

Mapana - Journal of Sciences
2023, Vol. 22, Special Issue 2, 383-406
ISSN 0975-3303 | https://doi.org/10.12723/mjs.sp2.22

A Survey on Spoofing and Selective Forwarding Attacks on Zigbee Based WSN

D. Shanmugapriya*, D Nethra Pingala Suthishni*,
V. Sasirekha†, G. Padmavathi‡ and M. Keerthika‡

Abstract

The main focus of WSN is to gather data from the physical world. It is often deployed for sensing, processing as well as disseminating information of the targeted physical environments. The main objective of the WSN is to collect data from the target environment using sensors as well as transmit those data to the desired place of choice. In order to achieve an efficient performance, WSN should have efficient as well as reliable networking protocols. The most popular technology behind WSN is Zigbee. In this paper a pilot study is done on important security issues on spoofing and selective forwarding attack on Zigbee based WSN. This paper identifies the security vulnerabilities of Zigbee network and gaps in the existing methodologies to address the security issues and will help the future researchers to narrow down their research in WSN.

Keywords: Zigbee, WSN, Protocol Stack, Spoofing and Selective Forwarding.

1. Introduction

Wireless Sensor Networks (WSN) can be defined as infrastructure-less and self-configured wireless network for observing environmental or physical conditions like pressure, motion, temperature, pollutants, sound or vibration as well as to directly

* Department of Information Technology, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India; Email: nethra_it@avinuty.ac.in
† Department of Physics, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India
‡ Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India

pass their information or data through the network to a sink which is also known as main location where the location is observed as well as analysed (Wood et al 2002) [1]. The sink or base station acts like an interface between the network and the user. WSN consists thousands of sensor nodes. The communication in between sensor nodes are done by means of radio signals. The sensor nodes are equipped with sensing as well as radio transceivers, power components and computing devices. In WSN, sensor node is constrained with resources that includes limited storage capacity, processing capability as well as communication bandwidth (Karlof et al 2003) [2]. The applications of WSN are more that includes IoT, agriculture, patient monitoring, environment monitoring etc.

2. Wireless Sensor Network (WSN)

The most popular technology behind WSN is zigbee. It is a low power wireless personal area network technology.

The architecture of WSN is illustrated below:

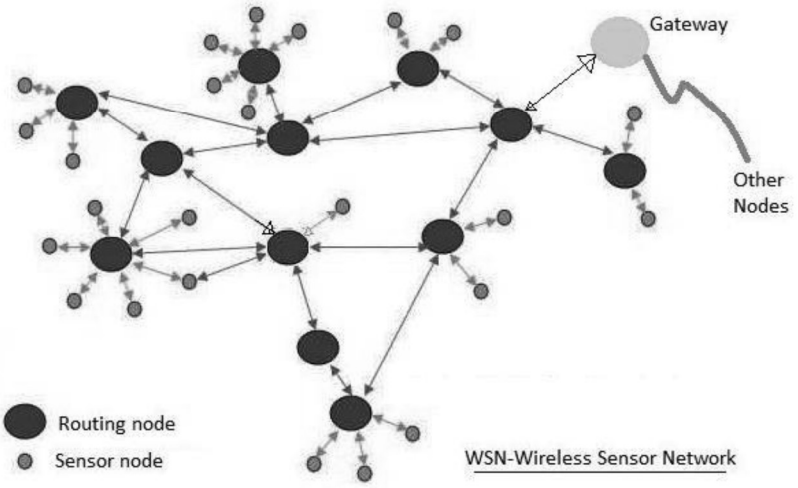


Fig. 1. WSN Architecture

WSN includes sensor nodes, base station and routing nodes. It is gaining more popularity recent days because of the availability of low-cost sensors, and its characteristics like flexibility to deploy anywhere and equipped with lifelong batteries (Justification ques 7) (Hung-Min et al 2007) [6].
The main components of WSN are distributed sensor nodes, sink nodes as well as software. Omni directional antenna, transceiver, power supply as well as DSP are the components embedded with each sensor. An IoT gateway is a software program or physical device that acts as connection point between cloud as well as sensors, controllers and intelligent devices (Ioannis et al 2007) [7]. The communication between micro-sensor network and Internet/other WSN is carried out via gateway. In WSN, thousands of sensors are distributed densely and randomly about 10 to 20 per square meter. WSN gains popularity due to the energy efficient batteries as well as flash memories of sensors. The algorithms used in WSN manages collision as well as congestions. The type of WSN is based on various factors like type of network, clustering type, method of communication, protocol, application as well as coverage. WSN is prone for security risks.

