Hierarchical Collision-free Addressing Protocol(HCAP) for Body Area Networks

Samaneh Movassaghi and Mehran Abolhasan
Faculty of Engineering and Information Technology
University of Technology, Sydney, Australia
Emails:{Seyedehsamaneh.Movassaghigilani,Mehran.Abolhasan}@uts.edu.au

Justin Lipman
Intel R&D
Shanghai China
Email: justin.lipman@intel.com

Abstract—**In Body Area Networks (BANs) the addressing scheme used to address nodes is fundamental to the effective operation of a BAN. This paper proposes a novel BAN addressing scheme called Hierarchical Collision-free Addressing Protocol (HCAP). Proposed scheme is collision free, reduces power consumption and tackles the address wastage problem. Two important scenarios (random location and fixed location) are defined and studied. Through a series of simulation results we show the efficiency and usability of the proposed scheme in Body Area Networks.**

Keywords- address allocation, Body Area Network, BAN

I. INTRODUCTION

In recent years, body area networks have emerged as a promising technology that will enable the interconnection of miniature, lightweight, low power monitoring devices (sensors) through wireless communication links. The collection of these tiny sensor nodes which compose the body area network, aim to improve the accuracy and speed of the way data is recorded. The sensors are capable of monitoring vital signals, providing real-time feedback which aids diagnostic procedures in health monitoring applications of a patient via continuous monitoring and providing information on the recovery process. However, BANs are subject to some constraints given limited energy resources, postural body movements and ultra-short wireless range [1].

Communication between the entities inside a BAN such as the sensors and the PDA (Personal Digital Assistant) is called *Intra-BAN communication*. External communication between the PDA and the central server is called *extra-BAN communication* [2]. BAN communication is achieved through the use of low-power wireless communication technologies such as IEEE 802.15.1 [3], IEEE 802.15.4 [4] and IEEE 802.11 [5 & 6]. More importantly, for actual data exchange and communication a unique identifier is required for each node. Any proposed scheme would need to satisfy the following requirements: self organizing, dynamic, scalable and be energy efficient.

Additionally, given limited address space in BANs [7] and the effect of address space usage on the addressing scheme, any proposed addressing scheme has to consider collision avoidance as a major goal while ensuring other important requirements are met.

In [7], an addressing planning scheme has been proposed for personal area networks of Zigbee using tree based arithmetic series. The method eliminates address duplication and wastage compared to other addressing schemes; however it is incapable of handling node mobility in a BAN. According to the movement of the body, nodes in a BAN may have different positioning relative to each other over a period of time. Consequently, the address allocation scheme has to support the nodes movement in conjuction witht the bodies movement.

A new IP address allocation algorithm, called Prophet [8] can be applied to large scale MANETs with low complexity, low communication overhead, even address distribution, and low latency. But, due to the considerable amount of address conflict when the network is expanded the method is found to not be convenient for usage in BANs. Following the idea in [8], the mathematical analysis of Prophet dynamic address allocation has been provided in [9]. Simulation results in [9] show the Prophet scheme to be very sensitive to network topology resulting in many address conflicts for some network configurations.

An effective address allocation mechanism has been proposed in [10] which has the advantages of providing an efficient way of allocating a 16-bit address space without wastage and also provides the possibility of network expansion without any limitations. Additionally, it provides real-time addresses for all nodes and is capable of supporting node mobility. The network in [11] uses CSMA/CA mechanism which is not efficient for BANs due to the power consumption and data rate constraints in BANs. In [11], a fully distributed address allocation algorithm with extremely low communication overhead has been proposed which also eliminates permanent duplication of IP addresses. The proposed scheme is completely free of periodical maintenance messages, timeouts, delays, and modification of existing network protocols. However, it requires a large area address space which is prohibitive given limitations of sensors used in BANs.

In [12], the problem of node mobility in general self-organizing network has been discussed and an effective addressing scheme based on Dynamic Address Allocation (DAA) has been proposed to solve the problem. It has the advantages of very high Packet Delivery Ratio (PDR) and low signaling overhead. However, it has a high end-to-end delay.

