Impact Factor Value 4.046 e-ISSN: 2456-3463
National Conference on Quality Up-gradation in Engineering, Science and Technology (NC-QUEST018)
Organized by College of Engineering and Technology, Dhanamgaon Rly-444709
International Journal of Innovations in Engineering and Science, Vol. 3, No.6, 2018
www.ijies.net

Securing on Demand Source Routing in Mobile Ad-Hoc Networks by Vampire Attacks

Mr. Palash P. Butle[1], Ms. Renuka M. Dev[2] , Prof. Amol V. Zade[3]

[3]Assitant Professor,[1-2]Students,
Dept. of Computer Science Engineering, DES'S COET Dhamangaon Rly, AMRAWATI -444709

Abstract-*Mobile Ad-hoc Network (MANET), is a sort of remote system which is foundation less and versatile in nature .MANET takes after multicast correspondence the same number of uses in MANET are assemble arranged in nature. MANET is vulnerable to various sorts of assault because of their extraordinary and inborn qualities, for example, absence of brought together specialist, restricted hub's battery control and so on. A standout amongst the most intense assault in Ad-hoc arranges is the Vampire assault. Vampire assault is the sort of asset exhaustion assault in which a vindictive hub is produced and these malevolent hubs makes and send messages with more happiness regarding hub's battery control than with the legitimate hub and prompts moderate consumption of hub's battery life. In this paper we proposed distinctive moderation technique to recognize and to diminish vampire assault .We considered the impact of vampire assault on AODV convention and the hypothetical based mimicked charts are likewise exhibited to investigate the execution of the Ad-Hoc organize in the nearness and nonattendance of Vampire assault by utilizing network simulator 2(ns2).*

Keywords—*Denial of service, security, routing, ad-hoc networks, draining life.*

I-INTRODUCTION

Wireless networking devices uses some sort of radio frequencies in air to transmit and receive data instead of using any physical media. Wireless networking devices operates in two mode i.e. infrastructure mode and ad-hoc mode. In infrastructure mode a connection is establish between wireless network and a wired Ethernet network and for the infrastructure mode there is requirement of at east one base station or access point. While the Ad-hoc mode in contrast to the infrastructure mode there is no requirement of any access point. Ad-hoc mode is a technique for remote gadgets to specifically speak with each other. Versatile Ad-Hoc arrange don't gangs any perpetual framework or physical spine. Portable hubs in the system progressively setup ways among themselves to transmit bundles to the goal. Because of versatility of the hubs MANET ought to have a few qualities which make them recognizable from traditional wired systems. MANET are self organizing and adaptive in nature which means that the nodes are spontaneously forming and deforming the networks and updating the routing table associated to each node. Thus MANET follows dynamic routing protocol.

A. Routing protocol-Routing is the process of moving a packet of data from source to destination. Routing is a key feature of internetworking. Each intermediary computer performs routing by passing along the message to the next computer. Part of this process involves analyzing a routing table to determine the best path. Routing protocol may be static routing protocol or dynamic routing protocol.

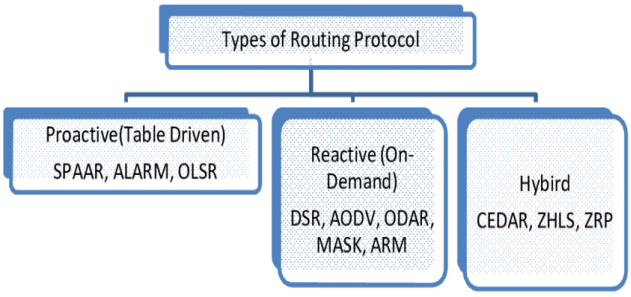

Fig 1: Routing protocol in MANET

There are mainly two routing protocols i.e. proactive and reactive. Table driven routing protocols which is also called as proactive protocol since they maintain the routing information even before it is needed. Proactive protocol classified into four types FSR, FSLS, OLSR, and TBRPF. The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. On demand routing protocol are also called as since they don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes in order to transmit and receive the packets. Reactive routing protocol is of two types AODV and DSR. Hybrid Routing, commonly referred to as balanced-hybrid routing, is a combination of distance-vector routing, which works by sharing its knowledge of the entire network with its neighbors and link-state routing which works by having the routers tell every router on the network about its closest neighbors. In this paper we are considering the effect of vampire attack on AODV protocol. In MANET communication starts between the nodes within each other's transmission range by broadcasting control messages between themselves directly. However, nodes beyond each other's range have to rely on some other node to relay messages. Challenges of MANET lead to security issues which include routing security, data forwarding security, link layer security, key management, intrusion detection and so on. In MANET many applications are group oriented in nature and can therefore benefit from multicast communication. Due to these inherent characteristics of MANET they are susceptible to different security attacks.

