ON THE RADAR

DECEMBER 15, 2019

Sensor Networks

A Technology Primer

BY MAXWELL SIMON, JANANI MOHAN

TYPE	CHARACTERISTICS	RISK FACTORS
Sensor	Detectability, Precision, Persistence, Resiliency, Speed, Vantage	Action-enabling, intrusive, preemptive, vulnerable

DOMAIN	COUNTRY
Space, Air, Land, Sea	United States, Russia, China, etc.

Introduction

Today, several technologies are going "smart," from homes to cars to medical supplies. Networks of sensors enable these technologies, using remote data collection to increase consumer situational awareness. While sensor networks are common in civilian life, they are also used by militaries to detect conventional and nuclear deployment.[1]

Sensor networks involve complex technological systems based on autonomous nodes that monitor environmental conditions such as light, heat, and radiation.[2] Nodes consist of sensors, data processors, communication devices, and power sources such as batteries.[3] They are interconnected through a network and can transmit data to other nodes or directly to the end user. Sensor networks are different from non-networked sensors because they transmit the data they collect back to the decision-maker instead of requiring in-person data access.[4] Many sensors utilize delay tolerant communications, where data is transmitted and stored from node to node until the data is within the

Sensor networks involve complex technological systems based on autonomous nodes that monitor environmental conditions such as light, heat, and radiation.

[1] Chee-Yee Chong and Srikanta Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges," *Proceedings of the IEEE* 91, no. 8 (2003): 1247–56.

[2] Wireless Sensor Networks Project Team, "Internet of Things: Wireless Sensor Networks" (Geneva, Switzerland: International Electrotechnical Commission, 2014), http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf.

[3] Vidyasagar Potdar, Atif Sharif, and Elizabeth Chang, "Wireless Sensor Networks: A Survey" (2009 International Conference on Advanced Information Networking and Applications Workshops, Perth, Australia: Digital Ecosystems and Business Intelligence Institute, 2009).

[4] Chong and Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges."

network range of the main transmission device.[5] Others rely on wireless mesh network connectivity, where data is constantly transmitted over the network, for more persistent observation.

State of Play

Sensor networks have a diverse range of applications across several physical domains (see **Table 1** below). For example, the U.S. military has ground, marine, air, and satellite-based sensors.[6] The U.S. military employs several sensors on land to provide midcourse missile coverage and identify nuclear threats. For example, DARPA's SIGMA program has developed a low-cost, high-efficiency radiation sensor network that can identify potential nuclear, biological, and chemical weapons and dirty bombs.[7] The U.S. military also deploys marine-based sensors in the open ocean. The Sea-Based C-Band Radar, for instance, is attached to a semi-submersible platform and includes a network of sensors which can track incoming missiles. Additionally, many military technologies have flexible location capabilities, meaning they are capable of being deployed on the ground, in the air, under water, and inside vehicles and buildings.[8] The Army Navy Transportable Radar Surveillance, which tracks and identifies missile trajectories, can be carried by air, ship, or on the ground, for example. The Navy Aegis Ballistic Missile Defense system, a sensor network that identifies ballistic missile threats, is also adaptable to ship and land locations. Furthermore, sensor networks are also deployable in space to enhance situational awareness. Examples include the U.S. military's Near Field Infrared Experiment, which was launched into orbit to identify and collect data on missile exhaust plumes, and the Space-based Kill Assessment (SKA), an infrared sensor network hosted on commercial satellites to detect missile signatures. The SKA is highly resilient because it relies upon a network of many interconnected sensors, each mated to a different satellite.[9] The total number of sensors and their placement would be dependent on each particular mission, and by tracking the signatures of incoming missiles and defensive interceptors, they create a wide network that is capable of verifying if missiles have been destroyed or still pose a threat. Traditionally, U.S. military sensor networks are air-gapped, a security procedure where the networks are kept physically isolated from public networks that are more vulnerable to threats.

Several other countries have also developed sensor network technologies. For example, China is building underwater sensor networks. These networks track environmental data affecting China's naval capabilities, including the speed at which submarines can move. These networks also enable Chinese surveillance of

---

[5] "Disruption Tolerant Networking," Analysis, *National Aeronautics and Space Administration* (blog), May 25, 2018, https://www.nasa.gov/content/dtn.

[6] U.S. Department of Defense Missile Defense Agency, "Sensors," October 3, 2019, https://www.mda.mil/system/sensors.html.

[7] Mark Wrobel, "SIGMA," U.S. Department of Defense, *Defense Advanced Research Projects Agency* (blog), n.d., https://www.darpa.mil/program/sigma.