In this paper a novel addressing scheme is proposed for identification of nodes in a BAN. It outperforms other proposed addressing schemes in terms of efficient usage of the limited address space in BANs while also considering collision avoidance and the limitation on feedback from nodes due to the issue of limited power consumption. Our addressing scheme, divides its address space into 3 subspaces. Based on which, any node that joins the network will get assigned with an address based on the other nodes in the network which are in its coverage area. The addressing protocol is designed such that it does not need a central server for addressing. In other words, our address allocation method is not centralized, but decentralized. In order to consider this transmission range, a coverage area is defined for each node that wishes to join the network.

This paper is organized as follows. Section 2 describes the system model. In Section 3, the description of the proposed addressing scheme, namely *Hierarchical Collision-free Addressing Protocol* (HCAP) is provided. In the same section, the scenario for address allocation towards the nodes is given. Section 4 provides the evaluation results of the proposed addressing scheme and its results through simulation. Finally, Section 5 concludes.

II. SYSTEM MODEL

A. Network Topology

The basic network architecture of a body area network is shown in Fig.1. It shows one possible placement of nodes for a human being with a height of 170cm and a width of 35cm. There are three different types of nodes in a BAN: one coordinator, a number of routers and child nodes. The *coordinator node* acts as a gateway to the outside world, another BAN, a trust centre or an access coordinator. Normally, the personal digital assistant (PDA) of a BAN is the coordinator node through which all other nodes communicate. The end devices are the barren nodes in a network which are termed *child nodes* and are therefore, limited to performing the embedded application. The nodes in between are the called the *routers* – these nodes have a parent node, possess a child node and relay messages.

A conventional body area network consists of a coordinator and a series of child nodes and routers in a star or peer-to-peer topology. In some cases these topologies can mix together to build up a mesh or cluster tree. However, due to the fact that the nodes in a BAN are designed to work in low-power configuration and the case of a weak connection between the links in some situations, there is a need for multihop communication. In essence, for communication between a node located at the waist with a node in the foot, an intermediate node will be required. Consequently, the addressing scheme proposed in this paper is based on a two-hop star topology.

B. Issues in addressing for Body Area Networks

In our proposed addressing scheme the following issues need to be taken into further consideration.

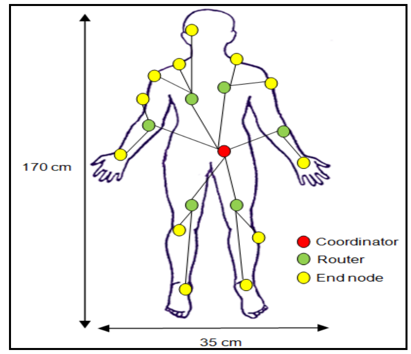

Figure 1. Node configuration in a BAN with star topology.

1) Limitation of address space in BANs: Due to the address space constraint in BANs[7], the size of the network, number of routers and children to be supported are limited. This short addressing space is kept for the identification of the child nodes, routers and the network coordinator [1]. The bigger the address space the more processing and transmission time and power is required, hence given the limited available power supply in the nodes, the shorter the address space, the greater the power savings.

2) Address interference/collision: Each node in the network needs to be given a unique and specific address once it wishes to join the network in order to eliminate traffic as well as providing efficient routing.

3) Node mobility for address allocation: Due to the change of topology in BANs which occurs due nodes leaving or joining the network, the proposed method should be adaptive with different topologies as well as considering address space usage and interference. However, in terms of node departure, in cases where a coordinator leaves the network, the whole network is bound to fail. However, if one of the routers or child nodes leaves the network, some considerations need to be met. In other words, once a router leaves the network, its child nodes are bound to network departure which causes a lot of deficiencies. In such a case, these child nodes should be supported via another router in the BAN neighborhood which is already in the network. For such an aim, the other routers in the network should assign an address to this node. After which, the next lowest number is assigned to the node. As for a child node departing the network, no significant issues arise.

4) Address wastage and duplication: Whenever a node wants to leave or join the network there should exist capability for efficient address reuse. This will additionally prevent address interference.

5) Limitation of network expandability: One of the major deficiencies of an address allocation is limitation in its expandability. An appropriate addressing scheme should provide enough space for the expansion of the maximum number of children of the routable device and so provide a good solution for expandability.

