INTRUSION DETECTION SYSTEM FOR WIRELESS SENSOR NETWORKS-MAC SPOOFING

[1]Jaharsh, [2]Lola Tejaswi
[1]Research Scholar, Department of Computer Science and Engineering, Amrita VishwaVidhyapeetham, Coimbatore.
[2]Research Scholar, Department of Computer Science and Engineering, Amrita VishwaVidhyapeetham, Coimbatore.
[1]jaharsh93@gmail.com, [2]lola.tejaswi@gmail.com

Abstract: Wireless sensor networks (WSNs) have emerged as an important and new area in wireless and mobile computing research. They have numerous functionalities that find their applications in our daily life. Security is hence an important issue in WSNs. The sensing technology combined with processing power and wireless communication makes it powerful for being exploited in abundance in future.MAC spoofing attack is the most common attack in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage, it creates more sophisticated results like reducing the trust of the entire system. In this paper we propose to use a physical property associated with each node , hard to falsify, and compute a unique signature value to each node using RSA algorithm and transmit it hidden in the data field at random positions in each packet, thereby increasing the randomness of the security.

Keywords: IDS (Intrusion Detection System), WSN (Wireless Sensor Networks), MAC(Media Access Control),MAC Spoofing.

1. INTRODUCTION

Intrusion Detection System (IDS) is an essential part of security for any network. As technology evolves the development of wireless networks and the attacks possible on these networks becomes a cause for concern. Wireless networks are easier to crack since the medium of communication is insecure. The problem of cooperative intrusion detection in battery-powered wireless mesh and sensor networks is challenging, primarily because of the limited resource availability to the participating nodes. In this paper, the primary focus is laid on the attacks that perpetrate on data transmitted between nodes – namely Mac-Spoofing. This is a major type of attack that these networks are susceptible to. In Mac spoofing, the intruder tries to spoof the mac-address of an authentic node which is already present in the network. The damage caused by this attack is very severe and can compromise the trust of the whole network. In this proposed solution, we provide, in addition to the MAC-address, a secondary Hash-value which is unique to each node and is placed at different random positions each time. The idea is to transmit the signature value in the packet without letting the intruder know the difference between the data and the signature value in the transmitted packet.

2. MAC ADDRESS

A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most network technologies, assigned by the manufacturer of a network interface card (NIC).The standard IEEE 802 format for printing MAC-48 addresses in human-friendly form is six groups of two hexadecimal digits, separated by hyphens (-) or colons (:), in transmission order (e.g. 01-23-45-67-89-ab or 01:23:45:67:89:ab).MAC addresses are formed according to the rules of one of three numbering name spaces managed by the Institute of Electrical and Electronics Engineers(IEEE): MAC-48, EUI-48, and EUI-64.This address is spoofed by an intruder who claims himself to be the authentic .

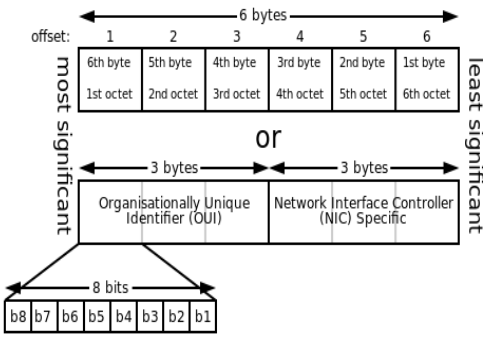

Figure 1: STRUCTURE OF MAC-ADDRESS

2.1 Known Attacks Using MAC Address Spoofing:

De-authentication Attack:

To join a wireless network a client has to choose an access point and authenticate itself to it before any further communication may start. This authentication protocol also includes a message that allows nodes to de-authenticate from each other with one single message. This message is in no way protected against spoofing. Hence anybody can send this message with a forged identity. As a consequence the attacked client will not receive further messages unless it re-establishes authentication. With one single de-authentication message the attacker provokes six messages for the re-authentication between the attacked client and the access point. If this attack is replayed periodically a victim could be kept from joining the network indefinitely.

