Cyber Attacks on Smart Farming Infrastructure

Conference Paper · December 2020

DOI: 10.1109/CIC50333.2020.00025

CITATIONS
3

READS
246

7 authors, including:

Maanak Gupta
Tennessee Technological University
47 PUBLICATIONS **349** CITATIONS
SEE PROFILE

Mahmoud Abdelsalam
Manhattan College
21 PUBLICATIONS **171** CITATIONS
SEE PROFILE

Sudip Mittal
University of North Carolina at Wilmington
52 PUBLICATIONS **561** CITATIONS
SEE PROFILE

Anupam Joshi
University of Maryland, Baltimore County
495 PUBLICATIONS **18,423** CITATIONS
SEE PROFILE

Cyber Attacks on Smart Farming Infrastructure

Sina Sontowski*, Maanak Gupta†, Sai Sree Laya Chukkapalli‡, Mahmoud Abdelsalam§,
Sudip Mittal¶, Anupam Joshi‖, Ravi Sandhu**
*†Dept. of Computer Science, Tennessee Technological University, Cookeville, Tennessee, USA
‡‖Dept. of Computer Science, University of Maryland, Baltimore County, Baltimore, USA
§Dept. of Computer Science, Manhattan College, Bronx, USA
¶Dept. of Computer Science, University of North Carolina Wilmington, NC, USA
**Dept. of Computer Science, University of Texas at San Antonio, San Antonio, Texas, USA
*ssontowsk42@students.tntech.edu, †mgupta@tntech.edu, ‡saisree1@umbc.edu, §mabdelsalam01@manhattan.edu,
¶mittals@uncw.edu, ‖joshi@umbc.edu, **ravi.sandhu@utsa.edu

***Abstract*—Smart farming also known as precision agriculture is gaining more traction for its promising potential to fulfill increasing global food demand and supply. In a smart farm, technologies and connected devices are used in a variety of ways, from finding the real-time status of crops and soil moisture content to deploying drones to assist with tasks such as applying pesticide spray. However, the use of heterogeneous internet-connected devices has introduced numerous vulnerabilities within the smart farm ecosystem. Attackers can exploit these vulnerabilities to remotely control and disrupt data flowing from/to on-field sensors and autonomous vehicles like smart tractors and drones. This can cause devastating consequences especially during a high-risk time, such as harvesting, where live-monitoring is critical. In this paper, we demonstrate a Denial of Service (DoS) attack that can hinder the functionality of a smart farm by disrupting deployed on-field sensors. In particular, we discuss a Wi-Fi deauthentication attack that exploits IEEE 802.11 vulnerabilities, where the management frames are not encrypted. A MakerFocus ESP8266 Development Board WiFiDeauther Monster is used to detach the connected Raspberry Pi from the network and prevent sensor data from being sent to the remote cloud. Additionally, this attack was expanded to include the entire network, obstructing all devices from connecting to the network. To this end, we urge practitioners to be aware of current vulnerabilities when deploying smart farming ecosystems and encourage the cyber-security community to further investigate the domain-specific characteristics of smart farming.**

***Index Terms*—Smart Farming, Precision agriculture, Security, Cyber-attack, Internet of Things, Denial of Service**

I. Introduction

In recent years, significant progress has been made in the agricultural sector to develop smart farming and precision agriculture technologies [1] [2]. Agriculture industry accounts for 6.4% of the world's economic production with a total of $5,084,800 million[1]. Agriculture, food, and related industries contributed $1.053 trillion to U.S. gross domestic product (GDP) in 2017[2]. Therefore, investing in the smart farming ecosystem and adopting new technologies will have a wider impact on the economy. Further, the rapid growth of population has significantly increased the demand for agriculture and food products. Traditional technologies driving the agriculture sector are incapable of meeting this demand and are becoming obsolete. This has also led the agriculture and food production sector to integrate data driven and Internet of Things (IoT) technologies to increase the quantity and quality of agricultural products. Smart Farming can be a possible solution to boost productivity and maintain product quality. There are numerous smart farming use cases [3]–[5] present globally, e.g., a controlled water supply, recording soil moisture at different levels [6] to increase crop yield. Various sensors allow collection of data and can upload it to the *cloud*. The collected data provides helpful information about varying environmental conditions and allows for a hands-off approach to smart farm monitoring [2]. Figure 1, shows an end to end interaction among various entities involved in the smart farming ecosystem.

As a result of introducing IoT and connected infrastructure to farms, the agriculture sector will develop a dependency on various information systems to manage and improve operations [7]. However, incorporating IoT systems into the agricultural sector amplifies various cyber risks. These risks are currently not sufficiently addressed because of limited investments in cybersecurity by domain specific companies. In addition, the lack of resources and know-how among members of the farming community will aggravate the issue. Smart farms are a target for foreign competitors and threats, which is a concern to the agricultural sector. Cyber attacks on the smart farming infrastructure enables an attacker to remotely control and exploit on-field sensors and autonomous vehicles (tractors, autonomous vehicles, drones, etc.). Potential agricultural attacks can create an unsafe and unproductive farming environment. For example, exploits that have the ability to destroy an entire field of crops, flood the farmlands, over spray pesticides using smart drones, etc. can cause unsafe consumption as well as economic deterioration. Such attacks in a large coordinated manner, also referred to as *Cyber-Agroterrorism* [7], [8], also have the potential for disrupting the economy of an agriculture-dependent nation. A report released in 2018 by the US Council of Economic Advisors[3]

[1]http://statisticstimes.com/economy/countries-by-gdp-sector-composition.php

[2]https://www.ers.usda.gov/data-products/ag-and-food-statistics-charting-the-essentials/ag-and-food-sectors-and-the-economy

