Deployment and Experimental Verification for Data Communication in Heterogeneous Wireless Networks

Azman Osman Lim and Youiti Kado
School of Information Science
Japan Advanced Institute of Science and Technology (JAIST)
1-1 Asahidai, Nomi City, Ishikawa Prefecture, 923-1292 JAPAN
E-mail: {aolim, youiti}@jaist.ac.jp

***Abstract*— With the growing interest in various wireless networks, the need for seamless connection and interoperability of heterogeneous wireless networks is becoming increasingly important. In this research, we focus on deploying the heterogeneous wireless networks, which consists of Wi-Fi networks and ZigBee networks. In heterogeneous wireless networks, data communication between pair of a sensor node and a mesh node is essential, meaning that the sensor node may receive data from the Wi-Fi device, and vice versa. We conduct some experiments to test and verify the interoperability issues, i.e., the coexistence radio interference and addressing of the heterogeneous wireless networks. We also investigate the effect of background traffic on the performance of heterogeneous wireless networks. The results reveal that both round-trip delay and packet loss increase as the background traffic increases.**

Keywords-heterogeneous wireless networks, WMN, WSN, deployment, experimental verification, addressing, coexistence radio interference

I. INTRODUCTION

With the significant development of wireless network technologies, such as the cellular mobile communications network, satellite network, wireless local area network (WLAN), mobile ad hoc network (MANET), and wireless sensor network (WSN), many application scenarios are available for users. For example, users can access the Internet through wireless fidelity (Wi-Fi) system to browse webpages, manage emails, conduct video conference, and so on. However, such application scenarios are limited to sustain the need of users. Users demand more variety of application scenarios, e.g., temperature automation in a Wi-Fi-enabled and WSN-enabled house. A user that is embedded sensors is automatically monitoring the temperature at the living room while the user is accessing the Internet through a laptop. Thus, the integration of different kinds of wireless networks leads to the emergence of heterogeneous wireless networks. The heterogeneous wireless network has great advantages in many aspects: it can expand the network coverage and strengthen its scalability and it can provide diversified services to meet various users' demands in the future. Heterogeneous wireless networks may serve a rich set of application scenarios, failure in communications among those heterogeneous wireless networks will result in many isolated information islands of different sizes in the future, which is against our will. Therefore, it is an inevitable trend of network development in the future to implement the seamless connection and interoperable of diversified heterogeneous wireless networks.

In fact, heterogeneous wireless networks are being intensively studied and evaluated mainly by computer simulation. However, simulation evaluations cannot always accurately account for many physical layer issues such as radio interference. Hence, a deployed testbed is required to be able to study the networking issues in a real-world environment. To the best of our knowledge, there is not so much experimental work on the heterogeneous wireless networks. In recent studies, You, et al. [1] have proposed a flexible heterogeneous mesh networking platform (FHMESH), which builds a gateway using software defined radio (SDR) technology. They conducted some preliminary experiments to justify that the FHMESH is flexible and universal for interconnecting various heterogeneous networks. Other researchers have also considered the coexistence issue of heterogeneous wireless networks. Hauer, et. al. [2] have investigated the effects of WLANs on body area networks (BANs). They reported that there is an empirical correlation between WLANs and BANs.

In this paper, we also focus on the coexistence between two major wireless standards that operate in the 2.4GHz ISM (Industrial, Scientific and Medical) band, namely IEEE802.11 WLAN [3] and IEEE802.15.4 ZigBee [4]. We use these two standards to construct a testbed for heterogeneous wireless networks using state-of-the-art, off-the-shelf technology. The aim of our research work is to resolve the interoperability issues that can influence the deployment of heterogeneous wireless networks. Yet, some verification experiments of the interconnection of this testbed are conducted. We further investigate the testbed performance on the effect of background traffic. Our experiments shed new lights on the real potentialities of heterogeneous wireless networks employing today's technology. We believe that our research work is an important step towards a realistic deployment of heterogeneous wireless networks.

The rest of the paper is structured as follows. The background of wireless mesh networks and wireless sensor networks are briefly reviewed in Section II. We explain the system design, hardware, software, and problems of the implementation in Section III. We describe our experimental topology and settings and present the experimental test and verification in Section IV. Section IV reports the discussions of the network performance of our testbed when the effect of background traffic is considered. In Section V we present our conclusions and plans for future work.