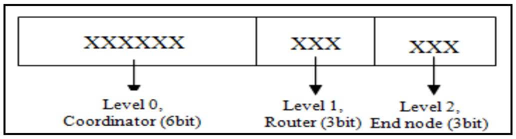

Figure 2. Addressing buffer

III. HIERARCHICAL COLLISION-FREE ADDRESSING PROTOCOL(HCAP)

Our protocol works such that each node which joins the BAN, is assigned with an address. It can choose whichever place it wants to be located in the body. In other words the subspace definition is not related to the protocol and has to work for any subspace.

It is important to note that each node knows of its role in the network beforehand. In essence, each node knows if it is the coordinator, router or child node in the network. In Table.1 and Table.2 an indicator (*Ind*) is defined which assigns the values 0, 1 and 2 for coordinator, router and child nodes respectively. In cases where the indicator is not considered, the HCAP protocol will not have much difference with the state where there is an indicator. When the indicator is not considered, all nodes in our coverage area will provide us an address response which increases the communication overhead. By considering an indicator, we can reduce the number of address responses optimistically and consequently reduce the communication overhead. As the coverage area of the coordinator includes all the subspace, once the coordinator has joined the network and has been assigned with an address it will be in the coverage area of all nodes. The coverage area is a parameter that has a major role in address assignment for each node. Therefore, in cases where the new joining node is meant to be a router it can easily communicate with the coordinator and get assigned with an address for it. However, in cases where the new joining node is meant to be a child node and detects a few routers in its coverage area, it first gets assigned with addresses from these few routers and then selects the lowest address as its selective address.

In our addressing scheme, an addressing buffer has been be specified which divides its number of bits into three parts. The first six bits (L_0 bits) assign the address of the coordinator. The reason for assigning 6 bits for the coordinator is based on the assumption of 64 coordinators with the capability of interference-free communication. In other words, the maximum number of coordinators capable of communication with each other without address interference is assumed to be 64. In this case, one of the required parameters for address allocation is defined. The next three bits (L_1 bits) define the address of the nodes in the first hop. We have assumed the maximum number of nodes in level one to be 7. Hence, the 3 middle bits of the buffer have been assigned for this aim. The numbers for address assignment towards the routers start with 1. The last three bits (L_2 bits) assign the address for the end devices allowing up to 7 child nodes for each router node.

Fig. 2 shows a 12 bit addressing buffer, which demonstrates the number of bits that have to be assigned for addressing each level. However, the number of bits assigned to each section of the addressing buffer can be specified based upon our choice given the number of coordinators capable of communication without interference and the maximum number of child nodes and routers in the network.

Table 1 shows the pseudo code for new nodes joining the network in the Hierarchical Collision-free Addressing Protocol (HCAP). Additionally; Table 2 shows the pseudo code for the existing nodes via the same addressing scheme. *ADR_REQ* is the address request message which is sent by the node. This message has to include the *Ind* within it as the address assigned depends on the role of the node. ADR_RSP is the Address Response message which is given in response to *ADR_REQ*, by which an address in assigned to that specific node. Once an address in assigned to a node, an *ADR_ACK* message is provided to inform the whole network of the allocation of that address. *Last_ADR* is the last address which has been assigned.

TABLE I. HCAP for New Nodes

```
For any new node in the network:
Send ADR_REQ & Ind;
Wait for ADR_RSP;
If (Receives no ADR_RSP)
        If (Ind=0)
            ADR=(0,0,0);
        If (Ind≠0)
            No address is assigned to that node;
Else If  (Receives one ADR_RSP)
        If  (Ind=0)
           ADR=ADR_RSP+(1,0,0);
        If (Ind=1)
           ADR=ADR_RSP+(0,1,0);
        If (Ind=2)
           ADR=ADR_RSP+(0,0,1);
Else If ( Receives a number of  ADR_RSP)
        If (Ind=0)
           m=argMax{first 6 bit of ADR_RSP_i}
           ADR=ADR_RSP_m+(1,0,0);
        If (Ind=1)
           m=argMin{third3 bits of ADR_RSP_i}
           ADR=ADR_RSP_m+(0,1,0);
        If (Ind=2)
           m=argMin{forth 4 bits of ADR_RSP_i}
           ADR=ADR_RSP_m+(0,0,1);
Send ADR_ACK
```

