ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.5

A Brief Review: To Enhance the Security and Battery Life in ZigBee Network

Navneet Singh[1], Anantdeep Kaur[2]
M.Tech Student[1], Assistant Professor[2]
Department of Computer Engineering
Punjabi University, Patiala, India

Abstract:
Zigbee is standard based wireless technology developed to resolve the unique requirements of low-power wireless sensor, low-cost and control networks in any market. But there are significant issues associated with the security in the ZigBee wireless Network. Along with this, it has been seen that battery consumption in the ZigBee wireless Network is very high. Various techniques have been discovered to improve the battery life in ZigBee Networks. In this paper, we will review the existing issues and propose a solution for resolving these security issues. We will review various methods that have been proposed for optimizing the active and sleep mode for efficient power consumption. Also, different techniques to optimize the battery life is demonstrated in this paper

Index Terms: ZigBee Network, sleep mode, battery consumption

I. INTRODUCTION

IoT (Internet of things) is one of significant information industry in the computer. And the internet ZigBee wireless technology is one of the main technology used in the IoT. It is preferable for situations where low data transmission rate, small-scale implementation, fewer communication data and easy installing and using is required [1]. Zigbee is standard based wireless technology developed to resolve the unique requirements of low-power wireless sensor, low-cost and control networks in any market. Using Zigbee, there is a limitless opportunity for development in the new markets along with the introducing innovation in the existing markets[1]. It is because Zigbee can be easily implemented and little power is required to operate it. There is no limit on theplace; it can be used anywhere [2]. The mainfeatures of the ZigBee wireless technology are that it uses 2.4 GHz radio frequency. This range of frequency allows easy to use and reliable standard. It provides great power consumption efficiency and wireless performance. Because of its various benefits, it has been employed in numerous application including the business, industrial users, government area and much more. Along with this, most of the standards provided by the ZigBee Network are green and save a significant amount of money of the users [4]. In simple words, ZigBee refers to high-level networking protocols which have been used in various application. there are numerous applications of the ZigBee network in the personal area as well. It includes:

- Building automation
- Home entertainment such as music and television.
- Home security such as door and window sensors
- Smoke, flood temperature sensors
- Home control, etc.

1.1. The Name ZigBee

The main operation of the Zigbee standards is to emulate the protocol with a bunch of simple and isolated organism that work together to solve the complex and tedious tasks. In this essence, the name Zigbee came from the domestic honeybee. To communicate important information to the hive member, honeybee uses a specific zig-zag type of dance. Therefore, the correlation of honeybee communication was directly related to the protocol and named it as "Zigbee [8].

1.2. ZigBee Alliance

It is an alliance for making low-power wireless where different companies work together to define an open global standard [6]. The main purpose of the ZigBee Alliance is to develop a specification that can easily converse idea to build diverse and unique network topologies with features that include high data security, reliability, and innovation. Along with this, the intended outcome of ZigBee Alliance is to provide interoperable application profileswhich are at the top of the IEEE 802.15.4 wireless standard. Thecompanies from a varied spectrum of categories are comprised in the ZigBee Alliance. These include the companies from chip manufacturing to the companies that integrate systems [12].

1.3. ZigBee device TYPES (components)

The devices which are used in the ZigBee network can be divided into two categories includingthe reduce function device (RFD) and Full Function Device (FFD) [3].

FFD can execute all the functions which are explained in the ZigBee Wireless Network Standard. It could act like all the roles in the Zigbee network. FFD also work as an important component of the ZigBee Network which is network coordinator. It is ideal for various network router functions if additional memory and computing power can be added into the full function device (FFD) [7].

On the other hand, **RFD** performs half functions compared to the FFD. It is apparent from its processing capacity and memory size which is approximately half than the full function device. It is employed in network-edge devices. It is suitable for the applications that require low power consumption [6].

ZigBee Coordinator (ZC): ZigBee coordinator is a special router and a full-function device. There is always one coordinator in every ZigBee Network. It is accountable for building the network. To build the network, it is necessary for the ZC to select the appropriate channel, extended network address, and PAN ID [10].

1. It selects the appropriate channel and forms a ZigBee network.
2. It is responsible for assigning the address to the nearby nodes and routers present in the network.
3. Other devices present in the network can leave and join the network with the permission of the ZigBee Network.
4. It has the list of all the neighboring nodes and routers, and it transfers packets to other devices by acting as an intermediate medium.