[8] Chong and Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges"; "SIGMA," U.S. Department of Defense, *Defense Advanced Research Projects Agency* (blog), n.d., https://www.darpa.mil/about-us/timeline/sigma.

[9] "Spacebased Kill Assessment" (Missile Defense Agency, February 17, 2017), https://www.mda.mil/global/documents/pdf/ska.pdf; Mike Gruss, "MDA Kill Assessment Sensors Would Be Commercially Hosted," *SpaceNews*, March 20, 2015, https://spacenews.com/mda-kill-assessment-sensors-would-be-commercially-hosted/.

adversary submarines.[10] India is developing its sensor networks through partnerships with the private sector. The Indian Army plans to use sensors to improve nighttime vehicular sensing.[11]

Overview of Sensors in Military Use		
Operations	Used to detect conventional weapons, nuclear weapons, other forms of WMD, and environmental factors. Used for navigation.	
Situational Awareness	Provide decision-makers with more timely, accurate data from remote locations on various environmental factors.	
Physical Domains	**Platforms**	**Example**
Land	Stationary platforms, mobile vehicles	*SIGMA Program*: sensors trace radiation signatures on land.
Sea	Marine flotation devices, mobile vehicles (ships), UUVs/USVs	*C-Band Radar*: sensors located in ocean to provide advanced warning for missiles.
Air	Unmanned aerial vehicles, airplanes, missiles	*Robo-Wing Program*: sensors are made more mobile and covert through aerial movement.
Space	Satellites; synthetic-aperture radar (SAR), optical hyperspectral	*Space-based Kill Assessment*: sensors located on commercial satellites track long-range threats. *Hyperspectral Imaging* (HSI): HSI sensors take hundreds or thousands of continuous images across the electromagnetic spectrum and create highly detailed images.[12] *Synthetic-Aperture Radar* (SAR): transmits sequential electromagnetic waves which are collected by sensors and processed into 2D and 3D images.[13]

Table 1. *Overview of the use of sensors in militaries.*

Sensor networks are widely used for military purposes for two primary reasons. First, military-grade sensor networks are increasingly based on existing commercial smart technology that is globally available and easily

[10] Eugene Chow, "China Has a Plan to Find the Navy's Submarines Deep in the Pacific," *The National Interest* (blog), January 29, 2018, https://nationalinterest.org/blog/the-buzz/china-has-plan-find-the-navys-submarines-deep-the-pacific-24231.

[11] Chowdhury, Amit Paul. "These startups are bringing IoT and sensor-based solutions to the defense sector in India." IoT India Magazine. https://www.iotindiamag.com/2017/06/startups-bringing-iot-sensor-based-solutions-defence-sector-india/ (accessed June 16, 2016)

[12] Bernadette Stadler and Meyer Thalheimer, "Hyperspectral Imaging: A Technology Primer," Analysis, *Center for Strategic and International Studies, On the Radar* (blog), November 15, 2018, https://ontheradar.csis.org/issue-briefs/hyperspectral-imaging-a-technology-primer/.

[13] Martin Krischt and Carsten Rinke, "3D Reconstruction of Buildings and Vegetation from Synthetic Aperture Radar (SAR) Images," *MVA*, 1998.

acquired. When stationed in space, sensors can be mounted to commercial satellites, taking advantage of infrastructure already in place.

Second, sensor technologies can be relatively cheap to develop and produce. Generally, sensor nodes tend to require little energy and have low storage, processing, and communication capabilities.[14] Because they are relatively inexpensive, vast arrays of sensors can be deployed in a given environment, especially important given their low data storage and power.[15]

The ease of developing sensor networks provides several opportunities to optimize their use.[16] Physical attributes could be adjusted to make sensors smaller and more light-weight. As these attributes improve, sensors will become less vulnerable to detection and destruction allowing them to operate for longer periods of time. Sensor self-formation could also be improved. Formation refers to sensors that can identify other friendly nodes and transmit data to those nodes. This is especially useful if nodes are "captured" by adversaries or degraded from environmental factors, increasing the likelihood that sensors are able to send data back to their parent states. Improvements in self-formation could also enhance sensor intelligence by allowing nodes to receive and respond to data in addition to transmitting it. If sensors can receive and transmit data to other sensors strategically, commands could be sent to certain sensors to change their operation pattern. This is particularly useful as sensors could be made intelligently ***mobile***, helping them avoid environmental threats.

