R. Roman, J. Zhou, and J. Lopez, "On the Security of Wireless Sensor Networks", *Computational Science and Its Applications (ICCSA05)*, LNCS vol. 3482, pp. 681-690, 2005.
http://doi.org/10.1007/11424857_75
NICS Lab. Publications: https://www.nics.uma.es/publications

On the Security of Wireless Sensor Networks

Rodrigo Roman[1], Jianying Zhou[1], and Javier Lopez[2]

[1] Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613
roman@lcc.uma.es, jyzhou@i2r.a-star.edu.sg
[2] E.T.S. Ingenieria Informatica, University of Malaga, 29071, Malaga, Spain
jlm@lcc.uma.es

Abstract. Wireless Sensor Networks are extremely vulnerable against any kind of internal or external attacks, due to several factors such as resource-constrained nodes and lack of tamper-resistant packages. As a result, security must be an important factor to have in mind when designing the infrastructure and protocols of sensor networks. In this paper we survey the "state-of-the-art" security issues in sensor networks and highlight the open areas of research.

1 Introduction

Wireless Sensor Networks [1], composed of hundreds or thousands of inexpensive, low-powered sensing devices with limited computational and communication resources, provide a useful interface to the real world with their data acquisition and processing capabilities. Sensor networks can be applied to a large number of areas, and its applications are continuously growing.

However, sensor networks are extremely vulnerable against any type of internal or external attacks, due to resource constraints, lack of tamper-resistant packaging, and the nature of its communication channels. In this scenario, any protocol, architecture or application which is not developed with security in mind is hardly useful.

As a result, it is essential to incorporate security, or at least to discuss whether it should be applied or not and why, inside the design of every aspect of a sensor network. In this paper, we present a survey of the "state-of-the-art" security issues and algorithms that a designer must have in mind while working with sensor networks.

The rest of the paper is organized as follows. In Section 2, we introduce the sensor network infrastructure and elements. In Section 3, we investigate the "state-of-the-art" security issues in sensor networks such as security primitives, key infrastructure, routing, data aggregation, auditory etc. In Section 4, we conclude our paper, highlighting the research challenges in those areas.

2 Sensor Network Infrastructure

The infrastructure of a sensor network can be divided into two parts, *data acquisition network* and *data dissemination network*.

– The data acquisition network contains the sensor network "per se": a collection of sensor nodes with the task of measuring the physical data of its surroundings, and one or more base stations in charge of collecting data from the nodes and forwarding control information from the users.
– The data dissemination network is a combination of wired and wireless networks that provides an interface of the data acquisition network to any user, and its security is out of scope of this paper.

Sensor nodes are densely deployed either very close or inside the object to be observed, and all measurements must be routed to the base station where users can have access to them. All the nodes are highly constrained devices. Their memory, computational power and battery life are very limited. On the other hand, base stations are not as constrained as the sensor nodes, and in most cases have no battery shortage problem.

Due to the extreme constraints of the network infrastructure, a sensor network is highly vulnerable against any external or internal attack, thus the infrastructure and protocols of the network must be prepared to manage these kinds of situations. Protecting the information flow not only requires a set of power-efficient encryption schemes, but also an effective key infrastructure in terms of key storage policies, key distribution procedures and key maintenance protocols. Collecting the information from a static or dynamic set of nodes and routing it through the error-prone, unreliable network is a difficult task as well. Moreover, the network should be able to monitor over any failures or security breaches in any of its members while self-configuring and self-healing itself.

3 Security Issues in Sensor Networks

3.1 Security Primitives

All sensor nodes inside a sensor network use power-efficient radio transceivers for their communications. Most of the existing sensor nodes operate in unlicensed frequency bands, but some nodes follow the IEEE 802.15.4 standard for Personal Area Networks [3]. In any case, a malicious adversary can easily get access to the information flow of a sensor network, because sensors are usually scattered in an uncontrolled or public environment and the wireless communication channel is inherently insecure. Consequently, any device can eavesdrop or inject packets inside the sensor network.

It is indispensable to provide basic security primitives to the sensor nodes in order to give a minimal protection to the information flow and a foundation to create secure protocols. Those security primitives are *symmetric key encryption* schemes (SKE), *message authentication codes* (MAC), and *public key cryptography* (PKC). Since sensor nodes are highly constrained in terms of resources, implementing the security primitives in an efficient way (using less energy, computational time and memory space) without sacrificing the strength of their security properties is one of the major challenges in this area.