[3]https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

978-1-7281-4146-6/20/$31.00 ©2020 IEEE
DOI 10.1109/CIC50333.2020.00025

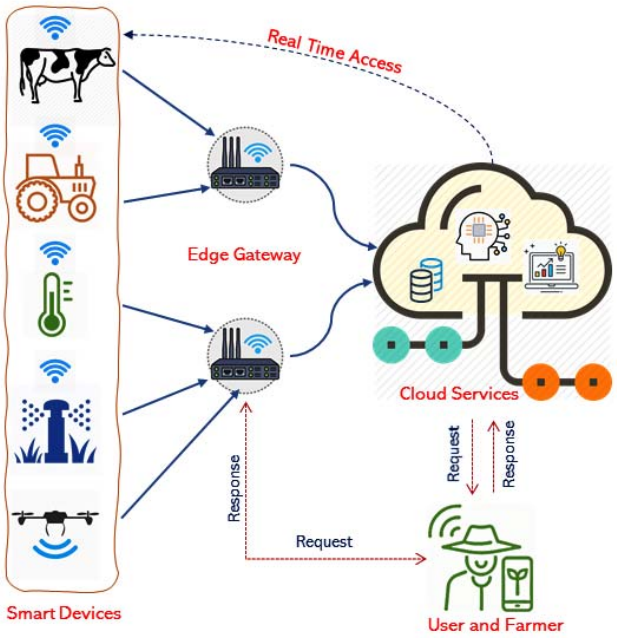


Fig. 1. Smart Farming Conceptual Architecture [10].

titled, "The Cost of Malicious Cyber Activity to the U.S. Economy" suggests the agriculture sector as one of the 16 critical infrastructure sectors that are important to both the U.S. economy and national security. It also reported that the agriculture sector experienced 11 cyber incidents in 2016. The Federal Bureau of Investigation (FBI) and United States Department of Agriculture (USDA) jointly issued a report [9] listing various threats to precision agriculture.

In this paper, a simple and cost-effective smart farm architecture is introduced where a DoS cyber-attack was carried out to show the vulnerabilities in the system. Smart farm IoT infrastructure is setup using Wi-Fi for monitoring an indoor plant which includes sensors that are connected to a Raspberry Pi[4] to facilitate monitoring. The data collected from the deployed sensors is sent to a cloud server for remote monitoring. A *Wi-Fi Deauthentication attack* was successfully executed which forced the Raspberry Pi to disconnect from the network, and prevented it from reconnecting. A MakerFocus ESP8266 Development Board WiFiDeauther Monster is used to detach the Raspberry Pi and prevent sensor data from being sent to the remote cloud. Additionally, this attack was expanded to include the entire network, obstructing all devices from connecting to the network. This caused the inability to receive sensor updates in the cloud, which can cause consequences for farmers who require live-monitoring. The demonstration of the Wi-Fi deauthentication attack exposes the weakness of the IEEE 802.11 protocol (2.4 GHz). Although this attack can be orchestrated in different IoT domains, it is particularly relevant in the smart farm domain due to wide use of cheap hardware such as low-cost sensors which increase the risk of a successful deauthentication attack, since not all sensors correctly support protected management frames. In addition, deauthentication attack tools commonly support 2.4 GHz wireless frequency instead of 5 GHz frequency. Due to the widespread of smart-farms, using 2.4 GHz is a more practical solution.

The rest of the paper is organized as follows - Section II presents an overview of cybersecurity and related work in smart farming domain. Section III discusses various types of cyber-attacks that could occur in the networking domain deployed on a smart farm. In section IV, we introduce our deployed architecture and later describe the experimental setup that demonstrates the Wi-Fi deauthentication attack. In section V, we provide the details of our process for launching a DOS attack and show the experimental results. In section VI, we present various use case scenarios of this attack. Finally, section VII provides some defense strategies against deauthentication attacks and VIII summarizes the work and suggests future work.

II. Related Work

Agricultural companies and farmers are moving towards various smart farming practices that rely on IoT devices for a better crop yield. Interconnecting various sensors deployed on the farm and allowing them to communicate through the Internet provides an attack surface. This has led to a rise in cyber-attacks on agriculture sector such as data breaches, denial of service attacks, website defacement, etc. Recently, Gupta et al. [10] highlighted security and privacy issues in the smart farming ecosystem. They presented a multi-layered architecture and identified potential cybersecurity issues in smart farming. Further, their work also illustrated scenarios of specific cyber attacks categorizing them into data, network, supply chain, and other common attacks.

A popular attack named 'The Night Dragon' [11] is an example where the attacker could steal a large amount of information from multiple petrochemical companies. Another example is the damage caused to a German steel mill [12] where attackers used spear phishing to gain access to the mill's office network and plant production systems.

The exponential rise in number of internet connected devices has raised security concerns especially, in the agriculture sector, as farmers will not be able to bear the potential loss and damage to crops. Therefore, at present, securing various sensors in the smart farm ecosystem is a key task for the agriculture sector. The U.S. Department for Homeland Security released a report [13] which emphasizes the importance of precision agriculture (PA) and associated cybersecurity threat and potential vulnerabilities. The report highlights the confidentiality, integrity, and availability model of information security in farming. It defines different technologies involved in smart farming including, on-farm devices, location and remote sensing technologies, machine learning, etc. It also briefly discusses the groups impacted including farmers,

[4]https://www.raspberrypi.org/

livestock producers, and also industries that support or rely on agriculture. This report also discusses hypothetical threat scenarios. Similarly, the security issues that could arise by deploying IoT sensors in the agriculture sector have been clearly elaborated by Jahn et al. [14] and Lopez et al. [15].

Different types of attacks can be executed by attackers, for instance, a denial of service (DoS) attack on a large scale by utilizing various IoT sensors deployed on the smart farm [16]. The *Mirai botnet* [17] in 2016 is one such example where multiple DoS attacks were launched by exploiting an army of connected smart home devices. Recently, researchers from a security firm named Sucuri [18] discovered that a DoS botnet could deliver 50,000 HTTP requests per second. Here, various websites were attacked by performing DDoS attacks. Similar conditions exist in the smart farming ecosystem. Thus, similar attacks are possible in the context of smart farming. Such attacks cannot only disrupt normal functions of different modules in an individual farm, but also can be leveraged to interrupt legitimate cyber services in other domains.

As many IoT related devices are present in each architectural layer of the smart farm ecosystem [10], these are prone to attacks and can be controlled by a central malicious system called *Botnet of Things* [19]. An army of infected farm IoT devices [20] can easily be used to infect many other networks through different mediums and hence a smart farm may turn out to be an internet of vulnerabilities for cyber criminals. Smart farms devices are not built with security as a concern and even if they did, users usually neglect the basic step of setting adequate cyber security defense mechanisms [10].