3. Zigbee Protocol Stack

International standards for WSN and devices such as ISA 100.11a, WirelessHART and Zigbee use stacks for providing a layered as well as abstract description of the protocol design. In the stack, each layer is a collection of related functions as well as each layer has the responsibility to provide services to the layer above it and also receive services from the layers below it (Bo Yu et al 2006) [3]. Some important requirements for the industrial applications of WSN are reliability, latency, update rates of sensor data, wireless transmission range, and power consumption. Reliability is the measure that conveys the percentage of accurate data that reaches its destination. It is used with stability which conveys the percentage of transmitted data successfully on an individual link basis. Data transmission in IEEE 802.15.4 is based on ACK. Transmitter expects ACK from receiver. Transmitter resends the packets when not receiving ACK within specified time frame. Retransmission of packets enables to achieve high reliability as well as stability in the network. Latency is a measure that conveys time delay. It represents the time for the data

to arrive to the destination from originating sensor. Link quality is the foremost factor that influences the latency. Latency and retransmission are increased due to poor quality links. Hop count is another factor tom increase latency. Update rate of sensor data as well as battery life of sensor are strongly correlated with each other. It is essential to have trade-off between update rates of sensor as well as battery life. Power consumption of sensor node is based on various factors such as update rate, link quality, and routing activities. Top standards of WSN are as follows

3.1 Zigbee Standards

Zigbee is a specification for a suite of high-level communication protocols using low power digital radios based on IEEE 802.15.4. It is simple to use as well as less expensive compared with other standards like Bluetooth. It is targeted for the applications that need low data rate as well as battery life and secure networking. It is a specification for higher protocol layer. The basis of protocol is AODV (Ad-hoc on-demand distance vector). It has two classes of network devices such as F-Full-function and reduced function devices. It can able to operate on both non-beaconed mode. Coordinator, router and end devices are the protocol devices in Zigbee Standard. It makes use of the security mechanism of 802.15.4. it has the features to employ integrity and encryption only. MAC layer security is not addressed explicitly through 802.15.4. Three types of keys for Zigbee security are master key, link key as well as network key. These keys can be set in coordinator or trust centre.

Comparison of Standards

Feature	**ISA 100.11a**	**Wireless HART**	**Zigbee PRO**
Scalability	Yes	Yes	Yes
Topology	Star, Mesh, combined star and mesh	Star, mesh, combined star and mesh	Mesh
Radio channel	TDMA/CSMA	TDMA	CSMA-CD
Security	High	High	High

Feature	ISA 100.11a	Wireless HART	Zigbee PRO
RF channel change	Yes	Yes	Yes
Noise/ Interface control	Yes	Yes	Yes
Interoperability	Yes	Yes	Yes
Context of application	Industrial	Industrial	Commercial
Keys	Asymmetric/ Symmetric	Symmetric	Symmetric
Reliability	Yes	Yes	No
Latency	Yes	Yes	No
Implementation	Challenging	Challenging	Easy

The study shows that, most of the weakness of ZigBee can be overcome with ISA.100 and wireless HART. One of the serious concerns about Zigbee is its security (Yu et al 2007) [4]. The security vulnerabilities of Zigbee based on the features related with security incorporated in design as well as manufacture. The security risks of are as follows:

- Sensitive data theft
  Sensitive data includes user data or encryption keys etc. It is vital to select as well as protecting the security keys used in the network.
- Node theft
  Node theft is the process of removing or moving the node from the current network to another where it can be accessed as well as controlled.
- Unauthorised control of a node
  It is accomplished from the process of node theft as well as that node will be utilized for the malicious activities. The theft node can be used to perform replay attacks etc (Kaplantzis et al 2007) [5].

- Network service loss
  Attackers use interference for jamming radio channel or entire radio band. Frequency agility in applications is one method to protect from this kind of attack. The survey is based on such vulnerable zigbee WSN standard.

3.2 Zigbee Technology

It is popular technology for low data rate wireless application. The devices of Zigbee are used everywhere including medical, smart energy as well as home automation. It has two bands of operation such as 2450MHz as well as 868/915MHz. The data rates of 868/915 as well as 2450MHz bands are 20-40 Kb/s and 250 kb/s (Justification of question 6). The network architecture of Zigbee is illustrated below:

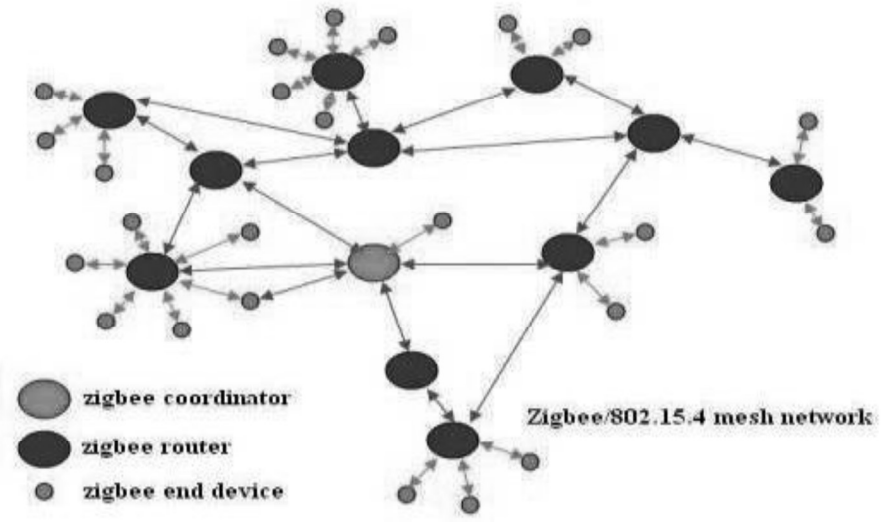


Figure 2. Zigbee Network Architecture

The main components of Zigbee network are end devices, router and coordinator. It supports mesh-routing (Hae Young et al 2007) [8].

