Sensor Networks and Security Issues

Dr. Virender Khurana
Senior Lecturer,
Vaish College of Engineering, Rohtak
Email: drvkkhurana@gmail.com

Abstract

In this paper we give an overview of the security issues in sensor networks. First we present the limitations of sensor networks that make security for such networks hard, but also their unique characteristics that can be exploited to fact model and discuss the requirements that a security protocol has to meet. Following that, we take a first step toward establishing a comprehensive set of security challenges for sensor networks. This overview helps identify research challenges and sets the security in sensor networks scene.

Introduction

The designs of many sensor network applications or protocols for lower layers assume that all nodes are cooperative and trustworthy. This is not the case, in most cases of real-world deployments, where the nodes are exposed to many threats that can severely damage the proper network functionality. There are many attacks designed to exploit the unreliable communication channels and the unattended sensor nodes. Most sensor networks actively monitor their surroundings, and it is often easy to deduce information other than the data monitored. Such information leakage often results in loss of privacy for the people in the environment. Moreover, the wireless communication employed by sensor networks facilitates eaves-dropping and packet injection by an adversary. The combination of these factors demands security for sensor networks to ensure operation safety, secrecy of sensitive data and privacy for people in sensor environments. Nevertheless, sensor networks cannot rely on human intervention to face an adversary's attempt to compromise the network or hinder its proper operation. Neither can they employ existing security mechanisms such as public key infrastructures that are computationally expensive. Instead, an autonomic response of the network that relies on the embedded pre-programmed policies and a coordinated, cooperative behavior is the most effective way to gain

maximum advantage against adversaries

Obstacles to Sensor Network Security

Although wireless sensor networks have an ad-hoc nature, there are several limitations that make security mechanisms proposed for ad-hoc networks not applicable in this setting. In particular, security in sensor networks is complicated by more constrained resources and the need for large-scale deployments. A summary of these limitations follows below:

Constrained Hardware

A wide range of sensor node platforms has emerged over the past five years. So far, for such devices, the trend has been to increase the lifetime of the nodes by decreasing the resources such as memory, CPU, and radio bandwidth. Therefore, motes have tiny resources, on the order of a few kilobytes of RAM and a few megahertz of processor. For example, The resources available by some popular mote platforms, like Mica2 developed by UC Berkeley in collaboration with the Crossbow corporation, or the BT node family from ETH Zurich. Establishing secure communication between sensor nodes becomes a challenging task, given these limited resources, as well as the lack of control of the wireless communication medium. Public-key algorithms, such as RSA or Differ Hellmann key agreement are undesirable, as they are computationally expensive. Instead, symmetric encryption /decryption algorithms and hash functions are between two to four orders of magnitude faster and constitute the basic tools for securing sensor network communications. However, symmetric key cryptography is not as versatile as public key cryptography, which complicates the design of secure application

Wireless Communication

Sensor nodes communicate through wireless communication, which is particularly expensive from an energy point of view (one bit transmitted is equivalent to about a thousand CPU operations). Hence one cannot use complicated protocols that involve the exchange of a large number of messages. Additionally, the nature of communication makes it particularly easy to eavesdrop, inject malicious messages into the wireless network or even hinder communications entirely using radio jamming.

Exposure to Physical Attacks

Unlike traditional networks, sensor nodes are often deployed in areas accessible by an attacker, presenting the added risk of physical attacks that can expose their cryptographic material or modify their underlying code. This problem is imagined further by the fact that sensor nodes cannot be made tamper-resistant due to increases in hardware cost. Therefore, sensor nodes are more likely to suffer a physical attack in such an environment compared to typical PCs, which are located in a secure place and mainly face attacks from a network.

Large Scale Deployment

Future sensor networks will have hundreds to thousands of nodes so it is clear that scalability is a prerequisite for any attempt in securing sensor networks. Security algorithms or protocols that were not designed with scalability in mind offer little or no practical value to sensor network security.

Aggregation Processing

An effective technique to extend sensor network lifetime is to limit the amount of data sent back to reporting nodes since this reduces communication overhead. However, this cannot be done unless intermediate sensor nodes have access to the exchanged data to perform data fusion processing. End-to-end confidentiality should therefore be avoided as it hinders aggregation by intermediate nodes and complicates the design of energy-aware protocols.

New Opportunities

Even though the unique characteristics of sensor networks pose some new challenges in security, they also lead to some new opportunities for designing secure protocols and open the door for an entirely new security paradigm. The same properties that allow an attacker to intrude into a sensor network can be used as defenses mechanisms, if exploited properly. Below we outline some of these characteristics from the security architect point of view.

Broadcast Communication

As we saw an attacker can take advantage of the wireless medium and broadcast communication

of sensor nodes for intercepting or jamming transmitted packets. In the same way, legitimate nodes can eavesdrop on the traffic passing through their neighborhood. This can constitute a powerful monitoring mechanism for suspicious or abnormal behaviors and lead to the detection of an intruder node.

Massive Redundancy

Sensor nodes are typically low-cost devices allowing sensor networks to pose large scale and massive redundancy. Due to these characteristics the loss or corruption of a sensor node can either be mitigated by redundant sensors or tolerated. Therefore, it is possible to device security protocols that tolerate failures and work correctly even if up to out of nodes are compromised byte attacker. Also, in case that the network becomes aware of the intrusion, it can restore its proper operation by using redundant information distributed in other parts of the network.

Sensors as Routers

All sensor nodes act as routers of information toward the base station, in contrast to traditional networks which are based on specific traffic concentration points. Therefore, in sensor networks traffic is distributed for load balancing purposes and it is impossible for an attacker to monitor or control it at certain points. This considerably increases the effort that she has to make, but it also allows the network to reconfigure itself easily in case of node compromises, by setting up alternative paths.

Threat Models

In sensor networks security, an attacker can perform a wide variety of attacks. Not all of them have the same goal or motivations. So, in order to plan and design better defense systems, we formulate a threat model that distinguishes between two types of attacks: outsider attacks and insider attacks. We now treat each one of these classes in turn.

Outsider Attacks

In an outsider attack (intruder node attack), the attacker node is not an authorized participant of the sensor network. Authentication and encryption techniques prevent such an attacker to gain

any special access to the sensor network. The intruder node can only be used to launch passive attacks, like.

Insider Attacks

Perhaps more dangerous from a security point of view is an insider attack, where an adversary by physically capturing a node and reading its memory, can obtain its key material and forge node messages. Having access to legitimate keys, the attacker can launch several kinds of attacks without easily being detected False data injection (stealthy attack): the attacker injects false aggregation results, which are significantly different from the true results determined by the measured value Selective reporting: the attacker stalls the reports of events that do happen, by dropping legitimate packets that pass through the compromised node. Of course, an adversary cannot have unlimited capabilities. There is some cost associated with capturing, reverse-engineering and controlling a node. Therefore, we should assume that the adversary can compromise only a limited number of sensor nodes. This fact the design of security protocols, as it is easier to offer some protection against a few compromised nodes, but not for the case where a large portion of the network is in control of the attacker.

Routing Attacks against Sensor Networks

The goal of an attacker, being insider or outsider, is to manipulate user data directly or trying to affect the underlying routing topology. What makes it even easier for her is the fact that most protocols for sensor networks are not designed having security threats in mind. As a consequence, deployments of sensor networks rarely include security protection and little or no effort is usually required from the side of the attacker to perform the attack. We mentioned some simple attacks in the previous section. However, there are more sophisticated attacks that exploit specific characteristics of the routing protocols in order effect the topology and gain access to the routed information. These attacks are described analytically by Karl of and Wagner .

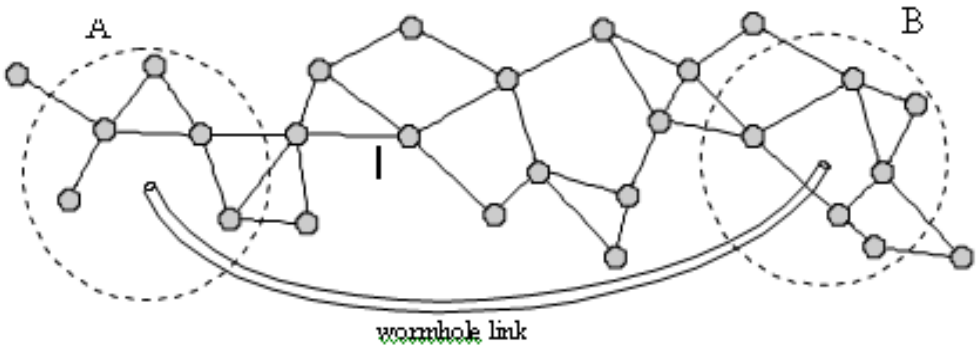

Figure 2.1 : A wormhole attack between two points in the network.

The Sinkhole Attack

The sinkhole attack is a particularly severe attack that prevents the base station from obtaining complete and correct sensing data, thus forming a serious threat to higher-layer applications. In a sinkhole attack, a compromised node tries to draw all or as much traffic as possible from a particular area, by making it look attractive to the surrounding nodes with respect to the routing metric. As a result, the adversary manages to attract all traffic that is destined to the base station. By taking part in the routing process, she can then launch more severe attacks, like selective forwarding, modifying or even dropping the packets coming through. Recently we identified several vulnerabilities of two popular routing protocols of sensor networks, namely the Mint Route and the Multi Hop, and showed how they can be exploited by an attacker to launch a sinkhole attack. It turns out that it is very easy for her to make the compromised node looks attractive to its neighbors or make them look less attractive and eventually make all nodes choose that node as their new parent.

The Wormhole Attack

The wormhole attack is a severe threat against packet routing in sensor networks that is particularly challenging to detect and prevent. To launch such an attack, an adversary establishes a low-latency link, referred as a wormhole link, between two points of the network, as shown in the operational, the adversary eavesdrops messages at one end and tunnels them (possibly selectively) to the other end, where the packets are retransmitted. The low-latency link used in

this attack as well as any devices attached at each end of the link belong only to the attacker and are not compromised resources of the network. The link is realized in such a way that packets can travel from one end to the other faster than they would normally do via a multi-hop route in the network. The sensor nodes cannot detect the existence of such a link, as it can be realized with other means, such as a wired connection or an out-of-band wireless transmission. As shown in the example of Figure, the net effect of the wormhole attack at the nodes within region think they are neighbors with the nodes within region B and vice versa. If the attacker carefully chooses the place of the wormhole's end-points then it can use it to completely disrupt routing and attract a significant amount of traffic. So, if one end of the wormhole is close to the base station then nodes situated multiple hops away could be convinced that they are only one or two hops away. As a result, these nodes will choose to use the high-quality link for their transmission enabling other kind of attacks such as the sinkhole attack.

The Sybil Attack

A Sybil attack is one in which an attacker uses a malicious device to create a large number of pseudonymous entities, using them to gain a disproportionately large influence. We refer to a malicious device's additional identities as Sybil nodes. Newsome introduce taxonomy of the different forms of the Sybil attack in sensor networks. In terms of communication, Sybil nodes can communicate directly or indirectly with legitimate nodes. In the latter case, legitimate nodes are able to communicate with the Sybil nodes through the malicious device, which claims to be able to reach the Sybil nodes. Moreover, the malicious device can fabricate a new identity for a Sybil node, or it can steal an identity from a legitimate node. Finally, in terms of time, the attacker may try to have the Sybil identities participate in the network all at once or present a large number of identities over a period of time, while only acting as a smaller number of identities at any given time. Sybil attack can be used against many protocols in sensor networks. In multi path routing, seemingly disjoint paths could in fact go through a single malicious node presenting several Sybil identities. If a geographic routing protocol is used a Sybil node could appear in more than one place at once, instead of having one set of coordinates. In-network processing is also susceptible to Sybil attack. An attacker can affect aggregation results of sensor readings by contributing to the operation many times. In the same way, she can affect a voting process amongst sensor nodes and make the system come to wrong conclusions. Therefore, Sybil

attacks can pose a significant threat to the normal operation of a sensor network.

