

Taking Sensor Networks from the Lab to the Jungle

Andrew S. Tanenbaum, Chandana Gamage, and Bruno Crispo
Vrije Universiteit Amsterdam



Researchers must address the systems aspects of wireless sensor networks.

Stopping the flow of illegal immigrants, smugglers, and terrorists across national borders is a hot topic from the jungles of Sri Lanka to the deserts of Arizona. Not surprisingly, people have suggested using sensor networks to detect these unlawful intruders. Other suggested applications of sensor networks include battlefield observation and forest fire detection. In these and other applications, people have proposed dropping cryptographically secure, battery-powered sensors from aircraft.

However, our investigations suggest that large-scale air-dropped sensor networks would not actually work well in practice or be cost-efficient using current technology. Although researchers have developed effective solutions to *network* problems easily simulated in the lab, they have not addressed the *systems* challenges associated with deployment in real-world conditions.

SENSOR NETWORKS

Sensor networks pose unique technical and logistical challenges. Unlike traditional local area and wide area networks,

- electricity is unavailable, requiring sensors to be battery powered;
- a wireline network is absent, requiring sensors to communicate using an ad hoc wireless network;
- roads are often nonexistent, requiring sensors to be air-dropped by manned or unmanned aircraft; and
- numerous sensors are needed, requiring sensors to be low cost.

As most large-scale sensor networks must operate under hostile conditions, researchers have focused on providing authenticity, integrity, and confidentiality protection for messages transmitted over the wireless network. The primary obstacles in this effort are the low speed of the sensors' CPUs, small amount of RAM available, and large amount of power needed to transmit each bit.

Many proposed cryptographic methods effectively counter injection of false data, modification of data, eavesdropping on wireless communication, cloning of nodes, and node capture. Other research on power-efficient MAC layer algorithms and routing protocols, distributed and cooperative schemes for node localization, and effi-

cient data aggregation techniques has likewise shown remarkable progress.

However, achieving reliable and secure radio communication is not the whole story. To examine the systems aspects of large-scale sensor networks, we acquired some commercially available sensors and measured their radio range, something that has not been widely reported in the literature.

We found the range of a typical low-cost sensor on the ground in an open field to be about 7 meters; at a height of 1 m, the range increases to about 35 m. Interestingly, the range in a forested area is comparable, primarily due to multipath signal propagation (C. Gamage et al., "Security for the Mythical Air-Dropped Sensor Network," *Proc. 11th IEEE Symp. Computers and Communications*, IEEE CS Press, 2006, pp. 41-47).

Thus, sensors must be spaced rather closely to avoid gaps in connectivity. Field experiments have shown the operating range for the acoustic, thermal, humidity, infrared, or magnetic sensing elements to be less than the radio range, necessitating even closer spacing of the nodes (A. Arora et al., "ExScal: Elements of an Extreme Scale Wireless Sensor Network," *Proc. 11th IEEE Int'l Conf. Embedded and Real-Time Computing Systems and Applications*, IEEE CS Press, 2005, pp. 102-108).

BORDER MONITORING

One of the most widely cited applications for sensor networks is monitoring national borders for humans attempting to surreptitiously cross on foot, especially at night. Along a long land border, such as the 3,100-km US-Mexico boundary, illegal crossings could happen at almost any point, requiring that the full length be under surveillance, lest intruders discover the weak spots.

Intrusion detection can be based on sound or vibration, which good-quality sensors can easily monitor but only within a range of less than 10 m. However, distinguishing between a person and a large wild animal moving in the underbrush is not so simple

due to the low-cost sensors' limited CPU power and memory.

Using our measured 7-m radio range, the US-Mexico border would need more than 440,000 sensors. Alternatively, only 88,000 sensors would be required if placed on 1-m long weighted sticks, but getting air-dropped sensors to land upright and stick in the ground exactly 35 m apart is nontrivial, especially in rocky terrain. To avoid breaks in the network, many more sensors would be needed in practice.

Further, since a sensor's battery life is typically six months, the airdrop must be repeated biannually. The resulting sensor forest would not be inconspicuous, although that may have some deterrence value. In our view, air dropping sensors is infeasible and planting them manually twice a year is highly labor intensive, precisely what the airdrop is supposed to eliminate. This calls into question one of the motivating factors for using large-scale sensor networks: ease of deployment.

When a sensor detects an intrusion, it sends a wireless message to the nearest border patrol post. Assuming that posts are spaced at 20-km intervals, a border patrol officer who jumps in his vehicle instantly and travels at 100 km/h could still take as long as six minutes to get to the sensor that raised the alarm. By that time, an intruder running 10 km/h away from the border could be anywhere in a semicircular area with a 1-km radius. Finding the person at night may not be easy, especially if the terrain offers places to hide.

