A Review on Impersonation Attack in Mobile Ad-Hoc Network

Nidhi Gour[1],Monika Agarwal[2],Heena Singh[3],Ajay Kumar[4]
[1,2,3](M.Tech Scholar, Department of Computer Science, JECRC University, Jaipur, Rajasthan, India)
[4](Assistant Professor, Department of Computer Science, JECRC University, Jaipur, Rajasthan, India)

ABSTRACT- *An ad hoc network is a collection of mobile nodes that dynamically form a temporary network and are capable of communicating with each other without the use of a network infrastructure or any centralized administration. Due to Open medium, dynamic topology, Distributed Cooperation, Constrained Capabilities ad hoc networks are vulnerable to many types of security attacks. Impersonation attack is special case of integrity attacks where by a compromise node impersonates a legitimate node one due to the lack of authentication in current ad hoc routing protocol. In this paper, we are describing the causes of impersonation attack and their vulnerable effects which give chance to a malicious node for doing other attacks too.*
We confirm with simple risk analysis that impersonation attacks offer attractive incentives to malicious criminals and should therefore be given highest priority in research studies. Our approach is to detecting and eliminating impersonation attack using secure routing protocols.

Keyword- *MANET, Impersonation attack, Risk analysis*

I. INTRODUCTION

Wireless network is the network of mobile computer nodes or stations that are not physically wired. The main Advantage of this is communicating with rest of the world while being mobile. The disadvantage of this is their limited bandwidth, memory, processing capabilities, open medium and less secure compared to wired devices. An ad hoc network is a collection of wireless mobile nodes that forms a transitory network without any centralized administration in such an environment. MANETs consist of mobile nodes that are free in moving in and out in the network.

Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network.

Seeing that wireless systems are increasingly being used for critical communication it is becoming a challenge to keep electronic data transmissions secure. In general, it is difficult to implement effective security in small-footprint devices having low processing power, low memory capacity and using unreliable, low bandwidth. It is proving challenging to adapt wire-line technologies to the constrained mobile/ wireless environment, enforce backward compatibility, and take account of heterogeneity [3]

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network [1].

II. IMPERSONATION ATTACK

Michel Barbeau et. al have explained in [2] that Enabling wireless technologies like WTLS (Wireless Transport Layered Security) within WAP (Wireless Application Protocol), WEP (Wired Equivalent Privacy), TKIP (Temporal Key Integrity Protocol), Counter Mode CBC-MAC, Wireless PKI, Smart Cards, offer security with various degrees of success. On the other hand wireless devices (smart phones, PDAs, etc.) with Internet connectivity are becoming easy targets of malicious code (Cabir, Skulls, Mquito, Wince.Duts, Metal Gear, Lasco, Gavno, etc.).

In reality wireless networks lack appropriate security infrastructure, and give potential attackers easy transport medium access. Rogue wireless access points deserve particular attention since they are not authorized
for operation. They are usually installed either by employees (that do not understand security issues) or by hackers (to provide interface to a corporate network). Attention has been paid to finding rogues by using:

Wireless sniffing tools (e.g., Air Magnet or Net Stumber), walking through facilities and looking for access points that have authorized Medium Access Control (MAC) addresses, vendor name, or security configuration,

- A central console attached to the wired side of the network for monitoring (e.g., Air Wave),
- A free Transmission Control Protocol (TCP) port scanner (e.g., Super Scan 3.0), that identifies
  enabled TCP ports.

Attacks can be undertaken from an armchair or war-walking or even war-driving. Malicious attackers can be divided into two types.

1) Focused attackers:

These are full time, dedicated professionals who have nothing better to do than target a specific enterprise.

2) Opportunistic attackers:

That will attack a wireless network because it is there (a target of opportunity with no functional level of security that can be easily compromised). Even if several attacks have been addressed including active/passive eavesdropping, man-in-the-middle, replay (including de-authentication and de-association), session hijacking, using traffic analysis, and masquerading, existing authentication schemes cannot fully protect hosts from well-known *impersonation attacks*.

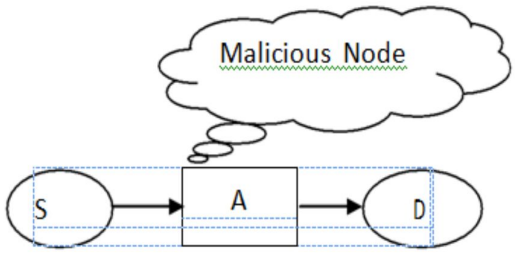
Impersonation attack is also called spoofing attacks in which a malicious node uses IP address of another node in outgoing routing packets. The aims of impersonation attacks to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key private key or even password of the nodes.[1]

A defective node or an opponent may preset multiple identities to a peer to peer network in order to appear and function as distinct node. By becoming part of the peer to peer network the opponent may then overhear communication.

The introduction of impersonation attack in any network there is a reduction of throughput in the network. Packet delivery ratio also drops and there is an increases checksum error and packet loss ratio.

In cryptography and computer security is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the
attacker.

The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances. A man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other — it is an attack on mutual authentication. So it is very important for any network to detect the impersonation nodes and isolate them from the network for the proper and smooth functioning of MANET.



