UNIVERSITY
OF TRENTO

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

38050 Povo – Trento (Italy), Via Sommarive 14
http://www.dit.unitn.it

HIERARCHICALLY DISTRIBUTED ACCESS CONTROL PROTOCOL FOR WIRELESS SENSOR NETWORK

G. Boato, F. G. B. De Natale, C. Fontanari, and A. Massa

June 2007

Technical Report DIT-07-044

Hierarchically Distributed Access Control Protocol for Wireless Sensor Networks

G. Boato[1], F. G. B. De Natale[1], C. Fontanari[2], and A. Massa[1]
[1]Dept. of Information Engineering and Computer Science, University of Trento,
Via Sommarive 14, I-38100, Trento, Italy, tel +39 0461 883193, fax +39 0461 882093
[2]Dept. of Mathematics, School of Information Technologies, Politecnico di Torino,
Corso Duca degli Abruzzi 24, I-10129, Torino, Italy, tel +39 011 5647521 fax +39 011 5647599
boato@disi.unitn.it; {denatale, andrea.massa}@ing.unitn.it; claudio.fontanari@polito.it

***Abstract*— We address the widely open problem of access control in wireless sensor networks (WSN). Namely, we apply a suitable threshold secret sharing scheme relying on advanced polynomial interpolation theory to design a distributed access control protocol exploiting the natural hierarchical structure of the WSN.**

I. Introduction

Wireless sensor networks (WSN) are commonly considered as one of the most important technologies for the 21st century, with challenging applications to environmental monitoring, emergency medical care, industrial remote control. As incisively summarized in [1], with respect to general mobile ad hoc networks (MANET), the peculiarities of a WSN are related to the unavoidable presence of at least one base station and to the fact that a sensor node has a small embedded processor with more limited memory and energy, thus imposing stronger light weighting requirements. Both WSN and MANET present a larger spectrum of efficiency and security problems than conventional wired and even wireless networks, mainly related to higher vulnerability of nodes, often placed in a hostile or dangerous environment where they are not physically protected and hence are easy to be captured, eavesdropped, or tampered. Indeed, as clearly explained in [2], misbehavior in a MANET, where nodes are both routers and terminals, can be defined as deviation from regular routing and forwarding and without suitable countermeasures the effects of misbehavior have been shown to dramatically decrease network performance.

Here we mainly focus on the crucial issue of additional node access. As pointed out in the recent contribution [3], little work has been reported so far to address the access control problem in sensor networks. As clearly explained in the same paper, the critical problem from this point of view is that under current sensor network security technology a malicious new node could join the network and become indistinguishable from legitimate new nodes. Here we exploit distributed access as a reliable solution. This way, a node trying to access the WSN needs to get authorization from different WSN participants. In the present paper we introduce a novel access control protocol based on a hierarchical secret sharing scheme. Namely, we propose to adapt distributed access to a fixed hierarchical structure. Just to suggest a couple of realistic examples, we outline the following scenarios:

(i) a reputation mechanism ([2]) is active–it can either be distributed (see for instance [4]), where each node rates the behavior of neighboring nodes and updates a reputation metric for each of them; or centralized (see for instance [4]), where a trusted supervision authority communicates with all nodes and store nodes reputations, thus alleviating the need for sharing locally kept reputation metrics;

(ii) the WSN is regarded as to be intrinsically hierarchical, with a higher level corresponding to the manager nodes in the base stations, a middle level collecting cluster heads with the role of master agents, and a lowest level with all other remaining nodes, acting as slave agents ([1]).

We propose a distributed access control scheme which takes into account such different trust levels. More precisely, we design a hierarchical secret sharing scheme which allows a new node to access the network by requiring authorization from a prescribed configuration of nodes of different levels. Communication among the new node and its neighbors in the network can be easily made secure (in particular from eavesdropping) by key pre-distribution or public key cryptography (see for instance [3]). Note also that hierarchical secret sharing

has already been successfully applied to security issues in ad hoc networks in [5].

We recall that a (k, n)-threshold sharing scheme allows to divide a secret into n shares and requires the knowledge of at least k out of n shares to reconstruct the original content. The basic scheme, due to Shamir [6], relies on standard Lagrange polynomial interpolation and allows a hierarchical variant by simply assigning a higher number of shares to higher level participants. Here instead we exploit a more sophisticated mathematical tool, namely, Birkhoff interpolation [7], which involves not only the polynomial, but also its higher order derivatives. Roughly speaking, the idea is to split the secret access key needed to access the network into several hierarchical shares and to provide each WSN node with a different share corresponding to its level. This seems to be more efficient (assigning just one share to each member) and realistic (attributing a qualitative rather than a quantitative difference between distinct levels). Next, the nice geometrical properties of Birkhoff polynomial interpolation allow a further node to join the network after reconstructing the secret key from a subset of nodes if and only if such a subset contains a prescribed number of members for each level in the network hierarchy.