B. Security attack in MANET - The security attacks in MANET can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. The classification of security attack is intrinsic because the attacker can feat either of the attack.

Passive attack: In passive attack attacker does not disturb the usual operation of the network, it just snoops the data exchanged in the network without altering it.

Active Attack: In contrast to passive attack an active attack goes to alter or destroy the data being exchanged in the network. Means in general passive attack take the data without altering it active attack disturb and alter the data. According to domain of the attacks, the attacks can be classified into two categories: Insider and Outsider attacks. Insider attacks are done by compromised nodes, which are actually the part of MANET network. Outsider attacks are carried out by outside or external nodes. Outsider attacks are easy to recognize and can be detected/prevented with cryptographic techniques (Encryption, Decryption, Private Key. However, insider attacks are very complicated. These attacks cannot be prevented with simple cryptographic techniques.

C. Related Work:

Imad Aad et al. [2] gives a detail explanation of 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.

Jae-Hwan Chang et al. [11] gives an overall understanding of Vampire attacks that has been defined as a new class of resource consumption attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes' battery power. 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

Gergely Acs et al. [3] discussed that the attacks against ad hoc routing protocols can be subtle and difficult to discover by

informal reasoning about the properties of the protocol. It is also demonstrated by presenting novel attacks on Ariadne. 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.

John Bellardo et al. [5] examined the 802.11 MAC layer and identified a number of vulnerabilities that could be exploited to deny service to legitimate users. Also 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.

Laura M. Feeney [19] has introduce energy consumption model which is treated as synonymous with bandwidth energy-consumption model needs to be compatible with packet-level, mobility-oriented simulations

John R. Douceur et al. [16] explained that the Peer-to-peer systems often rely on redundancy to diminish their dependence on potentially hostile peers. If distinct identities for remote entities are not established either by an explicit certification authority or by an implicit one these systems are susceptible to Sybil attacks, in which a small number of entities counterfeit multiple identities so as to compromise a disproportionate share of the system.

Daniel J. Bernstein et al. [7] gives an overall understanding of TCP and SYN cookies. There are several disparate ideas woven together on the TCP and SYN cookies threads. Even though most TCP implementations have a common ancestor, the details depend on the operating system and even the version of the operating system. Therefore any attempt at a general discussion will need to make some assumptions for the sake of being definite and the conclusions may not apply to all implementations or even in precise detail to any current implementation

Joppe W. Bos et al. [9] presented new software speed records for encryption and decryption when running AES-128 on the 8-bit AVR microcontroller, the Cell broadband engine architecture and NVIDIA graphics processing units. To achieve these performance records a byte-sliced implementation is employed while a T-table approach is used for our GPU implementations. The implementations targeting the Cell and GPU architectures process multiple streams in parallel to obtain the results.

Martin Feldhofer et al. [13] have explained a security-enhanced RFID system which allows the strong cryptographic authentication. With these security-enhanced RFID systems, we pave the way for new security-demanding applications and for the everyday usage of RFID technology. A symmetric challenge-response authentication protocol was proposed which was integrated into the existing ISO/IEC 18000 standard. The AES implementation has a chip area of 3,595 gates and has a current consumption of 8.15 μA at a frequency of 100 kHz. The encryption of 128 bits requires about 1000 clock cycles.

I. Vampire Attack-

Vampire attack means creating and sending messages by malicious node which causes more energy consumption by the network leading to slow depletion of nodes battery life. Wireless ad-hoc networks are mostly exposed to denial of service (DOS) attack because of their Ad-hoc organization. The most permanent denial of service attack is to entirely exhaust the batteries of the sensor nodes .Here the resource of interest is node's battery power. This is called Resource depletion attack. Resource depletion attacks at the routing protocol layer, which entirely disable networks by quickly exhausting the energy of the nodes. These resource depletion attacks are not precise to any particular protocol, but moderately trust on the properties of many popular classes of routing protocols. This resource depletion attacks are easy to bring out using malicious insider which is sending only protocol-complaint messages. A single adversary that is enemy can increase the network-wide energy usage by a factor O (N), where N is the number of network nodes in the worst case.

