

The Nodes which communicates in wireless medium to form an arbitrary and dynamic network in known as wireless Ad hoc Networks(Fig1.1). The most important thing in the ad hoc networks is the change in the topology as links in the network is not fixed and common. Every time they change because of their ad hoc nature. There are many routing protocols used for establishing communication between the two nodes. The main task of routing protocol is to identify the network topology, as network topology is continuously changing in mobile environment in order to make sure that each node is getting a network.

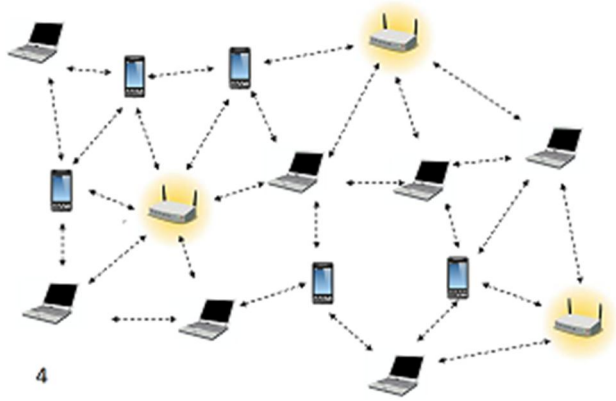


Fig 1.1

The new applications based on wireless sensor networks are emerging and they need a appropriate on request computing power, unbreakable connectivity and instantly deployable communication for military and the first responder. Such networks already display environmentally friendly conditions, industrial unit enactment, and troop setting out, to name a few solicitations. As wireless networks is more and more in use among users and companies so it's quite important to provide network connectivity all the time. The lack of availability of network can make the difference between businesses as usual and lost productivity, power outages, and environmental disasters. Thus high availability of these networks is a dangerous property, and should hold even under nasty conditions. Due to their ad hoc organizations, wireless ad hoc networks are on the whole vulnerable to denial of service DoS attacks and a big contract of investigation have been done to enhance survivability. These schemes can prevent attacks on the short term availability of a network; they do not attack that affect long-term availability the most permanent denial of service attack is to entirely deplete battery nodes. This is case of a resource running down attack, with battery control as the source of interest. Considered how protocols of routing, even those designed to be safe, lack of defenses from these attacks, which called as Vampire attacks, since they drain the power of the battery life from networks nodes.

These attacks are distinct from previously studied DoS, reduction of quality (RoQ), and routing infrastructure attacks as they do not

Volume 4 Issue VIII, August 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

disrupt immediate availability, but relatively work extra time to totally restrict a network. While some of the separate attacks are simple, and draining the power and resource energy 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 the knowledge there is little discussion, and no thorough analysis, mitigation, or routing-layer resource exhaustion attacks. Vampire attacks are not protocol-specific, in that they don't depend on properties of design or implementation faults of particular protocols of routing, but rather daring act general things of protocol classes such as link-state, space vector, routing of source and physical and ideal routing. Neither do these attacks depend on spilling over the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest draining of energy, checking an amount limiting solution. Since the Vampires use protocol-compliant messages, these attacks are very problematic to find and prevent.

A. Types of Vampire Attack

Vampire attack constitutes of two different types of attack called Stretch attack and Carousel attack. These two mainly focuses on reducing the energy of the nodes.