TABLE II. HCAP for Existing Nodes

```
For any router or coordinator in the a tanetwork:
Listen to ADR_REQ_i & Ind_i
If (Receives ADR_REQ)
    If(Ind=0)
        If(Ind_i=0 or Ind_i=1)
           Set ADR_RSP= Last_ADR;
           Send ADR_RSP;
           Listen to ADR_ACK;
        If  (Receive ADR_ACK)    Last_ADR= ADR_ACK;
        If(Ind=1)
        If(Ind_i=2)          Set ADR_RSP= Last_ADR;
          Send ADR_RSP;
          Listen to ADR_ACK;
        If (ADR_ACK)    Last_ADR= ADR_ACK;
```

Fig.3 shows the way an address is assigned to a new node joining the network. As can be seen, three time intervals are required for a node to be assigned with an address. In the first time interval an *ADR_REQ* is sent, in the next time interval an *ADR_RSP* is received. In the last time interval *ADR_ACK* is sent.

IV. SIMULATION RESULTS

We have performed simulation of the proposed scheme in MATLAB (version 7.9.0-R2009b) in a two hop star topology. Simulation results show that our proposed algorithm not only performs well in terms of address space usage, it out-performs other addressing schemes in collision avoidance, delivery latency and handling energy consumption.

Once a node wishes to join the network, it will first have to consider a subspace to which the node will enter. This subspace is assumed to be the first BAN, namely BAN_1. To define this subspace the range of the x and y coordinates should be defined. The value of the x coordinate is assumed to be $0<x<35$ and the value of the y coordinate is to be $0<y<170$. This specific assumption is based on the average length and height of a human being.

In the next step, the node requests an address in the defined subspace

A. *Random Location Scenario*

In this scenario, the nodes are randomly positioned on the body. It is assumed that the first node to enter the network is the coordinator. In the next step, all of the routers will join the network. Finally, all the child nodes will join the network in a row. This scenario aims to show the independence of nodes to their location and to take out the limitation of connection to a specific router and make it capable of connection towards the router through which it has a good connectivity link as well as the minimum number of child nodes.

For this study, we have assumed to have one coordinator, 7 routers and 12 child nodes. It is important to note that the coverage area of the coordinator is the whole subspace of the network. Therefore, once a router wants to join the network it will surely be in the coverage area of the coordinator and so does not need to be assigned with a coverage area. This parameter need only be defined for the child nodes which we have chosen to be 35cm.

Fig. 4 shows the result of the proposed scheme for the scenario which is mentioned above. As can be seen, all the routers (green nodes) have been provided with an appropriate address. Consequently, all child nodes can find a good parent node and an appropriate address. There is no address interference in this scheme and all nodes will have unique addresses

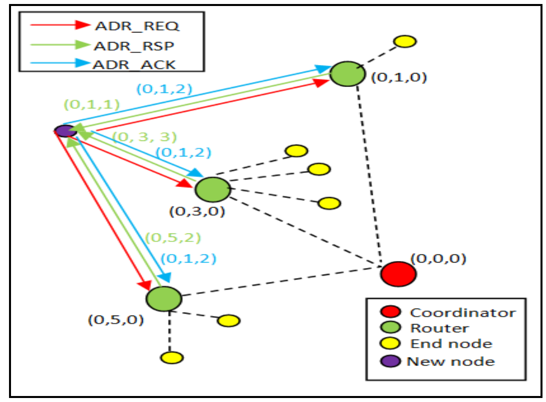

Figure 3. Address assignment procedure

B. *Fixed location scenario*

In this scenario, we assume that the nodes will arrive in a pre defined manner. In other words, they would know which position to be located in before joining the network. Based on which, we have to do the simulation by considering a fixed location for each node. Also, it is assumed that the first node to join the network is the coordinator. After which, there is no order on the way the nodes wish to join the network. However, in such a case there will be several scenarios for their attendance.

