ASSESSING SECURITY IN ENERGY-EFFICIENT SENSOR NETWORKS

Yee Wei Law, Sandro Etalle, Pieter H. Hartel
Faculteit Elektrotechniek, Wiskunde en Informatica, Universiteit Twente
Postbus 217, 7500 AE Enschede, The Netherlands
{ywlaw, etalle, pieter}@cs.utwente.nl

Abstract

In this paper, we describe why current research in ad hoc networks requires an effective assessment framework, and how our *system profile* proposal can be used for the purpose. With this tool at hand, we have managed to carve out manageable design spaces from the seemingly infinite possibilities of ad hoc mobile wireless networks.

1. Introduction

Wireless sensor networks combine the characteristic of ad hoc mobile wireless networks (ad hoc networks in short) at the system level, with the characteristics of sensors at the component level. Ad hoc networks are: (1) **ad hoc**: the network set-up is possibly short-lived; (2) **mobile**: the nodes are not attached to any fixed communications infrastructure as well as fixed energy supply; (3) **wireless**: the nodes communicate wirelessly. These three properties imply a series of constraints, that together with the constraints imposed by sensors (among which energy being the predominant), form the starting point of our security research.

In our opinion, the current research landscape lacks structure. Here, we show how prevalent (proposed) architectures are based on assumptions that are not only implicit but even conflicting at times. As an example of implicit assumptions, to curb selfishness, the Terminodes project introduces a virtual currency called *nuglets* [2]. To protect these nuglets from tampering, every node must be equipped with a tamper-resistant *security module*. At the same time, the proposed cross-certification architecture calls for public-key cryptography. In addition, as part of the Terminodes project, Hubaux *et al.* propose that each node maintains its own *certificate repository* [5]. These repositories store the

public certificates the node themselves issue, and a selected set of certificates issued by the others. It is thus concluded, although the Terminodes project does not specify, that the implicit assumptions or requirements of Terminodes are that they have to be (1) tamper-resistant, (2) capable of performing resource-intensive public-key cryptography, and (3) have sufficient storage for a potentially large certificate repository.

In direct contrast to the above approaches are Basagni *et al.*'s *pebblenets* [1] and Perrig *et al.*'s SPINS [6] which specifically avoid public-key cryptography that sensors are ill-equipped to handle. The different assumptions in public-key cryptography present an insurmountable barrier in unifying the earlier proposals with Basagni *et al.*'s or Perrig *et al.*'s. Of further interest is that Basagni *et al.*'s *pebbles* are required to be tamper-resistant to ensure forward secrecy. Building tamper-resistance into a sensor can substantially increase the cost of the sensor depending on the intended FIPS 140-1 level (`csrc.nist.gov`). This presents a case of potentially self-contradicting requirements within a single proposal.

Our contribution to providing structure is *system profiles*. System profiles are an effective means for assessing and categorizing s system according to its actual specification and requirements. Under this framework, we make it possible for architectural designs to relate to a set of fine-grained properties they should comply with, instead of a hypothetical and often arbitrary set of assumptions. Keeping one system profile in perspective at a time helps to prevent oversight and underestimation.

2. System Profiles

The inspiration of system profiles comes from Sun's Java™ 2 Platform, Micro Edition (J2ME) (`java.sun.com/j2me`), a Java platform targeted at low-end devices such as PDAs, cellphones etc. As the capabilities of these devices vary tremendously, Sun introduced the concept of *configurations*. Configurations map to Sun's two primary design targets: devices that can be held in the hand and devices that can be plugged into a wall. Hence there are two configurations: Connected Limited Device Configuration (CLDC) and Connected Device Configuration (CDC). CLDC targets resource-constrained devices with typically a 16/32-bit processor, and 128∼512 KB of memory available for the Java platform and applications; whereas CDC is for more powerful devices. The strategy of J2ME attests to the fact that one size does not fit all. We are adopting a similar profiling strategy. The only difference is what we are profiling are not the nodes themselves, but the systems.

We categorize different ad hoc networks into different system profiles, each of which is defined by a set of boolean *critical system parameters*.

(The boolean nature of the papameters is really an abstraction of a more refined scale that we would like to investigate in the future.) The following critical system parameters have been defined:

1. Message Confidentiality (MC) specifies the requirement for encrypting all network messages. Rationale: Although encrypting network messages is useful for battling traffic analysis by attackers, not all types of system require this level of security. A brute force approach of encrypting all messages regardless of necessity does not necessarily provide the highest level of security, nor is it energy-efficient. In the case where MC=F(alse), the confidentiality of the payload data is considered an application-dependent (as contrasted to system) requirement .

2. Tamper Resistance (TR) speficies whether there is an allowance for using tamper-resistant hardware to protect every node in the network. Rationale: To entrust a node with a key, we have to make sure the node itself does not divulge the key to unauthorized parties upon tampering. If not all nodes in the network can be made tamper-resistant, it is insufficient to rely on cryptography alone to ensure the integrity of any node, since any node can be tampered, with its keys compromised and its program modified. For such networks, cryptographic material cannot be kept at any node for any extended period, and supplementary means are necessary. It is for simplicity that this parameter is represented as a binary scale instead of a multi-level scale as in FIPS 140-1.

