ERCIM “Alain Bensoussan” Fellowship Scientific Report

Fellow:	Simon Duquennoy
Visited Location:	SICS – Swedish Institute of Computer Science
Duration of Visit:	12 months (01/10/2010 – 30/09/2011)
Scientific coordinator:	Thiemo Voigt

I – Scientific activity

Wireless Sensor Networks (WSN) are networks of resource-constrained, often battery-operated sensor nodes communicating wirelessly over multiple hops. In recent years, WSNs have begun to move towards multi-purpose networks of heterogeneous nodes using the Internet Protocol (IPv6) for interoperability. Such IP-connected sensor networks can natively interact with existing infrastructures, including the Internet, forming what is often referred to as the “Internet of Things” (IoT). This approach is promising but raises a number of research questions, in particular on how to conciliate energy-efficiency and the demanding application requirements of the IoT.

During my ERCIM fellowship, I worked on IP-based communication in low-power WSNs. The main research project I conduced aimed at improving bulk transmission in radio duty-cycled networks, in which the nodes spend most of their time (>99%) with their radio chip turned off, leading to significant lifetime extension. I proposed Burst Forwarding, a technique providing high throughput in multi-purpose networks while maintaining low-power operation even when facing interference and packet loss. I designed, implemented and experimentally validated this technique. This work was published in ACM SenSys 2011 [2], the most prestigious conference in the area of Wireless Sensor Networks.

I also worked on a number of satellite projects in collaboration with different people, either members of the group or external visitors. I learned a lot from these collaborations. I worked on adapting IPsec to WSNs [1,4,7], on application interaction via the CoAP protocol [3], and on application deployment in heterogeneous networks [5,6].

Finally, I was involved in various other activities: peer reviewing, student supervision and contribution to funded project proposals. I supervised a Master thesis student on routing in IP-based low-power networks. I was comity member for the following events: IEEE LCN 2011 (TPC member) IEEE SenseApp 2011 (TPC member), IEEE DCOSS 2011 (Demo Session Chair) and CONET 2011 (TPC member). I also reviewed for the following journals: ACM TOSN, Elsevier JSA, IEEE TPDS and Elsevier JSS.

I would like to thank Thiemo Voigt for welcoming me in the NES group, as well as the members of the group and visitors I worked with. Thanks to ERCIM for providing this fellowship and to Torsten Braun and Pedro José Marrón for hosting me during the Research Exchange Programme.

II – Publications during the fellowship

Referred Papers

[1] Shahid Raza, Simon Duquennoy, Joel Höglund, Utz Roedig, and Thiemo Voigt. **Secure Communication for the Internet of Things - A Comparison of Link-Layer Security and IPsec for 6LoWPAN**. *Security and Communication Networks, Wiley*, December 2011. To appear.

Abstract: The future Internet is an IPv6 network interconnecting traditional computers and a large number of smart objects. This Internet of Things (IoT) will be the foundation of many services and our daily life will depend on its availability and reliable operation. Therefore, among many other issues, the challenge of implementing secure communication in the IoT must be addressed. In the traditional Internet, IPsec is the established and tested way of securing networks. It is therefore reasonable to explore the option of using IPsec as a security mechanism for the IoT. Smart objects are generally added to the Internet using IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN), which defines IP communication for resource-constrained networks. Thus, to provide security for the IoT based on the trusted and tested IPsec mechanism, it is necessary to define an IPsec extension of 6LoWPAN. In this paper, we present such a 6LoWPAN/IPsec extension and show the viability of this approach. We describe our 6LoWPAN/IPsec implementation, which we evaluate and compare with our implementation of IEEE 802.15.4 link-layer security. We also show that it is possible to reuse crypto hardware within existing IEEE 802.15.4 transceivers for 6LoWPAN/IPsec. The evaluation results show that IPsec is a feasible option for securing the IoT in terms of packet size, energy consumption, memory usage, and processing time. Furthermore, we demonstrate that in contrast to common belief, IPsec scales better than link-layer security as the data size and the number of hops grow, resulting in time and energy savings.

[2] Simon Duquennoy, Fredrik Österlind, and Adam Dunkels. **Lossy Links, Low Power, High Throughput**. In *Proceedings of the International Conference on Embedded Networked Sensor Systems (ACM SenSys 2011)*, Seattle, WA, USA, November 2011

Abstract: As sensor networks move towards general-purpose low-power wireless networks, there is a need to support both traditional low-data rate traffic and high-throughput transfer. To attain high throughput, existing protocols monopolize the network resources and keep the radio on for all nodes involved in the transfer, leading to poor energy efficiency. This becomes progressively problematic in networks with packet loss, which inevitably occur in any real-world deployment. We present burst forwarding, a generic packet forwarding technique that combines low power consumption with high throughput for multi-purpose wireless networks. Burst forwarding uses radio duty cycling to maintain a low power consumption, recovers efficiently from interference, and inherently supports both single streams and cross-traffic. We experimentally evaluate our mechanism under heavy interference and compare it to PIP, a state-of-the-art sensornet bulk transfer protocol. Burst forwarding gracefully adapts radio duty cycle both to the level of interference and to traffic load, keeping a low and nearly constant energy cost per byte when carrying TCP traffic.