Existing sensor nodes are able to incorporate software-based SKE with minor overhead in terms of CPU, energy and memory footprint. A proof-of-concept implementation is the TinySec [4] project. Hardware-based SKE is also provided in nodes with radio chips conforming to the 802.15.4 standard [3], although not all the security suites used by the standard are actually secure [5].

Regarding the MAC, it is usually computed using a cipher block chaining construction, called CBC-MAC. It is efficient and fast, and reduces the memory footprint needed for the MAC calculations due to the shared primitives between itself and the SKE. It is used by both hardware [3] and software [4] configurations.

Finally, PKC in software has been usually rejected as "not possible" in a sensor network environment, but there were almost no experiments that backed up the claim. Some studies [6] claimed that *elliptic curve cryptography* (ECC) seemed to be a good candidate for implementing PKC over sensor networks due to its small key size, faster computation, as well as memory and energy savings compared with other algorithms such as RSA. That claim was empirically demonstrated by a recent work in the area that developed a usable PKC in TinyOS [7].

3.2 Global Key Infrastructure

The communication channels between any pair of devices inside the sensor network must be protected to avoid attacks from external parties. This protection is provided by the security primitives introduced in the previous section, but all those primitives need to store a set of secret keys inside every node. Thus it is necessary to have a global key infrastructure.

There are three basic factors in the design of a key infrastructure for sensor networks: *key storage*, *key distribution*, and *key maintenance*.

- Key storage policies indicate the number of keys that a sensor node needs to store in order to open secure communication channels with other peers. It will influence over the network resilience, which defines the percentage of the network that can be controlled by an adversary after he steals the keys from a subset of the nodes, and over the amount of memory available to the node.
- The key distribution protocols define how the keys are issued to the sensor nodes. A node can receive its keys before the initial deployment of the network or create its keys after the deployment using preloaded information.
- The key maintenance procedures specify how a node can be included into or erased from the network, receiving or nullifying a set of keys in the process.

In terms of key storage, there are two extreme design cases: *global keying* (a single key is created for the entire network) and *pairwise keying* (a node must store a key for every other node inside the network). Neither of these cases is feasible in a real scenario: Global keying has no network resilience while pairwise keying is not a scalable solution due to the memory constraints of the nodes. Therefore, security researchers have been trying to develop more optimal solutions, such as pairwise keying only with every direct neighbor.

"Key pool" paradigm, introduced in [8], seeks to obtain a balance in the key storage policy while predistributing the secret keys before the deployment. In this paradigm, every sensor retrieves a certain number of keys from a common "key pool", and only the nodes that share a key (or a certain set of keys [9]) from their own pools can interchange messages securely. The number of keys of a pool and the number of keys that every node retrieves from the pool are factors that influence over the network resilience, memory usage and network connectivity.

Evolutions of the original "key pool" scheme aim to optimize the construction of the key pool and/or the distribution of keys from the pool, assuring a local coverage of 100% in most cases while decreasing the size of the local pools. Those optimizations are based on the Bloom scheme [10–12] or on combinatorial designs [13]. Other schemes improve the distribution of the keys using "a priori" information about the physical deployment of nodes [14], where nodes that are in the same physical area receive keys from the same subset of the key pool.

Other protocols can offer a balanced key storage policy while creating the keys after the network deployment. There is one solution that relies on negotiating the pairwise keys of a neighborhood with the base station [15], although this would be inconvenient for highly populated networks. A simpler model allows nodes to negotiate with their neighbors the pairwise keys, in "clear", just after the network deployment [16], because the treat level at this point is, in most scenarios, very low.

The advent of public key cryptography over sensor nodes [7] opens a new, uncharted area in the field of key infrastructures for sensor networks. PKC could help on the secure creation of pairwise keys after deployment and on the key maintenance procedures, which is a field in key infrastructure not fully addressed in the previous schemes.

3.3 Local Key Infrastructure - Secure Groups

There are some situations during the lifetime of a sensor network where a subset of the sensor nodes must group themselves in order to cooperate and fulfill a certain task. These groups must have a local key infrastructure, allowing them to open secure channels between members of the group and to broadcast messages inside the group. Securing a group inside an already protected sensor network is not redundant, because there are some cases where the group needs that protection.

