**Zigbee Technology**

Zigbee is one of the most widely used wireless sensor network standards with low power, low data speed, low cost, and short-latency, easy to deploy and provides high security and high data reliability. The name Zigbee is derived from the pattern of bees between flowers, indicating the relationship between the nodes in a mesh network. [1], ZigBee is a technology for short range wireless data transfer especially designed for wireless low-power devices providing battery lifetimes up-to several years with a single AA battery. ZigBee is based on IEEE 802.15.4–2003 standard it adds the network and application layers on top of the Physical layer (PHY) and Medium Access Control layer (MAC), which are defined by IEEE 802.15.4–2003. ZigBee also provides enhanced security control and support for mesh networks.[2]

**why using Zigbee?**

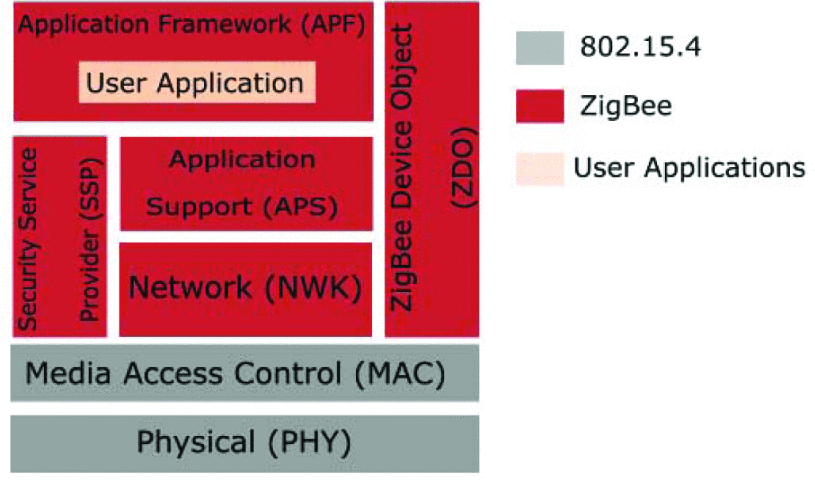
1. Reliable and self-healing
2. Supports a large number of nodes.
3. Easy to deploy and Secure
4. Very long battery life and low cost
5. It can be used globally and remotely upgradeable firmware
6. Open Standards protocol with no or negligible licensing fees
7. Low power (ability to operate on batteries measured in years)
8. Low maintenance (meshing, self-organizing)
9. Standards-based security AES 128). [1]

**ZIGBEE APPLICATION:**

The throughput of ZigBee is low, the rate of data transfer is about 250kbps. So, this ZigBee system is useful for applications that need a low data rate. Some of its applications are; Home Automation and Control, Automatic Meter Reading, Residential & commercial utility systems, Building Automation, Personal health care, Body area networks, Fitness monitoring: home, gym, on–the–move, ZigBee Smart Energy, Hospital & institutional, Patient monitoring, Cable replacements, Automotive, In-vehicle control: vehicular & entertainment, Status monitoring, Telecom Services. ZigBee's main scope and purpose is “home automation” including sensors and actuators, such as rain/light/smoke sensors, locks, and windows. [1], [2]

**ZigBee Network Architecture:**

ZigBee standard is built on the top of the IEEE 802.15.4 standards and defines two layers: physical layer (PHY) and media access layer (MAC) where they are the basis of other industrial wireless technologies. [3]



PHY - A layer defined by 802.15.4 which is responsible for modulation, demodulation, physical transmission of packets, and different mechanisms to avoid radio noise transmission interference. [3]

MAC - Another layer defined by 802.15.4 to identify network topologies where ZigBee built on top. Its main purpose is to avoid collisions while transmitting frames whose format just as the MAC addresses.[3]

NWK - This layer supports the ability to discover and join networks. It is a ZigBee layer that expands the network topologies defined by the 802.15.4 to allow the mesh networking. It also decides routes through ZigBee network and defines ZigBee addresses that are different than the MAC addresses. [3]

APS - Another ZigBee layer that is responsible for packets duplication filtering as well as maintaining a binding table of all nodes in the network. [3]

SSP - The ZigBee layer that provides security services for both NWK and APS as in device management, frame protection, and key establishment and transport. [3]

ZDO - A ZigBee layer that is responsible for the overall management of ZigBee device. It allows device discovery, manages binding requests, initializes both APS and NWK layers, and defines the device mode (coordinator, router, or end device) which will be explained later. [3]

