A Comparative Study of the Attacks on the Routing Protocol

Priti Lahane
MET.BKC.IOE, Nashik, India

ABSTRCT
A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. However, because routing protocol communicates with immediate neighbors and throughout the network it is vulnerable to different kinds of attack which hampers the availability of nodes in case of ad-hoc networks. This paper presents a comparative study of the attacks on the routing protocol. They are mainly sleep deprivation attack, Dos attack, state full protocol attack, stateless protocol attack, wormhole attack and vampire attack. This has been done by studying the impact these attacks gives on routing protocol. This would pavethe way to build a head-to-head comparative study that shows the kind of damage these protocols can cause and make protocols working miserable.

Keywords
Denial of services, Wireless sensor network

1. INTRODUCTION
Routing protocol Packets may pass through several networks on their way to destination. Each network carries a price tag, or a "metric"The router uses a "routingtable"to determine the path.There are routing protocols that different routing functionalitythat use multiple paths rather than a single path inorder to enhance the network performance. The fault tolerance (resilience) of a protocol is measured by the case that an different path exists between source and destination when the primary pathfails.A more useful metric forroutingprotocol performance is network survivability. The routing protocol should give the ensured that connectivity in a network is remain for as long as possible, and the energy health of the entire network should be of the same order Energy Aware Routing, protocol tries to ensure the survivability of low-energynetworks.

2. RELATED WORK
The routing protocol attack which is a categories in two ways i.e. attack on stateless protocol and attacks on state full protocol which is discuss below.

2.1 Directional Antenna Attack
Directional antenna preventers are able deposit a packet in different areas of the network, while it forwards the packet locally. The energy consumption happen nodes not have to process the original packet, but with the expected additional honest energy expenditure of O(d), where d is the network diameter, making the expected length of the path to an arbitrary destination from the furthest point in the network. The directional attack is a half-wormhole attack [2], since a directional antenna forms a private communication channel, but the node on the other end is may not be malicious. It can be performed more than once, depositing the packet at various distant points in the network, at the additional cost to the adversary for each use of the directional antenna. Packet Leashes may be a preventer but they may not protect against malicious message sources, only intermediaries can protected.

2.2 Wormhole Attacks
Wormhole attacks can be severe threats to routing protocols and some security enhancements is also needed. Largely routing protocols, nodes depend on the neighbor discovery procedure to create the local network topology. Because of the attackers' behavior towards the nodes i.e tunneling the neighbor discovery beacons through wormholes, the good nodes will get wrong information about their neighbors. This will choose a non-existent route. Zero interaction authentications (ZIA) [2] are able to protect the data on mobile devices from the illegal access. Decryption of file is needed only when an authentication token that is own by the user can directly communicate to the device through a short-range wireless channel. If a wormhole exists between the token and the device, the data may be disclosed.In ad hoc networks; malicious nodes may carry wormhole attacks for fabrication of a wrong scenario on neighbor relations among mobile nodes. The attack is responsible for threatening the safety of ad hoc routing protocols and some security enhancements is also needed. In a wormhole attack, if the malicious nodes have a dedicated channel, the tunneling procedure can be conducted in real time. Since the packets are resent in the exactly same way, encryption or authentication alone cannot prevent the attacks. Other nodes cannot tell whether the packets are from the real originator or from the sender. A group of collusive attackers can form a wormhole that has as many ends as the number of malicious nodes. Wormhole attacks are severe threats to routing protocols [5].

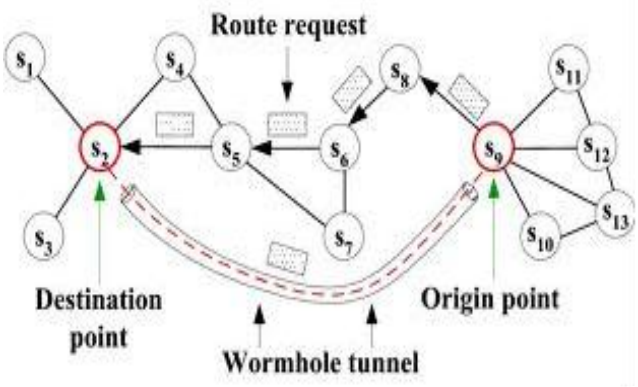

Figure 1.1 Wormhole attack

2.3 Denial of Services Attack
Path-based DoS attacks and defenses in routing protocols[1], including the use of one-way hash chains to minimize the number of packets sent by a respective node, limiting the rate of transmit ion of packets. This is useful for protection against traditional DoS, where the Dos floods honest nodes with large amounts of data, it is not useful for protection against

"intelligent" adversaries who uses small number of packets or packets has not been originates at all.

The DOS attack usually has the properties like Malicious which is performed deliberately, not accidentally. Accidental failures are areas of fault-tolerance and reliability engineering. Since such failures can produce equal amount of destructive results as DOS attacks, these properties are important contributions for the robustness of WSNs. A successful DOS attack degrades some capability or service in the WSN. Still the effect cannot be measurable, for example if it is prevented altogether, it can be said that an attack has occurred, but this attack has not. Note that disrupting the affected service may not be the end goal of the attacker [2]. Often the effect of an attack is much greater than the required effort to mount it. For example, sending a forged packet that overflows a remote buffer takes little effort, but may crash the server until an operator intervenes. Even in distributed-denial-of-service (DDOS) attacks, the effort to "recruit" zombies and issue an order to food a victim is small compared to the food of traffic that reaches the target. This kind of asymmetry is not necessary, but makes an attack easier and more economical for the perpetrator. Remote: Especially in distributed systems, an attacker usually can (and wishes to) carry out an attack over the network[4]. Often this is by unauthenticated or lightly authenticated users. The high profile of many types of DOS attacks would make physical presence uncomfortable for the attacker [6].

