Exploring Message Authentication in Sensor Networks

Harald Vogt

Department of Computer Science
ETH Zürich
vogt@inf.ethz.ch

Abstract. This paper explores the design space for message authentication in sensor networks. Several types of authentication are put into relation: end-to-end, hop-to-hop, and physical and virtual multipath authentication. While end-to-end authentication provides the highest and most general security level, it may be too costly or impractical to implement. On the other end of the security scale, hop-to-hop authentication can be implemented with little effort but provides security only to a highly restricted attacker. Multipath authentication provides an intermediate security level that may be appropriate for many applications of sensor networks, trading energy for security guarantees. Virtual multipaths offer an improvement, reducing energy demands while retaining crucial security properties of physical multipaths.

1 Introduction

Sensor networks are a novel paradigm for large-scale distributed systems. Individual sensor nodes are resource-restricted, typically battery-powered devices equipped with a radio interface for communication. A typical communication pattern is the aggregation of sensoric data and transmitting results to the edge of the network. Sensor networks are often operated in conjunction with fixed or mobile base stations that collect data, serve as network bridges and provide computational resources.

The potentially unlimited size of a sensor network with thousands of nodes and the need to manage with limited resources and conserve energy as much as possible, on each single node as well as throughout the network, makes secure communication challenging. Various factors are important: Nodes depend on each other for correct operation. Messages have to be transmitted over several hops, since direct communication between arbitrary nodes is impossible due to limited radio range. Nodes have little knowledge of other, distant nodes.

Wireless communication links and multi-hop message transmission are extremely vulnerable to eavesdropping and manipulation. A node that wants to collect sensor data from distant peers must at least be able to check the integrity of the received data. In a strict sense, this is only possible if data is authenticated. This, however, requires that the sender's identity is known and depends on the existence of a common security framework in which the sender and the

receiver are embedded. Such a framework is usually established by an institution that is trusted by both communication endpoints, e.g. a base station (online) or a certification authority (offline).

Many applications for sensor networks need only restricted communication modes, such as between nodes and the base station. In that case, security can be supported using the resources available at the base station. Sensor nodes are required only to have a trust relationship with the base station, which imposes moderate requirements on memory and cpu power of single nodes.

Several questions arise when base stations are assumed. Is there only one base station? Must all traffic be routed through it? Can I add my own base station, using the sensor network as a service? What happens if a base station is compromised? How about combining sensor networks that depend on different base stations? It seems that the dependence on a base station constrains the applicability of a sensor network. Additionally, efficiency can often be increased if communication does not involve a base station. Therefore, we would like to be able to build sensor networks in which node-to-node communication is possible in a secure way.

The purpose of this paper is to assess the options for protecting the integrity of messages in sensor networks without the need to rely on base stations. The goal is not to have a solution that protects against all kinds of attacks, but to achieve a certain level of security at reasonable cost.

One of the distinctive characteristics of sensor networks is the fact that the identity of individual nodes should not be important to the correct operation of the system. First, limited storage capacity makes it impossible for a node to keep specific information on even a moderate (compared to the overall network size) number of other nodes. Second, other attributes such as the geographical position or the quality of sensor measurements are more important to achieving the objective of a sensor network installation than the existence of a single specific node. If one node fails, another nearby node would take over its responsibilities. Thus, the identity of the data collecting node changes, but this fact should be transparent to clients or distant nodes that are interested mainly in data quality.

However, identity is important to be able to verify that a message has been sent by a legitimate entity. A simple trust framework for message transmission is hop-to-hop authentication of data, where there is one key per communication link. Here, communication endpoints have no knowledge about each other, but intermediate nodes are trusted not to manipulate the message. This trust is justified if nodes are correctly implemented and not subject to manipulation. The problem with this approach is the fact that even a small number of compromised nodes can severly affect the security of the network. The situation is similar when a globally shared key is used to authenticate messages. In the case of a globally shared key, all communication is compromised with even a single compromised node. With simple hop-to-hop authentication, a malicious node controls the traffic on all communication paths it is part of. Therefore, such a framework offers protection only against limited, external attacks.