APF - This ZigBee layer maintains the execution environment for the user applications, and it is responsible for data exchange between those applications. It also provides an endpoint for each device.[3]

**In any ZigBee network, there are three node types that perform useful work as acting a sensor. Nodes are:**

Coordinator: A parent node that starts up a network, selects the frequency, defines the PAN (personal area network) ID, and allows other children nodes to join the network. It can run other special services as in routing and security services. [3]

Router: This node is not a must in a ZigBee network, however; it is still commonly found and responsible for relaying messages to other nodes. [3]

End Device: A simple node that does only sending and receiving messages with no other special functionality in the ZigBee network. [3]

**Zigbee Security:**

ZigBee Security deploys AES 128-bit encryption algorithm, which includes security services such as key deployment, key forwarding, frame protection and device management. Security at ZigBee comes to an end in simplicity, openness and security. Each layer is responsible for supplying the frame from the source, each source and destination nodes have direct key exchange, and data is transmitted at each hop (end to end) without the need for decoding and encryption. [3]

There are a few security built-in services that ZigBee standard offers to secure frame communications between nodes:

It uses a symmetric cipher to maintain data privacy from being exploited by other parties without the possession of the cryptographic key. [3]

ZigBee deploys the AES algorithm with the Cryptographic block Ciphers Mode (Counter with CBC -MAC) encryption. It offers both authentication and confidentiality while data transferred. However, ZigBee simplifies the encryption process by enabling the reuse of the same key at each level of the ZigBee stack. [3]

To maintain data integrity from being modified by other parties, ZigBee deploys the message integrity check (MIC). This service may also ensure that data come from a node that has the cryptographic key. [3]

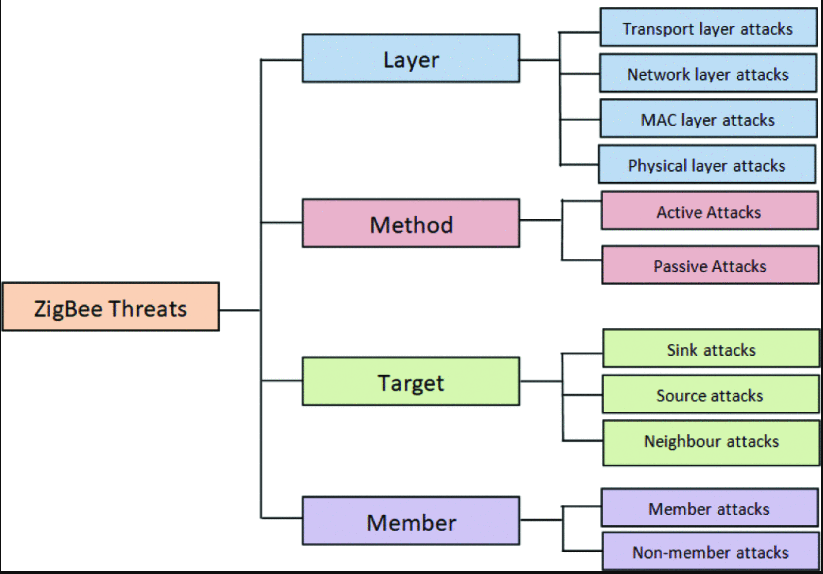
Authentication can be maintained in the NWK and APS layers using the active network key and the link key respectively. Consequently, information can be synchronized between devices while simultaneously providing authenticity through the shared keys. [3]

One valuable security built-in service the ZigBee utilizes is the trust centre. It manages new devices integrated into the network and it updates the network shared key regularly as well. Usually, the coordinator node is the trust centre and shall be recognized to all other nodes in the network. [3]

There are three types of security keys utilized by the ZigBee standard; master, network, and link key. Each key has different security functionality and can be shared between devices by different techniques. [3]

**ZigBee Security Issues and Vulnerabilities**:

ZigBee is characterized in a few built-in security services and features, however; its applications are still vulnerable to network attacks as in sniffing the network key which is sent in plaintext for instance. the fig below illustrate attacks on ZigBee can be categorized into the following: [3]



**Layers Attacks**

Transport Layer Attacks: This layer is utilized to support communication links for sensors newly joining the network. Attacks might include flooding and de-synchronization; where the targeted node is flooded by a numerous number of invalid connection establishment requests (flood attack), and forging packets to one or both ends of connection so that host requests to retransmit the missed packet frames (de-synchronization attack)[3].

