A Zigbee Mobile Router Supporting NeMo And Data Security In Health Monitoring Systems

Akshaya C. S. [1] **Mr. Manoj P. B.** [2]

[1]PG student, AMCEC, Bangalore,

[2]Associate Professor, Dept of E&C, AMCEC,

[1]*akshayacs86@gmail.com* , [2] *manoj0110@gmail.com*

Abstract: In this paper, we propose a Network Mobility (NEMO) based ZigBee Mobile Router architecture and operations for supporting the network mobility of ZigBee network. Also, we present a design and implementation of the ZigBee Mobile Router for healthcare system with encryption and decryptiontechniques. The architecture is particularly *useful to manage patient's mobility where each patient is equipped with ZigBee sensor nodes.*

I. INTRODUCTION

ZigBee is a low rate wireless communication technology using small, low-cost and low-power sensors based on IEEE 802.15.4 standard. In this paper, we focus on the scheme which supports mobility to ZigBee nodes. In order to provide mobility to ZigBee nodes, we adopt the NEMO (Network Mobility) protocol. If the NEMO is applied in the ZigBee sensor network, even though each ZigBee node does not equipped with mobility protocol, it can maintain connectivity with the Internet through the ZigBee Mobile Router as a network unit. Therefore, the network mobility of ZigBee sensor nodes can be supported by interoperable architecture between ZigBee and NEMO. In this paper, we propose interworking mechanism between ZigBee and NEMO for providing the network mobility of the ZigBee network. Also,

we implement the ZigBee Mobile Router for healthcare system. We describe the architecture of the ZigBee Mobile Router and the interworking mechanism between ZigBee and NEMO. In this scenario, some of ZigBee sensor nodes are deployed on a patent's body for medical surveillance. Also, the patient has one ZigBee Mobile Router for supporting the network mobility to such ZigBee sensor nodes. These nodes monitor vital signs such as heart beats or blood pressure rate and temperature information. The patient has the freedom of moving in his room or within the hospital. The sensing data is sent to the Health Management Server periodically. If the ZigBee Mobile Router moves to another IPv6 network and detects the movement, it creates a CoA (Care-of address) i.e. IPv6 address of the ZigBee Mobile Router at its current Internet attachment point. After that, the ZigBee Mobile Router sends a BU (Binding Update) message to its HA (Home Agent) in order to notify the movement.

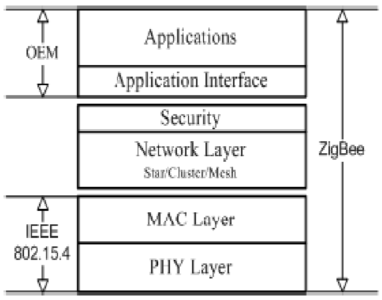

Fig. 1 ZigBee protocol Stack in relation to IEEE 802.15.4 standard

.

IEEE 802.15.4

Based on the PHY and MAC layers specified by the IEEE 802.15.4 WPAN standard, the ZigBee specification establishes a framework for the Network and Application layers. The protocol stack of ZigBee network is shown in Figure 1.

Frequency Band	868-868.6 MHz	1 channel; 20 kbps
	902-928 MHz	10 channels; 40 kbps
	2.4-2.4835 GHz	16 channels; 250 kbps
Channel Access	Slotted/Unslotted CSMA-CA	
Range	10 to 30 meters	
Addressing	Short 16-bit or IEEE 64-bit	

Table 1 Characteristics of the IEEE 802.15.4 Standard

In the PHY layer, IEEE 802.15.4 defines a total of 27 channels, namely: 16 channels with a data rate of 250 kbps on the license-free industrial scientific medical (ISM) 2.4-2.4835 GHz band; 10 channels with a maximum data rate of 40 kbps on the ISM 902 – 928 MHz band; and 1 channel with a data rate of 20 kbps on the 868.0 - 868.6 MHz band. Meanwhile, in the MAC layer, IEEE 802.15.4 controls access to the radio channel by using the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism or the optional slotted CSMA/CA mechanism in the beaconless and beaconed modes respectively. Table 1 summarizes the characteristics of the IEEE 802.15.4 standard. Two types of devices are specified in the IEEE 802.15.4 framework: a full function device (FFD) and a reduced function device (RFD). An FFD generally has more responsibilities than an RFD because it must maintain routing tables, participate in route discovery and repair, maintain the beacon framework, and handle join-
ing nodes. Moreover, an FFD can communicate with any other devices in its transmission range. In contrast, an RFD only needs to maintain a minimum amount of knowledge to stay in the network, and it does not participate in routing. Note that RFDs can only communicate with FFDs. Beyond these basic properties, IEEE 802.15.4 provides scanning, beaconing, and security functionalities for ZigBee. Implementation of these functionalities on the MAC layer simplifies the ZigBee design in that ZigBee does not have to implement these features itself. In an IEEE 802.15.4 enabled network, at least one FFD operates as the PAN coordinator; and FFDs and RFDs can interconnect to form star or peer- to-peer networks.