Coordinator

In order to establish zigbee network service, coordinator has to be installed initially that creates new personal area network. It connects two or more zigbee router through which it connects zig bee end devices to the network. It is responsible to select PAN ID as well as channel. It provides assistance in routing through mesh network as

well as joins the request from R as well as E. It provides support for the child devices. It does not enter into sleep mode.

Router
Router has to be joined into the Zig bee network in order to allow other R as well as E to join the personal area network. It also supports child devices. It also does not enter the sleep mode.

End Devices
It cannot allow other devices for joining the PAN and also it does not provide support for routing the data through the mesh network. It gets power through battery and does not provide support for the child devices. In order to reduce the battery consumption, it can enter into the sleeping mode. Zig bee network supports mash topology. The communication between Zig bee devices are carried out using 16 bit PAN number. The PAN ID of the coordinator is zero and other devices will be assigned with 16 bit number while joining PAN. The Zig bee network installation involves two steps such as network formation by coordination as well as joining the network by end devices and routers.

3.3 Zigbee Protocol Stack

The protocol stack of Zigbee includes physical layer, Media Access Control layer, network layer as well as application layer. The protocol stack of zigbee is illustrated in Fig. 3.

IEEE 802.15.4 defines the bottom most two layers such as physical as well as Media Access Control layers. It is closed to the hardware as well as directly controls as well as communicates with Zigbee radio. It transmits and receives data packets over the air.

It is responsible for the interface between network as well as physical layer. It provides PAN ID as well as network discovery through beacon requests. This layer is in charge of mesh networking and act as an interface between application and MAC layer. Application layer is the top layer in the Zigbee protocol stack. This layer support all the sub layer and Zigbee device objects.

Zigbee protocol is based on IEEE 802.15.4 was introduced by Zigbee Alliance.

