Security Mechanisms for Multi-Purpose Sensor Networks

Jan Steffan Marco Voss

{steffan,voss}@ito.tu-darmstadt.de

Abstract: Multi-purpose sensor networks provide an infrastructure that is shared by multiple parties for the execution of concurrent tasks. This setting has direct implications for security: Access to certain sensor nodes and visibility of sensor data has to be restricted to the authorized party. We extend our earlier work on scope based group management for wireless sensor networks with cryptographic mechanisms that meet those requirements under the given constraints[1].

1 Introduction

In [SFCB04] we introduced scoping as a means of partitioning a wireless sensor network (WSN) into groups of nodes at run-time. This enables the concurrent use of a sensor network for multiple applications. Such multipurpose WSNs are required in scenarios where the same WSN would be useful for multiple different tasks and parties. This not only requires means of dynamically assigning tasks and users to sets of sensor nodes, but also of enforcing the boundaries between different tasks, parties and node sets.

Scopes which are described briefly below provide a means of structuring a WSN by creating groups of nodes for different uses at runtime. This allows different parties to use the same sensor node infrastructure while preserving administrative separation.

In scenarios that involve multiple parties the capability of scopes to delimit tasks and parties to a certain groups of nodes needs to be complemented by adequate security measures that enforce these boundaries. In this paper we describe how authorization of scope creation and end-to-end data privacy can be implemented using nested scopes and public key cryptography.

Scopes Scopes are basically specifications of groups of nodes. The extent of a scope, i.e., the set of its member nodes, is specified through a boolean expression over node properties such as location or the availability of a certain sensor type. The central idea of this approach is that queries or other tasks are not disseminated to all sensor nodes, but only to a group of nodes that is specified by a previously instantiated scope.

Scopes can be created by an administrator or by another party that is privileged to do so. Scopes are persistent and can be used for multiple tasks in sequence. During its life-time

[1] A longer version of this paper is available as a technical report [SV05].

a scope's connectivity and set of member nodes is maintained in order to reflect changes in network topology and node properties.

Security Requirements We are focusing on data privacy issues of multipurpose WSNs, which imposes the following security requirements: *a)* Restrict access to the member nodes of a scope so that only authorized parties or entities are allowed; *b)* Restrict the visibility of clear-text sensor data collected by these nodes to the authorized party; *c)* A flexible mechanism for granting different levels of access to the various parties; *d)* Policies must be adaptable at run-time.

Additionally, the resource restrictions of WSN nodes demand lightweight cryptographic operations limited to those occasions where strong protection is really needed.

2 Cryptographic Protection of Scopes

Our security extension for scopes is based on public key cryptography. An important property is that expensive operations like the creation of key pairs or private key operations are limited to the node that manages a scope or to the WSN's gateway for externally managed scopes. The rest of the nodes are restricted to perform relatively lightweight public key operations. The feasibility of this within the constraints of WSNs was shown by Watro et al. in [WKfC+04].

2.1 Key Exchange

Access control is managed at the level of scopes. A *scope's owner* i.e., the entity or party that created the scope, remains associated with the scope throughout its lifetime. Before scope creation a public/private key-pair is generated by the owner. The private key remains at the owner while the public key is disseminated to the scope's member nodes with the scope creation request. There is one special global scope that includes all of the nodes. It is owned by an administrator and its public key is preinstalled on each node..

Any request or task directed to the member nodes of a scope have to be signed with the associated private key of the scope's owner. A party's request for the creation of a new sub-scope of the global scope has to be signed by the administrator. The party's public key associated with the new scope is disseminated with the scope creation. All tasks directed to member nodes of the scope have to be signed with the party's private key. Using the public key scope members can verify that messages really originate from the same party that created the scope. Other parties cannot request the execution of tasks within the scope neither request the creation of a nested sub-scope.

Sensor readings and other data originating from the member nodes of a scope is sent back to the scope's owner. The owner can request that data is encrypted with its public key that the scope members have received during scope creation or an individually established

symmetric key. Having encryption as an option allows us to tailor the use of resources to the applications needs on scope level.

2.2 Security Evaluation

Eavesdropping As described above sensitive data can be protected from disclosure by encrypting it with the scope's public key. Additional keys are introduced for each party using the WSN. To protect administrative messages from replay attacks they should contain a timestamp or transaction counter. Man-in-the-middle attacks are not possible since the public key of the global scope is preinstalled on each node. As long as the global scope's private key is not compromised, the authenticity of messages can be verified by each node.

Node capturing In contrast to WSNs secured by a shared symmetric key, an attacker does not gain any benefit by capturing a single node since it does not contain any secret key information. Our scheme does not prevent manipulation by inserting false sensor data. This however, is difficult to achieve in general as it would require the prevention of any manipulation of sensor nodes.

3 Conclusion

Although this scheme does not cover mutual authentication between any pair of sensor nodes it covers the most important security aspects of multi-purpose sensor networks: A mechanism for granting access to nodes within scopes to different parties and the option to restrict the visibility of sensitive data originating within the scope to the respective party. Both mechanisms are cryptographically protected and can be implemented in a way that complies well with the resource restrictions of sensor nodes. In addition, access privileges can be managed by an administrator, delegated to other parties based on a scope level.

References

[SFCB04] Jan Steffan, Ludger Fiege, Mariano Cilia, and Alejandro Buchmann. Scoping in wireless sensor networks: A position paper. In *Proceedings of the 2nd Workshop on Middleware for Pervasive and Ad-hoc Computing*, pages 167–171. ACM Press, October 2004.

[SV05] Jan Steffan and Marco Voss. Security Mechanisms for Multi-Purpose Sensor Networks. Technical Report TUD-CS-2005-2, TU Darmstadt, 2005.

[WKfC+04] Ronald Watro, Derrick Kong, Sue fen Cuti, Charles Gardiner, Charles Lynn, and Peter Kruus. TinyPK: securing sensor networks with public key technology. In *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 59–64, New York, NY, USA, 2004. ACM Press.