International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Survey on Creating ZigBee Chain Reaction using IoT

Sanjay M. Patil[1], Prof. Mirza Moiz Baig[2]
[1]M.Tech. Student, Department of Computer Science & Engineering J. D. C. E. M., Nagpur Maharashtra, India
[2]Assistant Professor, Department of Computer Science & Engineering J. D. C. E. M., Nagpur Maharashtra, India

ABSTRACT

To meet the sensors and control devices standards for wireless communication in high data rate communication with low latency and low energy consumption at lower bandwidth, Zigbee technology provides low cost and low power consumption which is best suited for various embedded systems widely deployed for controlling and monitoring applications where it covers 10-100 meters within the range. This communication system is less expensive and simpler than the other proprietary short-range wireless sensor networks as Bluetooth and Wi-Fi. The Internet of Things (IoT) is currently going through exponential growth, and some experts estimate that within the next five years more than fifty billion "things" will be connected to the internet.

Keywords : IoT, Wi-Fi, Zigbee.

I. INTRODUCTION

Zigbee supports different network configurations for master to master or master to slave communications. It can be operated in different modes as a result the battery power is conserved. Zigbee networks are extendable with the use of routers and allow many nodes to interconnect with each other for building a wider area network.

It employs a suite of technologies to enable scalable, self-organizing, self-healing networks that can manage various data traffic patterns. ZigBee is a low-cost, low-power, wireless mesh networking standard. In industry ZigBee is being used for next generation automated manufacturing, with small transmitters in every device on the floor, allowing for communication between devices to a central computer. This new level of communication permits finely-tuned remote monitoring and manipulation.

II. TECHNOLOGY USED

The Internet of Things (IoT) is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of this concept is the pervasive presence around us of a variety of things or objects – such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals.

Unquestionably, the main strength of the IoT idea is the high impact it will have on several aspects of everyday-life and behavior of potential users. From the point of view of a private user, the most obvious effects of the IoT introduction will be visible in both working and domestic fields. In this context, domotics, assisted living, e-health, enhanced learning are only a few examples of possible application scenarios in which the new paradigm will play a leading role in the near future. Similarly, from the perspective of business users, the most apparent

consequences will be equally visible in fields such as, automation and industrial manufacturing, logistics, business/process management, intelligent transportation of people and goods.

Several industrial, standardization and research bodies are currently involved in the activity of development of solutions to fulfill the highlighted technological requirements. This survey gives a picture of the current state of the art on the IoT. More specifically, it:

- provides the readers with a description of the different visions of the Internet of Things paradigm coming from different scientific communities;
- reviews the enabling technologies and illustrates which are the major benefits of spread of this paradigm in everyday-life;
- offers an analysis of the major research issues the scientific community still has to face.

Manifold definitions of Internet of Things traceable with in the research community testify to the strong interest in the IoT issue and to the vivacity of the debates on it. By browsing the literature, an interested reader might experience a real difficulty in understanding what IoT really means, which basic ideas stand behind this concept, and which social, economical and technical implications the full deployment of IoT will have. The reason of today apparent fuzziness around this term is a consequence of the name "Internet of Things" itself, which syntactically is composed of two terms. The first one pushes towards a network oriented vision of IoT, while the second one moves the focus on generic "objects" to be integrated into a common framework. Differences, sometimes substantial, in the IoT visions raise from the fact that stakeholders, business alliances, research and standardization bodies start approaching the issue from either an "Internet oriented" or a "Things oriented" perspective, depending on their specific interests, finalities and backgrounds.

III. RELATED WORK

In recent years numerous works on the security of IoT devices and protocols were published. Regarding connected lights, several vulnerabilities were discovered. Alex Chapman [1] managed to extract hard coded encryption keys used to encrypt data sent between LIFX brand light bulbs. From this he recovered the Wi-Fi password of the local network that was sent between the bulbs. Dhanjani[2] had shown DoS (denial of service) attacks against Philips Hue. Ronen and Shamir [3] have shown how to use the Philips Hue and LimitlessLed systems to create a covert channel to exfiltrate data from air-gapped networks, and to create strobes that can cause epileptic seizures. Heiland[4]found weaknesses in the Osram Lightify app such as unencrypted Wi-Fi passwords, lack of authentication in the gateway and vulnerable usage of ZigBee Home Automation profile. However those vulnerabilities are not related to the ZLL (ZigBee Light Link) protocol discussed in this paper. There are several works specific to the ZLL protocol and related products. Armknecht et al.[5] proposed a formal security model. Zillner[6] and Morgner et al.[7] demonstrated weaknesses in ZLL and ways to take over lights. 1. The Philips engineers we talk with stated that in a dense urban environment, the effective range can be less than 30 meters However to be able to take over lights from a distance they had to use custom hardware with much stronger transmission power. O'Flynn[8] reverse engineered some of the Philips Hue security design choices, where he raised the possibility of a lightbulb worm, but did not bypass either the firmware security protection or provide a spreading mechanism. The first power analysis attacks on Atmel AES hardware accelerators was done by Kizhvatov[9] against the Atmel XMEGA using AES-ECB mode. O'Flynn and Chen[10] used the same leakage model to attack the Atmel MegaRF128RFA1 hardware, and attacked the ZigBee CCM* mode of operation under the assumption of a known nonce. Jaffe[11] had shown an attack on counter mode