The other extreme is a pairwise end-to-end relationship between all communicating entities. Such relationships are, however, costly to establish and to maintain. As we will discuss in the following section, communication relationships are often ad hoc and short-lived, so the effort of establishing an end-to-end relationship may often not be justified.

An extension to simple hop-to-hop authentication is the use of multiple paths over which messages are transferred. Node-disjoint paths mitigate the impact of small numbers of compromised nodes that try to disrupt communication or manipulate messages. On the other hand, multipath message transmission has severe drawbacks, such as increased energy consumption. An alternative is the variation where a different path is chosen for each transmission, thus increasing the probability that a compromised node is circumvented, and the energy consumption is balanced among nodes.

These approaches are, however, limited by the connectivity of the network, which determines the number of node-disjoint paths between any two nodes. If an attacker chooses the attacked nodes carefully, the effectiveness of an attack can be drastically increased.

To counter the problems of multipath routing, we propose the use of multiple authentication paths over a single communication path [14], thus increasing the reliability of message transmissions, especially the protection of message contents against manipulation. This allows for secure communication between arbitrary nodes in the network with high probability without the requirements imposed by end-to-end techniques.

In Sect. 2, we discuss several communication patterns prevalent in sensor networks and touch upon their security requirements. Sect. 3 describes the security guarantees delivered by different authentication schemes. We argue in favor of virtual multipath authentication in the context of sensor networks. Sect. 4 briefly shows how keys can be established between neighbouring nodes, which is necessary for the proposed approach. The final two sections discuss related work and conclude.

2 Communication Patterns

There are some general communication patterns in sensor networks that are applicable to a wide range of applications. In this section, we argue that it is generally beneficial that sensor nodes exchange data with each other before a base station is involved. Thus arises the need for protection of this communication, which is discussed in the next section.

2.1 Content Based Routing

An important mode of operation in a sensor network is the routing of a message according to its contents, which is often inherently multicast [3, 5], instead of a designated receiver. Entities interested in certain types of events announce

their interest, or events are distributed based on geographical information, for example. The advantage is that event sources don't have to store a mapping from event types to identities of interested entities but need only keep a small amount of routing information, if any.

During such kind of communication, sender and receiver remain unknown to each other. The source does not know in advance, and will never learn, which are the receivers of its messages. This poses several security problems, such as the enforcement of access control policies and message authentication. From the receiver's point of view, it might not be important from which node exactly a message originates. The receiver's interest lies mostly in the integrity of messages. If end-to-end mechanisms are available, identity can be used to check the authenticity of the data, which also ensures integrity. In many cases it may be sufficient that message integrity is preserved with high probability, for example if there are many sources and messages are aggregated before taking crititcal actions.

A client outside of the network perceives the sensor network as a single entity, just like the user of a web service, who does not care about single machines. In contrast to the internet, where resources are plenty and certificates can be used to ensure service integrity, other means must be used for sensor networks. Also, web servers are kept in closed compartments, whereas sensors are deployed in open environments. Factors such as physical appearance are more likely to convince a client of the service quality.

2.2 Aggregation

Aggregation (and correlation) of sensor data is a prerequisite for detecting higher-order events that cannot be reliably inferred from data of single sensor nodes, for example the trajectory of a moving object [12]. A distinction can be made between *local* and *distant* aggregation. Many tasks involve the cooperation of neighbouring nodes, while distant nodes have to be involved for phenomena that affect large areas, such as earthquakes. While it might be possible to collect all data at a base station and perform the aggregation there, it is likely more efficient to aggregate data within the sensor network first.

