iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** XI **Month of publication:** November 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Survey on ZIGBEE Wireless Networks

Dr.V. Venkatesakumar [#1], J.Dhandapani [*2], K.Vishnu [#3], S. Arifkhan [*4]
[#1] *Assistant Professor, CSE Department, Anna University Regional Centre*
[*2 #3*4] *P.G Scholar, CSE Department, Anna University Regional Centre*

Abstract*: ZigBee is an emerging worldwide standard for wireless personal area network. The main aim is to provide low-power, cost effective, flexible, reliable, secure and scalable. It is totally different from the other personal area network standards like Bluetooth, UWB, and Wireless USB. Wireless networks are vulnerable to various kinds of attacks (Due to their vulnerability there is possibility of important information getting lost). Already, most of these networks have provided security for a trusted environment. But, still there is occurrence of security issues. In this work, we are discussing about the categories of routing protocols, security mechanism and problems of security mechanism in ZigBee network.
Keywords - ZigBee, Wireless PAN, Security, IEEE 802.15.4

I. INTRODUCTION

In the last two decades wireless networks are becoming extremely popular in all over the world. Most of the applications are presently in analysis pipeline that is focused on new technologies within the field of device systems. The goal is to find new strategies of management, energy and routing management so as to enhance user's comfort or reducing installation value for devices.

The ZigBee standard is developed by the ZigBee Alliance. The ZigBee Alliance was formed in 2002 as a non-profit organization. In 2003, The IEEE 802.15.4 was released, that was adopted by ZigBee Alliance on December 14, 2006. ZigBee standard was set up on the IEEE 802.15.4. ZigBee a set of high level communication protocols to produce personal area networks designed from little, low power digital radios. It is not designed for transferring large amount of information, It is intended for the following applications like smart home, building automation , health care ,smart energy ,telecommunication, network devices, light link control, input device(Easy-to-use touchpad's, mice, keyboards, wands),smart energy(home energy savings, IP based home energy management) and retail services [1].

The IEEE 802.15.4 and the ZigBee network are tightly coupled to provide the consumer standardization for low power and low rate wireless communication devices. IEEE 802.15.4 PHY layer provides ISM 2.4 GHz for sixteen channels, ISM 900 MHz for ten channels, and one channel uses 868 MHz It can also provides link quality indicator in order to characterize the quality of links between nodes, also data transmission and reception. The carrier senses multiple Access with Collision Avoidance mechanism for accessing the channel used by IEEE 802.15.4 MAC and also the above mechanism used by IEEE 802.11 and IEEE 802.15.3 [2]. Most of the communication standards mainly specified for monitoring highly critical industrial systems are based on the IEEE 802.15.4 standard [3]. ZigBee can be designed for employing a star, tree, mesh topology with low complexity and energy value.

ZigBee devices are designed for low cost and data rates [4]. ZigBee provides low power wireless networking and supports up to thousands of devices in a network. ZigBee standard defines physical (PHY) layer, medium access control (MAC) layer, network (NWK) layer and application layer and it also defines the mechanism of security services. The PHY layer and MAC layer are defined by IEEE 802.15.4. ZigBee defines network and application layer also [7].

The PHY layer primarily accomplishes functions such as On/Off of the transmitter, energy detection (ED), link quality instruction, idle channel assessment, channel selection, and data sending/receiving.MAC layer is responsible for generating network beacons (by coordinators), synchronizing the beacons, connecting and disconnecting personal area network, providing access mechanism, and establishing reliable communications links between MAC peer entities. The NWK layer assigns addresses to the devices, does device discovery, as well as security application and services, which may enter and leave the network. It establishes and maintains routing lists. The application layer is divided into the application support sub-layer, the Application layer framework and the ZigBee device objects (ZDO).

The device types supported by IEEE 802.15.4 and ZigBee are Full Function Device (FFD) and Reduced Function Device (RFD). FFD can communicate with both FFD and RFD, and it can be the PAN Coordinator, Router, and End Device. RFD can only communicate with FFD, so it can be only End Device. A ZigBee network has three types of devices: two of them, the coordinator (C) and the router (R), are FFD and there is a RFD called end device (ED). The C is the only one that can form a ZigBee network and is unique within the network.