3. Public-Key Cryptographic Capability (PKCC) refers to the capability of any node in the network to perform public-key cryptography. Rationale: This parameter determines whether public-key cryptographic technology can be employed. Note however that the fact that PKCC is true does not guarantee that public-key cryptography can or should be used extensively. It only indicates that the technology *can* be used, and the degree of usage depends on the architectural design. In general, to perform public-key cryptography, the processor speed is not the only issue, the deciding factor is the sufficiency of memory, therefore PKCC more or less translates to the sufficiency of memory.

4. Rich Uncles (RU) refers to the availability of Rich Uncle nodes, which are resourceful nodes, both in terms of computing resources and energy, that are suitable for the role of certification authorities, for example in the Rich Uncle Protocols [3]. These nodes might be floating or might be gateways to some external wired networks. If all nodes are equally "rich" (i.e. the network is homogeneous), we may assume that either every node is a Rich Uncle or no node is a Rich Uncle. Rationale: the existence of Rich Uncles confirms the possibilities of relegating resouce-intensive tasks and assigning important security roles to them,

thereby facilitating the use of certain hierarchical architectures and possibly public-key cryptography.

This selection of parameters is not meant to be exhaustive or definitive and yet we find it an unambiguous way for categorizing the types of system we know so far. We give a few examples below of how we classify some typical ad hoc network systems:

■ **Battlefield interpersonal communication** is a scenario where telecommunication devices, carried by vehicles and soldiers, communicate in an ad hoc fashion without the need as well as the danger of using a base station (whose compromise would jeopardize the entire mission). The requirement for MC and TR is obvious. The assumption for PKCC can also be justified, while RU may not be as readily assumed. Hence, MC=T, TR=T, PKCC=T, RU=F.

■ **Battlefield sensor surveillance** is the class of systems in which minute wireless sensors (e.g. chemical sensors, seismic sensors etc.) are dispatched in military zones for critical surveillance. Signals Intelligence data are meant to be gathered from Unmanned Aerial Vehicles (UAVs) and relayed to the forward operating base for analysis and correlation. Because of the low cost and disposable design of sensor nodes, TR, PKCC and RU cannot be assumed. MC is undoubtably critical. Hence, MC=T, TR=F, PKCC=F, RU=F.

■ **Spontaneous networking** is, as described by Feeney *et al.* [4], a technology that allows people to meet and use their laptops, PDAs, tablets etc. to start collaborating on some tasks through wireless networking, i.e. in the absence of a fixed infrastructure. For the same reason why IPsec is invented, MC is important. TR, as applied to consumer hardware, cannot currently be assumed. PKCC is generally available although the performance varies widely across the classes of device. By the psychological reasoning that nobody wants to spend more energy than the others, we can assume that nobody wants to be a RU. Hence, MC=T, TR=F, PKCC=T, RU=F.

■ **SPINS-type sensor networks** refer to the class of networks with sensors deployed around a central base station. The presence of the base station immediately guarantees the existence of a RU. Hence, MC=T, TR=F, PKCC=F, RU=T.

■ **EYES networks** is the class of networks we design for the EYES project (`eyes.eu.org`). We envision our prototype to be a congregation of sensor networks for intelligent buildings. The sensors are meant to collaborate to achieve some desired functions, but often in the course of performing such functions, privacy and security-sensitive data are transmitted, so MC is to be enforced. For economic reasons, TR is not assumed. We expect our node to have PKCC because each sensor

will carry a 1MB serial RAM, which is large enough for the purpose. We also do not want to rule out the possibilities of RU, since the office environment is largely under our control. Note that even with these assumptions in place, we are not restricting ourselves to any specific architecture, centralized or decentralized. What we have in mind of the topology is a sea of sensors, some of which mobile and some static, peppered by tiny islands of relatively resource-rich devices. Hence, MC=T, TR=F, PKCC=T, RU=T.

To wrap up, system profile is a means of classification and assessment, it does not dictate what architecture should be adopted for which particular profile.

3. Conclusion

Realizing that one size does not fit all, we have introduced a unified assessment framework based on the notion of system profiles, not only to remind ourselves of the valid set of assumptions and requirements, but also to allow ourselves to concentrate on one profile at a time. Our research exercise has testified it to be a useful tool in assessing ad hoc networks.

References

[1] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti. Secure pebblenets. In *Proceedings of the 2001 ACM Int. Symp. on Mobile Ad Hoc Networking and Computing*, pages 156–163. ACM Press, October 2001.

[2] L. Buttyán and J.-P. Hubaux. Nuglets: A Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks. Technical Report DSC/2001/001, Department of Communication Systems, Swiss Federal Institute of Technology, 2001.

[3] D.W. Carman, P.S. Kruus, and B.J. Matt. Constraints and approaches for distributed sensor network security. Technical Report #00-010, NAI Labs, 2000.

[4] L. Feeney, B. Ahlgren, and A. Westerlund. Spontaneous networking: An application-oriented approach to ad hoc networking. *IEEE Communications*, 39(6):176–181, Jun 2001.

[5] J.-P. Hubaux, L. Buttyán, and S. Capkun. The quest for security in mobile ad hoc networks. In *Proc. of the ACM Symp. on Mobile Ad Hoc Networking and Computing (MobiHOC '01)*, pages 146–155. ACM Press, October 2001.

[6] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar. SPINS: Security Protocols for Sensor Networks. In *Proceedings of the 7th Ann. Int. Conf. on Mobile Computing and Networking*, pages 189–199. ACM Press, 2001.