Experimental Validation of Opportunistic Direct Interconnection between different Wireless Sensor Networks

Krongboon Singhanat, Nick R. Harris, Geoff V. Merrett
Electronics and Computer Science, University of Southampton, UK SO17 1BJ
Email:{ks14g13,nrh,gvm}@ecs.soton.ac.uk

***Abstract*—Cooperation between Wireless Sensor Networks (WSNs) is needed in order to fully realise the vision for the Internet of Things (IoT). As endeavours towards IoT continue, compatibility and interoperability between distinctive networks in WSNs becomes crucial. However, considering the wide range of WSN applications, heterogeneity in the platforms and communication protocols in use is potentially unavoidable. To help integrate WSNs with IoT, this research studies a framework to enable Opportunistic Direct Interconnection (ODI) between distinctive WSNs. The interconnection of different WSNs, using different internal communication protocols, are practically validated with empirical experiments. ODI involves the addition of a lightweight shared protocol for interconnection between WSNs. The implementation confirms the feasibility of ODI as a practically obtainable system, and quantifies the low overheads in terms of memory and energy.**

I. Introduction

The vision for the Internet of Things (IoT) encourages interconnection and cooperation between separate systems. WSNs, which are constantly growing, can therefore be seen as a fundamental technology underpinning IoT. Therefore, collaboration between WSNs is gradually gaining attention in the research community, along with cooperation between heterogeneous systems in various communication technologies [1].

Typically, WSNs can be accessed through web services, provided by the front-end gateway [2], [3]. Hence, collaboration between WSNs can occur in the form of data exchange via web services, using Internet connections. Packet exchange via direct interconnection between co-located systems are infrequently considered or even possible because systems are conventionally designed to avoid interference, rather than promoting cooperation [4]. However, direct interconnection can offer an alternative channel for data exchange in absence of a backbone network. Futhermore, direct interconnection can support coooperation schemes to share network resources such as energy-trading to extend network lifetime, reconnecting of lost sections, or offering Internet connection to inaccessible areas [4]–[6].

Permitting interoperability between WSN systems across a range of applications is a considerable challenge for IoT. To counter this, there are suggestions to converge the differences between systems around the Internet standards [1], [3]. However, the full adoption of IP-based solutions in the context of WSNs are still under discussion for its necessity and efficiency [2]. Due to the different requirements and optimisations of target applications, and the future number of WSNs, the likelihood that local systems prefer their own native link protocol for internal communication remains considerable. Therefore, our research has studied a framework to establish direct interconnection between WSNs which engage in the collaboration but still maintain their selected link characteristics. This research follows the concept of Opportunistic Direct Interconnection (ODI) previously proposed in [4], [7]. This concept encourages collaboration between overlapping WSNs by enabling direct wireless connections between them.

The initial framework for ODI has been proposed and validated by OI-MAC [4], but this still requires WSNs to adopt OI-MAC as the only MAC protocol within the networks. In [7], the framework from ODI was updated to consider the heterogeneity of MAC protocols. While our previous work has validated OI-MAC experimentally [8].This new vision for heterogeneous ODI has only been evaluated through simulations.

In this paper, we report on the successful implementation and validation of ODI, enabling the interconnection of two distinctive networks, using different MAC protocols. One network using X-MAC and another network using RI-MAC are constructed with 12 eZ2500-RF2500 Texas instrument sensor nodes [9] to demonstrate communication across networks. The experimental results show that the memory overhead incurred by ODI is only marginally increased 10% and the energy cost to maintain ODI functionality is insignificant.

II. Heterogeneous Opportunistic Direct interconnection

WSNs are a fundamental component to realise smart and interactive environments in the vision for IoT. Therefore, if the IoT is realised, WSNs will be deployed in great numbers. Using Internet standards on top of IEEE 802.15.4 (6LowPAN, CoAP) [3] is the recent suggestion to integrate wireless links of WSNs with the Internet. Since IP-based solutions in WSNs have been implemented by middleware such as Contiki and TinyOS [1], the solutions are most likely to gain a lot of attention in practical implementations. However, integrating all nodes to the Internet is questionable for many reasons [2]. Therefore, instead of full integration, heterogeneous networks which are composed of both powerful and low-power nodes are expected. Low-power nodes will form a cluster around a powerful node, which acts as gateway. In each cluster, native protocols can be employed to optimise link characteristics, according to its internal behaviour or application requirements.

