An Internet of Things Wireless Sensor Network Data Exchange Model Based on Hierarchical Address Automatic Configuration and Header Compression Encoding Strategy

https://doi.org/10.3991/ijoe.v13i07.7374

Yuan-kun Yang*, Yong-qing Ji
Kunming Metallurgy College, Kunming, China
18288729590@sohu.com

Abstract—To explore the wireless sensor network data exchange model, an addressing strategy is applied to the Internet of Things, and the real-time communication between the underlying wireless sensor network and the Internet based on the IEEE 802.15.4 protocol is realized. In addition, Hierarchical address auto configuration strategy is adopted. First of all, inside the bottom network, it allows nodes to use link local address derived by 16-bit short address for data packet transmission. Secondly, Sink node in each underlying network accesses to the global routing prefix through the upper IP router, and combined with interface identifier, it forms Sink node global address, and realizes wireless sensor network and Internet data exchange. The research results show that the strategy has certain superiority in network cost, throughput, energy consumption and other performances. In summary, the proposed addressing strategy has the characteristics of effectively integrating heterogeneous networks, reducing system energy consumption, increasing network throughput and ensuring real-time system performance for the future Internet of things.

Keywords—address automatic configuration, header compression, network data

1 Introduction

The International Telecommunication Union identifies the key technologies of the Internet of things, such as radio frequency identification technology, sensor technology, nano technology and intelligent embedded technology. At present, one of the key problems to be solved in the Internet of things is the integration of the underlying heterogeneous network and the Internet. IEEE 802.15.4 communication protocol is short distance wireless communication standard, and compared with Bluetooth technology, it is more suitable for the communication among underlying wireless sensor network devices. IPV6 is the leading technology in the next generation Internet network layer, which has a larger advantage in the address space, message format, and security. However, before the advent of 6LoWPAN technology, it is almost impossi-

ble to complete the seamless connection between the underlying wireless sensor networks based on the IEEE 802.15.4 protocol and the Internet based on the IPv6 protocol. The adaptation layer introduced between the network layer and the data link layer mainly completes the following functions in the access process: (1) for the efficient transmission, perform fragmentation and reassembly of IPv6 data packet; (2) the network address automatic configuration; (3) to reduce IPv6 expenses, carry out header compression for the IPv6 group; (4) efficient routing algorithm.

Network address automatic configuration and IPv6 header compression two functions, for identifying each terminal node accessed to the Internet of things, make the nodes able to conduct the resource sharing and information exchange, having the most important significance. As a result, this research, focusing on the above two aspects, on the basis of the 6LoWPAN adaptation layer, achieves the unified addressing of the underlying wireless sensor network based on IEEE 802.15.4 protocol and the Internet based on IPv6 protocol, and ensures that the network layer provides flexible and simple, unconnected, and meeting QoS needs for the transport layer in the era of Internet of things.

2 Overview

The basic function of the 6LoWPAN protocol is to realize seamless link between the underlying wireless sensor network based on IEEE 802.15.4 protocol and the Internet based on IPv6 protocol, that is to say, to realize IP orientation of the underlying network, so as to provide real-time and reliable network protocol guarantee for the future large-scale application of Internet of things. However, there are some technical challenges in the field of addressing based on 6LoWPAN heterogeneous network [1-3].

First of all, the traditional IPv6 address automatic configuration scheme is not suitable for application to the Internet of things. There are three main reasons: (1) there is no central server with information throughout the network in the underlying wireless sensor network of Internet of things in general, so if a node wanted to add to the network, it is supposed to first of all configure the effective address [4-5]; (2) for the cable network, a broadcast message can reach all the nodes in the link, and the underlying wireless sensor network in the Internet of things usually uses wireless transmission, which has the characteristics of multi-hop routing, so a message will be delivered to the destination node by hop. The routing characteristics determine that the scheme like DHCP (Dynamic Host Configuration Protocol) is not suitable for Internet of things; (3) the underlying network of Internet of things is usually restricted by energy, and it needs to control the communication cost to the minimum. While the traditional address automatic configuration scheme will bring higher energy consumption, bandwidth consumption, communication delay and storage space for the overall Internet of things.