The structure of the paper is the following: in Section II we introduce the concept of access structure, while in Section III the distributed access control protocol is described. Some concluding remarks and future perspectives are reported in Section IV, while Section V is fully devoted to more technical mathematical arguments.

II. Hierarchical Access Structure

Here we describe how to manage the access key in a distributed way among nodes belonging to different levels of the fixed hierarchy (see example in Fig. 1).

Let the WSN be composed of n nodes and let us consider a collection Γ of subsets of the network. A threshold secret sharing scheme with access structure Γ is a method of sharing a secret among the nodes of the WSN, in such a way that only subsets in Γ can recover the secret, while all other subsets have no information about it. Hence we have to assume that Γ is monotone in the sense that if $V \in \Gamma$ then any set containing V also belongs to Γ. We also assume that the WSN participants are divided into $t+1$ levels, i.e., WSN$= \cup_{l=0}^{t} N_l$ with $N_i \cap N_j = \emptyset$ for every $i \neq j$ (levels may change in time due to the dynamic nature of the WSN). In order to reconstruct the secret, we require at least a fixed number of shares from each level (see example in Fig. 2).

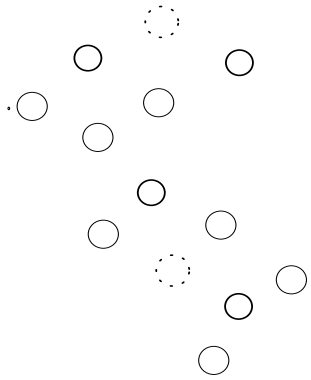

Fig. 1. Example of hierarchical WSN structure: dashed line nodes consist on nodes of higher level; thick solid line nodes are middle level nodes; thin solid line nodes consist on nodes of lower level.

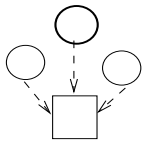

Fig. 2. Example of distributed access control: the squared node obtains the required authorization to join the network of Figure 1 from at least three nodes of middle or lower level, among which at least one of middle level.

Formally, if $0 < k_0 < \ldots < k_t$ is a strictly increasing sequence of integers, then a $(k_0, \ldots, k_t; n)$-hierarchical threshold secret sharing scheme distributes to each WSN participant a share of a given (periodically refreshed) secret access key S, in such a way that

$$\Gamma = \left\{ V \subset WSN : \#\left[V \cap \left(\cup_{l=0}^{i} N_l \right) \right] \geq k_i \ \ \forall i \right\} \quad (1)$$

Roughly speaking, a subset of nodes can reconstruct the secret key if and only if it contains at least k_0 members of level 0; at least k_1 members of level 0 and/or level 1; at least k_2 members of level 0 and/or 1 and/or 2; and so on.

More precisely, in order to define a suitable $(k_0, \ldots, k_t; n)$-hierarchical threshold secret sharing scheme for WSN node access control (see Fig. 3) we can proceed as follows.

1) Identify the secret key S for access control with a sequence $(S_0, \ldots, \ S_z)$ with $S_i \in \mathbb{R}$ for every $0 \leq i \leq z$.
2) Let $k = k_t$ and pick a polynomial

$$p(x) = \sum_{i=0}^{k-1} a_i x^i \quad (2)$$

where $a_i = \begin{cases} S_i & 0 \leq i \leq z \\ \text{random} & z+1 \leq i \leq k-1. \end{cases}$

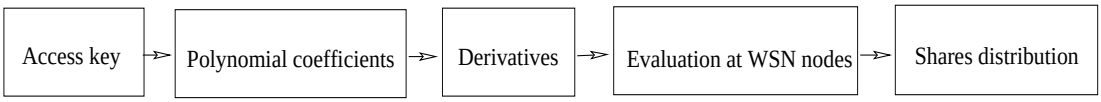

Fig. 3. Access key distribution among WSN participants.

3) Identify each node of level l with a random element $v \in \mathbb{R}$ and associate to v the share $p^{(k_{l-1})}(v)$, where $p^{(k_{l-1})}(v)$ denotes the k_{l-1}-th derivative of p and by definition $k_{-1} = 0$.

