Autonomic Communication Security in Sensor Networks

Tassos Dimitriou and Ioannis Krontiris

Athens Information Technology
{tdim, ikro}@ait.edu.gr

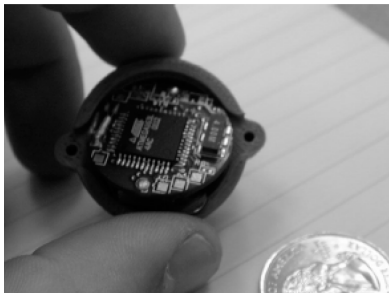
Abstract. The fact that sensor networks are deployed in wide dynamically changing environment and usually left unattended, calls for nomadic, diverse and autonomic behavior. The nature of security threats in such networks as well as the nature of the network itself raise additional security challenges, so new mechanisms and architectures must be designed to protect them. In an autonomic communication context these mechanisms must be based on self-healing, self-configuration and self-optimization in order to enforce high-level security policies. In this work we discuss the research challenges posed by sensor network security as they apply to the autonomic communication setting.

1 Introduction

During the past few years there has been an explosive growth in the research devoted to the field of sensor networks, covering a broad range of areas, from understanding theoretical issues to technological advances that made the realization of such networks possible. These networks use hundreds to thousands of inexpensive wireless sensor nodes over an area for the purpose of monitoring certain phenomena and capture geographically distinct measurements over a long period of time. Nodes employed in sensor networks are characterized by limited resources such as storage, computational and communication capabilities. As an example, Figure 1 shows a sensor node designed at UC Berkeley, along with its processor and radio characteristics. The power of sensor networks, however, lies exactly in the fact that their nodes are so small and cheap to build that a large number of them can be used to cover an extended geographical area.

Even though originally research on sensor networks was motivated my military applications, the availability of low cost sensors and the advances in communication networks have resulted in exciting applications [1, 2, 3] in a wide range of fields such as counterterrorism applications, environmental and habitat monitoring, disaster management and traffic control. One reason that make such networks attractive is the fact that they can be deployed rapidly and start operating without the need of any previous infrastructure or human intervention. For instance, sensor networks could be deployed directly in the region of interest to help rescuing efforts at disaster sites, or they could monitor conditions at a highly toxic environment, along an earthquake fault, or around a critical water reservoir.

I. Stavrakakis and M. Smirnov (Eds.): WAC 2005, LNCS 3854, pp. 141–152, 2006.



Processor	
CPU Clock	4 MHz
Program Memory	128K bytes
Serial Flash	512K bytes
EEPROM	4 K bytes
Current Draw	8 mA
Radio	
Center Frequency	433 MHz
Data Rate	38.4 Kbaud
Outdoor Range	1000 ft
Current Draw	25 mA (transmit)
	8 mA (receive)

Fig. 1. UC Berkeley's Mica mote and specifications

As most of the applications require the unattended operation of a large number of sensor nodes, this raises immediate problems for administration and utilization. Even worse, some times it is not possible to approach the deployment area at all, like for example in hostile environments of military applications. So, sensor networks need to become *autonomous* and exhibit responsiveness and adaptability to evolution changes in real time, without explicit user or administrator action.

Autonomic responses of sensor networks are especially important to counter security threats. Most sensor networks actively monitor their surroundings, and it is often easy to deduce information other than the data monitored. Such information leakage often results in loss of privacy for the people in the environment. Moreover, the wireless communication employed by sensor networks facilitates eavesdropping and packet injection by an adversary. The combination of these factors demands security for sensor networks [4, 5] to ensure operation safety, secrecy of sensitive data and privacy for people in sensor environments.

Nevertheless, sensor networks cannot rely on human intervention to face an adversary's attempt to compromise the network or hinder its proper operation. Neither can they employ existing security mechanisms such as public key infrastructures that are computationally expensive. Instead, an autonomic response of the network that relies on the embedded pre-programmed policies and a coordinated, cooperative behavior is the most effective way to gain maximum advantage against adversaries.