2.2 Power-saving Attack:

IEEE 802.11 power conservation functions also provide several vulnerabilities. A client, wishing to enter sleep mode, informs the access point (AP) so that it can buffer all inbound traffic for later transmission. Due to the timely synchrony of the clients and the AP all clients in power-saving mode know when to wake up to receive the traffic indication map (TIM). This TIM indicates if the AP has buffered packets for the client. Now the client may wake up and send a poll frame to signal the AP its readiness to receive the buffered packets. This mechanism offers two weak points for attackers. At first it is very easy to trick the AP into discarding the buffered traffic for a client in power-saving mode by simply spoofing the poll frame. Also by forging a TIM frame the client may be told that there are no buffered frames at all and the client will immediately return to power-saving mode. On the other hand an attacker may disturb the timely synchrony and consequently the client will wake up at the wrong time and will never receive a TIM resulting in the disruption of the network service.

2.3 Access-point Spoofing

Unlike the previous vulnerabilities the following two attacks do not directly rely on laws in the IEEE 802.11 MAC layer specification but rather in completely faking the AP's identity. If an attacker is able to spoof the identity of an AP he might lure clients into connecting to the fake AP instead of the legitimate one. The attacker only needs to emit a stronger signal than the legitimate AP. In many cases, public WLANs use web portals for user authentication. The attacker now might redirect the client to a faked web portal and steal the clients username and password. Alternatively the attacker can implement active man-in-the-middle attacks against SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI . The usage of IEEE 802.11i security mechanisms with integrated IEEE 802.1X would provide an effective protection against this attack.

2.4 Client Spoofing

By spoofing a legitimate wireless station (STA) an attacker may bypass an AP's MAC address-based access control list to gain access to a WLAN. This action is frequently the first step in infiltrating a network and followed by further attacks. Another possibility is to use the AP to decrypt traffic encrypted by WEP. In this attack an attacker impersonates a legitimate STA, captures WEP frames the STA sends, and retransmits these frames to the AP. The destination IP address in the WEP frames may be altered in order to trick the AP in transmitting the decrypted traffic to an Internet host controlled by the attacker. The usage of IEEE 802.11i security mechanisms with integrated IEEE 802.1X would provide an effective protection against this attack.

3. PROPOSED SOLUTION

3.1 PREVENTION BY ENCRYPTED SIGNATURE VALUES:

This method uses an additional authentication process beside MAC address filtering .Using unique information that belongs to every client in the network such as computer name, node ID. A unique signature value is computed. This value is inserted in the slack fields of the data frame. Thus, when a node receives an frame from a client, it will first check the MAC address, if it is legal the node will decrypt depending on the corresponding identifiers stored then compare the resulted signature value with the received one and decide whether to reject or accept the access. The idea is to transmit the signature value in

the packet without letting the intruder know the difference between the data and the signature value in the transmitted packet.

3.2 PROTOCOL FOR TRANSMITTING:

- Every time a node sends a packet, fetch the node id.Encrypt it with it' s private key using the RSA encryption algorithm This generated value acts as the signature value for that node.
- Generate a random value and store it in the header field of the node, in this case consider it called hidden pos.
- Store the generated encrypted value in that hidden position of the data field and transmit the packet.

3.3 PROTOCOL FOR RECEIVEING:

- Every time a node receives a packet read the mac address and the value of the hidden position in the header field.
- Fetch the encrypted signature from the hidden position in the data field.
- Decrypt it using the public key of the node and verify the signature value with the node id.

If it is an illegitimate node, it would not have any signature value which would decrypt and give back the unique information identity of the node(node-id).Thereby ensuring maximum security from any illegitimate nodes into entering the network.

To implement the protocol, an stimulation scenario of 5 nodes communicating with each other in NS2 is shown .We transfer two packets from each node to a receiver node. The nodes marked in blue are legitimate nodes communicating with the node marked in green. The node marked in red is a malicious node from outside trying to spoof the mac- address of node 2 and gain entry into the network.

