Hasani *et al. EURASIP Journal on Wireless Communications and Networking* 2013, **2013**:54
http://jwcn.eurasipjournals.com/content/2013/1/54

EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Collaborative routing and data delivery architecture for commercial wireless sensor networks

Bilal Hasani[1,3], Saima Zafar[2,3*], Ali Hammad Akbar[3] and Babar Ali Magsi[4]

Abstract

Lately, wireless sensor network applications have emerged for provision of commercial services to end users. This results in commercial deployment of sensor networks which is as an important research area due to a number of design and quality of service challenges. An important technical challenge for sensor service provision to end users is managing dynamic network conditions such as unreliability of sensor nodes and network links which results in frequent service outages. This research is aimed at addressing this challenge. It presents a novel architecture which utilizes the availability of multiple sensor networks under different administrative domains, deployed in an area such that maximum network connectivity and high service availability are ensured. The architecture incorporates modifications and enhancements at the medium access control and the routing layers of sensor nodes for the collaborative operation of sensor networks. The design is based on IEEE 802.15.4 standard and ad hoc on demand distance vector routing protocol. The proposed architecture is mathematically analyzed with regards to overheads associated with the design such as routing and communication, and techniques to minimize these overheads are recommended. Through simulations using OMNET++, we show that the proposed architecture effectively provides connectivity for disconnected nodes achieving an overall increase in throughput for all the cooperating networks.

Keywords: Collaborative routing, Architecture, Commercial sensor networks

1. Introduction

Low-rate wireless personal area networks (LR-WPANs) such as IEEE 802.15.4 typify the more generalized form of wireless sensor networks (WSNs) with their unique design space. These networks comprise small, low power, low cost, and multi-functional sensing devices working in collaboration for sensing and data delivery under robust network conditions. These features render the design of WSN challenging as compared to the conventional networks. The design requirements in WSN that have consistently been addressed by the research community are energy efficiency, scalability, and adaptability to varying network conditions such as unreliable sensor nodes and flaky communication links. The design is also influenced by the type of sensing application and its specific demands. Lately, bulk manufacturing of inexpensive sensor node hardware has resulted in commercial deployment of these networks in order to provide on-demand sensor services to end users. Analogous to the fast proliferation of cellular network services to end users owing to mass production of low-cost mobile handsets, we anticipate swift commercial deployment of sensor networks for sensor services in the near future because research efforts are now rapidly directed towards designing concurrent applications for sensor networks and technical support for commercial sensor services [1-6].

Various experimental or commercial sensor networks that have been deployed lately support applications like vehicle tracking, industrial surveillance, home automation, seismic activities monitoring, remote health monitoring for patients, and even wildlife tracking. Similar to the simultaneous co-existence of multiple cellular networks in the same coverage area with distinct, at times overlapping clientage, it is expected that in near future multiple sensor networks with different sensing capabilities would co-exist

---

* Correspondence: saima_zafar@yahoo.com
[2]Department of Electrical Engineering, National University of Computer and Emerging Sciences, Lahore, Pakistan
[3]Al-Khwarizmi Institute of Computer Science, University of Engineering & Technology, UET, Lahore, Pakistan
Full list of author information is available at the end of the article

in the same area. This anticipated scenario opens a new research dimension concerned with the co-existence of multiple sensor networks in the same geographical area which is maintaining quality of service for commercial users in the presence of link outages and limited resources. As of now, the research efforts directed towards addressing this issue remain insufficient. This mandates the attention and focus of the scientific community to design protocols and applications for co-existing sensor networks from the perspective of performance enhancement and reliability of services [1].

In order to minimize service outage, commercially deployed voice and data networks maintain backup links and hardware thus mitigating the effects of possible failure of primary links or hardware. Since the idea of multiple co-existing sensor networks is new, the contemporary failure resilience efforts in WSN are geared to provide similar forms of redundancy. However, such over-provisioned sensor networks remain vulnerable to unpredictable scope and gravity of failures, raising questions on the very viability of this approach. In this article, we present a collaborative routing and data communication architecture for co-existing sensor networks that aims to resolve network outage problems due to coverage holes and maintains symbiotic backup connectivity of participating networks. The architecture proposes modifications both at the medium access control (MAC) layer and the network layer of sensor nodes. MAC layer changes are required for managing traffic flows for shared channel communication while modifications in the routing protocol are necessary to maintain and collect important management information for co-existing sensor networks. We analyze the proposed design in terms of various associated overheads and show that the architecture achieves the desired objectives with an acceptable increase in overheads.

There are three basic design elements of the proposed architecture.

- *MAC layer design:* MAC layer algorithmic changes are required to realize native and foreign-channel access by multiple WSNs. A disconnected sensor node or even a group of such sensor nodes utilize the presence of other networks' nodes in its transmission range, communicating with them using certain channels. Algorithmic modifications are proposed in association procedure that allows native and foreign channel access and scheduling of nodes of co-existing sensor networks.
- *Routing protocol design*: Algorithmic changes are incorporated in the implementation of routing protocol in order to make multiple sensor networks mutually beneficial. The idea is to give sensor nodes the provision to employ nodes of other sensor networks for route discovery and data delivery.
- *Overhead modeling*: The proposed architecture is mathematically modeled in terms of energy overheads associated with MAC layer design and routing.

The remainder of the article is organized as follows. In Section 2, we discuss the related work. Section 3 defines the problem. In Section 4, we present comprehensive design of our proposed architecture. Section 5 presents mathematical analysis of proposed architecture in terms of various overheads. Section 6 presents simulation results using OMNET++. Finally Section 7 concludes the article.

2. Related work

The collaborative design of multiple sensor networks located in an area is a novel idea. Multi-application sensor networks and multi-channel communication, where a single WSN can switch channels for data communication, can be found in the literature. This concept forms the baseline implementation of our idea. We review the related work in this section. Multi-application WSN is a network formed by sensor nodes that are equipped with multiple sensors and different applications run over these nodes independently. The research work in this domain relates to the software design aimed at efficiently utilizing the hardware resources of a sensor node. In an earlier work [2], we presented the guidelines to bind multiple applications over a single sensor network at run time. The idea of virtual sensor network proposes virtualization of multiple applications running over a single sensor network [3]. Yu et al. [4] support concurrent application provisioning on a sensor network with an emphasis on over-the-air programming prospects. Mottola and Picco [5] propose a programming abstraction as a mean to support multiple applications over a single sensor network. Tsetsos et al. [6] discuss network architecture for sensor-based services and develop business model for such applications. Heinzelmanet al. [7] present middleware design to support multiple applications considering various real-life application scenarios. Bhattacharya et al. [8] present utility-based multi-application allocation and deployment environment as an integrated application deployment system for sensor network applications sharing the same infrastructure. Alomar and Akbar [9] propose a routing mechanism named “Carrefour Cast” that is based on aggregated ‘Route Requests’ and ‘Route Replies’ in order to decrease routing overhead in multi application set-up in multiple gateway environments. They optimize multiple applications provisioning by proposing network layer modifications.

In IEEE 802.15.4 standard, multi-channel communication is proposed for communication over multiple channels, and we use this design at the MAC layer in our proposed architecture for communication of co-existing

WSNs. Multi-channel communication is an established operational requirement in wireless ad hoc and sensor networks. Jain et al. [10] and Li et al. [11] present the idea of a dedicated control channel for negotiation of data channel access and synchronization for ad hoc networks. Ramakrishnan and Ranjan [12] present a sensor multi-channelMAC protocol for WSNs in a contention-based scheme that works with one control channel and eight data channels. MC-LMAC [13] is proposed for WSNs based on dedicated control channel but the goal is to maximize throughput using coordinated transmission over multiple frequency channels by scheduled access, where each sensor node is granted a timeslot and transmits without contention. Zhou et al. [14] propose multi-frequency MAC protocol for WSN viewed as one of the initial multi-channel MAC protocols designed for WSN. It is a slotted CSMA protocol where nodes contend for the medium before they transmit at the beginning of timeslot. Y-MAC [15] is another recently proposed multi-channel MAC protocol designed for WSNs that is based on scheduled access. Timeslots are assigned to receivers instead of senders and potential senders for the same receiver contend for medium at the beginning of each timeslot.

Recently, some researchers have investigated the usage of multiple channels to defy the limitations of single channel MAC protocols. In this regard, Ansari et al. [16] and Liu and Wu [17] designed a multi-radio MAC protocol, running on a sensor node platform equipped with two radio transceivers. This approach is economically unsuitable for WSNs due to an increase in hardware cost, battery consumption, and design complexity. Moreover, a multi-channel MAC protocol using single radio transceiver is fairly plausible since most commercial radio devices such as CC1000 [18] and CC2420 [19] provide programmable channel selection to support multiple channel operation.

3. Problem definition

WSNs are being deployed commercially for providing on-demand sensor services to end users. Consider an example scenario where three or more sensor service providers manage their sensor networks that are deployed for providing certain services. One of the networks provides area surveillance services for security the second network provides environmental monitoring services while third is a visual sensor network meant for providing images. If all of these networks happen to be co-located such that a number of nodes overlap, these networks are the potential candidates for implementing the collaborative design proposed in this study.