2 Limitations and Potential Attacks

Although wireless sensor networks have an ad-hoc nature, there are several limitations that make security mechanisms proposed for ad-hoc networks not applicable in this setting. In particular, security in sensor networks is complicated by more constrained resources and the need for large-scale deployments. A summary of these limitations follows below:

- *Constrained hardware*: Establishing secure communication between sensor nodes becomes a challenging task, given the limited processing power, storage, bandwidth and energy resources, as well as the lack of control of the wireless communication medium. Public-key algorithms, such as RSA [6] or Diffie-Hellman key agreement [7] are undesirable, as they are computationally expensive. Instead, symmetric encryption/decryption algorithms and hash functions are between two to four orders of magnitude faster [8], and constitute the basic tools for securing sensor network communications. However, symmetric key cryptography is not as versatile as public key cryptography, which complicates the design of secure applications.
- *Wireless communications*: Sensor networks use wireless communication which is particularly expensive from an energy point of view (one bit transmitted is equivalent to about a thousand CPU operations [9]). Hence one cannot use complicated protocols that involve the exchange of a large number of messages. Additionally, the nature of communication makes it particularly easy to eavesdrop, inject malicious messages into the wireless network or even hinder communications entirely using radio jamming.
- *Exposure to physical attacks*: Unlike traditional networks, sensor nodes are often deployed in areas accessible by an attacker, presenting the added risk of physical attacks that can expose their cryptographic material or modify their underlying code. This problem is magnified further by the fact that sensor nodes cannot be made tamper-resistant due to increases in hardware cost.
- *Large scale deployment*: Future sensor networks will have hundreds to thousands of nodes so it is clear that scalability is a prerequisite for any attempt in securing sensor networks. Security algorithms or protocols that have not designed with scalability into mind offer little or no practical value to sensor network security.
- *Aggregation processing*: An effective technique to extend sensor network lifetime is to limit the amount of data sent back to reporting nodes since this reduces communication overhead [10]. However, this cannot be done unless intermediate sensor nodes have access to the exchanged data to perform data fusion processing. End-to-end confidentiality should therefore be avoided as it hinders aggregation by intermediate nodes and complicates the design of energy-aware protocols.

All these limitations make sensor networks more vulnerable to attacks, ranging from passive eavesdropping to active interference. In particular, we distinguish attacks as outsider and insider attacks. In *outsider* attacks, the attacker may inject useless packets in the network in order to exhaust the energy levels of the nodes, or passively eavesdrop on the network's traffic and retrieve secret information. An *insider* attacker however, has compromised a legitimate sensor node and uses the stolen key material, code and data in order to communicate with the rest of the nodes, as if it was an authorized node. With this kind of intrusion, an attacker can launch more powerful and hard to detect attacks that can disrupt or paralyze the network.

3 Typical Security Requirements

Usually in sensor networks there exists one or more base stations operating as data sinks and often as gateways to other networks. In general a base station is considered trustworthy, ether because it is physically protected or because it has a tamper-resistant hardware. Concerning the rest of the network, we now discuss the standard security requirements (and eventually behavior) we would like to achieve by making the network secure.

- *Confidentiality*: In order to protect sensed data and communication exchanges between sensors nodes it is important to guarantee the secrecy of messages. In the sensor network case this is usually achieved by the use of *symmetric* cryptography as asymmetric or public key cryptography in general is considered too expensive. However, while encryption protects against outside attacks, it does not protect against inside attacks/node compromises, as an attacker can use recovered cryptographic key material [11] to successfully eavesdrop, impersonate or participate in the secret communications of the network. Furthermore, while confidentiality, when applied properly, guarantees the security of communications inside the network it does not prevent the misuse of information reaching the base station. Hence, confidentiality must also be coupled with the right control policies so that only authorized users can have access to confidential information.
- *Integrity and Authentication*: Integrity and authentication is necessary to enable sensor nodes to detect modified, injected, or replayed packets. While it is clear that safety-critical applications require authentication, it is still wise to use it even for the rest of applications since otherwise the owner of the sensor network may get the wrong picture of the sensed world thus making inappropriate decisions. However, authentication alone does not solve the problem of node takeovers as compromised nodes can still authenticate themselves to the network. Hence authentication mechanisms should be "collective" and aim at securing the entire network. Using intrusion detection techniques we may be able to locate the compromised nodes and start appropriate revoking procedures.
- *Availability*: In many sensor network deployments (monitoring fires, quality of water in reservoirs, protection against floods, battlefield surveillance, etc.), keeping the network available for its intended use is essential. Thus, attacks like denial-of-service (DoS) that aim at bringing down the network itself may have serious consequences to the health and well being of people. However, the limited ability of individual sensor nodes to detect between threats and benign failures makes ensuring network availability extremely difficult. Additionally, it is important that the network still operates under such scenarios and that its operation degrades in a predictable and stable way despite the presence of node compromises or failures.