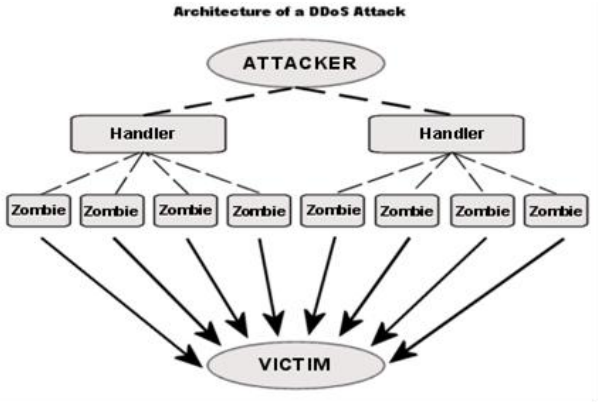

Figure 1.2 Distributed Denial of Service attack.

2.4 Vampire Attack

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 ofprotocol classes such as link-state, distance-vector, sourcerouting and geographic and beacon routing. Neither do these attacks depend on flooding the network with maximum amounts of data, but rather try to transmit minimal data as possible to achieve the largest energy drain, preventing a rate limiting solution. Since Vampires use protocol vulnerability these attacks are very difficult to detect and prevent [7].

Routing protocols are a victim to Vampire attacks, which are destroying, difficult to detect, and are easy spread using few malicious insider sending only protocol used messages. In the worst case, a single Vampire can increase network-wide energy usage because of the use of all the nodes in it[8].

These attacks are different from DoS, reduction of quality and routing structure attacks as they do not interfere immediate availability, but try to work overtime to totally disable a network.

3. COMPARISON

Packet leashes general mechanism for detecting and thus preventing against wormhole attacks this is achieved by geographical leash and temporal leash. A leash is any information that is added toa packet designed to restrict the packet's maximum allowed transmission distance. A geographical leash ensures that the destination of the packet is within a certain distance from the source. A temporal leash ensures that the packet hasan upper bound on its lifetime, which restricts the maximumtravel distance, since the packet can travel at most at the speedof light. Either type of leash can prevent the wormhole attack, because it allows the receiver of a packet to detect if the packettraveled further than the leash allows.

Defending against the Denial of services attack is carried out by defend against de authentication attack for this anaccess point, upon receiving a deauthentication request, places it on a waitqueue for a certain period of time. If time expires and no other traffic from thatnode has been seen, the request is honored and the node de authenticated. Onthe other hand, if traffic from that node is seen before time expires, the requestis dropped and not honored. Vampire attack is very difficult to detect and prevent because it uses the vulnerabilities of routing protocol[9]. For detecting vampire attack the combination of nodes forming a network is used then a packet containing data has been forwarded from each and every node the vampire attack forward the packet from each node consuming the energy of nodes and making the node lifeless this way detection of vampire attack has been done after detection for prevention the packet has been dropped at the same moment and prevent the attack from spreading[10].

4. CONCLUSION

The vampire attack detection has been done by using number of nodes and forwarding the data packets to different nodes which will drain the life of nodes which is very harmful for the data transmission process as compared to other network In this paper the comparative study of routing protocol attack has been done which will be useful for identifying solution for routing protocol attack and the general approach for working toward it..

5. REFERENCES

[1] John Bellardo and Stefan Savage, 802.11 denial-of-service attacks: real vulnerabilities and practical solutions, USENIX security, 2003.

[2] Packet leashes: A defense against wormhole attacks in wireless ad hoc networks, INFOCOM, 2003.

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

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

[5] Wormhole Attacks in Wireless NetworksYih-Chun Hu, *Member, IEEE,* Adrian Perrig, *Member, IEEE,* and David B. Johnson, *Member, IEEE*

[6] Jing Deng, Richard Han, and Shivakant Mishra, Defending against pathbasedDoS attacks in wireless sensor networks, ACM workshop onsecurity of ad hoc and sensor networks, 2005.

[7] Vampire attacks: Draining life from wireless ad-hoc sensor networksEugene Y. Vasserman and Nicholas Hopper Kansas State University of Minnesota, IEEE

[8] David B. Johnson, David A. Maltz, and Josh Broch, DSR: the dynamic source routing protocol for multihop wireless ad hoc networks, Ad hoc networking, 2001

[9] Guang Yang, M. Gerla, and M.Y. Sanadidi, Defense against low-rate TCP-targeted denial-of-service attacks, ISCC, 2004.

[10] Manel Guerrero Zapata and N. Asokan, Securing ad hoc routing protocols, WiSE, 2002

6. AUTHOR'S PROFILE

Priti Lahane received the B.E and M.E in Computer Science and Engg. Currently working as a Assistant Professor, Department of Information Technology in Mumbai Education Trust, Bhujbal Knowledge City, Institute of Engg. Nashik, INDIA.