A Shared Opportunistic Infrastructure for Long-lived Wireless Sensor Networks

Xiuchao Wu, Cormac J. Sreenan, and Kenneth N. Brown [*]

Department of Computer Science, University College Cork, Republic of Ireland
{x.wu, cjs, k.brown}@cs.ucc.ie

Abstract. In this paper, a Shared Opportunistic Infrastructure (SOI) is proposed to reduce total cost of ownership for long-lived wireless sensor networks through exploiting human mobility. More specifically, various sensor nodes are opportunistically connected with their corresponding servers through smart phones carried by people in their daily life. In this paper, we will introduce the motivations, present the architecture, discuss the feasibility, and identify several research opportunities of SOI.

1 Background and Motivations

Wireless sensor networks (WSN) are regarded as one of the most promising technologies for the new century. As related technologies mature, we expect that many WSNs will be deployed to provide services (e.g. environmental monitoring, water/gas/electricity meter reading, and structural health monitoring) over long periods. Figure 1 illustrates the architecture of a classical WSN [2], in which a dedicated sink is used to connect sensor nodes with their application server through the Internet. However, in some environments, it could become very expensive to deploy, operate and maintain this kind of wireless sensor networks.

To provide useful services, hundreds or thousands of sensor nodes are normally deployed in a large area (in some cases, sensor nodes may be sparsely deployed and the network is partitioned), and a large amount of data will be continuously generated by these sensors. In order to connect these nodes to the back-end server and/or have enough capacity for timely and energy efficiently forwarding these sensed data, multiple sinks that spread across the covered area must be deployed. These sinks, which are normally much more powerful and expensive than sensor nodes, will increase the hardware cost of the WSN. The monthly subscription fee for their Internet access will also increase the operational cost significantly.

In addition, it is hard to find appropriate sites (with power supply and Internet access point) to install these sinks, especially in outdoor environments. Although large solar panels and cellular networks could solve these issues, these

[*] This work is supported in part by the HEA PRTLI-IV NEMBES Grant (http://www.nembes.com/). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of NEMBES sponsors or the University College Cork.

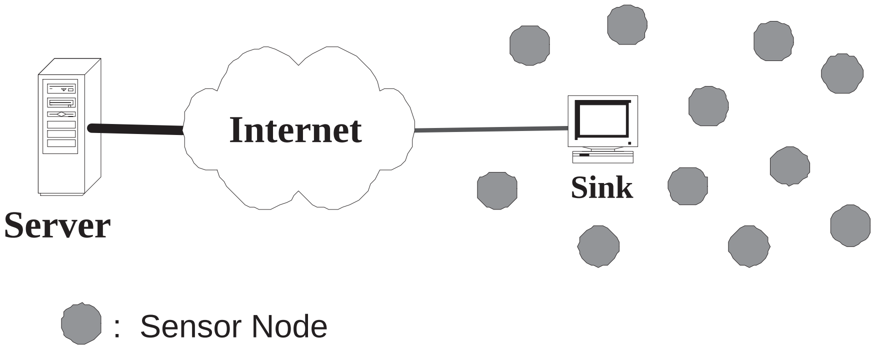

Fig. 1. The Architecture of Classical Wireless Sensor Network

devices will unavoidably increase the cost of each sink. More importantly, sinks with these devices tend to become attractive targets for theft when they are deployed at unattended sites.

Instead of fixed sinks, mobile robots or employees are also used to collect data directly from the covered area and distribute commands/tasks to sensor nodes [16][17]. However, mobile robots can not be applied in many environments and the salary for employees will significantly increase the operational cost.

Based on the above observations and the fact that many WSN applications are delay tolerant and are normally deployed in the area visited frequently by people, we propose a Shared Opportunistic Infrastructure (SOI) to reduce TCO (total cost of ownership) for these long-lived WSNs through exploiting human mobility. In the following sections, we present the architecture, discuss the feasibility, and identify several research opportunities of SOI.

2 The Architecture

In recent years, human mobility has also been exploited by participatory and opportunistic sensing [3][4]. The sensors on smart phones carried by people are used as mobile sensors to sense the world and many fantastic applications have been proposed [11][14]. However, sensors on smart phones will increase phone price and it may not be inappropriate for many sensors to be installed on smart phones. Hence, the feasible applications of participatory or opportunistic sensing are limited. As for SOI that uses smart phones to opportunistically connect sensor nodes to their corresponding servers, it can complement with participatory/opportunistic sensing and it is worthwhile to be investigated further.