II. Background

A. Wireless Mesh Networks

A wireless mesh network (WMN) [3] is an integration result of multihop communication and WLAN technology. To understand the network architecture of WMN, we first need to explain IEEE802.11 extended service set (ESS) and its difference from independent basic service set (IBSS). The IEEE802.11 ESS consists of multiple basic service sets (BSSs) connected through a distribution service (DS) and integrated with wired LANs [5]. The DS service (DSS) is provided by the DS for transporting MAC service data units (MSDUs) between access points (APs), between APs and portals, and between stations (STAs) within the same BSS that choose to involve DSS. The portal is a logical point for letting MSDUs from a non-802.11 LAN to enter the DS. The ESS appears as single BSS to the logical link control layer at any station associated with one of the BSSs.

The IEEE802.11 standard has pointed out the difference between IBSS and ESS. IBSS actually has one BSS and does not contain a portal or an integrated wired LANs since no physical DS is available. Thus, an IBSS cannot meet the needs of client support or Internet access, while the ESS architecture can. However, IBSS has its advantage of self-configuration and ad hoc networking. Thus, it is a good strategy to develop schemes to combine the advantages of ESS and IBSS. The solution being specified by IEEE802.11s [6] is one of such schemes. In IEEE802.11s, a meshed WLAN is formed via ESS mesh networking. In other words, BSSs in the DS do not need to be connected by wired LANs. Instead, they are connected via wireless mesh networking possibly with multiple hops in between. Portals are still needed to interconnect IEEE802.11 WLANs and wired LANs. Based on such a concept, the network architecture of WMN for the IEEE802.11s standard is illustrated in Fig. 1. There are three new nodes in this architecture. A mesh point (MP) is an IEEE802.11 entity that can support WLAN mesh services. A mesh access point (MAP) is an MP but can also work as an access point. A mesh portal (MPP) is a logical point where MSDUs enter/exit the mesh network from/to other networks such as a traditional 802.11 WLAN or a non-802.11 network. An MPP includes the functionality of MP and can be collocated with an IEEE802.11 portal. Because MPs do not have AP functionality but can work as relaying nodes, the meshed WLAN is not an ESS anymore.

The hybrid wireless mesh protocol (HWMP) is the default routing protocol for IEEE802.11s mesh networking. The HWMP that works on the data link layer of OSI model with 6-MAC-address scheme allows interoperability between devices of difference vendors. The foundation of HWMP is an integration of the reactive Ad hoc on-demand distance vector (AODV) protocol and the proactive tree based routing (TBR) protocol. The HWMP uses an airtime link metric for path selection, in which the airtime link metric is a measure for the amount of the consumed channel resources when transmitting a frame over a particular wireless link.

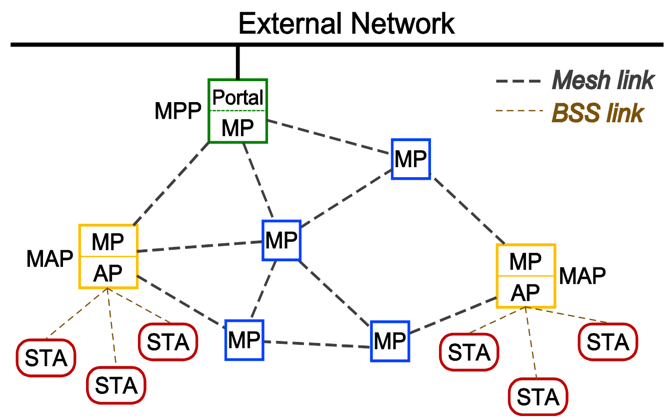

Figure 1. A basic architecture of WMN.

B. Wireless Sensor Networks

A wireless sensor network (WSN) is a network of nodes that cooperatively sense and may control the environment enabling interaction between persons or devices and the surrounding environment through wireless link. The sensed data is forwarded, possibly via multiple hops, to a sink (also denoted as a coordinator) that can use it locally or is connected to other network (e.g., Internet).