For example, in Fig. 5, the first node to enter the network is the coordinator which is assigned with (0, 0, 0) and the next node to join the network is the router which is assigned with (0, 1, 0). The next few nodes to join the network are its child nodes which are assigned with the addresses (0, 1, 1) and (0, 1, 2).

The reason for the definition of this scenario is that some nodes may join the network later. A child node may enter the network after all the routers have joined the network or there could be a case where a router will join the network with all its child nodes. Fig.5 shows that this scenario can be achieved via our proposed method which assigns collision-free addresses to the nodes without causing too much delay on the network. As a matter of fact, each node can be assigned with an address after three time intervals.

Due to the low number of child nodes in the random location scenario there will be a slight number of child nodes that are not in the coverage area of any router and so cannot be assigned with an address. On the other hand, we have assigned only three bits to each router to give addresses to its child nodes. This shows that we can only assign seven addresses. In such a case, if the number of child nodes around a router which can only be assigned via that router exceed 7, a number of child nodes would remain not assigned with any address.

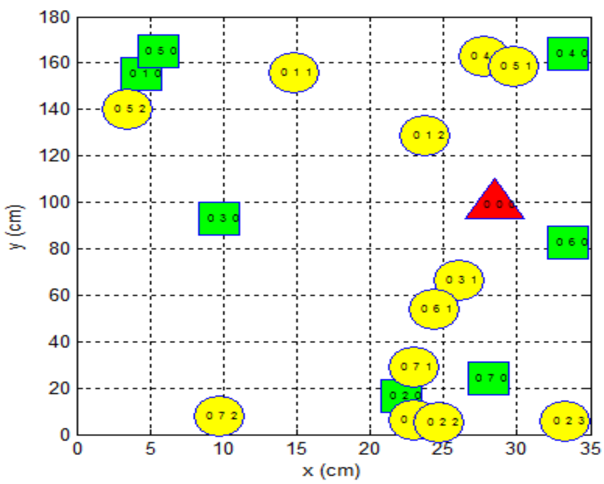

Figure 4. Simulation result for random location scenario, total number of nodes is 20 and the coverage radius of child nodes is 35 cm. The red node is the coordinator, green nodes are routers, and child nodes are shown in yellow.

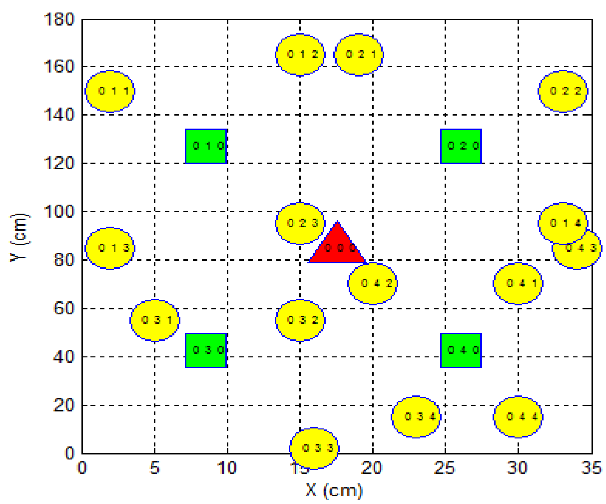

Figure 5. Simulation result for fixed location scenario, total number of nodes is 20 and the coverage radius of child nodes is 35 cm. The red node is the coordinator, green nodes are routers, and child nodes are shown in yellow.

C. Comparison towards our proposed strategy

In Fig.6, the average probability of address allocation failure has been shown based on different number of nodes and coverage areas assigned to the child nodes. Failure is interpreted as the addressing algorithm not being successful due to the following reasons: 1) The node is not in the coverage area of any of the other nodes. 2) The node is allocated close to a node which is fully occupied in terms of address allocation. As can be seen, if the coverage area is assigned with a very big number such as 100, approximately 50 nodes are capable of being assigned with an address with the probability of zero failure. In smaller coverage areas, such as 35 cm, a total of 20 nodes will be assigned with an address without any failure. In summary, in the random location scenario where nodes are not pre assigned with a position, the probability of failure will increase by the decrease in the coverage area. In a practical BAN deployment, nodes are not placed randomly, but with specificity to their function. Hence routers and child nodes will be placed accordingly so as to maximize their coverage and connectivity. In essence, they will be placed where they can take all the body into their coverage. As a result, in the fixed location scenario, this has been considered and so, there is no issue of address failure.