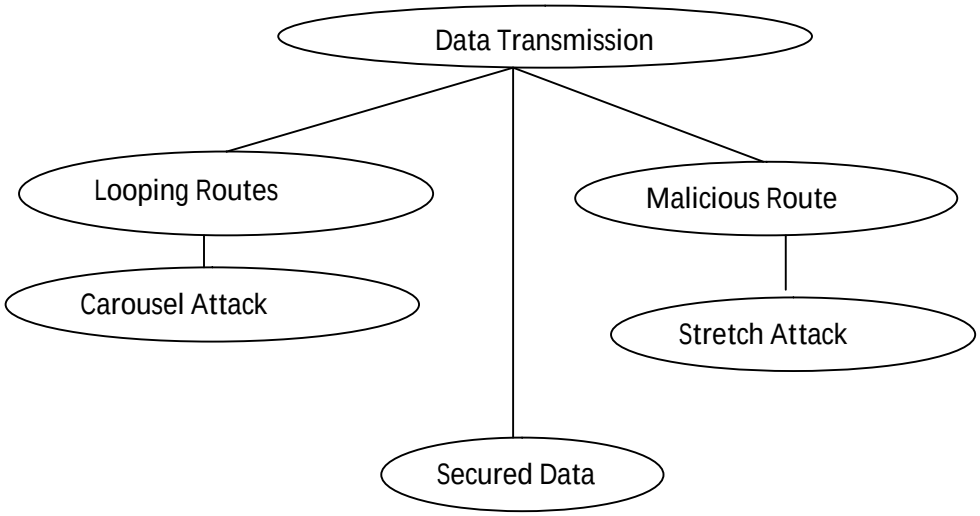


Fig 1.2 Types of Vampire Attacks

1) *Carousel attack:* In this type of attack, a malicious node sends a packet with a route composed as a series of loops, it targets source routing protocols by manipulating the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly travelling in the same set of nodes. Hence same node appears in the route many times. We call it the carousel attack, since it sends packets in circles. Times strategy can be used to increase the route length and in this way the energy is lost from the nodes.

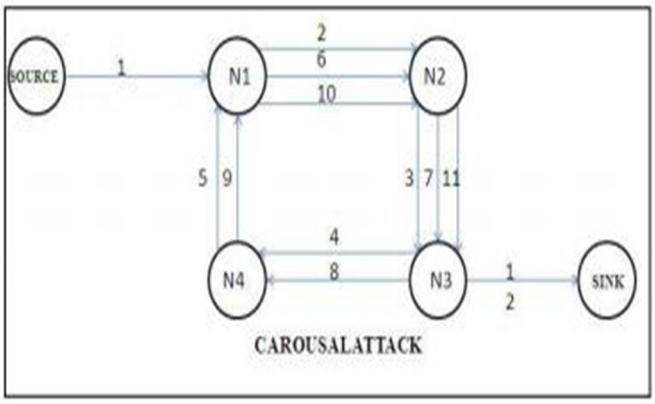


Fig.1.2 Carousel Attack

2) *Stretch attack:* In this type of attack, a malicious node artificially select long routes, causing packets to traverse a larger than optimal number of nodes. The honest path is very less distant but the malicious path is very long to make more energy

Volume 4 Issue VIII, August 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

consumption. In this stretch attack it mainly shows more uniform energy consumption for all the exiting nodes in the network. This attack mainly lengthens the route by causing more numbers of nodes to process the packet in the network. These attacks mainly make use of network-wide energy usage significantly at each and every node so that they are also affected until it reach destination.

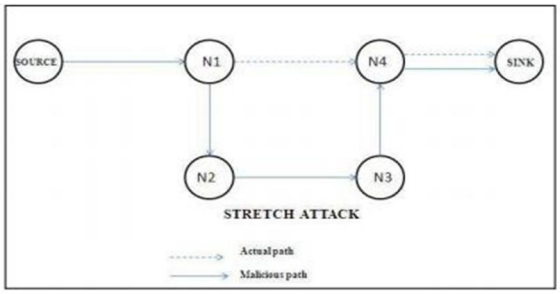


Fig 1.3 Stretch Attacks

II. ANALYSIS OF BATTERY DRAINING ATTACKS

In the table 1.1 various attacks and the disadvantages of those defenses is discussed in brief.