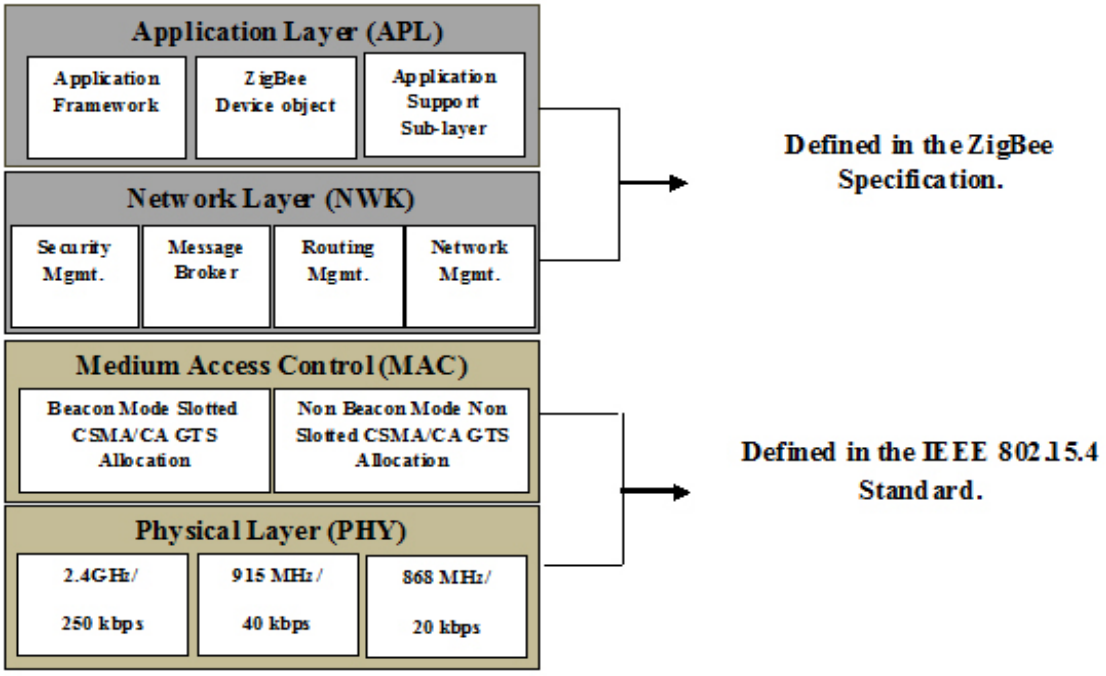


Figure 1: ZigBee protocol stack

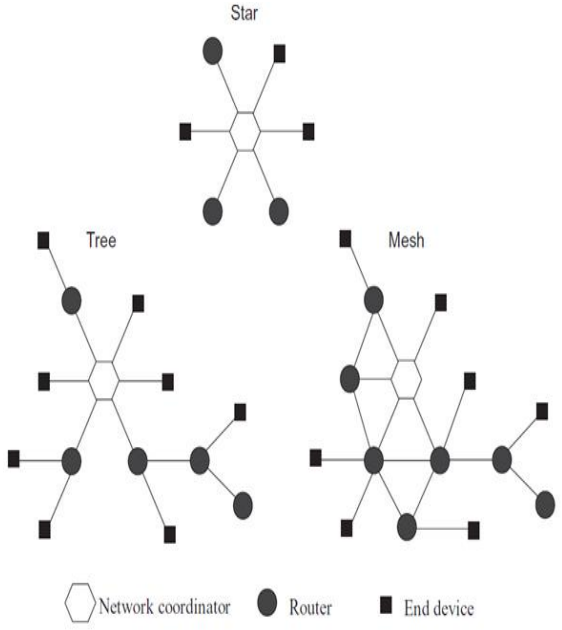


Fig 2: Topology Formation in ZigBee

The R has the same routing capabilities as the C, but can only join a network, never form it. A ZigBee end device, or ED, can only join the network and has no capacity for routing, it also should always be associated to a parent to be able to communicate and its most important characteristic is the capacity to shut down its radio during defined periods of time to save energy; while it is off its associated parent receives messages addressed to it and saves them so that they can be delivered when the ED radio is turned on and it requires data from its parent [8].

II. ROUTING PROTOCOLS

The nodes in the network perform the routing functions additionally to the inherent function of being the host. The limitation on wireless transmission range needs the routing in multiple hops. Therefore the nodes depend on each other for transmission of packets from source node to destination node via the routing nodes. The nature of the networks places two basic requirements on the routing protocols.

- It has to be distributed.
- The topology changes are frequent.

It should calculate multiple, loop-free routes whereas keeping the communication overheads to a minimum based on route discovery time. The Routing protocol specifies how routers in a network transfer information with each other and report changes. The Routing protocols enable a network to make dynamic adjustments to its network conditions, so routing decisions do not have to be predetermined and static. A routing protocol shares this information first among immediate neighbors, and then throughout the network. The different routing protocols are listed below:

- Pro-active routing protocols
- Reactive routing protocols
- Hybrid routing protocols

A. Proactive routing protocols -Table driven

This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables through the network. All the nodes of any protocol have to relay it is entire to its adjacent nodes. The entire nodes constantly update their position in order to send the data packet from one node to the opposite node when mutual agreement.