In commercial sensor networks discussed above, node or link failure results in performance degradation or loss of sensed data. These service outages may cause revenue loss for sensor network operator. Figure 1 shows three different sensor networks (in three different colors) operating with a flat multi-hop topology in the same region. These networks are managed by different network operators with independent sensing and data communication. The gateways operate as bridges between a sensor network and wired IP network. Figure 1 shows some isolated nodes and network portions not connected to the gateways. This undesirable situation is common in sensor networks where, with the passage of time, a properly deployed and fully connected network experiences network partitioning that result in unavailability of sensed data. A rudimentary solution is to deploy sensor network with high node density but it merely delays the occurrence of the problem. It results in redundancy of sensed data and excessive forwarding of packets in network which ultimately results in unnecessary energy expenditure reducing the life span of sensor nodes. This problem can be solved by utilizing the presence of multiple sensor networks deployed in the same region. Figure 1a shows logical connectivity of nodes and gateways and Figure 1b shows the physical layer

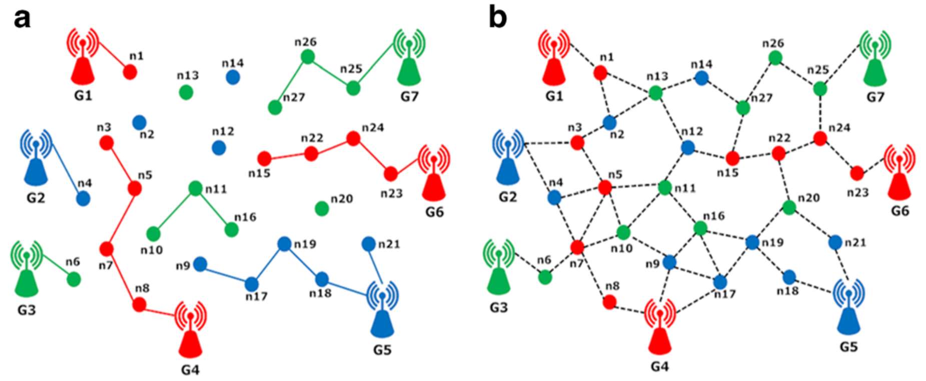


Figure 1 Connectivity between the nodes and their respective gateways and co-existing sensor networks showing physical layer visibility of sensor nodes.

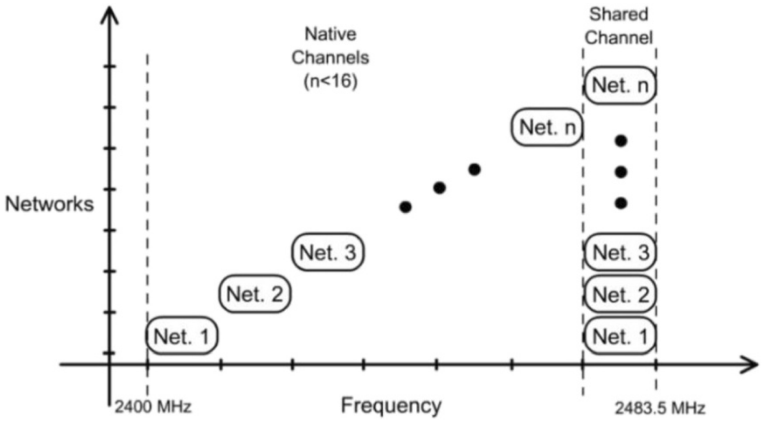


Figure 2 **Suggested channel allotment for co-existing sensor networks in 2.4-GHz ISM band.**

visibility of nodes (two nodes residing in each other's transmission range regardless of the network they belong to). In this study, we present a framework to utilize the presence of multiple sensor networks to solve the problems of network partitioning and node isolation.

4. Proposed architecture

In this section, we elaborate the architectural details of the framework by defining the design elements, making necessary assumptions, and giving details of the proposed MAC layer algorithm and routing protocol.

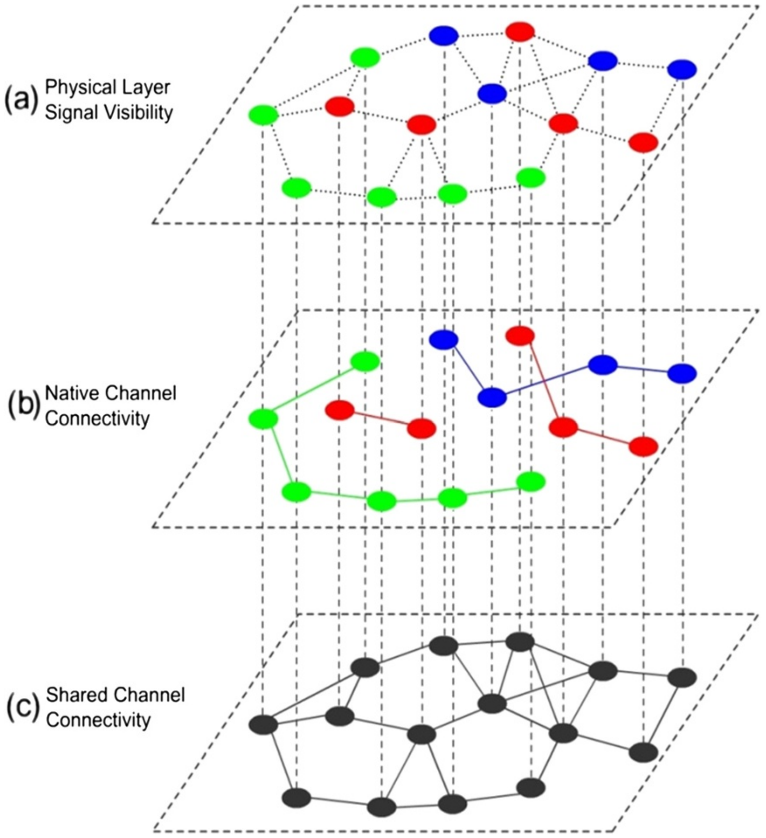


Figure 3 **Signal visibility, native, and shared channel connectivity of co-existing sensor networks.**

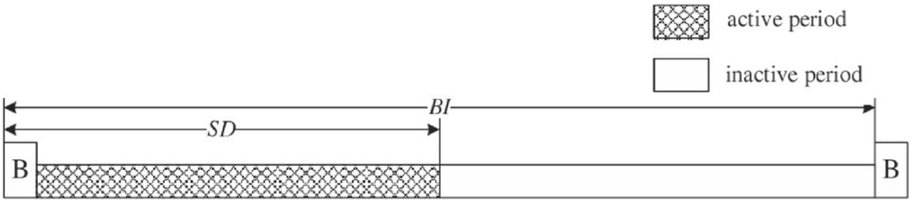


Figure 4 A simplified view of superframe structure in IEEE 802.15.4.

4.1 Design elements

The basic design considerations for cross-network communication from technical and economical viewpoints are as follows:

- The operator's first choice must be its home network, switching to cross-network communication only when home network is not available.
- The design must be mutually beneficial for all co-operating sensor networks. A sensor network offers routes to other networks while utilizing the routes through them for connectivity of its isolated nodes.
- The participation of nodes in cross-network communication must not be overwhelming compared to their participation in native network operations. There must be well-defined criteria to distinguish traffic these nodes carry for the native network from the cross-network traffic. Such criteria would ensure to limit packet processing at nodes that are not supposed to handle the cross-network traffic otherwise the design would not remain economically feasible for native network operations.
- The design must be transparent to the application and transport layer of nodes executing the applications.
- The new set of algorithms and protocols for cross-network communication must be based on existing standard protocols.
- The design must be simple to integrate medium access, routing and data delivery algorithms and protocols.

4.2. Design assumptions

The proposed architecture is based on few assumptions listed below.

- Sensor nodes operate in low duty cycle to save energy thus ensuring long network life.
- Each sensor network has gateway(s) and the data communication takes place between sensor nodes and gateway.
- We assume fixed channel assignment instead of dynamic channel assignment in sensor networks in order to minimize interference and reduce complexity.
- The data communication paradigm can be event based (triggered by sensor nodes) or on demand (triggered by gateways).
- The reconciliation of co-existing networks is managed through wired inter-connection in order to exchange information related to co-operative routing and data communication.

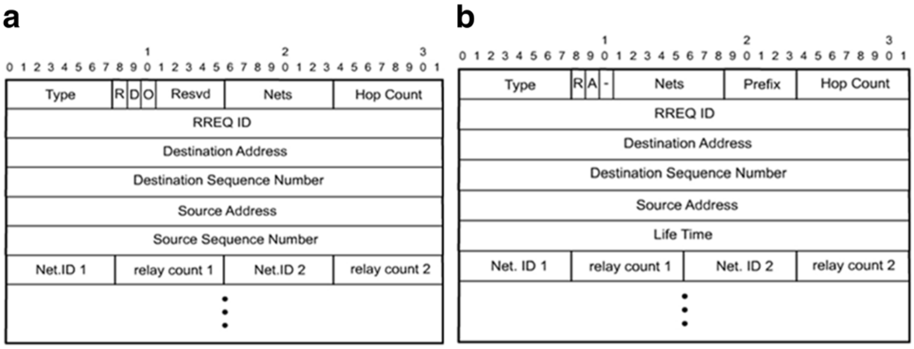
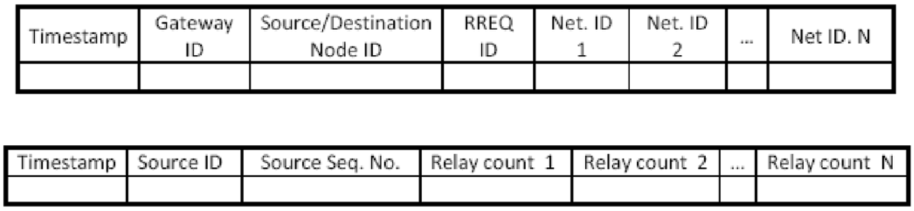


Figure 5 Modified AODV RREQ packet and modified AODV RREP packet.



