A Cryptographic Scheme for Real-World Wireless Sensor Networks Applications

S. Marchesani
Università degli Studi dell'Aquila – DEWS

L. Pomante
Università degli Studi dell'Aquila – DEWS

F. Santucci
Università degli Studi dell'Aquila – DEWS

M. Pugliese
Università degli Studi dell'Aquila – DEWS

{stefano.marchesani, luigi.pomante, fortunato.santucci}@univaq.it

marco.pugliese@ieee.org

This work deals with the cryptographic aspect of security applied to the WSN domain. In particular, it proposes a novel cryptographic scheme compliant to security requirements of real-world WSN applications (i.e. with very limited system resources). The proposed scheme exploits benefits from both symmetric and asymmetric ones where the keys, for each communicating node pairs, can be generated only if such nodes have been authenticated with respect to the network topology. In fact, the design of traditional secure networks is often based on asymmetric encryption. In such networks, the amount of available computational, memory and power resources make it possible to ignore the main pitfall of this strategy: the robustness of asymmetric algorithms is highly dependent on the length of the keys; length that affects the complexity of the involved algorithms. However, when computational resources are limited, asymmetric cryptography could be not feasible and symmetric cryptography must be revalued. In such a case, the most important problem to solve is *keys management*. As a main difference with respect to existing approaches, the proposed scheme doesn't rely on the pre-distribution of keys but it is based on their dynamic generation exploiting partial information stored on nodes. Then, through computationally inexpensive operations, a node can compute the decrypt/encrypt key in a single phase with no steps of setup/negotiation. Furthermore, the proposed approach allows to authenticate a message with respect to a set of planned network topologies. For this, it has been called TAK2 (*Topology Authenticated Key 2*, i.e. an improvement of [1]). Let be the *planned network topologies* the set of admissible network topologies planned by a service manager (i.e. *the planner*) to satisfy some service requirements. According to this definition, a network could automatically get the attribute of *certified network topology* where the certification authority is the planner itself. For this, the proposed scheme requires the offline definition of some data to allow their pre-distribution in the entire network. In fact, they are partial components needed to build the actual keys and are called *Local Configuration Data* (LCD). They define the topologies that each node is allowed to manage. LCD includes a *Private Key Component* and a *Local Planned Topology*. The security of proposed scheme is based on the confidentiality of such information so they have to be private (i.e. only a single node in the network can access to them) or at most restricted (i.e. any node in the network can access to them) and they cannot be random generated but they are calculated from deployment parameters that have to be secret (i.e. only the planner can access to them). In such a situation to violate the proposed scheme is more complex than solving the *Discrete Logarithm Problem*. Since the work refers to real-word WSN applications, TAK2 has been implemented in *nesC/TinyOS_1.x*. In particular, TAK2 has been integrated in the SW component provided by TinyOS_1.x to manage basic communications (i.e. *GenericComm*) while keeping its original interface to be completely transparent to the upper layers. Then, it has been replaced by the so called *SecureComm* component to provide the same interfaces while introducing described security mechanisms. The next step of the related project is to port the approach to the TinyOS_2.x platform so exploiting the proposed scheme with more recent HW/SW technologies.

Conference'04, Month 1–2, 2004, City, State, Country.

ACKNOWLEDGMENTS

This work has been partially supported by the *ERC Starting Grant VISION* (Contract n. 240555).

REFERENCES

[1] Pugliese M., Santucci F., Pair-wise Network Authenticated Hybrid Cryptographic Keys for Wireless Sensor Networks using Vector Algebra, 4th IEEE International Workshop on Wireless Sensor Networks Security, 2008