As sensors capabilities improve, their coverage size could increase as well. This would allow fewer sensors to be placed in the target region, reducing the risk of exposure. Increasing the lifespan of sensors would also reduce the risk of exposure to adversaries because sensors are particularly vulnerable during deployment, especially if the deployment involves an on-ground covert operation. Sensors could also become more covert if their illuminative characteristics, including electromagnetic and electronic signatures, are more effectively hidden. If technological signatures are minimized or only turned on during brief periods of time, adversaries will be less likely to detect the sensors. And, if adversaries somehow found the sensors, each node could be made to encrypt its stored data so that the data is protected from third-party access.

As sensors become less expensive, states with fewer resources will choose to operate sensors because they are an affordable yet powerful tool. Their inexpensiveness not only allows states to increase the number of sensors they deploy but also the sensing capabilities of individual sensor nodes within the network.

While these potential improvements are not exhaustive, they provide an overview of some of the key areas for sensor network advancement across several physical domains. In the United States, the Defense Advanced Research Projects Agency (DARPA) is currently working on SIGMA+ to advance their SIGMA sensors.[17] The original program includes a relatively "low-cost, high-efficiency" radiation detection program using spectroscopic gamma and neutron sensors.[18] SIGMA+ will increase the sensors' distance of detection and will detect a larger number of substances in chemical and biological weapons. The expected improvements are being designed to

---

[14] Rajat Gupta et al., "Security for Wireless Sensor Networks in Military Operations" (International Conference on Computing and Networking Technology, Tiruchengode, India: Institute of Electrical and Electronics Engineers, 2013).

[15] Arun Madhu and A. Sreekumar, "Wireless Sensor Network Security in Military Application Using Unmanned Vehicles," *IOSR Journal of Electrionics and Communication Engineering*, August 2014, 51–58.

[16] Boselin Prabhu, M. Pradeep, and E. Gajendran, "Military Applications of Wireless Sensor Network System," *A Multidisciplinary Journal of Scientific Research & Education* 2, no. 12 (December 2016).

[17] "DARPA Seeks to Expand Real-Time Radiological Threat Detection to Include Other Dangers," U.S. Department of Defense, *Defense Advanced Research Projects Agency* (blog), February 20, 2018, https://www.darpa.mil/news-events/2018-02-20.

[18] Wrobel, "SIGMA."

provide sensing capabilities ten times more sensitive than the current standard, enabling detection of attacks earlier and from a wider range of biological agents.

The program was tested along the Indianapolis Motor Speedway in April, 2018. Phase I will focus on expanding the existing sensor network with more sensitive detection systems and the final phase will integrate analytics into the system's detection mechanism, using previously collected data to inform future events.[19] DARPA is also currently working on the "Ocean of Things" project for marine sensors.[20] DARPA hopes to create floating sensor networks at low-cost through the development of intelligent floats to store passive sensor suites and cloud-based software to analyze sensor data. The sensor floats will transmit information intermittently, before safely sinking into the deep sea. DARPA has not publicly disclosed development progress since 2018 but has said sensors will track oceanographic and environmental data, as well as the movement of nearby vessels.[21] DARPA has also developed a small satellite sensors program with the goal of creating cheap and secure low-earth-orbit micro-sensors to use in providing "on-demand" intelligence for tactical warfare.[22]

Although the U.S. military has developed highly effective sensor networks, there are several possible areas for advancement; enhancing capabilities in low visibility environments and decreasing sensor detectability by enemy combatants will make them more capable.[23] Other countries are also advancing their multidomain sensor networks. For example, China is working to develop sensors for military and civilian use, building emplacements on four different outposts on the Spratly Islands and rapidly upgrading its existing anti-ship, anti-air, and anti-submarine sensors on its naval platforms. China's People's Liberation Army (PLA) researchers are developing smart networks that increasingly leverage artificial intelligence to train and learn from information acquired from sensors.[24]

Improvements to Situational Awareness

As countries continue to advance their sensor networks, their core situational awareness (SA) capabilities will improve. The improvements to SA provided by sensor networks are discussed in greater detail below.

Vantage: Sensor networks enhance SA through increased vantage by enabling the detection, tracking, and monitoring of threats within key strategic environments and locations. Sensor networks are sometimes used in adversary territory and are extremely useful in monitoring for early detection of adversary missile launches. They can be deployed on the ground, in the air, under water, on bodies, in vehicles, and inside buildings.

---

[19] Chris Galford, "DARPA SIGMA+ Program Tests New Sensors to Detect Chemical Threats Regionally," *Homeland Preparedness News*, May 2, 2019, https://homelandprepnews.com/stories/33677-darpa-sigma-program-tests-new-sensors-to-detect-chemical-threats-regionally/.

