Anti-Sensornet: Intruders and Countermeasure

Min-You Wu
Dept. of Computer Science and Engineering, Shanghai Jiao Tong University
Shanghai, China, mwu@sjtu.edu.cn

Abstract

This article addresses a new area of sensor networks — the anti-sensornet. Though the term anti-sensornet is scattered throughout literature, there is no systematic description of the anti-sensornet. In this article, we provide an introduction to anti-sensornet by analyzing the behaviors of intelligent intruders and the methods used to confront them including hiding sensor networks, enhancing detection capabilities and recovering from successful attacks.

1. Introduction

Field surveillance and intruder tracking are among the most important tasks concerning anti-terrorism and military affairs. More generally, surveillance of community places, office buildings, hospitals, banks and other important locations demands high detection probability against potential intruders. The recently emerging sensor network is nicely matched for these types of applications.

Most existing work in the sensor network research has focused on intelligence of sensors or sensor networks, such as tracking the movement of an intruder, where either the intruder is assumed to be non-intelligent, or issues of intruder intelligence are not addressed at all. A common assumption is that an intruder is unaware of the existence of the sensor network, and does not attempt to mask its physical measures, moving forward toward its destination. In real life, however, many intruders are intelligent. They attempt to hide themselves, choose better moving paths, or attack the sensor network. Most existing work on the security issues of sensor networks assumes fake nodes, captured nodes and DoS attacks. Few of them address the issue of detection avoidance.

Most current sensor networks fail to detect intelligent intruders as they were developed under the assumption of non-intelligent intruders. We, here, address this problem of how to build a robust sensor network for the surveillance of intelligent intruders. Anti-sensornet technology is developed for this purpose. The term anti-sensornet is found in literature [6][18]; we propose a more appropriate name, *sensornet countermeasure (SNCM)*, to describe this new technology.

In the context of SNCM, characteristics of intelligent intruders and their behaviors are investigated, as is the methodology on how to confront attack from an intelligent intruder. There are three topics in SNCM:

- hiding techniques for sensor networks in different phases;
- detection techniques that are designed specifically for intelligent intruders; and
- self-healing techniques that repair damage.

We must revisit and redesign sensor network protocols with the new assumption that intruders are intelligent. Techniques developed in this area will help people build more robust sensor networks that have a broader impact on the sensor network infrastructure.

2. Intelligent Intruders

Different types of intruders behave differently. A *non-intelligent intruder* is not aware of sensors or sensor networks. It will remain in place even when being detected or when some threat is approaching. It may walk around randomly, or travel straight toward its destination without considering potential dangers. In contrast, an *intelligent intruder* may take action to:

1. Gather information of the sensor network by
   - using a detector to scout the location, quantity, type, and capacity of surrounding sensor nodes;
   - deploying sensor nodes to collect information.
2. Avoid sensor network's detection by
   - masking or reducing its physical measures to conceal its own existence;
   - searching for the best moving path to avoid detection or tracking.
3. Alter behaviors of the sensor network by
   - physically destroying part of the sensor network;
   - interfering with sensing and/or communication of the sensor network;
   - obtaining the security key of sensor nodes;
   - capturing sensor nodes and utilizing them to attack other nodes;
   - changing routing behaviors of the sensor network;
   - applying a denial of service (DoS) attack on the sensor network.

Before further discussing intruder behavior, we briefly review the broader security issues for the sensor network such as a DoS attack, encryption, or node capture.

978-1-4244-5113-5/09/$25.00 ©2009 IEEE

An intruder could easily interfere with a sensor network by jamming the radio channel [17]. A similar approach can be reproduced on a MAC layer by using a denial of sleep technique [13]. The attacker broadcasts unauthenticated traffic into the network following all MAC rules, while keeping sensor nodes out of their sleep states. This attack could significantly reduce the energy efficiency of MAC protocols such as S-MAC, T-MAC and B-MAC.

On the network layer, there exist many types of attacks on routing protocols [8]. By spoofing, altering, or replaying routing information, attackers are able to create routing loops to attract or redirect network traffic in order to create black-holes or to drop messages. Attackers could also generate a HELLO message flood to disrupt operation in a sensor network. In [16], authors propose the Secure Implicit Geographic Forwarding, a family of configurable secure routing protocols that deal with these attacks.