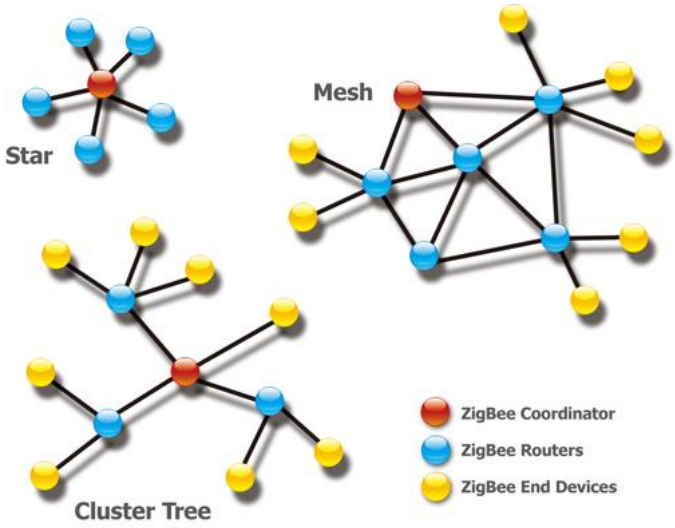

Figure.1. ZigBee Network Devices

ZigBee Router (ZR): A router is a full-function device (FFD). It is used in mesh and tree topologies to expand the coverage of the network. It finds out the best route from the source of the message to the destination. It performs almost all the functions that coordinator perform, but it also establishes the network [1].

ZigBee End Device (ZED): A ZED cannot relay data from other devices and have long battery life compared to other devices. The ZigBee end device requires the least amount of memory.

1.4. NETWORK TOPOLOGIES

Two types of network including the star topology and the peer-to-peer topology are managed through the IEEE 802.15.4 standard. We can also combine these two topologies to build a mesh network [7].

Star network formation

In ZigBee network, star formation develops when both the FFD and RFD communicate with the PAN coordinator. The first full functional device when establishing its own network become the coordinator representing the Personal Area Network (PAN). All the networks which are in the sphere of the coordinator possess unique PAN identity. The entire node including the FFD and RFD communicate to the PAN coordinator [4]. It has a flexible network structure and support tree shape, mesh shape and star shape topologies. In all of these topologies, the simplest one is the star topology. In this topology, all the communication is managed by the coordinator. On the other hand, ZigBee network with tree shape, communication between every two nodes. It is possible through its parent nodes. When one node wants to transmit data, the starting node becomes the parent node. After that parent node sends the data to the coordinator which further move it to the destination.

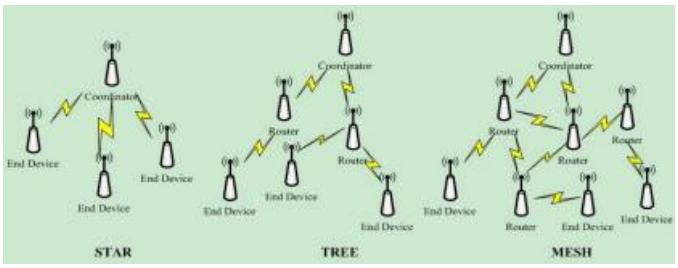

Figure.2. ZigBee Network Topologies

Peer-to-Peer network formation

The peer-to-peer network topology is different from the star topology. Similar to a star topology, peer-to-peer network topology also has the PAN coordinator, but unlike star topology, any device can communicate with another device without an intermediate connection [4].

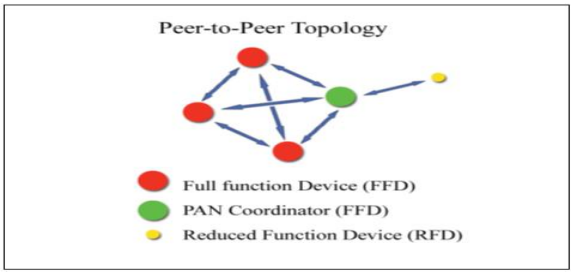

Figure.3. Peer-to-Peer Network topology

But all the devices should be in the range of one another for communication. The topology allows the formation of complex networks such as the mesh topology.

1.5. ZigBee Networking

We can extend the network through ZigBee using the mesh networking. In that scenario, thousands of nodes can communicate over a large area. Each Full Function device directs the messages and thus act as a router [4]. The routing protocol is used to select the most economical, reliable and shortest path between the sender and the receiver for communication. The protocol can also change the path dynamically as per the evolving conditions. Therefore, it builds an extremely reliable network, where the network diverts the communication path in the node failure case. This is similar to the concept of redundancy which is used on the Internet [3].

II. LITERATURE SURVEY

In this section, we will review all the research that has been done in the ZigBee Networks. The literature review provides insight into the key issues and the possible solution to these issues that emerge in the ZigBee Network.

