International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 16 • Issue 1 pp. 7-11 Jan - June 2024 www.csjournals.com

Security issues and Challenges in wireless sensor Networks

Manoj Goyal
Assistant Professor
Dept. of Electronics and Comm Engineering, KCT College of Engg. & Tech, Sangrur, Punjab

***Abstract*— Wireless Sensor Networks consist of small, low-power sensor nodes that communicate wirelessly to monitor physical or environmental conditions (temperature, motion, pressure, etc.). While they are valuable for military, industrial, healthcare, and environmental applications, they face** serious security challenges **due to resource constraints and open wireless communication. Wireless Sensor Networks is a grouping of wireless networking and entrenched system technology that monitors physical or environmental situation, such as temperature, sound, quivering, strain, motion or pollutant, at different locations and a spoofing attack is a one of the most common online attack in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage, it become more sophisticated defense mechanisms. Various defense mechanisms against spoofing attacks were analyze and this paper also describe the working mechanisms, advantages & disadvantages of each defense mechanisms.**

Keywords: Wireless Sensor Network, Spoofing attack

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are extremely distributed networks of undersized lightweight wireless nodes, Deployed in bulky numbers, Monitors the environment or system by measuring physical parameters such as temperature, pressure, humidity [6]. WSNs are networks that consist of sensors which are distributed in an ad hoc manner. These sensors work with each other to sense some physical incident and then the information gathered is processed to get appropriate results [1]. A WSN consists of protocols and algorithms with self-organizing capabilities.

Two of the elementary features of a WSN are the ad-hoc nature of the system which is expected to set up and maintain its individual communication architecture without the aid of a federal influence [1] and the fact that the sensor nodes are expected to operate for extensive periods of time without awareness from a higher-level presence (e.g. a human). These features are due fundamentally to the proliferation of wireless networking and sensor hardware technologies, allowing contemptible wireless devices to make wireless sensor networking a feasible alternative for personal, commercial, industrial, and military uses [2]. Resource limitations in the WSNs prevent us to directly apply the security mechanism of normal computer networks, completely different set of security protocols subsist for the sensor networks. Different security protocols for sensor networks have been evaluated against these vulnerabilities. Most of the attacks on some well known and widely used security protocols have been conversed, along with the possible countermeasures for these attacks [3]. The malice of the attacker can be in any direction including node imprison, physical tampering, spoofing, sniffing, and denial of service attacks. As more wireless and sensor networks are organized, they will increasingly become tempting targets for malevolent attacks. Due to the frankness of wireless and sensor networks, they are principally susceptible to spoofing attacks where an attacker forges its individuality to pretense as another device, or even creates multiple illicit identities. Spoofing attacks are a stern hazard as they symbolize a form of distinctiveness cooperation and can assist a variety of traffic injection attacks, such as evil twin access point attacks [4].

In this paper we judge the different types of Spoofing attacks and analyze the different defense mechanism with their pro and shortcoming. The remainder of this paper is organized as follows. We first review Spoofing attacks with different its type in section II. In section III, defense mechanisms were reviewed. In section IV, The different defense mechanism is reviewed. And section V, include the conclusion part.

II. SPOOFING ATTACKS

Spoofing attacks arise when the attacker is capable to root a user or a device on a system to believe that a piece of information came from a source from which it actually did not initiate [5]. Spoofing attacks can be IP Spoofing, MAC Spoofing, Web Spoofing, DNS Spoofing, and Email Spoofing etc.

IP Spoofing: In computer networking, the term IP address spoofing or IP spoofing refers to the creation of Internet Protocol (IP) packets with a counterfeit source IP address, called spoofing, with the principle of concealing the identity of the dispatcher or impersonating another computing system. IP spoofing can also be a scheme of harass used by network intruders to overwhelm network security measures, such as authentication based on IP addresses. This method of attack on a remote system can be enormously complicated, as it involves modifying thousands of packets at a time. This type of attack is the majority efficient where trust relationships exist between machines. IP Spoofing

possibility increased when Problem with the Routers, Routers look at Destination addresses only Authentication based on Source addresses only, and to change source address field in IP header field is easy.

MAC Spoofing: MAC spoofing is a method for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. Unlike IP address spoofing, where senders spoofing their address in a request direct the receiver into sending the response elsewhere, in MAC address spoofing the response is received by the spoofing party. However, MAC address spoofing is limited to the local broadcast domain.

Web Spoofing: Web Spoofing allow an attacker to create shadow copy of entire World Wide Web and creates misleading context in order trick the victim for online fraud.