Secure and efficient key distribution establishes authenticated communication in a sensor network and prevents any malicious physical access. Several key management systems have been proposed in [5] to improve detection of malicious captured nodes and bypassing vulnerable areas. Attackers could also intend to intercept the messages sent among sensor nodes. They can infect message integrity, predict message content, and replay the previous communication. TinySec [7] supports message authenticated code encryption and also uses initialization vectors to prevent prediction of an encrypted message.

A node-capture is a common type of attack on sensor networks. After a successful node-capture, the attacker has full control over the captured sensor including the cryptographic keys, which makes this type of attack difficult to detect; and thus, especially harmful. In [2], authors proposed the concept of a one-time sensor by preloading every sensor with a single cryptographic token before deployment to mitigate a node-capture attack.

This paper focuses on design issues for sensor networks considering intelligent intruders. An intelligent intruder scouts its surrounding environment in order to find out each sensor's location and sensing capability. Different assumptions can be made when designing a robust sensor network:

- the intruder is either moving or stationary;
- the sensor network is either deployed before or after the arrival of intruders;
- the intruder uses either a detector or many sensor nodes to collect information.

We assume that an intruder is equipped with a powerful directional detector that can determine the direction and the distance of a threat. Once a sensor network is detected, an intruder can take action. A stationary intruder, most likely dropped from a helicopter, can react by hiding itself or bypassing the functionality of the sensor network. A moving intruder, in addition to hiding itself and destroying the sensor network, can strategically search for the best path to its destination. If the sensor network is deployed before arrival of the intruder, the intruder can peek around then sneak into the sensing field, if bypass cannot be found. If the intruder is already in the field when the sensor network is deployed, the intruder can try to escape from surveillance by looking for a route with the lowest probability of being detected.

Both the intruder and the sensor network are attempting to detect, hide from and countermeasure each other. It is, however, not a symmetric battle. On the one side, is a single or a few large intruders, and on the other side, are a large number of small sensors. Thus, each part must engage in different technologies.

3. Confronting Intelligent Intruders

A sensor network is deployed for the purpose of surveillance. A sensor network that aims to detect intelligent intruders must:

- minimize its exposure to the intruder;
- maximize its surveillance capability;
- resist interference from the intruder, detect and repair failed portions of the sensor network.

Surveillance can be measured by coverage of a sensor network, such as the coverage percentage with a deterministic surveillance model [10]. Another way to measure surveillance is the average walking distance [4], where an intruder starts walking in a random direction until being detected by any sensor. The degree of surveillance can be calculated based on the average walking distance of all the points and all the directions in a sensing field. The trap coverage is similar to the average walking distance in that it guarantees that any moving object can move only a bounded distance before it is detected [3]. Yet another category of detection probability is the path-based surveillance, where the best path can be found with Voronoi diagrams [1]. Path-based surveillance is suited for measuring the quality of tracking an intruder.

Most sensor network protocols do not treat the intruder as intelligent. As a result, these sensor networks are easily exposed to the intruder, Therefore, the existing protocols and algorithms need to be reconsidered to be more robust and intelligent-intruder-resistant.

4. Hiding Sensor Networks

It is an interesting phenomenon that a sensor network is deployed to detect intruders but the intruder also scouts the sensor network for the purpose of anti-detection. Thus, the sensor network needs to be hidden from detection of intruders while retaining its functionality to detect intruders.

An intruder detects a sensor network by detecting sensing or communication signals. Many types of sensing, such as temperature, voice, or light, are passive and do not emit signals. Other sensors, such as ultrasound sensors, do emit a signal. In terms of hiding sensor networks, passive sensors are a wiser choice. In the situation where an active sensor must be used, we need to minimize the quantity and duration of emitted energy. The intruder's detector can also be passive or active. A sensor network can easily detect an intruder's active detector and hide from it. About communication signals, optical or electrical ones, a network using directional antennas limits its transmission area and has a better chance of being hidden from a potential intruder. However, Omni-directional antennas are most commonly used in today's wireless sensor networks.

In general, sensor network activity can be divided into three phases: *initialization, surveillance, and reporting*.

4.1. Initialization Phase

In the initialization phase when many activities are performed to configure and initialize a wireless network, communication signals can be particularly strong and therefore the sensor network can easily be scouted. There are two different strategies to hide sensor networks in its initialization phase: *slow initialization and fast initialization*.