Secondly, all the data on the Internet are transmitted by taking grouping as the transfer unit. The IP grouping in the network layer transmitted to the data link layer is the data portion of the link frame (MAC frame). But each kind of link layer protocol

will provide the upper limit of the length of the data frame - the maximum transfer unit MTU (Maximum Transfer Unit). The maximum link frame length defined by IEEE 802.15.4 protocol is 127byte, and removing the maximum frame overhead of about 25byte, the maximum length of remaining MAC frame is 102byte. If the safe mode is used, the frame length occupied by different security algorithms is different from a few bytes to a dozen bytes, so the length of the MAC frame load is about 81 byte.

3 Methods

On the basis of 6LoWPAN, this paper proposes an addressing scheme for the application of Internet of things. Addressing strategy consists of two parts: IPv6 address automatic configuration and header compression. For hierarchical address automatic configuration strategy, first of all, inside the underlying network, it allows nodes to use the link local address derived by 16-bit short address for data group and transmitting, and the link local address ensures the uniqueness of 16-bit short address of the duplicate address detection based on clustering; secondly, Sink node in each underlying network accesses to the global routing prefix through the upper IP router, and combined with itself interface identifier, it forms the global address of Sink node, and achieves the data exchange of underlying network and Internet.

Address automatic configuration: First of all, inside the underlying network, allow nodes to use the link local address derived by 16-bit short address for data grouping and transmission, and the link local address needs to ensure the uniqueness of 16-bit short address through DAD based on clustering; secondly, Sink node in each underlying network accesses to the global routing prefix through the upper IP router, and combined with the interface identifier (ID) calculated by IEEE EUI-64 address, it forms the global uni-cast address of Sink node, and achieves the data exchange of underlying network and Internet.

According to the needs, Sink node needs to provide 3 parameters: the number of child nodes that each parent node can connect up to the maximum is C_m, the number of routing nodes that the child node can connect up to the maximum is R_m, and the maximum length of the network is L_m, in which $C_m \geq R_{\mathrm{m}}$. Cskip(d)is the offset between the address configured by the parent node with network depth of d for its sub nodes, as shown in (1).

$$Cskip(d) = \begin{cases} 1 + C_m(L_m - d - 1), R_m = 1 \\ \dfrac{1 + C_m - R_m - C_m \cdot R_m^{L_m - d - 1}}{1 - R_m}, otherwise \end{cases} \tag{1}$$

When $C\mathrm{skip}(d)$ of a parent node is 0, it does not possess the ability of configuring address for its child node; when is greater than 0, other nodes can be accepted as its

child nodes, and they can configure different address for its child nodes. Making use of $C\text{skip}(d)$ as the offset, configure network address for the child nodes inside the network. The parent node configures address 1 greater than itself for the first routing node connected with it, and between the nodes connected with it, there is an offset difference of $C\text{skip}(d)$, and configures 16-bit short address for all the nodes in turn. It is assumed that the address of the parent node is A_{parent}, for the n-th child node, the address configuration formula is shown as follows:

$$A_n = A_{parent} + Cskip(d) \cdot (n-1) + 1(1 \le n \le R_m) \tag{2}$$

In order to avoid the reuse of the configured 16-bit short address in the network, we need to use DAD to determine the uniqueness of the address. Stateless DAD scheme does not need to maintain any allocation table, and it allows nodes to randomly or according to the hardware ID to configure the address, so we determine the uniqueness of the address by the implementation of DAD clustering. In the process of establishing the network, Sink node is used as the root node to establish the virtual logic tree structure, the depth of which is L=0. Starting from the root node, the existing network node, as the follow-up added parent node, builds the clustering, so the logic tree structure is growing. The virtual logic tree structure is shown in figure 1.

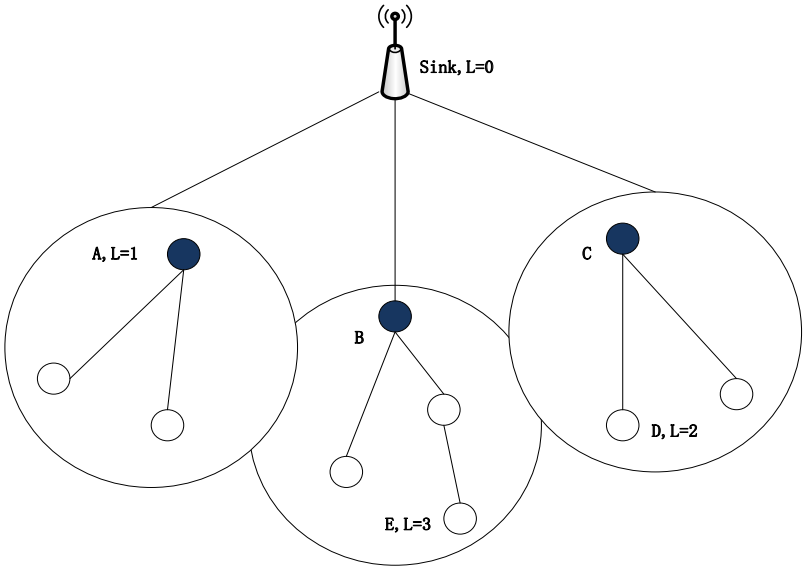

Fig. 1. DAD virtual logic tree structure

When one node E getting the address performs DAD, it only needs to carry out NS (Neighbor Solicitation) message confirmation with the cluster nodes in the cluster. The confirmation message within the cluster is passed to the root node Sinko through the parent node B with depth of 1. The Sink node carries out message confirmation

through the parent node A and C in other cluster structure, and obtains the information whether the address is occupied by the nodes in other clusters. Then, the Sink node uses all the confirmation information to verify whether the address of the node E is unique. If the address is unique, Sink node sends NA (Neighbor Advertisement) message to the node E, to inform whether the address of the node is valid; if the address is occupied by a node in the cluster, then Sink node will make use of NA message to inform whether the nodes that its address is invalid. In this case, it is supposed to combine with the routing strategy, and make use of the routing information to complete data transmission. The virtual logic tree structure reduces the number of information exchange and network communication range in the process of DAD, reduces the overhead of the underlying network system, and meets the design requirements of the Internet of things.

When a node gets 16-bit short address and determines the uniqueness, through the step (1), it will be converted into the 48-bit standard MAC address, and then use the 48-bit standard MAC address, and through the step (2) to get the automatically configured interface ID of IPv6 address:

First of all, 32-bit on the left side makes use of PAN ID of the source node and the latter added 16-bit to form, then the 32-bit domain is combined with the 16-bit short address of the the source node, to form a 48-bit standard MAC address, whose structure is shown in figure 2.

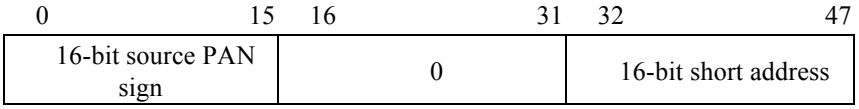

Fig. 2. 48-bit standard MAC address

In the middle of the above 48-bit MAC address, insert a section of 16-bit encoding FFFE, and converts into the 64-bit interface ID of IPv6 address, the structure shown in figure 3.

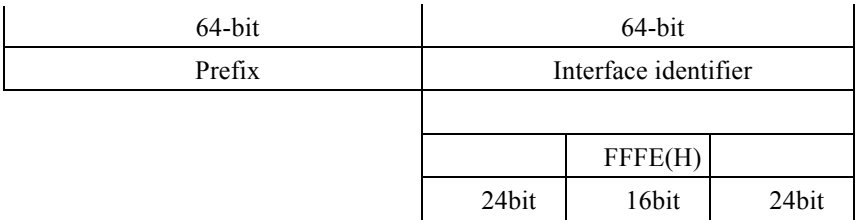

Fig. 3. 16-bit short address conversion format

A complete address automatic configuration scheme requires the prefix and the interface identifier two parts to complete. For the link local address, address automatic configuration scheme is relatively simple. Only by adding the link local address prefix FE80:: /64 in front of the converted interface identifier can it complete automatic configuration of the entire link local address.

Header compression:

The address is judged by implanting the GL bit in the identification bit. When the address type is a local link address, the IIPHC1 compression scheme is implemented, and the specific encoding format is shown in figure 4.

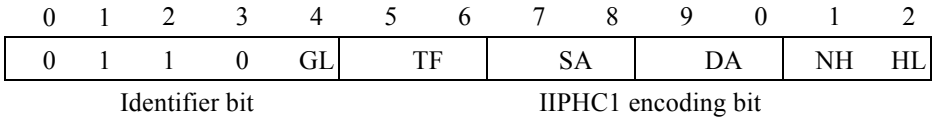

Fig. 4. IIPHC1 encoding format

The meaning of the field is as follows:

- 0110: refers to that the address type is IPv6 address, which is the address type that the GL bit common identifier needs to compress.
- GL (Global/Local: global/local link address identifier bit. In the scheme, GL=1, which indicates that the address type is local link address.
- TF (Traffic Class/Flow Label: Traffic class and flow label compression bit. Since that 8-bit IPv6 traffic class field are made up of 2-bit ECN(Explicit Congestion Notification) field and 6-bit DSCP(Differentiated Services Code Point) field, define the TF code as follows:
  - 00: traffic class and flow labels hold the default value;
  - 01: ECN and flow labels hold the default value and DSCP is omitted;
  - 10: traffic class hold the default value and the flow label is omitted;
  - 11: traffic class and flow label are omitted.
- SA (Source Address: source address compression bit)
  - 00: address prefix and interface identifier are not compressed;
  - 01: address prefix is not compressed, but the interface identifier is compressed;
  - 10: address prefix is compressed, but the interface identifier is not compressed;
  - 11: both of address prefix and interface identifier are compressed.
- DA (Destination Addresses: destination address compression bit
  - 00: address prefix and interface identifier are not compressed;
  - 01: address prefix is not compressed, but the interface identifier is compressed;
  - 10: address prefix is compressed, but the interface identifier is not compressed;
  - 11: both of address prefix and interface identifier are compressed.
- NH (Next Head: the next head compression bit)
  - 0: 8-bit next head field is not compressed;
  - 1: 8-bit next head field is compressed, and related next head compression algorithms are used;
- HL C Hop Limit: hop limit compression bit
  - 0: hop limit field is not compressed;
  - 1: hop limit field is compressed and the maximum of the hop limit field is 640

4 Results

C++ is used to compile a 6LoWPAN module, and it is embedded into the OMNeT++ simulation software Mobility Framework(MF) module, and the MF module contains IEEE 802.15.4 protocol. In the area of 40m*40m, 50 common nodes and 1 Sink node are arranged to demonstrate the effectiveness of the addressing strategy, in which the simulation settings parameters are shown in table 1.

Table 1. Simulation parameters

Parameters	The set value
The physical layer/ the link layer	IEEE802.15.4
Network adaptation layer	6LoWPAN
Maximum data packet size	90bytes
Network range	40m*40m
Simulation time	30min
Data flow type	CBR

The effectiveness of IOTAA address automatic configuration scheme is verified by two performance metrics: network overhead and time delay.

For the network overhead, simulation results of IOTAA, CCAA and Strong DAD are carried out on the simulation platform. In this study, the measure standard of network overhead is not the amount of energy consumed by the system in the implementation of the scheme, but by the number of message packets generated by the implementation of the scheme. Because in the underlying network of Internet of things, reducing the number of receiving and sending messages in the communication process is of great significance to reduce the energy consumption of the network. Figure 5 compares the network overhead of the three schemes: in Strong DAD scheme, when the number of underlying network nodes increases, the probability for each node random selection of address conflict increases, which needs more messages packet forwarding to alleviate the effects of address conflict brings, so the number of message packets show the exponential growth; CCAA scheme, because of using Trichromatic coordinates and node location information to achieve IPv6 address automatic configuration, compared with Strong DAD scheme, has been improved greatly; while the number of message packets of IOTAA in the 50 node case is within 200. On the one hand, it is because that the logic tree structure used reduces the virtual neighbor solicitation message forwarding range of duplicate address detection in IOTAA; on the other hand, because the network is not all network nodes needing access to the IPv6 global routing prefix for data forwarding and communication, it achieves better results than Strong DAD and CCAA.

The system throughput and RTT (Round-Trip Time) two performance metrics are used to verify the effectiveness of the IIPHC compression scheme.

In terms of system throughput, the HPHC scheme proposed in this paper is compared with the HC1 scheme in RFC4944 and the IPHC scheme in RFC6282 by simulation experiments. Figure 6 shows the average throughput of the system of the three

compression schemes as the data load increases. It can be seen from figure 6 that, because the HPHC scheme adopts a hybrid head compression scheme through judging the compression address type, the data load after HPHC scheme compression, compared with HC1 and IPHC scheme, made improvement about 30%^-60% in terms of throughput, which is one of the important advantages of IIPHC compression scheme.

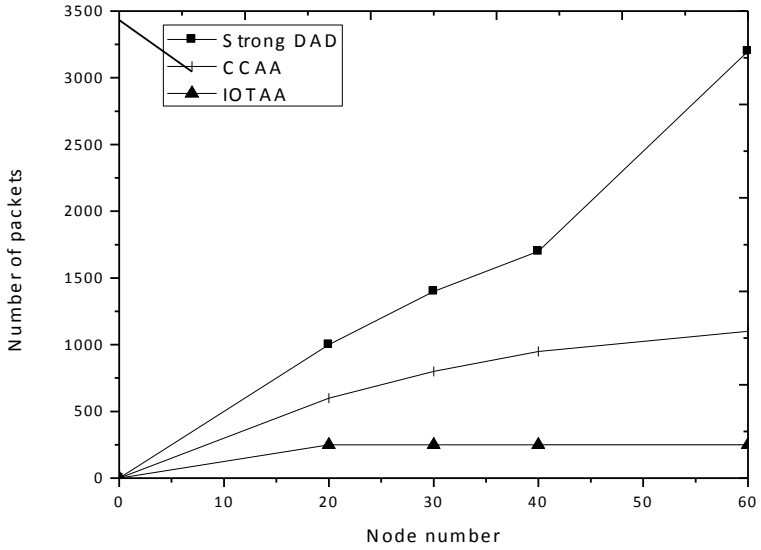

Fig. 5. Addressing strategy address automatic configuration network overhead comparison

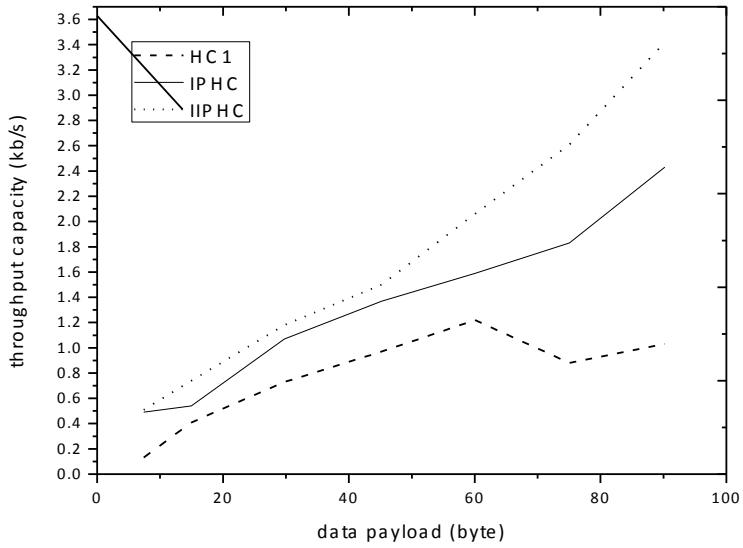

Fig. 6. Addressing strategy head compression throughput comparison

In RTT, through the comparison between HC1 and IPHC, the validity of the HPHC scheme in round-trip time is verified. As can be seen from table 2, the IIPHC uses less time on average round-trip delay and standard deviation. Compared with HC1 and IPHC, RTT needed for the implementation of HPHC scheme reduces about 50% and 25%, respectively. The simulation results show that the implementation of IIPHC scheme saves node storage space and reduces the system network overhead, and at the same time, it reflects the correctness of throughput performance index improvement.

Table 2. RTT comparison data

	The maximum RTT	**The minimum RTT**	**The average RTT**	**The standard deviation**
HC1	1.20	0.07	0.15	0.08
IPHC	1.08	0.05	0.07	0.07
IIPHC	1.11	0.01	0.05	0.05

Through the comparison simulation experiments of the addressing strategy IOTAA + IIPHC proposed in this paper with the addition of two kinds of combined addressing strategy StrongDAD + HC1 and CCAA + IPHC, we verify the energy efficiency of the proposed strategies in addressing in node transmission of IPv6 grouping process. As can be seen from figure 7 that, with the increase of the number of bytes of data load, the energy consumption of the addressing strategy proposed in this paper shows a linear growth, but it is always maintained in the order of 10-1mJ, and even if the transmission load reaches a maximum of 90 bytes, the energy consumption will remain within 1 mJ. StrongDAD +HC1 and CCAA + IPHC addressing strategy, with increased data load, the energy consumption is significantly higher than the addressing strategies proposed in this paper. As a result, the improved addressing strategy reduces the network energy consumption, and plays a certain role in reducing energy consumption for large-scale application of the underlying network of Internet of things.