The IEEE802.15.4 MAC standard [4] (or simply ZigBee standard) is a short-range communication system intended to provide applications with relaxed throughput and latency requirements in wireless personal area network (WPAN). The key features of ZigBee standard wireless technology are low complexity, low cost, low power consumption, low data rate transmission, to be supported by cheap either fixed or moving devices. The ZigBee standard defines an optional superframe structure, which is initiated and decided by the coordinator. The superframe is bounded by network beacons and containing both an active period and an inactive period. The active period composed of 16 equally sized slots, contains the frame beacon, the contention access period (CAP) slots, and the contention free period (CFP) slots. The first time slot of each superframe is used to transmit the beacon. The main purpose of the beacon is to synchronize the attached devices, identify the coordinator, and describe the superframe structure. The remaining slots are used by competing devices for communications during the CAP period. The devices use the slotted CSMA/CA-based protocol to gain access to compete for the time slots. All communications between devices must complete by the end of the current CAP. The CFP always appears at the end of the active superframe and starts a slot boundary immediately following the CAP. The inactive period (IP) defines a time period during which all network devices, including the coordinator, can go into a sleep mode in order to reduce energy consumption. In this mode, the network devices switch OFF their power and set a timer to wake up immediately before the announcement of the next beacon frame.

As shown in Fig. 2, a ZigBee network can adopt one of the three topologies: star, tree or mesh. The way that a message is routed from one node to another depends on these topologies. The ZigBee standard has three general types of node at the network level: coordinator, router and end device. All ZigBee networks must have only one coordinator, irrespective of the network topology. At the network level, the coordinator will perform three tasks. First, the coordinator will select the frequency channel to be used by the network by performing a spectrum scan (usually the channel is selected with the least detected energy). Second, the coordinator will start the network. Last, the coordinator will allow routers and end devices to connect to it (i.e., to join the network). The coordinator can also provide message routing, security management and other services. In a tree or mesh network, the presence of at least one router is required to relay messages from one node to another and end devices to connect to it. The main tasks of an end device at the network level are sending and receiving messages. An end device can often be battery powered and, when not transmitting or receiving, can sleep in order to conserve power. Note that end devices cannot relay messages and cannot allow other nodes to connect to the network through them.

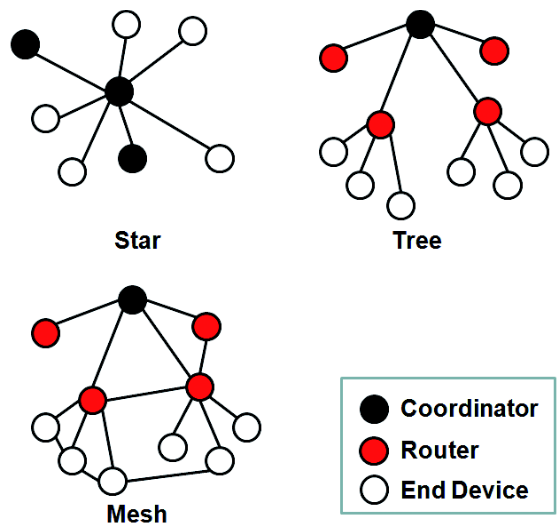

Figure 2. A ZigBee network can adopt one of the three topologies: star, tree or mesh.

III. Implementation Details

In this section, we provide the implementation details of our system for deploying the heterogeneous wireless networks. We first describe the system design. Next, the hardware and software that are used for the implementation on each of system are discussed. Last, how we set up the entire system and ensuring the system interoperability are also presented.

A. System Design

To design the architecture of the heterogeneous wireless networks, we use the model of WMN architecture as our design reference. We replace the access point (AP) and station (STA) of WMN architecture with the sink node (SN) and ZigBee node (ZN), respectively. In WMN, MAP originally provides network access services to STAs. Similarly, MAP in the heterogeneous wireless networks provides network access services to ZNs, but such services have to go through SN. As we can conclude, the architecture of heterogeneous wireless networks consists of three basic components: MAP, SN, and ZN as illustrated in Fig. 3(b).

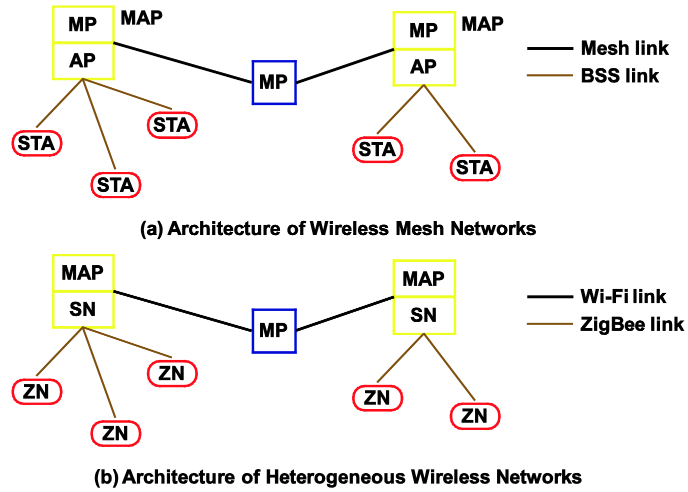

Figure 3. An architecture of heterogeneous wireless networks.