Table 1.1

S. No.	Attack	Features	Disadvantages of Defenses	References
1	Sleep Deprivation Torture	Prevents nodes from entering sleep cycle and depletes batteries faster	It considers attacks only at the Medium Access Control(MAC)	David R Raymond and Randy C Marchany ,2009
2	Resource Exhaustion	Mentions resource exhaustion at MAC and transport layers	Only offers rate limiting and elimination of insider adversaries	Anthony D Wood and John A.Stankovic,2002
3	Flood Attack	Multiple request connections to server, run out of resources	Punishes nodes that produce bursty traffic but may not send much data	Daniel J. Bernstein,1996
4	Reduction of Quality Attacks	Produce long term degradation in networks	Focus is only on transport layer and not on routing protocols.	Sharon Goldberg and David Xiao,2008
5	DoS Attacks	Malefactor overwhelms honest nodes with large amounts of data	Applicable only to traditional DoS, Doesn't work with intelligent adversaries i.e. protocol compliant	Jing Deng and Richard Han,2005
6	Wormhole attack & Directional Antenna attack	Allows connection b/w two non neighbouring malicious nodes : disrupt route discovery	Packet Leashes: Solution comes at high cost and is not always applicable	INFOCOM,2003
TECHNOLOGY		FEATURES	DISADVANTAGES	REFERENCES
Minimal Energy Routing		Increase the lifetime of power constrained networks using less energy to transmit and receive packets	Vampire attacks increase energy usage even in minimal energy routing	Jae-Hwan Chang and Leandros Tassiulas,2004

