NAT-ZigBee: NAT-Based Address Assignment for Scalable ZigBee Networks

Yuan-Yao Shih[1], Yu-Kai Huang[2],
Ai-Chun Pang[3], Pang-Feng Liu[4], and Wei-Ni Chu[4]

[1] Research Center for Information Technology Innovation,
Academia Sinica
`ckm@citi.sinica.edu.tw`
[2] Graduate Institute of Networking and Multimedia,
National Taiwan University
`d94944009@csie.ntu.edu.tw`
[3] Graduate Institute of Networking and Multimedia,
Department of Computer Science and Information Engineering,
National Taiwan University
`acpang@csie.ntu.edu.tw`
[4] Department of Computer Science and Information Engineering,
National Taiwan University
`{pangfeng,r95074}@csie.ntu.edu.tw`

Abstract. ZigBee has been considered as one of the promising communication protocols for low-rate wireless personal area networks. Among the well-known ZigBee topologies, ZigBee cluster-tree is especially suitable for wireless sensor applications with its supporting of power-saving operation and light-weight routing. Due to the restriction of configuration parameters, some devices could be prohibited to join a ZigBee cluster-tree network and become *orphans*. The orphan problem leads to the difficulty in smoothly increasing the network coverage or device density. In this paper, we propose an NAT-based address assignment framework for a scalable ZigBee network which locally resolves the orphan problem without the reconfiguration of a whole network, while the light-weight ZigBee tree routing is maintained. The experimental results show that the proposed framework can significantly reduce the number of orphan devices compared to the original ZigBee address assignment scheme.

1 Introduction

Recent advances in wireless communications and micro-electromechanical technologies have strong impacts on the development of wireless sensor networks (WSNs) [2]. IEEE 802.15.4 is a promising standard for wireless sensor applications with special considerations on energy efficiency and communication overheads [1]. Based on the physical (PHY) and medium access control (MAC) layers of IEEE 802.15.4, the ZigBee alliance defines the specification for upper-layer (including network and application layers) protocols. Among the well-known ZigBee topologies, ZigBee cluster-tree is especially suitable for low-power and

X. Zhang and D. Qiao (Eds.): QShine 2010, LNICST 74, pp. 307–315, 2011.

low-cost WSNs because it supports multi-hop communication with power-saving operation, and requires few resources for routing.

For a ZigBee cluster-tree network, some system configuration parameters must be determined before its topology formation. The parameters include the maximum number of children of a router (Cm), the maximum number of child routers of a router (Rm), and the depth of the network (Lm). Under the topology configuration, an accordingly distributed address assignment policy is executed for routing purpose. The topology configuration and address assignment enable a light-weight routing protocol for ZigBee devices, but limit the overall system capacity. In ZigBee, a device can successfully join a network if it associates with a proper parent device (i.e., router) and is assigned a network address. Due to the restriction of Cm, Rm, and Lm, some devices with a physical connection to a router could fail to join the network and become unaddressed. This problem is referred to as the orphan problem.

This paper aims at the proposing of flexible address assignment for a ZigBee cluster-tree network so that the system capacity can be effectively increased without violating the ZigBee specification. In the past years, notable research results have been presented for address assignment in wireless ad-hoc and sensor networks. In wireless ad hoc networks, some automatic address assignment approaches based on the concept of IP networks were presented to avoid human interventions [13] [15] [14]. The methodologies proposed in [8,6,7] ensure address uniqueness for node mobility. The reduction of address space for energy efficiency in WSNs were also investigated [3][11][17]. Unfortunately, the results of these works could not be directly applied to ZigBee networks due to its unique system characteristics.

Some alternative addressing configurations which might violate the ZigBee specification were proposed by Yen, et al. [16] as an effort to reduce the possibility of unaddressed devices. On the other hand, the work done by Pan et al. [10] is one of the pioneering studies to address the orphan problem in a ZigBee cluster tree network. They proved the NP-Completeness of the orphan problem, and proposed a better network formation to reduce the number of orphan devices. Pan et al. [9] also proposed ZigBee addressing and routing schemes for a special network topology.

Even though the existing approaches dealt with the orphan problem to increase system capacity for ZigBee networks, the scalability issue has not been well addressed in these works. In a constructed WSN, the information of some interest areas could be required for further investigation. Then new sensor devices should be deployed in an existing ZigBee network to increase the network coverage or device density in the areas. However, the newly deployed devices could be unaddressed due to their geographical locations such that the expected performance is hardly achieved. In this paper, we propose an NAT (Network Address Translation) based address assignment framework, called "NAT-ZigBee" for a scalable ZigBee cluster tree network. Once a newly deployed device fails to join the network, one of its neighboring devices is upgraded to or replaced with an NAT router to assign a private address and perform the address translation for the orphan device, while the remaining devices are not affected. In NAT-ZigBee, the existing ZigBee tree routing is not violated, and the orphan problem can be locally addressed without the reconfiguration of a whole system. The capability of our NAT-ZigBee is evaluated by extensive simulations.