Intuitively speaking, an evaluation of the polynomial itself carries more information than an evaluation of any of its derivatives since it involves more coefficients; therefore it sounds reasonable to assign to a participant of higher level the evaluation of a lower order derivative. In such a way, we will be able to apply Birkhoff interpolation theory to properly define and effectively manage a hierarchical access structure.

III. Access Control Protocol

In order to access the WSN, a node v_{new} needs to reconstruct the secret key S. We propose the following strategy (see Fig. 4).

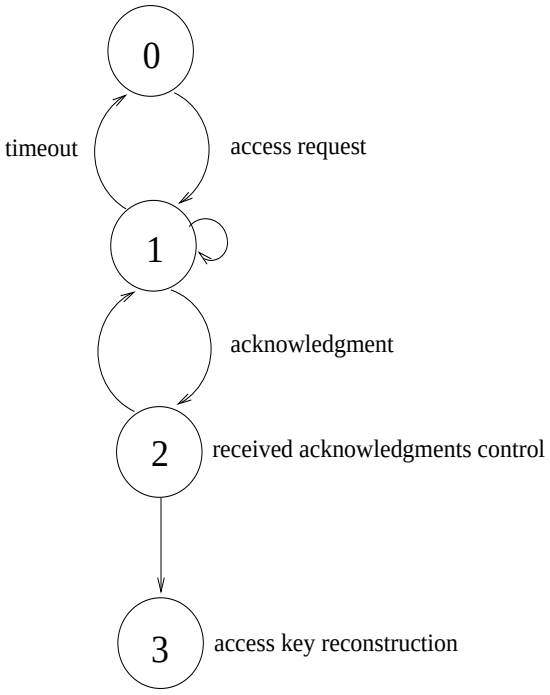

Fig. 4. Access control protocol.

1) Starting from the idle state (state 0), the node v_{new} sends an access request in broadcast, starting at the same time a suitable timeout procedure in order to avoid deadlocks, and waits for acknowledgments from the network (state 1).
2) A node v_i, already belonging to the network, can reply to v_{new} by sending in unicast an acknowledgment containing the data $\left(k_0, \ldots, k_t; l_i, v_i, p^{(k_{l_i-1})}(v_i)\right)$, where l_i denotes the hierarchical level of v_i. After receiving any acknowledgments, v_{new} stores them (state 2) until either v_{new} collects a subset of shares belonging to the access structure Γ or time expires, in which case the access control protocol fails.
3) The node v_{new} has now at its disposal the shares corresponding to a subset $V = \{v_1, \ldots, v_m\} \in \Gamma$ with $m \geq k$. Up to reordering we may assume that $v_i \in V_{l_i}$ with $l_i \leq l_j$ for every $i \leq j$. Consider the $m \times k$ matrix M_V whose i-th row is given by

$$\frac{d}{dx^{k_{l_i-1}}}\left(1, x, x^2, \ldots, x^{(k-1)}\right)(v_i) \qquad (3)$$

In order to reconstruct the secret key S, v_{new} has to solve the following linear system:

$$M_V \begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} p^{k_{l_1-1}}(v_1) \\ \vdots \\ p^{k_{l_m-1}}(v_m) \end{pmatrix} \qquad (4)$$

in the unknowns $a_0, \ldots, a_{k-1}$. Indeed, the fact that $V \in \Gamma$ implies that (4) has a unique solution (see Mathematical Appendix), corresponding by definition of the coefficients a_i to the secret key S (state 3, see also Fig. 5). Hence the access control protocol is over and v_{new} can access the network.

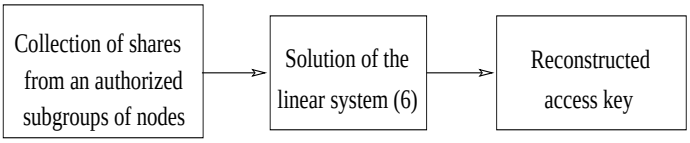

Fig. 5. Access key reconstruction.

We point out that the same procedure could be adapted (by replacing S and Γ with the access key S' and the access structure Γ' corresponding to a higher level of the WSN hierarchy) by a node v already belonging to the network in order to upgrade its level.

IV. Conclusion

After reviewing the peculiarities of WSN among MANET and providing a couple of examples of natural hierarchical structures for WSN, we have introduced a novel distributed access control protocol for WSN which is adapted to a fixed hierarchical structure. The protocol is based on a sophisticated threshold secret sharing scheme relying on advanced polynomial interpolation theory. Full rigorous mathematical details have already been provided, while a thorough both numerical and experimental evaluation of the proposed method is currently the subject of work in progress.