B. Hardware

In this section, we provide the hardware details for each component that used in this research work. Fig. 4 shows the mesh access point, sink node, and ZigBee node that are connected with each other and formed a basic system unit for heterogeneous wireless networks.

1) *Mesh Access Point (MAP):* A laptop is used for implementing a MAP or a MP. The architecture of this laptop is a Hewlett-Packard Mini 2140, 1.6 GHz Intel Atom N270 with a memory of 2 GB RAM. Beside that, the operating system is running on WindowsXP. This laptop has one wireless interface card, namely Broadcom 4322AG IEEE802.11a/b/g/draft-n whereby the radio is operated at 2.4 GHz. Beside that, this laptop has one Ethernet interface and one USB port, which allows the laptop to have a serial connection with a sink node. Meanwhile, the USB port is used for supplying power to the sink node.

2) *Sink Node (SN):* For a SN, we use an evaluation board TK-850/SG2+UZ, which is a product from NEC Electronics Incorporation. This TK-850/SG2+UZ uses 32-bit single chip microcontroller (µPD70F3281YGC). All of the ROM, RAM, and circumference circuit are efficiently built in one chip on a single board. High-speed operation is realized via the 20 MHz internal clock. The high speed RAM of 32 KB and the flash memory of 384 KB are built into CPU chip. The TK-850/SG2+UZ contains a UZ2400 radio frequency board. The UZ2400 is operating at 2.4 GHz according to ZigBee standard. The TK-850/SG2+UZ contains a temperature sensor.

3) *ZigBee Node (ZN)*: A 78K0 UZ that is same company's product is used as a ZN. The 78K0 UZ that is an evaluation kit

for WPAN is using a 8-bit single chip microcontroller (μPD78F0537DGA). The 78K0 UZ is ready to accommodate ZigBee standard. In the microcontroller chip, 128 KB of flash EEPROM is programmable from PC via USB connection with any additional flash programming hardware. The USB connection can be utilized not only for flash programming, but also for user applications and power supply. The 78K0 UZ also contains a temperature sensor.

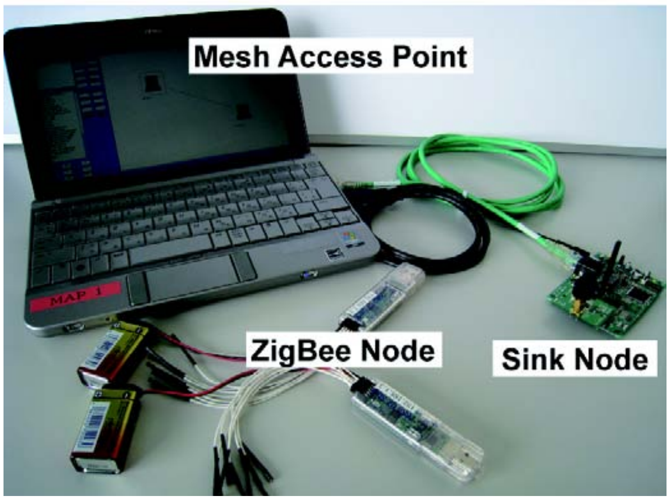

Figure 4. Mesh access point, sink node, and ZigBee node are formed a basic system unit for heterogeneous wireless networks.

C. *Software*

The software implementation is done in two different network environments. First, a ZigBee stack is selected as the wireless protocol to implement WSNs. Second, a DECENTRA [7] is chosen as the wireless stack to implement WMNs due to its easy-to-use driver support. In this section, we provide the software details for both ZigBee stack and DECENTRA in the following paragraphs.

To develop a basic application on both devices: TK-850/SG2+UZ and 78K0 UZ using the ZigBee stack, we use Project Manager V6.11 and Flash EEPROM programmer PG-FGL, in which both are working on WindowsXP OS environment. The Project Manager V6.11 is an integrated development environment platform. An editor, compiler, and debugger are managed on the Project Manager V6.11. On the other hand, The Flash EEPROM programmer PG-FGL is used to program, erase, and verify object code in the embedded Flash EEPROM in the microcontroller via USB cable from PC. To turn on the ZigBee stack for WSNs, we use a Shell-customized, which is a command-line interface (CLI). This Shell-customized is also embedded with the Internet Control Message Protocol (ICMP). For example, an alphabet letter '*p*' that represents the common '*ping*' command can be used.