All this discussion suggests that it is necessary to develop networks that exhibit autonomic security capabilities, i.e. be resilient to attacks and have the ability to contain damage after an intrusion.

4 Issues in Sensor Network Security Research

A security architecture for sensor networks must integrate a number of security measures and techniques in order to protect the network and satisfy the desirable requirements we have outlined. In what follows we describe some of these components (and the techniques involved) that are currently under research in sensor networks and we discuss some open challenges with respect to autonomic communication behavior.

4.1 Key Establishment and Initial Trust Setup

One important component of autonomic communication is programmable and controlled group communication. Members leave and join the group according to some membership rules and follow the same behavior pattern within the group. When setting up a secure sensor network, one must be able to embed trust rules that govern the security level of group communications as well as the self-configuration nature of the network. This includes discovering new nodes and adding them in the group as well as identifying and isolating malicious ones. Eventually this translates in establishing cryptographic keys between the members of the group.

Key establishment protocols used in traditional networks are well studied but cannot be applied here due to the inherent limited capabilities (CPU power, memory, etc.) of sensor nodes. Moreover, key-establishment techniques need to scale to networks with tens of thousands of nodes. Simple solutions such as network-wide keys [12] are not acceptable from a security point of view since compromising a single node leads to compromise of the entire network, leaving no margins for self-healing. On the other hand, having each node sharing a separate key with every other node in the network is not possible due to memory constraints (each node usually has a few KBs of memory).

Typically, the problem of initial trust setup can be solved by allocating to each sensor node a randomly selected subset from a pre-established set of keys [13, 14, 15]. Then sensors can communicate securely if they have one or more keys in common. However, these techniques offer only "probabilistic" security as compromising a node may lead to security breaches in other parts of the network. Some other techniques exist [16, 17] that are designed to restrict an adversary that compromised a node to a small portion of the network supporting in-network processing at the same time, but more research is needed in this area.

In order for sensor nodes to be able to communicate safely using established cryptographic keys, a key refresh mechanism is also needed. In an autonomic scenario, re-keying is equivalent with self-revocation of a key when the network detects an intrusion or the lifetime of the key has expired. In order to keep the desirable security level intact the network itself has to determine that rekeying is needed and initiate the appropriate mechanisms. Re-keying is thus a challenging issue, since new keys must be generated in a collaborative and energy-efficient manner, so not all security architectures can support them.

4.2 Resilience to Denial of Service Attacks

Adversaries can limit the value of a wireless sensor network through DoS attacks making it imperative to defend against them. DoS attacks can occur at multiple protocol layers [18], from radio jamming in physical layer to flooding in transport layer, all with the same goal: to prevent the network from performing its expected function. Adversaries can involve malicious transmissions into the network to interfere with sensor network protocols and induce battery exhaustion or physically destroy central network nodes. More disastrous attacks can occur from inside the sensor network if attackers compromise some of the sensors themselves. For example, they could create routing loops that will eventually exhaust all nodes in the loop.

Determining that the network is subject to a DoS attack is a very challenging problem. Especially in large-scale deployments, it is hard to differentiate between failures caused by intentional DoS attacks and nominal node failures. An autonomic sensor network must be able to *monitor* the network traffic and look for suspicious patterns that match some possibly learned rules about what is normal or abnormal behavior [19]. Then it can respond according to the type of the attack.

Potential defenses include techniques such frequency hopping, spread spectrum communication [20] and proper authentication. What is needed, however, is an autonomic coordinated response to defend against DoS attacks with a minimum latency between the detection and a coordinated response. One example could be the use of unaffected nodes to map the affected region and then route around the jammed portion of the network [21]. Further progress in this area is needed to allow for greater security against DoS attacks.