According to the above mentioned perspective, this research assumes that WSNs are separated into network domains. A network domain can refer to a WSN system or subsystem that consists of low-power sensor nodes in a star or multi-hop topology, connected with base stations or powerful platforms (cluster head inside platform-heterogeneous networks). These powerful platforms are responsible for sophisticated application services of network domains. Sometimes, boundaries of domains can be defined by technical requirements or by authorities. In each domain, sensor nodes can choose specific protocol stacks for communication within the domain's boundary. Opportunistic Direct Interconnection (ODI) refers to the ability to opportunistically share information or network services between these distinctive domains by enabling direct wireless connectivity that is not preconceived at the design time.

III. Principles of ODI

A. Concept Overview

A fundamental condition for wireless connectivity is compatibility between physical layer, i.e., radio interfaces. Although variations in the radio hardware exist at moment, radio standards are likely to converge as IoT gradually develops and matures. In this research, compatibility between radio interface is assumed by using the same radio hardware for sensor nodes in different domains.

At the link layer, ODI requires two functions in addition to those of the host MAC protocols [4], [7]:

- **Neighbour Discovery** Neighbour Discovery In order to build interconnection, neighbouring networks and their associated parameters must be identified.
- **Cross Boundary Transmission (CBT)** To communicate between domains, a common protocol, implemented by both sides, is required.

In [7], the ODI framework reserves two logical channels for ODI functions: 1) Common CHannel (CCH) reserved for neighbouring discovery and 2) Cross Boundary CHannel (CBCH) reserved for sending and receiving data across the boundary. OI-MAC, using Low Power Polling (LPP), is proposed for this purpose [7].

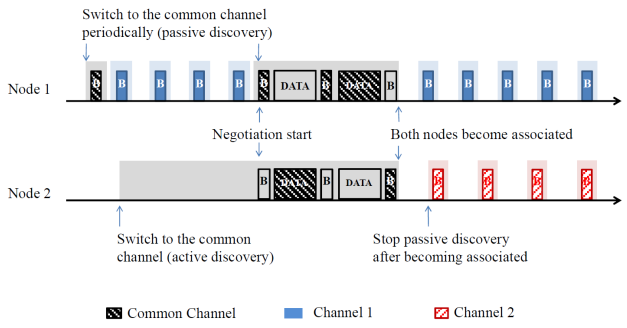

Fig. 1. Theoretical timing diagram of Neighbour Discovery (reproduced from [4])

Neighbour Discovery requires sensor nodes to scan neighbouring networks at run-time by listening on the Common Channel for a certain period of time (active discovery), while pre-existing domains switch to the common channel periodically and send a discovery beacon to search for newly deployed networks (passive discovery). If two domains encounter each other, they will exchange necessary information and become associated. The sensor nodes which discovered the neighbouring network are called Boundary Nodes, acting as gateway to the neighbouring network. This process of Neighbour Discovery is shown in Figure 1.

If two co-located domains agree to engage in ODI scheme, Cross Boundary Transmission will be performed by Boundary Nodes, using OI-MAC. Therefore, Boundary Nodes will check the CBCH in periods defined by a pseudo-random sequence. In cases where data is pending, Boundary Nodes will wait for a beacon from the destination network before transmitting data upon the reception of the destined beacon (Figure 2).