The remainder of this paper is organized as follows. Section 2 overviews the ZigBee system architecture and motivation. Section 3 describes the proposed NAT-ZigBee framework for a scalable ZigBee network, and the performance of our proposed NAT-ZigBee is also evaluated by extensive simulation results in this section. Finally, Section 4 concludes this paper.

2 Zibgee Overview and Motivation

The ZigBee alliance aims at the development of a reliable, cost-effective, and low-power wireless network [5]. It specifies the network-layer and application-layer protocols upon the IEEE 802.15.4 standard [1] which defines the PHY and MAC for low-rate wireless personal area networks. This section overviews the ZigBee system architecture, and elaborates on the motivation of this work.

There are three types of ZigBee devices, and they are coordinator, router and end device [5]. The ZigBee coordinator is the most complicated device in a network, and provides the initialization, maintenance, and controlling functions for the network. The ZigBee router has a forwarding capability to route sensed data to a sink device. The data forwarding is not needed for a ZigBee end device, and its hardware requirement is minimal. A ZigBee device has two kinds of address: IEEE address and network (NWK) address. The 64-bit IEEE address is designed as a unique identifier for a device, and the 16-bit network address is used for routing. Also, a ZigBee device can support up to 240 endpoints, and each endpoint is uniquely associated an application object. The endpoint in ZigBee is analogous to a port in TCP/IP.

Each device in ZigBee maintains a neighbor table which records IEEE/network address mapping, relationship (e.g., parent/child), and link-state information of the neighbors residing in the coverage area of the device. The neighbor table is used for network association when a device joins the network or tries to connect to a new parent device, and is updated every time the device receives the packets from its neighbors. According to the ZigBee specification [5], if multiple devices with the same network address exist in the neighbor table, all the related entries are invalid such that the routing operations could fail.

ZigBee supports three kinds of network topology: star, cluster-tree, and mesh. In a star network, multiple ZigBee end devices directly connect to a ZigBee coordinator, and communications between any two end devices should be done through the coordinator. For cluster-tree and mesh networks, devices can communicate with each other in a multi-hop fashion. The cluster-tree topology is especially suitable for low-power and low-cost wireless sensor networks because of its power-saving operation and light-weight routing. A superframe structure is supported in ZigBee cluster tree topology such that the power-saving operation provided in IEEE 802.15.4 MAC layer can be utilized to achieve energy efficiency. Also, a distributed address assignment scheme defined in ZigBee enables a light-weight tree routing protocol without routing information maintenance.

In a ZigBee cluster-tree network, the topology is formulated by using the following three parameters, i.e., maximum number of children of a router (Cm), maximum number of child routers of a router (Rm), and depth of the network (Lm). Based on the parameters, a parent device can locally determine a unique 16-bit network address to its child devices. The distributed address assignment procedure is described below. The ZigBee coordinator is the root of the cluster-tree network, and normally has the network address 0. Each router is pre-allocated a finite sub-block of the address space for its children. To enable the pre-allocated concept, each router of depth d calculates a $Cskip(d)$ to decide the number of addresses allocated to every router-capable child device. $Cskip(d)$ is calculated as follows.

$$Cskip(d) = \begin{cases} 1 + Cm \cdot (Lm - d - 1), & \text{if } Rm = 1, \\ 1 + \dfrac{Cm \cdot (1 - Rm^{Lm-d-1})}{1 - Rm}, & \text{Otherwise.} \end{cases}$$

Then the distributed address assignment can be executed accordingly with $Cskip(d)$. For each parent device with address A_{parent} of depth d, the network addresses A_k for its kth router-capable child and A_n for its nth end device child are defined as follows.

$$\begin{aligned} A_k &= A_{parent} + 1 + Cskip(d) \cdot (k - 1) \\ A_n &= A_{parent} + Cskip(d) \cdot Rm + n. \end{aligned} \tag{1}$$

A ZigBee device can successfully join a network if it connects to a parent device and is assigned a network address by the parent device. A parent device shall not accept children's association once the acceptance violates the parameter settings of Cm, Rm, or Lm. Therefore, some devices might be prohibited to join the network, and become orphans even if they have strong physical connections to the network. In a WSN, the information of some interest areas could be required for further investigation after the network is constructed. Since the reconfiguration of a whole network is not cost-efficient or even impossible, new sensor devices should be deployed in an existing network to increase the network coverage or device density in some interest areas. However, under the ZigBee addressing assignment, the newly deployed devices could be unaddressed due to their geographical locations. Consequently, it is difficult for a ZigBee network to smoothly scale up and achieve expected performance.