With slow initialization, if the amount of messages is under control and the radiation level is low enough, the probability to be detected by an intruder can be reduced. On the other hand, fast initialization, despite its intensity, reduces the duration to complete initialization such that an intruder, at most, can only gain partial knowledge on the existence of a sensor network but not details about the number of sensor nodes, their distribution or capacity.

One approach for fast initialization is to divide all the sensors into single-hop clusters which can be self-initialized simultaneously. This method accelerates the initialization process. In the Parallel Initialization (PI) algorithm [9], ($\beta \log n$) Cluster-Head (CH) candidates are assigned before deployment, where n is the number of sensor nodes and β is the redundancy coefficient. After deployment, these CH candidates either organize into single-hop clusters by broadcasting their ID information, or become a cluster member (CM) by the abdication mechanism. When this procedure completes, each sensor knows whether it is a CH or CM, and each CM knows its connecting CH. Figure 1 shows a topology graph of a sensor network with n = 1000 generated by PI. In terms of initialization time, PI algorithm achieved a constant time independent of the size of sensor network n, and demonstrated a substantial improvement from other two related methods, CTP protocol (TinyOS2.0 standard) and the NoSE protocol [12].

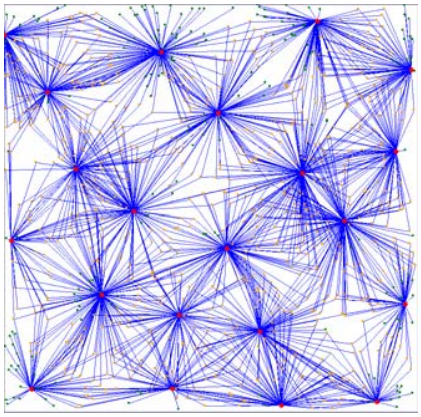

Figure 1. Sensor network topology generated by PI algorithm.

4.2 Surveillance Phase

The second phase, surveillance, is sometimes called the normal phase. For hiding communication signals, it is ideal to eliminate all communications. This is not practical in many situations because a minimal number of messages must be exchanged among sensor nodes to keep the network connected. For hiding sensing signals, activities and signal strength are minimized. Even with a low signal, it is still possible for a sensor network to be scouted since sensors have to periodically wake up for sensing and communication to retain their functionalities.

Normally, an intruder needs to scout the existence and location of every sensor node in order to make a decision. An interesting observation is that even if missing a small percentage of the sensor network information it may result in a fatal consequence for the intruder [20]. With the hundreds or thousands of nodes in a sensor network, it is inevitable for an intruder to overlook some of them. In addition, not all sensor nodes are equally important. Some of them are placed in more strategic locations and should be hidden away more frequently. Utilizing these characteristics, the sensor network can be designed to incorporate

different sleeping schedules for its sensor nodes to improve its hiding techniques during the surveillance phase. Thus, some sensor nodes with a high priority to be hidden can be selected to sleep longer, therefore, becoming invisible to intruders at a relatively long time period. This way, it will be hard for the intruder to obtain a complete picture of the sensor network and to make well-informed decisions.

We can go even further by hiding some sensor nodes completely from the intruder. A *latent* node is defined as a node that keeps silent until the reporting phase. Once it starts to report by sending messages, it turns back to a normal node. Thus, a latent node sends messages only when important information needs to be reported. When deploying such latent nodes, the sensor network must ensure their connectivity. That is, when a latent node is ready to report, it can connect to a normal node to forward its message to the destination.

4.3. Reporting Phase

When a sensor network in its surveillance state has detected a possible intruder, it should responsively report the information to the base station. The reporting phase could make the sensor network vulnerable to exposure, due to its increased signal strength resulted from intensive communication activities. Taking advantage, an intruder can throw a cobble onto the field on purpose just to trigger sensor network's reporting activities. An approach to confronting this strategy is *lazy reporting*, that is, the sensor network postpone the reporting for a time period. Though the principle of lazy reporting is simple, it is difficult to find out an appropriate delay time period. If it is too short, the sensor network may expose itself too soon. If it is too long, the sensor network could miss the opportunity to report an important event in time. It is a tradeoff to decide whether to report at the first sign of detection or to postpone reporting until the detection has been repeatedly confirmed.