Timestamp	Gateway ID	Source/Destination Node ID	RREQ ID	Net. ID 1	Net. ID 2	...	Net ID. N

Timestamp	Source ID	Source Seq. No.	Relay count 1	Relay count 2	...	Relay count N

Figure 6 RREQ database, and unicast database.

- The networks operate using non-overlapping addressing schemes such that a sensor node can identify a packet by the addressing scheme of source/destination.

4.3. MAC layer design

At the MAC layer, basic operation of IEEE 802.15.4 standard for LR-WPANs remains unchanged while algorithmic modifications and enhancements are incorporated in order to realize communication between different sensor networks. MAC Layer design is illustrated in the following sections.

4.3.1. Channel assignment for co-existing sensor networks

The sensor nodes operate in two logical channels, a native channel and a shared channel. The native channel is reserved for each sensor network and the shared channel is shared among all networks. A network uses the native channel for carrying out communication within the network while it switches to the shared channel for collaborative mode operation. The ISM band can accommodate up to 15 native channels belonging to 15 different networks and the remaining channel is used as shared channel as shown in Figure 2. As an example, consider three coexisting sensor networks (in three different colors) as shown in Figure 3 along with the resulting network configuration. The figure shows physical layer signal visibility, native channel connectivity, and shared channel connectivity of the three networks. The shared connectivity shows that all nodes belonging to different networks can communicate with each other as long as they are within the transmission range. The resulting network operating in shared channel is shown as a single big network with all nodes (in black color).

4.3.2. Implementation of shared channel connectivity

The implementation of shared channel connectivity requires smart engineering approach to utilize typically available hardware on sensor nodes and to avoid the need for additional hardware components. Our main goal is to enable each sensor node to operate in two logical networks. Given that sensor networks generally operate in the beacon-enabled configuration, it is possible to use a portion of inactive time of radio transceiver to switch to the shared channel. Thus, a single radio module can be used for multi-channel operation through scheduling. A simplified view of IEEE 802.15.4 super-frame structure is shown in Figure 4 displaying active and inactive periods bounded by beacon frames. The terms beacon order (BO) and super-frame order (SO) are used to describe configurations of active and inactive periods in a super-frame. We define duty cycle of super-frame as:

$$\text{Duty cycle} = \frac{\text{Active period}}{\text{Active period} + \text{inactive period}}$$

$$\text{Duty cycle} = \frac{\text{SD}}{\text{BI}} \tag{1}$$

where SD stands for super-frame duration and BI stands for beacon interval. Using expressions for SD and BI [20] we get

$$\text{Duty cycle} = \frac{A\text{ base superframe duration}*2^{\text{SO}}}{A\text{ base sulperframe duration}*2^{\text{BO}}}$$

$$\text{Duty cycle} = \left({}^{1}/{}_{2}\right)^{\text{BO}-\text{SO}} \quad (2)$$

In IEEE 802.15.4 standard [3], it is stated that SO and BO are selected based on the following equation $0 \le \text{SO} \le \text{BO} \le 14$. For energy-efficient operation, it is essential to maintain SO less than BO. If SO is less than BO by a minimal value of 1, the resulting duty cycle from Equation (2) is found to be 50%. The highest possible duty cycle with energy saving is 50% and that corresponds to the case when active period is equal to inactive period. Such a long inactive period can be utilized to schedule another instance of super-frame structure working independently to the already running super-frame. Such scheduling is achieved through *a priori* synchronization amongst the sensor networks such that the two super-frames operate in the two frequency channels independently, one in native channel and the other in shared channel. Every node, no matter to which native channel it belongs, switches to the shared channel and *expects* an orphaned message [19] from a disconnected node to arrive. A node disconnected from its native channel can now use the common channel to associate to such a node in order to establish a

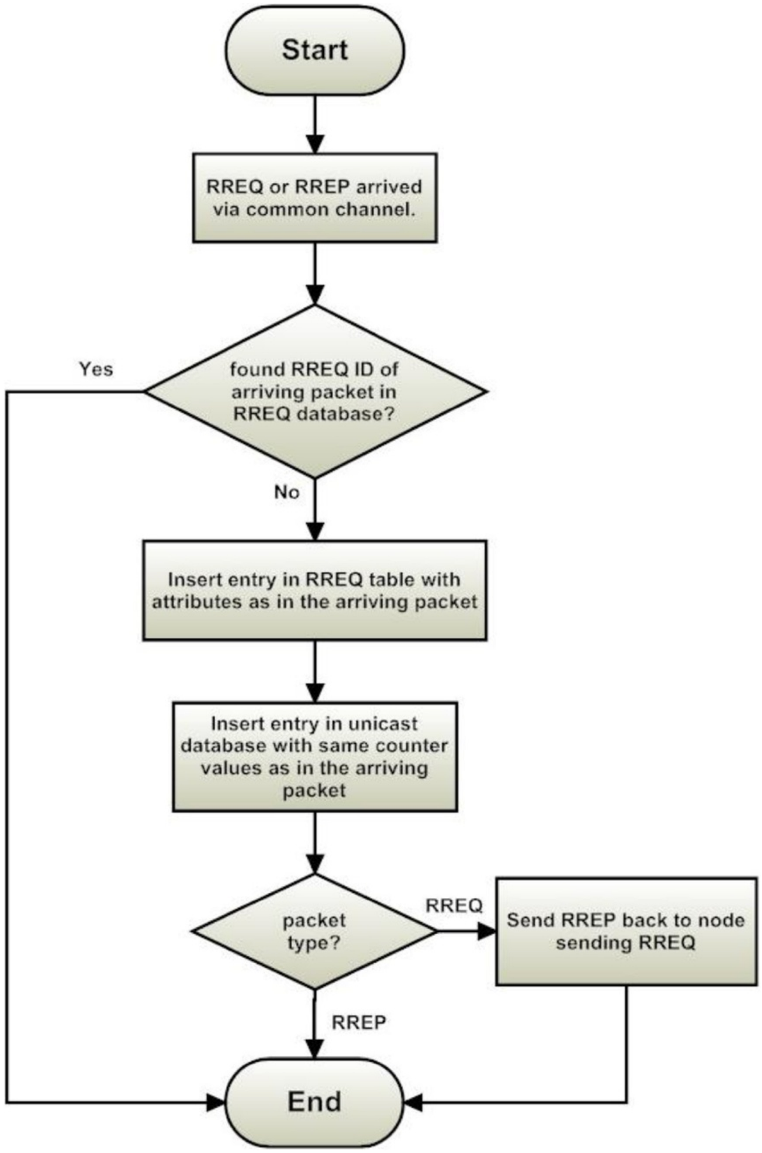


Figure 7 **Algorithm at gateway to handle RREQ or RREP.**

connection to its parent network. This connectivity is intermittent and persists only within the superframe duration. The disconnected node gets to access its respective gateway through such *borrowed* connectivity. This is a simple and low-cost approach to implement shared channel connectivity between nodes of co-existing sensor networks.

4.4. Routing protocol enhancements

The design of routing protocol is an important part of the proposed architecture because it deals with minimizing the routing overhead, ensuring end-to-end data delivery, and defining the rules of interaction among co-existing networks. The network layer enhancements are not concerned with routing engine but relate to the maintenance and aggregation of charging and billing information at each network provider's end. A sensor network first attempts to discover a route through its native channel. In case of success in route discovery through native network, assistance from co-existing sensor networks is not required. But when that fails, the sensor node or gateway switches to common channel for route discovery. The design of routing protocol accommodates billing and charging information in routing and data packets while keeping data and communication overhead as low as possible. Although we select ad-hoc on demand distance vector (AODV) routing protocol for the proposed enhancements due to its application in

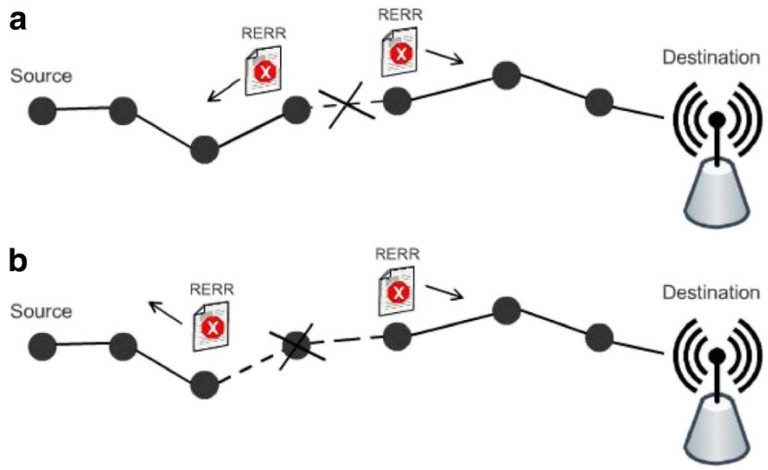


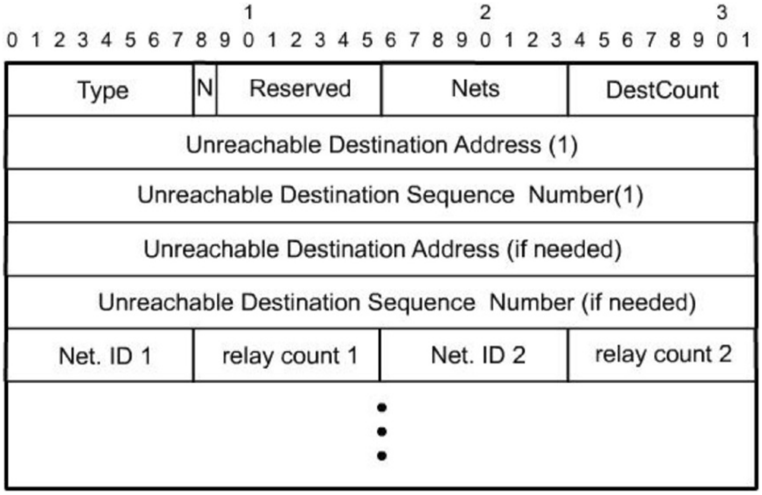
Figure 8 Route failure occurrence: (a) due to link failure, (b) due to node failure

sensor and ah-hoc networks but these modifications are simple and generic and can also be implemented in other routing protocols.