DNS Spoofing: DNS Spoofing is the art of making a DNS entry to point to another IP than it would be supposed to point to. DNS Spoofing is the trick of making a DNS entry to point to some IP other than it would be supposed to point to -- hijacking the identity of the server. With modern bind daemons this is a difficult thing to do without breaking into the server or some parts of network infrastructure (routers, switches, etc).

Email Spoofing: E-mail spoofing is e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. Because core SMTP doesn't provide any authentication, it is easy to impersonate and forge emails. It is usually fraudulent but can be legitimate. It is commonly used in spam and phishing e-mails to hide the origin of the e-mail message.

By changing certain properties of the e-mail, such as the From, Return-Path and Reply-To fields (which can be found in the message header), ill-intentioned users can make the e-mail appear to be from someone other than the actual sender. The result is that, although the e-mail appears to come from the address indicated in the Form field (found in the e-mail headers), it actually comes from another source.

III. Defense Mechanisms

Detection of Spoofing Attack: If you monitor packets using network-monitoring software such as net log, look for a packet on your external interface that has both its source and destination IP addresses in your local domain. If you find one, you are currently under attack. Another way to detect IP spoofing is to compare the process accounting logs between systems on your internal network. If the IP spoofing attack has succeeded on one of your systems, you may get a log entry on the victim machine showing a remote access; on the apparent source machine, there will be no corresponding entry for initiating that remote access

Prevention Spoofing Attack: The best method of preventing the IP spoofing problem is to install a filtering router that restricts the input to your external interface (known as an input filter) by not allowing a packet through if it has a source address from your internal network. In addition, you should filter outgoing packets that have a source address different from your internal network in order to prevent a source IP spoofing attack originating from your site. If your vendor's router does not support filtering on the inbound side of the interface or if there will be a delay in incorporating the feature into your system, you may filter the spoofed IP packets by using a second router between your external interface and your outside connection.

Configure this router to block, on the outgoing interface connected to your original router, all packets that have a source address in your internal network. To prevent IP spoofing happen in your network, the following are some common practices:

- Avoid using the source address authentication. Implement cryptographic authentication system wide.
- Configuring your network to reject packets from the Net that claim to originate from a local address.
- Implementing ingress and egress filtering on the border routers and implement an ACL (access control list) that blocks private IP addresses on your downstream interface.

The various detection and prevention methods are used in WSN to defend against spoofing attacks. These are

(i) *Ingress and Egress filtering*

- Ingress – An ISP prohibits receiving from its stub connected networks packets whose source address does not belong to the corresponding stub network address space
- Egress – A router or a firewall which is the gateway of a stub network filters out any packet whose source address does not belong to the network address space.[7]

(ii) *TCP Intercept:* Router checks the real host behind the source address by completing the 3-way handshake and if connection with client is established, then address considered not spoofed.[7]

(iii) *Demote system:* The DEMOTE system performs spoofing attack detection by analyzing the RSS trace for each mobile node identity. The main idea of the DEMOTE technique is to use the relationship between the RSS and the physical location of a mobile device to perform spoofing attacks detection. If a spoofing attack is present, the RSS trace from *claimed* node identity is the mixture of two RSS traces: one belongs to the victim node and the other belongs to the spoofing node. These two RSS traces are correlated to the different locations of the two

physical nodes and are thus not highly correlated to each other. Under normal situations, i.e., there is no spoofing attack present; the RSS trace from one node trace is separated into two traces, those two traces are highly correlated to each other as they are determined by the movement pattern of a single mobile node. [8]

(iv) *Forge Resistance Relationship (FRR) Method:* This method generates many false negatives and false positives in various network scenarios. [9] where *Dobsm* is the observed value of *Dm* between two clusters. [12]

(v) *Discrete Event System (DES) Approach:* DES detector based IDS for detecting ARP response spoofing uses an active probing mechanism and does not violate the principles of network layering architecture. Further, this being a software based approach does not require any additional hardware to operate. [13]

(vi) *Forge Resistance Relationship With Rate Analysis (FRR-RA) Method:* In FRR-FR method, packets detected spoofed by FRR method are again analyzed by transmission rate method. Packet detected spoofed by both method is dropped from analyzing window of packets to avoid raising false positive alarms for previous 'n' consecutive packets. [10]

(vii) *Change – Point Detection Method:* This scheme based a storage-efficient data structure and a changepoint detection method. The storage-efficient data structure, which is a variant of Bloom filter [15], is used to generate a hash digest of the traffic. The change-point detection method is based on the CUSUM algorithm [16] which is a nonparametric change point detection method. After some information about the traffic is extracted and stored in the Bloom filter, CUSUM is then applied to detect abnormal changes in the digested traffic. [14]