However, it is important to note that our allocation scheme results in more latency compared to the prophet address allocation which only requires 2 time intervals for its latency. But, there is a trade off via this choice of address allocation given the increased probability of address collisions.

In Fig.7, average power consumption of each node has been drawn for networks with different number of nodes and coverage areas. We have done these calculations for the random location scenario. We consider each of the nodes to have the same amount of power consumption in each transmission. Consequently, the overall power consumption is relative to the number of transmissions. As can be seen in Fig.7, our power consumption is very high in cases where the coverage radius is in its maximum or minimum. In case of very large coverage areas, the numbers of nodes in that coverage area are a lot. Consequently, we will get more address responses which increases the overall power consumption. However, in cases where there are fewer number of nodes, there is a larger amount of address requests which results in bigger power consumption.

According to Fig.6 and Fig.7, the bigger the coverage area the lower the probability of failure. But, there will be an increase in power consumption. On the other hand, in cases where the coverage area is small, the probability of failure will increase whereas the power consumption will decrease. In summary, there is a trade-off between the average ratio of node failure and power consumption.

Table 3 represents a comparison between the proposed scheme and two other methods, LAA [10] and Prophet [8]. Compared to the LAA (Last Address Assignment) [10] addressing scheme, which is a centralized addressing scheme in which all the nodes are allocated with an address from the coordinator, there is no collision occurrence. But in such a multi-hop network, each node should spend a lot of time for its message to be sent to the coordinator. In Table 3, we consider the latency of message transmission to be the round trip time which is equal to 2t. In LAA, l is the level of network with the node in it. Additionally, in LAA and Prophet, each node has to know its parent in order to be allocated with an address. As latency increase with the number of levels in the network, the LAA scheme is considered unsuitable for BANs as they also require multi-hop communication. In our addressing scheme, we have solved the collision issue without adding much latency and each node is allocated with an address by its coordinator.

Prophet address allocation is a mathematical based algorithm for distributed address allocation. Even though, the Prophet scheme leads to lower latency compared to the other methods, it has a major drawback of high probability of collision occurrences in multihop networks. However, in terms of scalability, Prophet scheme is the best algorithm. But, it is important to note that prophet scheme for larger networks should be optimized in order to reduce address conflict. The same transmission time is allocated between any pair of sensors.

As BANs deal with low power applications, the address allocation scheme should be such that it does not require that much time in terms of address allocation due to the fact that the increase in the number of transmissions results in higher power consumption. Our address allocation scheme has aimed to reduce latency as well as minimize the number of collisions. On the other hand, our allocation scheme is convenient in terms of network expansion as we can change the number of bits assigned to each level. Additionally, in terms of node

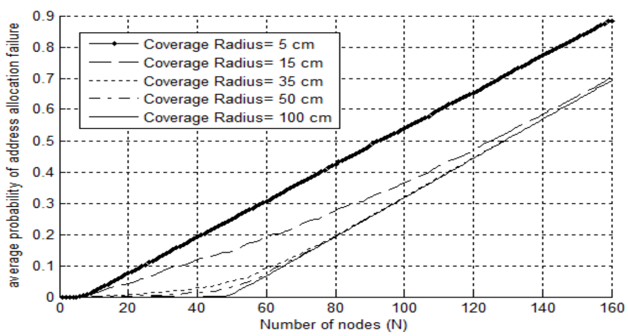

Figure 6. Average probability of address allocation failure versus different number of nodes for different values of coverage radius