Alcaraz and Lopez (2010) reviewed three standards Wireless Hart, ZigBee Pro and ISA 100.11a and analyzed their security. There are various communication standards such as Wireless Hart, ZigBee Pro, and ISA 100.11a to carry out the control processes in real time. Various potential; security threats and

vulnerabilities has been identified in this paper. Along with the paper provide significant solutions to mitigate these potential risks, threats, and vulnerabilities of these three standards.

Burchfield et.al [2007] reviewed the throughput of the ZigBee Network. Used a three-phase approach in order to measure and attain the maximum possible throughput in ZigBee. The practical calculation, Ns-2 simulation, and the last hardware implementation were the three main phases of the research. The first two phases helped to obtain the approximate practical upper bound of 120kbps. On the other hand, thelast phase helped to increase the overall throughput of the system. The result of the implementation shows that the throughput of the ZigBee Wireless Network has been increased to agreat extent with the proposed hardware method [2].

Mihajlov and Bogdanoski [2011] presented a performance evaluation of ZigBee which is IEEE 802.15.4 standard, including Media Access Control (MAC) sub-layer and the Physical (PHY) layer, which permits a simple communication between the sensors. They delivered a precise simulation model regarding the specifications of IEEE 802.15.4 standard. They simulated and analyzed two different states, where we examine the performance and topological features of the IEEE 802.15.4 standard using OPNET simulator. They compared the three possible topologies (Star, Mesh, and Tree) to each other [3].

Qianqian and Kejin [2009] deliberated the security structures of ZigBee wireless network, analyzed the security of NWK, MAC, and APL layer. They completelyanalyzed the encryption and authentication in ZigBee technology and proposed ideas for network security protection that effectively solves the integrity, confidentiality, and access control problems in wireless network communication [4].

Radmand et.al [2014] presented two different methods for grasping the cryptographic key in ZigBee. These are the remote attack and physical attack. They also conducted surveys and categorized some other attacks which can be performed on ZigBee networks that include spoofing, eavesdropping, DoS and replay attacks at different layers of the communication link. From this analysis, it is shown that some vulnerabilities still present in the existing security schema used in the ZigBee technology [5].

Anantdeep et.al [2010] In order to enhance the mobile node's power consumption, effective transmission power control based on LQ (link quality) and handover sequence based on MAC broadcast are employed. Experimental results illustrate that by using the proposed architecture, power consumption and communication time of mobile nodes can be reduced by 42.8%, and 1.2 seconds respectively[6].

Bimaljeet Kaur and Anantdeep Kaur [2016] Improved design and implemented an electrocardiogram monitoring system using wireless ZigBee topologies that can be utilized for remote ECG analysis, monitoring, and diagnosis. By using wireless network topologies such as mesh, star, etc. The program as the main design, a number of important problems have been considered in them i.e. network robustness, network creation, data throughput, route maintenance, data loss, and in particular node status indication and power consumption [7].

O. Ayurzana, & S., Tsagaanchuluun. (2016) developed an energy efficient ZigBee wireless module. To develop the ZigBee wireless module, the MG2455-F48 RF SoC chip was used In this paper. It was developed with an 8051 family microcontroller and 2.4 GHz RF part. To makes the module movable; battery is used in the ZigBee wireless module.

Q. Pan, J. Wu, Y. Wang and J. Ni, (2011).considered a simple P2P (point-to-point) bike WSN(Wireless sensor Network). Various bike parameters including the speed and cadence were checked, monitored and transmitted through the ZigBee wireless communication-based protocol. Because of the every rotation of the bike wheel, all the bike parameters are monitored and transmitted continuously that does not allow sleep mode for a long time. This eventually causes a high power consumption. Therefore, new algorithm names as Redundancy and Converged Data (RCD) has been proposed in the paper. this new algorithm allows sensor node to went into the sleep mode while maintaining its performance parameters as well [9].

M. Kasraoui, A. Cabani, &, J. Mouzna, (2012) provided a synthetic study in order to analyse the performance of the routing protocols. Along with this, enhancement in the routing protocols of the ZigBee standard used in Wireless Sensor Network (WSN) is given. The paper shows optimization of the different routes from the source to the destination. The objective of the research was to enhance the existing protocol for its scalability and using the enhanced protocol in the variable network sizes. ZBR-M solution is proposed in this paper [10].

III. FINDINGS

We researched the previous work in the ZigBee network. The table given below represent our findings from the previous researches that have been done in the same field of ZigBee Networks.

