Cyber-Physical Security for Wireless Sensor Networks

Position Paper

Gordon W. Skelton, PhD
Center for Defense Integrated Data (CDID)
Jackson State University
1230 Raymond Road Box 1200
Jackson, MS 39204
gskelton@c-did.com

Abstract

Cyber-Physical Security is an important topic that needs to properly address. Of particular concern is the field of wireless sensor networks which possess special characteristics that make them especially vulnerable to attacks and natural disasters. This position paper focuses on the critical issues and calls for directed research for finding solutions to these issues.

1. Introduction

Wireless sensor networks (WSNs) are comprised of numerous individual nodes capable of sensing, receiving and transmitting data. Each of the nodes may contain a variety of sensors capable of collecting essential data about the environment in which it is located. These nodes are often placed in remote/hazardous locations where maintenance and replacement of the individual nodes may present considerable risk for the individual. Furthermore, the isolated location of these nodes puts them in the position of easily being attached, damaged, captured or destroyed. In addition, the limited capacity of individual nodes prevents the use of traditional encryption and security measures.

2. Characteristics of Wireless Sensor Networks

Wireless sensor networks are composed of individual wireless nodes which contain the sensors, a microprocessor and the necessary transceiver to form the wireless network. A sink or base station is used to gather the data collected by the individual nodes and forwarded via the wireless network. The WSN is designed to be deployed in situations where data acquisition and decision support is to be continuous without the need for human intervention. This requirement of autonomy requires that WSNs must be robust, physically secure and resistant to tampering, both physically and wirelessly. Many of the commercially available nodes do not presently meet all of these requirements.

In addition to cyber-physical security, the available sensors are often quite limited. Sensors may be limited to light, humidity, temperature, GPS, vibration and acoustical which do not meet all of the needs of a simple security or monitoring system. Even, with these sensors, there is no means by which they can be easily protected to prevent the reporting of false or artificially generated data.

For most applications one must be able to protect the sensors, the data they are producing and the transmission of that data.

3. Threats to Wireless Sensor Networks

There are a number of different types of threats and attacks to WSNs. Such attacks include:

1) Physical attacks that can impact the coverage of the WSN and in many cases make the WSN inoperable [1]. Because of the widespread placement of the individual nodes in an often non-secure and unmonitored area, individual nodes are subject to capture. An invader can capture one or more nodes and learn crucial security information from the node itself. For instance, if a public/private key is being employed in creating a secure wireless sensor network, the private key may be acquired by interrogating the captured node. In addition, the captive node can be reprogrammed allowing it to provide counterfeit data or simply flooding the network with RTS which would eventually result in a denial of service by overwhelming the limited bandwidth of the wireless sensor network, thus preventing legitimate data from being transmitted by other nodes on the network.

2) Attacks against network layer - One means of attacking routing protocols is to simply introduce invalid routing information thus causing inconsistencies in routing and confusing the network.

Karlof and Wagner [2] examined the issues surrounding routing and wireless sensor networks. They classified the common types of network layer attacks. Table 1 lists those types of attacks:

Table 1 – Common attacks against network layer

Type of Attack	Description
Spoofed, altered, replayed information	May cause routing loops, repel network traffic, extend or shorten source routes, generate false error messages, partition network, increase end-to-end latency
Selective forwarding	Only forward certain messages, often attempts to explicitly include malicious node in the data flow
Sinkhole attack	Attract nearby network traffic through compromised node
Sybil attack	Single node presents multiple identities to the other nodes in a network, posing as a group of nodes
Wormholes	Create a 'low-latency out-of-bound' channel to different part of network allowing for messages to replayed
Hello flood attack	Protocol which requires 'hello' advertisement, can be use to announce counterfeit nodes so neighbors incorrectly trust them
Acknowledgement spoofing	If using an link-layer acknowledgement protocol acknowledgements can be created that cause other nodes to receive information about other nodes

Each of these different types of threats must be carefully analyzed and evaluated as to which type of countermeasure is best suited. As can be seen from the above discussion, one may have difficulty in finding a 'silver bullet' solution to the issues of cyber-physical threats to WSN security.

