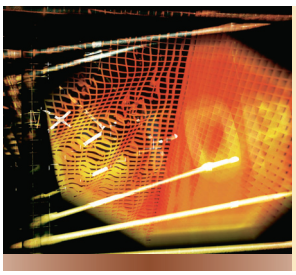
# Security and Privacy in Sensor Networks

**Haowen Chan and Adrian Perrig,** Carnegie Mellon University

Sensor networks offer economically viable solutions for a variety of applications. For example, current implementations monitor factory instrumentation, pollution levels, freeway traffic, and the structural integrity of buildings. Other applications include climate sensing and control in office buildings and home environmental sensing systems for temperature, light, moisture, and motion.

Sensor networks are key to the creation of *smart spaces*, which embed information technology in everyday home and work environments. The miniature wireless sensor nodes, or motes, developed from low-cost off-the-shelf components at University of California, Berkeley, as part of its *smart dust* projects, establish a self-organizing sensor network when dispersed into an environment.

The privacy and security issues posed by sensor networks represent a rich field of research problems. Improving network hardware and software may address many of the issues, but others will require new supporting technologies.



**Sensor networks pose security and privacy challenges that will require new technological solutions.**

## SENSOR NODE COMPROMISE

We expect future sensor networks to consist of hundreds or thousands of sensor nodes. Each node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical attack. The networks may be dispersed over a large area, further exposing them to attackers who capture and reprogram individual sensor nodes.

Attackers can also obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node. Once in control of a few nodes inside the network, the adversary can then mount a variety of attacks—for example, falsification of sensor data, extraction of private sensed information from sensor network readings, and denial of service.

Addressing the problem of sensor node compromise requires technological solutions. For example, cheap tamper-resistant hardware could make it challenging to reprogram captured sensor nodes. However, making nodes robust to tampering is not economically viable. We must therefore assume that an attacker can compromise a subset of the sensor nodes.

Hence, at the software level, sensor networks need new capabilities to ensure secure operation even in the presence of a small number of malicious network nodes. *Node-to-node authentication* is one basic building block for enabling network nodes to prove their identity to each other. *Node revocation* can then exclude malicious nodes.

Achieving these goals on resource-limited hardware will require lightweight security protocols. Further, all communications and data-processing protocols used in sensor networks must be made *resilient*—that is, able to function at high effectiveness even with a small number of malicious nodes. For example, routing protocols must be resilient against compromised nodes that behave maliciously.

## EAVESDROPPING

In wireless sensor network communications, an adversary can gain access to private information by monitoring transmissions between nodes. For example, a few wireless receivers placed outside a house might be able to monitor the light and temperature readings of sensor networks inside the house, thus revealing detailed information about the occupants' personal daily activities.

Encrypting sensor node communications partly solves eavesdropping problems but requires a robust key exchange and distribution scheme. The

scheme must be simple for the network owner to execute and feasible for the limited sensor node hardware to implement. It must also maintain secrecy in the rest of the network when an adversary compromises a few sensor nodes and exposes their secret keys. Ideally, these schemes would also allow revocation of known exposed keys and rekeying of sensor nodes.

The large number of communicating nodes makes end-to-end encryption usually impractical since sensor node hardware can rarely store a large number of unique encryption keys. Instead, sensor network designers may opt for hop-by-hop encryption, where each sensor node stores only encryption keys shared with its immediate neighbors. In this case, adversary control of a communication node eliminates encryption's effectiveness for any communications directed through the compromised node. This situation could be exacerbated if an adversary manipulates the routing infrastructure to send many communications through a malicious node.

More robust routing protocols are one solution to this problem. Another solution is *multipath routing*, which routes parts of a message over multiple disjoint paths and reassembles them at the destination. Efficient discovery of the best disjoint paths to use for such an operation is another research challenge.