For a supposedly unmanned operation, the costs are significant. Stationing an officer at each of the 155 posts needed along the US-Mexico border 168 hours a week would require four shifts and thus at least 620 people, plus 155 vehicles. When added to the expense of semiannual sensor replacement (currently \$100 per unit, exclusive of deployment), monitoring the border would cost many tens of millions of dollars per year.

Given such costs, alternative approaches such as building a long fence must be considered. Further, the

presence or absence of better cryptography is hardly the factor that will drive deployment, despite what some researchers appear to believe.

BATTLEFIELD OBSERVATION

Researchers also have proposed using sensor networks as a means of secretly observing enemy activities on a battlefield. This solution calls for small unmanned aerial vehicles (UAVs) to fly at very low altitudes over the designated area and deploy thousands of sensor nodes, which would establish clusters of ad hoc networks to sense and collect data on the movement of personnel and vehicles.

Air-dropping sensors is infeasible and planting them manually twice a year is highly labor-intensive.

Here, too, the sensors' limited radio range is a major problem. For example, more than 10,000 nodes would be required to monitor just 1 square kilometer. Not only would the high density of nodes make concealment of the network impossible, but a single soldier with a pair of binoculars could monitor the area more cost-effectively.

For much larger areas, the cost of sensors alone makes this approach untenable. In addition, deploying so many nodes would require either a large number of UAVs operating simultaneously or several UAVs making multiple passes over the battlefield, neither of which is likely to elude enemy observation.

FOREST FIRE DETECTION

In some respects, a sensor network is more feasible as an early warning system for forest fires. While border monitors must be able to respond to an intrusion within minutes, firefighters have considerably more time to respond to activity detected by thermal or smoke sensors.

In addition, carefully placing nodes close to vulnerable areas such as hilltops subject to lightning strikes can substantially reduce the number of sensors required to cover a large geographic area. Our experiments have shown that multipath radio signal propagation actually provides a longer radio hop distance in dense vegetation than in open spaces.

However, the most important systems aspect of a fire-detection sensor network is its lifetime. Unlike a border-monitoring network with many detected events over a moderate lifetime or a battlefield observation network with a massive number of detected events over a relatively short lifetime, the fire detection network must operate for a very long period of time to discover a comparatively rare event.

Nodes in a forest sensor network are subject to random failures due to battery exhaustion as well as antennas being reoriented in the wrong direction by falling branches, curious animals, wind, and so on. Because such networks relay messages hop by hop, failure of several closely spaced nodes could partition the network into noncommunicating subnetworks. Thus, a sensor that detects an actual fire might not be able to get its message to the nearest base station.

Newer sensors with theoretical radio ranges up to 10 times longer than those we tested are becoming available, but they are more sensitive to noise and their potential utility is still an open issue. In any case, increasing sensors' radio range would not address the need for closely spaced border patrol stations, sensors' short battery lifetime, the limited range of the sensors themselves, and other problems.

Sensor networks using existing technology could effectively be deployed on a limited scale—for example, to guard the perimeter of a fixed and valuable asset, such as a military base, oil refinery, or nuclear reactor, or to replace wired SCADA systems that monitor industrial machinery. In these cases, the

sensors can be accurately installed by hand, are relatively inexpensive, and are wired to the electricity grid, giving them greater range and eliminating the need for frequent replacements due to battery exhaustion.

But even here, caution is required. During the Soviet occupation of Afghanistan in the 1980s, rebels threw live rabbits over base fences to trigger motion detectors. After several weeks of false alarms, the bases turned off the motion detectors, allowing surreptitious attacks, a clear failure to factor systems aspects into the design.

Although sensor networks have a bright future, researchers must spend more effort on the systems aspects of these networks rather than only the network aspects of MAC protocols, message routing, data aggregation, node localization, and security. ■

Andrew S. Tanenbaum is a professor in the Department of Computer Science at Vrije Universiteit Amsterdam. Contact him at ast@cs.vu.nl.

Chandana Gamage is a postdoctoral researcher in the Department of Com-

puter Science at Vrije Universiteit Amsterdam. Contact him at chandag@cs.vu.nl.

Bruno Crispo is an assistant professor in the Department of Computer Science at Vrije Universiteit Amsterdam. Contact him at crispo@cs.vu.nl.

**Editor: Bill Schilit, Intel Research
Seattle; bill.schilit@intel.com**



Computer

Innovative Technology for Computer Professionals

Welcomes Your Contribution

**Computer
magazine
looks ahead
to future
technologies**

IEEE
computer
society
60TH anniversary

- **Computer**, the flagship publication of the IEEE Computer Society, publishes peer-reviewed technical content that covers all aspects of computer science, computer engineering, technology, and applications.
- Articles selected for publication in **Computer** are edited to enhance readability for the nearly 100,000 computing professionals who receive this monthly magazine.
- Readers depend on **Computer** to provide current, unbiased, thoroughly researched information on the newest directions in computing technology.

**To submit a manuscript for peer review,
see **Computer's** author guidelines:**

www.computer.org/computer/author.htm