According to the Internet Security Alliance (ISA) [21] attacks on agriculture sector are a relatively low cost ventures that would in turn need a deployment of heavy financial resources to defend this ecosystem. Therefore, it is important for the agriculture sector to understand the consequences of cyber attacks and be conscious of the security challenges that can arise due to massive use of internet connected devices in the farming ecosystem. Artificial Intelligence based security methods have become popular in recent years [22]–[24]. Securing smart farms using established security frameworks would also provide a solution to the above, like the Smart Farming Access Control (SFAC) system [25]. Here the goal of the system is to help farmers create and enforce access control rules for their smart farms. The authors also discussed various access control scenarios on a smart farm and how rules written in the Semantic Web Rule Language (SWRL) [26] can be used to determine access.

Next, we discuss in detail various types of network attacks on smart farms.

III. Types of Network Attacks on Smart Farm

In recent years, several security threats [27]–[31] have been observed in IoT domain. Similar attacks can happen on smart farming ecosystem. It is predicted that the attacks on smart farming ecosystem are heavily dependent on the architecture and protocols used in deploying the connected environment. For example, an architecture that uses sensors that work with the *Zigbee*[5] protocol can have additional attacks such as a replay attack that might be difficult to implement on other protocols. The following network attacks listed below can be orchestrated in smart farms that use IEEE 802.11[6] protocol:

Password Cracking: Hacking the Wi-Fi encrypted protocols is never a complicated task. One of the most popular ways to do that is by cracking the Wi-Fi password that would exploit the user's network. The requirements needed to complete this attack are very minimal such as laptop or desktop running Kali[7] Linux which utilizes aircrack-ng[8] that has a suite of tools. In addition, a remote card that supports monitor injection mode is required. In order to capture the packets that are transmitted in air, a tool named *airodump-ng* from the aircrack-ng suite is used. With requirements being satisfied, an attacker can now capture the WiFi Protected Access (WPA) handshake by sending deauthentication packets to the Wi-Fi connected host. Finally, a dictionary attack is performed by testing Wi-Fi passwords present in a previously used word list [32].

Evil Twin Access Point: The Evil Twin access point allows an attacker to get credentials by creating a rogue access point. The rogue access point is set up on a reliable network without any permission and tries to persuade a wireless client into associating it with the reliable access point. Also, the rogue access point exploits automatic access point selection techniques. WPA2 is still susceptible to Evil Twin access point attack. This can be a successful approach because BSSID and SSID are simple to retrieve that play an important role in setting up a rogue access point. The attack particularly takes advantage of the auto connect options of the network on the client side [33]. This attack can easily be implemented on smart farms which utilize the 802.11 protocol.

Key Reinstallation Attacks: This attack exploits vulnerabilities of the 4-way handshake in WPA2 that secures the modern Wi-Fi. An attacker can trick the victim into reinstalling an already in use key. This is done by manipulating and replaying the cryptographic handshake messages in order to reset the key's associated parameters to its initial values. This would allow packets to be replayed, decrypted and/or forged. Basically, any information that a victim transmits can be decrypted [34]. Vendor patches have been distributed addressing the vulnerability. In such case, it totally depends on the availability of the patch for a device and the user's effort to update their devices. Similar to the evil twin access point attack, smart farms that use IEEE 802.11 and have outdated versions without patch are still susceptible to this attack.

Kr00k - CVE-2019-15126: This vulnerability affects devices with Wi-Fi chips that belong to Broadcom[9] and Cypress[10]. These Wi-Fi chips are most commonly used in Wi-Fi enabled devices such as smart phones, IoT gadgets, etc. In order to encrypt a part of the communication, an all

[5]https://zigbeealliance.org/solution/zigbee/
[6]http://www.ieee802.org/11/
[7]https://www.kali.org/
[8]https://www.aircrack-ng.org/
[9]https://www.broadcom.com/
[10]https://www.cypress.com/products/wi-fi

Fig. 2. Indoor plant remote monitoring IoT setup.

zero encryption key is used by these vulnerable devices. Therefore, an attacker who wants to launch an attack can decrypt some wireless network packets which are transmitted by these devices. Kr00k also effects Wi-Fi access points and both WPA2-Person, WPA2-Enterprise protocols with AES-CCMP encryption. Patches to fix this vulnerability have been released. However, it is unclear about the number of devices that have been fixed until now [35]. This vulnerability also affects smart farms that include vulnerable devices or access points that use 802.11.

ARP spoofing attack: The Address Resolution Protocol (ARP) spoofing attack targets a vulnerability of the ARP protocol. This type of attacks are usually carried out over the local area network (LAN). In this scenario, an attacker fakes the MAC address of the gateway and convinces the victim to send frames to the fake address instead of the destined gateway. In fact, ARP accepts replies without issuing any requests. Also, there is no way to verify a sender since there are no authentication methods in standard ARP. The data traffic can be manipulated and recorded by using ARP spoofing. Therefore, ARP spoofing can be used as a Man-in-the-middle attack to eavesdrop on traffic. Additionally, it can also be used for DoS and session hijacking [36].

DNS spoofing attack: In this attack, traffic is directed to a fake website due to the altered Domain Name System (DNS) records. An example is the DNS cache poisoning attack. In this attack, the attacker is used to intercept the traffic between the client and the gateway router. The attacker can now read DNS messages and has two options. In the first option, the attacker can change the IP of the NS (name server) in the DNS response message. In the second option, the attacker can use the same query ID and fake IP to create response messages for the NS. This immensely benefits the attacker because in both the cases, the IP is forged to his benefit [37].

IV. System Architecture and Experimental Setup

The architecture of deployed single smart farm is based upon Microsoft FarmBeats Student Kit[11] for precision agriculture. In our setup, we have made some modifications, which include an additional sensor. The Microsoft FarmBeats

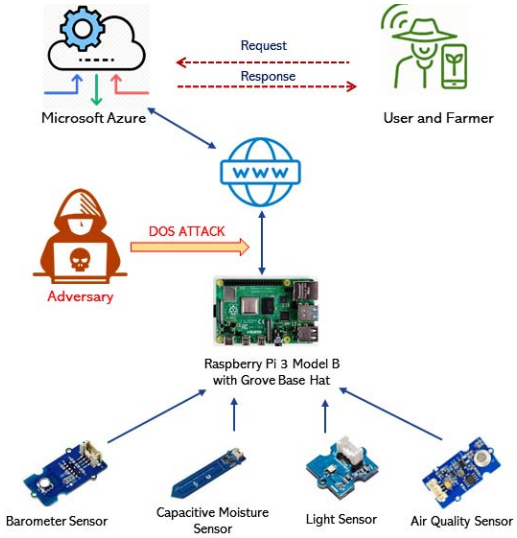


Fig. 3. System Architecture and Attack Surface.

