A new approach towards authenticated key agreement schemes for resource-constrained devices

Christian Gorecki, Christian Behrens and Rainer Laur

ITEM – Institute for Electromagnetic Theory and Microelectronics
Department of Physics and Electrical Engineering, University of Bremen
Otto-Hahn-Allee, NW1
D-28359 Bremen, Germany
{gorecki, behrens, laur}@item.uni-bremen.de

Abstract: This paper describes a novel solution for authenticated key agreement for wireless sensor networks (WSN) in logistics. The retrieved data may not be spoofed as it is used to generate information about the quality of the freight, especially for sensitive freight like food. Instead of relying on pre-configuration, every sensor node is authenticated immediately before deployment (e.g. loading into a container) by adding an RFID-interface to every WSN node.

1 Introduction

Freight monitoring in supply chains is becoming ever important in supply chain management due to quality issues or legal requirements, especially in food logistics [Eu02]. The retrieval of up-to-date measurement data about the transportation environment (e.g. temperature, humidity, concentration of gases, shocks and vibrations) is used to generate information about the quality of the transported goods. This information may be linked with the status of the transportation media (e.g. type, speed, position etc.) and economic considerations (e.g. current pricing at neighbouring destinations, costs of logistic carriers), to support autonomous cooperating logistic processes [Fre04]. Communication security is one of the key issues towards the integration of WSN into supply chain management. The WSN must be protected from unauthorised access in order to prevent espionage and manipulation of sensor data (and thereby altering the quality information) or theft of the freight itself. Robust mechanisms for mutual authentication of the WSN devices and cryptographically secure means of communication have to be designed and implemented whereas the key-distribution marks the central issue for all subsequent security modules.

2 System Concept

A WSN system may be integrated into supply chain management by adding a gateway at transportation system level (e.g. a container). This gateway collects all data from the WSN and processes the gathered data and is able to communicate to distant logistic servers and networks using UMTS or WLAN.

The WSN nodes are transported together with the freight (e.g. fixed to pallets or boxes). When they are loaded into the transport media, they perform certain monitoring tasks that are defined by the transported freight.

As key distribution marks the central issue for secure communication appropriate means for secure key distribution have to be implemented. Pre-configuration of the nodes using network-wide keys or random key pre-distribution [Per04] is widely used in WSN systems but carries the risk that if one or a number of nodes have been compromised by an attacker, communication security becomes useless. The usage of Public-key cryptography (PKC) implies shared secrets or a trusted authority to enable secure key agreement schemes [Gua01]. But PKC is usually too resource intensive for common WSN hardware. The most suitable approach for WSN to yield the highest grade of security is the use of *cluster keys* for every group of nodes in a hierarchical cluster-based routing scheme [Kar03].

RFID is already a very popular technology in supply chain management. The freight is identified by its tags. These can be read during the loading process onto a transportation media using dock door readers. The basic idea now is to also employ this system for authentication mechanisms inside the WSN. This is done by employing RFID interface ICs (e.g. [Atm02]). These chips provide an RFID Read/Write-tag's functionality with an interface to a microcontroller.

3 Key agreement strategy

The WSN uses an IEEE 802.15.4[Ieee03] compliant RF interface. The gateway acts as the PAN-Coordinator and trusted authority for this network. The WSN network employs a cluster-based topology with sensor nodes serving as cluster-heads. A secure channel between the gateway and all cluster-heads is assumed. The RFID-system is considered to be specially secured (e.g. using cryptographic checksums, special antenna patterns, shielding etc.) to avoid eavesdropping of this channel.

When a sensor node is loaded together with the freight it is identified by its RFID interface. The gateway registers the sensor node database and writes an initial secret to the WSN node. In order to join the WSN the node waits for reception for a beacon frame on the RF link. This beacon frame inhibits Token1, composed of the cluster-head's ID and another initial secret that is shared between the Cluster-head and the gateway. The registering node sends a connect request including Token2. Token2 is comprised of the registering node's ID and its initial secret with the gateway. After reception of Token2 the clusterhead sends a node ID request to the gateway. If the registering node is authenticated, the gateway sends the registering node's initial secret to the clusterhead. The cluster head is now able to compute a set of keys from these collected parameters. This set is now included inside a Message Authentication Code (MAC) that forms Token3. If Token3 was successfully verified by the registering sensor node the clusterhead is implicitly authenticated. The registering node now answers to Token3 with another MAC (Token4) computed with the same key set.

Now a secure channel for distribution of cluster keys and configuration information is established. As all important exchanged messages and parameters are time-stamped, the proposed mechanism is protected against replay attacks.

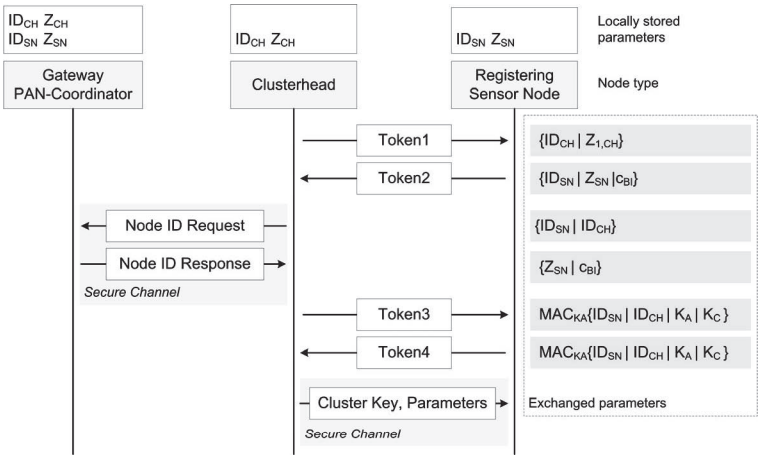

Figure 4: Registration procedure for a sensor node

4 Conclusion

A robust mutual authentication solution was presented using an additional RFID interface for superseding pre-deployment of keys. The key agreement scheme includes protection against replay and spoofing attacks. Due to its small footprint the scheme may also be used for authentication in other mobile systems. It may be integrated in IEEE 802.15.4 networks without significant communication or memory overhead.

References

[Atm02] Atmel AT88RF001 Datasheet, http://www.atmel.com/dyn/resources/prod_documents/DOC1943.PDF

[Eu02] EU REGULATION (EC) No 178/2002, http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_031/l_03120020201en00010024.pdf

[Fre04] Freitag et.al.: "Selbststeuerung logistischer Prozesse – Ein Paradigmenwechsel und seine Grenzen" (in german), Industrie Management, 20(2004)1, GITO, Berlin, 2004

[Gua01] J. Guajardo et.al.: „Efficient Implementation of Elliptic Curve Cryptosystems on the TI MSP430x33x Family of Microcontrollers", PKC 2001, Korea, 2001

[Ieee03] IEEE Standard 802.15.4: "Wireless MAC and PHY Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)", IEEE Press, 2003

[Kar03] C. Karlof et.al.: "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, vol. 1, 2003.

[Liu03] D. Liu et.al.: "Establishing Pairwise Keys in Distributed Sensor Networks", Proceedings of the 10th ACM CCS '03, 2003

[Per04] A. Perrig et.al.: "Security in Wireless Sensor Networks", Communications of the ACM, Vol. 47, No. 6, 2004