B. Reactive routing protocols – On –demand

This type of protocols finds a route like on demand by flooding the network with route request packet. Main disadvantage of these protocols,

- High latency time in route finding.
- Excessive flooding will cause network hamper.

C. Hybrid routing protocols - both proactive and reactive

This type of protocols combines the benefits of proactive and reactive routing. The routing is at the start established with some proactively prospected routes and so serves the demand from additionally nodes through reactive flooding. The selection for one or alternative method requires predetermination for typical cases.
The main disadvantages of such algorithms are,

- The amount of nodes activated.
- Reaction to traffic demand depends on inclination of traffic volume.

TABLE I
COMPARISON OF ROUTING PROTOCOLS

	Proactive routing protocols	**Reactive routing protocols**	**Hybrid routing protocols**
Definition	The proactive routing protocol periodically updates the topology info, therefore it, Continuously has associate up -to-date best routing path. The representative samples of proactive routing protocols are OLSR, WRP and DSDV. Proactive protocols are table-driven and can actively verify the layout	The reactive routing protocol invokes the route discovery procedure only if an application requests transmission of information. Thus, it doesn't generate the control packet overhead if there's no knowledge packet to transmit, whereas it causes long delay to search out a routing path. AODV, DSR, and	The hybrid routing protocols that use a combination of each proactive and reactive routing protocols. This hybrid protocol is used to find a balance between the proactive and reactive protocols. Samples of hybrid routing protocols embody Core Extraction Distributed ad hoc Routing Protocol (CEDAR), Zone Routing Protocol (ZRP), and Zone based hierarchical Link State Routing Protocol (ZHLS).

	of the network.	TORA are samples of the reactive routing protocol.	
Traffic	Less amount of traffic, If node mobility is low. However the quality of node is high, then routing info within the routing table invalidates terribly quickly. This additionally chooses an oversized amount of traffic overhead generated when evaluating these unneeded routes.	Reactive protocols are most suited for networks with high node mobility or wherever the nodes transmit information infrequently. Reactive routing protocols provide a great amount of traffic overhead.	Low node quality. This kind of protocols provides fewer amounts of traffic overhead and delay, more bandwidth efficient.
Time	Route selection time is smaller amount.	Route selection time is additional.	Route selection time is smaller but sometimes it may vary.

III. SECURITY SYSTEM OF ZIGBEE

By using of the wireless networks the question of their security become more important. In a wireless networks we need to deal with two challenges.

- Errors free information transmission and also the integrity check.
- To secure information against their capture and to avoid attacks against network.

Error free information transmission standard IEEE 802.15.4 uses Frame Check Sequence that is making verification for framework [7]. FCS is employed for data integrity, which can be corrupted due to noise. For the integrity check, ZigBee standard used MIC (Message Integrity Code) that ensures information authentication. For the purpose of data confidentiality the encryption standard AES (Advanced Encryption Standard) is employed. ZigBee standard supports the subsequent security mechanisms:

- Data encoding.
- Devices verification data verification.
- Protection against unauthorized frames.

ZigBee security mechanism has such functions as encryption, integrity checking and authentication, applying to MAC layer, Network layer or Application support sub-layer. It adopts AES-128 encryption for the confidentiality and a series of security mechanism derived from AES algorithmic rule for the integrity and legitimacy. The security mechanism provides security services for network connection deviceauthentication, information transmission, key establishment, key transport, device management [6].

A. Frame Check Sequence – FCS

The Standard IEEE 802.15.4 uses 16-bits FCS control field based on CRC (Cyclic Redundancy Check). It is a detection technique that is employed to detect potential errors in incoming packet.

B. Data confidentiality

The IEEE 802.15.4 standard supports the AES (Advanced encryption Standard) in order to keep up the information confidentiality. The AES algorithmic rule is 128-bit block cipher that supports three key lengths (128, 256, 512

bits) declared by NIST (National Institute of Standards and Technology), that is also employed by the ZigBee standard with key length of 128-bits.

C. Data authentication

Data integrity is achieved by authentication code messages MIC. Message authentication code could be a function that by a secret key produces an output fixed-length value that is the authenticator. The cryptanalytic checksum MIC could be a block of bits of constant length that is attached to the original message. If MIC provided by the transmitter is equal with MIC calculated by the receiver, the information is going to be considered as authentic. The level of information legitimacy is enhanced by increasing the amount of bits in the MIC. The ZigBee and IEEE 802.15.4 standards support 32-bit, 64-bit, and 128-bit MIC choice.