Another method is to design a message routing algorithm to bypass the intruder. Upon the detection of intruders in sensor fields, sensor nodes can collaborate with each other to set up a perimeter in order to isolate the intruder based on an estimation of an intruder's probing intensity. The area inside the perimeter is considered the vulnerable area, and messages sent from one sensor node to the other bypassing this area to hide themselves from intruders and to prevent exposure of sensor nodes. Using directional communication will allow sensor nodes to further reduce the chance to be detected, providing more protection to sensor networks.

5. Enhancement of Detection Capability

Many techniques have been proposed to effectively track an intruder [4]. An intelligent intruder finds a best path to escape, that is, a path that has the lowest probability of being detected. Therefore, one possible approach is to block the best path. The current solution to finding the best path is to use the Voronoi diagram as shown in Figure 2 (a) [1], where each line segment maximizes the distance from the nearest sensor. Meguerdichian [11] has pointed out that the path of maximal breach of surveillance in the sensor field lies on the Voronoi diagram lines. Finding such a path requires the knowledge of the entire sensor network.

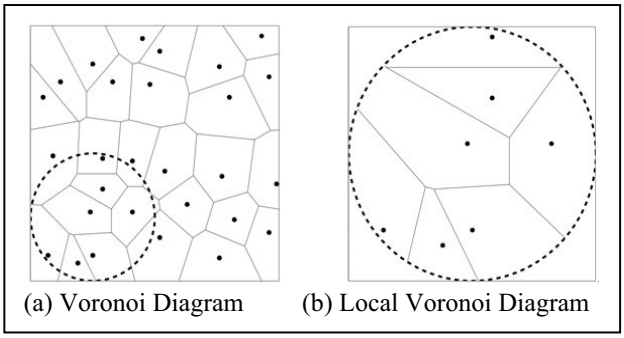

Figure 2. The Voronoi Diagrams.

An intelligent intruder, situated in a monitored region, is looking for the best path to traverse or escape. There are two basic criteria to evaluate the best path. First, the less the exposure, the better the path is. If the intruder can find and follow the path with the least exposure, it can escape from surveillance without being detected. Second, the shorter the path, the shorter the time to traverse and to be exposed.

Assume that all locations are at points of intersection and traversal is along lines of the diagram. If the current location of the intruder is S, and its final destination D, from S to D, there could be multiple paths available. With each single hop (or segment), from U to V, a traversal cost $C_{U,V}$ is defined as a product of its exposure $e_{U,V}$ and its length $l_{U,V}$. Assume that the intruder is situated at point W which has k neighbors, $Z_1, Z_2, \ldots Z_K$. If the intruder is moving towards neighbor Z_I, its associated traversal cost to its destination $C_{W,D}$ will be $C_{W,Zi}+C_{Zi,D}$. Therefore, the optimal path is determined by one of its neighbors Z_J such that $C_{W,Zi}+ C_{Zi,D}$ is smaller than or equal to that of any other neighbor Z_i. Following the optimal path is equivalent to selecting the next neighbor to traverse. If a global Voronoi diagram is available, the Dijkstra algorithm can be applied to find such an optimal path.

In practice, since an intruder has a limited detection range, it is not always possible to find an optimal path. Instead, it uses only local information to obtain an approximation of the best path. The intruder scouts the field and locates the sensors in its scope to obtain a *Local Voronoi Diagram (LVD)*, as shown in Figure 2(b). Note that the intersection points and lines in LVD and those in the corresponding part of the global Voronoi diagram are not necessarily identical. It is infeasible to recursively compute neighbor's traversal cost $C_{Zi,D}$ due to lack of global information. As an alternative, a geographic distance from point Z_i to destination D can be used as an approximation of the traversal cost. Thus, once a LVD_W is generated for the intruder's current location W, the next hop can be determined by choosing a neighbor. When the intruder arrives at Z_j, another LVD_{Zj} is generated, and so on. In some extreme cases, no neighbor is found in an intruder's scope, and the intruder can move directly towards the destination for a reasonable distance to regenerate a new LVD. One experiment shows that with local information, there are about 30% more exposure and 5.5% longer length than that with global information [19]. This approach can also be used for another interesting problem. Assume the intruder has the equipment to interfere or even destroy a single sensor node at a time, which sensor is to be the object? Each sensor node in LVD is evaluated for impact of this removal. The node will be selected such that its removal will result in a better path compared to removing any other node in LVD.