Year	Researchers	Algorithm/Method	Issue Identified	Countermeasure
2010	Cristina, and J. Lopez	Reviewed three methods of wireless communication network	Sniffing, jamming, overloading, flooding, etc. security issues has been identified	Check blacklist, identity validation mapping, redundancy collision control, etc. countermeasures has been provided.
2007	Burchfield, T. Ryan	hardware implementations on Ember Corporation EM2420 based development equipment	Low ZigBee Wireless Network throughput	Increased the overall throughput of ZigBee Wireless Network.
2009	M. Qianqian and B. Kejin	Reviewed ZigBee Network Protocol	Confidentiality, integrity and access control problem has been identified.	Provided opinion for network security protection.

2011	Mihajlov, Boris, and Mitko Bogdanoski	Evaluated performance of ZigBee and analyzed two different scenarios for topology features	Identified issues in the current WSNs.	Proposed two models for efficient implementation of WSNs.
2011	P. Radmand, et al	Two different ways remote attack and physical attack grabbing the cryptographic key in ZigBee	Vulnerabilities in sensor because of the limited memory, energy, and capability	Provided anoverview of vulnerabilities and how to tackle them.
2016	A.Kaur et al	surveyed existing work in Zigbee technology to communicate ECG signals	network creation, route Maintenance, network robustness, data loss and various other issues have been identified.	Proposed a new method for resolving the issues and compressed sensing
2010	B. Kaur and A. Kaur	power control based on link quality and handover sequence based on MAC broadcast are employed	High power consumption	Proposed method for energy efficiency
2016	O. Ayurzana, & S., Tsagaanchuluun.		High energy consumption by the ZigBee wireless module	Hardware technique to solve the power consumption issues
2011	Q. Pan, J. Wu, Y. Wang and J. Ni.	Hardware technique used with MG2455-F48 RF SoC chip	High energy consumption by ZigBee wireless module battery	The proposed hardware technique proved to be energy efficient.
2012	M. Kasraoui, A. Cabani, &, J. Mouzna	Redundancy and Converged Data (RCD) algorithm	Less sleep mode time for the sensor node	Increased the sleep mode time for the sensor mode while maintaining the performance parameters with the proposed method.

IV. CONCLUSION

In this paper, we have reviewed the ZigBee Networks, its architecture and main network components. ZigBee is one of the robust wireless communication standards which is managed by the ZigBee Alliance. Zigbee is standard based wireless technology developed to resolve the unique requirements of low-power wireless sensor, low-cost and control networks in any market.The results and the finding from the previous work have been demonstrated in this paper. All the key findings will help to conduct further research about the ZigBee Networks.

V. REFERENCES

[1]. Cristina, and J. Lopez. "A security analysis for wireless sensor mesh networks in highly critical systems." IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 40.4 (2010): 419-428.

[2]. Burchfield, T. Ryan, S. Venkatesan, and Douglas Weiner. "Maximizing throughput in ZigBee wireless networks through analysis, simulations, and implementations." Proc. Int. Workshop Localized Algor. Protocols WSNs. 2007.

[3]. M. Qianqian and B. Kejin. "Security analysis for wireless networks based on ZigBee." Information Technology and Applications, 2009. IFITA'09. International Forum on. Vol. 1. IEEE, 2009.

[4]. Mihajlov, Boris, and Mitko Bogdanoski. "Overview and analysis of the performances of ZigBee-based wireless sensor networks." International Journal of Computer Applications 29.12 (2011): 28-35.

[5]. P. Radmand, et al. "ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys." P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2010 *International Conference on. IEEE*, 2010.

[6] A.Kaur et al. "A brief review: ECG-based Health Monitoring System through Zigbee Sensor Networks." *Imperial Journal of Interdisciplinary Research*, 2.6, 2016.

[7].B. Kaur and A. Kaur "Mobile Zigbee Sensor Networks." arXiv preprint arXiv: 1004.4465 (2010).

[8]. O. Ayurzana,&S., Tsagaanchuluun. (2016). The design of Energy Efficient ZigBee Module. *Journal of Communication and Computer*, *13*(7), 373-377. doi:10.17265/1548-7709/2016.07.006

[9]. Q. Pan, J. Wu, Y. Wang and J. Ni. "An Implementation Method for ZigBee Network Layer," *International Journal of Communications, Network and System Sciences*, 4, pp: 626-629, 2011.

[10]. M. Kasraoui, A. Cabani, &, J. Mouzna, "Improvement of Zigbee Routing Protocol. *2012 IEEE International Conference on Green Computing and Communications*, 788-793. doi:10.1109/greencom.2012.150, 2012.

[11]. J. Kaur, A. Kaur, and J. Singh. "An Efficient Hybrid Topology Construction in Zigbee Sensor Network," International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), 2014.

[12]. C. Zhang and W. Luo, "Topology Performance Analysis of Zigbee Network in the Smart Home Environment," *International Conference on Intelligent Human-Machine Systems and Cybernetics*, 438-440, 2014.