[3] Matthias Kovatsch, Simon Duquennoy, and Adam Dunkels. **A Low-Power CoAP for Contiki**. In *Proceedings of the Workshop on Internet of Things Technology and Architectures (IEEE IoTech 2011)*, Valencia, Spain, October 2011

Abstract: Internet of Things devices will by and large be battery-operated, but existing application protocols have typically not been designed with power-efficiency in mind. In low-power wireless systems, power-efficiency is determined by the ability to maintain a low radio duty cycle: keeping the radio off as much as possible. We present an implementation of the IETF Constrained Application Protocol (CoAP) for the Contiki operating system that leverages the ContikiMAC low-power duty cycling mechanism to provide power efficiency. We experimentally evaluate our low-power CoAP, demonstrating that an existing application layer protocol can be made power-efficient through a generic radio duty cycling mechanism. To the best of our knowledge, our CoAP implementation is the first to provide power-efficient operation through radio duty cycling. Our results question the need for specialized low-power mechanisms at the application layer, instead providing low-power operation only at the radio duty cycling layer.

[4] Shahid Raza, Simon Duquennoy, Tony Chung, Dogan Yazar, Thiemo Voigt, and Utz Roedig. **Securing Communication in 6LoWPAN with Compressed IPsec**. In *Proceedings of the International Conference on Distributed Computing in Sensor Systems (IEEE DCOSS 2011)*, Barcelona, Spain, June 2011

Abstract: Real-world deployments of wireless sensor networks (WSNs) require secure communication. It is important that a receiver is able to verify that sensor data was generated by trusted nodes. It may also be necessary to encrypt sensor data in transit. Recently, WSNs and traditional IP networks are more tightly integrated using IPv6 and 6LoWPAN. Available IPv6 protocol stacks can use IPsec to secure data exchange. Thus, it is desirable to extend 6LoWPAN such that IPsec communication with IPv6 nodes is possible. It is beneficial to use IPsec because the existing end-points on the Internet do not need to be modified to communicate securely with the

WSN. Moreover, using IPsec, true end-to-end security is implemented and the need for a trustworthy gateway is removed.

In this paper we provide End-to-End (E2E) secure communication between IP enabled sensor networks and the traditional Internet. This is the first compressed lightweight design, implementation, and evaluation of 6LoWPAN extension for IPsec. Our extension supports both IPsec's Authentication Header (AH) and Encapsulation Security Payload (ESP). Thus, communication endpoints are able to authenticate, encrypt and check the integrity of messages using standardized and established IPv6 mechanisms.

[5] Simon Duquennoy, Niklas Wirström, Nicolas Tsiftes, and Adam Dunkels. **Leveraging IP for Sensor Network Deployment**. In *Proceedings of the International Workshop on Extending the Internet to Low power and Lossy Networks (IP+SN 2011)*, Chicago, IL, USA, April 2011

Abstract: Ease of deployment has always been seen as a major selling point of wireless sensor networks, yet experience has shown deployment to be difficult. We argue that parts of these difficulties have come from the lack of a generic networking layer and of well-tested, generic transport protocols in traditional sensornet deployments. We believe that the use of low-power IPv6 can help by providing node-level addressing, point-to-point routing, and generic well-tested transport protocols. We evaluate the performance of HTTP/TCP and CoAP/UDP over a duty cycled radio layer, showing that with a small modification to the duty cycling layer results in a dramatic improvement in performance at a retained low power consumption. Based on our experiences, we introduce an in-network caching mechanism that significantly improves the performance of software updates in incrementally deployed sensor networks. Our results are the first steps towards a deployment tool for IP-based sensor networks.

Demos (presented at conferences)

[6] Simon Duquennoy, Niklas Wirström, and Adam Dunkels. **Demo: Snap - Rapid Sensornet Deployment with a Sensornet Appstore**. In *Proceedings of the International Conference on Embedded Networked Sensor Systems (ACM SenSys 2011)*, Seattle, WA, USA, November 2011

[7] Shahid Raza, Simon Duquennoy, Thiemo Voigt, and Utz Roedig. **Demo Abstract: Securing Communication in 6LoWPAN with Compressed IPsec**. In *Proceedings of the International Conference on Distributed Computing in Sensor Systems (IEEE DCOSS 2011)*, Barcelona, Spain, June 2011

III – Attended Seminars, Workshops, and Conferences

- **ACM SenSys'10 conference**, 3/11 – 5/11/2010, Zurich, Switzerland, as an attendee
- **ACM/IEEE IPSN'11 conference**, 12/04 – 14/04/2011, Chicago, USA, as an attendee and presenter in the collocated IP+SN workshop
- **Negotiation meeting** for the EU FP7 CALIPSO project, 4/05/2011, Brussels, Belgium
- **AdHoc'11**, 10/05 – 11/05/2011 Gottröra, Sweden, as an attendee
- **IEEE DCOSS'11 conference**, 27/06 – 29/06/2011, Barcelona, Spain, as demo session chair, author of a paper, and authors of a demo
- **Kick-off meeting** of the EU FP7 CALIPSO project, 20/09/2011, Paris, France

IV – Research Exchange Programme

My first visit was hosted by Prof. Torsten Braun, at the University of Bern (SARIT), from May 23rd to 27th 2011. I presented my PhD work and my on-going postdoc work at the weekly group seminar. During the rest of the week, I had planned individual meetings with the group members. Finally, I attended the PhD defence of Thomas Staub, as well as a talk by his opponent, Andreas Kassler.

My second visit was hosted by Prof. Pedro José Marrón, at University of Duisburg-Essen (Franhaufer), from June 13th to 17th 2011. I also presented my work to about 25 people, and had individual meetings with the group members.