Considering that the sensed data may be totally unrelated with the person that passes through sensor nodes, SOI uses real money as the incentive, and Public Key Infrastructure (PKI) techniques are adopted to satisfy the security requirements. Figure 2 shows the architecture of SOI, in which Data Collection

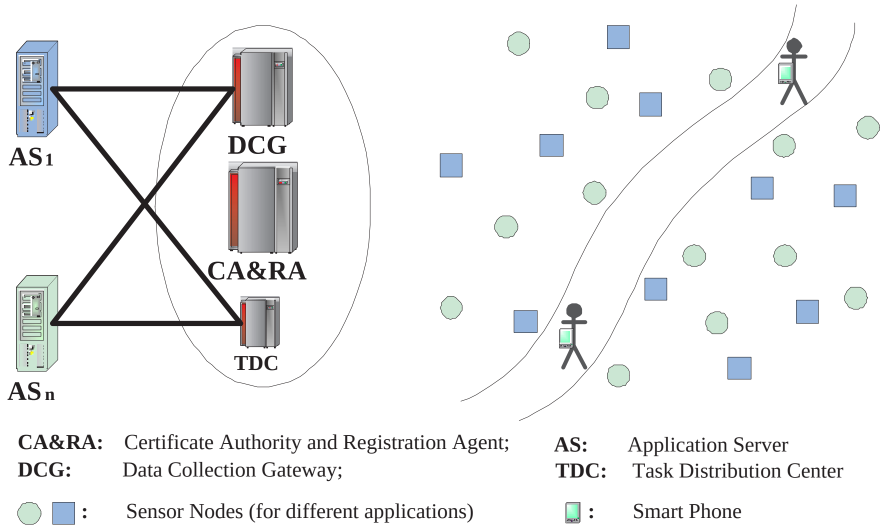
AS1
ASn
DCG
CA&RA
TDC
CA&RA: Certificate Authority and Registration Agent;
DCG: Data Collection Gateway;
AS: Application Server
TDC: Task Distribution Center
: Sensor Nodes (for different applications)
: Smart Phone

Fig. 2. The Architecture of SOI

Gateway (DCG), Task Distribution Center (TDC), and smart phones carried by people connect sensor nodes with their corresponding application servers (AS) opportunistically. CA&RA (Certificate Authority and Registration Agent) is responsible to register these entities and issue certificates to establish trust relationships among them. To alleviate the workload of CA&RA, application provider can use its certificate (issued by CA&RA) to sign one certificate for each sensor node. With the certificate chain installed on a sensor node, it can authenticate itself with smart phones.

The sensed data is collected by smart phones carried by people who pass through the covered areas in their daily life. According to delay requirements and the price paid by application providers, smart phones will then upload these data to DCG immediately through a cellular network, intermittently through open Wi-Fi hot-spots, or through a home broadband network. DCG will then forward these data to their corresponding ASs. In order to control sensor nodes, ASs can post tasks (command, code image, etc.) on TDC so that smart phones can download the appropriate tasks based on their locations and pass to the related sensor nodes. TDC may also broadcast node density in each area and the price offered by application providers. Based on these information, smart phone can decide whether to participate the system and which sensor nodes it will collect data from.

SOI can support many interesting applications. For instance, tourists can opportunistically collect data from sensor nodes deployed in national parks, city residents can be involved with various wireless sensor networks (weather stations, meters in buildings, etc.) deployed for serving the city, etc.

With SOI, application providers need not buy, deploy, or maintain sinks. Communication costs can also be decreased through exploiting human mobility. Hence, TCO for long-lived WSNs can be reduced significantly. As for people, the intervention from the user can be reduced with carefully designed softwares and it is a strong motivation to earn money automatically during daily life. DCG, TDC, and CA&RA can also survive through claiming their share of the money paid by application providers.

Although SOI could provide many benefits, there are also a lot of issues to be concerned. In the following two sections, we will briefly discuss its feasibility and identify some research opportunities in the context of SOI.

3 Feasibility Analysis

One prerequisite of SOI is that smart phones must be able to talk with sensor nodes that belong to different WSNs. Considering that IEEE 802.15.4 [1] has been well standardized for WSNs, one low-power and cheap IEEE 802.15.4 radio installed on the smart phone is enough. With the maturity of WSN applications (such as health care, home automation, etc.), many devices with IEEE 802.15.4 radio will come to the market. Since the smart phone is a very good candidate as the unified bridge between a user and these devices, we can expect that IEEE 802.15.4 radio will be deployed on smart phones soon. We hope that SOI can also motivate the deployment of IEEE 802.15.4 on smart phones.

SOI should also provide enough incentives for people to participate. Not only the real money paid to people, the burden of user registration should be alleviated, their privacy must be respected, and a payment system is required so that people can get their earned money conveniently. Fortunately, since smart phones are used in SOI, mobile telecoms are the best candidates for operating CA&RA and these issues can be solved easily in this case.

The current registration process for phone services can be reused for SOI user registration. During this process, the certificates can be issued and installed on the smart phone, and the necessary softwares can also be installed. These softwares can also be pre-installed by the smart phone manufacturers.