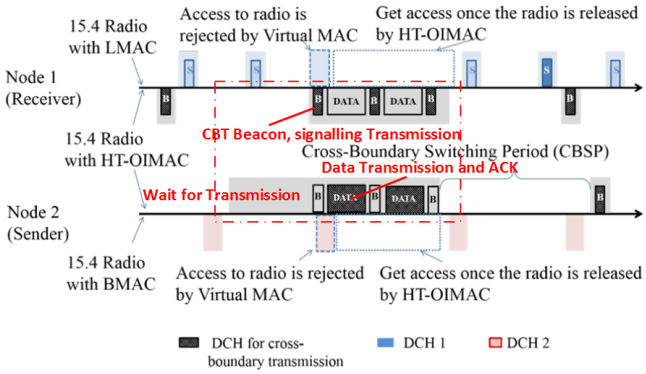

Fig. 2. Theoretical timing diagram of Cross Boundary Transmission, showing the possession change of radio interface, controlled by the Virtual MAC (reproduced from [7])

B. Architecture and Design

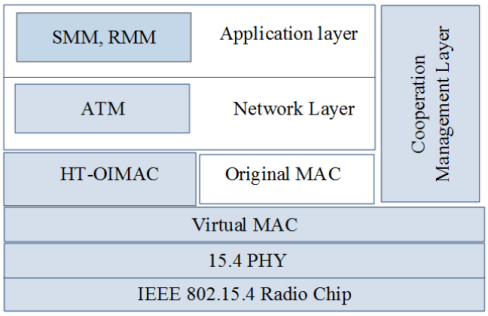

Fig. 3. The ODI framework, showing the necessary additional modules in each protocol stack (reproduced from [7])

The key principle of ODI is the establishment of direct interconnection between different protocol stacks while minimising side effects on the original purposes of the communication architecture. As IEEE 802.15.4 is well-known and widely used in WSNs, compliant radio chips, are used to present the compatibility of radio interfaces. To enable ODI, the framework requires the cross-domain protocol and the native MAC protocol to co-exist simultaneously. The concept

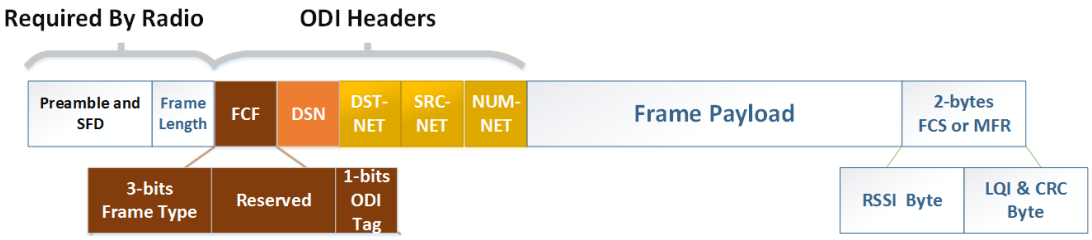

Fig. 4. Frame format of ODI packets, composed of the destination/source network, the number of associated networks, Frame Control Field, and Data Sequence Number

of a *Virtual MAC* is introduced to manage the schedule for both MAC protocols, which request access to the same radio interface. Figure 2 shows this possession switching between the cross-domain protocol (HT-OIMAC) and the native MAC protocol of each domain (LMAC and BMAC are used in [7]).

Figure 3 shows the architecture of the framework. The diagram indicates necessary modifications in each protocol stack. Regarding the modification in the network layer, the ODI framework requires an Address Translation Module (ATM) to translate the frame header of incoming/transmitted packets between the ODI frame format and the native frame format. In the application layer, ODI suggests using web service description language to describe and exchange available application/ network services. The Resource/Service Management Module (RMM/SMM) are introduced in the application layer to define, manage, and advertise the available services [7]. In order to provide application or network services, RMM/SMM may need the direct control over the behaviour of lower protocol stacks such as regulating the transmission power of the transceiver, adjusting the duty cycle, or changing the cost functions to determine packet routes in the routing protocol. Due to this, the Cooperation Management Module (CML) is introduced to observe and set the adjustable parameters in the MAC and NET layers.

IV. Implementation

Since the heterogeneous ODI framework, mentioned in the previous section, has up until now only been evaluated through simulation, we will implement it on real hardware for the purposes of validation. In this experiment, the framework is programmed using C language on eZ430-RF2500 sensor nodes from Texas Instrument. The compatibility of radio interfaces between domains is provided by using the same radio chip.