[20] "Ocean of Things Aims to Expand Maritime Awareness across Open Seas," Department of Defense, *Defense Advanced Research Projects Agency* (blog), December 6, 2017, https://www.darpa.mil/news-events/2017-12-06.

[21] "Ocean of Things Aims to Expand Maritime Awareness across Open Seas."

[22] Chris Simi, "Small Satellite Sensors," Department of Defense, *Defense Advanced Research Projects Agency*, n.d., https://www.darpa.mil/program/small-satellite-sensors.

[23] Richard Nabors, Donald A. Reago, and Nathan Burkholder, "Complex Environments Call for Better Sensors," *United States Army* (blog), December 9, 2018, https://www.army.mil/article/198814/complex_environments_call_for_better_sensors.

[24] Elsa Kania, "EMERGING TECHNOLOGIES, EMERGING CHALLENGES — THE POTENTIAL EMPLOYMENT OF NEW TECHNOLOGIES IN FUTURE PLA NC3," NAPSNet Special Reports (Nautilus Institute for SEcurity and Sustainability, September 5, 2019), https://nautilus.org/napsnet/napsnet-special-reports/emerging-technologies-in-future-pla-nuclear-command-control-and-communications/.

Sensor networks can offer more dense or sparse coverage depending on the number of sensors deployed.[25] The effective range of individual node sensors varies depending on the antenna design, but the average range is between 100 and 250 feet. There are other sensor designs with ranges up to 1000 feet, though larger coverage area often comes with the tradeoff of a shorter node lifetime.[26]

Speed: Extensive sensor networks do not, by themselves, necessarily increase decisional speed, and could significantly slow down decision-making if data inflows are so great that they overwhelm existing computational power. Battlefield networks and sensors are yielding yottabytes (2^{80} bytes) of raw data that must first be analyzed to offer improvements in situational awareness. The U.S. Navy, specifically, has developed an increasing demand for the data generated by intelligence, surveillance, and reconnaissance (ISR) sensors, but the amount of data generated has become overwhelming. Challenges include slow download times, large amounts of unorganized raw data, and unfiltered analyst workstations.[27]

An important challenge identified by the U.S. Army is processing data quickly enough to make decisions in a timely fashion, requiring greater investment in High Performance Computing (HPC) platforms—which the U.S. Army Research Laboratory Technical Implementation Plan characterizes as a near-term need—to improve complex sensor and heterogeneous data processing.[28] Others have suggested converting data storage into a cloud system, similar to that used by the National Security Agency or Google, to limit the transmission of raw data and rely more heavily on metadata.[29]

Importantly, sensor networks must be paired with appropriate, and improved, computational power if they are to improve decisional speed. If speed of analysis can match the more rapid information inflow currently provided by robust networks of sensors, knowledge of adversary actions could be obtained more quickly as well.

Resiliency: Sensor networks allow for the resilient production of data unadulterated from disturbances caused by conflict (e.g., land movement due to nearby bombing). For example, when sensors are built with more resilient topologies, each node stores the information being transmitted and connects to multiple other nodes in the system. This ensures that if one node is destroyed accidentally or by an adversary, the information will be sent to a state's decision-making apparatus without harming the data-collecting and transmitting capabilities of the other nodes. Furthermore, since each sensor is relatively cheap to produce, the network can be made more resilient by deploying additional redundant sensors.

Detectability: Most sensors are stationary and produce traceable electronic signals, making them more vulnerable to detection. However, by using delay tolerant networks, sensors can transmit data intermittently, rather than producing constant electronic signals. Reducing transmissions to the absolute minimum, both in duration and frequency of emission, lessens the chance of adversary detection.[30] Steps such as camouflaging and miniaturizing of sensors can also improve concealment. The DARPA Robo-Wing Program, for example, is

---

[25] Chong and Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges."

[26] Potdar, Sharif, and Chang, "Wireless Sensor Networks: A Survey."

[27] Isaac Porche et al., "Data Flood: Helping the Navy Address the Rising Tide of Sensor Information" (Washington, DC: RAND Corporation, 2014), https://www.rand.org/pubs/research_reports/RR315.html.

[28] U.S. Army Research Laboratory, "Technical Implementation Plan, 2016-2020" (U.S. Department of Defense, 2016), https://www.arl.army.mil/www/pages/172/docs/Technical_Implementation_Plan_v2_FINAL.pdf.