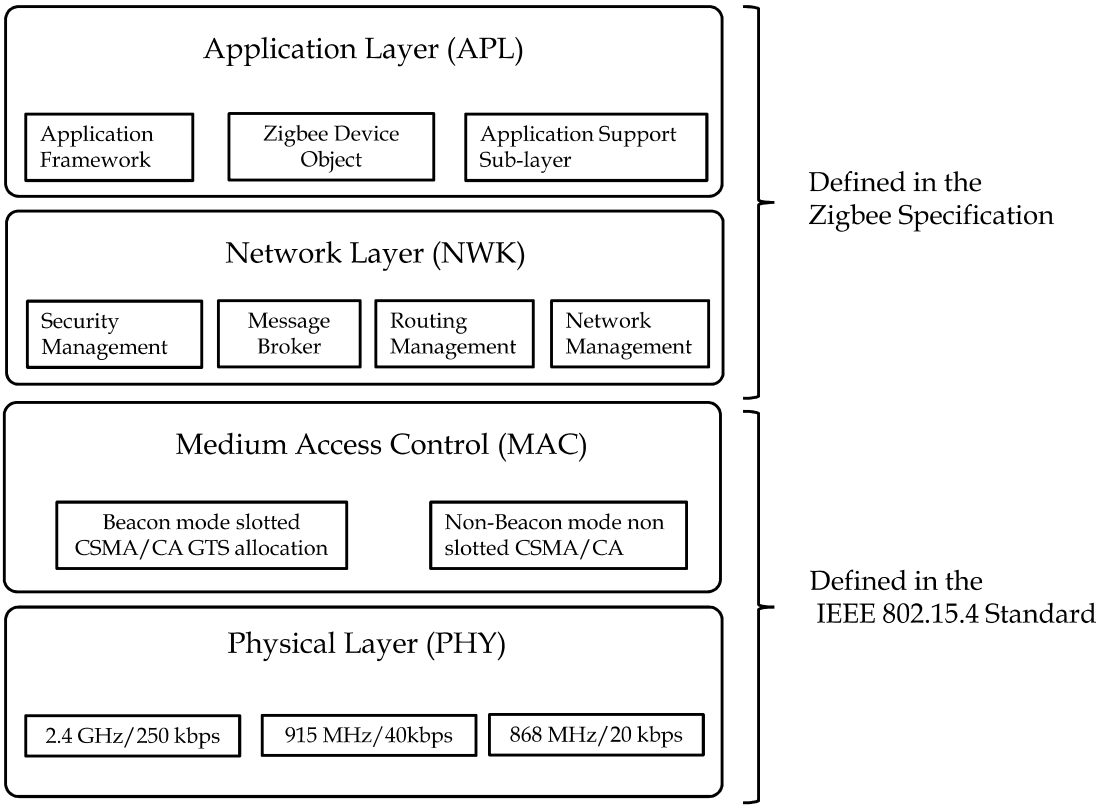


Fig. 3. Zigbee Protocol Stack

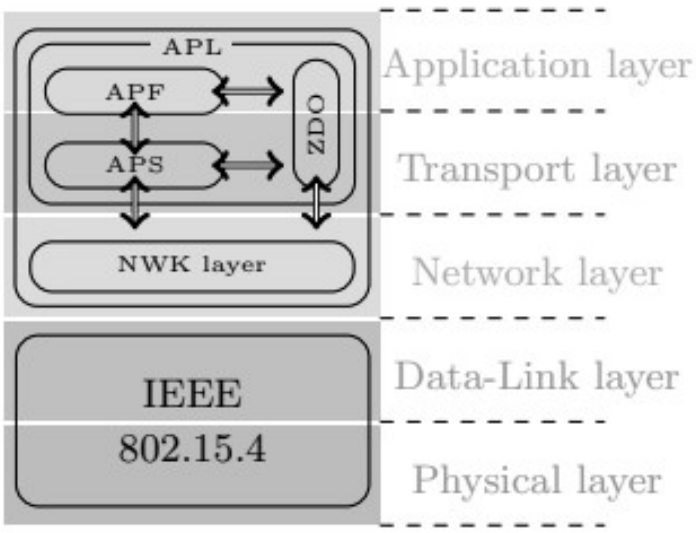


Fig. 4. Zigbee Communication Layers

The upper layers are networking as well as application layers. Application layer includes application framework, application sub-

layer and device object. The network layer offers various functionalities like route discovery, multi-hop routing, security, maintenance as well as leaving or joining network. APF has 254 APOs and each APO represent a software to control particular hardware unit like lamp, switch and so on. Each APO is assigned with local unique end point number that enables communication among the APOs (Hai et al 2008) [9].

ZDO (Z-Zigbee D-Device O-Object) – The main functionality of ZDO is to offer services to the application object (APO) as well as permits them for discovering IoT devices as well as services in the network. Various services of ZDO are network, communication as well as security management.

A-Application S-Sub L-Layer (APS)

APS acts as an interface between ZDO as well as APO for managing data transmission. Zigbee Alliance provides profile to APS to confirm for creating an application. Application profile enables the communication between APO by defining protocols as well as message format (Brown et al 2008) [11]. Application profile (AP) is helpful for the interoperability between applications of different manufacturers.

Routing

The PHY as well as MAC layers in Zigbee are specified based on IEEE 802.15.4. It provides tree, star as well as mesh topologies. The device that compose Zigbee network is either RFD or FFD and their names can be changed change for becoming router or ED. A Zigbee ED is an FFD or RFD and acts a simple device. The FFD device is a Zigbee router that has routing capabilities. A unique Zigbee coordinator in the network belongs to an FFD and controls the whole network. Routing algorithm in Zigbee is based on its network topology.

Tree Topology

It adopts tree-based routing algorithm. The topology consists of parent and child nodes and relationships are established using join operations. Routers maintains address details of parents as well as children. In order to establish a communication between a parent and child, they should synchronize between them.

Mesh Topology

It is more complex than tree topology and it is more powerful and resilient. Routers have routing table as well as router discovery algorithm for constructing or updating the routing information on path nodes. It uses discovery routing algorithm to find router that do not exists in the routing table. It switches over to the tree-based mode to find routing information when required resources are not available to adopt the algorithm such as route discovery. The algorithm "route discovery" is an essential part to discover route between source and destination. The routing table is maintained by router as well as coordinator for implementing route discovery process. Zigbee adopts ADOV as well as broadcasts techniques for reaching destination.

3.4 Zigbee Security

Zigbee is the main protocol used in IoT networks. IoT devices can be connected through the Zigbee WSN and further it is attached to the Internet via IoT Gateway. Zigbee based IoT networks are widely used in home and office environment. The latest version of Zigbee is 3.0. The Zigbee devices can interoperate with each other as well as exchange data in the same network. Zigbee standard consists various security features such as access control (AC) lists, frame counters (FC) as well as encryption techniques for the communications. The communication between devices in the Zigbee network is based on symmetric key. Communication is carried out in the form of encrypted data. It uses Advanced Encryption Standard (AES).

Centralized Trust Node

Security is centralized through the means of centralized node that authenticates the nodes attempt to join in the network. This centralized node is also known as Trust Center. This node acts as coordinator which creates the network.

Network Key Security

During authentication phase, the device which joins get encryption key from Trust center. The key is randomly generated one and which is same for all the devices in the network. This key is known as network key. It is used for the nodes to communicate such as including user as well as protocol maintenance data at the network

level. While distributing the key to the node, the key is encrypted using the pre-configured key which is acknowledged to the Trust center as well as node.

Link Key Security

In network, only two nodes share a key for their communication which is known as link key or an application key. It gives additional layer of security among the communicating nodes. Messages can be communication secure with both network as well as link key.