TABLE I
Specification of Deployed Smart Farming Sensors.

Sensor	Interface	Power Supply
Grove-Air Quality sensor	Analog	3.3/5V
Grove-Light Sensor v1.2	Analog	5V
Grove - Capacitive Moisture Sensor	Analog	3.3/5V
Grove - Barometer Sensor (BME 280)	I2C	3.3/5V

Student Kit includes Microsoft Azure[12] cloud services and a Raspberry Pi with soil moisture, light, ambient temperature, and humidity sensors to collect data to improve productivity, increase yield, and save resources, together with data driven [38] applications. The kit was chosen as the architecture because of its comparable cheap cost, ease of installation, and set-up. In addition, all the data from the Microsoft FarmBeats Student Kit is collected to get a broad picture of precision agriculture deployment and allow researchers to use it as a testbed to deploy proof of concepts smart farming solutions.

The architecture used in this case is used to monitor an indoor plant over an extended period of time. The setup of the architecture which monitors the indoor plant can be seen in Figure 2. The single smart farm multi-layer architecture can be seen in Figure 3, where the Raspberry Pi and its sensors are mounted on an indoor plant to monitor its metrics. As can be seen in Figure 3, the network communication between Raspberry Pi and cloud (Microsoft Azure) will be intercepted and interrupted by a DoS attack, which prevents the Raspberry Pi from connecting to the network. This deployed architecture adapts and extends widely discussed IoT and Cyber Physical System (CPS) multi-layer architectures [39]–[43]. These architectures recognize the use of cloud and edge services, and the infinite capabilities provided by them to fully harness the data generated from smart devices at the physical layer [44]–

[11]https://farmbeatsstudentkit.com/Student

[12]https://azure.microsoft.com/en-us/

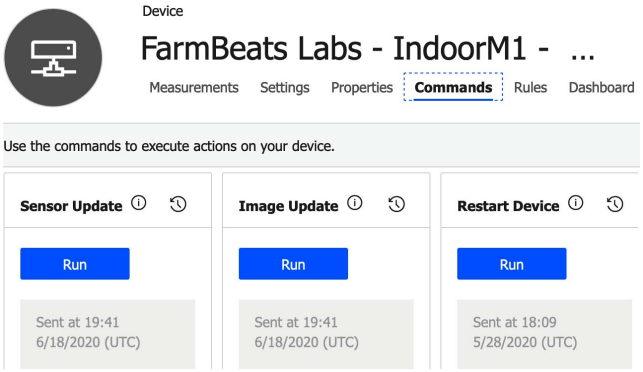


Fig. 4. Successful Sensor Update in Cloud

[51]. The four sensors that were used to monitor indoor plant are listed below (specifications in Table I):

- A *barometer sensor* to detect atmospheric pressure, altitude, temperature, and humidity.
- A *grove light sensor* has light dependent resistor to detect the intensity of the indoor light.
- An *air quality sensor* to detect harmful gases such as carbon monoxide, acetone, and alcohol.
- A *capacitive moisture sensor* measures soil moisture sensor based on capacitance changes.

These sensors were chosen because of their helpful application in monitoring in smart farm. A light sensor is helpful for successfully growing a plant since some plants need more light than others. If there are harmful gases in the air, that might prevent the plant from reaching its full growing potential and therefore an air quality sensor was chosen. Most plants require a specific range of water and the capacitive moisture sensor can display when it is time to water the plant. Different plants require different temperatures, humidity, pressure, and altitude and therefore a barometer sensor was used in this architecture.

These sensors are made by Grove[13], and require a Grove Base Hat[14] for them to be attachable to the Raspberry Pi 3 Model B. The Grove Base Hat provides Digital, Analog, 12C, PWM and UART port. An MCU is build-in which allows for a 12-bit 8 channel ADC [52]. The Grove Base Hat is mounted on a Raspberry Pi 3 Model B. The Raspberry Pi runs Windows 10 IoT Core[15] which is optimized for smaller devices that have a display or no display. This image is specifically targeted towards embedded IoT devices. IoT Core runs on ARM processors which allows it to be run on the Raspberry Pi [53]. The Raspberry Pi 3 Model B is connected to a personal 2.4 GHz Wi-Fi network. Since a 2.4 GHz network provides coverage at a longer range compared to 5 GHz network, it is applicable to a smart farm environment since the architecture can be farther away from the wireless access point. For this architecture, the transmission time of data was not of critical

[13]https://www.seeedstudio.com/category/Sensor-for-Grove-c-24.html
[14]https://www.robotshop.com/en/grove-base-hat-raspberry-pi-zero.html
[15]https://www.microsoft.com/en-us/software-download/windows10IoTCore

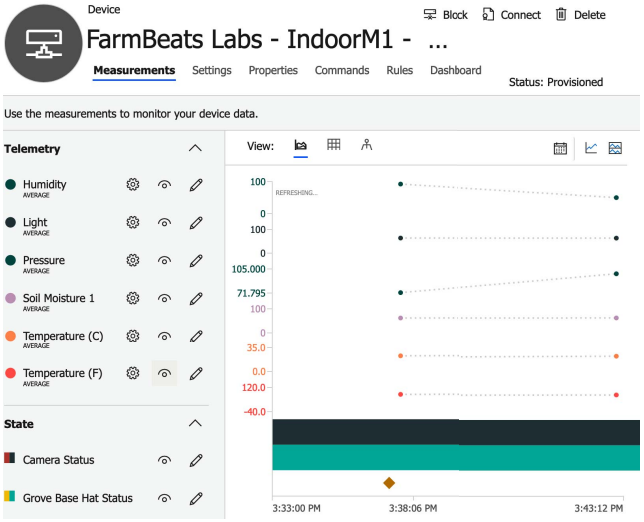


Fig. 5. Microsoft Azure IoT Template Graph.

importance, therefore 2.4 GHz network was used. Alternate protocols that could have been used include Bluetooth and Zigbee. Especially, the application of sensors that use bluetooth or Zigbee to communicate with the Raspberry Pi is another option for a smart-farm architecture. However, in our deployed case only the 802.11 protocol was used to emphasize simplicity and cost-effectiveness. In addition, the Raspberry Pi 3 Model B is connected to Microsoft Azure Cloud Service, more specifically the Azure IoT Central[16]. The connected sensors send updated data to the cloud as displayed by Figure 4. The cloud allows the sensor data to be manually updated and the Raspberry Pi to be rebooted. If the architecture includes an attached web camera, it would force an update of the image. Data analytic can be accessed by logging into the Azure IoT Central Cloud which provides a template that includes graphs and other visualizations as can be seen in Figure 5. It displays the sensor data as an average over time to visualize changes in the metrics such as changes in temperature, which can be helpful to get a quick overview of the sensor data captured from the field. The telemetry on the left, such as humidity and light, is displayed on the right on the graph in the same color. As an example, temperature stayed constant at about 22 degrees Celsius over five minutes. Any drastic change such as barometric pressure can be explained by the fact that the device rebooted shortly before the first value was read, as seen by the diamond under the graph in Figure 5, and therefore the sensor was still calibrating.

V. Methodology and Demonstration

A denial of service attack was successfully achieved by implementing a Wi-Fi deauthentication attack. In summary, the communication between the Raspberry Pi and the Wi-Fi access point was interrupted by using a Wi-Fi deauther tool. We used

[16]https://azure.microsoft.com/en-us/services/iot-central/

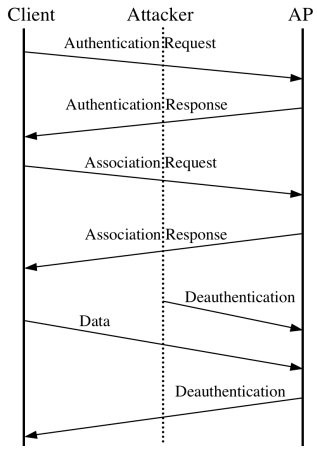


Fig. 6. Graphical Depiction of Deauthentication Attack [54].

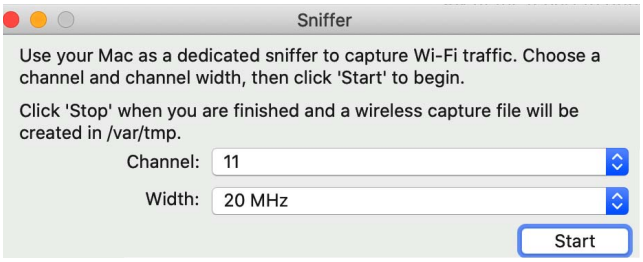


Fig. 7. Packet Sniffing using Wireless Diagnostics in MacOSX.

the MakerFocus ESP8266 Development Board WiFi Deauther Monster, which allowed us to disconnect the Raspberry Pi off the network which therefore caused no data to be sent to the Azure cloud. In addition, we expanded the attack to include the whole network and therefore disabled any devices to connect to the network. The deauther sends packets that disconnect devices but does not interfere with any frequencies.

A. *Overview of the Wi-Fi Deauthentication Attack*

A Wi-Fi deauthentication attack is successfully implemented on a smart farm architecture that is connected to a 2.4 GHz network. This attack falls under Denial of Service (DoS) attacks and exploits 802.11 vulnerabilities [55], [56]. An attacker starts by monitoring raw frames that include information such as source and destination Media Access Control (MAC) addresses to find the targeted victim. For example, Wireshark packet capture can be used to identity traffic patterns and therefore identify the victim. In this case, it was known that the victim is sending sensor updates every few seconds to minutes to the cloud, therefore looking at packet activity can help to identify the victim. The adversary sends spoofed deauthentication frames with spoofed source MAC address of access point or victim station once data or association response frame is found [55], [56]. In general, deauthentication frames are sent by a station or access point (AP) when all communications are terminated. Deauthentication is not a

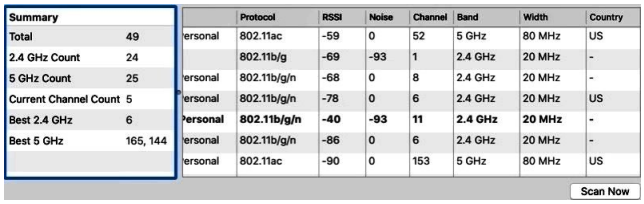


Fig. 8. Scanning for Channels.

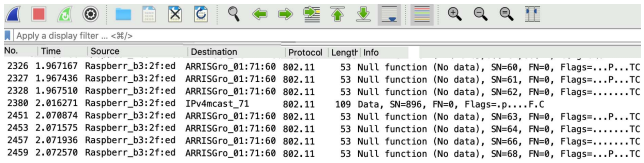
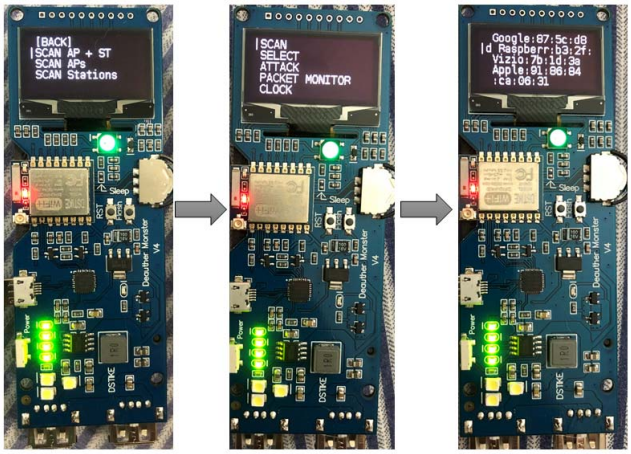


Fig. 9. Packet Capture of some Raspberry Pi Packets.