IV. ZIGBEE SECURITY ISSUES

A. Channel Defects

ZigBee uses 868 MHz, 915 MHz, 2.4 GHz ISM bands. But, most wireless LANs currently operate at 2.4 GHz ISM band, such as Bluetooth, wireless USB and Wi-Fi, which may affect the frequency band very noisy. This problem will make defects in channel.

B. Routing defects and network address assignment

In ZigBee network the addresses distributed to the nodes can be modified or even repeated in some cases. For example a node or a coordinator is removed or broken, or rejoined in, or a network is reconstructed. Thus it is tough to send the information to the right destination.

C. Communication key eavesdropping

The ZigBee security based on AES is a symmetrical encryption algorithmic rule. Each party shall negotiate the keys for encryption before communication. But during the negotiation illegitimate eavesdropping cannot be prevented, particularly in a new node connection. In this case, attackers will simply tap the keys during the key distribution.

D. No anti-denying

ZigBee has no identity authentication mechanism and no anti-denying capability. When attacks on the wireless sensor network are increasingly diverted and automated, ZigBee is subject to impersonation attack. Public key mechanism or digital signature can be adopted. Because node authentication reject the denying of message sent.

V. CONCLUSION

ZigBee standard has higher security, that offers functions like encryption, integrity checking and authority identification. In this work, we have mentioned the security system, security issues and also the basic routing protocols. But yet, ZigBee has security issues in the circles. In Future; to overcome these security issues, we are going to make some changes on routing methods, security system.

VI. ACKNOWLEDGEMENT

Dr.V. Venkatesakumar is presently working as Assistant Professor in The Department of Computer Science and Engineering, Anna University Regional Centre, Coimbatore. He received his Bachelor of Engineering Degree from Bharathiyar University, Master of Engineering Degree and Ph.D from Anna University Chennai. He has more than ten years of Teaching Experience. He has published many papers in reputed International Journals and has chaired many Conferences. He is a Life Member of International Association of Computer Science and Information Technology, International Association of Engineers and in many International Associations. His research interest includes Cloud Computing, Internet of Things, Big Data Analytics, Operating System, Software Engineering and Web Technologies.

Dhandapani.J is pursing M.E Computer Science and Engineering (Specialization with Networks) in the Department of Computer Science and Engineering, Anna University Regional Centre, Coimbatore. He received his Bachelor of Technology from The Rajaas Engineering College, Anna University, Tirunelveli. He has published paper in reputed International Journal. His research interests are Wireless networks, Network Security,