Authentication is an important issue in protecting secure groups. A message addressed to all or a subset of the group must be properly authenticated, or any message from inside or outside the sensor network can be mistaken, deliberately or not, as addressed to the group. Confidentiality is also important, because in some cases, such as measuring critical factors in nuclear power plants, the group would want to hide the measurements from the other parts of the network. Finally, the integrity of the messages is critical as well, because without it the measurements and control messages would be prone to be attacked.

As in the global key infrastructure, there are three basic factors to be solved when designing the key infrastructure of a secure group: key storage policies,

key distribution protocols, and key maintenance procedures. However, securing a sensor group is completely different from securing the entire network. First, groups are normally created dynamically, when the base station commands to do so or where a particular set of readings (e.g., a truck approaching) force the network to organize itself. In these cases the keys of the group must be negotiated and distributed to all the members. Second, the nodes belonging to a group must be able to store all the necessary keys for the secure communications, having in mind that there may be no memory space at all in some extreme cases. Third, nodes will be added and deleted from the group in a more frequent basis, as for example when a truck is moving over the sensor field. These maintenance operations must be safe for the group, in the sense that an external node should not enter into the group when it is not invited and an internal node should not leave the group when it is not the time. Finally, the group should satisfy two more requirements: "forward security", where nodes left the group should not be able to access the current information flow of the group, and "secure tunnel", where a measurement made by the group and directed to the base station should not be accessed by the routing nodes in some essential cases, such as the nuclear power plant scenario.

The topic of secure grouping has not been intensely researched over the past years, and only few resource-demanding solutions exist [17]. An exception has been the protection of static groups, created before the initial deployment of the network, where more powerful nodes called "cluster heads" are in charge of managing and protecting the group [18]. Still, new optimal schemes that allow the sensor network to create and maintain secure groups by itself using as less resources as possible are needed.

3.4 Routing

In wireless sensor networks it is not possible to transmit messages directly (i.e., in one hop) from one node in the network to another. Therefore, it is necessary to provide a routing infrastructure. Designing routing algorithms is a challenging area [19]. All the nodes inside the sensor network should be reachable (*connectivity*) while covering the maximum possible area of environment using their sensors (*coverage*), even when the nodes inside the network start to fail due to energy shortage or other problems (*fault tolerance*). The algorithm should also work with any network size and node density (*scalability*) and provide a certain quality of service. At the same time, designers must try to lower the memory usage and energy consumption of the algorithms.

Security is another factor that cannot be ignored in the design of routing algorithms. Any potential adversary has a wide range of attacks at his disposition [20, 21] to manipulate the routing subsystem and take control over the routes, resulting in eavesdropped, altered, spoofed or discarded packets. The key infrastructure may help in the defense against routing attacks by authenticating nodes and protecting the confidentiality and integrity of the packets, but it is not enough to protect the whole routing infrastructure. Therefore, it is essential to make the routing algorithm robust against such attacks.

In the literature, there has been some work that protects previously existent routing protocols such as directed diffusion [22]. Another branch of research focused on discovering new protection techniques. For example, in [23] the route discovery algorithm creates redundant paths from the nodes to the base station, taking advantage of the network density. Also, in [24] nodes equipped with physical location services can locate and map the routing holes in the network. But most of the existent routing protocols do not take security into account in any step of their design. As a conclusion, the main challenge in this area is to discover new protection techniques and apply them into new algorithms, without sacrificing primary design factors such as connectivity, coverage, scalability, etc.

3.5 Data Aggregation

Inside a sensor network, the nodes generate an immense amount of raw data product of their measurements. In most cases these data are needed at the base station, thus there is a great cost, in terms of energy consumption and bandwidth usage, on transporting all the data from the nodes to the base station. However, since nodes are physically near each other, the data likely have some type of redundancy. The role of aggregation is to exploit this redundancy by collecting the data from a certain region and summarizing it into one report, hence decreasing the number of packets sent to the base station.