A sensor network is looking for ways to enhance its detection capability. Given characteristics of intruders, we could design smart algorithms to protect the sensor network by disabling the detection capabilities of the intruder. For example, an intelligent intruder is normally able to choose an optimal path of movement utilizing Voronoi Diagram in order to minimize its exposure. Such an optimal path can be blocked by deploying additional sensors [21]. Another interesting approach to enhancing detection capability of the sensor network is to configure a network topology such that in every detection range of the intruder, the optimal path calculated by the intruder's algorithm is as different as possible from the optimal path. An example is shown in Figure 3 where the dotted line is the best path while the solid line is the path found by the intruder using LVD.

This method can be further developed by hiding latent nodes. The intruder is then led onto a sub-optimal path due to lacking of complete information. We need to determine which sensors are more critical and should be hidden. The objective is to guide the intruder along a suboptimal path in order to maximize the detection probability. With the hiding technique, an intelligent intruder is unable to make a reliable decision. Assume that we have a few latent sensor nodes that can be placed in some location where the intruder passes through. As shown in Figure 4, if the sensor node in the small circle is hidden, the intruder will head to the right, and thus, be detected by the latent node. In contrast, a single sensor node can on purpose signal constantly to distract the intruder from scouting the rest of the field by capturing all of its attention. With these methods, we can increase the detection probability. Yet, the intruder could be smart enough to predict the behaviors of a smart sensor network and take action to confront it. Further study can apply game theory to explicate this dilemma; however, this is out of the scope of this article.

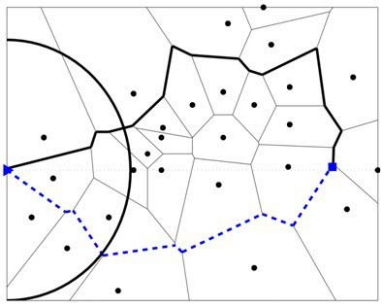

Figure 3. An example where an intruder does not choose the best path (dotted); and instead, takes an alternative sub-optimal path (solid) found by LVD.

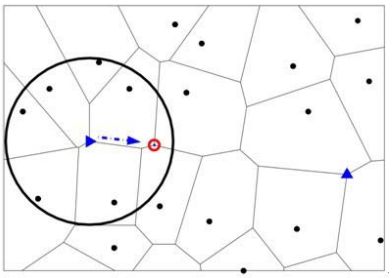

Figure 4. An example where the latent node in the small circle is hidden. The intruder will head to the right, and be detected by the latent node.

6. Recovery and Anti-interference Technology

An intruder can destroy or capture sensors in the field, disabling the sensor network. To ensure the functionality of a sensor network, protection is an important issue. Work in [15] addressed the self-protection problem using sensor nodes. Minimum p-

self-protection for a wireless sensor network is defined by two criteria. First, any wireless sensor node can be monitored by at least p active sensor nodes. Second, the number of active nodes in a sensor network is reduced. This is a NP-complete problem. Both centralized and distributed approximate solutions to minimum 1-self-protection are provided in [15]. Efficient, centralized and distributed approximate algorithms are designed for the minimum p-self-protection problem in sensor networks with heterogeneous or homogeneous sensing radius [14].

When a sensor network is attacked by an intruder, part of the network could be nonfunctional and unable to detect intruders, leaving a hole in the network. There are several approaches to recovering from sensor network failure. First, we can utilize the redundant sensor nodes, which are normally in the sleep state, and will wake up when they are called on to repair the network. Second, mobile sensors can be used for self-healing. This approach is particularly useful when all the sensors in the same area malfunction. A sensor network also needs anti-interference techniques to make itself robust against interference.

7. Conclusion

Countermeasure techniques for sensor networks look at the behaviors of both intelligent intruders and sensor networks. We discussed some issues and related techniques in this article. It can be viewed as the first step toward the development of the anti-sensornet or sensornet countermeasure technique.