5 Conclusion

The technical challenges of applying IPv6 address in the future Internet of things are analyzed, and the addressing strategy suitable for the underlying network is put forward to expand to Internet of things. In addition, two effective solutions are proposed, and the network layer provides simple and flexible, unconnected, and reliable grouping service to the transport layer. As a result, the MAC layer does not need to consider how the physical layer to realize the details of bit transmission. The simulation results show that the proposed addressing strategy has the characteristics of effectively integrating heterogeneous networks, reducing system energy consumption, increasing network throughput and ensuring real-time system performance for the future Internet of things. However, there are still many uncertainties in the large-scale application of the Internet of things, and the relevant key technologies are remained to be broken through.

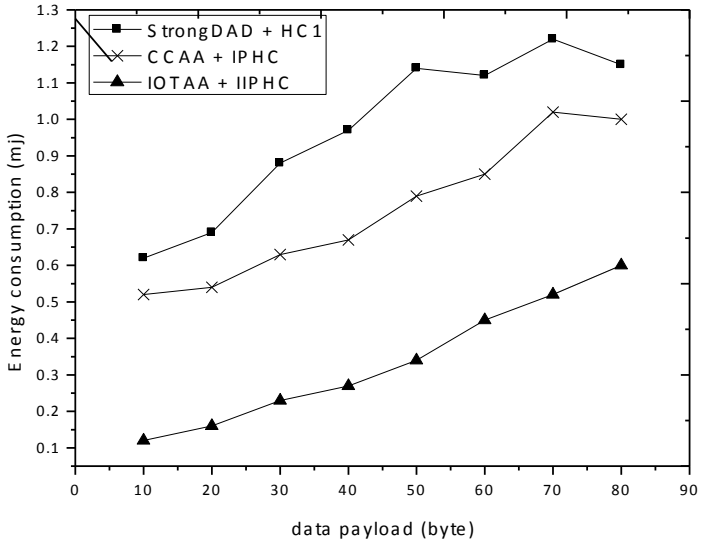

Fig. 7. 3 kinds of addressing strategies energy comparison

6 References

[1] Fabre, A., Martinez, K., Bragg, G.M., Basford, P.J., Hart, J., Bader, S. and Bragg, O.M., 2016, November. Deploying a 6LoWPAN, CoAP, low power, wireless sensor network: Poster Abstract. In Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM (pp. 362-363). ACM. https://doi.org/10.1145/2994551.2996707

[2] Raza, S., Duquennoy, S., Höglund, J., Roedig, U. and Voigt, T., 2014. Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN. Security and Communication Networks, 7(12): 2654-2668. https://doi.org/10.1002/sec.406

[3] Fabre, A., Martinez, K., Bragg, G., Basford, P., Hart, J., Bader, S. and Bragg, O., 2016. Deploying a 6LoWPAN, CoAP, low power, wireless sensor network.

[4] Liu, Y., He, Y., Li, M., Wang, J., Liu, K. and Li, X., 2013. Does wireless sensor network scale? A measurement study on GreenOrbs. IEEE Transactions on Parallel and Distributed Systems, 24(10): 1983-1993. https://doi.org/10.1109/TPDS.2012.216

[5] Gutiérrez, J., Villa-Medina, J.F., Nieto-Garibay, A. and Porta-Gándara, M.Á., 2014. Automated irrigation system using a wireless sensor network and GPRS module. IEEE transactions on instrumentation and measurement, 63(1): 166-176. https://doi.org/10.1109/TIM.2013.2276487

7 Authors

Yuan-kun Yang (corresponding author) is with Kunming Metallurgy College, Kunming, China (18288729590@sohu.com).

Yong-qing Ji is with is with Kunming Metallurgy College, Kunming, China.

Article submitted 23 May 2017. Published as resubmitted by the authors 27 June 2017.