Review on address assignment mechanism in ZigBee wireless sensor networks

Nikunj saholia
Pg student, Computer Engineering department
Marwadi education foundation's group of institutions

Shraddha joshi
Asst. Prof., Computer Engineering Department,
Marwadi education foundation's group of institutions

Abstract

Addressing plays an important role in networking. Addresses are used as unique identifiers to identify sensors during data delivery. Some addressing assignment techniques for ZigBee wireless sensor network are described in this paper. Addressing mechanisms are the techniques for assigning the address to nodes in the network. Wireless sensor network consists of different sensing nodes, when they are added to the network; they are given a unique address for identification. Small wireless sensor networks should be assigned such addressing mechanisms which can achieve good performance. SAAM, DAAM, Long thin wireless sensor network addressing scheme and distribute address assignment scheme are discussed in this paper. All these mechanisms have their properties, limitations and advantages. For assigning the address to any node in the wireless sensor network includes different mechanisms and these addressing mechanisms can be compared in terms of their performance to evaluate which addressing mechanism is most suitable for the different wireless sensor network. All these addressing mechanisms have difference in their performance.

Keywords- ZigBee, SAAM, DAAM, Long Thin WSN, Distributed addressing, Wireless Sensor Network.

1. Introduction

A Wireless Sensor Network (WSN) consists of spatially
distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. Addressing plays vital role in traditional IP based networks. an IP address is globally unique and is assigned to each node. IP addresses should be unique so that node can be identified uniquely.. In wireless sensor networks (WSNs), each sensor in the network is given an address for unique identification. Addressing schemes proposed for sensor networks can be categorized as 'Stateful' and 'stateless'. [1] Stateful approach makes use of an address allocation table. 'Stateless' approach does not use allocation tables. When new node enters in the network then it will be assigned with some address therefore it can be identified uniquely in the network. Some addressing mechanisms don't assign the address uniquely while some mechanisms do not guarantees the maximum utilization of available addresses.

Type of wireless sensor network depends upon the application. When low cost small area network is required, ZigBee wireless sensor network [2] can be used. ZigBee is an IEEE 802.15.4 wireless communication standard. It is used to build low power consumption and low cost network. It is also called a representative protocol for wireless sensor network. IEEE 802.15.4 defines lower layers of protocol stack which are MAC and PHY. IEEE 802.15.4 standard gives the advantage of a powerful physical radio. It also consist logical network, security and application software in its architecture. ZigBee can be implemented in star networks, peer-to-peer networks, mesh networks and cluster-tree networks. ZigBee services include personal health care, telecom services, pc and peripherals, lighting control, access control and so many more. ZigBee/IEEE 802.15.4 wireless sensor network presents different addressing mechanisms. In this paper we have describe four different addressing schemes which are: Stochastic Address Assignment Mechanism (SAAM), Distributed Address Assignment Mechanism (DAAM) [3], Long Thin Wireless Network [4] address assignment scheme and Distributed Borrowing Addressing Scheme.

The remainder of this paper is organized as follows. Section II describes the introduction of ZigBee wireless standard. Section III describes the addressing mechanisms SAAM, DAAM, long thin wireless network and distributed borrowing addressing scheme. Finally, section IV is a conclusion summarizing the study.

2. The overview of ZigBee network layer

The ZigBee IEEE 802.15.4 covers the physical layer and the MAC layer of low-rate WPAN. IEEE Standard 802.15.4 defines the physical layer and medium access control sub layer specifications. It has low-data-rate wireless connectivity. It supports fixed, portable and moving devices. ZigBee used where very limited battery consumption is required. The IEEE 802.15.4 standard defines the device types that can be used in a LR-WPAN which are Full Functional Device (FFD) and Reduced Functional Device (RFD). [5] Three different types of data transfer exist in ZigBee network. Data transfer from a device to the PAN coordinator, data transfer from the PAN, Peer-to-peer data transfer. Figure 1 shows the ZigBee stack with its layers.