4. Selective Forwarding Attack in WSN

It is a malicious attack in which attack selectively drop IP packets from forwarding. In this type of attack, an attacker participates in the routing process as normal model and selectively drops packets that arrive from the neighbouring nodes. In this scenario, an attacker forward only non-critical IP packets and discard the critical IP packets. Karlof Wagner implemented selective forwarding (SF) attack. This attack is also known as Gray Hole (GH) attack (Justification of 8). In this, malicious nodes focus for stopping the packets or selectively forward packets by dropping important packets. There are different forms of selective forwarding. One of the forms of selective forwarding is malicious node selectively drop the packets based on its specific source/destination address or group of source/destination addresses. This results in DoS attack for a specific or group of nodes. An example of selecting forwarding with the perspective of DoS attack is illustrated below:

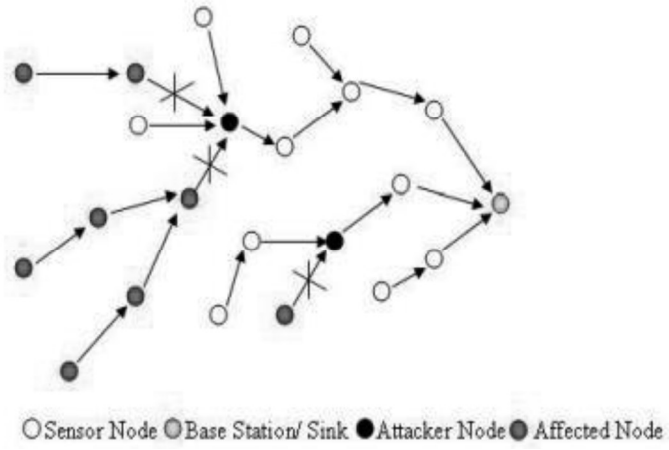


Fig. 6. Selective Forwarding with DoS Attack

The malicious nodes in WSN may also acts as black hole. The malicious nodes refuse to forward each packets that they have. In addition to that, malicious nodes may also forward the packets to the incorrect route that creates disloyal routing information in the network.

Another type of SF attack is neglect as well as greed. Here, the malicious node randomly neglect for routing some packets. It actively participate in the network as well as send acknowledge to the sender for receiving the packets but it drops the packets randomly. Such types of nodes are known as neglectful nodes. When the malicious node gives excessive priority for some packets means that is known as greedy. Another type of SF is delay-packets. Here malicious nodes delay on packet forwarding and creates confusions in the network.

The below example illustrates the selective forwarding attack.

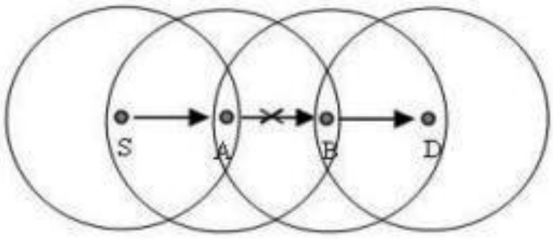


Fig. 7. SF Attack

Here, source „S" and destination „D". Packets are arriving from source in order to reach to destination „D". Packets reach destination „D" via the nodes „A" and „B". The node „A" may be malicious node and selectively forwards packets to the neighbouring node „B". It drops some packets and not forwarding to the neighbouring node „B" or route the packets into wrong path.

Another type of SF attack is blind letter attack. When the legitimate forwards the packet to its neighbouring node, it assumes that, packets successfully forwarded but actually the malicious node drops those packets without any notice to the sender.

Selective forwarding cause severe damage for the network. There are various measures proposed in the literature for selective forwarding network.

Table 1: Table for Selective Forwarding Attack

S. No.	Author and Year	Proposed work	Algorithm	Observation
1	Q. Zhang et al. 2019	E-Watchdog	Election algorithm	E-watchdog reduces the false detection rate by 25% and improves the detection accuracy by 10%
2	A. Petal et al. 2022 [39]	Reputation based RPL-Protocol	RPL	The proposed approach detects and isolates selective forwarding attack accurately with low false alarm.
3	X. Huang et al. 2022	Artificial immune system based on the danger model is established to detect network attacks	screen-confirm scheme, Support vector machine	In the proposed method the missing detection rate is less then 1.3%, The false detection rate is 4.3%.
4	J. Jung et al. 2022	Secure IoT Routing Selective Forwarding Attacks and	RPL	The proposed method gives high detection rate of 34%.

S. No.	Author and Year	Proposed work	Algorithm	Observation
		Trust-based Defenses		
5	J. Ding et al. 2022	Detect the selective forwarding attack under a harsh environment.	Reinforce ment learning (RL) algorithm, double-threshold density peaks clustering (DT-DPC) algorithm.	The proposed method has low FDR:1% and MDR:10%. Network throughput increases by about 4% under a harsh environment
6	M.Ezhilarasi et al. 2022. [40]	Detect routing attacks in wireless sensor networks.	fuzzy and feed-forward neural networks	Average detection rate of 97.8% and a maximum detection accuracy of 98.8%
7	J.Ding et al. 2021	Detect selective forwarding attacks by clustering the Cumulative Forwarding Rates (CFRs) of all sensor nodes	Noise-Based Density Peaks Clustering (NB-DPC)	The NB-DPC has a low Missed Detection Rate (MDR) and False Detection Rate (FDR) of below 1%.

5. Spoofing Attacks in WSN

Spoofing attacks is an attack in which an attacker impersonates an authorised user or device for stealing data, spreading malware as well as bypassing access control. There are various types of spoofing

such as IP Spoofing, Web Spoofing, MAC Spoofing, Email Spoofing, etc.