DECENTRA can handle peer-to-peer communications on WMNs properly. However, it is very difficult for a current routing technology used on the Internet to keep on refreshing routing information under the topology of networks changes very frequently. DECENTRA can handle this kind of situation by using unique routing protocol, called Jnutella Routing Protocol (JRP). We describe the detail of JRP based on an example of a network topology shown in Fig. 5(a). In Fig. 5(a), circles with letters show MPs, and solid lines show sessions between MPs. JRP adopts a proactive type technology that builds a routing table initially regardless of a schedule of a data transfer, by exchanging link statuses shown in Fig. 5(b) between neighboring MPs. Fig. 5(b) shows the situation that B is acquiring link statuses from neighboring A, D, and C. Since D transfers information of E and F pulled from D's routing table to B, in which B can detect E and F beyond D. DECENTRA does not exchange all known link statuses at the same time. However, DECENTRA changes a refresh rate based on MPs' "*scope*", which means a number of hops between MPs. It is highly possible that link information of a MP located needlessly far from the other MP does not exchange link statuses in between themselves. For example, in a case of changing refresh rate as scope 3, as shown in Fig. 5(c), F is deleted from link information that B transfers, and F is not registered on a routing table of 3-hop range from A's view. By this method, a bandwidth for exchanging link information regularly can be saved lower. To overcome the communication in between A and F issue, DECENTRA adopts on-demand type source routing technology. DECENTRA's theoretical range of unicast communication is $S+\delta$, as S is a scope of exchanging link status, and as δ is a depth of "*routing stack*". In DECENTRA, historical routing information is registered in a packet itself, and it is called as "*routing stack*". And the packet has "*stack pointer*", which indicates a location of the number that has to be acquired next. This means the routing stack of the packet that reaches a destination has information to go back to an original MP.

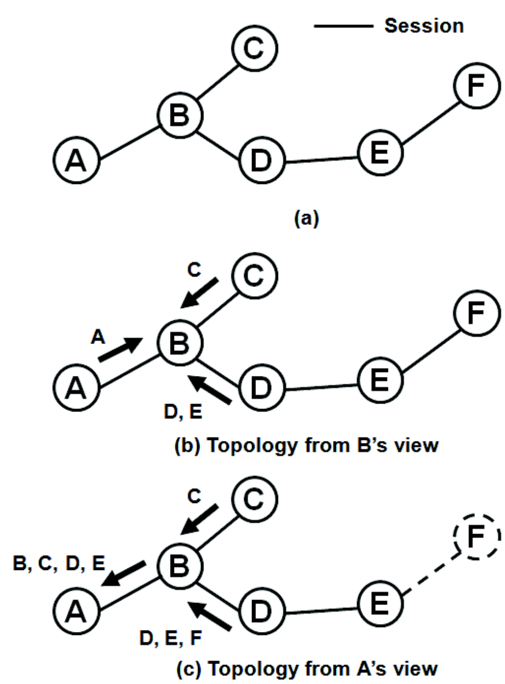

Figure 5. A network of WMN can formed by using DECENTRA.

D. Implementation Issues

In this section, we describe the implementation issues in the aspects of radio interference and addressing for accomplishing the interoperability of heterogeneous wireless networks.

Both Wi-Fi device and ZigBee device that are used in this research operate in the 2.4 GHz ISM band. The characteristics of both networks differ greatly, resulting in an asymmetric coexistence problem. To begin with, the output power of ZigBee device is typically as low as 0 dBm (1 mW), whereas the output power of Wi-Fi device is usually 15 dBm (31.6 mW) or above. Furthermore, both techniques require a listen-before-send prior to every transmission, the sensing slot for Wi-Fi device is 20 μs while the ZigBee slot is much larger at 320 μs. Thus, this will have a large impact on their collision probabilities, resulting in a heavily reduced duty cycle or low channel usage. Fig. 6 illustrates the radio interference can be existing in between the Wi-Fi link and ZigBee link. To mitigate this problem, the SN can become the Network Channel Manager, which acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. Each ZN or SN is responsible for tracking transmit failures using the *Transmit_Failure* field in the neighbor table and also keeping a network layer information base (NIB) counter for total transmissions attempted. If the total transmissions attempted is over 7 or the transmit failures exceeds 25% of the messages sent, the ZigBee device may have detected interference on the channel in use. The SN is then responsible for conducting a spectrum scan on all channels and selecting a free channel. If this spectrum scan does not indicate higher energy on the current channel, no action is taken.