4.4.1. Route discovery

In AODV protocol, the route discovery process involves flooding of Route REQuest (RREQ) and unicast of Route REPly (RREP) to RREQ originator. The route discovery process for modified routing protocol is discussed as follows:

- *Route request:* The modified RREQ packet is shown in Figure 5a. The field 'Nets' is added before 'hop count', and 'trailer information' about contributing networks is appended at the end of the packet. 'Nets' represents the number of networks, other than native network that have forwarded the RREQ packet. If the packet is only processed by the native network (e.g., when packet is sent via native channel) the value in 'Nets' would be zero which means packet has no trailer information and is only using the native network resources. The trailer is appended to represent the networks that have forwarded the RREQ packet. Each network that forwards or broadcasts the packet inserts its unique 8-bit network ID and count of packet relay (8-bit "relay count" field). Thus, the 'Nets' value reports the number of exterior networks that participate in packet transmission and the trailer entries that are appended at the end of the packet provide information about those exterior networks.



Type	N	Reserved	Nets	DestCount
Unreachable Destination Address (1)				
Unreachable Destination Sequence Number(1)				
Unreachable Destination Address (if needed)				
Unreachable Destination Sequence Number (if needed)				
Net. ID 1	relay count 1		Net. ID 2	relay count 2
• • •				

Figure 9 Modified AODV RERR packet.

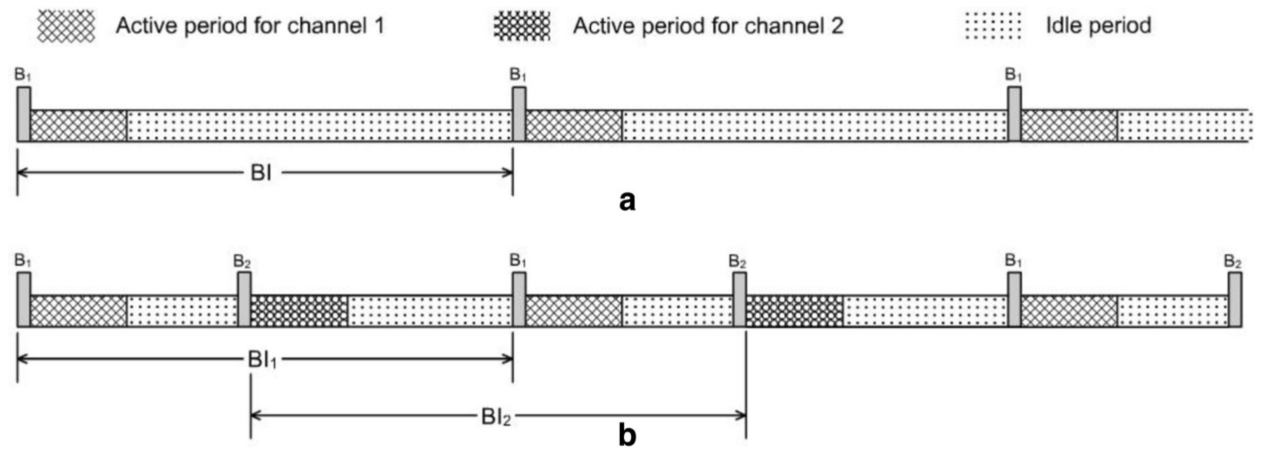


Figure 10 **Structure of super-frames: (a) for a standard design, (b) for proposed design.**

- *Route reply:* Route reply process is similar to the single sensor network route reply process with the same modifications as described in route request process. The role of 'Nets' value and packet trailer information is same as described in RREQ packet format and the packet format for RREP is shown in Figure 5b.
- *Algorithm at sensor node*: The sensor node runs an algorithm for common channel route discovery which is simple and is explained as follows:

  1. If a packet arrives through flooding and requires response, the sensor node sends response packet with 'Nets' field set to zero without any trailer information. An example of this case is the arrival of RREQ packet.
  2. If a packet arrives through unicast and requires response, the sensor node sends response packet with the same value of 'Nets' and trailer fields as in the arriving packet. This way the gateway is informed about the complete forwarding information of packet round trip. An example of this case is receiving data packet.
  3. RREP and ACK packets do not require response thus there is no special handling for these packets at the sensor node. Data packets are not part of the route discovery process and are discussed later.

4.4.2. Gateway functionality

The gateways are unconstrained devices in terms of resources and administer cross-network communication. The gateways play an additional role in the routing activity which is discussed in this section.

- Route discovery process
- During the route discovery process, the gateway tracks the record of relays by foreign network nodes through 'Nets' field, corresponding Net IDs and their relaying counter. Two possible scenarios in route discovery are:

  - If route discovery is initiated by sensor nodes, receiving gateway records external network relays listed in RREQ packet. The gateways distinguish RREQs by RREQ source address and RREQ ID. If RREQ is not already registered with gateway, it registers it in database and responds with RREP. If already registered, it updates the record. This gives an accurate measurement of reverse path and related data path cost.
  - If route discovery is initiated by either of the gateways, all gateways broadcast RREQ with same RREQ ID because destination node is unknown. The destination node responds to first arriving RREQ as per AODV, and RREQ corresponds to the path between node and closest gateway. The closest gateway notifies the originator gateway if it is not the originator of RREQ packet itself. RREP informs gateway about the cost of RREP.

- Management information sharing
- Each sensor network belonging to an operator is associated with a management and database server. The central database server is linked with each gateway and records attributes of the shared network resources. Individual database servers of each network operator are connected to the central database server in order to exchange pricing information. The gateway upon receiving a packet through shared channel updates its database server.

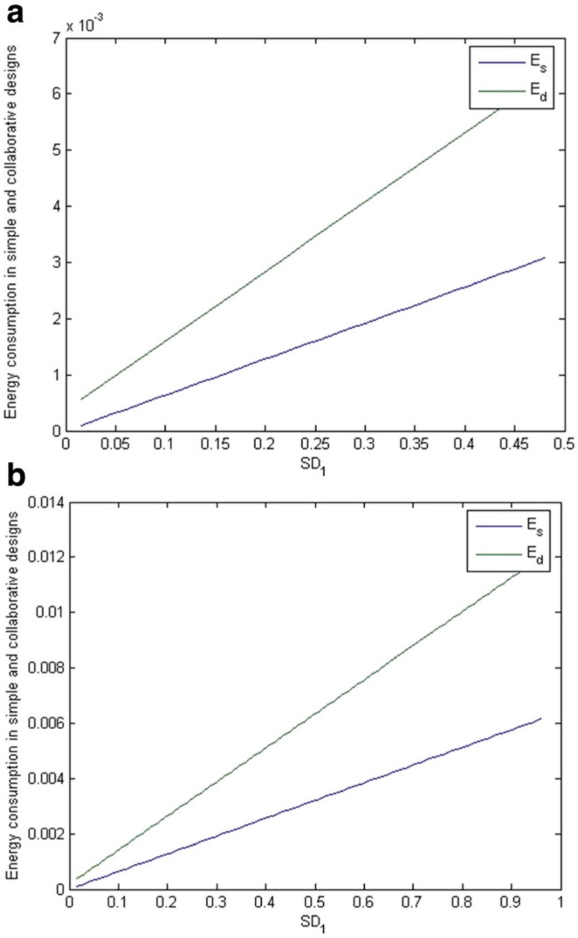


Figure 11 $E_s$and $E_d$versus SD_1: (a) SO for $SD_2 = 2$, (b) SO for $SD_2 = 1$.

These databases are RREQ database and unicast database (Figure 6). RREQ database records the arrivals of RREQ packets. A gateway may receive duplicate RREQ through different paths as a result of flooding but RREQ arriving through the shortest path is added in database after ensuring that RREQ is not registered at other gateways of the same operator. ‘Gateway ID’ is the destination address of the receiving gateway that responds to the RREQ through the shortest path. ‘Source Node ID’ is the ID of the node originating RREQ and ‘RREQ ID’ is the ID of the RREQ packet. Hop count is the minimum hop count value in arriving RREQs. ‘Relay count’ is the hop count in foreign networks identified through their respective ‘Nets’ fields (see Figures 5 and 6). For each arriving RREP or data packet, the gateway updates the unicast database for recording the cost of traversal. This method is useful for measuring the cost of transmission of packets in unicast since the exact number of forwarding by each network is retained in the packet. Figure 7 gives the algorithm at gateway to handle RREQ, RREP or data packets. The database information is periodically updated by individual database servers at the central database server for reconciliation of revenue based on predefined network resource sharing agreement.