2.3 Node-to-Node vs. Base-Oriented Communication

It is often assumed that security-relevant communication should involve a base station. This is reasonable, since it is much easier to guarantee end-to-end security properties in conjunction with a well-equipped base station. However, some tasks, such as aggregation, are more efficient when performed to an extent as large as possible within the network. Requiring a base station restricts the applicability of a sensor network. We hope that our examples show that node-to-node communication is a valuable concept for sensor networks. If this type of communication is about to take place in a sensor network, appropriate security mechanisms have to be adopted. In the following, we argue that other means

beside end-to-end mechanisms are feasible and can give appropriate security guarantees.

3 Security Guarantees

What are appropriate security guarantees for a sensor network? In this section, we try to shed some light on the space of possibilities. End-to-end properties are usually considered as the highest level of security achievable, since all potential intermediaries are eliminated (apart from denial of service attacks). But end-to-end properties are nullified if an endpoint is compromised – and in sensor networks, every node is an endpoint. (This is in contrast to a virtual private network, where only a small subset of internet hosts are considered legitimate endpoints.)

Possible failure of nodes should be designed into algorithms for sensor networks as it is highly likely that a certain percentage of them will fail during normal operation. A sensor network should be able to tolerate a certain number of malicious nodes as well. The security of a sensor network is then a function of the ratio of compromised vs. correct nodes, and can be expressed as the probability of being able to compute correct results from sensor data. This security model is supported by other approaches we present in this section, besides end-to-end mechanisms.

3.1 End-to-End

The usual approach for securing communications in a network is to establish an end-to-end trust relationship between the sender and the receiver of a message. An important distinction in this regard is that between *entity authentication* and *message authentication*. In the first case, the mere identity of a communication peer is verified, while in the latter case, the origin of a message and the integrity of its content is assured. We are mainly interested in the latter.

End-to-end mechanisms are based on the existence of a trusted authority. This authority issues credentials and verification tools to all nodes. Credentials are used to assert the authenticity of data packets. Verification can be done either "online" or "offline", online meaning that the trusted authority is active and can be contacted. Thus, it is necessary for each node to establish a trust relationship with the authority server only. This approach is pursued with the μTESLA protocol [9], for example. Offline verification means that each node is self-sufficient and can verify other nodes' credentials on its own. This can be implemented with public key cryptography.

Most practical sensor networks rely on online base stations. These are not necessarily created for security purposes, but are required for other tasks, such as positioning [11] and data aggregation [13]. Since base stations can be equipped with much more resources than sensor nodes, adding security features on top of them is a viable approach.

We see several problems with the end-to-end approach to security, especially in the context of sensor networks:

- **Extensibility.** As the size of a sensor network grows, paths between a base station and individual nodes become longer. This induces a growing delay and increased traffic at more nodes and increased load on the base station.
- **Interoperability.** Sensor networks from different operators cannot be combined easily, since all traffic must be routed through the base stations for authentication.
- **Base station as single point of attack.** An attacker will always try to choose the easiest way attacking a system. If a large part of the traffic is routed through one base station, this base station becomes an attractive target and must be protected appropriately. This might be challenging in certain settings (e.g. when the base station needs to be located within a hostile area), while in others, this might be advantageous (e.g. when the base station is under constant surveillance). Protecting the base station only, however, might result in a false sense of security. If an attack on the base station is virtually impossible, an attacker will concentrate on the sensor nodes themselves, which cannot go without protection (increasing overall cost).
- **Unbalanced energy consumption.** The need to route a large portion of data traffic through a base station implies that sensor nodes near this base station spend their energy faster than nodes that are farther away. Thus, sensors need to be more densely deployed around base stations, or designed asymmetrically. Both solutions increase cost.
- **Computing power requirements.** While symmetric key operations are feasible on small sensor nodes, asymmetric key cryptography, required by offline verification, is not feasible for many types of sensor nodes.