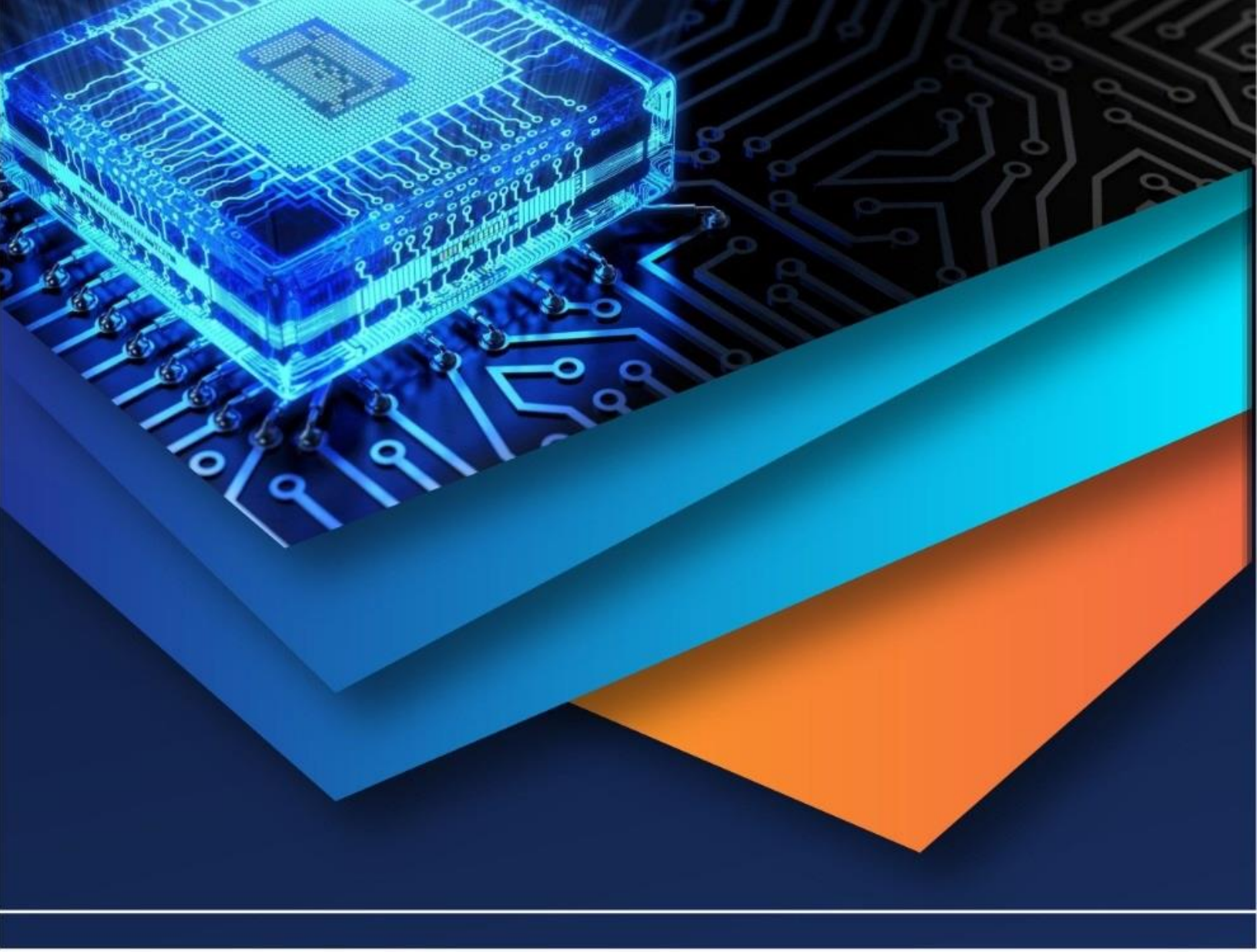
Security Protocols and Network Management, Web mining, and VANET

Vishnu k completed his Bachelor of Technology in Information Technology in 2012 from College of Engineering and Management, Punnapra, Kerala under Kerala University, Trivandrum. Currently, he is pursuing his Master of Engineering in Computer Science & Engineering from Anna University Regional Centre, Coimbatore. He has published paper in reputed International Journal. His research areas include (web mining, data mining, cloud computing and wireless networks).

Arifkhan.S completed his B.E in Computer Science And Engineering in 2013 from College Of Bannari Amman Institute Of Technology In Sathyamangalam. Currently, He is pursuing his M.E Computer Science and Engineering from Anna University Regional Centre, Coimbatore. His research areas include Cloud Computing and Wireless Networks.

REFERENCES

[1] ZigBee Alliance, ZigBee Specifications www.ZigBee.org.
[2] Taehong Kim, Seong Hoon Kim, Jinyoung Yang, Seong-eun Yoo, and Daeyoung Kim, "Neighbor Table Based Shortcut Tree Routing in ZigBee Wireless Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 3 MARCH 2014.
[3] J. Peerenboom and R. Fisher, "Analyzing Cross-Sector Interdependencies", IEEE Computer Society, HICSS, IEEE Computer Society, pp. 112–119, 2007.
[4] IEEE 802.15.4: Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), ISBN 0-7381-4996-9, IEEE Computer Society, 2006.
[5] Atefeh Khatiri, Ghasem Mirjalily, Ahmad Khademzadeh, "Energy-Efficient Shortcut Tree Routing in ZigBee Networks", Fourth International Conference on Computational Intelligence, Communication Systems and Networks, 2012.
[6] C. Alcaraz 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, vol. 40, Issue 4, pp. 419-428. ISSN 1094-6977, July 2010.
[7] Ing. Jan Durech, prof. Ing. Maria Franekova, "Security attacks to ZigBee technology and their practical realization", IEEE 12th International Symposium on Applied Machine Intelligence and Informatics, January 23-25, 2014.
[8] E. Dalila Pinedo-Frausto, J. Antonio Garcia-Macias," An Experimental analysis of Zigbee Networks", Computer Science Dept, CICESE Research Center.
[9] Bin Yang, "Study on Security of Wireless Sensor Network Based on ZigBee Standard", International Conference on Computational Intelligence and Security, 2009.
[10] T. Malm, J. Herard, J. Boegh, M. Kivipuro, Validation of safety related wireless machine control systems. NT Technical report TR 605, Oslo, Norway, ISSN 0283-7234, 2007.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY