An Address Conflict Resolving Scheme of Inter-drone Ad Hoc Communications for Hide Densely Deployed Low Power Wide Area Networks

Jaeho Lee[1] and Bong-Ki Son[2(✉)]

[1] Department of Information and Communications Engineering, Seowon University, 316, 1st Science Building, 377-3 Musimseoro, Seowon-Gu, Cheongju, Chungbuk 28674, South Korea
izeho@seowon.ac.kr
[2] Department of Computer Engineering, Seowon University, 315, 1st Science Building, 377-3 Musimseoro, Seowon-Gu, Cheongju, Chungbuk 28674, South Korea
bksohn@seowon.ac.kr

Abstract. Most of many communication technologies employed address identification method but many of them have not presented appropriate solution in which communication nodes would be widely and densely deployed. In this case, manually assigned ID generation method can be aggravately inefficient where there can have heterogeneously manufactured devices. In swarm flight of drone environmet, it can be high probability that multiple drones which were individually manufactured by different manufactural companies can configured with the same ID values, however, there is nothing solution in the current standard specifications of ad hoc communications, representatively as IEEE 802.15.4 or Zigbee standard. In order to find practical solution on the real world, we present an appropriate solution for dynamic ID generation with low conflict probability and for detection and avoidance method of ID conflict.

Keywords: Inter-drone communications · Ad hoc · Swarm flight · Address conflict · Dynamic ID generation

1 Introduction

Recently, the theme of Drone has been increasingly spotlighted under the unmanned system such as field discovery, measuring environmental parameters, disaster surveillance, and unmanned delivery service with another emerging theme of IoT(Internet of Things). Furthermore, swarm flight drone systems have been appearing as state of the art technology and this have been extremely promoting inter-drone communications.

In the actual environment, most of drones launched into the world market have just employed Wi-Fi as a role of video stream transmissions and FM analog radio for remote controlling drone attitude and position. However, for swarm flight of drone, communicational function between clustered drones should provide long range to cover

J.J. (Jong Hyuk) Park et al. (eds.), *Advances in Computer Science and Ubiquitous Computing*, Lecture Notes in Electrical Engineering 421, DOI 10.1007/978-981-10-3023-9_17

wide area and ad hoc delivery method with high energy efficiency. Hence, the realistic solution for above requirement can be in Zigbee technology which was designed for low-powered ad hoc communications based on MAC and PHY specifications defined from IEEE 802.15.4e and IEEE 802.15.4 g respectively.

On the other hand, many Zigbee devices recently launched on the real market provided only manual ID configuration method because the specifications of this technology cannot present dynamic or adaptive ID generation method, so every communication device has been just following with manufacture-compliant approach; most of all manufacturer employed 48bit IEEE address structure but didn't provide ID assignment method. If any operator employed heterogeneously manufactured drone products on the same application field, there is high probability of ID conflict on the same field.

For addressing this problem with the practical scenario, we designed a new solution composed of dynamic ID generation, based on Hash mechanism for reducing the probability of ID conflict, and effective detection and avoidance method for incurred ID conflict.

2 Dynamic PANID Generation and Conflict Avoidance

2.1 Hash Based Dynamic PANID

In Zigbee technology, the structure of all communication nodes was composed of PANID, for routing mechanism on each PC(Personal Coordinator) on widely deployed Ad hoc environment, and Node_ID, for local routing mechanism belonging to a PC; as a result, every PC just finds PANID for inter-PC routing. In other word, overall ad hoc routing function can be possibly miss-operated if any PC was configured with conflicted or duplicated ID value to any other PC on the whole networks. In general, IEEE address policy clearly gives unique ID function but it is difficult to be employed on MAC and routing layers due to the high length, so this cannot resolve the above problem because the specifications of IEEE 802.15.4e and IEEE 802.15.4 g employed only PANID which defined as 16bit length but not 48bit IEEE address.