ZigBee Network Layer

Based on IEEE 802.15.4, the ZigBee Alliance specifies the standards for the network layer and the application layer. Specifically, the ZigBee network layer defines how the network is formed and how the network address is assigned to each participating ZigBee node. Note that the assigned address is the *only* address for routing and data transmission in ZigBee networks. Three types of devices are defined in ZigBee: the ZigBee coordinator, ZigBee routers, and ZigBee end devices. An RFD can only be a ZigBee end device; whereas an FFD can be either a ZigBee coordinator or a ZigBee router. The ZigBee coordinator is responsible for starting a new network. The coordinator and routers are \routing capable". However, ZigBee end devices cannot participate in routing and have to rely on their corresponding ZigBee parent routers for that functionality. Every node in a ZigBee network has two addresses: a 16-bit short network address and a 64-bit IEEE ex- tended address. The 16-bit network address is assigned to each node dynamically by its parent coordinator/router when the node joins the network. *This address is the only address used for routing and data transmission*; it is analogous to the IP addresses used on the Internet.

The extended address, on the other hand, is similar to an MAC address, which is a unique identification of each device, and is usually fixed when the device is manufactured. There are two address allocation schemes for the 16-bit short network address in ZigBee networks: the *static address allocation scheme* and the *tree address allocation scheme*. Both schemes work in a similar fashion in that the parent node assigns an address \block" to each of their child routers, which in turn allocate it to their respective descendent nodes. The coordinator/router is responsible for maintaining the remaining number of free address spaces, the address block size, and the address to be assigned next. Usage of the two address allocation schemes depends on the routing protocol selected.The ZigBee standard accommodates both mesh and tree topologies, which deploy di®erent routing mechanisms, and respond differently to nodal mobility.

II. LITERATURE SURVEY

With wireless networking technologies permeating nearly every aspect of our working and living environments, simple appliances and numerous traditional wired services can now be efficiently connected wirelessly. This provides simple yet effective control/monitoring convenience, while allowing very interesting applications to be developed on top of these wireless network-enabled gadgets. The ZigBee standard, which is designed to interconnect simple devices, represents the latest attempt to realize this wireless network vision. In the business environment, ZigBee wireless technology can facilitate better automated control/management of facilities and assets. Additionally, there are many ZigBee applications for home-appliance networks, as well as in the areas of home healthcare, medical monitoring, consumer electronics, and environmental sensors.ZigBee is a network and application layer specification developed by a multi-vendor consortium called the ZigBee Alliance. Backed by more than 150 member companies, the ZigBee standard was ratified in late 2004, and released for public non-commercial use in June 2005. Although various ZigBee compliant product prototypes and application scenarios have been developed or defined by the industry, the performance and support facilities of ZigBee networks have not been thoroughly evaluated.

In an environment richly connected/embedded with ZigBee devices, major topological changes can occur due to device failures, mobility, and other factors. Device mobility is unavoidable in certain applications, such as the health monitoring application for the elderly described, where a ZigBee enabled health monitoring sensor alerts the hospital, through a home ZigBee wireless network, if a health-related emergency occurs. The consequences could be disastrous if the ZigBee home network failed to relay the alert message as intended. Therefore, understanding the fundamental behavior of ZigBee networks is important for determining the feasibility/suitability of various applications. In particular, knowledge of how nodal mobility affects the performance of ZigBee routing protocols is essential.

Mobility is undoubtedly a part of the ZigBee vision, and it is important for the proper functioning of many envisioned ZigBee applications. Since mobility is anticipated and unavoidable, adequate mobility support is necessary to ensure ubiquitous connections among mobile devices. However, without a publicly available ZigBee routing implementation, no evaluation or additional development can be carried out by the research community. Furthermore, without ZigBee simulator support, it is difficult to analyze and evaluate the suitability of mobile applications in ZigBee networks.

III. WORKING OF ZIGBEE AND NEMO

Since a ZigBee end device does not have routing capabilities, problems arise if it moves outside the range of its current parent router, and acquires another network address from a new parent router. Figure 3 illustrates two instances of the issue.

In Figure 3a, the mobile end device moves outside the range of its parent router, but the source node continues sending data to it. When the device fails to find its original parent router, it will associate with a new parent router and acquire a new network address. Since the end device can no longer be found via its \old" network address, data reception ceases completely, and it cannot be recovered by any available ZigBee mesh routing mechanisms (i.e., route discovery). When the route cannot be found, a route error message will be delivered to the source node, and trigger the *Device Discovery* process in the application layer. After the source node discovers the end device's new network address, the data transmission will resume (after another route discovery procedure, and assuming the end device does not move again). In this simple case, the data is only interrupted while the source receives the route error message and completes the device discovery process.

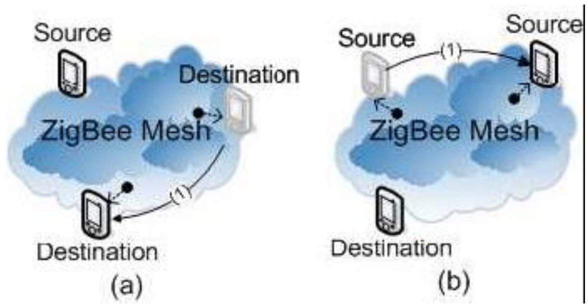

Fig. 3 (a) The source transmits data to the mobile destination which moves at time (1), and acquires a new network address in the new location. The network/application recovery mechanism is triggered and recovers the path. (b) The mobile source transmits data to a stationary destination. It then moves at time (1), and acquires a new network address in the new location, but data transmission is only interrupted temporally.