One possible approach to solve this problem is to establish a new network in the unaddressed area and install a ZigBee gateway to connect the new network to the original network. The new network will be supervised by an additional coordinator, and the coordinator can be either elected from the existing devices in the unaddressed area or served by a new powerful device. An inter-coordinator protocol is also needed to synchronize the system information between the networks. Obviously, this approach would significantly increase the deployment cost for a scaling network. On the other hand, the orphan problem can be solved by a stochastic addressing scheme proposed in the enhanced ZigBee version called ZigBee PRO [4]. ZigBee PRO randomly assigns network addresses to devices and sorts out conflicts by continuously monitoring. However, the continuing messages exchanges occurring from monitoring and resolving for address conflict could cause significant energy consumption. Since ZigBee PRO is not standardized and compatible with legacy ZigBee specification, the system upgrading requires reconfiguration and installation for a whole network.

3 NAT-Based Address Assignment for a Scalable ZigBee Network

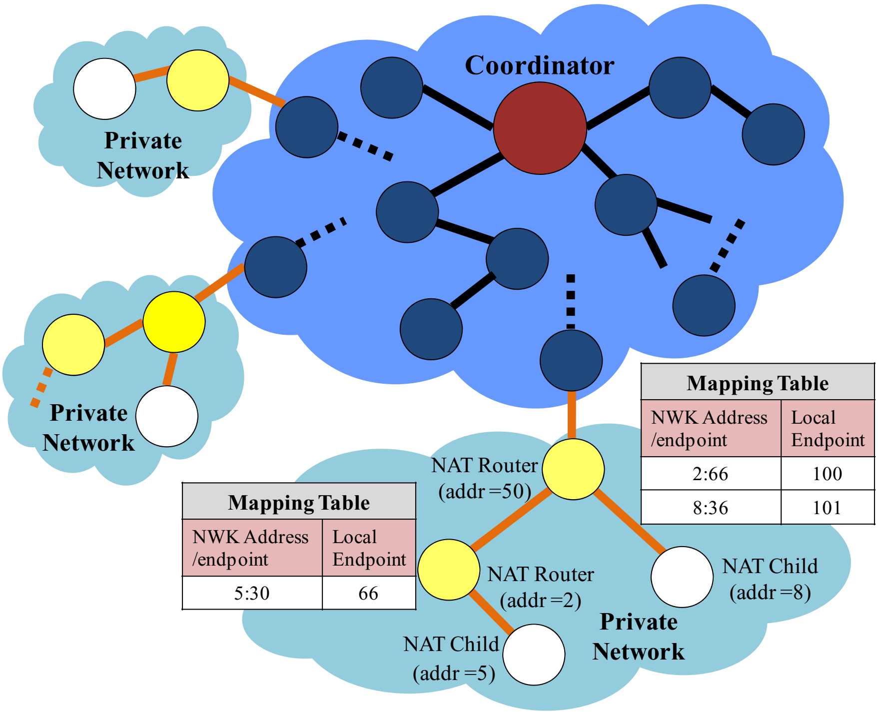
3.1 NAT-ZigBee: An NAT-Based Address Assignment Framework

In this subsection, we propose an NAT-based address assignment framework, called NAT-ZigBee, for a scalable ZigBee cluster-tree network. This solution is motivated from the Network Address Translation (NAT) developed by IETF [12], which solves the IP address shortage in IPv4 to allow private networks with internal addresses to connect public networks.

In NAT-ZigBee, the orphans are assigned private addresses and one of the orphan's neighboring devices is upgraded to or replaced with performs address translations. The mapping table for address translations can be constructed as an extension of the existing neighbor table described in Section 2. Therefore, these original orphans can join the network to carry on their sensing tasks without significant upgrading cost and message exchanges. The proposed approach preserves existing ZigBee tree routing, and locally addresses the orphan problem without the reconfiguration of a whole system. Consequently, a ZigBee cluster-tree network can smoothly scale up.

Network Address and Port Translation (NAPT) is one of the NAT techniques to transparently map a set of private network addresses and corresponding TCP/UDP ports to a small set of public network addresses and ports. In the private network, the hosts are uniquely assigned private addresses for identification. The NAT router provides address translation service by maintaining mapping entries of private address/port and public address/port. As mentioned in Section 2, the endpoint in ZigBee acts as a port in TCP/IP to identify different applications. By combining endpoints with network addresses, the NAT approach is basically applicable in ZigBee networks. Each NAT-ZigBee router transparently assigns the private address and translates the network address/endpoint for its NAT children, so the other devices are not affected.

Our NAT-ZigBee framework follows a multi-level NAT structure where a NAT router could have one or more NAT routers as its child, such that more orphans can be accommodated to further increase network scalability. Figure 1 shows an example of our NAT-ZigBee architecture. Each top-level NAT router establishes a respective private network, and data packets can be transparently forwarded to destinations with address translations level by level.



NWK Address /endpoint	Local Endpoint
2:66	100
8:36	101

NWK Address /endpoint	Local Endpoint
5:30	66

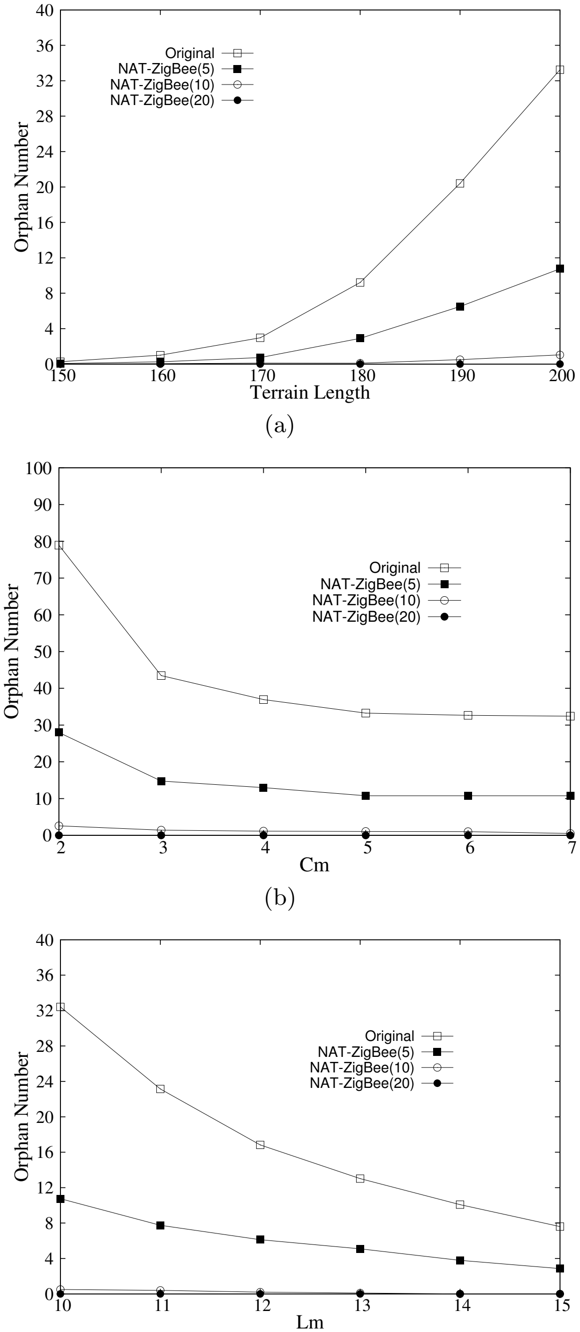
Fig. 1. The system architecture of NAT-ZigBee

3.2 Performance Evaluation

In this subsection, the capability of the proposed NAT-ZigBee is demonstrated. In the simulation model, the formation of cluster-tree topology is based on ZigBee specification [5], and the transmission range of each device is 20 meters.

In this experiment, 200 sensor devices are randomly distributed in a square terrain, and the ZigBee coordinator is placed in the center of the square. Figure 2 shows the orphan number under different network parameters. The original cluster-tree address assignment scheme specified in the ZigBee standard is used for comparison baseline. The performance of the proposed NAT-ZigBee is not compared with that in [10] since they are complementary works and can work well with each other. In the experiment, the performance of NAT-ZigBee is evaluated with the private network address spaces 5, 10, and 20.

Figure 2 (a) shows the effects of terrain length on the orphan number. It is observed that the occurrence of orphans increases as the terrain increases, since the sparse topology reduces the associations in the network. In this figure, the proposed NAT-ZigBee significantly decreases the number of orphans even with a extremely small private address space (i.e., 5). Moreover, this figure shows that the orphan problem seldom occurs when the private address is greater than 10 which is still a small portion against the whole address space.