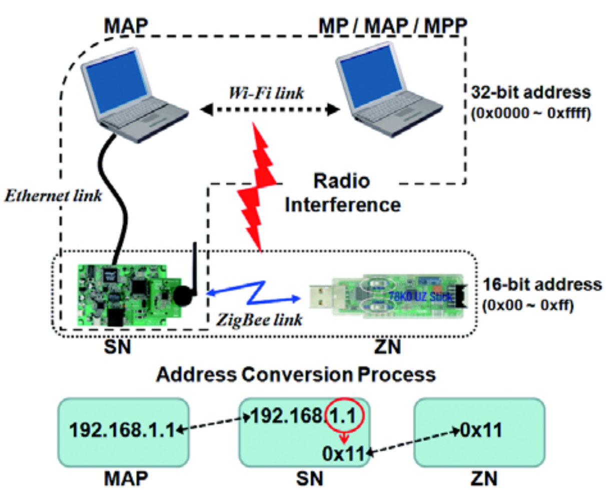

Figure 6. The interoperability issues in heterogeneous wireless networks: radio interference and addressing.

Another problem that encountered by the heterogeneous wireless networks is the addressing issue. Traditional IP-based protocols may not be applied directly to WSNs. Furthermore, ZNs that are deployed in an ad hoc manner need to be self-organizing as the ad hoc deployment of these nodes requires the system to form connections and cope with the resultant nodal distribution especially that the operation of WSNs is unattended. In WSNs, sometimes getting the data is more important than knowing the IDs of which nodes sent the data. Second, in contrast to typical communication networks, almost all applications of sensor networks require the flow of sensed data from multiple sources to a particular SN. This, however, does not prevent the flow of data to be in other forms (e.g., multicast or peer-to-peer). Due to such differences, a global addressing scheme shall be planned prior to the deployment of heterogeneous wireless networks. To explain this, we can observe the Fig. 6. In Fig. 6, there are two types of address: 32-bit IP-based address and 16-bit ZigBee-based short address. By using the global addressing scheme, we specify that a ZN holds the IP-liked address, e.g., 192.168.1.1. Such information should be stored at the corresponding SN, which performs a function of address conversion resolution from the IP-based address to ZigBee-based short address, and vice versa. Upon the address conversion is done, the SN sends a message to the ZN with the short address of 0x11.

IV. Experiments

It is very important to point out that the purpose of this research work is not to evaluate the performance of heterogeneous wireless networks, which consists of Wi-Fi and ZigBee by computer simulation. Instead, it is presenting a practical testbed of heterogeneous wireless network environment. In the following paragraphs, we describe the network topology and experimental settings of this testbed.

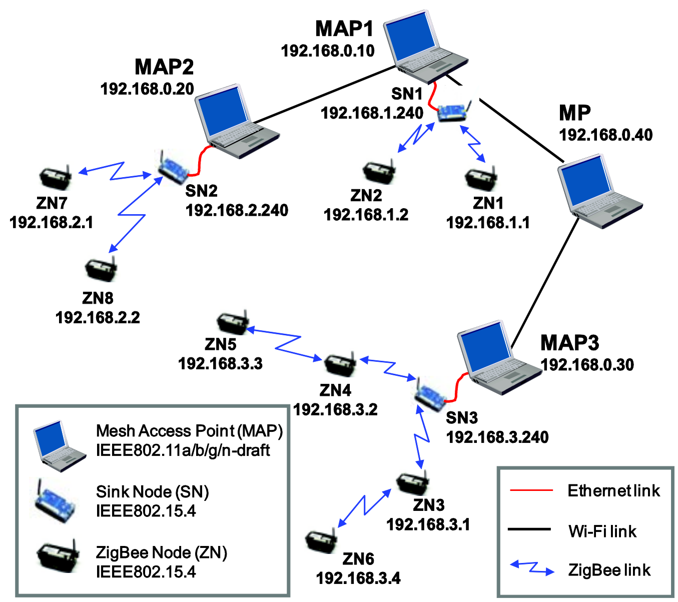

Figure 7. An overall network topology for the experiment.