Aggregated data can be easily attacked by a malicious adversary, even if the communications are protected against any data injection attack or data integrity attack. If an aggregator node is being controlled by an adversary, it can easily ignore the data received from its neighbors and create a false report. Trusted aggregators can still receive false data from faulty nodes or from nodes being controlled by an adversary.

By using strong aggregation functions that are resilient against internal attacks, it is possible to defend the network against false data coming from malicious or faulty nodes. As an example, the author in [25] developed a theoretical framework for analyzing the resilience of a number of natural aggregation functions borrowing ideas from the field of robust statistics, although the aggregation is supposed to be carried out in the base station.

There are also solutions that discover whether the reports sent by a malicious aggregator are forged or not. In one approach [26] the aggregator must create a proof of its neighbors' data (e.g. using a Merkle hash tree), which will be used in a negotiation with the base station to demonstrate the authenticity of the data used to construct the report. Other approaches [27] take advantage of the density of sensor networks by using the nodes in the neighborhood of the aggregator as witnesses. Finally, it is also possible to filter the packets containing the report and the proofs in their way to the base station, hence decreasing the amount of traffic created by false aggregations (e.g. by using a Bloom filter [28]).

The field of secure aggregation has still room for more improvements. Interactive protocols between aggregators and the base station require more traffic for the negotiation, introduce a delay in the aggregation service, and are not scalable without an aggregation testing hierarchy. Proof-based systems usually require a

negotiation between the aggregator node and its witnesses and increase the size of the reports sent to the base station. New solutions should try to minimize the amount of negotiations carried out by these algorithms, and to introduce new ways to early detect and eliminate false reports.

3.6 Auditory

In a sensor network the user will have, in most cases, only access to the base station or to the data dissemination subsystem connected to the base station. As a result, any change of the internal state of a node in the network, such as low energy level or hardware failure, will go unnoticed unless the node itself reports to the base station. Therefore, it could be interesting to provide an auditory subsystem inside the network to query about its internal status and to receive information about internal events.

A possible application of that auditory subsystem could be an *intrusion detection system* (IDS). IDS can monitor the activities of a network, gathering and analyzing audit data, in order to detect intrusions and alert users when an attack is taking place. IDS is in fact a "second line of defense" - if a malicious adversary takes control of certain parts of a system, IDS is able to detect it and activate countermeasures.

An IDS architecture for sensor networks could take advantage from concepts and techniques of IDS schemes employed in ad hoc networks [29]. However, those IDS techniques cannot be applied directly to sensor networks due to their unique features. Every sensor node cannot have a full-powered IDS agent, because of its high constraints in terms of battery life and processing power. Besides, since the density of sensor networks is usually high, it is also redundant and a waste of resources to force every node to analyze all the packets from its neighborhood. Therefore, the most basic problem that an IDS must face is how to distribute the detection tasks over the nodes.

There are other challenging problems to be solved in the field of IDS over sensor networks as well. An IDS architecture must be simple and highly specialized, able to analyze the specific protocols used over the network and react against specific sensor network threats. The set of rules used by the IDS algorithms for detecting rogue nodes must be easy to parse, their results must consume little memory space, and there must be some policy to manage those results when the memory is full. The alerts generated by the IDS infrastructure should reach the base station as soon as possible, no matter where they were generated. Finally, the IDS agents located inside the network should be able to interchange information in order to achieve a better detection performance.

As a side note, there are partial solutions in the literature that are able to check the integrity of the nodes belonging to the network, such as health monitoring [30], sensor readings analysis [31], and code attestation techniques [32]. These solutions could be integrated into an IDS system for improving its effectiveness.

3.7 Other Issues

A sensor network needs a secure infrastructure to protect itself from external or internal attacks targeting the confidentiality, integrity and authentication properties of its communication channels. However, this is not enough for certain scenarios. There are extra properties that some networks must comply with (e.g., privacy) and there are some applications whose security requirements over a constrained scenario are still unknown (e.g., agents).

Privacy, in certain situations such as a battlefield, is an essential property. There are three types of privacy threats [33]. If an adversary can determine the meaning of a communication exchange because of the existence of a message and the context of the situation, there is a *content privacy threat*. If an adversary is able to deduce the identities of the nodes involved in a communication, there is an *identity privacy threat*. And if the adversary is able to infer the physical location of a communication entity or to approximate the relative distance to that entity, there is a *location privacy threat*.