4.3 Resilience to Node Compromises

Due to the nature of their deployment, sensor nodes are exposed to physical attacks in which an attacker can extract cryptographic secrets or modify their code. In [11], the authors demonstrate how to extract cryptographic keys from a sensor node using a JTAG programmer interface in a matter of seconds. One solution to this problem would be the use of more expensive tamper resistance hardware; however, this solution would increase the cost per sensor considerably, thus ruling out deployment of sensor networks with thousands of nodes. Moreover, trusting tamper resistant devices can be problematic [22].

So, the challenge here is to build networks that operate correctly even when several nodes have been compromised and behave in an arbitrarily malicious way. One approach would be the design of proactive networks of sensors in which the sensors at regular time intervals run a protocol to update their cryptographic key material. Combined with the fact that an adversary would have to capture a large percentage of the sensors in the same time interval, security of the network would be enforced. In general, it is very difficult for an adversary to obtain global information about the entire network. Instead, an attacker only has limited information connected with the nodes she compromises. This can be turned into

a defensive mechanism for the sensor network, if the compromised region can be located [23] successfully.

As a result, it would be vital to sensor network security if there was a mechanism that could effectively detect malicious code in sensor nodes and give an assurance that they are running the correct code. Lately *software-based code attestation* has been proposed as a mechanism like this. For example, SWATT [24] enables an external verifier to verify the code of a running system to detect maliciously inserted or altered code, without the use of any special hardware. This enables new intrusion-detection architectures, where other sensor nodes can play the role of the verifier and alert the rest of the network in case a compromised node is detected. We believe that this direction could offer a serious defence mechanism for sensor networks and propose it as a future research.

4.4 Routing Security

Routing and data forwarding is an essential service for enabling communication in sensor networks. Unfortunately, currently proposed routing protocols suffer from many security vulnerabilities [25] (selective forwarding, replayed messages, sinkhole and Sybil attacks, etc.), especially due to node compromises in which a single compromised node suffices to take over the entire network. Cryptographic primitives, such as encryption and authentication, are not enough to secure routing protocols; carefully re-designing these protocols with security as a goal is needed as well.

For example, multipath routing [26, 27] has been proposed as a solution. Redundant disjoint paths are used, so even if an intruder compromises a node, information can be routed by alternative paths. This strategy however provides *intrusion-tolerant* security. An autonomous communication paradigm should provide *intrusion-detection* capabilities, in order to enable self-healing processes and enable routing and other network functions to be adapted accordingly.

A closely related problem is that of secure location determination (discussed in the next subsection), which is a prerequisite for secure geographic routing. This is so because in an adversarial environment a malicious node can claim a false position to the infrastructure in order to create routing loops, or have all traffic routed through it. Nevertheless, in autonomic sensor networks, routing strategies may change in order to *adapt* to network changes [28, 29, 30]. So, for example, if location service for geographic routing becomes unavailable then a different routing strategy must be employed.

In conclusion, securing routing means providing an adaptive mechanism that secures packet flow in the network under various threats. As autonomic routing in sensor networks becomes an attractive challenge, providing security requires new design goals, like adaptability, and extensibility.

4.5 Location Aware Security

Many applications of sensor networks require location information, not only for routing purposes, but also for determining the origin of the sensed information or preventing threats against services [31, 32]. Many localization techniques have

been proposed, but little research has been done in securing the localization scheme [33, 34, 35, 36]. Security in this case is twofold: Each node must determine its own location in a secure way (secure localization) and each node must verify the location claim of another node (location verification).

Since providing each node with a GPS receiver increases its cost, many localization services assume the presence of a few such nodes (usually more powerful also), which communicate their coordinates in the network and allow the rest of the nodes to estimate their position. This communication provides malicious attackers with the chance to modify measured distances and make nodes believe that they are at a position which is different from their real one. Furthermore, without location verification mechanisms, a dishonest node can cheat about its own position in order to gain unauthorized access to some services, or avoid being penalized. As more and more protocols and services are based upon location awareness, enabling sensors to determine their location in an un-trusted environment becomes essential.