V. Mathematical Appendix

Here we provide the theoretical framework for secret reconstruction, namely we show that the following holds:

Theorem 1. *The secret S can be reconstructed from the shares belonging to V if and only if $V \in \Gamma$.*

The key point is that (4) is a Birkhoff interpolation problem according to the following:

Definition 1. *Let $E = (E_{i,j})$, $i = 1, \ldots, m$; $j = 0, \ldots, k-1$, be an $m \times k$ interpolation matrix, with k entries equal to one and all remaining ones equal to zero. Let $X = x_1, \ldots, x_m$, $x_1 < x_2 < \ldots < x_m$, be a set of m distinct interpolation points. The associated Birkhoff interpolation problem is given by the k interpolation equations*

$$p^{(j)}(x_i) = B_{i,j} \tag{5}$$

for every i, j with $E_{i,j} = 1$, where $p^{(j)}$ denotes the j-th derivative of a polynomial p of degree $\leq k-1$, $B_{i,j} \in \mathbb{R}$ are given data, and the unknowns are the k coefficients $a_0, \ldots, a_{k-1}$ of p.

Moreover, recall from [7], p. 126, that by elementary linear algebra if the interpolation matrix $E = (E_{i,j})$, $i = 1, \ldots, m$; $j = 0, \ldots, k-1$ does not satisfy the following *Pólya condition*

$$\#\{E_{i,j} = 1 : j \leq h\} \geq h + 1, \quad 0 \leq h \leq k-1 \tag{6}$$

then the corresponding Birkhoff interpolation problem admits infinitely many solutions.

The interpolation matrix $E_V = (E_{i,j})$, $i = 1, \ldots, m$; $j = 0, \ldots, k-1$ associated to (4) is:

$$E_{i,j} = \begin{cases} 1 & \text{if } j = k_{l(i)-1} \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

The proof of Theorem 1 is based on the following auxiliary result (see [5] Lemma 1):

Lemma 1. *$V \in \Gamma$ if and only if E_V satisfies the Pólya condition.*

Proof of Theorem 1: First we show that if $V \notin \Gamma$ then the secret S cannot be reconstruct by V. Indeed, by Lemma 1 E_V does not satisfy Pólya condition and it follows that the corresponding Birkhoff interpolation problem admits infinitely many solutions. Thus V cannot reconstruct the secret.

Next, we have to check that if $V \in \Gamma$ then V is enough to recover the secret S. In order to do so, by Lemma 1 and our random selection of the interpolation points, we can apply Theorem 10.1 in [7], p.128, and conclude that the Birkhoff interpolation problem admits a unique solution, which conveys the embedded secret. Hence Theorem 1 is completely proven. □

References

[1] D. Shangwei and Y. Xiaobu. *Exploring hierarchy architecture for wireless sensor networks management*. Proc. of the IFIP International Conference on Wireless and Optical Communications Networks, 2006.

[2] S. Buchegger and J.-Y. Le Boudec. *Self-Policing Mobile Ad Hoc Networks by Reputation Systems*. IEEE Communications Magazine, July 2005, 101–107.

[3] Y. Zhou, Y. Zhang and Y. Fang. *Access control in wireless sensor networks*. Elsevier Ad Hoc Networks, Vol. 5 (2007), 3–13.

[4] S. Vassilaras, D. Vogiatzis and G. S. Yovanof. *Security and Cooperation in clustered mobile ad hoc networks with centralized supervision*. IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2 (2006), 329–342.

[5] E. Ballico, G. Boato, C. Fontanari, and F. Granelli. *Hierarchical secret sharing in ad hoc networks through Birkhoff interpolation*. Advances in Computer, Information, and Systems Sciences, and Engineering. Proceedings of IETA 2005, TeNe 2005 and EIAE 2005. Springer (2006).

[6] A. Shamir. *How to Share a Secret*. Communication of the ACM, Vol. 22 (1979), 612–613.

[7] R. A. DeVore and G. G. Lorentz. *Constructive Approximation*. Grundlehren der Mathematischen Wissenschaften 303, Springer-Verlag, Berlin, 1993.

[8] J.-P. Berrut and L. N. Trefethen. *Barycentric Lagrange Interpolation*. Siam Review, Vol. 46, No. 3 (2004), 501–517.