A. Types of vampire attack-

Vampire attack

Attack on stateless protocol Attack on state full protocol

Carousel attack

Stateless protocol -A stateless protocol is a protocol with no any conservation of information by either source or destination. Data packets are sent from sender without expectation of acknowledgments from receiver. In stateless protocol there is no need of any type of server that retains or conserves the session information or status about each communications senders and receiver for the duration of multiple requests. A UDP connection-oriented session does not maintain information about the communication session between sender and receiver so the UDP session is a stateless protocol session. Examples of stateless protocols include the Internet Protocol (IP), and the Hypertext Transfer Protocol (HTTP).

***Carousel* attack –**carousel attack is a type of vampire attack in which an adversary or malicious insider transmits a data packet with the route which is composed of series of loops such that same nodes appears in route many times. This type of strategy can be used to increase the path length of the route in the network. Fig 1 addressed to carousel attack. From fig 1 , the packet sent from source to the sink visit the same nodes again and again instead of reaching to the destination. This creates a loop and hence increases the route length of the network.

Stretch attack- Stretch attack is the type of stateless vampire attack in which malicious nodes or adversary chooses a longest path instead of choosing a shortest and secure path defined by the source node while transferring the packets to the destination.fig 2, in stretch attack the honest node are shown by dotted line while the malicious nodes are shown by dash line.

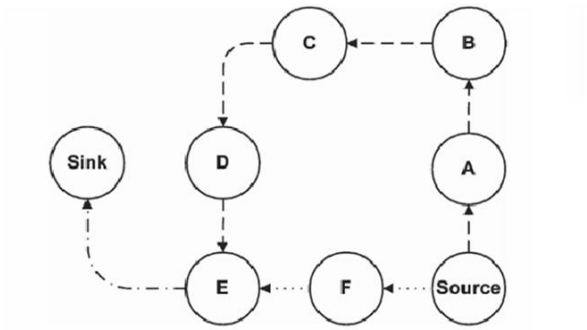

Fig 1: Carousel attack

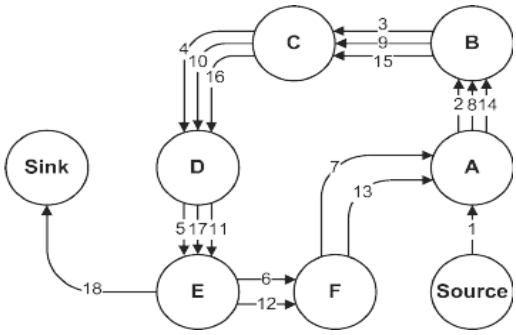

Fig 2: Stretch attack

C. State full protocol-

In contrast to the stateless protocol a protocol that requires to maintains a server to retain all the information of the communication session between sender and receiver is known as the state full protocol. A TCP connection-oriented session systems maintain all the information about the communication session so it is a 'state full' connection

Directional Antenna attack: Directional antenna attack is a vampire attack in which more energy of mobile node wasted by restarting the packets in various parts of the network. In this attack an adversary deposits the packet at the arbitrary locations of the network. The original packets get traversed by the nodes that not have had to process it. So energy of these nodes gets wasted in the directional antenna attack. These Attacks is also known as half-wormhole attacks, since it constitutes a private communication channel. It is also use to mitigate wormhole attack.

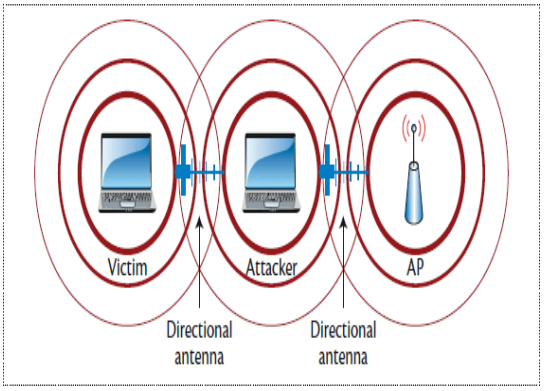

Fig 3: Directional antenna attack

Malicious discovery attack-

Malicious discovery *attack* is also known as spurious route attack. It falsely claims that link is down or claims a new link in non-exiting node.