In above figure S is the source and D is destination and A is intermediate node. Another node that is malicious node replaced its identity with intermediate node and hides its actual identity with other nodes. So when source send any message to other nodes within the network then that malicious node also get that message and misused all the information Impersonation attack is main cause of colluding attack in which compromised node injected malicious node in to the network and make number of replicated copy of malicious node for doing future attacks in overall network.

III. RISK OF IMPERSONATION

Impersonation takes the form of device cloning, address spoofing, unauthorized access, rogue base station (or rogue access point) and replay. [2]

- Device cloning consists of reprogramming a device with the hardware address of another device. This can be done also for the duration of one frame, which is an operation termed MAC address spoofing. This is a known problem in unlicensed services such as Wi-Fi/802.11. It is an enabler for unauthorized access and various attacks such as the de-association or de-authorization attack.

- In Wi-Fi/802.11 networks, the identity of a device, i.e. its hardware address, can be easily stolen over the air by intercepting frames. Presently, no wireless access technology offers perfect identity concealment over the air.

- Impersonation of a legitimate user can be done to obtain unauthorized access to a

wireless network. There are three options for authorization:

- Device list-based: If device list-based authorization is used only, then the probability of a subscriber impersonation attack is likely.

- X.509-based : X.509-based authorization uses certificates installed in devices by their manufacturers. X.509-based authorization is used, the probability for a subscriber to be the victim of impersonation is possible in particular if certificates are hard coded and cannot be either renewed or revoked.

- EAP-based:The Extensible Authentication Protocol (EAP) is a generic authentication protocol can be actualized with specific authentication method, If EAP-based authorization is used, we believe that at this time it is safe to say that the probability of a subscriber impersonation attack is possible.

The risk of impersonation in wireless networks is critical since the threat can be materialized into several forms of attack. Countermeasures are needed to address the threat.

IV. DETECTING IMPERSONATION ATTACKS USING DEVICE AND USER PROFILES

As Michel Barbeau et. al have explained in [2], this attack is carried out by obtaining the MAC address of a legitimate device, using tools that are readily available, e.g. NetStumbler. This address is programmed into another device and subsequently used for obtaining unauthorized access to a Wireless Local Area Network.

- The continued use of an access control list (ACL), based on MAC addresses, which are easily supple, is no longer a viable strategy.

- In order to address device cloning and MAC-address spoofing, authentication based resolution strategies and intrusion detection-based countermeasures have been proposed.

- The use of public-key cryptography, the use of intruder location or user mobility patterns, is less susceptible to forgery and impersonation attacks. For one thing, as intrusion detection mechanisms, both exploit behavioral characteristics or features, which are more difficult to forge or replicate.

- Both strategies require that an association, between a given MAC-address and its corresponding profile, be maintained for the purpose of detecting MAC-address spoofing. Essentially, it exemplifies the concept of using two or more pieces of identification for corroborating the identity of individuals.

- AirDefense does prevent MAC address spoofing by looking at the address prefix. Nevertheless, this approach is limited in that the IDS makes a distinction between devices based only on the manufacturer's identification.
- The need to identify devices, there is an opportunity to further explore the use of device-based and user-based features for addressing the aforementioned problem.

We described the safety measure against all of above attack in AODV routing protocol for Ad hoc network that have been proposed by the authors in [4],[5] that are:
a) Secure Ad hoc On Demand Distance Vector (SAODV)
b) Authenticated Routing for Ad hoc Network (ARAN)
c) TESLA
d) ARIADNE
e) Secure Efficient Ad hoc Distance Vector (SEAD)
f) Security Aware Routing **(**SAR)
g) Secure Routing Protocol (SRP)
h) Cooperation Of Nodes Fairness In Dynamic Ad-Hoc Networks (CONFIDENT)
g) Novel Approach for Secure Routing Protocol **(**NASRP)

V.CONCLUSION

In this paper we propose a strategy to counter the Impersonation attacks prevalent in Mobile Ad Hoc Networks. The solution is found to achieve the required security with minimal additional delay and overhead. Additionally to authenticate the non mutable fields using digital signature the eligibility of intermediate node is blocked.
Our future work intends to be in the direction of simulating the protocol in a larger network and try to minimize the overhead and delay by using the Intermediate node eligibility.

REFRENCES

[1] Aakansha Jain, Khushboo Sawant "Effect of Impersonation Attack on Mobile Ad Hoc Network" *Indian Journal of Research,2(3),* March 2013, 17-19.

[2] Michel Barbeau, Jyanthi Hall and Evangelos Kranakis "Detecting Impersonation Attacks in Future Wireless and Mobile Networks" *Natural Sciences and Engineering Research Council of Canada*

[3]LathaTamilselvan and Dr. V. Sankaranarayanan "Prevention of Impersonation Attack in Wireless Mobile Ad hoc Networks"*International Journal of Computer Science and Network Security, 7(3),* March 2007, 118-123.

[4] Tahira Farid and Anitha Prahladachar "Secure Routing with AODV Protocol for Mobile Ad Hoc Networks " University of Windsor.

[5] Preeti Bathla, Bhawna Gupta "Security Enhancements in AODV Routing Protocol" *International Journal of Computer Science and Technology Vol. 2*, june 2011,295-298.