ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

# Performance Analysis of Non-Beacon Enabled IEEE 802.15.4 based Secured Wireless Sensor Network

**Surender.R[1], S. Srinivasan [2]**

Assistant professor, Department of Electronics and Communication Engineering, Christ College of Engineering & Technology , Pondicherry, India[1]

Assistant professor, Department of Electronics and Communication Engineering, Christ College of Engineering & Technology, Pondicherry, India[2]

**Abstract**: Zigbee an IEEE 802.15.4 standard for low power and Low Rate Wireless Personal Area Networks (LRWPANs) are evolving as a promising technology to bring envisioned ubiquitous paragon, into realization. It is moulded on the physical layer and medium access control defined in IEEE 802.15.4. Since it's a low power device, throughput enhancement is a challenging task in non-beacon enabled Zigbee network. Further, Zigbee interacts with sensitive data and operates in hostile unattended backgrounds. It is imperative that security concern can be addressed from the deployment of the system. To enhance throughput in the secured network, a home-node with Internet Protocol Security (IPsec) is deployed which is implicated in this paper. Performances metrics like throughput and delay are determined, analysed and compared with the prevailing network. The simulation model of IEEE 802.15.4 based wireless sensor network is modelled using OPNET.

**Keywords**: Home-node, IEEE 802.15.4, IPsec, OPNET, Zigbee

## I. INTRODUCTION

IEEE 802.15.4 based wireless sensor networks has gained significant attention among researchers in recent years. Zigbee wireless technology has been widely used in industry due to the advantage of low power consumption and low cost. The IEEE 802.15.4 protocol is adopted as a communication standard for Low-Rate Wireless Local Personal Area Networks (LR-WPANs). Zigbee aimed at remote control and sensor applications. It is suitable for operation in ruthless radio environments and in isolated locations. It is built on IEEE 802.15.4 standard which defines the physical and MAC layers [1]. The MAC layer of the IEEE 802.15.4 standards can operate in either beacon enabled or non-beacon enabled mode.

The beacon enabled mode involves periodic transmission of beacon messages for network synchronization and association [2]. This synchronization allows the beacon enabled mode to operate on slotted Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism. On other hand, nodes are not synchronized in non-beacon enabled mode. This is due to absence of periodic beacon transmissions. Therefore, in this mode unslotted CSMA/CA mechanism facilitates the decentralised communication among the nodes [3].
Apart from the absence of periodic beacons and its consequences (e.g., absence of network-wide synchronization and superframe structure), major difference between slotted and unslotted CSMA/CA mechanisms is their nature of time evolution. Zigbee supports different network topologies. They are mesh network topology, a star topology, cluster tree or hybrid architecture. The cluster tree topology is basically a grouping of star and mesh network.

The device employed in this purpose has maximum operating frequency at 2.4 GHz with data rate of 250 Kbps [4]. Several studies have investigated the performance analysis in non-beacon enabled Zigbee WSNs [5]. Mu-Sheng et al. [6] performed a comprehensive performance evaluation of Zigbee wireless networks in beacon enabled and non-beacon enabled modes. Their results illustrated that utility of either beacon enabled or non-beacon enabled mode is dependent on specific application.

T.H.Woon and T.C. Wan [7] has implemented IEEE 802.15.4 standard by providing a comprehensive performance analysis of small scale peer-to-peer networks. Zigbee is very vulnerable to multiple kinds of security attacks. The wireless nature limits the amount of energy processing; storage resources and absence of any physical protection render [8]. Matthias Wilhelm et al made an attempt to Secure Key Generation in Sensor Networks [9]. However security in nonbeacon enabled network is limited.

Hence an attempt has been made to analyse the performance such as throughput and delay of nonbeacon enabled IEEE 802.15.4 based secured WSN using IPsec which is discussed in this paper. The rest of the paper is structured as follows: Section 2 presents the prevailing network of IEEE 802.15.4 standard.

Section 3 deals with an overview of modification and enhancement done in the prevailing network. Simulated results are discussed in Section 4. Conclusion and future work are drawn in Section 5.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 3, Issue 3, March 2014*

## II. OVERVIEW OF IEEE 802.15.4 ARCHITETURE

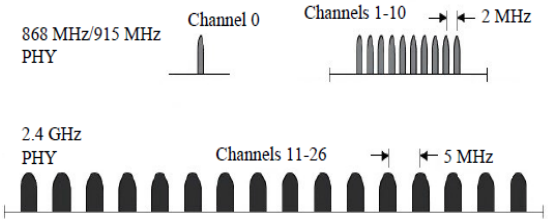


Fig 1 illustrates different frequency bands of Zigbee

ZigBee is a specification for a high level communication protocols. It creates personal area networks built from small, low-power digital radios. The new IEEE 802.15.4 standard defines the Physical layer (PHY) and Medium Access Control sub-layer (MAC) specifications for low data rate wireless connectivity among relatively simple devices. It consumes minimal power and typically operates in the Personal Operating Space (POS) of 10 meters or less. The main features of IEEE 802.15.4 standard are low reliable data rates, low power consumption, and low cost. MAC layer of IEEE 802.15.4 specifies two types of channel access mechanism: beacon enabled and non-beacon enabled [10]. Un slotted Carrier-Sense Multiple Access with Collision Avoidance (CSMA-CA) is used by non-beacon enabled mode as the MAC protocol. MAC protocol of beacon enabled networks use a slotted CSMA-CA with a super frame structure that is managed by the Personal Area Network (PAN) coordinator.

The MAC layer defines two types of nodes. They are Reduced Function Devices (RFDs) and Full Function Devices (FFDs). FFDs can operate in three different modes namely a PAN coordinator, router, or a device. FFDs can communicate to other FFDs or RFDs, while an RFD can only communicate to FFD. When acting as a network coordinator, FFDs send beacons that provide communication, synchronization and network connection services to other nodes. RFD's can act as an end-device and is used for simple applications. IEEE 802.15.4 generally operates in one of the three network topologies: star, peer-to-peer (mesh), and cluster tree. These topologies are described in detail by B.E. Bilgin and V.C. Gungor in [11].

FFD is chosen to as the PAN coordinator in star topology. It uses a master-slave network model. All other devices in the network can only directly communicate with it. This is different from a peer-to-peer topology. Each device communicates with other devices in the network, as long as they are in radio range with one another. Cluster tree networks are considered as a special case of mesh networks in which the majority of nodes are FFDs and RFDs can connect to the network as leaf nodes. In addition, RFDs can only communicate with FFDs. The advantage of non-beacon enabled mode is that it allows for easy scalability and self-organization of sensor networks. In addition, a nodes' receiver does not have to frequently power up to receive a beacon. However, delivery of data is not guaranteed in non-beacon enabled mode frames within a specified time delay.

## III. PROPOSED WORK

Zigbee comprises of three types of device: Co-ordinator, Router and end device. Coordinator forms the base of network tree and bridge to other networks. There is one ZigBee Coordinator in each network since it is a device that initiates the network. It stores information about the networks, including trust centre and repository for security keys. Router can act as an intermediate and it will update the nodes in the network. It passes on data from one device to other devices. The work of end device is to communicate with PAN coordinator node. It cannot retrieve data from other devices. This configuration allows the node to be in sleep mode and thereby giving long battery life. A Zigbee device requires least amount of memory and it is less expensive to fabricate a Zigbee device [12].

The proposed work differs from prevailing works by the way of deploying a home-node in the non-beacon enabled network. Deploying a node in the network is a phenomenal task which upturns delay in the network. Fig. 2 shows the deployment of home- node with IPsec in zigbee network. The function of home node is to regulate routing in the network and IPsec provides end to end security. The home node role is to route all the traffic in the network accurately so that it can enhance the throughput. The function of IPsec is to route all the traffic from the end device in a secure manner. It uses IPsec to route and forwards to the co-coordinator or vice versa. IPsec is a protocol suite for secured internet protocol for authentication and encrypts each IP packet of a communication session. Fig 3 shows the architecture of IPsec. IPsec protocol incorporates Authentication Header (AH) and Encapsulating Security Payload (ESP). It provides data confidentiality, origin authentication, integrity, and anti-replay protection for ESP payload. ESP protocol can be used alone or with AH protocol, or tunnel mode of IPsec. It is an end-to-end security scheme operating in Internet Layer of Internet Protocol Suite.

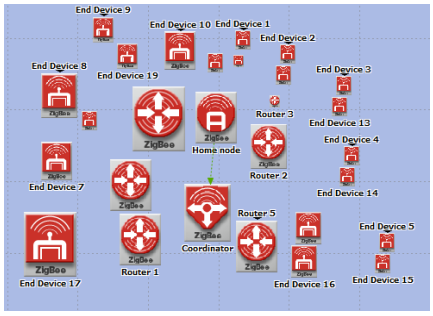


Fig 2 Deployment of home-node in zigbee network

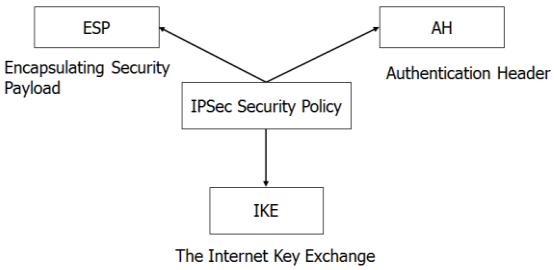


Fig 3 Architecture of IPsec

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

It can be used in defensive with data flows between a pair of hosts, between a pair of security gateways or between a security gateway and a host. AH can be used in combination with ESP protocol, or in tunnel mode of IPsec. IPsec tunnel mode protects site-to-site traffic between networks and site-to-site networking through Internet. The green arrow shown in Fig 2 indicates the flow of traffic from home-node to co-ordinator and vice versa. These two functions complement each other which makes non-beacon enabled network into an effective network for communication.

## IV. SIMULATION RESULTS

The objective of this paper is to analyse the performance of non-beacon enabled IEEE 802.15.4 based secured wireless sensor network. The scenario considers 500x500m$^2$ as coverage area with 100 and 300 nodes to evaluate the performance of network with home-node IPsec. It is then compared with that of existing scenario. OPNET attributes are outlined in table1.

TABLE 1
OPNET ATTRIBUTES FOR SIMULATON

| **Parameters** | **Values** |
|---|---|
| Zigbee band | 2.4GHz |
| Data rate | 240Kbps |
| Modulation | O-QPSK |
| Protocol | AODV |
| Coverage area | 500x500 m$^2$ |
| No. of nodes | 100,300 |
| MAC layer | CSMA/CA |
| Topology | Cluster Tree |
| Network | Non-Beacon enabled |

### *A. Throughput Analysis*

The simulation result shown in fig 4 compares average throughput between 100nodes and 300nodes for network with 500x500 m$^2$ scenario. The throughput for the scenario without home-node IPsec is found to be 49 kbps for 100nodes and 88Kbps for 300nodes.After deploying home node IPsec, throughput of the scenario is found to be 63 kbps for 100nodes and 90Kbps for 300nodes. Further, the value of throughput is increased due to increase in number of nodes. It is also inferred from fig 4 that network deployed with home- node IPsec enhances throughput of the network than that of the network without home node IPsec.

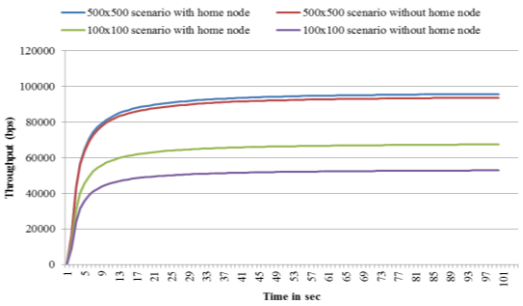


Fig 4 Comparison of average throughput of scenario with 500x500 m$^2$ for 100nodes and 300 nodes

### *B. Average MAC delay Analysis*

Simulation result shown in fig 5 depicts the comparison of average delay between 100nodes and 300nodes for 500x500 m$^2$ scenario. The MAC delay of prevailing network scenario is 10ms for 100nodes and 14ms for 300nodes. The MAC delay of the proposed network is increased to 13ms for 100nodes and 17ms for 300 nodes. The increase in delay is due to more time duration taken by the network to access the channel. Table 2 shows the comparison of different attribute with and without deploying home-node with IPsec.

### *C. Average end to end Analysis*

The simulation result shown in fig 6 portrays the comparison of average end to end delay between 100nodes and 300nodes for coverage area of 500x500 m$^2$ network. For scenario without home- node IPsec, end to end delay is found to be 29ms for 100nodes and 49ms for 300nodes. After deploying home-node IPsec in the network, end to end delay was found to be 49ms for 100nodes and 68ms for 300nodes. The function of IPsec is to provide security in the network which in turn increases the end to end delay in the network.

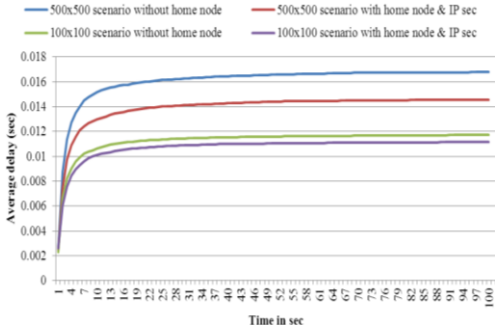


Fig 5 Comparison of MAC delay of scenario with500x500 m$^2$ for 100 nodes and 300 nodes

TABLE 2 COMPARISON OF DIFFERENT ATTRIBUTES

| **Coverage range of network (m$^2$)** | **No. of nodes in network** | **Average Throughput (kbps)** | | **Average MAC delay(ms)** | | **Average end to end delay (ms)** | |
|---|---|---|---|---|---|---|---|
| | | ***No home-node*** | ***With home-node &IPsec*** | ***No home-node*** | ***With home-node& IPsec*** | ***No home-node*** | ***With home-node &IPsec*** |
| 500x500 | 100 | 49 | 63 | 10 | 13 | 29 | 35 |
| | 300 | 88 | 90 | 14 | 17 | 49 | 68 |

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 3, Issue 3, March 2014*

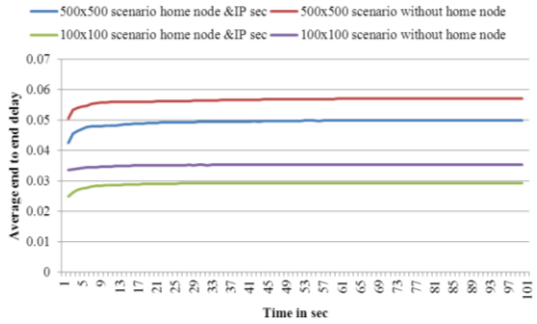


Fig 6 Comparison of average end to end delay of scenario with 500x500 $m^2$ for 100nodes and 300 nodes

## V. CONCLUSIONS

In this paper, performance analysis of non- beacon enabled IEEE 802.15.4 based secured wireless sensor network. It has been investigated using OPNET and performance parameters are examined. The work is modelled on non-beacon enabled networks and simulations are performed for realistic node densities and simulation times. The simulation results shows that home-node with IPsec outperforms prevailing network in terms of throughput. Future work focus on evaluation of performance metrics based on different routing and security algorithms. Mobility management can also made for further up gradation in the performance of network.

## REFERENCES

[1] Alaparthi Narmada, Parvataneni Sudhakara Rao "Zigbee Based WSN with IP Connectivity", Proceeding of Fourth International Conference on Computational Intelligence, Modelling and Simulation, Kuantan, Malaysia, pp 178 - 181, September 2012.

[2] Yanjun Zhang, Siye Wang, Zhenyu Liu, Wenbiao Zhou, Dake Liu " Performance Analysis of Wireless Sensor Network Based on NS-2," Proceeding of International Conference on Systems and Informatics, Yantai , China, pp 1445 – 1448, May 2012.

[3] M. Gribaudo, D. Manini, A. Nordio, and C. Chiasserini, "Transient Analysis of IEEE 802.15.4 Sensor Networks", IEEE Transactions on Wireless Communications, Volume 10, Issue 4, pp. 1165 –1175, April 2011.

[4] S. Mohanty, S.K. Patra. "Quality of service analysis in IEEE 802.15.4 mesh networks using MANET routing," Proceeding of International Conference on Computing Communication and Networking Technologies, Karur ,Tamil Nadu, pp. 1-7, July 2010.

[5] F. Wang, D. Li, and Y. Zhao, "Analysis of CSMA/CA in IEEE 802.15.4," Institution of Engineering and Technology for Communications,Volume 5, Issue 15, pp. 2187 –2195, October 2011.

[6] L. Mu-Sheng, L. Jenq-Shiou, Y. Wen-Chi, Y. Min-Chieh, J.-L.C. Wu, "On transmission efficiency of the multimedia service over IEEE 802.15.4 wireless sensor networks," Proceeding of 13th International conference on Advanced Communication Technology, Seoul ,South Korea, pp 184-189, February 2011.

[7] T.H.Woon and T.C. Wan ," Performance Evaluation of IEEE 802.15.4 Ad Hoc Wireless Sensor Networks: Simulation Approach," Proceeding of IEEE Conference on systems, Man, and Cybernetics Taipei, Taiwan, pp 1443 – 1448, October,2006

[8] V. Kumar, S. Tiwari. "Performance of routing protocols for beacon-enabled IEEE 802.15.4 WSNs with different duty cycle." Proceeding of International Conference on Devices and Communications, Mesra, Jharkhand, pp. 1-5, February 2011.

[9] Wilhelm, M. ; Martinovic, I. ; and Schmitt, J.B.,"Secure Key Generation in Sensor Networks Based on Frequency-Selective Channels" IEEE Journal on Selected Areas in Communications, Vol.31, Issue 9, pp. 1779 – 1790, September 2013.

[10] Pollin, S.; Ergen, M.; Ergen, S.C.; Bougard, B.; Catthoor, F.; Bahai, A.;Varaiya, P.; "Performance Analysis of Slotted Carrier Sense IEEE 802.15.4 Acknowledged Uplink Transmissions",. IEEE Conference on Wireless Communications and Networking, Las Vegas, Nevada, pp: 1559 – 1564, April 2008.

[11] B. Lauwens, B. Scheers, and A. Vande Capelle, "Performance analysis of unslotted CSMA/CA in wireless networks", Springer Telecommunication Systems, Volume 44, Issue 1-2, pp. 109–123, June 2010.

## BIOGRAPHIES

**R. Surender** received his B.Tech Degree from Rajiv Gandhi College of Engineering and Technology affiliated to Pondicherry University, Pondicherry in 2006. He has obtained his M.Tech. Degree from Pondicherry Engineering College affiliated to Pondicherry University, Pondicherry in 2008. He is currently working as Assistant Professor in Department of Electronics and Communication Engineering, Christ college of Engineering & Technology, Pondicherry, India. His areas of interests include Wireless communication, Sensor networks and Computer communication.

**S.Srinivasan** received the B.Tech. Degree in Department of Electronics and Communication Engineering (2007) and M.Tech. Degree (2011) in Department of Electronics and Electrical Engineering from Mailam Engineering College affiliated to Anna University. He is currently working as Assistant Professor in Department of Electronics and Communication Engineering, Christ college of Engineering & Technology, Pondicherry, India. His areas of interests include Wireless communication, Image Processing and Embedded System.