Network Layer Attacks: This layer is responsible for routing process and network traffic. Attacks might include wormholes and selective forwarding attacks. In the wormhole attack; there should be two malicious nodes that are located on different hops of the network. When a sender node transmits a data frame, one malicious node tunnels this data to the other malicious node and by which it will send it to the neighbouring nodes in turn. Consequently, the sender node is tricked that malicious nodes are close by one or two hops where these two malicious nodes might be out of range [3].

MAC Layer Attacks: It incorporates the MAC header that helps the receiver to know the length of the packet, retransmits of frames in case of errors, and allocates resources for newly joined nodes. Link layer jamming is one example of MAC layer attacks that is launched to create DoS by interrupting messages exchange between transmitting and receiving nodes. This would degrade and reduce the performance of the network consequently [3].

Physical Layer Attacks: Attacks are mainly exploiting the common radio signal by jamming to either eavesdrop or tamper the data packet frames [3].

**Method Attacks**

Active Attacks: This attack requires an actual interception of the network where the adversary can modify the data, inject fault data frames, consequently; the network performance is negatively affected. Moreover, data integrity and confidentiality are compromised [3].

Passive Attacks: Unlike active attacks, no actual interception of the real communication stream, but rather attacker monitors the data traffic without affecting its integrity. However; the confidentiality of information is exposed as sensitive information can be collected for some other malicious intent [3].

**Target Attacks**

Sink Attacks: Sinkhole or simply the sink attack can take place when a malicious node announces a route to be the shortest path. And since all routing algorithms o select the shortest path, it will attract more network traffic to be tunnelled toward it. Usually, this attack is combined with wormhole attack [3]

Source Attacks: In these attacks, the adversary compromises one legitimate node to act as a black hole node; a node that selectively drops received packets or all received packets to trick other neighbouring nodes to search for another rout as the previous one has failed.[3]

Neighbour Attacks: This type of attack exploits the process of discovering other neighbouring nodes by broadcasting HELLO message. A malicious node sends HELLO message with a high transmission power, and hence the receiving nodes consider this node as its neighbour and will send the sensed packet data in return. Consequently, a huge amount of energy will be wasted, and congestion might occur consequently. [3]

Member Attacks: Sometimes are referred as outcast and insider attacks. In the case of outcast attacks; the attacker node is not part (non-member) of the network but authorized to threat the network. On the other hand, the insider (member) attack takes place when a malicious node is part of the network either by compromising it or the attacker has loaded a fake profile and asked to join the network [3].

Energy Depletion Attack (Ghost Attack): attacker sends faked messages to lure node to intentionally to deplete that node’s energy by redundant security-related computations. This will cut back the node’s lifetime and enable the attacker to launch several after-depletion attacks as in Denial of Service (DoS) and reply attacks accordingly [3].

All threats against ZigBee security are not only focused on just interfering, sabotaging, or manipulating the data itself, indeed, a physical attack is possible against ZigBee-enabled networks. [2]

Since ZigBee is often used in increasingly important applications, such as controlling the infrastructure of critical systems in a commercial building, industrial plant, utility grid, or a home security system, it is very important to design the ZigBee-enabled network in such a way that the devices are also protected from physical attacks. This means, for example, placing the devices to such locations that are hard to reach and protecting them with some kind of surveillance (e.g. by using an intrusion detection and prevention system). [2]

If an attacker is capable of stealing a ZigBee device, it is possible to extract its data and even the stored security keys. It is important that either some kind of automatic system exists for noticing missing devices or that periodical checks are being made. In a case of a missing device, the security keys must be updated immediately to prevent unauthorized use of the whole ZigBee-enabled network. [2]

References:

1-@inproceedings{ramya2011study,

title={Study on ZigBee technology},

author={Ramya, C Muthu and Shanmugaraj, M and Prabakaran, R},

booktitle={2011 3rd International Conference on Electronics Computer Technology},

volume={6},

pages={297--301},

year={2011},

organization={IEEE}

}

2- @inproceedings{vidgren2013security,

title={Security threats in ZigBee-enabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned},

author={Vidgren, Niko and Haataja, Keijo and Patino-Andres, Jose Luis and Ramirez-Sanchis, Juan Jose and Toivanen, Pekka},

booktitle={2013 46th Hawaii International Conference on System Sciences},

pages={5132--5138},

year={2013},

organization={IEEE}

}

3- @inproceedings{khanji2019zigbee,

title={ZigBee Security Vulnerabilities: Exploration and Evaluating},

author={Khanji, Salam and Iqbal, Farkhund and Hung, Patrick},

booktitle={2019 10th International Conference on Information and Communication Systems (ICICS)},

pages={52--57},

year={2019},

organization={IEEE}

}