Autonomous Defenses for Security Attacks in Pervasive CPS Infrastructure

Anthony D. Wood, Vijay Srinivasan, and John A. Stankovic
Department of Computer Science
University of Virginia
{wood | vs8h | stankovic}@cs.virginia.edu

1. Introduction

Cyber-physical systems (CPS) integrate computation with sensing, control, and physical systems and will enable development of next-generation services and smart infrastructure across many application domains. However, a significant impediment to the use of CPS in trusted and *trustworthy* systems is their vulnerability to security attacks.

Some properties of CPS that exacerbate security concerns are intrinsic to the systems, and so cannot be deferred for later reconciliation with an already functional system. First, risk of security threats grows with the value and criticality of the assets under control of the CPS. Second, an open, distributed, pervasive system has a large attack surface because it is easily accessible by attackers. These concerns are exacerbated by the long lifetimes of CPS that guarantee the evolution of unforeseen attacks after the systems are fielded. Finally, as a platform for CPS, wireless sensor networks (WSN) also have resource constraints that increase asymmetries between the system and its attackers.

In this article, we first describe examples of active and passive attacks on CPS security and then propose design requirements and solution approaches based on results from our previous work. We argue that trustworthy CPS must be designed for robustness using autonomous defenses, clusters of solutions, and the right mix of randomization and regularization to allow continued operation despite unforeseen attacks.

2. Security and Privacy Attacks

Active and passive attacks may be perpetrated at all levels of CPS, including physical, network, and application layers [3]. At the lowest layers, wireless networks rely on a shared communication medium, which is vulnerable to denial of service attacks from jamming [5]. A successful attack at this level disrupts the operation of all layers above, even if they employ adequate methods for ensuring the classical security properties. Results have shown that even a single compromised (re-programmed) network node can cause significant disruption at low cost in energy to the attacker.

Without interference from jamming, network communication may be functional yet subjected to passive overhearing-based attacks that exploit physical properties of the system to violate security [1]. Our study of several residential sensor networks showed that even assuming encrypted undecipherable radio messages, an eavesdropper can use inference techniques to infer a person's current activity and daily habits, by snooping on just wireless fingerprints and transmission timestamps.

An active attacker may further attempt to manipulate message routing and network coordination by injecting messages, replaying old ones, or slicing protocol interactions [2]. These attacks can render the network inoperative, shorten their lifetime, or be used as a platform for further attacks.

Addressing these and other attacks while meeting functional objectives and satisfying platform constraints is a key research challenge for CPS.

3. CPS Design Requirements for Security

Our solutions for the above attacks have suggested five key properties or goals of CPS design that improve robustness: containment, continuity, adaptivity, robustness, and efficiency.

3.1. Decentralized protocols are needed to *contain the damage* from attacks.

In a large-scale system that is openly accessible, multiple attacks may be ongoing continually in various parts of the system. Without some isolation or containment of the impact of the attacks, the entire network may be unreliable or unavailable. It is not feasible in large-scale CPS to "reboot" the system to recover from attacks; rather, the system must contain attacks so that other parts of the system are relatively

unaffected. Decentralized protocols that limit dependences on other nodes are part of an effective defense.

For example, in the DEEJAM protocol for defeating jamming [4,5], network transmission schedules are computed by every node for its neighbors, and links are isolated to avoid selective link jamming attacks. In the SIGF routing protocol [2], attacks are contained to the one- or two-hop neighborhood around an attacker by allowing every node to make routing decisions independently. All the parts of our FATS solution suite [1], such as adding random delays to messages, radio signal attenuation, fingerprint masking and enforcing periodic transmissions, are applied on individual nodes in the network. Thus, even if the adversary takes control of nodes from one part of the network she still cannot infer useful information from other areas.

3.2. Network services must *continue to operate* despite active attackers.

In addition to containing attackers spatially so that nodes elsewhere are minimally affected, reliability and security will be improved if even nodes that are close to the attackers can also continue to operate, albeit with reduced capability.

A design principle that DEEJAM and SIGF have used to good effect in this regard is to incorporate *non-determinism* in the protocols. Neighboring nodes in DEEJAM compute random idle listen schedules known only to the pair of communicating neighbors. This provides the primary defense against selective link jamming, because a compromised neighbor obtains no information about its neighbors' links with other nodes. In SIGF, random selection of forwarding candidates is a core part of the algorithm, and ensures continued operation that is gradually degraded as more nodes are compromised.

3.3. *Adaptive mechanisms* are needed to react to network, attack, and application variability.