To realise the concept of the Virtual MAC, a clear interface between the radio module and the MAC layer is defined. Scheduling between both MAC protocols is programmed using timer-interrupts. By bundling shared procedures into atomic modules, the memory usage is significantly reduced (see Section VI-B). To achieve the purposes of ATM, a packet handling module is implemented to manage the packet buffer and translate packet headers.

From an implementation viewpoint, Neighbour Discovery and Cross Boundary Transmission provide the same set of operations which can be implemented together in the same module. To exchange packets in Cross Boundary Transmission, the operation of OI-MAC is extended from a unidirectional link to a bidirectional link. Figure 5 shows a sequence diagram of the process of Neighbour Discovery and Cross Boundary Transmission. A beacon (CBT Beacon) with the same frame format can serve as a discovery frame in Neighbouring Discovery Process or as a polling signal in Cross Boundary Transmission. In the first encounter with another neighbouring network, the associated node will broadcast a discovery and become a gateway for interconnection with the discovered network.

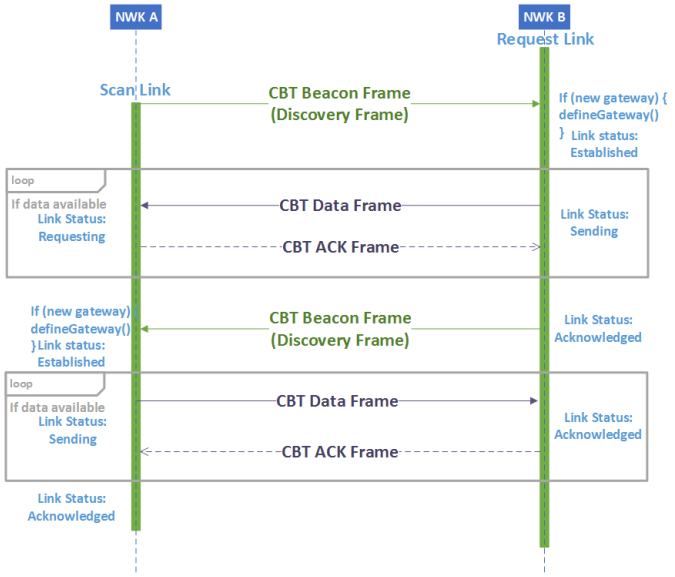

Fig. 5. Sequence diagram, demonstrating universal procedures of ODI

The frame format of the ODI framework requires 5 bytes of information. The Frame Control Field indicates the frame type and an ODI tag, which signifies that the packet is an ODI packet. A 1-byte header is required to indicate the number of the current associated network (NUM-NET). Additionally, the identities of the destination/source networks (DST/SRC-NET) must be contained in each packet. An ODI scheme is a local collaboration between co-located domains, therefore the identity of the network (NET-ID) can be contained in one byte. NET-ID can randomly assigned at the start-up phase. The newly-deployed network must check the detected NET-ID and choose another character to represent its identity in cases of NET-ID duplication. The ODI frame format is presented in Figure 4.

The packet forwarding scheme is realised by a gradient-based routing protocol. A packet is destined to a specific

gateway. Packets are passed on to the next hop which has a lower route cost to the destined gateway, as long as the packet buffer of the next node in the route is still vacant. The route cost is calculated by the number of hops and the link quality. If a new neighbouring network is discovered, all nodes with the direct access to the neighbouring network will be defined as a new possible gateway. All nodes will introduce a route cost for this new gateway, after the discovery have been broadcast. This implementation aims to prove the connectivity in lower layers of the framework by using a sense and send application. The application layer are conceptualised in this framework to provide the initial guideline for further implementation on cooperation scheme between WSNs on top of ODI.

V. Experimental Setup

To evaluate the ODI framework, a scenario of two co-located network domains is constructed. Each domain operates in its own logical channel with its preferred communication protocols. Domain A employs low-power listening with strobed preamble (X-MAC) as MAC protocol. It is deployed in the proximity of Domain B, which uses RI-MAC for internal communication. Each domain contains a Sink Node and 6 other nodes, 3 of which are equipped with the ODI capabilities. The topology presents the common cases where two networks partially overlap. Sensor nodes are positioned at distances (tx Power of -12 dB) to build a multi-hop topology. Figure 6 illustrates the network topology in the chosen scenario.