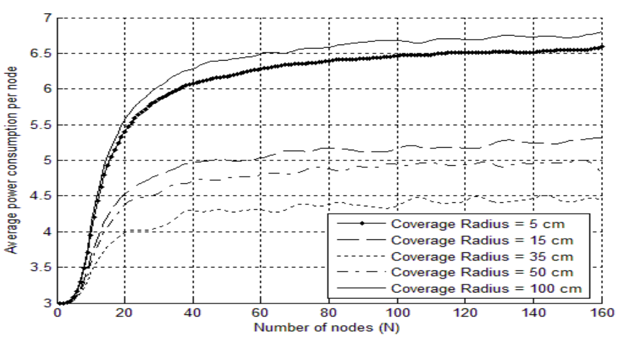

Figure 7. Average power consumption per node versus N

TABLE III. Comparison toward other schemes

	Prophet [8]	LAA [10]	HCAP
Require each node to know its parent	Yes	Yes	No
Conflict	Networks with 2 levels or more have high probability of collision	No	No
Latency	*O(2t)*	*O(2t * 2 * l)*	*O(2t *3)*
Address allocation mechanism	Distributed	Centralized	Distributed
Scalability	High	Small	Medium

departure, our allocation scheme is suitable and does not require extra communication for solving this issue and the child nodes should only find a new router via the proposed method.

V. Conclusion

This paper proposes a novel address allocation scheme after a detailed study on several address allocation algorithms. This method of addressing is collision free and independent of node configuration, as well as providing efficient address space usage and the capability of address reuse. In terms of energy efficiency, as each node does not require more than three time intervals for being allocated with a unique address, it is considered to be convenient for low-power applications in BANs. We have also reached the point that the number of bits assigned to each level need to change dynamically for different applications which can be considered in future work.

References

[1] M. Quwaider, and S. Biswas "On-body Packet Routing Algorithms for Body Sensor Networks", First International Conference on Networks and Communications. NETCOM '09.

[2] Dokovski, N.T. and van Halteren, A.T. and Widya, I.A. (2004) BANip: Enabling Remote Healthcare Monitoring with Body Area Networks. In: FIDJI 2003 International Workshop on Scientific Engineering of Distributed Java Applications, 27-28 Nov 2003, Luxembourg.

[3] IEEE Standard for Information Technology Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs), *IEEE Standard 802.15.4 Working Group Std.*, 2005.

[4] IEEE Standard for Information Technology Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low- Rate Wireless Personal Area Networks (LR-WPANs), *IEEE Standard 802.15.4 Working Group Std.*, 2006.

[5] IEEE 802.11b™, IEEE standard for information technology Telecommunicationsand information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: wireless LAN medium access con trol and physical layer specifications, http://standards.ieee.org/getieee802/download/802.11b-1999.pdf, 1999.

[6] J. Espina, T. Falck, and O. Mlhens, "Network topologies, communication protocols, and standards," *Body Sensor Networks*, Ed. Javier Espina, Springer, London, December 2007.

[7] J.I. Agbinya, M.A. Agbinya , "A New Address Allocation Scheme and Planning of Personal Area and Sensor Networks," *International Symposium on Parallel and Distributed Processing with Applications, 2008. ISPA '08.*, Proceeding, pp.463-470, 10-12 Dec. 2008

[8] H. Zhou, L.M. Ni, M.W. Mutka, "Prophet address allocation for large scale MANETs," *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol.2, no., pp. 1304- 1311 vol.2, 30 March-3 April 2003.

[9] C. Lauradoux, and M. Minier, "A Mathematical Analysis of Prophet Dynamic Address Allocation", inria-00429480, version 1 - 4 Nov 2009.

[10] H.I.Jeon and Y.Kim; , "Efficient, Real-Time Short Address Allocations for USN Devices Using LAA (Last Address Assigned) Algorithm," *The 9th International Conference on Advanced Communication Technology*, vol.1, no., pp.689-693, 12-14 Feb. 2007

[11] Z.Hu and B.Li, "ZAL: Zero-Maintenance Address Allocation in Mobile Wireless Ad Hoc Networks," *25th IEEE International Conference on Distributed Computing Systems, 2005. ICDCS 2005. Proceedings*, pp.103-112, 10-10 June 2005.

[12] S.C. Jha, B. Jouaber, K.M. Ahmed, "Dynamic-address-allocation based scalable routing protocol in context of node mobility," *IEEE Wireless Hive Networks Conference, 2008. WHNC 2008.*,Proceeding, pp.1-6, 7-8 Aug.2008.