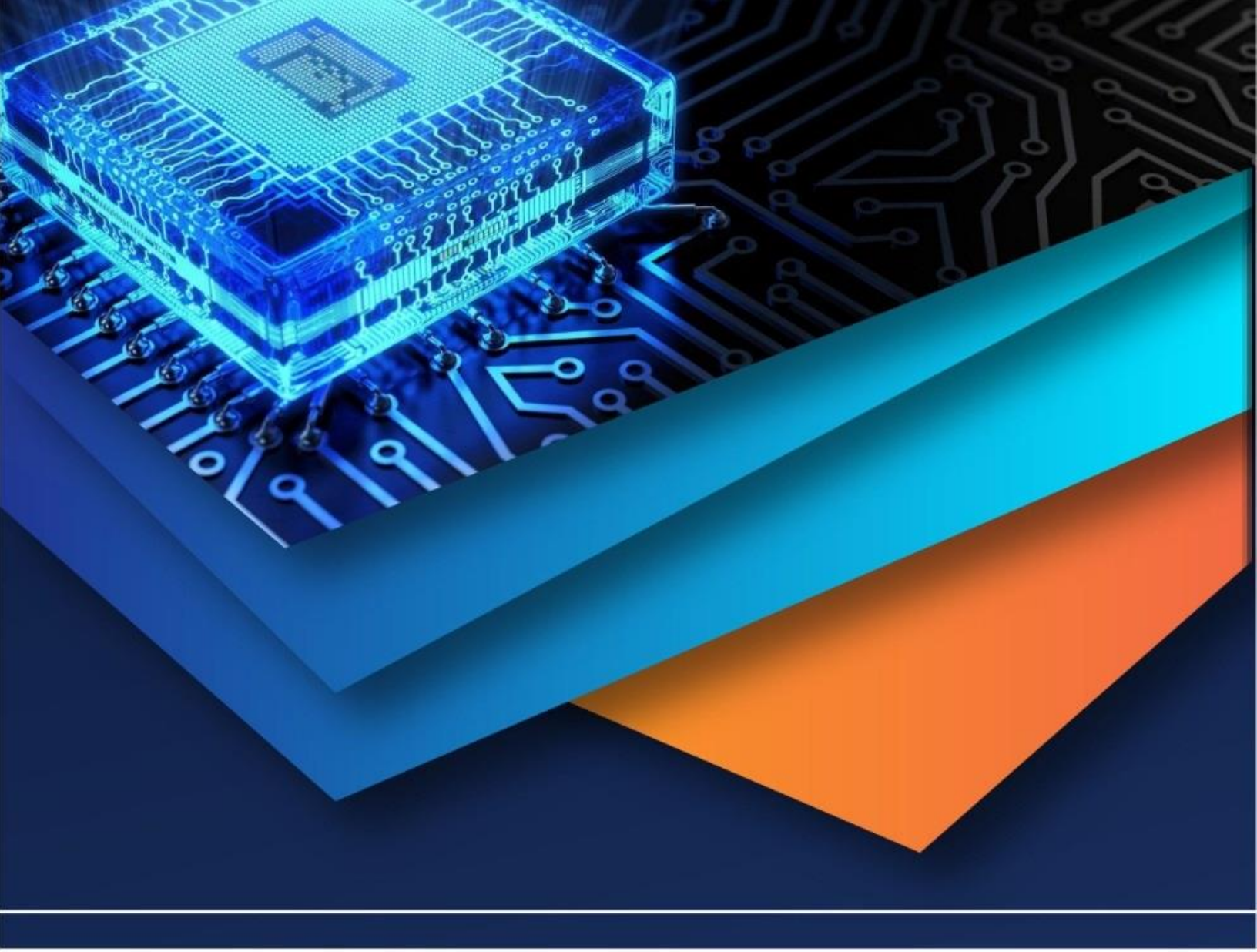
III. CONCLUSION AND FUTURE WORK

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 putting into practice, but rather interpretation vulnerabilities in amount of popular protocol programs. In the avoidance of data from Vampire attacks process it can only be able to detect and find the attacks has been done. The various proposed systems are ineffective in stopping the vampire attack as discussed in the paper.

In future it is possible to detect and mitigate vampire attacks by detecting its effect on the various working layers. So these attacks can be avoided if known what the area of the attack is.

REFERENCES

[1] Frank Stajano and Ross Anderson, The resurrecting duckling: security issues for ad-hoc wireless networks, International workshop on security protocols, 1999.
[2] Haowen Chan and Adrian Perrig, Security and privacy in sensor networks, Computer 36 (2003)
[3] Denial of service attacks(Timothy J. McNevin, Jung-Min Park), 2004
[4] Path-quality monitoring in the presence of adversaries(] Sharon Goldberg, David Xiao),2008.
[5] Packet leashes: A defence against wormhole attacks in wirelessad hoc networks, INFOCOM, 2003.
[6] Securing ad hoc routing protocols,(Manel Guerrero Zapata and N. Asokan), 2002.
[7] P.Goyal, V.Parmar, R. Rishi,"MANET:vulenerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.
[8] S.Y.Han, D.Lee, "An Adaptive Hello Messaging Scheme for Neighbor Discovery in ONDemand MANET Routing Protocols", IEEE COMMUNICATION LATTERS, VOL.17. NO.5.MAY 2013.
[9] S.Pandey, V.Prakash, S.Yadav, "QOS Optimization of Multipath Routing in MANET", International Journal of Emerging technology, Volume 3,.Issue 8, August 2013.
[10] M.Swathi, B.Pravallika, N.V.Muralidhar," Implementing And Comparison of MANET Routing Protocols using NS2", International Journal of Emerging technology, Volume 4, Issue 2, February 2014 | [6] S.Arvind Kumar, D.Divakaran, "Detecting and Avoiding Network attacks using routing protocol in Wireless Sensor networks", COMPUSOFT, volume.3, Issue.4, April 2014.
[11] G.Vijyanand, R.Muralidharan," Overcome vampire Attacks problem in wireless ad hoc sensor network by Using distance vector protocols", International Journal Of Computer Science and Mobile Applications" Vol.2, Issue.1, January2014.
[12] M.G.Aruna, G.Y.Nivedita, "Vampire Attacks: Wearing Out Life of Wireless Adhoc Sensor Networks", ISOR Journal of Computer Engineering, Volume.16, Issue 3, June 2014.
[13] J.Anand, K.Sivachandar,"Vampire Attack Detection in Wireless Sensor Network", International Journal of Engineering Science and Innovative Technology, Vol.3, Issue.4, July 2014.
[14] L. Santhaosh, A.V.Krishna Mohan, "Prevention of Resource Attack in Wireless Sensor Network" Proceedings 5th SARC-IRF International Conference, Bangalore, India, May, 2014.
[15] S.Kaul, H.Samuel, J.Anand," Defending against Vampire attacks in wireless sensor networks", International Journal of Communication Engineering Applications, Volume 5, Article C084, March 2014 | [12] G. Yan, K.Ibrahim, Basic simulator for Wireless ad hoc Network, computer science department, VA 23529 | [13]Fan Li, Y. Wang, "Routing in Vehicular Adhoc Networks Networks: A Survey", IEEE vehicular Technology Magazine, Volume 2, Issue.2, June 2007



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY