Vulnerability Assessment in the Smart Farming Infrastructure through Cyberattacks

Sebastian Linsner[1], Rashmi Varma[1] and Christian Reuter[1]

Abstract: The Internet of Things (IoT) has a significant impact on agriculture. So-called Smart Farming uses drones and a variety of sensors to measure climate, irrigation, soil moisture or GPS position. With this rapid influx of technology increases the threat that vulnerabilities in those technologies are being exploited for malicious intent. To show the impact of cyberattacks on agriculture, we present a simulation of several attacks on a ZigBee-based wireless sensor network. We conduct a delay attack, an interference attack and three different routing attacks (sinkhole, blackhole and selective forwarding attack). Those attacks are simulated using NETA with the OMNET++ framework. We will show that the security of WSN is influenced by factors like energy consumption or computation power, which can conflict with other interests like low per-unit costs.

Keywords: Smart Farming; Precision Agriculture; Vulnerability Assessment; Internet of Things; Wireless Sensor Network

1 Introduction

Facing the growth of the world's population, the production of food needs to be optimized. One promising approach is called Precision Agriculture or Smart Farming (SF). SF is the use of IT with agricultural principles, taking spatial and temporal variability into account through data collection in the agricultural production process. The collected data helps to minimize potential production risks emerging from environmental parameters and human actions, contributing to create adequate conditions for sustainable agriculture. In line with our vision of resilient smart farming [Re19, Re18], this paper investigates the impact of Wireless Sensor Networks (WSN) on agriculture and which risks arise from vulnerabilities in this technology. Therefore, the central research question is: *Why should farmers invest in security when using WSN?*

WSN provide detailed information about relevant factors for crop growth and health. Sensor nodes can measure the moisture and structure of the ground, evaluate leaf color or detect parasites. This allows farmers to plan agricultural processes like irrigation or fertilization more precisely and increase the yield of their farms. However, these processes rely on the correctness of the aggregated data. Therefore, the security of WSN is crucial for effective Smart Farming. To demonstrate this, attacks are simulated and their consequences on agriculture are highlighted.

[1] Technische Universität Darmstadt, Science and Technology for Peace and Security (PEASEC), [linsner|reuter]@peasec.tu-darmstadt.de; www.peasec.de

2 Background

In the context of agriculture, several requirements of WSN are even more crucial than in other IoT-related contexts. A WSN deployed in the fields of a farm needs to provide a sufficient coverage of the whole area. The nodes should be placed in a way that provides resilience towards the failing of single sensors. This leads to increased costs for farmers. Therefore, the nodes should be designed in a way that ensures a long lifetime to prevent additional costs. One criterion for this is low energy consumption: the battery-powered nodes should use energy efficient algorithms and a low communication range to ensure a longer lifespan.

Further requirements arise from the context of smart farming: all data should be available in real-time because crops are very sensitive to environmental influences. An example for this is irrigation: too intense or too spare irrigation results in lower crop quality or the loss of the whole harvest, while optimal irrigation reduces the wastage of water and energy. One problem arising from that requirement is the propagation loss of sensor data due to crop density. A dense vegetation can interrupt the radio signals and lead to packet loss. This must be modeled with adequate loss models [Le06, Ra16]. A more serious problem in this context is the threat of attacks [Lu09]. If an attacker is able to manipulate the sensor data or the network traffic, the crops could be destroyed. This is not only a monetary loss for the farmer but also a threat for society if those attacks are conducted on a large scale. Therefore, it is necessary to expand the security research on WSN further into the domain of agriculture and point out consequences of cyber attacks.

The requirements listed above can stand in conflict with each other. For example, the need for low energy consumption conflicts with security. The wireless traffic can easily be monitored if it is not encrypted. The process of encryption improves security but reduces the battery lifespan. Therefore, hardware manufacturers have to make compromises regarding different requirements. Using the example of the ZigBee-Protocol [ZA12], we show that insecure settings can lead to serious vulnerabilities. If ZigBee is operated in standard security mode, an attacker can insert malicious nodes after eavesdropping the network-key, which is transferred in plaintext over the network. This can be achieved with tools like KillerBee [Wr09]. Even more dangerous is physical access to the nodes. An attacker can extract software and secret keys stored in the hardware [Wa05]. This scenario is very likely in the context of agriculture because the nodes are installed on the fields and the standard key delivered with the firmware is often not changed. Those vulnerabilities are considered for the simulation of attacks in section 3.

The following is assumed for the simulation: the attacker can exploit the vulnerabilities stated above. By eavesdropping the network-key, a malicious node can be inserted into the network. The attacker has physical access to the devices in the field and is able to steal keys and compromise the software. The device of the attacker has more computation power than the nodes in the network and has no constraint regarding energy.

Three metrics are considered as relevant: The **throughput** describes the ratio of successfully received packages in relation to the number of sent packages in the network. The **end-to-end delay** is the time that one package needs to reach the destination after it is sent. This is a very crucial metric because of the real-time requirement of WSN in agriculture. Therefore, packages must reach their destination before the pre-defined timeout or the package will be resent. The third metric that is considered is the **power consumption**. This describes the amount of power needed by a node to process and forward a package to the destination. As stated above, this amount must be very low to ensure a long lifespan of the node.

To conduct the attack two tools were used: OMNET++ is an open-source framework to simulate networks. On top of that, NETA was used to simulate network attacks. NETA extends the OMNET++ data structures, enabling the definition of compromised nodes.

3 Simulation of Attacks

The simulation is based on two different scenarios. First, we consider a star topology. All nodes communicate directly with the network controller. The nodes send packages every 30 seconds before entering sleep mode to reduce energy consumption. This setup is used for the delay attack and the interference attack. For the routing attacks, we use a mesh topology with six sensor nodes to simulate package propagation in the network.

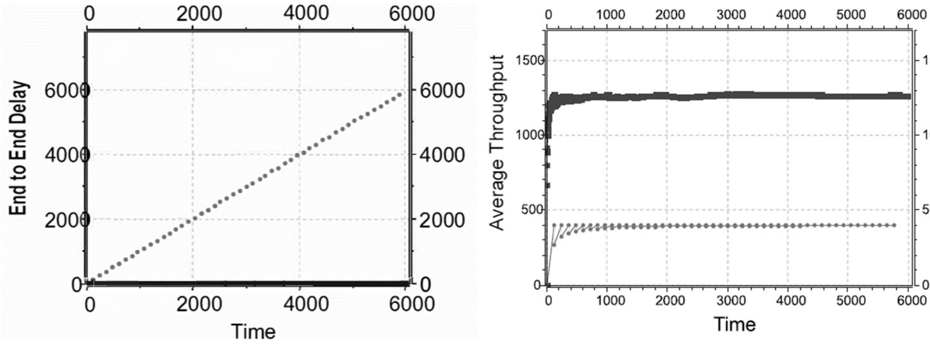

Fig. 1: Results of the Delay Attack: on the left: the end-to-end delay of the packages. On the right: throughput of the WSN in the baseline condition (black curve) and under attack (gray curve)

Attacks on the Star Topology. *Delay Attack:* during the simulation, it was assumed that the attacker was able to capture the controller of the WSN and is delaying every packet routed through it by 60 seconds. Due to the fact that packets are considered as lost after retransmitting them thrice, the congestion in the buffer of the controller leads to packet loss. Therefore, the throughput decreased rapidly to about one-third of the baseline throughput, while the end-to-end delay increased linearly over time (see Fig. 1). This attack can lead to the malfunction of the whole system: required sensor data is not available, and control signals get lost. In the context of Smart Farming, the wrong setup of machines poses a threat to the crops.

Interference Attack: similar to the Delay Attack, we assume that the controller of the network has been captured by the attacker. The interference attack is conducted by flooding the network with irrelevant packages so that data from the nodes in the field will be dropped due to network overload. The higher computation power compared to the nodes allows the attacker to keep the communication channel busy. Besides the threats resulting from data loss, another negative effect occurs: due to the traffic overhead in the network, the energy consumption increases. This can cause a shorter lifespan of agricultural nodes and therefore increased costs for farmers.

The delay attack and the interference attack allow the attacker to drop packages randomly. Specific attacks on target devices can be conducted with routing attacks [MAJ11].

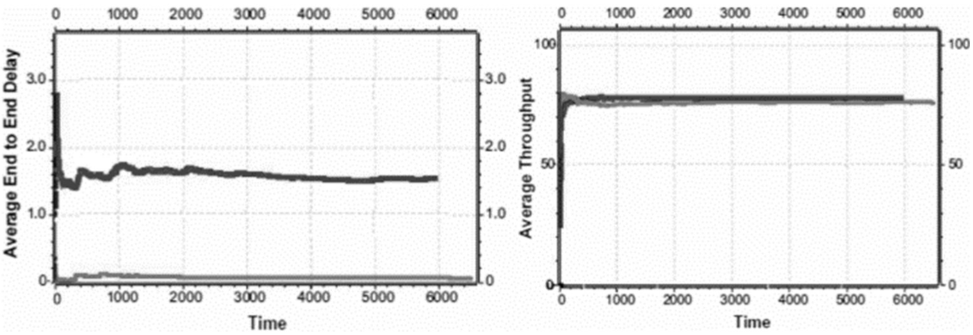

Fig. 2: Results of the Sinkhole Attack: on the left: the end-to-end delay of the packages in the baseline condition (gray curve) and under attack (black curve). On the right: throughput of the WSN in the baseline condition (gray curve) and under attack (black curve)

Routing Attacks in a Mesh Topology: in the setup with the mesh topology, one malicious node infiltrates the network to conduct routing attacks. We present three different attacks: the sinkhole attack is used to reroute the traffic in the network. On top of that, the blackhole or the selective forwarding attack can be used to manipulate the traffic.

Sinkhole Attack: to conduct a sinkhole attack, the attacker inserts a malicious node into the network which pretends to have the shortest path to the destination. Therefore, all traffic will be routed over this specific node. This allows the attacker to get access to all information propagated in the network. Because of the longer route through the network, the end-to-end delay is increased significantly, but as shown in Fig. 2, the throughput is not affected. Another effect of this attack is the increased consumption of energy. This can cause a shorter lifespan of the nodes and therefore increased costs for farmers.

Blackhole Attack: this attack pattern is based on a sinkhole attack. After attracting all traffic of the network, all packages are dropped. Therefore, the throughput of the network is reduced to zero. This attack is easy to detect, but before it is stopped, no data or control signals can be transmitted. This is a severe harm to the continuation of the business. In agriculture, only short timespans for critical events like sowing or harvest exist. Sensor data is used to detect the optimal point of time for harvest. When a blackout attack is conducted during this period of time, serious damage can be caused.

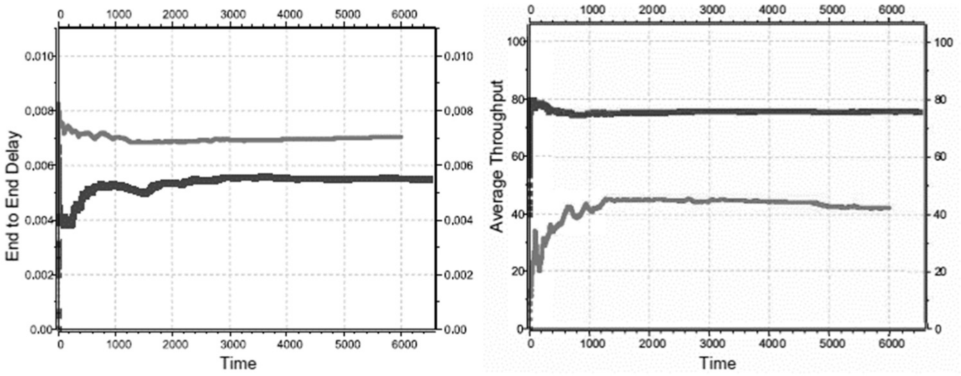

Fig. 3: Results of the Selective Forwarding Attack: on the left: the end-to-end delay of the packages in the baseline condition (black curve) and under attack (gray curve). On the right: throughput of the WSN in the baseline condition (black curve) and under attack (gray curve)

Selective Forwarding Attack: to avoid detection, a more sophisticated attack can be launched. Instead of dropping all traffic, only some packages are dropped. This is called a selective forwarding attack or grayhole attack. In our simulation, packages are dropped randomly with a probability of 0.5. The results are shown in Fig. 3. In our scenario, the attack is easily detected. The reason for this is the high drop probability. By choosing lower probabilities, this attack becomes harder to detect. Considering the fact that a sinkhole attack has to be conducted in preparation for a selective forwarding attack, the attacker knows all the traffic routed through the network. An analysis of this data allows an identification of different types of data packages and their purpose when the traffic is not encrypted. Therefore, the attacker can identify different devices and conduct a very precise attack by dropping only the control data for one specific device. Because such an attack is harder to detect, it can cause serious harm over a longer period of time.

4 Conclusion

Conflicting requirements regarding WSN in agriculture can pose security risks when farmers are not aware of the impact of cyberattacks and use insecure modes of operation. Security measures as encryption can diminish the risks, but result in higher costs for the farmers. More nodes are needed to provide redundancy and the software-based security mechanisms consume more power, resulting in a shorter lifespan for the hardware. This conflicts with the farmers' interest to keep the costs low. Smart Farming helps them to maximize the yield of their farms by controlling the environmental parameters and assisting farmers to make decisions. However, this way farmers become dependent on the correctness of the received data. As shown above, insecure standard modes and insecure keys allow attackers to infiltrate the system and manipulate the traffic. For example, important data can be dropped to prevent that warnings are generated when parasites are detected, or control data for the irrigation system is blocked to cause harm to the crops. Farmers need to develop awareness for those risks to operate their WSN correctly and benefit from this technology. Facing the possible damage resulting from cyberattacks in the real world, both for the business of the farmers as well as for societies depending on food production, farmers should invest in security measures allowing for resilient smart farming [Re19].

Acknowlegements: Geobox-I was supported by funds of the German Government's Special Purpose Fund held at Landwirtschaftliche Rentenbank. HyServ (01IS17030B) was supported by the German Federal Ministry for Education and Research (BMBF).

Literature

[Le06] Lee, J. et al.: Distributed and energy-efficient target localization and tracking in wireless sensor networks. Comput. Commun. 29/13-14, S. 2494-2505, 2006.

[Lu09] Lupu, T.-G. et al.: Main Types of Attacks in Wireless Sensor Networks. In: WSEAS international conference. In: Proc. WSEAS International Conference: Recent advances in computer engineering, S. 180-185, 2009.

[MAJ11] Mohammadi, A.; Atani, R.E.; Jadidoleslamy, H.: A Comparison of Routing Attacks on Wireless Sensor Networks. J Information Assurance and Security 6, S. 195-215, 2011.

[Ra16] Raheemah, A. et al..: New empirical path loss model for wireless sensor networks in mango greenhouses. Comput. Electron. Agric. 127, S. 553-560, 2016.

[Re18] Reuter, C. et al.: Resiliente Digitalisierung der kritischen Infrastruktur Landwirtschaft - mobil, dezentral, ausfallsicher. In: (Dachselt, R.; Weber, G., Hrsg.): Mensch und Computer 2018: Workshopband. GI, Dresden, S. 623-632, 2018.

[Re19] Reuter, C. et al.: Resilient Smart Farming (RSF) – Nutzung digitaler Technologien in krisensicherer Infrastruktur. In Proc. 39th Annual conference of GIL: Digitalisierung für landwirtschaftliche Betriebe in kleinstrukturierten Regionen - ein Widerspruch in sich?, Vienna 2019.

[Wa05] Wang, X. et al.: Search-based physical attacks in sensor networks: Modeling and defense. In: 14th Int. Conf. Computer Communications and Networks, S. 489-496, 2005.

[Wr09] Wright, J.: KillerBee : Practical Zigbee Exploitation Framework. In: 11th Toorcon Conference, San Diego, 2009.

[ZA12] ZigBee Alliance, Inc.: ZigBee specification document 053474r20, 19.09.2012. http://www.zigbee.org/wp-content/uploads/2014/11/docs-05-3474-20-0csg-zigbee-specification.pdf, Stand 03.12.2018.