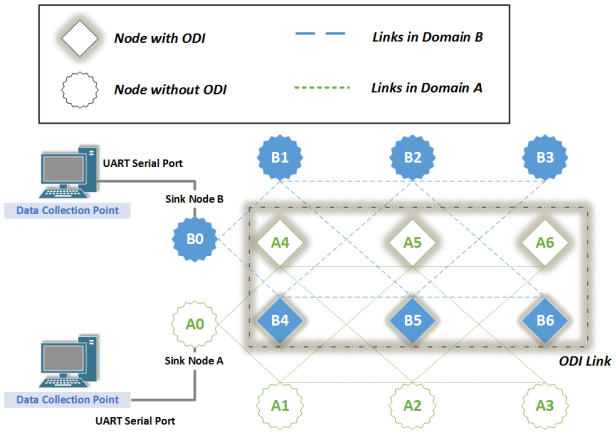

Fig. 6. The network architecture used in the experimental evaluation.

Each remote node periodically sends the ambient temperature to the Sink Node of its own domain. After the neighbouring domain is discovered, half of generated packets will redirect to Boundary Nodes for Cross Boundary Transmission. Each packet contains the sequence ID to detect lost packets and the footprint of every node on the route to track routes. The data generation rate is varied to evaluate the performance of the framework. The scheduling between OI-MAC and the native MAC protocol is governed by the sleep period, Neighbour Discovery Period (T_{NDS}), and Cross Boundary Transmission Period (T_{CBT}). When T_{NDS} or T_{CBT} are reached, an interrupt is generated to send a notification to Virtual MAC. The sleep period is set at 2 seconds, T_{NDS} is set at 12 seconds, and T_{CBT} is set at 4 seconds. T_{CBT} will be randomly generated by a pseudo-random sequence with the average value at 4 seconds

VI. Experimental Results

A. Validation of Functionality

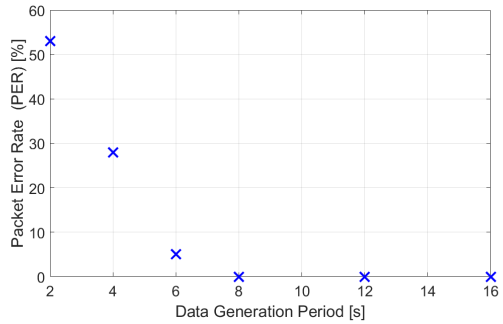

Fig. 7. PER vs. Data generation period, showing the saturated point of the framework

Results show that packets can be successfully transmitted across the boundary. The Packet Error Rate (PER) is recorded against the data generation rate (see Figure 7). During light traffic, the framework successfully delivers the packets across the boundary. However, delivery errors increase as the rate of data generation approach the saturated value. As the generation rate becomes higher, all Boundary Nodes are buffering packets to transmit. Every sender waits for the same beacon. Additionally, Collision Avoidance is not included in RI-MAC. Therefore, the contention of hidden terminals leads directly to collisions. This also results in Boundary Nodes, staying longer in CBCH with low rate of successful transmissions. At the same time Boundary Nodes in CBCH obstruct the internal flow of packets towards their own Sink Node.

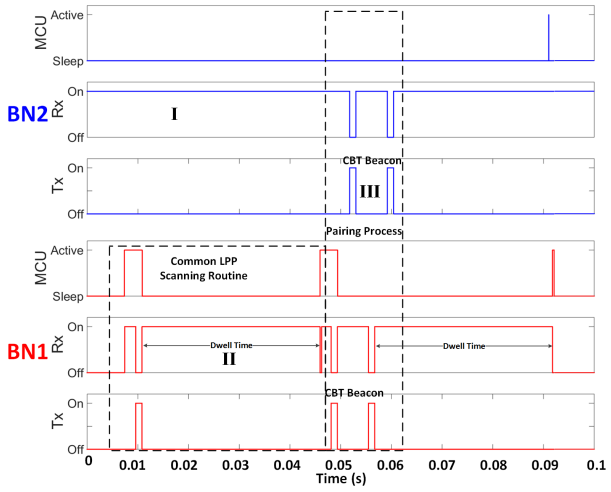

Fig. 8. Experimentally obtained timing diagram showing the operations of Boundary Nodes in the pairing process