4.6 Data Fusion Security

The paradigm of autonomic communication includes the *filtering* of large data feeds in order to retrieve useful information [37]. In sensor networks, thousands of sensor nodes that monitor an area generate a substantial amount of data which may be unnecessary and inefficient to be returned at the base station. Instead, certain intermediate nodes collect this data, autonomously evaluate it and reply to the aggregate queries of a remote user (Figure 2). So, data aggregation shifts the focus from address-centric approaches to a more *context* aware approach that enables sensor networks to maintain a logical view of the data.

The resource constraints and security issues make designing mechanisms for information aggregation in large sensor networks particularly challenging since aggregation nodes constitute single points of failure. An attacker upon compromising such a node may have access to valuable information and most importantly by changing the value of this information may present a wrong picture

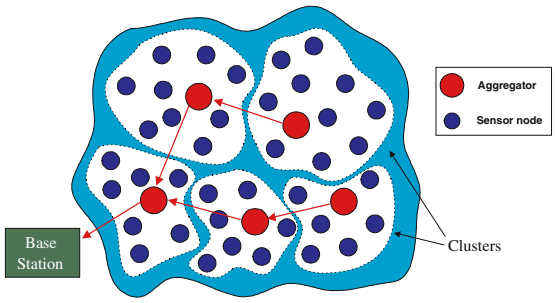


Fig. 2. An aggregation hierarchy in a sensor network. Aggregators collect information coming from the same cluster, process it and forward suitable summaries towards the base station, thus saving valuable energy resources. Although aggregators are shown bigger than simple sensor nodes, it should not be inferred that they are more powerful.

about the sensed world, thus leading to bad decisions. Several proposals for secure aggregations exist [38, 39, 40], but some open issues remain, like reorganizing the security infrastructure in case of energy depletion of an aggregation node.

4.7 Efficient Cryptographic Primitives

Because sensor nodes have limited computational and storage capabilities, traditional security solutions are often too expensive for sensor networks. More research in this domain is necessary, especially in exploring the use of efficient asymmetric cryptographic mechanisms for key establishment and digital signatures as a means for leveraging trust in sensor networks and solving some of the problems mentioned above.

Recently, elliptic curve cryptography (ECC) has emerged as a suitable public key alternative for sensor networks [41, 42], providing high security for relatively small key sizes. Since many traditional public key protocols can be turned to their EC equivalents, public-key infrastructure based on elliptic curves appears to be an attractive choice for sensor networks.

5 Autonomic Communication Challenges in Securing Sensor Networks

From the discussion in the previous sections, we see how autonomic communication behavior offers opportunities to increase security in sensor networks. We now summarize these autonomic characteristics and discuss what is needed in order to provide an integrated and complete solution for sensor networks security.

- *Self-configuration:* As the energy of sensor nodes is reduced by computation and communication, some nodes are expected to be disabled during the lifetime of the network and new ones must be deployed. Autonomic communication architectures must allow for sensor nodes to leave and join the network on-the-fly, without compromising the security level. Network configuration may also change in mobile sensor networks, resulting in new formation of groups. In all cases, the network must be able to automatically reconfigure its state, keeping the security level consistent.
- *Self-awareness:* Before a sensor network is able to respond to a security threat, it must be able to recognize it. This requires knowledge about the network's state (or more realistically, the state of neighboring nodes) and network monitoring for abnormal behaviors of sensor nodes or data traffic. To characterize normal and malicious behavior, appropriate rules must be generated, based on statistics, induction and deduction.
- *Self-healing:* Once the network is aware that an intrusion has taken place and have detected the compromised area, appropriate actions must be taken. The first one is to cut off the intruder as much as possible and isolate the compromised nodes. After that, proper operation of the network must be restored. This may include changes in the routing paths, updates of the cryptographic material (keys, etc.) or restoring part of the system using

redundant information distributed in other parts of the network. Autonomic behavior of sensor networks means that these functions must be performed without human intervention.

- *Self-organization:* Self-organization of thousands of nodes allow a sensor network to perform complex operations in a dynamic communication environment. Emphasis must be given on distributed services that allow secure location awareness, secure data fusion and implementation of complex cryptographic operations, such as access control, authentication, etc. In order to provide the needed functionality, self-organization mechanisms need to be highly scalable and adaptable.
- *Self-optimization:* Since sensor networks can be subject to unpredictable security attacks, they must be able to update their configuration on-the-fly to enable optimal behaviors in response to these changes. For example, sensor nodes should be able to function under the sudden communication load often caused by widespread security incidents, like a DoS attack, by triggering the appropriate measures.