Often a particular trade-off is selected at design time that will not be appropriate at all times in the lifetime of the system. Protocol families, design-time reconfigurability, design for extensibility, and automatic and managed runtime adaptation are all beneficial for overcoming this limitation, and should be reflected in the design of CPS.

DEEJAM and SIGF both incorporate feedback loops to enhance their robustness. DEEJAM monitors the packet loss on the channel to control termination of its fountain-code-based fragmentation scheme. SIGF uses a reputation mechanism to penalize the bad behavior of neighbors by weighting the random forwarding candidate selection. These parameters cannot be chosen optimally at design or deployment time because they depend on transient channel conditions as well as whether attackers are present at runtime. Similarly, each of our FATS solutions varies in terms of applicability to particular sensors or scenarios, real-time characteristics, device capabilities and cost. By analyzing these tradeoffs and using a hybrid approach, we provide system designers the option of dynamically adapting and combining solutions based on various constraints.

3.4. Solutions must be *robust to faults* from attacks and the environment.

As a result of significant resource constraints in many CPS, some attacks cannot be prevented and will degrade performance or interrupt service. Taken together with the dynamics and unpredictability of environmental embedment, these pose challenges for the fault-tolerance of CPS. Traditional fault tolerance techniques often assume independence of faults and must be carefully considered to see whether they deter malicious attackers.

SIGF builds upon the earlier work of Implicit Geographic Forwarding (IGF), which specifies a collaborative next-hop selection mechanism that was shown to be quite efficient and robust to node failures and mobility. However, because it relies on neighbor cooperation it is easily attacked by a malicious node. In SIGF we layered additional defenses to reject this and other attacks while preserving high performance.

3.5. Security designs and mechanisms must be *efficient* to satisfy resource constraints.

Resource limitations are a central constraint of many CPS, with lifetime, form factor, and cost all placing pressure on the computational and memory capabilities of devices. Trade-offs among these constraints are application specific, but for most applications security is *not the only priority* and efficient designs are mandatory.

Often, protocols designed to satisfy mainly security goals are too heavyweight for frequent use on low-end devices. For example, we found that some of our FATS solutions, such as enforcing periodic transmissions, were more feasible and effective on simple, binary sensors in certain locations, while using small random delays were more effective in hiding other activities cheaply. Combining several of our solutions in a hybrid fashion provided higher security with significantly lower costs than applying a single solution to the entire system.

When designing SIGF, we defined a family of three protocols that layer atop one another. The most efficient uses primarily non-determinism as a defense, but cannot resist certain attacks. To it we added a locally-kept reputation to improve its security. The last member of the family uses cryptographic operations to strongly defend against most attacks—at the added expense of sharing and maintaining more state with neighbors. In this way, SIGF can be adaptively tuned "in the field" to provide more or less security in response to an estimate of the current threat, and maintain as much efficiency as possible.

4. Conclusion

WSN can serve as a flexible, ubiquitous and easily deployable platform for CPS applications such as homeland defense, infrastructure protection, surveillance and healthcare. Problems that must be overcome include the limited capacity of these devices and the openness due to wireless communication. Attacks such as jamming and overhearing combined with sophisticated inference can render these systems ineffective. Proposed security solutions must be lightweight, operate in the presence of attacks, utilize the inherent redundancy and thwart adversary inference techniques. Solutions found in our DEEJAM, SIGF and FATS work begin to address these issues in a comprehensive manner.

5. References

[1] V. Srinivasan, J. Stankovic, and K. Whitehouse, "Protecting your daily in-home activity information from a wireless snooping attack," in *Proceedings of the 10th international Conference on Ubiquitous Computing (UbiComp '08)*, Seoul, Korea, September, 2008.

[2] Anthony D. Wood, Lei Fang, John A. Stankovic, Tian He, "SIGF: A Family of Configurable, Secure Routing Protocols for Wireless Sensor Networks," in *The Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2006)*, Alexandria, VA, October, 2006.

[3] Anthony D. Wood, John A. Stankovic, "Denial of Service in Sensor Networks," in *IEEE Computer*, 35(10):54-62, October 2002.

[4] Anthony D. Wood, John A. Stankovic, "Online Coding for Reliable Data Transfer in Lossy Wireless Sensor Networks," in *The 5th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS '09)*, Marina Del Rey, CA, June 2009.

[5] Anthony D. Wood, John A. Stankovic, Gang Zhou, "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks," in *The 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, San Diego, CA, June 2007.