Figures 8 and 9 show the timing diagrams of Neighbour Discovery and Cross Boundary Transmission respectively. The timing diagrams are composed from voltage signals, captured from I/O ports of the operating hardware. The timing diagrams demonstrate the Microcontroller and radio status of the associated nodes (Tx/Rx), including their packet transmissions. To clearly demonstrate the process, the sleep period of both

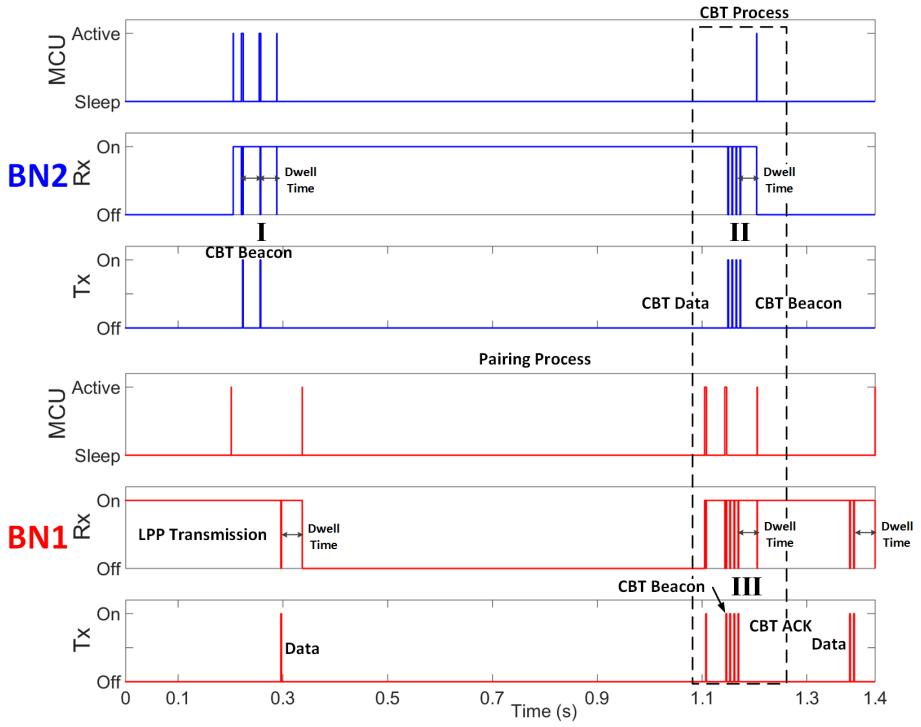

Fig. 9. Experimentally obtained timing diagram showing the event that packets are transmitted across the boundary

domains is set shorter at 512 ms. In the scenario, Domain A is deployed after Domain B. At Point I, BN2 (Domain A) is listening for a CBT Beacon in the Common Channel, while BN1 does a channel sampling (II). Then, BN1 (Domain B) changes its communication channel to the Common Channel and sending a CBT Beacon. Both side exchanges data (III) and go back to the original network routines. Figure 9 illustrates Cross Boundary Transmission from Domain A to Domain B. At Point I, BN2 arrives in CBCH and sends out a couple of CBT Beacons, then waits to send data packets across the boundary. BN1 arrives at CCH and broadcasts a CBT Beacon, BN2 receives CBT Beacon then sends data packets (II) and a CBT Beacon to invite back data packets from the other side. BN1 replies to each data packet with an ACK.