The HELLO Flood Attack

Many WSN protocols require nodes to broadcast HELLO packets for neighbor discovery purposes. After just a few messages have been exchanged, most nodes have a complete picture of their immediate vicinity and a routing topology logically forms in a self-organizing fashion. However, if a laptop-class attack broadcasts such packets with large enough transmission power; she could convince every node in the network that the adversary is its neighbor and advertise attractive routing pathways through itself. After convincing portions of the network that it is truly the best routing option, it might choose to ignore incoming messages, effectively disabling large portions or even the entire network. Unlike the rest of attacks we described so far, the HELLO flood attack does not require an attacking node to create legitimate traffic to be successful. So, for example, even an outsider attacker can capture legitimate "HELLO" messages as they breezed through the air and then forward them with a more powerful antenna. Those messages would reach other nodes well beyond the actual reach of a real sensor node's hardware. It's easy to see that this forwarding and redistribution leads to false network topologies and bogus routing information.

Conclusion

In this paper we have presented an overview of current research challenges on sensor networks security. While addressing the challenges presented in this chapter may protect sensor networks from specific threats, what has been lacking is a holistic approach that encompasses autonomic responses over a broad range of attacks. A research challenge therefore, would be the design of an adaptive security architecture that can monitor the sensor network, recognize a security threat and respond by a coordinated self-healing mechanism. Investigate the approach and describe an intrusion detection system that can offer opportunities for increasing sensor networks security and guaranteeing a robust and survivable solution.

References

[Aga06] A. Agah, M. Asadi, and S. K. Das. Prevention of DoS attack in sensor networks using repeated game theory. In ICWN '06: Proceedings of the 2006 International Conference on Wireless Networks, pp. 29–36.2006.

[Ami08] S. O. Amin, M. S. Siddiqui, and C. S. Hong. Detecting jamming attacks in ubiquitous sensor networks. In SAS '08: Proceedings of the IEEE Sensors Applications Symposium, pp. 40–45. 2008.

[Bec06] A. Becher, Z. Benenson, and M. Dornseif. Tampering with motes: Real-world physical attacks on wireless sensor networks. In SPC '06: Proceeding of the 3rd International Conference on Security in Pervasive Computing, vol. 3934 of Lecture Notes in Computer Science, pp. 104–118. Springer, 2006.

[Gu08] Q. Gu and R. Noorani. Towards self-propagate mal-packets in sensor networks. In Wise c '08: Proceedings of the first ACM conference on Wireless network security, pp. 172–182. ACM, New York, NY, USA, 2008.

[Ham06] A. Hamid, Mamun-Or-Rashid, and C. S. Hong. Routing security in sensor network: HELLO flood attack and defence. In ICNEWS '06: Proceedings of the First International Conference on Next-Generation Wireless Systems, pp. 77–81. 2006.

[Har05] C. Hartung, J. Balasalle, and R. Han. Node compromise in sensor networks: The need for secure systems. Technical Report CU-CS-990- 05, Department of Computer Science, University of Colorado, 2005.

[Kro07c] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos. Intrusion detection of sinkhole attacks in wireless sensor networks. In M. Kutylowski, J. Cichon, and P. Kubiak, editors, Algorithmic Aspects of Wireless Sensor Networks – ALGOSENSORS, vol. 4837 of Lecture Notes in Computer Science, pp. 150–161. Springer, 2007.

[Kro08a] I. Krontiris and T. Dimitriou. Launching a sinkhole attack in wireless sensor networks; the intruder side. In First International Workshop on Security and Privacy in Wireless and Mobile Computing, Networking and Communications. Avignon, France, October 2008.

[Kro08b] I. Krontiris and T. Dimitriou. Security issues in biomedical sensor networks. In First International Symposium on Applied Sciences in Bio-Medical and Communication Technologies (ISABEL '08). Aalborg, Denmark, October 2008.

[Kul05] S. S. Kulkarni and L. Wang. MNP: Multihop network reprogramming service for sensor

networks. In Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), pp.7–16. 2005.