(viii) *Trace route and Cooperation With Trusted Adjacent Nodes Based Method:* This method can detect and block the intruder from external network, which intrudes trusted network by IP spoofing attack. Additionally, for the case that only the local security system is run, because the trusted adjacent node monitors cooperatively the generating external attacks in the local node, the method can effectively reply IP spoofing attack. [11]

(ix) *Silence Method:* SILhouette Plot and System EvolutioN with minimum distanCE of cluster, which evaluates the minimum distance between clusters on top of the pure cluster analysis to improve the accuracy of determining the number of attackers. The number of attackers *K* in SILENCE is thus determined by:

$$K = \begin{cases} Ksp \text{ if } Ksp = Kse; \\ Ksp \text{ if } \min(Dobsm)Ksp > \\ \quad \min(Dobsm)Kse; \\ Kse \text{ if } \min(Dobsm)Ksp < \\ \quad \min(Dobsm)Kse, \end{cases}$$

where *Dobsm* is the observed value of *Dm* between two clusters. [12]

(x) *Discrete Event System (DES) Approach:* DES detector based IDS for detecting ARP response spoofing uses an active probing mechanism and does not violate the principles of network layering architecture. Further, this being a software based approach does not require any additional hardware to operate. [13]

(xi) *Forge Resistance Relationship With Rate Analysis FRR-RA) Method:* In FRR-FR method, packets detected spoofed by FRR method are again analyzed by transmission rate method. Packet detected spoofed by both method is dropped from analyzing window of packets to avoid raising false positive alarms for previous 'n' consecutive packets. [10]

Change – Point Detection Method: This scheme based a storage-efficient data structure and a changepoint detection method. The storage-efficient data structure, which is a variant of Bloom filter [15], is used to generate a hash digest of the traffic. The change-point detection method is based on the CUSUM algorithm [16] which is a nonparametric change point detection method.

After some information about the traffic is extracted and stored in the Bloom filter, CUSUM is then applied to detect abnormal changes in the digested traffic. [14].

IV. Analysis

The defense mechanisms against spoofing attacks were studied and a comparative analysis is done which include the working mechanism and describe their advantages and disadvantages as summarized in table 1.1

V. Conclusion

WSNs are networks that consist of sensors which are distributed in an ad hoc manner. Various security protocols for sensor networks have been evaluated against these vulnerabilities. As more wireless and sensor networks are deployed, they will increasingly become tempting targets for malicious attacks. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin access point attacks.

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 16 • Issue 1 pp. 7-11 Jan - June 2024 www.csjournals.com

Table 1.1 (Comparison of defense mechanisms)

Defense Methods	Working Mechanism	Advantage	Disadvantage
Ingress and Egress filtering	Network address based	Make sure that incoming packets are actually from the networks that they claim to be from. And monitoring & potentially restricting the flow of information outbound from one network to another	Allows Spoofing within a stub network and Deployment is costly
TCP Intercept	Three-way TCP handshake	If connection with client is established, then address considered not spoofed	Applicable only to TCP. Cannot protect UDP traffic or any other connectionless traffic
Spoofing Prevention Method (SPM)	Network address based	Tag a simple key for leaving packet, & then verify the key in target host	The algorithm is complicated and practical application is difficult
FDPM (Flexible deterministing packet marking)	IP traceback system based	Little computing, better tracing capacity.	Consume more resources, such as memory or routing routers.
TNA (Tracing network attacks to their source)	IP traceback system based	IP traceback to identify the true IP address of the attack host	Each router deploy a special tracing equipment to store the IP or MAC
IP2HC scheme	Hop cont filtering detecting based	Detection method based on the hop count filtering, no false positives.	More memory overhead is needed for maintaining mapping table.
Demote system	Received Signal Strength (RSS) based	This is highly effective and efficient in detecting spoofing attacks in mobile environment.	RSS traces are much less correlated under spoofing attacks.
Forge Resistance Relationship (FRR) Method	Based on behavior of change in sequence Number	Its anomaly detection rate is high and gives a large number of false positives.	This has no way to find the sequence number of genuine station.
Forge Resistance Relationship With Rate Analysis (FRR-RA) Method	Based on behavior of change in sequence Number	This method generates less percentage of false positive and false negative alarm.	This method requires lot of computation power and overhead in sending periodic probing.
Trace route and Cooperation With Trusted Adjacent Nodes Based Method	Based on traceroute and the cooperation with trusted adjacent nodes	Only trace the route information by software method	It is key that how to get the IP address of access host.
Silence Method	Distance cluster based	Provide better accuracy in determining the number of attackers	More computation & works only under normal conditions
Discrete Event System (DES) Approach	IDS based for detecting ARP response spoofing	It reduces additional ARP traffic and does not require any additional hardware to operate.	This require extension for attacks as request spoofing, man in middle and denial of service.
Change – Point Detection Method	Based on the CUSUM Algorithm	It maximizes the utilization of the hash table entries and minimizes the false positive rate.	It is not reasonable for large real network.