IP Spoofing

An IP address (Internet Protocol) is a unique identity for a computer in the network. The data transmission in computer network is occurred in terms of IP packets. Each IP packet has header that has source as well as destination address. The IP header is useful to route the

packets in a network. In IP spoofing attack, an attacker modifies the source address with spoofed or faked in the IP packet‟s header. The attacker performs spoofing attack by intercepting the IP packets during the communication between legitimate source as well as destination (Broumandan et al 2012) [29]. The attackers intercept IP packers and modify header data before it sending to the legitimate destination. IP address spoofing impersonates other devices that the IP packet arrives from legitimate source. It enables the adversaries for hacking the target as well as stealing data or performing malicious activities without any detection. IP address spoofing enables attackers for hiding their identity and pretends as trusted sources as well as bypassing the IP address authentication. Some of the malicious use

of IP address spoofing are DDoS attacks, mask botnet devices and Man-in-the –Middle attack. IP spoofing attack can be used for obtaining access of computers through maskingbotnets. A botnet represents a group of computers that are controlled by the hacker from a single source. IP spoofing enables the attacker for masking the botnet and making malicious activities.

IP spoofing also enables the attacker to perform Man in the Middle attack for interrupting the communication between computers, altering IP packets as well as transmitting them without any traces.

DDoS attack is a form attack that enables the sources inaccessible by legitimate sources. It is a brute force attack for crashing or slows down the server. Attackers use the spoofed IP address and communicate with the target with the aim of slowdown that target.

MAC Spoofing

Every NIC (Network Interface controller) has a unique Media access control address. On a LAN, computers use MAC address to communicate data with each other. MAC address is a hardware address. Computers use NIC to connect with network as well as it gives unique identity for the computer. MAC spoofing is the activity of modifying the MAC address on a NIC card. Intruder change the MAC address for entering into a target network as authorised entity. One of the techniques to resolve the issue of MAC spoofing is by using Reverse address resolution protocol.

DNS Spoofing

DNS spoofing is an attack in which modified DNS records are used for redirecting online traffic to a malicious or fraudulent website that mimics the desired destination. In the fraudulent website, users are prompted for providing their credentials through which attackers steal the credentials as well as sensitive data from the user.
Potential methods to achieve DNS poisoning are as follows:

Man in the Middle Attack

The attacker intercepts the communication between the user as well as DNS server for routing users to the malicious IP address.

Compromising DNS Server

Attacker may directly attack the DNS server and configure the DNS lookup table to return malicious IP address for the DNS request.

Table 2: Table for Spoofing Attack

S. No.	**Author and Year**	**Proposed Work**	**Algorithm**	**Observation**
1	SHAFIQUE et al. 2021	Protection of the UAVs from the Global Positioning System (GPS) signal spoofing attack	SVM	Acc: 99%

S. No.	Author and Year	Proposed Work	Algorithm	Observation
2	A. Luo et al. 2021	Detect fake audios synthesized by advanced methods.	Dynamic routing algorithm	EER: 1.07% Min-t DCF: 0.0328%
3	A.Javed et al. 2021	voice spoofing attacks on VCSs in single- and multi-hop network environments	acoustic ternary patterns (ATP) with Gammatone cepstral coefficients (GTCC) features.	The proposed countermeasure for reliable detection of 1st- and 2nd-order replay, cloning, and cloned-replay attacks.
4	T. Khoei et al. 2022	security solutions to protect unmanned aerial vehicles	Ensembling method using 10 machine learning algorithm: SVM, NB,DT,KNN, LDA, RF, ANN, LR,EN,and AdaBoost	Accuracy: 99.6%, PD:98.9%, PFA:1.56%, PM:1.09%, PT:1.24 s.
5	P. Jiang et al. 2021	DeePOSE: deep learning model, to address the noise introduced in	convolutional and recurrent neural network	Detection accuracy: 80%, False alarm < 8%.

S. No.	Author and Year	Proposed Work	Algorithm	Observation
		sensor readings and detect GPS spoofing attacks on mobile platforms		
6	B. Davidovich et al. 2022	Video stream captured by a drone‟s camera, for the real-time	Calculation of correlation between frames using Brute-force method.	The proposed method provides a level of security that detects any GPS

6. Conclusion

Zig bee is popular technology for low data rate wireless application. The devices of Zigbee are used everywhere including medical, smart energy as well as home automation. It is still, vulnerable for various security attacks. Zig bee security vulnerabilities are due to the following causes such as protocol as well as poor implementation of protocol. Lack of storing security keys such as network and link results in identification of those keys through reverse-engineering the firmware. In addition to that, insecurely sharing keys over the air between coordinator and devices results in sniffer steal those keys. Adversaries may also do energy depletion attack by sending burst of packets that have invalid security headers and sending packets to the devices at higher rate than the configured polling rate. Zigbee protocols results various jamming attacks such as radio and link layer. Attacks related to link key are default link key, un-encrypted link key as well as re-using link key. ACK spoofing as well as dropping are the attacks related to ACK in Zigbee. This paper focuses on spoofing and selective forwarding attack.