4. Method to Improve Physical Survivability

There are a number of means by which one can support the physical survivability of a WSN. [1] Each of the following techniques is addressed in the following sections of this paper. The techniques are:

1. Manual Battery/Node Replacement
2. Redundancy
3. Re-supply/Reseeding
4. Mobile Sensors for Fill-in
5. Battery Life Management/Extension
6. Rechargeable Power Supply (solar panels)

Manual Battery/Node Replacement

If the WSN is located in an easily accessed area, the number of sensors is less than X, and the critical nature of the WNS does not require the sensor field to

be active 24/7, then the individual batteries for each of the nodes can be replaced on a fixed schedule well before they begin to fail. Furthermore, any failed nodes can be replaced at that interval or as the network indicates that the nodes are not longer responding.

4.2 Redundancy

Over population of a sensor field is one approach to increasing the probability of survival of a WNS. In this scenario, calculations are used to determine the number of additional nodes required to maintain the life of the WSN for a given period of time. The additional sensors are then located throughout the sensor network at a predetermined interval.

4.3 Aerial Re-supply

One suggested means by which a WSN can be maintained for a longer period of time is through the use of aerial re-supply. In this scenario, a static WSN would report the loss of coverage to the sink. At that point, the request for re-supply would be issued. Using information from the WSN a map of the area would be constructed. This data is then fed to an onboard sensor distributor that controls the distribution of new sensor nodes. The airborne distribution vehicle could be either a UAV or a manned vehicle. In either case, the area of the sensor field which has either no live sensors or the number of living sensors falls below a predetermined threshold would be repopulated and the sensor field returned to an acceptable population level.

4.4 Mobile Sensor Fill-in

Collaboration among sensors has the benefit of providing verification before an external entity is alerted of a particular event. This collaboration, however, may require that more than one sensor be located at close proximity to the initial detection. For this reason one may choose to employ mobile devices which support neighboring sensors, thus creating a mobile wireless sensor.

An extension of the application of mobile sensors would be the use of these sensors to fill-in whenever a failure in the next work occurred. These sensors could either be deployed as reserve sensors waiting for their assignment to a particular location in the sensor field, or a whole sensor field could be mobile, thus allowing for the reconfiguration of the sensors whenever a failure of one or more sensors occurred.

4.5 Battery Life Management/Extension

A considerable amount of research has been directed toward solving the battery-life problem for WSNs. Recognized as a primary concern for wireless sensor networks, numerous efforts have been directed toward addressing the problem of battery life deterioration. Many different solutions have been proposed, each of which hopes to contribute to extending the life of the battery. From examining the breath of the research, it is recognized that there is no one solution to the problem. Research has focused on reducing the amount of time in which a single node is active in the WSN [3], [4]. By reducing the activities of a node and increasing the time that the node sleeps then the battery-life can be prolonged. In addition, research has examined different protocols that allow the node to sleep until it is needed to assist in routing and / or sensing.

Additional research, which goes beyond the question of battery longevity in WSNs, addresses the overall question of how to store more energy in a small package that could be employed in wireless devices, e.g. cell phones, PDAs, laptops. With the enhanced life of batteries used in these devices WSNs would also directly benefit. Intel has been actively involved in research on the extension of batteries for mobile devices.

The life of a battery, even in the present day, has a direct correlation with the amount of energy consumed. To extend the life of a battery without changing its fundamental composition one can simply reduce the amount of time the device operates. This principle is the fundamental basis for research on protocols used in WSNs. A number of different protocols have been suggested that assist in reducing transmission time for individual nodes. Sensing does consume energy; however, the move expensive operation, in terms of battery life, is transmission either in the form of data transmission from the node or as a router in the WSN.

4.6 Rechargeable Power Supply (solar panels)

Highly dependent upon the type of sensor being used in the WSN, solar panels can provide adequate power to an individual sensor to allow for extended life over that provided by a simple battery pack. Such

rechargeable sensors have been successfully deployed for environmental monitoring, particularly with stream and river gauges.

The most important piece of the wireless sensor network node is the energy storage device, usually a battery. Above all else, it is awareness of this finite energy reserve that drives the design of the system. Wireless energy scavenging devices can help stretch the energy reserve, but the length of any sensor network deployment envelope is ultimately shaped by the amount of energy available to the node. When the energy runs out, either the deployment is over or a person must be sent into the field to either replace the node or its batteries. If this occurs often then we might just send a person out to collect the data eliminate the WSN altogether.