There are some preliminary studies on originator location privacy and content privacy [33] that explore the privacy of some existing routing protocols. But in general, privacy over sensor networks is an unexplored area of research. It is important to discover and explore the scenarios where a privacy threat exists, and investigate and develop new solutions to solve these problems.

Since the sensor networks are still in their infancy, there are some applications whose security is not yet fully investigated. An example is the area of mobile agents [34], which provide an interesting tool for collaborative processing. However, any adversary could be able to inject a malicious agent inside a node or to modify the results being collected by the agent. Therefore, researchers should investigate how to provide secure code and secure results inside a highly constrained environment.

4 Conclusion

Security in wireless sensor networks is a field of research that is growing rapidly and achieving tangible results applicable to real-life scenarios. Nevertheless, there is still room for more improvements in this area. Fields such as public key cryptography and intrusion detection systems over sensor networks are fairly new. It is necessary to develop secure routing algorithms while complying with essential design properties, such as connectivity, coverage and fault tolerance. Also, secure data aggregation algorithms should be more optimal, and the privacy of the information flow should be taken into account.

Other open areas of research [35] include tolerating the lack of physical security, optimizing the security infrastructures in terms of resources (energy and computation), detecting and reacting over denial of service attacks, and raising the question of the social privacy problems that sensor networks might create. Finally there are some areas, such as the management and protection of mobile nodes and base stations, and the secure administration of multiple base stations with delegation of privileges, that are yet developed.

References

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. *Wireless sensor networks: a survey.* Computer Networks, 38(4), March 2002.
2. Crossbow Technology, Inc. *MICA2 and MICAz, Wireless Measurement Systems.* http://www.xbow.com.
3. IEEE Standard, 802.15.4-2003. *Wireless medium access control and physical layer specifications for low-rate wireless personal area networks.* May 2003, ISBN 0-7381-3677-5.
4. C. Karlof, N. Sastry, D. Wagner. *TinySec: a link layer security architecture for wireless sensor networks.* In Proceedings of 2nd International Conference on Embedded Networked Sensor Systems (SensSys'04), November 2004.
5. N. Sastry, D. Wagner. *Security considerations for IEEE 802.15.4 networks.* In Proceedings of 2004 ACM Workshop on Wireless security (Wise'04), October 2004.
6. N. Gura, A. Patel, A. Wander, H. Eberle, S. C. Shantz. *Comparing elliptic curve cryptography and RSA on 8-bit CPUs.* In Proceedings of 2004 Workshop on Cryptographic Hardware and Embedded Systems (CHES'04), August 2004.
7. D. J. Malan, M. Welsh, M. D. Smith. *A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography.* In Proceedings of 1st IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (Secon'04), October 2004.
8. L. Eschenauer, V. D. Gligor. *A key-management scheme for distributed sensor networks.* In Proceedings of 9th ACM Conference on Computer and Communications Security (CCS'02), November 2002.
9. H. Chan, A. Perrig, D. Song. *Random key predistribution schemes for sensor networks.* In Proceedings of 2003 IEEE Symposium on Security and Privacy (S&P'03), May 2003.
10. W. Du, J. Deng, Y. S. Han, P. K. Varshney. *A pairwise key pre-distribution scheme for wireless sensor networks.* In Proceedings of 10th ACM conference on Computer and communications Security (CCS'03), October 2003.
11. J. Lee, D. R. Stinson. *Deterministic key predistribution schemes for distributed sensor networks.* In Proceedings of 11th Annual Workshop on Selected Areas in Cryptography (SAC'04), August 2004.
12. R. Wei, J. Wu. *Product construction of key distribution schemes for sensor networks.* In Proceedings of 11th Annual Workshop on Selected Areas in Cryptography (SAC'04), August 2004.
13. B. Yener, S. A. Camtepe. *Combinatorial design of key distribution mechanisms for wireless sensor networks.* In Proceedings of 9th European Symposium on Research in Computer Security (ESORICS'04), September 2004.
14. W. Du, J. Deng, Y. S. Han, S. Chen, P. K. Varshney. *A key management scheme for wireless sensor networks using deployment knowledge.* In Proceedings of IEEE INFOCOM'04, March 2004.
15. A. Perrig, R. Szewczyk, V. Wen, D. Cullar, J. D. Tygar. *SPINS: Security protocols for sensor networks.* In Proceedings of 7th International Conference on Mobile Computing and Networking (MOBICOM'01), July 2001.
16. R. Anderson, H. Chan, A. Perrig. *Key infection: smart trust for smart dust.* In Proceedings of 12th IEEE International Conference on Network Protocols (ICNP'04), October 2004.
17. J. Zachari. *A decentralized approach to secure group membership testing in distributed sensor networks.* In Proceedings of 2003 Military Communications Conference (MILCOM 2003), October 2003.

