Stealthy Attacks in Wireless Ad Hoc Networks

Rohinee Bankar Prajakta Mehetre Swati Salve

ABSTRACT

Stealthy packet dropping comprises two attacks: Identity Delegation and Colluding Collision. Stealthy packet dropping disrupts the packet from reaching the destination through malicious behavior at an intermediate node. Wireless ad hoc networks do not have a router as gateway, every node can act as the gateway. The source and target node necessarily need to be out of range. The intermediate node is actually legitimate in nature, but is made to act in such a way that it does not route the packet to the destination

Keywords

packet dropping, wireless ad hoc networks.

1. INTRODUCTION

Wireless Ad hoc Network is a network of PCs communicating with each other without an infrastructure. Ad hoc Networks are an important platform in military warfare [5],[6]. A typical ad hoc network must contain at least two workstations connected to each other. Several traffic attacks on wireless ad hoc networks include wormhole [1], rushing [2], and Sybil [7] attacks. Other attacks are blackhole, selective forwarding, and delaying, in which, respectively, a malicious node drops data (entirely or selectively) passing through it, or delays its forwarding. In a wormhole attack an attacker neither modifies packets nor takes over any wireless node but captures packets in one region and tunnels it to another region. The attacker can then carry out flow analysis or a blackhole attack. In a blackhole attack black holes accept packets and drop them without letting the source realizing that the packet did not reach the destination. Consider a scenario in which a node called S wants to transfer a packet to a compromised node I. I is supposed to relay the packet to the next-hop node T. In the identity delegation attack, node E which lies in the range of S uses I’s identity and transmit the packet. Since E is almost at the same place as S, T does not receive the packet while S is made to believe that I relays the packet to the next hop. In the colluding collision attack, two malicious nodes lying in the range of T transmit packets simultaneously which results in a collision of packets at T. Therefore, T is unable to receive the correct packet while the malicious nodes appear to be performing their functionality correctly.

TABLE 1: Summary of Stealthy Attacks[8]

Attack name	**Attack Description**	**Attack instantiation requirement**
Identity Delegation	Delegate the relay responsibility to a colluding partner close the sender.	One compromised node in the route between sender and receiver and one external node close to the compromised node.
Colluding Collision	Simultaneous transmission to create a collision at the next hop.	One compromised node in the route between sender and receiver and one external node close to the next hop from the compromised node.

2. IDENTITY DELEGATION

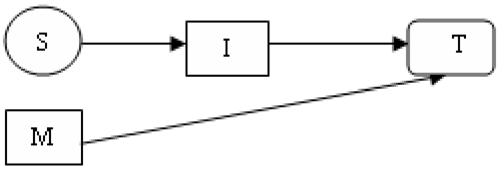

Figure 1: Identity delegation illustration scenario[8]

In this form of the attack, the malicious node is close to the sender. Consider the scenario shown in Figure 1, node S sends a packet to a node I to be sent to node T. I lies in the range of S and T. The attacker delegates the identity of I to node M close to S. So when S sends the packet to I, M uses the delegated identity of I and transmits the packet. Since S and T are out of range of each other, T will again not be able to receive the packet sent by S.

3. COLLUDING COLLISION

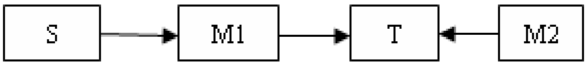

Figure 2: Colluding collision illustration scenario[8]

Consider the scenario shown in Figure 2. The malicious nodes M1 and M2 lie in the range of T. M1 receives a packet from S to be sent to T. M2 sends a packet to T immediately when M1 does the same. Thus T is unable to get the packet sent by M1.

4. PROPOSED WORK

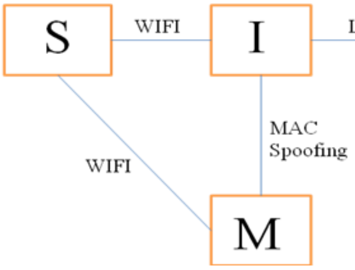

Figure 3: Network setup and Identity Delegation

Consider scenario shown above where source node S wants to send a packet to target node T. To show a stealthy attack S and T have to be out of range of each other. So we connect S and intermediate node I by a wireless ad hoc network and I and T by LAN Cable.

If S and T cannot ping each other we use "route add" command at I to establish a route between S and T. Another alternative to establish the route is to use jpcap at I to transfer the packet from I's wired IP address to its wireless IP address and vice a versa.

For Identity Delegation

The Address Resolution Protocol (ARP) maps the IP addresses and MAC addresses on local networks. Malicious node M should access the ARP table of S which contains IP and Mac address of I. It should then replace I's Mac address with its own. Thus it is spoofing I's Mac address. So whenever S will send a packet to I using I's IP address the packet will eventually be transferred to M since Mac addresses of M and I are the same.

5. EVOLUTION OF AD HOC NETWORKS

Traffic problem increases in the network due to:

- emerging wireless network elements such as ad-hoc routers and sensors in the existing framework and
- end-to-end service abstractions that facilitates application development.