Employing end-to-end security techniques is the most secure mode of operating a sensor network. For a successful attack, an attacker must gain control either over all involved sensor nodes (or a majority thereof), or over the base station. Therefore, both the base station and the sensor nodes have to be protected against manipulation.

3.2 Hop-to-Hop Authentication

If individual sensor nodes are well protected against tampering, it is reasonable to rely on them to reliably and correctly forward messages on behalf of other nodes. Attacks on communication links can be thwarted by link encryption and authentication, or the use of a (regularly updated) globally shared key [1]. Adversaries that are not capable of planting their own nodes within the network or take control of existing nodes, cannot manipulate messages.

But if an adversary manages to compromise even a single legitimate node, the danger arises that all communication within the network becomes subject to eavesdropping and manipulation, for example through a successful sinkhole attack [8]. Thus, the integrity of every single node is important for the security of the overall network. In this sense, every node depends on each other. This

is an extremely strict requirement, which is unlikely to be met in practical deployments. Hop-to-hop authentication is therefore only suitable under a severly restricted adversary model.

3.3 Multiple Path Authentication

Multiple paths mitigate the problem of dependence. Instead of relying on a single node to forward messages correctly, a node cooperates with a number of nodes in its neighbourhood. A message can be sent on alternating paths, or on multiple paths in parallel. Both reduces the impact of isolated failures. Multipath routing has been used mostly for fault tolerance and load balancing, and recently for failure recovery [7] in sensor networks. Disjointness is often not strictly required for such applications.

Multipath routing in conjunction with hop-to-hop authentication results in multipath authentication. A message is sent over multiple, strictly disjoint, paths. If different versions of a message are received, the recipient chooses the majority version. All other paths can be markes as untrustworthy, since they delivered a presumably incorrect message. This is similar to the approach described in [10], where PGP keys are authenticated over multiple disjoint paths (these are not communication paths, but paths in a certification graph).

There are several problems with multipath authentication, when physically disjoint paths are used:

- More nodes need to spend energy on routing.
- Multiple disjoint paths require a minimum degree of connectivity. Some nodes may be only loosely connected to the network and cannot profit from multipath routing.
- It is more demanding to find and maintain sets of disjoint paths between two communication endpoints, compared to a single path. In the worst case, multipath routing boils down to (partial) flooding of the network, for example when a message is to be delivered to several nodes in different parts of the network.

Apart from these problems, multipath authentication reflects an important concept in sensor networks: cooperation of neighbouring nodes. By authenticating messages to each other, they eliminate the impact of maliciously behaving nodes.

3.4 Virtual Multipath Authentication

Instead of transferring multiple physical copies of the same message, we can restrict ourselves to one physical communication path with superimposed (virtual) authentication paths. These are established among nodes on the communication path that share pairwise secret keys. The distribution of these shared keys can be random,or can be based on a regular pattern. Here, we are focusing on a regular distribution.

A regular distribution guarantees that there exists a number of node disjoint authentication paths between any two communicating nodes. The following simple scheme defines such a regular key distribution. It provides two authentication paths per communication path. We call it the *Canvas* scheme [14].

Initially, each node shares a secret key with each of its neighbours. Neighbours include all nodes that are reachable either through a direct communication link, or through at most one intermediate node (which has to be a direct neighbour). Sect. 4 describes how to establish such a key setup. This guarantees that on any communication path between two nodes, there exist two disjoint authentication paths. Note that also direct communication links are authenticated. Fig. 1 shows an example.

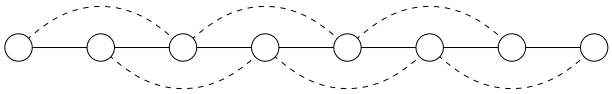

Fig. 1. A *Canvas* communication path

Message forwarding works as follows. A message travelling a path $S_0, S_1, S_2, \ldots, S_n$ is authenticated twice before it is forwarded. S_0 creates MACs intended for nodes S_1 and S_2. S_0 can only reach S_1 directly and relies on S_1 to transmit the MAC intended for S_2. Before S_1 forwards the message, it creates two new authentication codes itself for S_2 and S_3. This is continued until the message reaches its final destination.