request, but a notification. That means that if a station wants to deauthenticate from an AP or an AP wants to deauthenticate from stations, either device can send the deauthentication frame and cannot be refused by either party except when management frame protection is involved. A deauthentication automatically causes disassociation because authentication is a prerequisite for association [55]. The sending of spoofed deauthentication frames forces the targeted station to become unauthenticated and therefore is disconnected from the network. The attacked station then tries to reconnect and to prevent that re-connection the attacker continuously keeps sending the deauthentication frames. The sequence of this attack is shown in Figure 6. To be able to reconnect, the attacked client is forced to repeat IEEE 802.11 authentication and association process. The station is unable to connect to the network through prolonged sustaining of the spoofed frames [55]. This repeating transmission of frames is considered a DoS attack against the target MAC address which is then prevented to access the network. This kind of attack is difficult to detect because the frames are sent directly to the client without any detection or logging by the access point (AP) or Intrusion Detection System (IDS). In addition, MAC filtering process is unable to prevent this attack [56]. Often such attacks are used to prevent unauthorized stations from connecting to access points by wireless IDS vendors [55]. A prime reason this attack is possible is due the fact that management frames are not encrypted in IEEE 802.11 protocol. However, the protocol 802.11w prevents Wi-Fi deauthentication attacks by including cryptographic protection to deauthentication and dissociation frames. Therefore, those frames are very hard to be spoofed in a DoS attack [57]. An important reason for successful demonstration of this attack is because many vendors have not updated their hardware and software to 802.11w. In the following subsection, we will detail how this attack is orchestrated in a single smart farm setup.



a). Scanning for Access Point and Stations b). Main Menu c). Select Raspberry Pi

Fig. 10. Steps for Completing a DoS Attack

B. Steps to a DoS Attack

In order to organize a DoS attack, first, packets were sniffed to ensure the connectivity of Raspberry Pi and to see whether the packets are encrypted. Wireless Diagnostics in Mac OSX was used to sniff the packets, as shown in Figure 7. The built in Wi-Fi stumbler tool was used to identify channels and widths to use for packet sniffing, as illustrated in Figure 8. The channel was found to be 11 for the network. After the channel was identified, the sniffer on Mac OSX was used to trace network traffic on that channel. The packet capture was opened with WireShark[17] shown in Figure 9. These displayed packets are filtered by the source. In our case, the source of these packets is attacked Raspberry Pi which is transmitting packets to the router (ARRISGro) and using IP multicast (IPv4mcast) to send packets to multiple sources in one transmission. The device is sending null data to the connected router to establish that it is in *active* state and that the transmission of frames from the AP to Raspberry Pi should be as expected. After the packets were sniffed, the Wi-Fi deauthentication attack was started. These packets are encrypted in WPA2 which prevents similar attack possibilities.

To successfully implement a Wi-Fi deauthentication attack, the Wi-Fi deauther tool needs to be in range of the network. The MakerFocus ESP8266 Development Board WiFi Deauther Monster comes with an antenna to improve its ability to catch the signal, which makes an adversary located at a Wi-Fi enabled smart farm to perform such attack. Note that this attack only works on a 2.4 GHz network. Steps of completing the attack are listed below (shown in Figure 10). These steps may be different in case another deauther tool is used.

1) The first step is to scan for access points and stations, as can be seen in Figure 10 (a). This is the most important step because if the desired station or access point cannot be found, the attack cannot happen. Depending on the signal strength, the antenna can be attached to the Deauther tool. Stations and access points found during this step will be needed for step 2.
2) When trying to deauther the Raspberry Pi, we need to go back to the main menu as seen in Figure 10 (b), and select the Raspberry Pi under stations as displayed in Figure 10 (c). Since we scanned for stations and access points in step 1, the Raspberry Pi was found and appears under stations now. With this step, we selected the Raspberry Pi as the station that we want to attack.
3) The last step is to organize the attack, which means going back to the main menu and under attack, selecting the deauther attack. A deauthentication frame is now sent to the Raspberry Pi and therefore disconnecting it from the network. The attacked Raspberry Pi is not connected to the network anymore, and the cloud cannot receive any sensor update. Figure 11 shows that when trying to update the sensors during the attack, no updates were received.

[17]https://www.wireshark.org/

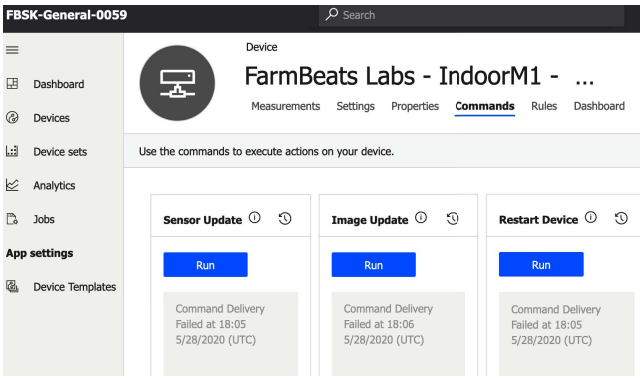


Fig. 11. Raspberry Pi unable to connect with FarmBeats Console.

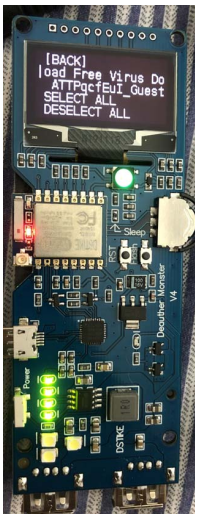


Fig. 12. Attack on Entire Network.

Attacking the Entire Network: This attack is possible on

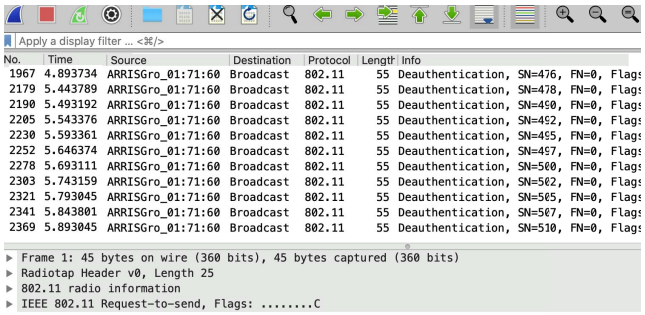


Fig. 13. Deauthentication Frames Packet Capture during Entire Network Attack.

our architecture because only one AP is used. If more than one AP is used, they need to be in reach of the deauther tool. The deauther tool includes a 8 dbi antenna, which has a range of about 1500 ft. A different antenna can be purchased to increase the signal if needed to reach all of the APs. The attacked Raspberry Pi is connected to the Wi-Fi network named 'Free Virus Download'. This network is selected in the deauther tool to attack the complete network as shown in Figure 12. The steps for implementing the expanded network attack are similar as for disabling an individual station. First, access points and stations need to be scanned, then the network needs to be selected under APs. And finally, the deauther attack needs to be selected in the main menu. The Wi-Fi deauther attack was done on the whole network which resulted in the disconnection of all devices connected to the network including the Raspberry Pi. Packet capture in Figure 13 displays the router sending deauthentication frames to the stations on the network. This packet capture is filtered by packet info and is therefore not in order. This filtering by packet info was done to show that a large number of deauthentication frames have been sent repeatedly to prevent stations from connecting to the network. This proves that the Wi-Fi deauthentication attack was a success due to the inability of the Raspberry Pi to connect to the network and sending sensor updates.