(a)

(b)

(c)

Fig. 2. The performance of the proposed NAT-ZigBee

Figure 2 (b) and (c) shows the effects of Cm and Lm on the orphan number in a 200×200 terrain. Without loss of generality, Rm is set to be equal to Cm in the experiment. Also, Figure 2 (b) adopts the setting of $Lm = 10$ and Figure 2 (c) adopts the setting of $Cm = 5$. Since the network formulation can be more easily achieved by large configuration parameters, the curves decreases as Cm and Lm increase. However, Figure 2 (b) indicates that the orphan problem cannot be eliminated even under a large Cm due to the topology restriction. Specifically, these figures show that NAT-ZigBee has a significant performance improvement even under a small Cm and Lm. Therefore, with NAT-ZigBee, the network can operate well even with inappropriate parameters settings.

4 Conclusion

ZigBee supports low-rate wireless communications for short-range data transmissions. The ZigBee cluster-tree topology is suitable for wireless sensor applications due to its power-saving operation and light-weight routing. However, the orphan problem in a ZigBee cluster-tree network leads to the difficulty in system scalability. In this paper, we proposed an NAT-based address assignment framework, called NAT-ZigBee, for a scalable ZigBee network. NAT-ZigBee locally resolves the orphan problem without the reconfiguration of a whole network while the light-weight ZigBee tree routing is maintained. The experimental results indicated that NAT-ZigBee can significantly reduce the number of orphan devices compared to the original ZigBee address assignment scheme.

Acknowledgements. This work was supported in part by the Excellent Research Projects of National Taiwan University under Contracts 99R80304 and 99R80300, by the National Science Council under Contract NSC98-2221-E-002-200-MY3, and by Institute for Information Industry.

References

1. 802.15.4-2003 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) (2003)
2. Akyildiz, I.F., Sankarasubramaniam, Y., Su, W., Cayirci, E.: A Survey on Sensor Networks. IEEE Comm. Magazine 40, 102–114 (2002)
3. Ali, M., Uzmi, Z.A.: An Energy-efficient Node Address Naming Scheme for Wireless Sensor Networks. In: IEEE International Networking and Communications Conference, INCC (2004)
4. ZigBee Alliance. ZigBee-Pro Stack (January 2008)
5. ZigBee Alliance. ZigBee Specifications (October 2007)
6. Bernardos, C., Calderon, M., Moustafa, H.: Survey of IP Address Autoconfiguration Mechanisms for MANETs. Internet Draft (October 2007)
7. Mohsin, M., Prakash, R.: IP Address Assignment in a Mobile Ad Hoc Network. In: MILCOM (November 2002)

8. Nesargi, S., Prakash, R.: MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network. In: IEEE INFOCOM (April 2002)
9. Pan, M.-S., Fang, H.-W., Liu, Y.-C., Tseng, Y.-C.: Address Assignment and Routing Schemes for ZigBee-based Long-Thin Wireless Sensor Network. In: IEEE Vehicular Technology Conference, VTC (2008)
10. Pan, M.-S., Tseng, Y.-C.: The Orphan Problem in ZigBee-based Wireless Sensor Networks. In: ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, MSWiM (October 2007)
11. Schurgers, C., Kulkarni, G., Srivastava, M.B.: Distributed On-demand Address Assignment in Wireless Sensor Networks. IEEE Transaction on Parallel and Distributed System 13(10), 1056–1065 (2002)
12. Srisuresh, P., Holdrege, M.: IP Network Address Translator (NAT) Terminology and Considerations. RFC 2663 (August 1999)
13. Sun, Y., Belding-Royer, E.M.: A Study of Dynamic Addressing Techniques in Mobile Ad Hoc Networks. Wireless Communications and Mobile Computing 4(3), 315–329 (2004)
14. Weniger, K.: PACMAN: Passive Autoconfiguration for Mobile Ad Hoc Networks. IEEE Journal on Selected Areas in Communications (JSAC) (March 2005)
15. Weniger, K.: Passive Duplicate Address Detection in Mobile Ad Hoc Networks. In: IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, USA (March 2004)
16. Yen, L.-H., Tai, W.-T.: Flexible Address Configurations for Tree-Based ZigBee/IEEE 802.15.4 Wireless Networks. In: International Conference on Advanced Information Networking and Applications (2008)
17. Zhou, H., Mutka, M.W., Ni, L.M.: Reactive ID assignment for sensor networks. In: IEEE Mobile Adhoc and Sensor Systems Conference, MASS (2005)