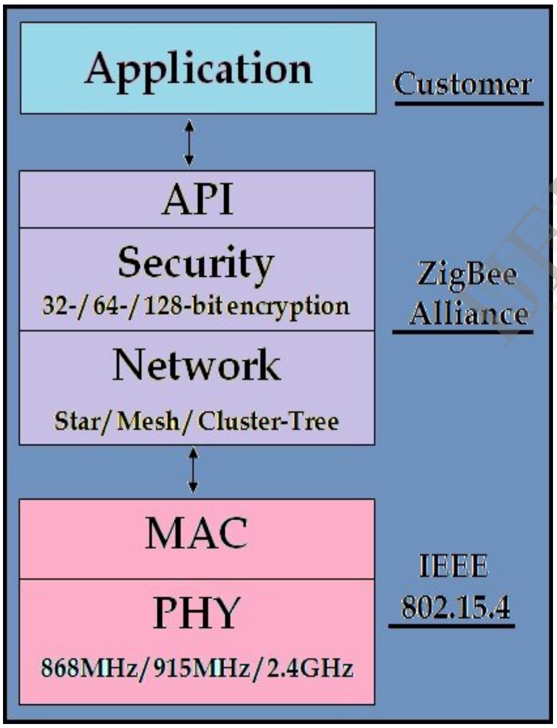


Fig 1 ZigBee stack

a. Devices in the network layer

ZigBee coordinator (ZC): Responsibility of ZC is to take care of initializing, maintaining, and controlling the network.

ZigBee router (ZR): ZigBee router belongs to the network backbone which is useful for routing a node.

ZigBee end device (ZED): ZED is used in a tree network. The coordinator and routers can announce beacons in the network.

ZC, ZR and ZED are very essential devices in ZigBee wireless sensor network. Each of them handles their assigned task to synchronize the operation in network. Lm, Cm and Rm are topological parameters for a ZigBee Tree. Lm is the maximum depth value of the tree. In the figure.1, the maximum depth of the tree is 3 which is Lm. Cm is the maximum number of children of a ZC/ZR. Rm is the maximum number of children of a ZC/ZR that can be route. The head node is considered as ZC. The nodes at the Lm are always ZEDs, which can be shown in the below figure 2.

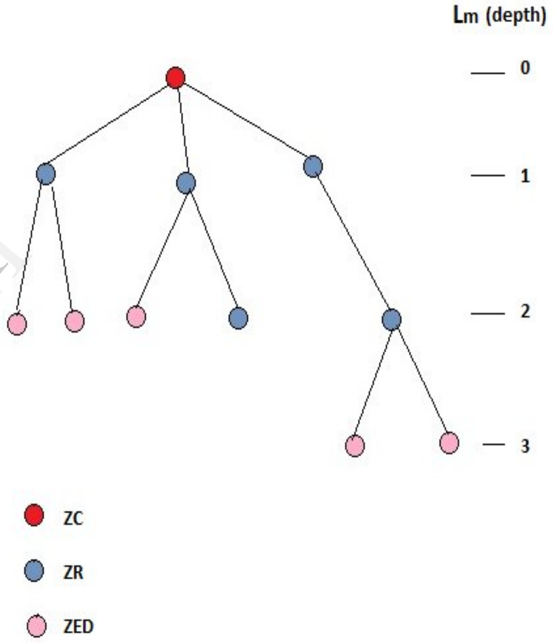


Fig 2. ZigBee tree structure

b. *Security in ZigBee 802.15.*

The algorithm that is used for encryption in ZigBee network is the Advance Encryption Standard. It provides a security baseline including the ability to maintain an ACL and use symmetric cryptography for data encryption. The higher level layers decide when security is needed and the upper layers are responsible for device authentication and key management. The security mechanism covers the network and the application layer. End-to-end security is also supported in ZigBee where the source and destination devices have access and use the same share key.

Contribution and assumptions

It's not possible to build a global addressing scheme for the deployment of large number of sensor nodes. Classical IP based protocols are useless for the wireless sensor networks. However, there are so many addressing mechanisms derived for wireless sensor networks. ZigBee is IEEE 802.15.4 wireless communication standard when low power and low cost is required. There are different addressing mechanisms proposed for ZigBee standard. Our assumption is to incorporate any one clustering algorithm of wireless sensor network with the addressing mechanism proposed in ZigBee standard. Performance of the sensor network will be evaluated in two cases, with implementing ZigBee addressing mechanism in our clustered wireless sensor network and without using it.

3. Addressing mechanisms

a. *Stochastic Address Assignment Mechanism (SAAM)*

Stochastic Address Assignment Mechanism (SAAM) Proposed in ZigBee in 2007. It checks whether or not addresses are duplicate after assigning random addresses to the nodes. On-demand [6]-[7] protocol or table-driven protocol [8] is used for routing when packets are transmitted in the network, at the time of transmission addresses are assigned in random order. Addressing is not hierarchical in the network. Address conflicts occur when two or more devices select an identical network address. Some device may conflict therefore they need to rejoin the network. Thus, conflicting devices will get a new address. Tree-based routing is no longer feasible with SAAM. These routing protocols are inappropriate for low power and low capacity wireless sensor networks because they require frequent broadcasts and large packet header size. It also demands high memory.

- *Address assignment mechanism in SAAM*

The AODV routing protocol is used in the SAAM. It routes packets in the sensor network. the address conflict resolution may occur and therefore it takes more time to establish the network. Power capacity is also limited in sensor network. Thus, speed of the network is less than wired network commonly used with AODV. SAAM and AODV routing are not efficient ideas for sensor networks.

b. *Distributed Address Assignment Mechanism (DAAM)*

DAAM organizes all the nodes in tree networks and routes packets using address information without requests for extra routing tables. It also doesn't need route retrieval processes and still it guarantees the uniqueness of addresses with a regular address assignment technique.

The aim of DAAM is to make a self-organizing [9] wireless sensor network. it is difficult to expand the network area in a scalable manner using DAAM. When any node wants to enter in the network then newly entering node N requests address assignment to parent node P. parent node P can assign the address to the newly entering node N by the equation 1.1. In centralized methods all nodes are managed by central node. Linear addressing assignment requires an additional table for routing. It also needs messages for route setup and an additional header format. It fails to maintain the advantage of DAAM and centralized addressing also takes too much delay before address assignment because they have to communicate with central node. The delay may cause timeout of the association process and address assignment may be fail. The addressing mechanism should be such that it achieves a higher address assignment success rate and it also guarantees the uniqueness of addresses. Therefore different addressing assignment mechanisms should be tested for comparison and use them according to respective application.

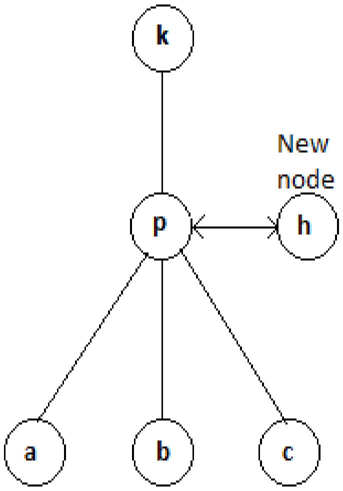


Fig 3. Address configuration in DAAM

- *Working of DAAM*

In DAAM, a parent node utilizes Cm, Rm, and Lm to compute a Cskip function. Cskip is used to compute the size of its children's address pools. Maximum tree depth is denoted by L_m, the maximum number of children is C_m and the maximum numbers of children that can be route are R_m.

$$Cskip = \{ 1 + C_m * (L_m - d - 1) \} \qquad if\ R_m = 1 \ldots (a)$$

$$= \{ 1 + C_m – R_m – C_m *[R_m \wedge(L_m - d - 1]) / 1 – R_m \} \qquad Otherwise \ldots (b)$$

Equation 1.1

Cskip(d) is the depth value of parent. Suppose parent node at depth d has an address: Ap. nth child router is assigned to an address: Ap + (n-1) × Cskip(d) + 1
And nth child end device is assigned to an address:
Ap + Rm × Cskip(d) + n

- *Properties of DAAM*

Locations in the same sub tree are allocated a continuous address block. It uses hierarchical addressing and the addresses of each device are assigned by its parent. Here it reserves an address for each possible location in the tree. Routing is done without using a routing table.

- *Weakness of DAAM*

It fails in providing flexibility. The highest address can be used in this mechanism is: Cskip(0)* R_m + C_m – R_m. Addresses higher than this cannot be used.

Depending on the network size and network structure, both SAAM and DAAM addressing schemes have their advantages and disadvantages. Especially the network structure can be analyzed by the addressing scheme, since the network depth can be limited.

C. Long Thin WSN addressing scheme

Wireless sensor network applications differ in many areas and Long-Thin Network is used in many applications. Long-Thin Network is one the topologies. Some of the applications of LTN are in surveillance, leakage detection, flood protection, vibration detection, monitoring tunnels, street lights monitoring, pedestrian detection and so many other. ZigBee propose a new addressing mechanism which is easy to use in long thin wireless sensor network. Goal of this addressing scheme is to automatically form a long thin WSN, give addresses to nodes and conduct routing process. Proposed long linear network topology is called Long Thin Wireless Sensor Network (LT-WSN) which is based on ZigBee. All nodes in LT-WSN are divided into clusters. Each cluster contains one head and a bridge. All other nodes are in-between head and bridge of the cluster.

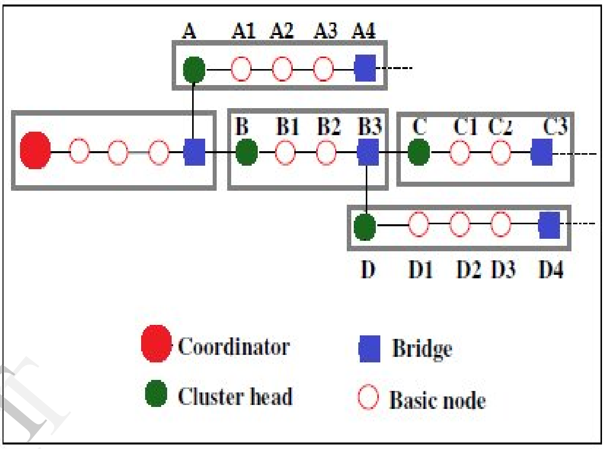


Fig 4. Long thin wireless sensor network

In the given figure 4, long thin wireless sensor network structure contains different clusters; the first node of the first cluster is coordinator. Last node of every cluster is bridge which connects with another cluster's head. If the bridge fails, the network will be down. The nodes in between the head node and bridge are general nodes. Manual intervention is also necessary to elect a new cluster head or bridge because these nodes are defined manually by the network administrator at the startup of the network.

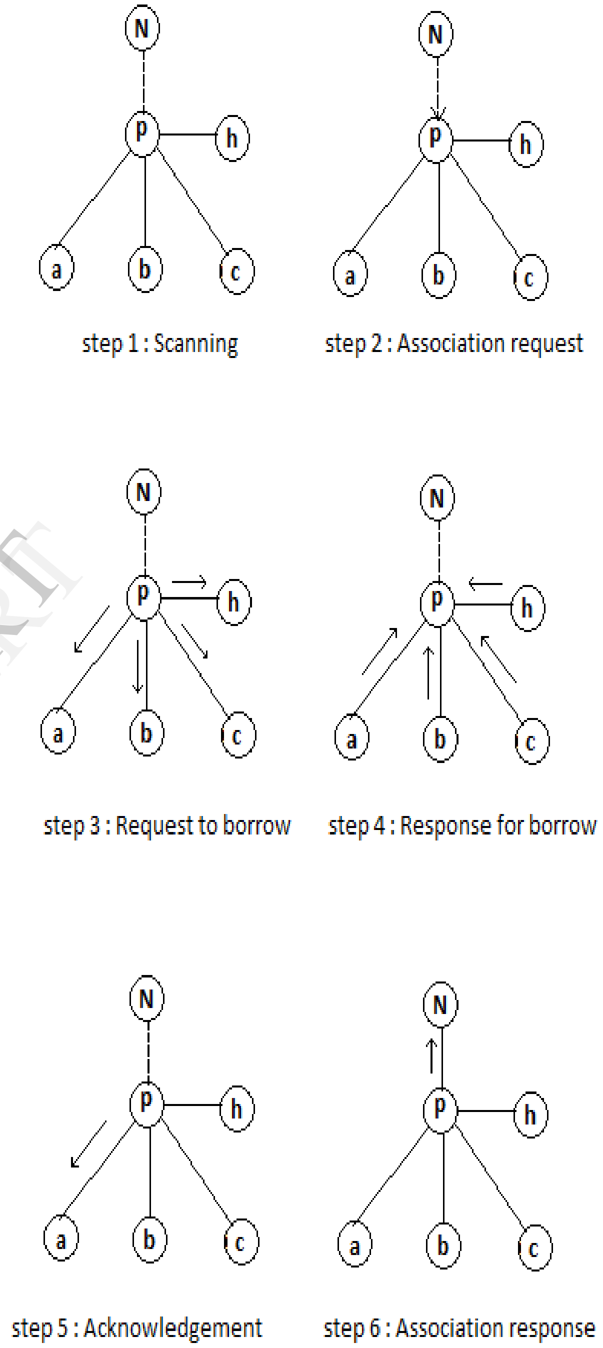
D. Distributed Borrowing Addressing Scheme

Distributed borrowing addressing scheme is the advance mechanism than SAAM and DAAM. It preserves the advantage of DAAM and also provides scalability in it. The working of distributed addressing mechanism is explained in this context. If a new node enters in a ZigBee network then it should find candidate nodes for its parent. Distributed borrowing addressing scheme can be explained in figure 5. If the new node enters in a network and if it is in the radio coverage of parent node p, new node can be assign address by its parent by analyzing the unoccupied child addresses available. Routers take care of the beacon frames to be broadcast. These beacon frames consists the number of children that they can add which are the number of remaining addresses which can be assigned. And these addresses are called as available address count. When available addresses remaining, parent node will assign if it gets association request by any node. If the available address count is zero or the tree depth is Lm or more then the new node gets the address by "address borrowing" scheme.

- If parent node p receives an association request from newly entering node N and if parent node has a limit of 3 children, an address for node N cannot be assigned because node p already has nodes a, b, and c as children therefore node p should broadcast an address borrowing request (AB_REQ) messages to borrow addresses from its parent node and children which are called neighbor nodes. The neighbor nodes h, a, b, and c respond to node p with address borrowing response (AB_RSP). This message includes Available Address and Available Address Count. If AAC is zero then AB_RSP message will not be transmitted.

- The selection procedure for borrowing address is done by following steps. First of all an AA of the node with the biggest AAC is selected and if the AACs are identical then an AA of the neighbor node with the highest address will be selected. This is a method of borrowing unused addresses from neighbor nodes and adopting them. This mechanism solves the problem that addresses cannot be assigned to nodes newly entering a network due to tree depth and limits on the number of children in the case of DAAM. Different simulation tools can be used for simulation. Uniform node placement and random node placement can be performed by the tool.

- The working of distributed borrowing addressing mechanism is explained in the above context. According to the IEEE 802.15.4 standard, a device sends the data request command for the association response message to the coordinator macResponseWaitTime symbols after the acknowledgment of an association request command. The maximum value of macResponseWaitTime symbol is 64× BaseSuperframeDuration, which is 983 ms at the 2.45 GHz band. Time taken to exchange AB_REQ and AB_RSP messages is the delay between an association request command and an association response command. MacAckWaitDuration is the maximum number of symbols to wait for an acknowledgment frame to a transmitted data frame. The data rate of the IEEE 802.15.4 standard is 250 kbps at the 2.45 GHz.



step 1 : Scanning

step 2 : Association request

step 3 : Request to borrow

step 4 : Response for borrow

step 5 : Acknowledgement

step 6 : Association response

Fig 5. Working mechanism of DIBA

4. Comparison

Addressing mechanisms differ from each other by different parameters. What entity is used to construct address, addressing bits, address space size, time required to construct address, wastage of address space and complexity are some addressing parameters. Comparison between some parameters of addressing mechanisms is tabulated in table 1.

TABLE I
Comparison of addressing mechanism parameters

	Addressing Parameter	Wastage of address
SAAM	No. of nodes: k	Medium
DAAM	Cm , Rm , Lm	High
LTWSN	No. of cluster	Medium
DIBA	Cm, Rm, Lm	Low

5. Conclusion

The performance of DIBA can be evaluated by demonstrating the effects of varying the tree depth limit and the node density in the network. Improvement rate of DIBA can be compared with SAAM and DAAM. By using distributed borrowing addressing mechanism, address assignment rates are higher than other addressing schemes. Network coverage will also be more in this mechanism as compared to SAAM, DAAM and long thin WSN. By using some routing algorithms, semi-scalable network can be achieved which are also suitable for ZigBee IEEE 802.15.4 wireless sensor networks.

6. References

[1] K. Weniger and M. Zitterbart, “Address autoconfiguration in mobile adhoc networks: current approaches and future directions,” IEEE Network, Vol. 18, 2004, pp. 4-11.

[2] M.-S. Pan, C.-H. Tsai, and Y.-C. Tseng, “The orphan problem in zigbee wireless networks,” IEEE Transactions on Mobile Computing, vol. 8, pp. 1573–1584, 2009.

[3] IEEE TG 15.4b, Part 15.4: Wireless medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), IEEE Standard for Information Technology, 2006.

[4] Distributed Borrowing Addressing Scheme for ZigBee/IEEE 802.15.4 Wireless Sensor Networks by Sungjin Park, Eun Ju Lee, Jae Hong Ryu, Seong-Soon Joo, and Hyung Seok Kim

[5] Automatic Discovery of Topologies and Addressing for Linear Wireless Sensors Networks by Moussa D´ethi´e Sarr, Franc¸ois Delobel, Michel Misson, Ibrahima Niang Clermont University, University Blaise Pascal, Limos, 2012

[6] C.E. Perkins and E.M. Rouyer, “Ad-hoc On-Demand Distance Vector Routing,” Proc. IEEE WMCSA, 1999, pp. 90-100.

[7] K. Akkaya and M. Younis, “A Survey on Routing Protocols for Wireless Sensor Networks,” Ad hoc Networks, vol. 3, no. 3, May 2005, pp. 325-349.

[8] J.N. Al-Karaki and A.E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey,” IEEE Wireless Commun., vol. 11, no. 6, Dec. 2004, pp. 6-28.

[9] C.E. Perkins and P. Bhagwat, “Highly Dynamic Destination Sequence-Vector Routing (DSDV) for Mobile Computers,” Proc. ACM SIGCOMM, 1994, pp. 234-244.