REFERENCES

[1] D. Nesarajan, L. Kunalan, M. Logeswaran, S. Kasthuriarachchi, and D. Lungalage, "Coconut Disease Prediction System Using Image Processing and Deep Learning Techniques," in *2020 IEEE 4th International Conference on Image Processing, Applications and Systems (IPAS)*, 2020, pp. 212–217.

[2] [14] A. Abade, P. A. Ferreira, and F. de Barros Vidal, "Plant diseases recognition on images using convolutional neural networks: A systematic review," *Comput. Electron. Agric.*, vol. 185, no. 106125, 2021.

[3] [15] S. Mehta, V. Kukreja, and D. Bordoloi, "Grape Leaf Disease Severity Analysis: Employing Federated Learning with CNN Techniques," in *2023 World Conference on Communication & Computing (WCONF)*, 2023, pp. 1–6.

[4] [16] B. Anitha. and S. Santhi., "Disease Prediction in Coconut Leaves using Deep Learning," in *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, 2023, pp. 258–264.

[5] [17] R. K. Megalingam *et al.*, "Coconut trees classification based on height, inclination, and orientation using MIN-SVM algorithm," *Neural Comput. Appl.*, vol. 35, no. 16, pp. 12055–12071, 2023.

[6] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[7] Patrick Tague and Radha Poovendran, "Modeling Node Capture Attacks in Wireless Sensor Networks" Forty-Sixth Annual Allerton Conference Allerton House, UIUC, Illinois, USA September 23-26, 2008

[8] Asif Habib, "Sensor network Security Issues at Network Layer", ICAST 2008

[9] Yingying Chen, Wade Trappe, Richard P. Martin, "Detecting and Localizing Wireless Spoofing Attacks", Proceedings of the Fourth Annual IEEE Communications Society, pp: 193-202, Secon 2007.

[10] Sean Convery, "Network Security Architectures", CCIE No. 4232

[11] Pooja Kumari "Study of Security in Wireless Sensor Networks", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (5) , 2010, 347- 354

[12] Srikanth T.S.S, Sri Lakshmi Ramya S "Spoofing Prevention Method"

[13] Jie Yang, Yingying Chen and Wade Trappe, "Detecting Spoofing Attacks in Mobile Wireless Environments", Proceedings of the Sixth Annual IEEE Communications Society, Secon, 2009.

[14] Bansal, R. Tiwari, S. Bansal, D, "Non-cryptographic methods of MAC spoof detection in wireless LAN", 16th IEEE International Conference on Networks, pp:1-6, IEEE ICON- 2008.

[15] Shikha Goel ,Sudesh Kumar, "An Improved Method of Detecting Spoofed Attack in Wireless LAN", First International Conference on Networks and Communications (NETCOM), pp: 104-108, Chennai, 2009.

[16] Yunji Ma, "An Effective Method for Defense against IP Spoofing Attack", 6th International Conference on Wireless Communications

[17] Networking and Mobile Computing (WiCOM), pp: 1-4, Chengdu City, 2010

[18] Jie Yang, Yingying Chen, Wade Trappe, Jerry Cheng, "Determining the Number of Attackers and Localizing Multiple Adversaries in Wireless Spoofing Attacks", proceeding of IEEE INFOCOM, pp: 666-674, 2009.

[19] Neminath H, S Biswas, S Roopa, R Ratti, S Nandi, F.A. Barbhuiya, A Sur and V Ramachandran, "A DES approach to Intrusion Detection System for ARP Spoofing Attacks", 18th Mediterranean Conference on Control & Automation (MED), pp: 695-700, Marrakech, Morocco June 23-25, 2010

[20] Wei Chen, Dit-Yan Yeung, "Defending Against TCP SYN Flooding Attacks Under Different Types of IP Spoofing", International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, pp: 38-43, 2006.

[21] B. H. Bloom. "Space/time trade-os in hash coding with allowable errors. Communications of the ACM", 13(7), pp: 422—426, July 1970.

[22] B. Brodsky. "Nonparametric Methods in Change-Point Problems", Kluwer Academic Publishers, Netherlands, 1993.

[23] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[24] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[25] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350