These problems are caused due to environments such as cellular data services, WiFi facilities, Ad-hoc mesh networks for broadband access, vehicular networks and sensor networks. These wireless application scenarios increase service requirements for the future Internet as summarized below:

- Many users want to access the net from different geographic locations by using mobile network devices.
- Up to date location services that provide information on geographic position.
- Evolution of distributed control of network topology.
- **Security and privacy considerations for mobile nodes and open wireless channels.**
- **Reduced monopolizing of a network.**
- Sensor network features such as aggregation and in-network Processing.
- Economic motives to encourage efficient sharing of resources.

6. PROBLEMS IN AD HOC NETWORKS

- **Autonomous**- No centralized administration entity is available to manage the operation of the different mobile nodes.
- **Dynamic topology**- Nodes can be added and removed from the network dynamically. Links of the network vary timely.
- **Device discovery**- Whenever a new node is added in the network it needs to be identified and made known to all existing nodes in the network to facilitate appropriate route selection.
- **Bandwidth optimization**- Wireless links have relatively lower capacity than the wired links.
- **Limited resources**- Battery power and storage capacity are limited resources of mobile nodes.
- **Scalability**- The network should be able to provide a satisfactory service even in the presence of a large number of nodes.
- **Limited physical security**- Mobility implies higher security risks such as a shared wireless medium can be used by both legitimate network users and malicious attackers. Spoofing and denial-of-service attacks should be considered.
- **No infrastructure and self operated**- The ad hoc network should work efficiently in case any node moves out of its range.
- **Poor Transmission Quality**- An ancient problem of wireless communication caused by several errored sources that result in degradation of the received signal.
- **Ad hoc addressing**- Challenges in standard addressing scheme to be implemented.
- **Network configuration**- Since the entire ad hoc network infrastructure is dynamic in nature there is dynamic connection and disconnection of the variable links.
- **Topology maintenance**- Updating information of dynamic links among nodes in ad hoc networks is a major challenge.

7. IMPLEMENTATION DETAILS

7.1 JPCAP

Jpcap is a software that receives and sends network packets from Java applications. It can:

- capture raw packets directly from the wire.

- identify packet types and determine corresponding Java objects (for Ethernet, IPv4, IPv6, ARP/RARP, TCP, UDP, and ICMPv4 packets).
- filter the packets according to user-specified rules before dispatching them to the application.

Jpcap can be used to develop many kinds of network applications, including:

- network and protocol analyzers
- network monitors
- traffic loggers
- traffic generators
- network intrusion detection systems (NIDS)
- network scanners
- security tools

7.2 ARP Spoofing

ARP spoofing is a hacking technique where an attacker modifies the ARP table of a machine. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing may allow an attacker to access data frames on a LAN, modify the traffic, or even stop the traffic. Often the attacker can carry out other attacks, such as denial of service, man in the middle, or session hijacking.

To access your current ARP entries use the following command: arp -a

To add an entry in the ARP table, use the following command: arp –s <IP Address> <Mac Address>

Similarly to delete an entry in the ARP table, use the following command: arp –d <IP Address>

As shown in Figure 3, the malicious node M will send ARP packets to node I regularly after a particular time interval so that the ARP table of S will contain an entry of I's IP address and M's Mac address. Thus, when S will send a packet to I using I's IP address it will eventually reach M instead of reaching I since the ARP table of S contains M's Mac address for I's IP address due to Mac Spoofing.

8. ACKNOWLEDGMENTS

The authors would like to thank the University of Pune and Prof. Dr.B.S Karkare (The Principal of Vishwakarma Institute of Information technology) for giving the opportunity to work in this domain. A special thanks to Prof. K.H.Wanjale(HOD) , Prof. S.A.Tiwaskar and Prof. S.J.Thaware for their complete support and guidance.

9. REFERENCES

[1] Y.C. Hu, A. Perrig, and D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proc. ACM Workshop Wireless Security (WiSe '03), pp. 30-40, 2003.

[2] Y.C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, pp. 1976-986, 2003.

[3] I. Khalil, S. Bagchi, and N. Shroff, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks," Proc. Int'l Conf. Dependable Systems and Networks (DSN '05), pp. 612-621, 2005.

[4] I. Khalil, S. Bagchi, and N.B. Shroff, "MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks," Ad Hoc Networks, vol. 6, no. 3, pp. 344-362, May 2008.

[5] I. Stojmenovic, Handbook of Sensor Networks: Algorithms and Architecture. Wiley, 2005.

[6] F. Ye, H. Luo, J. Cheng, S. Lu, and L. Zhang, "A Two-Tier Data Dissemination Model for Large-Scale Wireless Sensor Network," Proc. Eighth ACM Ann. Conf. Mobile Computing and Networking, pp. 148-159, 2002.

[7] Q. Zhang, P. Wang, D. Reeves, and P. Ning, "Defending against Sybil Attacks in Sensor Networks," Proc. Int'l Workshop Security in Distributed Computing Systems (SDCS '05), pp. 185-191, 2005.

[8] I.Khalil, S.Bagchi, "Stealthy Attacks in Wireless Ad hoc Networks: Detection and Countermeasure".