B. Memory Usage

This framework suggests using multiple communication protocols in memory-constraint devices to solve the incompatibility in the MAC layer. Regarding the memory usage, the results support the assumption that implementation of multiple protocols incurs only a marginal increase of memory footprint. Flash memory and RAM usage are recorded after implementation. From the total available 1 kilobytes of RAM, we use approximately 500 bytes, of which around 16 percent is used for communication systems. The Virtual MAC consumes insignificant space in RAM because the co-existing MAC protocols are programmed in event-driven architecture, and never activated at the same time. In terms of flash memory, we use in total 8096 bytes to implement RI-MAC. By adding X-MAC, the memory footprint slightly increases to 8330 bytes. After including ODI, the required memory footprint is 9030 bytes. Figure 10 visualises the comparison of the memory usage.

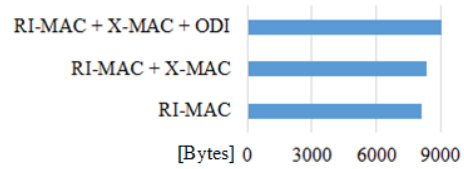

Fig. 10. Comparison of memory usage in the implementation of multiple protocols

The memory usage of the framework can vary, depended on the chosen internal protocols. However, the results in this implementation show that the memory footprint of multiple protocols can be reduced significantly with a careful design of modules, therefore the impacts of ODI in terms of memory usage are minimal.

C. Energy Consumption

The energy consumption of ODI can be comprehensively analysed by using the fact that both ODI functions (Neighbour Discovery and Cross Boundary Transmission) follow the same process of LPP. The common routine of LPP composes of sending a Beacon and listening to an incoming packet for a certain period of time (Dwell Time). Under the assumption that the operational voltage is approximately constant, the relative energy cost (consumed charge) of the ODI framework can be evaluated, by the area under the curve of captured current profile. Figure 11 shows the current profile of a common routine of Neighbour Discovery and Cross Boundary Transmission, captured at a supply voltage of 3V (V_{dd}) by an Agilent N6705B DC Power Analyzer.

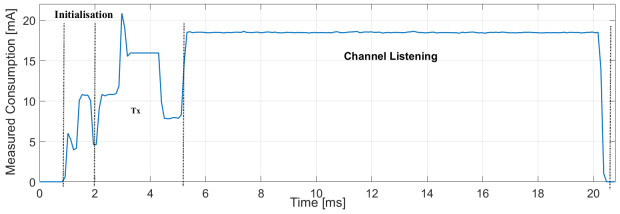

Fig. 11. Experimentally obtained current profile of the process of channel sampling in OI-MAC

From the captured results, the relative energy per routine ($E_{routine}$) is measured approximately at 1.1 mJ. The current consumption of channel listening (I_{listen}) is measured at 18.5 mA. Using the experimentally obtained values, the relative energy cost of Neighbour Discovery can be evaluated by the following equation:

$$E_{NDS} = I_{listen} \cdot T_{NDS} \cdot V_{dd} + \frac{T_{op} \cdot E_{routine} \cdot V_{dd}}{T_{NDS}} \quad (1)$$

E_{NDS}: Energy overhead of Neighbouring Discovery, T_{op} : Operation Time $\left(\frac{Q_{cap}}{I_{avg}}\right)$, Q_{Cap} : Battery Capacity [mAh], I_{avg} : Average Current [mA]

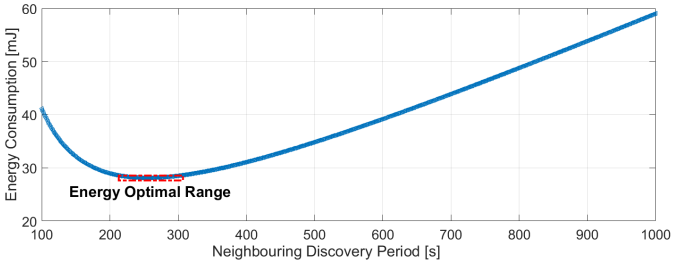

Fig. 12. The modelled relation, showing the optimal range for T_{NDS} at 253 seconds

From Equation 1, the most energy-optimised T_{NDS} can be determined. Figure 12 shows the graph of the relation between the energy consumption and the Neighbour Discovery period. According to the measured current profile, the Neighbour Discovery period is optimised approximately at 250 seconds, which consumes 28 mJ, equivalent to 0.13 percent of 2 typical AAA-Batteries (2000 mAh at 3V).