As for privacy, compared to phone service registration, SOI does not need any further personal information and all personal information is held only by CA&RA. Each smart phone will get multiple certificates without any personal information. Hence, DCG and TDC can not identify the person based on the certificates. DCG and TDC will also conceal the certificates from ASs. With this scheme, to infer the movement of a specific person, application providers must let sensor nodes transmit user certificates inside the data forwarded by smart phones. Since multiple certificates without any personal information are issued to each user, application providers must pay for transmitting these certificates and they still cannot easily violate user privacy (locations, tracks, movement patterns, etc.). To avoid being tracked through wireless interface card, MAC address pseudonyms [8] can also be adopted by smart phones.

As for payment, the phone billing system can be utilized to pay the money to users. Through the cooperation among DCG, TDC, and CA&RA, application providers will be charged and the money can be deposited to phone bill accounts of the users correspondingly.

Since mobile telecom acts as CA&RA, misbehavior entities, such as smart phone users who discard data and application providers who refuse to pay, can be kicked out from the system through revoking their certificates. In serious situations, further punishments are possible since these entities had registered with mobile telecom.

In addition, data delivery latency in SOI could be huge since smart phone users may not visit some sensor nodes for a long period. However, many wireless sensor network applications are delay-tolerant and sensor nodes could be equipped with large-capacity flash cards for buffering the sensed data. For example, analysis of environmental monitoring data is rarely urgent, and meter readings for billing purposes can be delayed by weeks. In the case that data delivery latency must be low, some alternative methods must be provided. SOI still could be helpful in the periods with abundant user mobility.

4 Research Opportunities

In SOI, there are some unique challenges to be solved. Many problems, that have been studied in delay-tolerant network [10][18], wireless sensor network [13][15], participatory or opportunistic sensing [5][6], etc., should also be re-scrutinized in the context of SOI. In the following sub-sections, we will discuss several topics that should be worthwhile to be investigated further.

4.1 Architecture and Protocols

The architecture of SOI should be refined. The functions of each entity and their trust relationship must be clarified. The protocols used among these entities should also be designed carefully. The main point is to ensure user privacy, detect abnormal behaviors of each kind of entity, and provide security schemes required by an E-Payment system, such as non-repudiation and non-replicability.

4.2 Computation Cost of Sensor Nodes and Smart Phones

PKI is used by SOI to satisfy the security requirements. Although smart phones are now very powerful and some PKI chips have already been developed for sensor nodes, it is still worthwhile to study how to reduce the number of slow and expensive private key operations [9]. Due to the regularity of human mobility [7], some sensor nodes and smart phones will encounter frequently. Hash chains [12] could be used to reduce the number of private key operations carried out by these familiar strangers for authentication.

It should also be desirable to decouple private key operations from the process of data exchange so that protocols will not be interfered and sensor nodes could schedule these operations in a better way. For example, data can be signed by sensor nodes when there is no smart phone nearby and/or when energy supply from the environment is abundant in the case that energy harvesting (solar panel, etc.) is exploited.

4.3 Contact Probing

Contact probing had been well studied in delay tolerant network [18]. With the assumption that mobile nodes are always active, mobile nodes learn contact arrival process and adjust the frequency of probing accordingly with the aim to save energy and reduce contact miss probability. However, sensor nodes in SOI are normally duty-cycled and contact probing scheme should be re-scrutinized. It is worthwhile to study how smart phones and sensor nodes can find each other timely for collecting data as much as possible. Contact probing scheme should also be energy efficient for both smart phones and sensor nodes.

In the context of SOI, smart phones are not suitable for initiating contact probing. If so, smart phones must probe with a high frequency as sensor nodes are duty-cycled. Consequently, smart phones will waste their energy and wireless channel will be congested by these probing packets. Hence, it should be better to let smart phones keep listening and let sensor nodes probe when they wake up according to their duty-cycle. This issue has been studied further in [20][19].

When sensor nodes could form a connected network, these nodes may also cooperate to improve the performance further. For example, sensor nodes may predict the mobility of the smart phone that they are talking with. They can then activate the corresponding nodes at appropriate time so that the smart phone can be probed timely.

Within SOI, CA&RA can also be used to deduce the density of sensor nodes and the number of SOI users in the current cell. This information can be broadcasted through base station and smart phones can adjust their behaviors correspondingly. For example, according to user density, a smart phone can adjust its back-off window, that is used before responding to a probing packet broadcasted by a sensor node, with the aim to reduce packet collision.

4.4 Data Replication and Distribution

As sensor nodes in SOI may not be visited by smart phones for a long period, the sensed data should be replicated and distributed for data reliability under node failure [10].