6 Conclusion

In this paper we have presented an overview of current research challenges on sensor networks security, highlighting their autonomic communication aspects. A progress has been made in providing specialized security mechanisms, like key establishment, secure localization, secure aggregation or secure routing. While these mechanisms may protect sensor networks from specific threats, what has been lacking is a *holistic* approach that encompasses autonomic responses over a broad range of attacks. A research challenge therefore, would be the design of an adaptive security architecture that can monitor the sensor network, recognize a security threat and respond by a coordinated self-healing mechanism. In this sense, autonomic communication techniques offer opportunities for increasing sensor networks security and guaranteeing a robust and survivable solution.

References

1. Chong, C.-Y., Kumar, S.P.: Sensor Networks: Evolution, Opportunities, and Challenges. In: Proc. of the IEEE (8)**91** (2003) 1247–1256
2. Tubaishat, M., Madria, S.: Sensor networks: an overview. IEEE Potentials (2)**22** (2003) 20–23
3. Rajaravivarma, V., Yang, Y., Yang, T.: An overview of Wireless Sensor Network and applications. In: Proc. of the 35th IEEE Southeastern Symposium on System Theory (2003) 432–436
4. Hu, F., Sharma, N.K.: Secure Wireless Sensor Networks: Problems and Solutions. In: Proc. of International Conference on Computer, Communication and Control Technologies (CCCT 2003)
5. Shi, A., Perrig, A.: Designing Secure Sensor Networks. IEEE Wireless Communications (6)**11** (2004) 38–43

6. Rivest, R., Shamir, A., and Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM (2) **21** (1978) 120–126
7. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions on Information Theory **22** (1976) 644–654
8. Carman, D., Kruus, P., Matt, B.: Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs (2000)
9. Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., Pister, K.: System architecture directions for networked sensors. In: Proc. of the 9th International Conference ASPLOS-IX (2000) 93–104
10. Intanagonwiwat, C., Govindan, R., Estrin, D.: Directed diffusion: A scalable and robust communication paradigm for sensor networks. In: Proc. of the 6th Annual Inter. Conference on Mobile Computing and Networking (MobiCOM '00), 2000
11. Hartung, C., Balasalle, J., Han, R.: Node Compromise in Sensor Networks: The Need for Secure Systems. Tech. Report CU-CS-990-05, Univ. of Colorado (2005)
12. Basagni, S., Herrin, K., Bruschi, D, Rosti, E.: Secure pebblenets. In: Proc. of the ACM Inter. Symposium on Mobile Ad Hoc Networking and Computing, 2001
13. Eschenauer, L., Gligor, V. D.: A key-management scheme for distributed sensor networks. In: Proc. of the 9th ACM Conference on Computer and Communications Security, Washington D.C., USA (2002) 41–47
14. Chan, H., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks. In: Proc. of the IEEE Symp. Security Privacy, Berkeley, CA (2003)
15. Du, W. , Deng, J. , Han, Y.S., Varshney, P.K.: A pairwise key pre-distribution scheme for wireless sensor networks. In: Proc. of the 10th ACM Conference on Computer and Communications Security, Washington D.C., USA (2003) 42–51
16. Dimitriou, T., Krontiris, I.: A Localized, Distributed Protocol for Secure Information Exchange in Sensor Networks. In: Proc. of the 5th IEEE Intern. Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks (WMAN), 2005
17. Zhu, S., Setia, S., Jajodia, S.: LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. In: Proc. of the 10th ACM Conference on Computer and Communications Security (CCS03), Washington D.C. (2003) 62–72
18. Wood, A. D., Stankovic, J. A.: Denial of Service in Sensor Networks. IEEE Computer **35**(10) (2002) 54–62
19. Jones, A.K., Sielken, R.S.: Computer system intrusion detection: a survey. Technical Report, Computer Science Department, University of Virginia (2000)
20. Pickholtz, R.L., Schilling, D.L., Milstein, L.B.: Theory of spread-spectrum communications - A tutorial. IEEE Transactions on Communications **30** (1982) 855–884
21. Krontiris, I., Dimitriou, T.: GRAViTy, Geographic Routing Around Voids. In preparation.
22. Anderson, R., Kuhn, M.: Low cost attacks on tamper resistant devices. In: IWSP: 5th International Workshop of Security Protocols, Lecture Notes in Computer Science **1361** Springer-Verlag (1997) 125–136
23. Deng, J., Han, R., Mishra, S.: Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks. In: Proc. of the IEEE International Conference on Dependable Systems and Networks (DSN) (2004) 594–603
24. Seshadri, A., Perrig, A., Doorn, L., Khosla, P.: SWATT: SoftWare-based ATTestation for Embedded Devices. In: Proc. of the IEEE Symposium on Security and Privacy (2004) 272–282
25. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: Attacks and countermeasures. In: Proc. of the 1st IEEE International Workshop on Sensor Network Protocols and Applications (2003)