Before a node forwards a message, it checks the authentication codes from the two preceding nodes. If both codes indicate that the message has not been manipulated, the node forwards the message. An exception arises when a message is created, where only one MAC needs to be checked by the immediate neighbour of the source node.

It is obvious that two adjacent nodes can cooperatively compromise the communication path. They are able to manipulate and inject arbitrary messages that are routed through them. This seems to be only a slight improvement over simple hop-to-hop authentication at first. Instead of compromising one node, an attacker now has to gain control over two of them. And since they are co-located, an attack should be easy. Thus it seems nothing much is gained.

In order to show that the Canvas scheme provides a significant improvement, we first have to make clear what types of attacks we can expect to counter with the security schemes proposed in this paper, and which we cannot.

If there is an attack possible that exploits a fault present in all sensor nodes, and the attack can be automated (like a typical attack on hosts in the internet), the effort to compromise only one node is essentially as high as to compromise a large number of nodes or even all of them. Such attacks cannot be countered by any of the security schemes described in this paper. They must instead be be

tackled by careful system design, intrusion detection techniques, quick response etc.

We propose a metric, called "live paths", to assess the security of a sensor network. A path is called *live* if and only if its both endpoints are not compromised. The rationale is that if an endpoint is compromised, it does not contribute meaningfully to the overall result of a computation. This is true even if end-to-end security measures are avaialable. The set of of live paths is thus an indicator of the quality of the network.

Additionally, we call a path "functional" if it is both live and the endpoints can communicate securely. With simple hop-to-hop authentication, a path becomes non-functional if at least one node on the path is compromised. With the Canvas scheme, a path remains functional unless two adjacent nodes are compromised. Note that under end-to-end security, a live path is always functional.

A simulation on a sensor network with 280 randomly placed nodes on a plane of 500 on 500 square meters and a communication range of 50 meters shows the impact of an attack under the different security schemes (Fig. 2). The simulated attacker acts "smart" with regard to the Canvas scheme. Instead of attacking isolated nodes, pairs of nodes are being attacked. A path is always a shortest path between a pair of nodes.

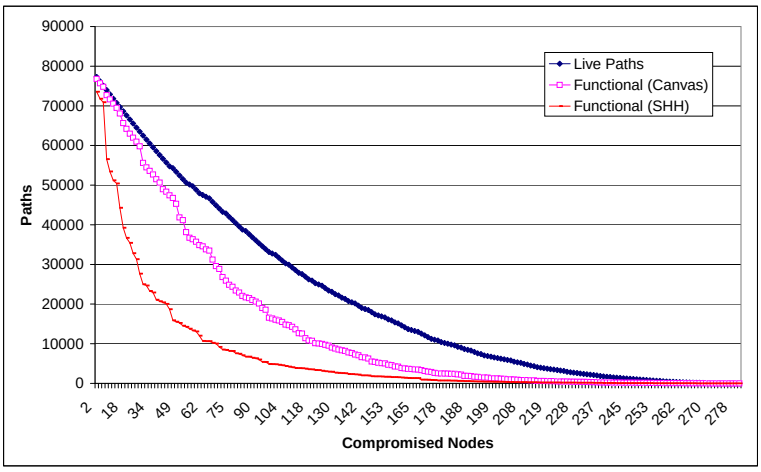

Fig. 2. Degradation of functional paths in a network under attack with regard to different security schemes

Obviously, the quality of the network degrades with the number of nodes being compromised, meaning that secure communication becomes less likely. The number of functional paths drops sharply when the simple hop-to-hop scheme (SHH) is employed. The Canvas scheme is more resilient and guarantees secure communication for a significantly larger fraction of the nodes. The optimum

achievable – through end-to-end techniques – is represented by the curve denoting the live paths.