A. Network Topology

The overall network topology consists of 3 MAPs, 1 MP, 3 SNs, and 8 ZNs. This network topology was deployed on one floor of an indoor environment. The dimension of the floor of the building are 20 m×40 m. In this network topology, MAPs and MP are specified by Wi-Fi standard and these devices operate at a data rate of 11 Mbps, meanwhile SNs and ZNs that are specified by ZigBee standard are operated at a data rate of

250 kbps. Their link connections are illustrated in Fig.7. Since there is no Dynamic Host Configuration Protocol (DHCP) server in this topology, each device is configured a pre-defined IP address. As we can observe, the overall topology network is divided into four physical subnetworks. Each subnetwork consists of a group of SN and ZNs, except the MP.

B. *Settings*

DECENTRA is used to handle the data communication on MAPs and MP. For such purpose, the parameters of JRP routing protocol is set based on the given values in Table I.

TABLE I. PARAMETER SETTINGS FOR JRP

Parameter	Value
Scope	3
Refresh rate	2 seconds
HELLO rate	2 seconds
Neighbor expiration time	15 seconds
Neighbor deletion time	15 seconds
Table expiraton time	15 seconds
Table deletion time	20 seconds
Link threshold	20

C. *Tests and Verification*

To investigate the interconnection for the heterogeneous wireless networks, we perform a preliminary test and verify the usability of our testbed. Therefore, our goal is to simply validate the usability of our testbed, not focusing on verifying the absolute performance of the heterogeneous wireless networks. In this preliminary test, we conduct the experiment using two MAPs, two ZNs, and one SN. We use the Shell-customized perform tasks in between all the connected ZigBee devices. In Fig. 8, a snap shot of CLI environment at MAP1 when an alphabet letter '*f*' that represents the path computation command is performed. In this experiment test, we can confirm that two hops are needed for the communication between MAP1 and ZNs. We also use a DECENTRA viewer to display the result of interconnection wireless links. Fig. 9 shows a snap shot of the graphical display of the network topology.

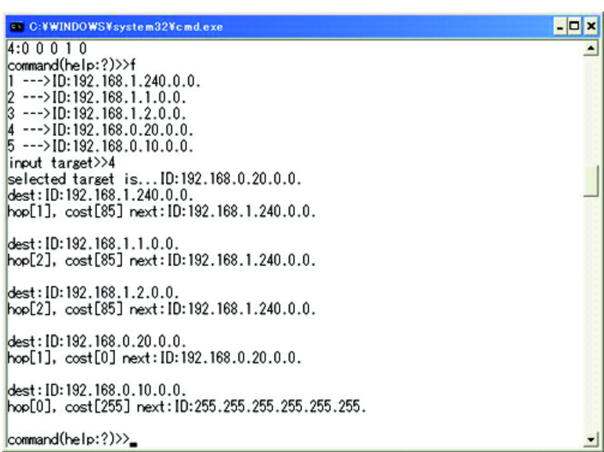

Figure 8. Snap Shot of the CLI environment at MAP1.

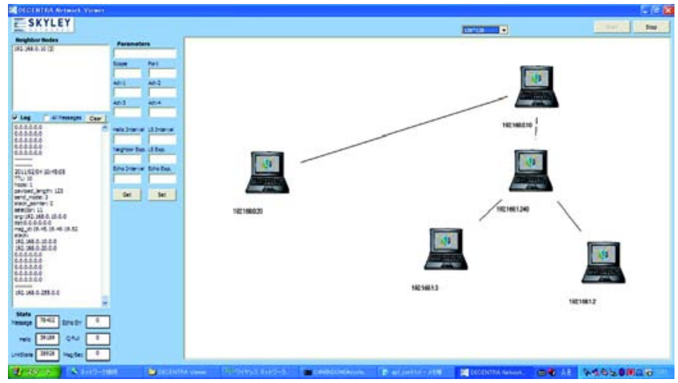

Figure 9. Snap Shot of the DECENTRA viewer at MAP1.

D. *Discussions*

In this section, we conduct an experiment for the entire network topology as shown in Fig. 7. We use '*ping*' command to measure the round-trip delay and '*iperf*' version 2.0.2 for generating different background traffic at inter-MAP. In '*iperf*', a constant bit rate User Datagram Protocol (UDP) stream is created for both ways communication in between two MAPs. The MP was performed to send the '*ping*' command to all the ZNs. The round-trip delays of all the ZNs are collected and averaged. Fig. 10 plots the round-trip delay versus the background traffic. As we can see in Fig. 10, the round-trip delay increases as the background traffic at inter-MAP increases. In addition, the variation also increases significantly when there is more background traffic. When the background traffic is 2 MB, the average round-trip delay is about 1391 milliseconds. On the other hand, the packet loss becomes burstier as the background traffic at inter-MAP increases. As a result, we can summarize that there is a strong correlation between round-trip delay as well as packet loss and the background traffic. Needless to say, there are many research challenges that need to be addressed before our testbed can be used in a real-world environment.