26. Ganesan, D., Govindan, R., Shenker, S., Estrin, D.: Highly-resilient, energy-efficient multipath routing in wireless sensor networks. ACM SIGMOBILE Mobile Computing and Communications Review **5**(4) (2001) 11–25
27. Deng, J., Han, R., Mishra, S.: INSENS: Intrusion-tolerant routing in wireless Sensor NetworkS. Report CU CS-939-02, CS Dept. , University of Colorado (2002)
28. He, Y., Raghavendra, C.S., Berson, S., Braden, B.: A Programmable Routing Framework for Autonomic Sensor Networks. In: Proc. of the 5th Annual International Workshop on Active Middleware Services (AMS 2003)
29. Legendre, F., Dias de Amorim, M., Fdida, S.: Some Requirements for Autonomic Routing in Self-organizing Networks. In: Proc. of the 1st International Workshop on Autonomic Communication (WAC 2004), Berlin, Germany (2004)
30. Santivanez, C., Stavrakakis, I.: Towards Adaptable Ad Hoc Networks: The routing Experience. In: WAC 2004, Berlin, Germany (2004)
31. Liu, D., Ning, P.: Location-based pairwise key establishments for static sensor networks. In: Proc. of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN '03), Fairfax, VA (2003)
32. Lazos, L., Poovendran, R.: Energy-Aware Secure Multicast Communication in Ad-hoc Networks Using Geographic Location Information. In: Proc. of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2003)
33. Sastry, N., Shankar, U., Wagner, D.: Secure Verification of Location Claims. In: Proc. of the ACM Workshop on Wireless Security (2003)
34. Lazos, L., Poovendran, R.: SeRLoc: secure range-independent localization for wireless sensor networks. In: Proc. of the ACM Workshop on Wireless Security, Philadelphia, PA (2004)
35. Capkun, S., Hubaux, J.P.: Secure Positioning of Wireless Devices with Appplication to Sensor Networks. To appear in Proc. of IEEE INFOCOM (2005)
36. Du, W., Fang, L., Ning, P.: LAD: Localization Anomaly Detection for Wireless Sensor Networks. In: Proc. of the 5th IEEE Inter. Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks (WMAN 05), 2005
37. Davide, F.: Strategic direction towards Autonomic Communication. Telecom Italia Learning Services (2004)
38. Hu, L., Evans, D.: Secure Aggregation for Wireless Networks. In: Proc. of Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL (2003)
39. Przydatek, B., Song, D., Perrig, A.: SIA: Secure Information Aggregation in Sensor Networks. In: Proc. of the First International Conference on Embedded Networked Sensor Systems (SenSys) (2003) 255–265
40. Dimitriou, T., Foteinakis, D.: Secure In-Network Processing in Sensor Networks. In Proc. of the 1st Workshop on Broadband Advanced Sensor Networks (IEEE BASENETS), San Francisco (2004)
41. Malan, D., Welsh, M., Smith, M.: A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography. In Proc. of the 1st IEEE Inter. Conference on Sensor and Ad Hoc Communications and Networks, 2004
42. Blass, E.-O., Zitterbart, M.: Towards Acceptable Public-Key Encryption in Sensor Networks. To appear in Proc. of the 2nd International Workshop on Ubiquitous Computing (2005)