It may be subject to debate to what degree live and functional paths are a meaningful metric for the security of a sensor network. On an abstract level, it seems to be sensible. Consider for example a user who wishes to query the sensor network and connects to an arbitrary (non-compromised) node. The more functional paths there are to other nodes, the higher the probability will be that the resulting data has a certain quality.

To summarize, we bring forward two arguments that show that the Canvas scheme can be a significant improvemet.

1. The effort that must be invested for an attacker to compromise a communication path is doubled. This can be enough to detain a potential attacker, if individual nodes are sufficiently protected. Similarly, we can say that if the probability for a successful attack on a single node is small enough, it is highly unlikely that an attacker succeeds in compromising two adjacent nodes.
2. Even if the attacker manages to compromise a certain number of nodes, the impact is rather small at first. With a growing number of compromised nodes, the Canvas scheme performs significantly better than hop-to-hop authentication.

The Canvas scheme makes it necessary that with each message, three MACs are transmitted. It is therefore affordable only for messages of a certain size. Also, several symmetric key operations (verification and MAC creation) are necessary at each hop. This could be a several drawback if such computations are energy intensive or slow on a certain node type. However, there is room for improvement, for example by using specialized, more efficient cryptographic hardware support.

Finally, we would like to point out that the Canvas scheme can be generalized such that more than two authentication paths are available per communication path. This is achieved by increasing the "reach" of a node to its k-hop neighbours. The distance between a pair of nodes sharing a key would increase. In the extreme case, we would arrive at the end-to-end situation, where each node shares a key with each other (if k equals the diameter of the network).

4 Key Setup

Several proposals have been made for setting up keys in sensor networks. One of the most intriguing has been made by Eschenauer and Gligor [6]. Each node is assigned an identity that uniquely determines a limited set of key values being drawn from a common set. The identity can be made public without helping a potential attacker. Based on their identities, two nodes can determine their common subset of key values. This subset is unique to this pair of nodes with high probability and can be used to exchange a secret key without the use of computationally intensive public key cryptography.

The key setup for the Canvas scheme is straightforward. A node establishes a unique secret key with each of its neighbours, including the ones that are not directly reachable, based on their identities. A man-in-the-middle attack is impossible since identities are unique. A node imitating several identities would have to produce key values he does not know.

Note that with such an identity scheme, also end-to-end security properties can be established, if each endpoint knows the identity of the other one. However, as we have shown above, a distinctive end-to-end relationship is rather the exception. Also, after the initial phase, the memory storing the key values could be reused for applications. Then, no more keys can be negotiated.

5 Related Work

Virtual authentication paths have been studied by Beimel and Franklin [2], who differentiate between the communication graph of a network, and the authentication graph defined by the keys shared among nodes. They give a characterization of reliable message transmission, which depends on the connectivity of the communication graph and the union of both graphs.

Multipath routing for sensor networks is examined in [7] with a focus on failure recovery and minimization of energy consumption. Strictly disjoint paths are not required, but it is desirable to have backup paths in case of failure.

Zhu et al. [16] discuss several important issues in sensor network security. It is assumed, for example, that sensor nodes can withstand a physical attack at least for a small amount of time, which gives the sensors time for neighbour detection and key establishment. In this work, protocols are given for establishing keys on several levels, including group, cluster and pairwise keys, which are based on the identity of nodes.

The idea of establishing pairwise keys based on pre-distributed random values is explored in several papers [4, 6, 15]. Chan et al. [4] uses multiple paths for key reinforcement, which further helps increase the resilience against link key compromise.

In a paper by Zhu et al. [17], interleaved message authentication, similar to our *Canvas* approach, is used for filtering false messages on their way from a sensor node to the base station. This principle is applied in addition to strong source authentication using a key that is shared between the base station and the sensor node.