Our demonstration of the Wi-Fi deauthentication attack exposes the weakness of the IEEE 802.11 protocol (2.4 GHz), which requires attention and especially relevant not only in smart farming but also other IoT domains. By using 802.11w, management frames are encrypted and will make deauthentication attack much more difficult to implement. However, our deployed Wi-Fi network and numerous other similar networks do not have 802.11w implemented.

VI. Implications of Deauthentication Attacks

Wi-Fi Deauthentication attack is one of the major availability attacks [58] which disrupts communication networks and equipment availability, and negatively impacts the smart farms productivity. In our experiments, the Raspberry Pi can be considered an online connected equipment (e.g, smart sensor or drone). Wi-Fi Deauthentication attack targets the Raspberry Pi and detaches it from the network. This attack impacts smart farms in multiple scenarios. A few are discussed below.

Sensor data obstruction: Data acquired from various sensors is the foundation of a smart farm, where most decisions are automated based on the data. For instance, the smart farm's irrigation system activates and deactivates based on the soil water level measured by the moisture sensors. Typically, it is based on a simple certain threshold; however, modern smart irrigation systems consider more dynamic factors that require real-time data analytics and AI technologies. Real-time AI services can be used to determine how environmental factors influence the crops being irrigated as well as how soil moisture responds to irrigation for different crops, soils, and environmental conditions. As such, Deauthentication attacks, which prevent moisture sensors from connecting to the network, obstruct real-time communication and disrupt the irrigation system's decision. This leads to crops over or under-watering, and eventually damage crops, negatively affecting a successful harvest. The potential damage of this particular scenario is also valid for livestock, where sensors monitoring their food, water, and health status are unavailable.

Controlling connected devices: As stated in section III, a deauthentication attack can be the basis for a subsequent evil twin access point or a password cracking attack. The attacker fetches the authentication details of the farmer by redirecting the farmer to a similar fake network. After that, the attacker gains access to the entire smart farm where he can control various devices to intentionally cause damage. For example, the attacker can damage the crops by controlling agricultural drones to spray excessive fertilizers over the plants. This would result in damaging crops at an early stage and bring huge loss.

It is important to recover from DoS attacks and communication disruptions quickly before any substantial damage takes place. As such, detection and recovery techniques should be well researched. Such attacks, if launched on a large scale, can cause dramatic economic loss to an entire country.

VII. Defense against Deauthentication Attack

Enabling IEEE 802.11w-2009 prevents and detects deauthentication attacks by protecting the management frames due to encryption. IEEE 802.11w is required by WPA3. For deauthentication and dissociation frames that are sent after key establishment, pair-related one-time keys are used: one for the access point and one for the client, where then the client determines if the deauthentication is valid. Reasonable priced 802.11w-2009 routers are common in big companies like Cisco or Aruba. One possible reason for that might be production costs. An encryption capability issue that involves a missing cipher can cause routers not to be 802.11w capable which can cause issues in the production cycle. 802.11w requires Robust Security Networks (RSN) that use, for example, AES/CCMP encryption. 802.11w requires the vendor to update their code/firmware on both APs and client side. Also, on some routers, IEEE 802.11w needs to be enabled and is not automatically enabled. The Raspberry Pi 3 Model B in this architecture does not support 802.11w because the

network interface card does not support the encryption protocol required for the protected management frames. However, the Raspberry Pi 3 model B+ has protected management frames capabilities. Therefore, updated hardware with in-built encrypted management frame functionality can protect against such attacks.

VIII. Conclusion & Future Work

In the last few years, smart farming has become popular and widely adopted. This transition has been accelerated further because of crop productivity and quality benefits while lowering the overall cost. However, this shift towards a connected ecosystem, exposes new attack surfaces, and provides opportunities for attackers to exploit vulnerabilities.

In this paper, we demonstrate a Denial of Service (DoS) attack on a smart farm ecosystem. We implemented a Wi-Fi deauthentication attack on the smart farm Wi-Fi network with a MakerFocus ESP8266 Development Board WiFiDeauther Monster, which obstructed a deployed sensor from connecting to the network. In addition, the attack was expanded to the entire network which prevented any smart device from connecting to a central cloud. This inability to not receive real-time sensor updates can negatively impact the data driven applications and overall functionality of a farm. The demonstration of the Wi-Fi deauthentication attack exposes a weakness of the IEEE 802.11 protocol (2.4 GHz). The ability and ease of carrying out a DoS attack in the precision agriculture ecosystem can have serious implications and a large scale coordinated attack can disrupt national economies.

For future work, we plan to expand on other attacks on smart farming infrastructure including evil twin access point and password cracking. In addition, we will extend these attack to include protocols such as zigbee and bluetooth to launch attacks such as man-in-the-middle and replay.

Acknowledgment

This work is partially supported by the NSF SFS Grant DGE-1565562, Faculty Research Grant Program at Tennessee Technological University, NSF CREST HRD-1736209 and by the National Institute of Standards and Technology (NIST) under Grant 70NANB18H265.

References

[1] John V Stafford. *Precision agriculture'19*. Wageningen Academic Publishers, 2019.

[2] Muhammad Shoaib Farooq, Shamyla Riaz, Adnan Abid, Kamran Abid, and Muhammad Azhar Naeem. A survey on the role of iot in agriculture for the implementation of smart farming. *IEEE Access*, 7:156237–156271, 2019.

[3] Deepak Vasisht, Zerina Kapetanovic, Jongho Won, Xinxin Jin, Ranveer Chandra, Sudipta Sinha, Ashish Kapoor, Madhusudhan Sudarshan, and Sean Stratman. Farmbeats: An iot platform for data-driven agriculture. In *14th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 17)*, pages 515–529, 2017.