In the context of SOI, not only the cost of sensor node's energy and storage, application providers must also pay for data replications collected by smart phones. Hence, replication overhead should be deterministic and should be as small as possible. Instead of multiple copies, source-based erasure coding approaches, such as Reed-Solomon Codes, could be adopted. These data slices are then distributed among sensor nodes for reliability and each data slice should be signed separately for non-replicability.

When distributing these data slices, not only data reliability, many other issues should also be considered. For example, sensor nodes in SOI may have different probability to be visited by smart phones. If data slices can be distributed according to contact and storage capacity of these nodes, network throughput can be increased and the latency of data delivery can be decreased. In addition, due to network topology, some sensor nodes need forward data for other nodes. For load balancing, they may ask other nodes to sign their data slices.

A two-phase data distribution should be suitable for SOI. In the first phase, for both data reliability and load balancing, data slices are forwarding to several nodes with less contact capacity, at which data slices are signed. In the second phase, the signed data slices are forwarded to nodes with more contact capacity for higher throughput and lower latency.

Data replication and distribution will unavoidably consume storage and energy resources. Hence, there are many tradeoffs to be considered when designing these schemes. When solar panels are used by sensor nodes for energy harvesting, it is also very valuable to study how to synchronize these operations with energy supply of the deployment environment.

5 Future Work

This paper presents the concept and the architecture of SOI. In future work, we will refine the architecture and design the protocols and algorithms used by the entities of SOI. We also plan to implement a prototype of SOI for investigating this topic further.

References

1. IEEE 802.15.4, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). IEEE, 2006.
2. I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Computer Networks*, 38:393–422, 2002.
3. J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava. Participatory sensing. In *World Sensor Web Workshop (in conjunction with Sensys)*, 2006.
4. A. T. Campbell, S. B. Eisenman, N. D. Lane, E. Miluzzo, and R. A. Peterson. People-centric urban sensing. In *ACM/IEEE WICON*, 2006.
5. C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos. Anonysense: Privacy-aware people-centric sensing. In *Mobisys*, 2008.
6. N. Edalat, W. Xiao, C.-K. Tham, E. Keikha, and L.-L. Ong. A price-based adaptive task allocation for wireless sensor network. In *MASS*, 2009.
7. M. C. Gonzlez, C. A. Hidalgo, and A.-L. Barabsi. Understanding individual human mobility patterns. *Nature*, 453:779–782, 2008.
8. M. Gruteser and D. Grunwald. Enhancing location privacy in wireless lan through disposable interface identifiers: a quantitative analysis. *Mobile Networks and Applications*, 10(3):315–325, June 2005.

9. W. Hu, P. Corke, W. C. Shih, and L. Overs. secfleck: A public key technology platform for wireless sensor networks. In *EWSN*, 2009.
10. S. Jain, M. Demmer, R. Patra, and K. Fall. Using redundancy to cope with failures in a delay tolerant network. In *SIGCOMM*, 2005.
11. S. Kang, J. Lee, H. Jang, H. Lee, Y. Lee, S. Park, T. Park, and J. Song. Seemon: Scalable and energy-efficient context monitoring framework for sensor-rich mobile environments. In *Mobisys*, 2008.
12. L. Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24:770–772, 1981.
13. C. Liu, J. Wu, and I. Cardei. Message forwarding in cyclic mobispace: the multi-copy case. In *MASS*, 2009.
14. M. Mun, S. R. annd Katie Shilton, N. Yau, J. Burke, D. Estrin, M. Hansen, E. Howard, R. West, and P. Boda. Peir, the personal environmental impact report, as a platform for participatory sensing systems research. In *MOBISYS*, 2009.
15. B. Pasztor, M. Musolesi, and C. Mascolo. Opportunistic mobile sensor data collection with scar. In *MASS*, pages 1–12, 2007.
16. R. C. Shah, S. Roy, S. Jain, and W. Brunette. Data mules: Modeling a three-tier architecture for sparse sensor networks. In *IEEE SNPA Workshop*, pages 30–41, 2003.
17. A. A. Somasundara, A. Kansal, D. D. Jea, D. Estrin, and M. B. Srivastava. Controllably mobile infrastructure for low energy embedded networks. *IEEE Transactions on Mobile Computing*, 5(8):958–973, august 2006.
18. W. Wang, V. Srinivasan, and M. Motani. Adaptive contact probing mechanisms for delay tolerant applications. In *Mobicom*, pages 230–241, 2007.
19. X. Wu, K. N. Brown, and C. J. Sreenan. Exploiting rush hours for energy-efficient contact probing in opportunistic data collection. In *The 4th International Workshop on Sensor Networks (in conjunction with IEEE ICDCS)*, 2011.
20. X. Wu, K. N. Brown, and C. J. Sreenani. SNIP: A sensor node-initiated probing mechanism for opportunistic data collection in sparse wireless sensor networks. In *The First International Workshop on Cyber-Physical Networking Systems (in conjunction with IEEE INFOCOM)*, 2011.