The energy overhead of Cross Boundary Transmission (E_{CBT}) can vary, depended on the link characteristics. The total consumption consists of the deterministic components and nondeterministic components. The deterministic components compose of the energy of periodically sending a beacon and listening (see Figure 11) and the energy of tx/rx process. This part of energy consumption can be traded off with performance, by varying Cross Boundary Transmission Period (T_{CBT}). However, the nondeterministic components, composed of the energy incurred by idle listening and collisions, are affected by other factors such as link quality, contention, topology, traffic, and the efficiency of the chosen protocol. As the techniques used for Cross Boundary Transmission still need improvements, the thorough evaluation of E_{CBT} will be included in future work.

VII. Conclusions

As the differences between protocol stacks in WSNs may continue to exist in the future, this research studies the ODI framework to enable interconnection between co-located domains of WSNs to help integrate WSNs with native protocols in the IoT. The ODI framework proposed uses OI-MAC as the common protocol to communicate between domains, while allowing each separate domain to use its own protocol for internal communication. This work implements the proposed framework to build cross boundary transmission between RI-MAC and X-MAC networks as an example. The practical implementation reveals that the framework can successfully build interconnection across boundaries. The memory usage of the framework implementation can vary due to the internal protocols chosen, but the careful design of the shared modules can greatly minimise the memory footprints. The energy consumption, required to enable the fundamental functions of ODI has been evaluated by measuring the current profile of operating hardware. The data can be used to solve the optimisation problem to calculate the energy-optimised discovery period. The experimental results confirm the ODI framework as a physically obtainable system with minimal overhead in terms of memory and energy. However, this is a first step and future work will look to further improve the integration of shared protocols and evaluate performance limitations e.g. scalability, network capacity, and also to extend the work to the application layer by implementing an example case study.

References

[1] L. Mainetti, L. Patrono, and a. Vilei, "Evolution of wireless sensor networks towards the Internet of Things: A survey," *2011 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp. 1–6, 2011.

[2] C. Alcaraz, P. Najera, J. Lopez, and R. Roman, "Wireless Sensor Networks and the Internet of Things : Do We Need a Complete Integration ?" *1st International Workshop on the Security of the Internet of Things (SecIoT'10)*, no. July 2015, pp. 1–8, 2010. [Online]. Available: https://www.nics.uma.es/system/files/papers/calcaraz10.pdf

[3] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, S. Member, G. Boggia, and M. Dohler, "Standardized Protocol Stack for the Internet of (Important) Things," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1389–1406, 2013.

[4] T. Jiang, G. V. Merrett, and N. R. Harris, "Opportunistic Direct Interconnection between Co-Located Wireless Sensor Networks," *2013 22nd International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–5, Jul. 2013.

[5] ——, "Opportunistic energy trading between co-located energy-harvesting wireless sensor networks," *Proceedings of the 1st International Workshop on Energy Neutral Sensing Systems - ENSSys '13*, pp. 1–6, 2013.

[6] H. Zia, N. R. Harris, and G. V. Merrett, "The impact of agricultural activities on water quality: A case for collaborative catchment-scale management using integrated wireless sensor networks," *Computers and Electronics in Agriculture 96*, 2013.

[7] T. Jiang, "Opportunistic Direct Interconnection and Cooperation Between Co-Located Wireless Sensor Networks," Ph.D. dissertation, University of Southampton, 2015.

[8] K. Singhanat, T. Jiang, G. V. Merrett, and N. R. Harris, "Empirical Evaluation of OI-MAC : Direct Interconnection between Wireless Sensor Networks for Collaborative Monitoring," *Ieee Sas*, 2015.

[9] "eZ430-RF2500 Development Tool User's Guide," 2009. [Online]. Available: http://www.ti.com/lit/ug/slau176d/slau176d.pdf