D. Countermeasures -We are dealing with the vampire attack which is energy depletion attack i.e. it consumes more energy of the nodes while sending the packets or transmitting the data. To deal with this attack in network we need a system which can detect, identify and remove the attack. As we are dealing with the vampire attack which is either sending packets through long route or sending the packets through the nodes which involves the loop in the sending path of the network that means the vampire attack is initially attacking the nodes and then through these nodes attack starts to operate maliciously on packet. So there is need to stare at nodes initially to stop the vampire attack from introducing in the network. So in this report we have introduced the new concept called the clustering. To overcome this attack through concept clustering, we will be making the group of the nodes called as the cluster. Each cluster contains group of approximately 20-30 nodes in it. In addition we allocate one node as the master node among the cluster which is called as the head of the cluster. The header node is selected on the basis of the criteria of how old the node is in the clustering or we can say that the oldest node among them all is selected as the header node in the cluster. The header node has most crucial work to do as it is now responsible to manage the network, the header node has all the information of other nodes in the cluster, such as the routing path, the source from which packet is being delivered, the destination to which the packet is to be sent, the information of previous node and also the foremost node. The header node pays attention to every action of node in the cluster i.e. it makes sure that the packet which is to be sent is going through the right path. If somewhere down the line, any misbehave by node exists or certain malicious behaviour by any node

in the cluster is noticed the header node instantly takes action against these nodes by suspending them or by isolating them from the communication path. There can be number of clustering units in the field which completely depends upon the number of nodes in the communication.

III. CONCLUSION AND FUTURE SCOPE

In the conclusion we define the vampire attack that the type of resource depletion attack as one of the most powerful attack in mobile ad-hoc network which completely destroy the network by draining battery power from mobile nodes. We proposed different types of vampire attacks such as carousel attack, stretch attack, packet forwarding and directional antenna attack. We explore different mitigation methods to bind the damage from vampire attack. Ad-hoc wireless sensor network promises exciting new applications future work.

Reference

[1] *Daniel Bernstein and Peter Schwabe, New AES software speed records, INDOCRYPT, 2008.*

[2] Imad Aad, Jean-Pierre Hubaux, and Edward W.Knightly, Denail of service resilience in ad hoc networks, mobicom,2004.

[3] Gergely Acs, Levente Buttyan, and Istvan Vajda, Provably secure on demand source routing in mobile ad hoc networks, IEEE Transactions on mobile computing 05(2006),no.11.

[4] Tuomas Aura, Dos-resistant authentication with client puzzles, International workshop on security protocols, 2001.

[5] Daniel Bernstein and Peter Schwabe, New AES software speed records, INDOCRYPT, 2008.

[6] INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications 29 (2006), no. 2.

[7]Daniel J. Bernstein, Syn cookies, 1996. http://cr.yp.to/syscookies.html

[8]I.F. Blake, G. Seroussi, and N.P. Smart, Elliptic curves in cryptography, Vol. 265, Cambridge University Press, 1999.

[9]Joppe W. Bos, Dag Arne Osvik, and Deian Stefan, Fast implementations of AES on various platforms, 2009.

[10]Haowen Chan and Adrian Perrig, Security and privacy in sensor networks, Computer 36 (2003), no. 10.

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

[12] Thomas H. Clausen and Philippe Jacquet, Optimized link state routing protocol (OLSR), 2003.

[13] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, Strong authentication for RFID systems using the AES algorithm, CHES, 2004.

[14]INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications 29 (2006), no. 2.

[15]Packet leashes: A defense against wormhole attacks in wireless Ad-Hoc networks, INFOCOM, 2013.

[16]Jing Deng, Richard Han, and Shivakant Mishra, "Defending against path based DOS attacks in wireless sensor networks" ACM workshop on security of ad hoc and sensor networks, (2005).

[17]Rahul C. Shah and Jan M.Rabaey,"Energy aware routing for low energy ad hoc sensor networks"(2002). [18]T. English, M. Keller, Ka Lok Man, E. Popovici, M. Schellekens, and W. Marnane, A low-power pairing-based cryptographic accelerator forembedded security applications, SOCC, 2009.

[19]Laura M. Feeney, An energy consumption model for performance analysis of routing protocols for mobile ad hoc networks, Mobile Networksand Applications 6 (2001), no. 3.