This subsection presents dynamic PANID generation method based on Hash algorithm, as shown in Fig. 1. On this mechanism, every PC generates its PANID based on Hash algorithm which uses 48bit IEEE address of given PC as a seed value. So every PC has lowest probability of PANID duplication.

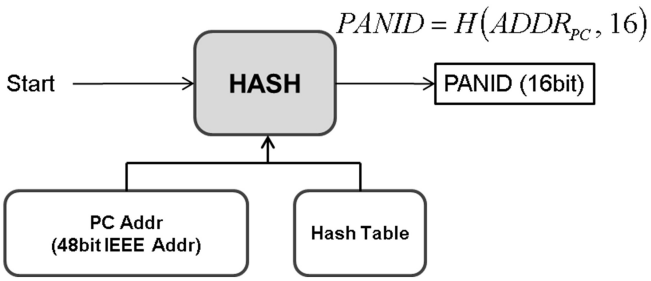

Fig. 1. Hash-based PANID generation method.

After a PC generated PANID with Hash, it should disseminate its PANID for reducing the probability of PANID confliction, because dynamic PANID generation scheme can make less conflict probability by considering neighbor's PANID if it can be aware. So this scheme makes initial flooding mechanism which let every PC sends dynamically generated PANID to its neighbor PC with broadcast transmission, as shown in Fig. 2.

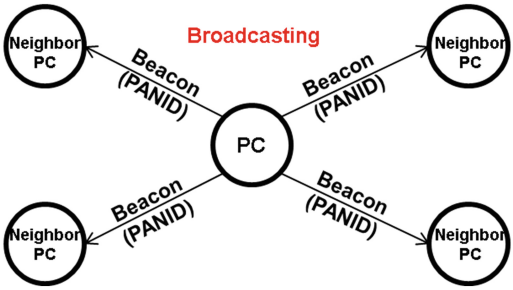

Fig. 2. PANID broadcast mechanism from the PC which just makes dynamic PANID.

If a PC detects confliction between own PANID and received PANID broadcasted from neighbor area, it can discard own PANID and generate PANID again with the different seed value.

2.2 PANID Conflict Detection and Avoidance Method

Even though the previous subsection illustrated how it provides lowest PANID confliction probability with Hash algorithm and unique 48bit IEEE address, there is still probability of PANID confliction when the network size grows up to large scaled swarm flight environment of drone. Hence, we additionally designed PANID conflict detection method and avoidance method, as shown in Figs. 3 and 4 respectively. In Fig. 3, the PC located on the middle of the figure can overhear every packet which would be delivered via the PC, so it can be aware of PANID confliction derived from far-located PC. In ad hoc environment, every packet would be delivered in hop by hop, so every intermediate PC can check the PANID included on the packet and check whether it is conflicted with its PANID or not.

Moreover, if a PC detects PANID confliction with long-distanced PC, the PC detecting the conflict would notify this event to the originated source PC by flooding the packet including the event of PANID confliction. The reason of using flooding method is that all PCs have to know the conflicted PANID on the whole ad hoc environment because they should change their PANID if any PC has the same PANID with the event packet.

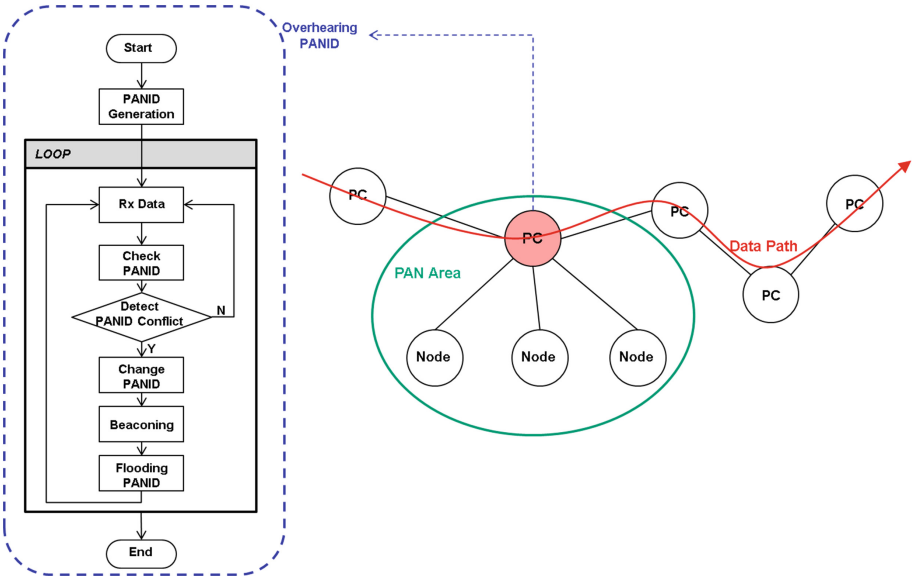

Fig. 3. PANID conflict detection method.

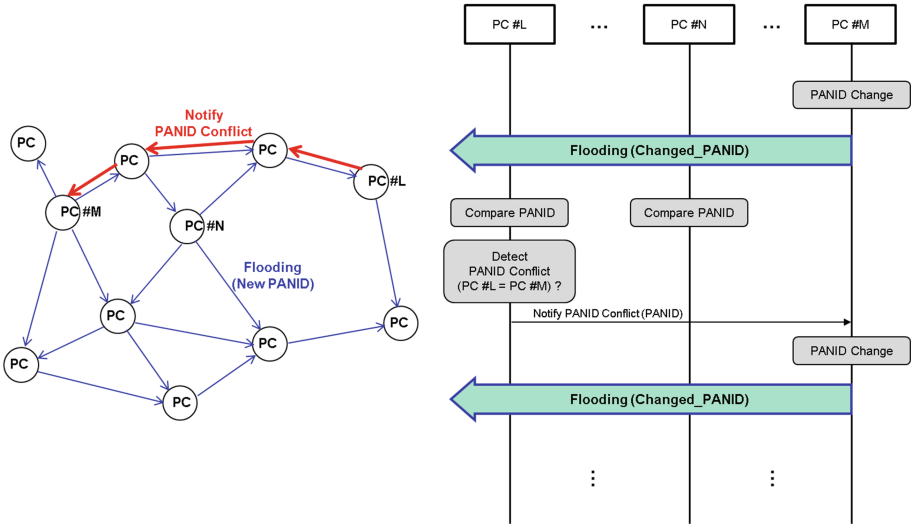

Fig. 4. Notification for PANID conflict.

3 Evaluation

Depending on the proposed scheme illustrated on the previous section, we performed simulation-based experiments to verify the performance of our scheme for the evaluations. Figure 5 shows the results of PANID confliction event number and the PDR (Packet Delivery Ratio) according to the traffic increment on the whole ad hoc environment. For the objective perspective, we employed DSDV as a representative proactive routing algorithm and AODV as a representative reactive routing algorithm. In these results, we found that proactive routing algorithm can present lower PANID conflict event comparing with reactive routing, and also found that PANID confliction could be overcome according to increment of the packet delivery frequency. Moreover, regardless of PANID confliction increment, we can found that PDR would be maintained up to 82 % on the whole traffic environment. With these results, we can verify the proposed scheme can basically prevent the confliction event of PANID and can also address from PANID confliction with the avoidance scheme we proposed.

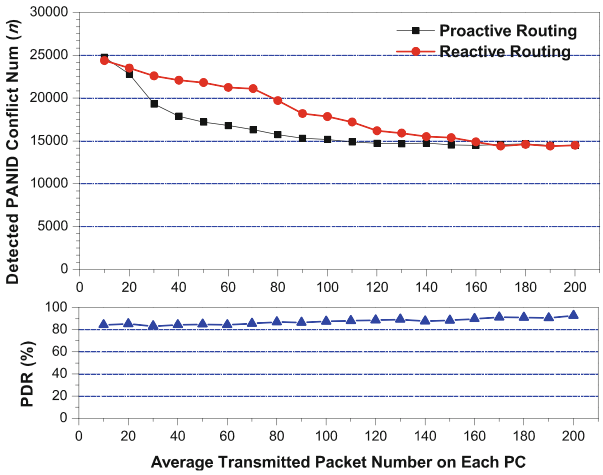

Fig. 5. Number of PANID confliction and PDR according to the traffic amount.

4 Conclusion

We presented dynamic PANID generation method based on Hash algorithm with the seed of 48bit unique IEEE address, and illustrated conflict detection and avoidance method, and prove the performance of the proposed scheme with the results of simulation-based experiments, for verifying that the proposed scheme will be useful on the environment of drone swarm flight which has the characteristics of high PANID conflict probability due to the heterogeneously manufactured multiple drones. For further research, we will design MAC protocol for meeting the fundamental requirement of massively deployed drone environment, with continuing this proposed scheme.

References

1. Zigbee Specification, Zigbee Alliance Inc., September 2012
2. http://www.ieee.org
3. IEEE, IEEE Standard for Local and Metropolitan Area Networks, Part 15.4 (Low-Rate Wireless Personal Area Networks), September 2011
4. Chiang, C-C., Wu, H-K., Liu, W., Gerla, M.: Routing in clustered multihop, mobile wireless networks with fading channel. In: Proceedings of IEEE SICON, pp. 197–211, April 1997
5. Perkins, C.E., Royer, E.M.: Ad-hoc on-demand distance vector routing. In: WMCSA 1999 Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications, pp. 90–100, February 1999
6. Haas, Z.J., Pearlman, M.R., Samar, P.: The zone routing protocol (ZRP) for ad hoc networks. Internet Draft, draftietf-manet-zone-zrp-04 (2002)
7. Johnson, D.B., Maltz, D.A.: Dynamic source routing in ad-hoc wireless networks. In: Imielinski, T., Korth, H.F. (eds.) Mobile Computing. The Kluwer International Series in Engineering and Computer Science, vol. 353, pp. 153–181. Springer, Heidelberg (1996)
8. Lee, J.: A new routing scheme to reduce traffic in large scale mobile ad-hoc networks through selective on-demand method. Wirel. Netw. **20**(5), 1067–1083 (2014)
9. Wang, L., Olariu, S.: A two-zone hybrid routing protocol for mobile ad hoc networks. IEEE Trans. Parallel Distrib. Syst. **15**, 1105–1116 (2004)
10. Busch, C., et al.: Approximating congestion + dilation in networks via 'quality of routing' games. IEEE Trans. Comput. **61**(9), 1270–1283 (2012)
11. Lee, J.: A traffic-aware energy efficient scheme for WSN employing an adaptable wakeup period. Wirel. Pers. Commun. **71**(3), 1879–1914 (2013)
12. Saxena, N., Roy, A., Shin, J.: A QoS-based energy-aware MAC protocol for wireless multimedia sensor networks. In: Proceedings of Vehicular Technology Conference (VTC), pp. 183–187, May 2008
13. Lu, C., Blum, B., Abdelzaher, T., Stankovic, J., Tian, H.: RAP: a real-time communication architecture for large-scale wireless sensor networks. In: Proceedings of IEEE Real-time Systems Symposium (RTSS), pp. 55–66, December 2001
14. Lee, J.: A massive transmission scheme in contention-based MAC for wireless multimedia sensor networks. Wirel. Pers. Commun. **71**(3), 2079–2095 (2013)
15. Weniger, K.: PACMAN: passive autoconfiguration for mobile ad hoc networks. IEEE JSAC, Wirel. Ad Hoc Netw. **23**, 507–519 (2005)