Acknowledgement

The author would like to thank Jialiang Lu, Linghe Kong, Zhou Sha and Nicole Kwoh for their help and constructive comments. This research was partially supported by 973 Program of China under grant No.2006CB303000 and NSF of China under grant No.60773091.

References

[1]. F. Aurenhammer, “Voronoi diagrams - a survey of a fundamental geometric data structure.” ACM Comput., Surv., 23(3): 345-405, 1991.

[2]. K. Bicakci, C. Gamage, B. Crispo and A. Tanenbaum, “One-time sensors: A novel concept to mitigate node-capture attacks,” European Workshop: Security and Privacy in Ad-hoc & Sensor Networks, 2005.

[3]. P. Balister, Z. Zheng, S. Kumar and P. Sinha, “Trap Coverage: Allowing Coverage Holes of Bounded Diameter in Wireless Sensor Networks,” Infocom 2009.

[4]. C. Gui and P. Mohapatra, “Power conservation and quality of surveillance in target tracking sensor networks,” ACM MobiCom, Sep 2004.

[5]. D. Huang, M. Mehta, D. Medhi, and L. Harn, “Location-aware key management scheme for wireless sensor networks,” ACM workshop on Security of Ad Hoc and Sensor Networks, pp. 29–42, Oct 2004.

[6]. I. Karaaslan, “Anti-Sensor Network: Distortion-Based Distributed Attack in Wireless Sensor Networks,” M.Sc. Thesis, Dept of EEE, Middle East Technical University, Ankara, Turkey, 2008.

[7]. C. Kalor, N. Sastry, and D. Wagner, “TinySec: A link layer security architecture for wireless sensor networks,” Int’l Conf. on Embedded Networked Sensor Sys, 2004.

[8]. C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and counter-measures,” Ad Hoc Networks, Elsevier, pp. 293–315, 2003.

[9]. L.H. Kong, L. Fu, X. Liu and M.Y. Wu, “Accelerating Initialization for Sensor Networks,” IEEE Globecom, Dec 2009.

[10]. X. Y. Li, P-J. Wang and O. Frieder, “Coverage in wireless ad hoc sensor networks,” IEEE Transaction on Computers, 52(6):753-763, June 2003.

[11]. S. Meguerdichian, F. Koushanfar, G. Qu, and M. Potkonjak, “Exposure in wireless ad-hoc sensor networks,” ACM MobiCom, July 2001.

[12]. A. Meier, M. Weise, J. Beutel and L. Thiele, “NoSE: Neighbor Search and Link Estimation for a Fast and Energy Efficient Initialization of WSNs”, TIK-Report, No. 285, 2008.

[13]. D. Raymond, R. Marchany, M. Brownfield, and S. Midkiff, “Effects of denial of sleep attacks on wireless sensor network MAC protocols,” IEEE Workshop on Information Assurance, pp. 297–304, 2006.

[14]. Y. Wang, X. Y. Li and Q. Zhang, “Efficient Self Protection Algorithms for Static Wireless Sensor Networks,” IEEE Globecom, 2007.

[15]. D. Wang, Q. Zhang, and J. Liu, “Self-protection for wireless sensor networks,” IEEE ICDCS, 2006.

[16]. A. Wood, L. Fang, J. Stankovic, and T. He, “SIGF: A family of configurable, secure routing protocols for wireless sensor networks,” ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 35–48, Oct 2006.

[17]. A. Wood, J. Stankovic, and S. Son, “JAM: A jammed-area mapping service for sensor networks,” the 24th IEEE Int’l Real-Time Systems Sym., Dec 2003.

[18]. Z. Yang, E. Ekici, Dong Xuan, “A Localization-Based Anti-Sensor Network System,” Infocom 2007.

[19]. W. Zhang, M. Li, and M.Y. Wu, “Anti-detection: How does a target traverse a sensing field,” Int'l Conf. on Embedded Software and Systems (ICESS), Dec 2005

[20]. W. Zhang, M. Li, M.Y. Wu and W. Shu, “Smart Path-finding with Local Information in a Sensory Field,” Int’l Conf. on Mobile Ad-hoc & Sensor Networks, Dec 2006.

[21]. S. Zhou, M.Y. Wu and W. Shu,``Improving Mobile Target Detection on Randomly Deployed Sensor Networks," Int’l Journal of Sensor Networks, to appear.