encryption with unknown nonce, but would require 2 16 sequential block operations on our hardware with the same nonce while our firmware can have at most 2 14 traces. Moreover, modifying the method by which the counter updates (using a linear feedback shift register, for example) would present a serious challenge to his attack.

Routing in ZigBee network is exactly different from the routing in traditional MANET networks because the routing protocols or algorithms in MANET are mainly concerned about the node mobility while in ZigBee network Full Function Devices (FFD) can serve as network coordinators or network routers, Reduced Function Devices (RFD) can only associate and communicate with FFDs. Therefore, the node heterogeneity plays an important role in ZigBee network routing. Nia-Chang et al.[12] performed a comprehensive study to check how the different mixture of nodes affects the performance of zigbee mesh network routing. The research was particularly done to find out the impact of heterogeneous nodes i.e mobile ZigBee routers and mobile ZigBee end devices on the performance of the ZigBee mesh routing. The results of his research shown that big performance differences will be there if the the network is highly heterogeneous and the routing performance in ZigBee network will also degrade if the network consists of large number of end devices .As a result, the packet delivery ratio also worsens. Moreover, comparing to AODV routing results, significant differences in routing performance have seen, when network nodes are not assumed to be equally capable. It has also revealed that the ZigBee end devices tend to perform worse than ZigBee routers in both sending and receiving packets, since the end devices incur much overhead in associating with new parents when there is network mobility. On the other hand, ZigBee routers typically suffer less packet loss when there are intensive amounts of mobility in the ZigBee network, yet the additional service overhead of ZigBee (such as association with children devices) still degrades the performance of ZigBee routers in almost all scenarios.

Another research area to be noticed is the effect of the mobile nodes on the performance of ZigBee protocol . Jiasong Mu and Kaihua Liu[13] analyzed the effect of the mobility of the nodes and the change of the network dimension in Zigbee networks. The whole research was carried out by using tool named OPNET. This analysis was done by using various routing strategies such that Suppress Route Discovery (SRD), Enable Route Discovery (ERD) and Force Route Discovery (FRD) with the change of node mobility and network dimensions. After the extensive evaluation, it has found that although the forced routing made the network to always find the shortest path in the network, but the FRD always had the worst performance. In the dynamic networks, ERD had the greatest efficiency as it is more suitable for the dynamic environments. AODV and ERD have the same working methodologies and both gives the best performance working with dynamic environments. As to the stable network, ERD and SRD had similar efficiency in the small ones. However, the SRD based on tree routing, required no memory cache. SRD also had the lowest network load when the scale of the network expanded. Whereas the ERD might do reduplicate routing due to the restricted memory space. The SRD was the best routing option for the stable networks and the ERD performed most efficient in the unstable networks.

The positioning of the nodes is considered to be the most important factor for improving the performance (e.g., throughput) of ZigBee networks .Using the mobile sink is often considered as a safeguard against the so-called hot-spot problem and the effects of mobile coordinator on the performance of the Zigbee network also need to be considered. In order to analyze the impact of keeping the coordinator mobile in a zigbee mesh network, Harsh Dhaka et al.[14] performed extensive simulation, using OPNET

Modeler and the results indicated that keeping the sink static gives the best performance. If a trajectory has to be chosen for other reasons, then the trajectory should give a considerable amount of time to each route that is the link route for a segment of the network. Otherwise (as in the case of Diagonal trajectory), it would result in a lower throughput. The factors that need to be considered specifically are: the type of the trajectory along with the node density and the network traffic. These are the factors that decide the performance of the system. Random topology is chosen to prevent exceptionally low throughput. Having the routers placed within range for effective meshing gives sharper curves which are closer but even in this case, it is better to keep the sink static at a location from where each route has an access to the sink possible with minimum hops. In circumstances sink movement is necessary, clever selection of the trajectory is essential for achieving the best throughput.