## PRIVACY OF SENSED DATA

Sensor networks are tools for collecting information, and an adversary can gain access to sensitive information either by accessing stored sensor data or by querying or eavesdropping on the network. Adversaries can use even seemingly innocuous data to derive sensitive information if they know how to correlate multiple sensor inputs. For example, an adversary that gains access to both the indoor and outdoor sensors of a home may be able to isolate internal noise from external noise and thus extract details about the inhabitants' private activities.

The main privacy problem, however, is not that sensor networks enable the collection of information that would otherwise be impossible. In fact, much information from sensor networks could probably be collected through direct site surveillance. Rather, sensor networks aggravate the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information in a low-risk, anonymous manner. Remote access also allows a single adversary to monitor multiple sites simultaneously.

**The large number of communicating nodes usually makes end-to-end encryption in sensor networks impractical.**

Ensuring that sensed information stays within the sensor network and is accessible only to trusted parties is an essential step toward achieving privacy. Data encryption and access control is one approach. Another is to restrict the network's ability to gather data at a detail level that could compromise privacy. For example, a sensor network might anonymize data by reporting only aggregate temperatures over a wide area or approximate locations of sensed individuals. A system stores the sensed data in an anonymized database, removing the details that an adversary might find useful.

Another approach is to process queries in the sensor network in a distributed manner so that no single node can observe the query results in their entirety. This approach guards against potential system abuse by compromised malicious nodes.

## DENIAL-OF-SERVICE ATTACKS

As safety-critical applications use more sensor networks, the potential damage of operational disruptions becomes significant. Defending against denial-of-service attacks, which aim to destroy network functionality rather than subverting it or using the sensed information, is extremely difficult.

DoS attacks can occur at the physical layer—for example, via radio jamming. They can also involve malicious transmissions into the network to interfere with sensor network protocols or physically destroy central network nodes. Attackers can induce battery exhaustion in sensor nodes—for example, by sending a sustained series of useless communications that the targeted nodes will expend energy processing and may also forward to other nodes.

More insidious attacks can occur from inside the sensor network if attackers can compromise the sensor nodes. For example, they could create routing loops that will eventually exhaust all nodes in the loop.

Potential defenses against denial-of-service attacks are as varied as the attacks themselves. Techniques such as spread-spectrum communication or frequency hopping can counteract jamming attacks. Proper authentication can prevent injected messages from being accepted by the network. However, the protocols involved must be efficient so that they themselves do not become targets for an energy-exhaustion attack. For example, using signatures based on asymmetric cryptography can provide message authentication. However, the creation and verification of asymmetric signatures are highly computationally intensive, and attackers that can induce a large number of these operations can mount an effective energy-exhaustion attack.

## MALICIOUS USE OF COMMODITY NETWORKS

The proliferation of sensor networks will inevitably extend to criminals who can use them for illegal purposes. For example, thieves can spread sensors on the grounds of a private home to detect the inhabitants' presence. If the sensors are small enough, they can also plant

them on computers and cell phones to extract private information and passwords. With widespread use, the cost and availability barriers that discourage such attacks will drop.

Sensor detectors offer one possible defense against such attacks. A detector must be able not only to detect the presence of potentially hostile wireless communications within an area that may have significant levels of radio interference but also to differentiate between the transmissions of authorized and unauthorized sensor networks and other devices. Such technologies might not prevent unauthorized parties from deploying sensor networks in sensitive areas, but they would make it more costly, thus alleviating the problem somewhat.

Sensor networks are set to become a truly pervasive technology that will affect our daily lives in important ways. We cannot deploy such a critical technology, however, without first addressing the security and privacy research challenges to ensure that it does not turn against those whom it is meant to benefit. ■

***Haowen Chan*** *is doctoral student in the Department of Computer Science at Carnegie Mellon University. Contact him at haowenchan@cmu.edu.*

***Adrian Perrig*** *is an assistant professor with appointments in the departments of electrical and computer engineering, engineering and public policy, and computer science at Carnegie Mellon University. Contact him at perrig@cmu.edu.*

**Editor: William A. Arbaugh, Dept. of Computer Science, University of Maryland at College Park; waa@cs.umd.edu**