18. Y. W. Law, R. Corin, S. Etalle, P. H. Hartel. *A formally verified decentralized key management architecture for wireless sensor networks*. In Proceedings of 2003 Personal Wireless Communications (PWC'03), IFIP WG 6.8 - Mobile and Wireless Communications. September 2003.
19. J. N. Al-Karaki, A. E. Kamal. *Routing techniques in wireless sensor networks: a survey*. To appear in IEEE Wireless Communications.
20. C. Karlof, D. Wagner. *Secure routing in wireless sensor networks: attacks and countermeasures*. In Proceedings of 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.
21. J. Newsome, E. Shi, D. Song, A Perrig. *The sybil attack in sensor networks: analysis & defenses*. In Proceedings of 3rd IEEE International Workshop on Information Processing in Sensor Networks (IPSN'04), April 2004.
22. R. Di Pietro, L. V. Mancini, Y. W. Law, S. Etalle, P. Havinga. *LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks*. In Proceedings of 32nd International Conference on Parallel Processing Workshops (ICPP'03), October 2003.
23. J. Deng, R. Han, S. Mishra. *A performance evaluation of intrusion-tolerant routing in wireless sensor networks*. In Proceedings of 2nd IEEE International Workshop on Information Processing in Sensor Networks (IPSN'03), April 2003.
24. Q. Fang, J. Gao, L. J. Guibas. *Locating and bypassing routing holes in sensor networks*. In Proceedings of IEEE INFOCOM'04, March 2004.
25. D. Wagner. *Resilient aggregation in sensor networks*. In Proceedings of 2nd ACM workshop on Security of Ad Hoc and Sensor Networks (SANS'04), October 2004.
26. B. Przydatek, D. Song, A. Perrig. *SIA: Secure information aggregation in sensor networks*. In Proceedings of 1st International Conference on Embedded Networked Sensor Systems (SenSys'03), November 2003.
27. W. Du, J. Deng, Y. S. Han, P. K. Varshney. *A witness-based approach for data fusion assurance in wireless sensor networks*. In Proceedings of GLOBECOM'03, December 2003.
28. F. Ye, H. Luo, S. Lu, L. Zhang. *Statistical en-route filtering of injected false data in sensor networks*. In Proceedings of IEEE INFOCOM'04, March 2004.
29. Y. Zhang, W. Lee. *Intrusion detection techniques for mobile wireless networks*. ACM/Kluwer Wireless Networks Journal, 9(5):545-556, September 2003.
30. C. Hsin, M. Liu. *A Distributed monitoring mechanism for wireless sensor networks*. In Proceedings of 2002 ACM Workshop on Wireless Security (WiSe'02), September 2002.
31. S. S. Doumit, D. P. Agrawal. *Self-organized criticaly & stochastic learning based intrusion detection system for wireless sensor networks*. In Proceedings of 2003 Military Communications Conference (MILCOM'03), October 2003.
32. A. Seshandri, A. Perrig, L. Van Doorn, P. Khosla. *SWATT: software-based attestation for embedded devices*. In Proceedings of 2004 IEEE Symposium on Security and Privacy (S&P'04), May 2004.
33. C. Ozturk, Y. Zhang, W. Trappe, M. Ott. *Source-location privacy for networks of energy-constrained sensors*. In Proceedings of 2nd IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems (WSTFEUS'04), May 2004.
34. H. Qi, Y. Xu, X. Wang. *Mobile-agent-based collaborative signal and information processing in sensor networks*. Proceedings of the IEEE, 91(8)1172-1183, August 2003.
35. A. Perrig, J. Stankovic, D. Wagner. *Security in wireless sensor networks*. Communications of the ACM, 47(6)53-57, June 2004.