Figure 3b shows a scenario where the mobile end node acquires a new network address while it is sending data. In this case, data transmission will be temporally disrupted until the mobile end node finds a new parent router to associate with. If the data flow is two-way, a route discovery and *Device Discovery* process would be triggered at the receiver (since the source has changed its network address), and the disruption would be compounded. Even so, the situation would be recoverable, so long as the mobile end device does not move out of range again.

IV.SIMULATION RESULTS

The interworking mechanism between ZigBee and NEMO to apply it in the healthcare system has been simulated

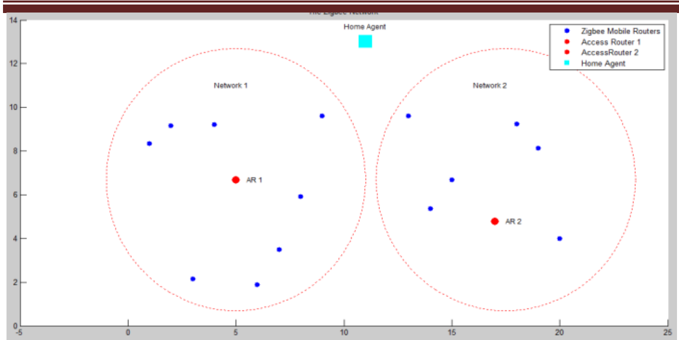

Fig.4 Graphical representation of two Zigbee networks with supporting NeMo

Figure 4 shows a scenario that a ZigBee Mobile Network moves to another network away from home network. In this scenario, some of ZigBee sensor nodes are deployed on a patent's body for medical surveillance. Also, the patient has one ZigBee Mobile Router for supporting the network mobility to such ZigBee sensor nodes. These nodes monitor vital signs such as heart beats or blood pressure rate and temperature information. The patient has the freedom of moving in his room or within the hospital. The sensing data is sent to the Health Management Server periodically.

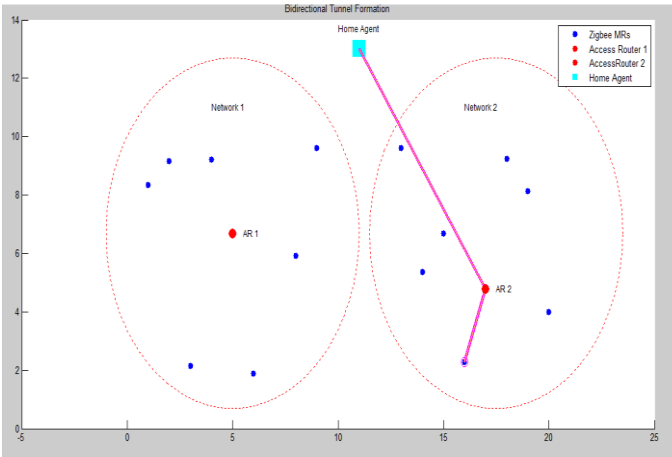

Fig 5: Sending binding update and bidirectional tunnel formation.

If the ZigBee Mobile Router moves to another IPv6 network and detects the movement, it creates a CoA (Care-of address) i.e. IPv6 address of the ZigBee Mobile Router at its current Internet attachment point. After that, the ZigBee Mobile Router sends a BU (Binding Update) message to its HA (Home Agent) in order to notify the movement. The BU message includes a proposed ZigBee PAN Coordinator option.

Fig: Command window showing Zigbee Nemo interoperation.

At the same time, the ZigBee Mobile Router stores the mobility information in Binding Update List table and establishes a bidirectional tunnel between ZigBee Mobile Router and HA. Upon receipt of the BU, the HA updates the ZigBee Mobile Router's information with ZigBee network, CoA and home address for Binding Cache Entry, and replies by sending a BA (Binding Acknowledgement) message.

V.CONCLUSION

Simulation of interworking mechanism between ZigBee and NEMO for supporting the ZigBee network mobility has been done. We shall try to implement NEMO based ZigBee Mobile Router for the healthcare system using a hardware model.

VI.REFERENCE

1. Handbook of Instrumentation - R.S.Khandpur
2. Instrumentation and measurements - Leslie Cromwell
   a. Fred. J. Wejnbell
   b. Erich. A. Pleiffer
3. ZigBee Document 053474r13, "ZigBee Specification," Dec. 2006,
4. http://www.zigbee.org/.
5. IEEE Computer Society, "IEEE Std. 802.15.4-2003," Oct. 2003.
6. V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network
7. Mobility (NEMO) Basic Support Protocol," IETF RFC 3963, Jan. 2005.
8. "NEMO Platform for Linux (NEPL)," http://www.nautilus6.org/nemo/.
9. TinyOS Community Forum, http://www.tinyos.net/.