4.4.3. Handling route errors

When there is a node or a link failure on an active route, route error messages are generated. Since communication is between sensor nodes and gateway(s), node or link failure results in loss of path originated or terminated at the gateway. The Route ERRor (RERR) message is generated to inform both ends of the ongoing session about error, as shown in Figure 8. RFC 3561 defines RERR packet format which includes information about all unreachable destinations. In shared channel operation, the cost of traversal of RERR is required. RERR packets are unicast packets and are handled in shared channel operation in a similar manner as RREQ or RREP. Figure 9 shows the modified AODV RERR packet for shared channel operation. In case

Table 1 Parameters for plots in Figure 11(SD_1versus$E_s$and SD_1versusE_d)

Parameter	Value
E_r	0.0123 J
BI	1.92 s (for BO = 7)
SD_1	(a) 0.015 s (for SO = 0) to 0.48 s (for SO = 5)
	(b) 0.015 s (for SO = 0) to 0.96 s (for SO = 6)
SD_2	(a) 0.06 (for SO = 2)
	(b) 0.03 (for SO = 1)

of link loss, two different RERR packets are sent on both sides of the point of failure. The gateway receives RERR packet through route still connected to it. In Figure 8, the route still connected to gateway appends 'network IDs' and relay count in the packet. The gateway retrieves information about contributions of networks still connected to it. But it is unable to estimate RERR forwarding going on the other side of route failure. This information is provided in RERR packet as addresses of unreachable nodes in the fields 'Unreachable Destination Address'. Since addressing of networks is non-overlapping and addressing schemes of

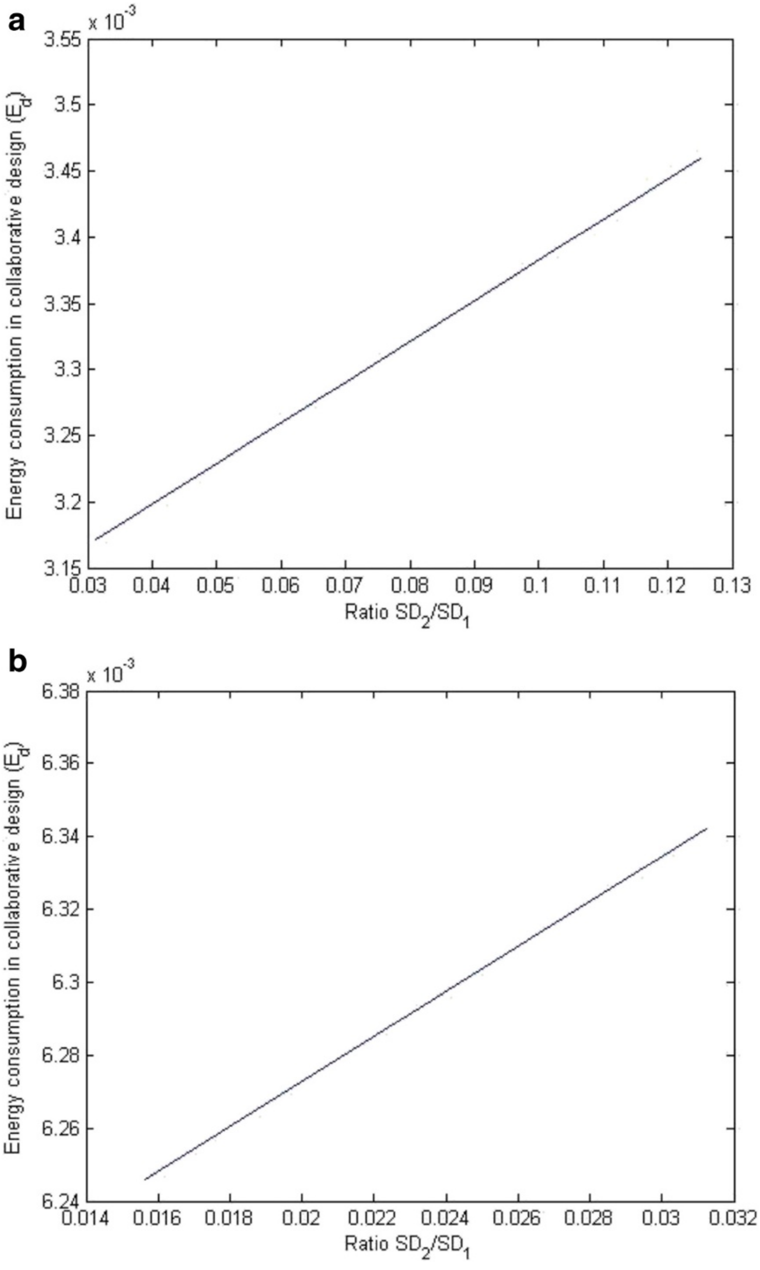


Figure 12 E_d**versus** SD_2/SD_{1c}**: (a) SO for** $SD_1 = 5$**, (b) SO for** $SD_1 = 6$**.**

Table 2 Parameters for plots in Figure 12(SD_2/SD_1versusE_d)

Parameter	Value
E_r	0.0123 J
BI	1.92 s (for BO = 7)
SD_1	(a) 0.48 s (for SO = 5)
	(b) 0.96 s (for SO = 6)
SD_2	(a) 0.015 s (for SO = 0) to 0.06 (for SO = 2)
	(b) 0.015 s (for SO = 0) to 0.03 (for SO = 1)

networks are known, the gateway can estimate the number of times RERR is forwarded by the exterior networks on the other side of route failure. Combining the information related to relay count and unreachable IDs of arriving RERR packet, the gateway inserts an entry in the unicast database for recording the cost of RERR packet.

4.4.4. Data delivery process

The data delivery process initiates after a route is established. To estimate the cost of data delivery in shared channel, modified header and trailer are used in combination with the underlying network layer protocol of sensor network. Traditional networks use Internet Protocol (IP) as the network layer protocol but it is highly inappropriate for sensor networks due to large packet overhead and many functions not required in sensor networks. IEEE 802.15.4 can handle a maximum payload of 127 bytes so smaller or compressed versions of headers are used at network layer. uIP [21] is an example of such IP version which can be modified to record number of contributing networks and their respective 'relay count' in common channel by using 'Nets' field in the header and trailer information. The algorithms given for sensor nodes and gateways for routing also apply to data packets.

5. Mathematical analysis

In this section, we mathematically analyze our proposed architecture. We estimate overhead due to MAC layer and routing layer enhancements for the framework which establishes two logical networks to which a sensor node belongs and evaluate additional costs associated with this collaborative design. Optimizations to minimize overheads are also suggested. The packet overhead associated with the collaborative design is also analyzed.

Table 3 Parameters for co-existing sensor networks

Parameter	Explanation
N	Total number of networks
n_j	Number of nodes of a sensor network
A	Area of deployment (in m^2)
ρ_j	Node density for a single sensor network (nodes per unit area)
r_o	Transmission radius of node (in meter)
λ_j	Average rate of route requests/node for sensor network

5.1. Overhead at MAC layer

The MAC layer design involves scheduling of two independent superframe structures at distinct frequency channels by the PAN coordinator so that the sensor network operates in two independent network topologies without interference and disruption. This scheduling of channels at the radio transceiver is shown in Figure 10. The superframe structure defines the portion of beacon interval when a node is active for transmission or reception. E_r represents the energy for keeping radio transceiver ON for a unit time including the cost of turning radio ON and OFF. In standard MAC design where SD_1 is superframe duration and BI is beacon interval, the standard energy consumption (E_s) is given as [add reference of standard IEEE802.15.4]:

$$E_s = E_r * \left(\frac{SD_1}{BI}\right) \tag{3}$$

Implementing the scheduling based approach as shown in Figure 10b, if SD_1 represents the first superframe duration and SD_2 represents the second superframe duration, the energy consumption in collaborative design E_d is given as:

$$E_d = E_r * \left(\frac{SD_1 + SD_2}{BI}\right) \tag{4}$$

The value of E_d in terms of E_s is

$$E_d = E_s * \left(1 + \frac{SD_2}{SD_1}\right) \tag{5}$$

The overhead factor between energy consumption in conventional sensor network design and our proposed design is SD_2/SD_1. Equation (5) shows that the energy overhead in collaborative design can be minimized by keeping SD_2 low. Although keeping SD_2 low causes reduction in throughput and increased transmission delay, nonetheless this may be an acceptable option considering the availability of a shared channel backup.

Figure 11 shows the variation of E_s and E_d with SD_1 based on Equations (3) and (4). The values of parameters for these graphs are given in Table 1. Figure 11a shows the variation of E_s and E_d with SD_1 when SO is set to 2 and Figure 11b shows variation of E_s and E_d with SD_1 when SO is set to 1. The energy consumption in collaborative design increases at a higher rate as compared to the single network operation however it can be controlled by varying the SO for SD_2. Figure 12 shows the plots of E_d versus SD_2/SD_1 based on Equation (5). The values of parameters for these plots are given in Table 2. In Figure 12a, SD_1 is

Table 4 Example of parameters of thee co-existing sensor networks

	Network 1	Network 2	Network 3
Number of nodes	70	75	60
Area (m^2)	100	100	100
Transmission radius (m)	1.5	1.5	1.5
Node density	0.7	0.9	0.6

set to 0.48 s based on SO = 5 and E_d is plotted for varying SD_2 (for SO = 0 to 2) and in Figure 12b, SD_1 is set to 0.96 s based on SO = 6 while SD_2 is varied (for SO = 0 to 1). The figure shows that the energy consumption in collaborative design increases with increasing second superframe duration as the nodes switch to the shared channel for a longer period.

5.2. Overhead at routing layer

In order to estimate routing overhead for the collaborative design, we assume 'N' number of sensor networks existing in an area where $N = 1, 2, 3, \ldots$, ρ = node density (nodes per unit area), r_o = transmission radius of nodes (in meters), A = area (in m^2) and n = number of nodes. The network parameters for co-existing sensor networks are listed in Table 3. When operating in shared channel, the effective node density of sensor network represented as ρ_{shared} is the sum of node densities of all networks, given as

$$\rho_{\text{shared}} = \sum_{k=1}^{N} \rho_k \tag{6}$$

The effective number of nodes of a network in shared channel is the sum of nodes of all networks, given as

$$n_{\text{shared}} = \sum_{k=1}^{N} n_k \tag{7}$$

The probability of graph connectivity for shared channel operation is computed in [22] as follows:

$$P(\text{connected}) = \left(1 - e - \frac{{}^{n}\text{shared}\pi {r_o}^{2}}{A}\right)^{n_{\text{shared}}} \tag{8}$$

If area and transmission radius remain constant, increasing the number of nodes results in improved connectivity. It is clear from (8) that in shared channel connectivity, the effective number of nodes is large and the probability of connectivity is close to 1.

As an example, consider three sensor networks in a region carrying out shared channel communication with network parameters given in Table 4. Using (8) and Table 4, the connectivity probabilities (probability of connected graph) for each network are

$$\begin{aligned} P(\text{connected})_{\text{Net.1}} &= \left(1 - e^{-\rho\pi {r_o}^{2}}\right)^{n} = 0.6073812 \\ P(\text{connected})_{\text{Net.2}} &= 0.6874498 \\ P(\text{connected})_{\text{Net.3}} &= 0.4190625 \end{aligned} \tag{9}$$

When a network switches to a shared channel communication, the effective number of network nodes is the sum of nodes of all networks, i.e., 205. The graph between connectivity and number of nodes (Figure 13) shows that connectivity probability is almost 1 for 205 nodes while it is more than 0.95 for 100 nodes. The graph shows that reasonable connectivity can be maintained with lesser number of co-operating nodes.

We know that on-demand routing protocols are based on flooding of route request while resulting route reply arrives as unicast. Consider a network, let n_j be the

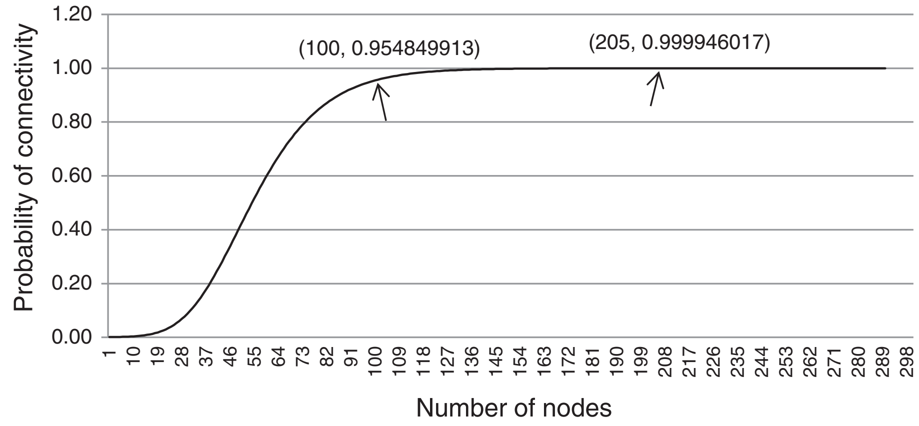


Figure 13 Connectivity probability for shared channel operation for $r_o = 1.5$.

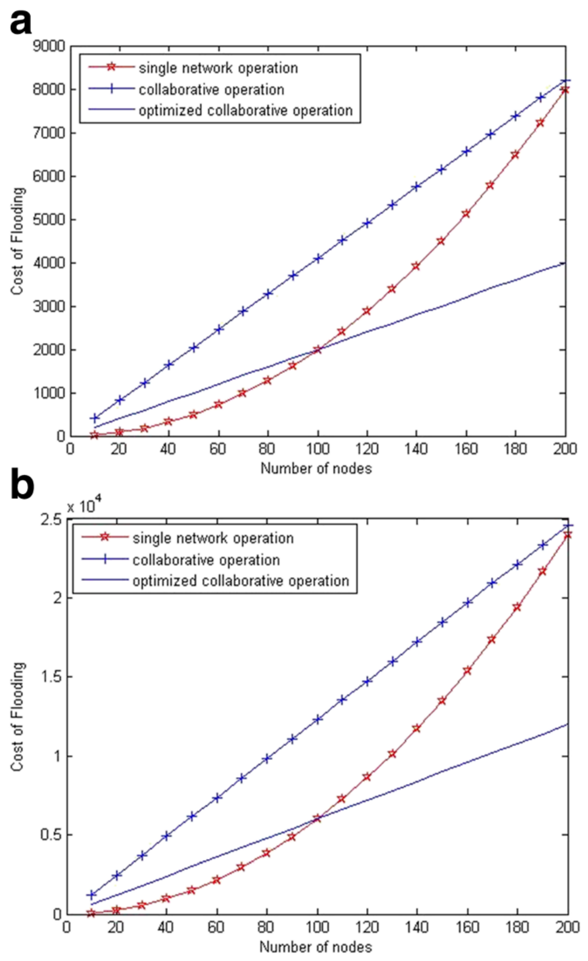


Figure 14 Cost of flooding versusnumber of nodes for single network operation, collaborative operation, and optimized collaborative operation: (a) average rate of route requests (λ) = 20%, (b) average rate of route requests(λ) = 60%.

number of nodes where $j < N$ and λ_j is the average rate of route request generation for each node. The total number of route requests generated per second in the network are $n_j{}^*\lambda_j$. During flooding, each route request is processed and forwarded by each node once. The cost of flooding represented as C_f during the routing process is given in [23] as follows:

$$C_f = \lambda_j * \mathsf{n_j}^2 \tag{10}$$

If the sensor network operates in shared channel, the total number of route requests generated remains the same but the number of nodes that receive and forward route requests is equal to the sum of nodes of all co-existing sensor networks denoted by n_shared. The cost of flooding per second for shared channel represented by C_f' is given as follows:

$$\begin{aligned} C'_f &= \lambda_j * \mathsf{n_j} * \mathsf{n_{shared}} \\ C'_f &= \lambda_j * \mathsf{n_j} * \sum_{k=1}^{\mathsf{N}} \mathsf{n_k} \end{aligned} \tag{11}$$

The factor of summation in (11) can be split as follows:

$$\begin{aligned} C'_f &= \lambda_j * \mathsf{n_j} * \left(\mathsf{n_j} + \sum_{k=1}^{\mathsf{N}} \mathsf{n_k} \right), \quad \forall \mathsf{k} \neq \mathsf{j} \\ C'_f &= \left(\lambda_j * \mathsf{n_j}^2\right) + \left(\lambda_j * \mathsf{n_j} * \sum_{k=1}^{\mathsf{N}} \mathsf{n_k} \right), \quad \forall k \neq j \\ C'_f &= C_f + \left(\lambda_j * n_j * \sum_{k=1}^{N} n_k \right), \quad \forall k \neq j \end{aligned} \tag{12}$$

Equation (12) shows that $\lambda_j * n_j * \sum_{k=1}^{N} n_k$ is an additive overhead factor as compared to overhead in normal flooding. Thus, routing overhead which corresponds to flooding by nodes of all co-existing networks is excessively increased. The flooding cost for nodes of recipient network is not much increased but the co-existing networks receive a large number of packets to be forwarded. This analysis reinforces the routing overhead conclusion drawn earlier where Figure 13 shows that having too many nodes in an area does not improve connectivity as connectivity probability saturates beyond a particular node density.

5.2.1. Routing overhead optimization

In this section, we propose an optimization of routing overhead by employing stochastic forwarding or gossiping [24]. It is a simple method to reduce flooding overhead due to uncontrolled forwarding in route discovery. In a typical flooding-based route discovery, each node forwards route request exactly once. In gossiping, each node is assigned a forwarding probability P_g which is less than 1 and set to maintain maximum connectivity with least packet forwarding. Assigning P_g is challenging in dynamic network conditions. When employing gossiping in shared channel communication, the network operators must agree upon a base value of shared channel connectivity in order to find the number of nodes required to achieve this connectivity. From Figure 13, we observe that the number of nodes required to achieve a connectivity probability of 0.95 is 100. The forwarding probability is set by each network based on the number of its nodes and the total number of nodes of all networks. We assume that all networks contribute the same number of nodes for route discovery. Let P_r be the probability of connectivity required for shared channel connectivity and n_r be the number of nodes required to attain P_r. There are N networks and n_j number of nodes of jth network where $1 \le j \le N$. Our design

Table 5 OMNET++ simulations setup

Parameter	Explanation
Standard	IEEE 802.15.4
Total number of sensor networks	4
Terrain (area)	1000 × 1000 m^2
Number of nodes in area	60
Number of nodes in observed network	32
Simulation time	100 s

requires each network to participate equally so a gossiping probability of $P_{j(g)}$ which is given as follows:

$$P_{j(g)} = \frac{n_r}{n_j * N} \quad \text{for} \;\; n_r \le \left(n_j * N\right) \tag{13}$$

The validity condition for (13) is $n_r \le (n_j * N)$. If this condition is not satisfied for a network, it is unable to carry out shared channel communication due to less number of nodes. Due to node failure, the number of nodes associated with a network may decrease with time therefore n_j must represent the active number of network nodes at a given time in the calculation of gossiping probability. The network that satisfies this condition has dense node deployment and less gossiping probability which results in minimizing routing overhead and consequently energy consumption. For gossiping in common channel, the cost of flooding represented in (11) is

$$\text{Cost of flooding for shared channel with gossiping} = \lambda_j * \mathrm{n_j} * \sum_{\mathrm{k}=1}^{\mathrm{N}} \mathrm{P_{k(g)}} * \mathrm{n_k} \tag{14}$$

If the networks have an agreement on connectivity probability of 0.95 with 100 nodes, assuming all nodes of networks as active, the gossiping probability for each network using (13) is computed as follows:

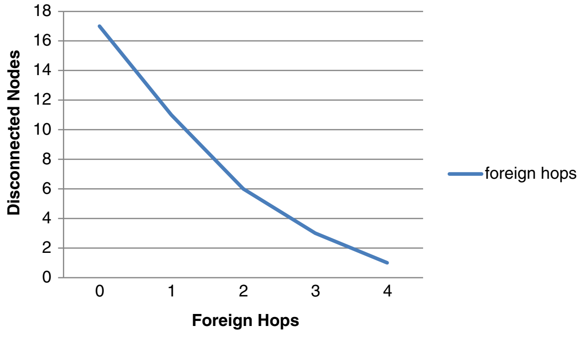


Figure 15 Number of foreign hops versus number of disconnected nodes.

$$P_{1(g)} = \frac{100}{70*3} = 0.4762$$

$$P_{2(g)} = \frac{100}{75*3} = 0.4444$$

$$P_{1(g)} = \frac{100}{60*3} = 0.5556$$

To verify required connectivity, the effective number of nodes in shared channel communication using gossiping is

$$n_r = P_{1(g)} * \mathrm{n_1} + \mathrm{P_{2(g)}} * \mathrm{n_2} + \mathrm{P_{3(g)}} * \mathrm{n_3}$$

$$n_r = 0.4762*70 + 0.4444*75 + 0.5556*60$$

$$n_r = 33.334 + 33.33 + 33.336$$

$$n_r = 100$$

This shows that all networks participate equally in terms of the effective number of nodes for gossiping-based shared channel connectivity. Gossiping results in reducing the number of nodes forwarding RREQ packets from 205 to 100 which reduces the cost of route discovery process thus minimizing routing overhead associated with shared channel communication.

Figure 14 shows the variation of cost of flooding with increasing number of nodes for single network operation, collaborative operation, and the optimized collaborative network based on Equations (10), (11), and (14). The gossiping probabilities for the three networks are as computed above and the network parameters as given in Table 4. The figure shows that for a given average rate of route request generation by the nodes, the cost of flooding for a single network operation varies exponentially while the cost of flooding for the collaborative operation increases linearly however when routing overhead is optimized using the gossiping technique the cost of flooding increases at a slower rate. This shows that the collaborative design with routing overhead optimization is feasible in terms of cost of flooding when compared with the single network operation.

5.3. Packet overhead

The proposed design for shared channel communication introduces additional fields in routing packets resulting in packet overhead. This increase is proportional to the number of networks contributing in forwarding of packet. If *P* bytes is the size of normal routing or data packet for traditional sensor networks and *P′* bytes is the size of routing or data packet for shared connectivity (both packets are considered to be the same size at the network layer for mathematical convenience), then

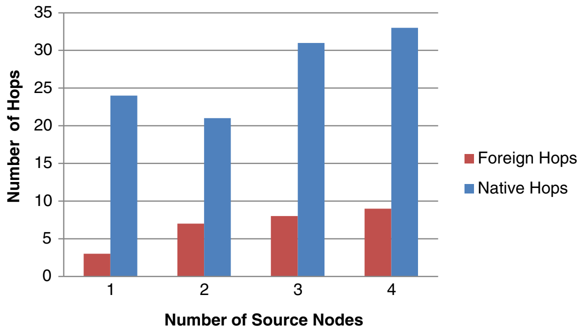


Figure 16 Number of source nodes versus number of foreign and native hops.

$$P' = P + \beta k \tag{15}$$

β is the number of bytes for representation of the ID of a particular network and its respective forwarding count in packet trailer. k represents the number of networks participating in packet forwarding, it is same as "Nets" value in packet and $0 \le k \le N - 1$, where N is the total number of participating networks. In our proposed design, 2 bytes are required for keeping the record of forwarding by a particular network (1 byte for network ID and 1 byte for forwarding count) therefore β is 2. A different value of β can also be used. The ratio $P\prime/P$ is given by the following expression:

$$\frac{P'}{P} = 1 + \frac{\beta k}{P}, \tag{16}$$

where $\beta k/P$ is the additive overhead factor and is inversely proportional to packet size in single sensor network operation. The selection of an appropriate packet size is an open research issue in sensor networks. A larger packet size reduces data overhead but is more susceptible to packet losses due to noisy medium. Maximum payload allowed in IEEE 802.15.4 is 127 bytes and it corresponds to minimum packet overhead based on (16).

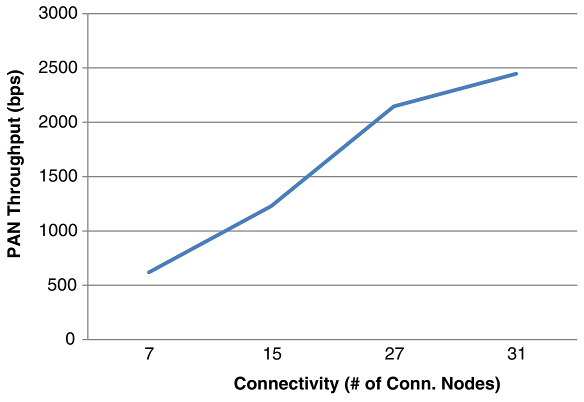


Figure 17 Connectivity (number of connected nodes) versus throughput of a single network.

6. Simulation results

This section presents the performance evaluation of our proposed architecture through OMNET++ simulations. First, we observe the impact of foreign network connectivity on disconnected nodes of a sensor network. Disconnected nodes are those nodes which disconnect from their native network due to link failures, etc. Another major focus of simulations is to evaluate the protocol in terms of number of foreign hops when number of source nodes is increased. The simulation setup details are given in Table 5. We simulate three sensor networks located in an area that are implementing our proposed design for collaborative routing and data transfer. We evaluate performance in a single network comprising of 32 nodes where with the passage of time, a number of nodes are disconnected from the network. If the number of foreign network hops were to become excessive as compared to native network hops especially when the number of disconnected nodes increases, it would be interesting to see if collaborative design stays efficient or not.

6.1. Impact of collaborative design on connectivity of nodes

It has been observed that in a WSN that is deployed in an area, the connectivity of sensor nodes declines with time due to mobility or link breakage which results in a number of disconnected or isolated sensor nodes. We evaluate our proposed design for this situation and observe the impact of foreign network collaboration on connectivity of the disconnected nodes. It is observed that as nodes start connecting to their sinks or base stations through available foreign network nodes in their radio range, the total number of disconnected nodes in a network start declining sharply. This can be observed through Figure 15 which shows that as number of foreign hops increase, number of disconnected nodes decreases. This is a favorable result which shows a sharp decline in disconnected nodes when collaborative design in implemented. When number of foreign hops increases linearly, number of disconnected nodes declines almost exponentially. We deduce that our proposed design gives excellent results and quality of service in terms of reducing isolated nodes while adding only a trivial amount of burden for the foreign networks involved in collaborative design.