[29] Porche et al., "Data Flood: Helping the Navy Address the Rising Tide of Sensor Information."

[30] Michael Winkler et al., "Theoretical and Practical Aspects of Military Wireless Sensor Networks," *Journal of Telecommunications and Information Technology*, February 2008, 37–45.

developing sensors disguised as small insects.[31] Through these methods, detectability is decreased, allowing sensors to operate for longer periods without detection.

Precision: Precision—the level of detail and quality of information collected—is significantly improved by sensor networks, which offer the potential to collect more robust data over wider geographic areas. Sensor technology is also becoming increasingly sensitive to its surroundings, allowing for the collection of relevant information far away from the source. Furthermore, sensor networks communicate data among each of the nodes within the network, allowing the sensors to compare and compile the data to achieve higher confidence in data accuracy.

Because sensors do not sort through raw data, they must be paired with sufficient computation power to effectively characterize data and improve information quality for decision-makers.

Persistence: Sensor networks can collect data continuously and allow for persistent SA. However, continuous use of sensors and constant transmission of data increases the likelihood that an adversary will detect transmissions and requires significant energy. Previously, sensor networks were powered by AA batteries, which only allows an operation lifetime of days to weeks. However, with improved battery technologies and the use of alternate energy sources such as solar power, advanced sensors have the ability to operate for months to years without being replaced. Another way to prolong the lifetime of the sensor nodes is programming sensors to sleep for intermittent periods until they are needed, also lowering detectability of transmissions. Operators can also decrease the number of sensor nodes deployed and limit the use of low-level raw signal communication which requires more bandwidth and energy.

Risk Factors for Strategic Stability

While sensor networks improve SA, there are also potential risks that sensors pose to strategic stability. Although sensor networks are not ***destructive***, they are ***vulnerable*** to detection and destruction because adversaries can easily deny their use if they are aware of the sensors' location and existence.

Sensor networks are also ***preemptive*** because they provide situational data and early warning in advance of on-ground maneuvers or missile launches, possibly harming strategic stability. Data gathered by sensor networks can be used defensively to determine potential threats and offensively to improve intelligence by being deployed in adversary territory or from space-based systems. Sensors can also predict the location of strategic assets such as ICBMs and submarines by measuring environmental changes in radiation and heat.

Sensor networks are ***intrusive*** because ground-based and ocean-based sensors must be located within the environment that they are monitoring. To deploy sensors in these conditions, states would either have to conduct aerial drops, leaving the sensors vulnerable to detection and destruction, or physically travel to the location which could lead to detection and fatalities. These issues are multiplied because the location must be close to the target monitoring area and targets like combatant military bases have additional security hurdles to overcome. It is important to note that adversary states may feel threatened by the use of sensor networks if nodes are stationed close to military assets.

The extent that space-based monitoring is considered intrusive is not necessarily clear, as sensors stationed in space can provide detailed information within adversary territory without entering their airspace.

---

[31] Peter Shadbolt, "Robo-Wings: Military Drones That Mimic Hawks and Insects," *CNN*, January 14, 2015, https://www.cnn.com/2015/01/14/tech/mci-drone-robohawk-robofly/index.html.

Sensors stationed on earth must remain clandestine to collect suitable data, especially when operating within hostile territories. If adversaries were to discover sensor nodes monitoring military assets, it would risk stability. Sensors remaining secret are therefore key to the accuracy and persistence of data gathered.

Because sensor networks have multiple situational uses, sensors are ***action-enabling***, allowing states to maneuver against adversaries by collecting and acting on intelligence. Adversaries might perceive these actions as escalatory or threatening, prompting them to first escalate themselves, thus harming stability. With greater capabilities and information, the potential for faulty data or misinterpretation also exists, as it does with other technologies. This poses a risk to stability if greater perceived vantage and precision gives operators misguided confidence in the hostile intentions behind an adversary's actions.

Conclusion

Sensor networks offer great potential to improve situational awareness by enhancing vantage, precision, and persistence. With relatively low development and production costs, they can vastly expand the amount of information received from land, air, sea, and space. Importantly, however, many countries, the United States included, need to further enhance their ability to process the immense amount of data that sensor nodes collect by further developing their computational resources and data management capabilities. Operators of sensor networks will otherwise be overwhelmed by raw data inflows and unable to complete timely analysis.

Especially from space-based platforms, sensor networks can provide detailed information about conventional and strategic assets. Like many emerging ISR technologies, they may dramatically improve situational awareness, though there are potential tradeoffs with strategic stability during a crisis.