Ran Peng et al.[15] performed an extensive analysis to check the Zigbee network performance. According to this analysis, a strategy is proposed for the selection of ZigBee routing based on the various data services. The simulation results shown that this routing selection strategy gives excellent network performance with very less energy consumption. Additionally, the power control is not much considered in ZigBee Routing specification. But in case of the ad hoc wireless network application, power control is the most significant issue in ZigBee. So a power control strategy was also proposed to improve the ZigBee routing, the simulation results show that the proposed power control strategy will greatly balance the node energy, avoid that nodes use up all the battery power and die too early.

IV. CONCLUSION

Zigbee will play an important role in the future in the areas such as home automation, smart lighting, smoke and intruder warning traffic management, war fields etc. Zigbee technology is very useful from the perspective of the security as the devices maintain a list of trusted devices within the network and frame integrity to protect data from being modified by parties without cryptographic keys. The wireless communication technologies are rapidly spreading to many new areas, including the wireless sensors and the importance of the use of wireless technologies in data acquisition, building control, monitoring systems and automation of manufacturing processes will grow in future. Zigbee has a very promising future in front of it. Since the IOT devices are eminently focused on sending information between devices, or from them to Internet; one of the key measures to be taken, would be the protection of information traveling through them. In most cases this information travels through wireless networks or through public networks, which are vulnerable to being attack.

V. REFERENCES

[1]. A. Chapman. (2014) Hacking into internet connected light bulbs. Online]. Available: http://www:contextis:com/resources/blog/hacking-internet-connected-light-bulbs/

[2]. N. Dhanjani. (2013) Hacking lightbulbs: Security evaluation of the philips hue personal wireless lighting system. Online]. Available: http://www:dhanjani:com/docs/HackingLighbulbsHueDhanjani2013:pdf

[3]. E. Ronen and A. Shamir, "Extended functionality attacks on iot devices: The case of smart lights," in 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016, pp. 3–12.

[4]. D.Heiland. (2016) R7-2016-10: Multiple osram Sylvania osram lightify vulnerabilities. Online]Available: https://community:rapid7:com/community/infosec/blog/2016/07/26/r7-2016-10-multiple-osram-sylvania-osram-lightify-vulnerabilitiescve-2016-5051-through-5059

[5]. F. Armknecht, Z. Benenson, P. Morgner, and C. M¨uller, "On the Security of the ZigBee Light Link Touchlink Commissioning Procedure." Online]. Available: https://www1:informatik:uni-erlangen:de/filepool/publications/zina/ZLLsec-SmartBuildingSec16:pdf

[6]. T. Zillner, "Zigbee exploited - the good, the bad and the ugly," in Black Hat USA, 2015. Online]. Available: https://www:blackhat:com/docs/us-15/ materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp:pdf

[7]. P. Morgner, S. Mattejat, and Z. Benenson, "All Your Bulbs Are Belong to Us: Investigating the Current State of Security in Connected Lighting Systems," arXiv preprint arXiv:1608.03732, 2016.

[8]. C. OFlynn, "A lightbulb worm?" 2016. Online]. Available: https://www:blackhat:com/docs/us-16/materials/us-16-OFlynn-A-Lightbulb-Worm-wp:pdf

[9]. I. Kizhvatov, "Side channel analysis of AVR XMEGA crypto engine", in Proceedings of the 4th Workshop on Embedded Systems Security. ACM, 2009, p. 8.

[10]. C. O'Flynn and Z. Chen, "Power Analysis Attacks against IEEE 802.15. 4 Nodes," COSADE, 2016.

[11]. J. Jaffe, "A first-order dpa attack against aes in counter mode with unknown initial counter," in International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2007, pp. 1–13.

[12]. Nia-Chiang Liang, Ping-Chieh Chen, Tony Sun, Guang Yang, Ling-Jyh Chen, and Mario Gerla, "Impact of Node Heterogeneity in ZigBee Mesh Networks." IEEE International Conference on Systems, Man and Cybernetics, p.p.187-191, October 2006, Taipei, Taiwan.

[13]. Jiasong Mu and Kaihua Liu, "Effect of node mobility and network dimension to the Zigbee routing method." 6th International Conference Wireless Communications Networking and Mobile Computing (WiCOM), p.p. 1-5, September 2010, Tianjin, China.

[14]. Harsh Dhaka, Atishay Jain and Karun Verma, " Impact of Coordinator Mobility on the throughput in a Zigbee Mesh Networks." IEEE 2nd International Advance Computing Conference, p.p. 279-284, June 2010, Patiala, India.

[15]. Ran Peng, Sun Mao-heng, Zou You-min, "Zigbee Routing Selection Strategy Based on Data Services and Energybalanced ZigBee Routing." IEEE Asia-Pacific Conference on Services Computing (APSCC'06), p.p. 400-404, December 2006, Tongji, China.