References

[1]. A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," in *Computer*, vol. 35, no. 10, pp. 54-62, Oct. 2002, doi: 10.1109/MC.2002.1039518

[2]. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in Ad Hoc Networks, Vol. 1, No. 2, 2003, pp. 293-315. https://doi.org/10.1016/S1570-8705(03)00008-8

[3]. Bo Yu and Bin Xiao, "Detecting selective forwarding attacks in wireless sensor networks," *Proceedings 20th IEEE International Parallel & Distributed Processing Symposium*, 2006, pp. 8 pp.-, doi: 10.1109/IPDPS.2006.1639675.

[4]. B. Yu and B. Xiao, "CHEMAS: identify suspect nodes in selective forwarding attacks," in Journal of Parallel and Distributed Computing, Vol. 67, No. 11, 2007, pp. 1218-1230. https://doi.org/10.1016/j.jpdc.2007.04.014

[5]. S. Kaplantzis, A. Shilton, N. Mani and Y. A. Sekercioglu, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines," *2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information*, 2007, pp. 335-340, doi: 10.1109/ISSNIP.2007.4496866.

[6]. Hung-Min Sun, Chien-Ming Chen and Ying-Chu Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," *TENCON 2007 - 2007 IEEE Region 10 Conference*, 2007, pp. 1-4, doi: 10.1109/TENCON.2007.4428866.

[7]. K. Ioannis and T. Dimitriou, "Toward intrusion detection in sensor networks," in 13th European Wireless Conference, April 2007, pp.1-7. doi: 10.1119/ISSNIP.2007.55431.

[8]. Hae Young L, Tae Ho C. Fuzzy-based reliable data delivery for countering selective forwarding in sensor networks. Hong Kong, China, Springer-Verlag, 2007, p. 535-544. https://doi.org/10.1007/978-3-540-73549-6_53

[9]. T. H. Hai and E. -N. Huh, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge," *2008 Seventh IEEE International Symposium on Network Computing and Applications*, 2008, pp. 325-331, doi: 10.1109/NCA.2008.13.

[10]. Y. K. Kim, H. Lee, K. Cho and D. H. Lee, "CADE: Cumulative Acknowledgement Based Detection of Selective Forwarding Attacks in Wireless Sensor Networks," *2008 Third International Conference on Convergence and Hybrid Information Technology*, 2008, pp. 416-422, doi: 10.1109/ICCIT.2008.271.

[11]. J. Brown and X. Du, "Detection of Selective Forwarding Attacks in Heterogeneous Sensor Networks," *2008 IEEE International Conference on Communications*, 2008, pp. 1583-1587, doi: 10.1109/ICC.2008.306.

[12]. Padmavathi DG, Shanmugapriya M. A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576. 2009 Sep 3. https://doi.org/10.48550/arXiv.0909.0576

[13]. H. Deng, X. Sun, B. Wang and Y. Cao, "Selective forwarding attack detection using watermark in WSNs," *2009 ISECS International Colloquium on Computing, Communication, Control, and Management*, 2009, pp. 109-113, doi: 10.1109/CCCM.2009.5268016

[14]. X. Lei, X. Yong-jun, P. Yong and Z. Yue-fei, "A Polynomial-Based Countermeasure to Selective Forwarding Attacks in Sensor Networks," 2009 WRI International Conference on Communications and Mobile Computing, 2009, pp. 455-459, doi: 10.1109/CMC.2009.230

[15]. C. Tumrongwittayapak and R. Varakulsiripunth, "Detecting sinkhole attack and selective forwarding attack in wireless sensor networks," 2009 7th International Conference on Information, Communications and Signal Processing (ICICS), 2009, pp. 1-5, doi: 10.1109/ICICS.2009.5397594.

[16]. W. Xin-sheng, Z. Yong-zhao, X. Shu-ming and W. Liang-min, "Lightweight defense scheme against selective forwarding attacks in wireless sensor networks," 2009 International

Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2009, pp. 226-232, doi: 10.1109/CYBERC.2009.5342206.

[17]. Y. B. Reddy and S. Srivathsan, "Game theory model for selective forward attacks in wireless sensor networks," 2009 17th Mediterranean Conference on Control and Automation, 2009, pp. 458-463, doi: 10.1109/MED.2009.5164584.

[18]. G. Li, X. Liu and C. Wang, "A sequential mesh test based selective forwarding attack detection scheme in wireless sensor networks," 2010 International Conference on Networking, Sensing and Control (ICNSC), 2010, pp. 554-558, doi: 10.1109/ICNSC.2010.5461599.

[19]. S.-B. Lee and Y.-H. Choi, A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks, In Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN‟06), pp. 59-70, 2006. “ https://doi.org/10.1145/1180345.1180353

[20]. S. Zhu, S. Setia, and S. Jajodia, LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks, The 10th ACM Conference on Computer and Communications Security (CCS ‟03), 62-72, 2003. https://doi.org/10.1145/1218556.1218559

[21]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Proceedings of the 6th annual international conference on Mobile Computing and Networking (MobiCom ‟00), 2000, pp. 255–265. https://doi.org/10.1145/345910.345955

[22]. N. Nasser and Y. Chen, SEEM: Secure and energy efficient multipath routing protocol for wireless sensor networks, Computer Communications, Volume 30, Issue 11-12, pp. 2401-2412, September 2007. https://doi.org/10.1016/j.comcom.2007.04.014

[23]. N. Ahmed, S. S. Kanhere, and S. Jha, “Intrusion Detection Techniques for Mobile Wireless Networks,” Mobile

Computing and Communications Review, Vol. 9, No. 2, pp. 418, 2005.