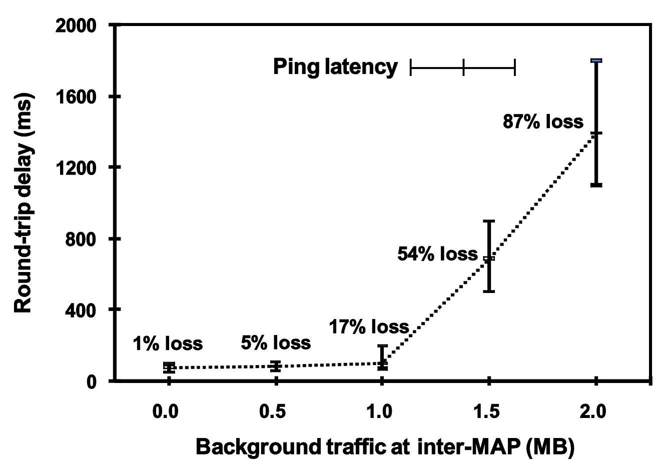

Figure 10. Effect of background traffic at inter-MAP on round-trip delay and packet loss.

V. CONCLUDING REMARKS

We have deployed the testbed of heterogeneous wireless networks, which comprises of Wi-Fi networks and ZigBee networks. From the experiments, we observed that both different wireless networks are interoperated properly regardless of the coexistence radio interference and addressing issues. We also known that both round-trip delay and packet loss increase as the background traffic at inter-MAP increases. In conclusion, the research work gives a rough indication on the deployment issues of heterogeneous wireless networks and thus we shall improve these current issues for seamlessly deploying the realistic heterogeneous wireless networks, which might consist of a combination of different types of wireless networks. Future work will concentrate on connecting the MP as a MPP to the Internet. In particular, we are interested in accessing and monitoring the WSNs from Internet.

ACKNOWLEDGMENT

We greatly appreciate the fruitful discussions with Mr. H. Umeda of the Skyley Networks, Inc. This work was supported in part by a Grant-in-Aid for Young Scientists (B) from the Ministry of Education, Culture, Sports, Science and Technology (MEXT), Japan, Grant number is 19700077.

REFERENCES

[1] L. You, C. Dong, G. Chen, Y. Dai, and W. Zhou, “FHMESH: A flexible heterogeneous mesh networking platform,” in The 6th Int. Conf. on Mobile Ad-hoc and Sensor Networks (MSN), pp.189–192, December 2010.

[2] J.H. Hauer, V. Handziski, and A. Wolisz, “Experimental study of the impact of WLAN interference on IEEE802.15.4 body area networks,” Lecture Notes in Computer Science, vol. 5432, pp.17–32, 2009.

[3] I.F. Akyildiz, X.D. Wang, and W.L. Wang, “Wireless mesh network: A survey,” in Computer Networks, vol.47, no.4, pp.445–487, March 2005.

[4] Part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs), ANSI/IEEE Standard 802.15.4-2006.

[5] Part II: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, ANSI/IEEE Standard 802.11-1999.

[6] Amendment: Mesh networking, IEEE P802.11s/D8.00, January 2011.

[7] Skyley Networks Inc., Available: http://www.skyley.com/.

[8] A. Hamidian, et al., “Deployment and evaluation of a wireless mesh network,” in The 2nd Int. Conf. on Advances in Mesh Networks (MESH), pp. 66–72, June 2009.

[9] J. Leal, A. Cunha, M. Alves, and A. Koubaa, “On a IEEE802.15.4/ZigBee to IEEE802.11 gateway for the ART-WiSe architecture,” in IEEE Conf. on Emerging Technologies and Factory Automation (ETFA), pp.1388–1391, September 2007.

[10] P. Pandey, S. Satish, J. Kuri, and H. Dagale, “Design & implementation of IEEE802.11s mesh nodes with enhanced features,” in IEEE 6th Int. Conf. on Mobile Adhoc and Sensor Systems (MASS), pp.639–644, October 2009.