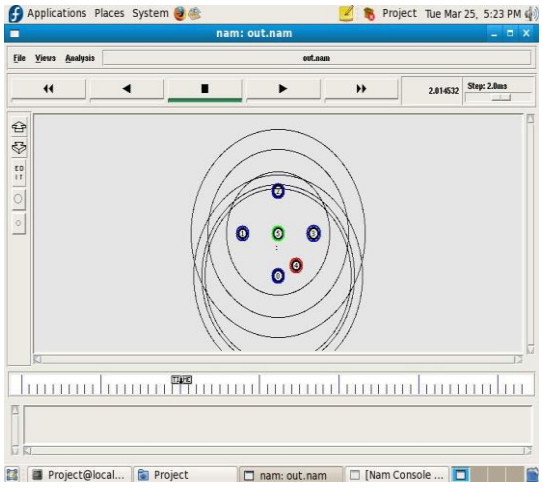

Figure 2: Node Processing

Every time node 0 sends a packet it encrypts it's unique information (node id) and generates a random position number. This encrypted value is kept in that random position in the data field. This position is stored in the header field of the packet and transmitted. When the receiver (node 5) gets the packet, it fetches the signature value from the data field and decrypts it with the public key of that node. If the decrypted value of the signature node gives back its node id then the packet can be accepted. A screenshot of the actual implementation of the packet transfer and node processing is shown.

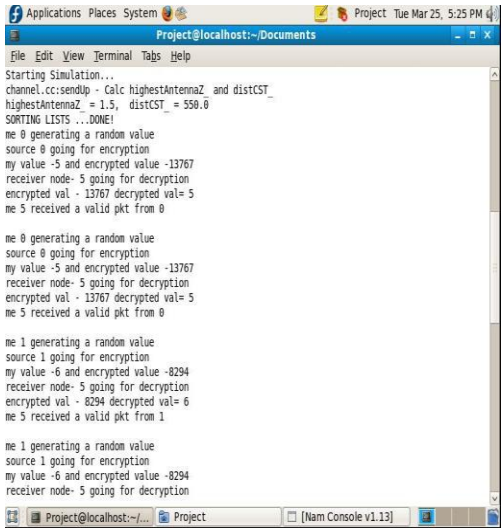

Figure3: Packet Transfer and Node Processing

4. RESULT

The packets sent from a legitimate node are received and accepted by the receiver it fetches and decrypts the signature value and verifies its identity as a legitimate node, whereas the packet from the malicious node is not accepted since it does not have proper signature value which decrypts back to give its node id.

5. CONCLUSION

The above proposed algorithm is implemented to prevent MAC SPOOFING compared to the others as it is more suitable for a resource constrained wireless network and provides greater efficiency. This protocol is designed to reduce the work load on the node and provides reliable security and finds abundant scope to be used in the future.

REFERENCES

[1] Journal of Computer Science 8 (10): 1769- 1779, 2012 ISSN 1549-3636;Prevention of Spoofing Attacks in the Infrastructure Wireless Networks;Wesam S. Bhaya and Samraa A. AlAsady,University of Babylon, Information Technology College, Iraq

[2] International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009; MAC SPOOFING AND ITS COUNTERMEASURES; First A. Deepak Gupta1, Second B . Gaurav Tiwari1, Third C. Yachin Kapoor2 and Fourth D. Praveen Kumar, India.

[3] International Journal of Network Security, Vol.9, No.2, PP.164{172, Sept. 2009; Combating Wireless LAN MAC-layer Address Spoofing with Fingerprinting Methods; GÄuenther Lackner, Udo Payer, and Peter Teu

[4] Sequence Number-Based MAC Address Spoof Detection; Fanglu Guo and Tzi-cker Chiueh Computer Science Department Stony Brook University, NY 11794.