A common solar panel can generate a 40mA 4.8 volt current. Even though this is not extremely efficient, it is able to provide the necessary energy required to maintain a wireless sensor node [5]. Solar panels can be used as a substitute for batteries; however, one will still have to include rechargeable batteries onboard the sensor node in order to support the operation of the sensor nodes during times that sunlight is not available. All of these requirements lead to increased individual node cost.

5. Other Potential Solutions

There are a number of suggested approaches that can be used in place of traditional encryption. One such approach uses dynamic routing [6]. This approach, along with other proposed ones, needs extensive testing in order to properly evaluate its effectiveness.

[7] proposes a framework of survivability model which adopts software rejuvenation methodology, which helps the wireless sensor networks to recover from a filed state (based on individual nodes) to a healthy state.

[8] proposes a general architecture for security and survivability in wireless sensor networks with heterogeneous sensor nodes and identifies metrics that quantify the performance of the network. The interaction between security and survivability for wireless sensor network is also addressed.

[9] suggests a holistic approach to security in WSNs. Their approach looks at various layers involved in the WSN from the application to the physical layer. Still, this approach does not address the simplistic threat to WSNs, destruction of the individual nodes.

Cyber-physical security for WSNs calls for the development of a set of requirements that addresses both the nature and construction of the nodes and the network, along with the architecture by which the data / control is transmitted wirelessly. For this reason, solutions may have to be layered, such as discussed in [2]. Even then, one must address the location of the individual nodes, the terrain in which they are deployed and the probability of the different threats identified for the particular deployment.

6. Conclusions

Standards for cyber-physical security for Wireless Sensor Networks must be developed and strictly adhered to by manufacturers of the different components of said systems. These standards may include the capability to support encryption and controlled access the data and the nodes themselves. Tamper proof nodes are essential the security of WSNs, particularly when they are being used for security and critical infrastructure protection. Such standards must be able to meet the requirements of the Department of Homeland Security, the Department of Defense and the Department of Energy where WSNs will play critical roles in daily operations.

Protocols must be developed that provide for long term survivability. Current research is being carried out; however, this research must be brought into the commercial design and deployment of WSNs in order to have a controlled environment in which one has a reasonable expectation of the life of individual nodes and the sensor network in general.

Research must be continued that will allow for the development of alternative emergency harvesting techniques that can be deployed in hostile environments thereby reducing the risk to individuals responsible for maintaining WSNs. This research should be coupled with ongoing research in battery life extension and reliability that is being carried out in other fields of endeavor.

7. References

[1] Skelton, G.W., Holton, A. *Survivability in Wireless Sensor Networks.* Proceedings of the IEEE SoutheastCon, 2006.

[2] C. Karlof and D. Wagner. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures., *Sensor Network Protocols and Applications (SNPA'03)*, May 2003

[3] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", Hawaiian Int'l Conf. on Systems Science, January 2000.

[4] K. Akkaya and M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County Baltimore, MD younis@csee.umbc.eduhttp://www.cs.umbc.edu/~kemal1/mypapers/Akkaya_Younis_JoAdHocRevised.pdf

[5] V. Raghunathan, A. Kansal, J. Hsu, J. Friedman, and M. Srivastava, "Design Considerations for Solar Energy Harvesting Wireless Embedded Systems", Networked and Embedded Systems Lab (NESL), Department of Electrical Engineering University of California, Los Angeles, CA

[6] Pathan A., Lee H., and Hong C. *Security in Wireless Sensor Networks: Issues and Challenges,* Proceedings of the ACACT 2006.

[7] Dong Seong Kim, Khaja Mohammad Shazzad, Jong Sou Park, A Framework of Survivability Model for Wireless Sensor Network, Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)

[8] Yi Qian, Kejie Lu and David Tipper, Towards Survivable and Secure Wireless Sensor Networks, Performance, Computing, and Communications Conference, 2007. IPCCC 2007. IEEE InternationalKlonowski,

[9] Klonowski, M. and Kutylowsi, M. *Security Challenges for Wireless Sensor Networks – Dynamic Routing as a Security Paradigm,* ERCIM News, http://ercim-news.ercim.org/content/view/517/705/