6.2. Impact of number of disconnected nodes on performance of collaborative design

In this simulation, we are interested in examining the impact of number of disconnected nodes on the performance

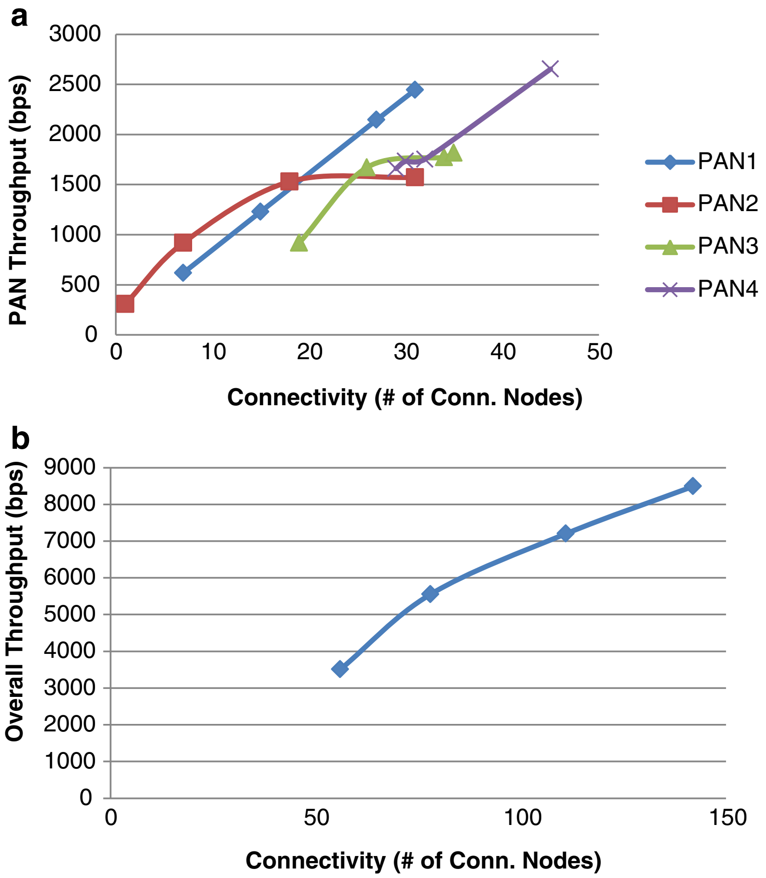


Figure 18 **(a) Connectivity (number of connected nodes) versus throughput of individual PANs and (b) connectivity (number of connected nodes) versus overall throughput of all collaborating networks.**

of the collaborative design. If number of foreign network hops becomes excessive as compared to native network hops especially when number of disconnected nodes increases, collaborative design would not be efficient and vice versa. Figure 16 shows that when disconnected nodes implement the collaborative design, the number of foreign hops is negligible as compared to native network hops and when the number of such disconnected nodes increases, this trend continues. This is an encouraging observation which shows that the collaborative design does not lose its aptness and effectiveness as the number of disconnected nodes increases.

6.3. Impact of collaborative design on throughput

The impact of the collaborative design on throughput of a single network or the overall throughput of all networks can be observed by observing the impact of connectivity of nodes on throughput. We simulated this scenario based on simulation parameters given in Table 5 and increased the connectivity of nodes while observing throughput of a single network. Figure 17 shows single network throughput versus connectivity, it can be observed that there is a considerable increase in throughput as the number of connected nodes increases but after a certain level of nodes connectivity which is around 85%, increase in throughput is not sharp. Figure 18 shows the overall throughput of all the shared networks versus connectivity. We simulate a shared network of four collaborating PANs which are isolated in the beginning but achieve connectivity through foreign network hops. We observe the impact of this connectivity on individual network throughput (Figure 18a) which shows that throughput is improved in all networks that achieve connectivity. We observe the impact of connectivity improvement on overall throughput of all networks as shown in Figure 18b which shows a steady improvement in cumulative throughput of collaborating networks.

7. Conclusion

Commercial sensor networks are aimed at providing persistent and stable sensor services to the end users. However, this type of service provision is negatively affected by the uncertain network conditions like node and link failures. This results in network partitions resulting in frequent undesirable service outages or unavailability of sensed data. In a scenario where multiple sensor networks overlap within a geographical area which may or may not be under the same administrative control, these networks could be enabled to utilize mutual resources in order to ensure desired network performance and quality of service. We presented a routing and data delivery architecture for mutually beneficial collaborative operation of commercial sensor networks with IEEE 802.15.4 and AODV as the building blocks. We conclude that collaborative operation of commercial sensor networks results in ensuring connectivity of isolated nodes and is mutually beneficial for all participating networks. We plan to take up pricing issues for the proposed collaborative design as future work.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]School of Electrical Engineering, KTH - Royal Institute of Technology, Stockholm, Sweden. [2]Department of Electrical Engineering, National University of Computer and Emerging Sciences, Lahore, Pakistan. [3]Al-Khwarizmi Institute of Computer Science, University of Engineering & Technology, UET, Lahore, Pakistan. [4]Department of Electrical Engineering, COMSATS Institute of Information Technology, Lahore, Pakistan.

Received: 7 April 2012 Accepted: 10 February 2013
Published: 28 February 2013

References

1. K Sohraby, D Minoli, T Znati, *Wireless Sensor Networks: Technology, Protocols, and Applications* (Wiley, New York, 2007)
2. AH Akbar, AA Iqbal, K Kim, Binding multiple applications on wireless sensor networks, in *Proceedings of the Grid and Pervasive Computing Conference (GPC '06)* (Lecture Notes on Computer Science 3947, Taiwan, 2006), pp. 250–258
3. P Jayasumana, Q Han, TH Illangasekare, Virtual sensor networks—a resource efficient approach for concurrent applications, in *Proceedings of the Fourth International Conference on Information Technology (ITNG '07)* (Las Vegas, 2007), pp. 111–115
4. Y Yu, LJ Rittle, V Bhandari, JB LeBrun, *Supporting concurrent applications in wireless sensor networks, Motorola Labs, Technical Report*, 2006
5. L Mottola, GP Picco, Using logical neighborhoods to enable scoping in wireless sensor networks, in *Proceedings of the 3rd International Middleware Doctoral Symposium (MDS '06)* (Melbourne, Australia, 2006), pp. 6–11
6. V Tsetsos, G Alyfantis, T Hasiotis, O Sekkas, S Hadjiefthymiades, Commercial wireless sensor networks: technical and business issues, in *Proceedings of the Second Annual Conference on Wireless onDemand Network Systems and Services (WONS '05)* (St. Moritz, Switzerland, 2005), pp. 166–173
7. W Heinzelman, A Murphy, H Carvalho, M Perillo, Middleware to support sensor network applications. IEEE Netw. Mag. **18**(1), 6–14 (2004)
8. S Bhattacharya, A Saifullah, C Lu, GC Roman, Multi-Application deployment in shared sensor networks based on quality of monitoring, in *IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS'10)* (Washington, DC, USA, 2010), pp. 259–268
9. A Alomar, AH Akbar, Carrefour Cast: A new routing protocol to support multiple applications in multiple gateway environments of wireless sensor networks, in *World Congress on Science, Engineering and Technology (WCSET '09)* (Singapore, 2009)
10. N Jain, S Das, A Nasipuri, A multichannel CSMA MAC protocol with receiver-based channel selection for multihop wireless networks, in *Proceedings of the 10th IEEE International Conference on Computer Communications and Networks (IEEE IC3N* (Phoenix, Arizona, USA, 2001), pp. 432–439
11. J Li, Z Haas, M Sheng, Y Chen, Performance evaluation of modified IEEE 802.11 MAC for multi-channel multi-hop ad hoc network, in *Proceedings of the 17th International Conference on Advanced Information Networking and Applications (AINA '03)* (Xi'an, China, 2003), pp. 312–317
12. M Ramakrishnan, V Ranjan, Multi channel MAC for wireless sensor networks. Int. J Comput. Netw. Commun. (IJCNC) **1**(2), 47–54 (2009)
13. OD Incel, L Hoesel, P Jansen, P Havinga, MC-LMAC: a multi-channel MAC protocol for wireless sensor networks. J Ad Hoc Netw. **9**(1), 73–94 (2011)
14. G Zhou, C Huang, T Yan, T He, JA Stankovic, TF Abdelzaher, A multifrequency MAC specially designed for wireless sensor network applications. ACM Trans. Embed. Comput. Syst. **9**(4), 1–41 (2010)
15. Y Kim, H Shin, H Cha, Y-MAC: an energy efficient multi-channel MAC protocol for dense wireless sensor networks, in *Proceedings of ACM/IEEE International Conference on Information Processing in Sensor Networks, (IPSN '08)* (St. Louis, Missouri, USA, 2008), pp. 53–63
16. A Ansari, X Zhang, P Mähönen, Multi-radio medium access control protocol for wireless sensor networks. Int. J Wirel. Sensor Netw. **8**(1), 47–61 (2010)
17. Z Liu, W Wu, A dynamic multi-radio multi-channel MAC protocol for wireless sensor networks, in *Proceedings of the Second International Conference on Communication Software and Networks, (ICCSN '10)* (Singapore, 2010), pp. 105–109
18. *"Chipcon, CC1000 Single Chip Very Low Power RF Transceiver", Datasheet.* http://focus.ti.com/lit/ds/symlink/cc1000.pdf
19. *"Chipcon, CC2420 2.4 GHz IEEE 802.15.4/ZigBee ready RF transceiver", Datasheet.* http://www.ti.com/lit/gpn/cc2420
20. Y Huang, A Pang, A comprehensive study of low-power operation in IEEE 802.15.4, in *Proceedings of the 10th ACM symposium on modeling, analysis, and simulation of wireless and mobile systems (MSWiM '07)* (Crete Island, Greece, 2007), pp. 405–408
21. A Dunkels, Full TCP/IP for 8-bit architectures, in *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services (MobiSys '03)* (San Francisco, USA, 2003), pp. 85–98
22. C Bettstetter, On the minimum node degree and connectivity of a wireless multihop network, in *Proceedings of the 3rd ACM International Symposium on Mobile AdHoc Networking and Computing (MobiHoc '02)* (Switzerland, 2002), pp. 80–91
23. P Jacquet, L Viennot, *Overhead in mobile ad-hoc network protocols, Institut national de recherche en informatique et en automatique (INRIA) Research Report* ((RR-3965, INRIA), Rocquencourt, France, 2000)
24. ZJ Haas, JY Halpern, L Li, Gossip-based ad hoc routing. IEEE/ACM Trans. Netw. **14**(3), 479–491 (2006)

doi:10.1186/1687-1499-2013-54
Cite this article as: Hasani *et al.*: Collaborative routing and data delivery architecture for commercial wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking* 2013 **2013**:54.