[24]. X. Pu, Z. Yan, S. Mao, Y. Zhang and Y. Li, "The sequential mesh test for a proportion," in Journal of East China Normal University, No. 1, 2006, pp. 63-71. https://xblk.ecnu.edu.cn/EN/Y2006/V2006/I1/63

[25]. L. Xiao et al., "PHY-Authentication Protocol for Spoofing Detection in Wireless Networks," 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, 2010, pp. 1-6, doi: 10.1109/GLOCOM.2010.5683463.

[26]. F. A. Barbhuiya, S. Biswas and S. Nandi, "An active DES based IDS for ARP spoofing," 2011 IEEE International Conference on Systems, Man, and Cybernetics, 2011, pp. 2743-2748, doi: 10.1109/ICSMC.2011.6084088.

[27]. Ferdous A Barbhuiya, Santosh Biswas and Sukumar Nandi, "An Active Host-based Intrusion detection system for ARP-related attacks and its verification", IEEE Trans. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011. https://doi.org/10.5121/ijnsa.2011.3311

[28]. Wesam S. Bhaya and Samraa A. AlAsady, "Prevention of Spoofing Attacks in the Infrastructure Wireless Networks," proc IEEE Journal of Computer Science 8 (10): Page(s): 1769-1779, 2012.

[29]. A. Broumandan, A. Jafarnia-Jahromi, V. Dehghanian, J. Nielsen and G. Lachapelle, "GNSS spoofing detection in handheld receivers based on signal spatial correlation," Proceedings of the 2012 IEEE/ION Position, Location and Navigation Symposium, 2012, pp. 479-487, doi: 10.1109/PLANS.2012.6236917.

[30]. J. Yang, Y. Chen, W. Trappe and J. Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 44-58, Jan. 2013, doi: 10.1109/TPDS.2012.104.

[31]. Q. Zeng, H. Li and L. Qian, "GPS spoofing attack on time synchronization in wireless networks and detection scheme design," MILCOM 2012 - 2012 IEEE Military Communications Conference, 2012, pp. 1-5, doi: 10.1109/MILCOM.2012.6415619.

[32]. Z. Zhang, M. Trinkle, L. Qian and H. Li, "Quickest detection of GPS spoofing attack," MILCOM 2012 - 2012 IEEE Military Communications Conference, 2012, pp. 1-6, doi: 10.1109/MILCOM.2012.6415722.

[33]. Hao Yang, Haiyun Luo, Yi Yang, Songwu Lu and Lixia Zhang, "HOURS: achieving DoS resilience in an open service hierarchy," International Conference on Dependable Systems and Networks, 2004, 2004, pp. 83-92, doi: 10.1109/DSN.2004.1311879.

[34]. Ahmed M.AbdelSalam ,Wail S.Elkilani and Khalid M.Amin, "An Automated approach for Preventing ARP Spoofing Attack using Static ARP Entries" Proc IEEE (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014. doi=10.1.1.676.4047

[35]. Y. Chen, W. Trappe and R. P. Martin, "Detecting and Localizing Wireless Spoofing Attacks," 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2007, pp. 193-202, doi: 10.1109/SAHCN.2007.4292831..

[36]. Archana Shelar and M.D.Ingale, "Modeling Security with Localization of Multiple Spoofing Attackers in Wireless Network," The International Journal Of Engineering And Science (IJES), Volume 3, Issue 01, Pages 01-06, 2014. DOI:10.1109/TPDS.2012.104

[37]. J. Yang, Y. Chen, W. Trappe and J. Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks," in IEEE Transactions on Parallel and Distributed

Systems, vol. 24, no. 1, pp. 44-58, Jan. 2013, doi: 10.1109/TPDS.2012.104.

[38]. K. Salah, J. M. Alcaraz Calero, S. Zeadally, S. Al-Mulla and M. Alzaabi, "Using Cloud Computing to Implement a Security Overlay Network," in IEEE Security & Privacy, vol. 11, no. 1, pp. 44-53, Jan.-Feb. 2013, doi: 10.1109/MSP.2012.8

[39]. Patel, Anshuman, and Devesh Jinwala. "A reputation-based RPL protocol to detect selective forwarding attack in Internet of Things." International Journal of Communication Systems 35.1 (2022): e5007.

[40]. Ezhilarasi, M., Gnanaprasanambikai, L., Kousalya, A. et al. A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks. Soft Comput (2022). https://doi.org/10.1007/s00500-022-06915-1.

[41]. Shafique, Arslan, Abid Mehmood, and Mourad Elhadef. "Detecting signal spoofing attack in uavs using machine learning models." IEEE Access 9 (2021): 93803-93815.