6 Conclusion

Sensor networks constituted from a huge number of small, resource-restricted devices, need an understanding of security that takes their applications, their architectures and the capabilities of single nodes into consideration. Sensor networks operate under much tighter constraints than networks of personal devices (where humans are present most of the time) or conventional distributed systems like

local area networks. In this paper, we have presented part of the design space for communication security in sensor networks, focusing on message integrity. The approach of virtual multipath authentication prefers localized communication over long-distance protocols and is thus scalable to very large network sizes.

References

1. Stefano Basagni, Kris Herrin, Danilo Bruschi, and Emilia Rosti. Secure Pebblenets. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, pages 156–163. ACM Press, 2001.
2. A. Beimel and M. Franklin. Reliable Communication over Partially Authenticated Networks. *Theoretical Computer Science*, 220(1):185–210, 1999.
3. David Braginsky and Deborah Estrin. Rumor Routing Algorthim for Sensor Networks. In *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications*, pages 22–31. ACM Press, 2002.
4. Haowen Chan, Adrian Perrig, and Dawn Song. Random Key Predistribution Schemes for Sensor Networks. In *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pages 197–213. IEEE, May 2003.
5. Frank Dürr and Kurt Rothermel. On a Location Model for Fine-Grained Geocast. In *Ubicomp 2003: Ubiquitous Computing*, volume 2864 of *LNCS*, pages 18–35. Springer-Verlag, 2003.
6. L. Eschenauer and V. D. Gligor. A Key-Management Scheme for Distributed Sensor Networks. In *CCS'02*. ACM, 2002.
7. D. Ganesan, R. Govindan, S. Shenker, and D. Estrin. Highly-Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks. *Mobile Computing and Communications Review*, 1(2), 1997.
8. Chris Karlof and David Wagner. Secure Routing in Wireless Sensor Networks. *Elsevier Ad Hoc Networks*, 1(2-3):295–315, September 2003.
9. Adrian Perrig, Rober Szewczyk, J. D. Tygar, Victor Wen, and David E. Culler. SPINS: Security Protocols for Sensor Networks. *Wireless Networks*, 8(8):521–534, 2002.
10. Michael K. Reiter and Stuart G. Stubblebine. Resilient Authentication Using Path Independence. *IEEE Transactions on Computers*, 47(12):1351–1362, 1998.
11. Kay Römer. The Lighthouse Location System for Smart Dust. In *Proceedings of MobiSys 2003 (ACM/USENIX Conference on Mobile Systems, Applications, and Services)*, pages 15–30, San Francisco, CA, USA, May 2003.
12. Kay Römer. Tracking Real-World Phenomena with Smart Dust. In *1st European Workshop on Wireless Sensor Networks (EWSN)*, volume 2920 of *LNCS*, pages 28–43. Springer-Verlag, 2004.
13. Robert Szewczyk, Joseph Polastre, Alan Mainwaring, and David Culler. Lessons from a Sensor Network Expedition. In *1st European Workshop on Wireless Sensor Networks (EWSN)*, volume 2920 of *LNCS*, pages 307–322. Springer-Verlag, 2004.
14. Harald Vogt. Integrity Preservation for Communication in Sensor Networks. Technical Report 434, ETH Zürich, Institute for Pervasive Computing, February 2004.
15. S. Zhu, S. Xu, S. Setia, and S. Jajodia. Establishing Pair-wise Keys for Secure Communication in Ad Hoc Networks: A Probabilistic Approach. Technical Report ISE-TR-03-01, George Mason University, March 2003.

16. Sencun Zhu, Sanjeev Setia, and Sushil Jajodia. LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. In *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS)*, pages 62–72. ACM Press, 2003.
17. Sencun Zhu, Sanjeev Setia, Sushil Jajodia, and Peng Ning. An Interleaved Hop-by-Hop Authentication Scheme for Filtering False Data Injection in Sensor Networks. In *IEEE Symposium on Security and Privacy*. IEEE, 2004.