[4] Andreas Kamilaris, Feng Gao, Francesc X Prenafeta-Boldú, and Muhammad Intizar Ali. Agri-iot: A semantic framework for internet of things-enabled smart farming applications. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 442–447. IEEE, 2016.

[5] Sjaak Wolfert, Lan Ge, Cor Verdouw, and Marc-Jeroen Bogaardt. Big data in smart farming–a review. *Agricultural Systems*, 153:69–80, 2017.

[6] Hemavathi B Biradar and Laxmi Shabadi. Review on iot based multidisciplinary models for smart farming. In *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, pages 1923–1926. IEEE, 2017.

[7] Luís Barreto and António Amaral. Smart farming: Cyber security challenges. In *2018 International Conference on Intelligent Systems (IS)*, pages 870–876. IEEE, 2018.

[8] O Shawn Cupp, David E Walker, and John Hillison. Agroterrorism in the us: key security challenge for the 21st century. *Biosecurity and bioterrorism: biodefense strategy, practice, and science*, 2(2):97–105, 2004.

[9] Fbi warns farmers of cyber-security threat with precision ag use, Jun 2016.

[10] Maanak Gupta, Mahmoud Abdelsalam, Sajad Khorsandroo, and Sudip Mittal. Security and privacy in smart farming: Challenges and opportunities. *IEEE Access*, 8:34564–34584, 2020.

[11] Maria Bartnes, Ali Zand, Gianluca Stringhini, and Richard Kemmerer. Targeted attacks against industrial control systems: Is the power industry prepared? *Proceedings of the ACM Conference on Computer and Communications Security*, 2014:13–22, 11 2014.

[12] BBC. Hack attack causes 'massive damage' at steel works. https://www.bbc.com/news/technology-30575104. [Online].

[13] Aida Boghossian et al. Threats to Precision Agriculture. Technical report, U.S. Department of Homeland Security, 2018.

[14] Molly M. Jahn et al. Cyber Risk and Security Implications in Smart Agriculture and Food Systems. Available at : https://jahnresearchgroup.webhosting.cals.wisc.edu/wp-content/uploads/sites/223/2019/01/Agricultural-Cyber-Risk-and-Security.pdf (Accessed on: 2019/11/14), 2019.

[15] Daniel Lopez, Maria Uribe, Claudia Santiago, Andrés Torres, Nicolas Guataquira, Stefany Castro, Pantaleone Nespoli, and Felix Gomez Marmol. Shielding iot against cyber-attacks: An event-based approach using siem. *Wireless Communications and Mobile Computing*, 2018, 10 2018.

[16] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. Ddos in the iot: Mirai and other botnets. *Computer*, 50(7):80–84, 2017.

[17] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. Understanding the mirai botnet. In *26th {USENIX} Security Symposium ({USENIX} Security 17)*, pages 1093–1110, 2017.

[18] Sucuri. IoT botnet: 25,513 CCTV cameras used in crushing DDoS attacks. https://www.csoonline.com/article/3089298/iot-botnet-25-513-cctv-cameras-used-in-crushing-ddos-attacks.html. [Online].

[19] Tarini Tyagi. Botnet of things: Menace to internet of things.

[20] Georgios Kambourakis, Constantinos Kolias, and Angelos Stavrou. The mirai botnet and the iot zombie armies. In *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*, pages 267–272. IEEE, 2017.

[21] ISA. CYBERSECURITY IN THE FOOD AND AGRICULTURE SECTOR. https://isalliance.org/sectors/agriculture/. [Online].

[22] Sowmya Ramapatruni, Sandeep Nair Narayanan, Sudip Mittal, Anupam Joshi, and Karuna Joshi. Anomaly detection models for smart home security. In *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pages 19–24. IEEE, 2019.

[23] Sandeep Nair Narayanan, Sudip Mittal, and Anupam Joshi. Obd_securealert: An anomaly detection system for vehicles. In *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 1–6. IEEE, 2016.

[24] Sai Sree Laya Chukkapalli, Sudip Mittal, Maanak Gupta, Mahmoud Abdelsalam, Anupam Joshi, Ravi Sandhu, and Karuna Joshi. Ontologies and artificial intelligence systems for the cooperative smart farming ecosystem. *IEEE Access*, 8:164045–164064, 2020.

[25] Sai Sree Laya Chukkapalli, Aritran Piplai, Sudip Mittal, Maanak Gupta, Anupam Joshi, et al. A smart-farming ontology for attribute based access control. In *6th IEEE International Conference on Big Data Security on Cloud (BigDataSecurity 2020)*, 2020.

[26] Horrocks, Ian, Patel-Schneider, Peter F, Boley, Harold, Said Tabet, Said, Grossof, Benjamin, Mike Dean, and Mike. Swrl: A semantic web rule language combining owl and ruleml. *W3C Subm*, 21, 01 2004.

[27] Linus Wallgren, Shahid Raza, and Thiemo Voigt. Routing attacks and countermeasures in the rpl-based internet of things. *International Journal of Distributed Sensor Networks*, 9(8):794326, 2013.

[28] Masoumeh Safkhani and Nasour Bagheri. Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things. *The Journal of Supercomputing*, 73(8):3579–3585, 2017.

[29] Pericle Perazzo, Carlo Vallati, Dario Varano, Giuseppe Anastasi, and Gianluca Dini. Implementation of a wormhole attack against a rpl network: Challenges and effects. In *2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, pages 95–102. IEEE, 2018.

[30] Kuan Zhang, Xiaohui Liang, Rongxing Lu, and Xuemin Shen. Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal*, 1(5):372–383, 2014.

[31] Bishnu Prasad Gautam, Katsumi Wasaki, Amit Batajoo, Suresh Shrestha, and Sato Kazuhiko. Multi-master replication of enhanced learning assistant system in iot cluster. In *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, pages 1006–1012. IEEE, 2016.

[32] N. Pimple, T. Salunke, U. Pawar, and J. Sangoi. Wireless security — an approach towards secured wi-fi connectivity. In *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pages 872–876, 2020.

[33] Anil Kumar and Partha Paul. Security analysis and implementation of a simple method for prevention and detection against evil twin attack in ieee 802.11 wireless lan. In *2016 international conference on computational techniques in information and communication technologies (ICCTICT)*, pages 176–181. IEEE, 2016.

[34] Mathy Vanhoef and Frank Piessens. Key reinstallation attacks: Forcing nonce reuse in wpa2. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1313–1328, 2017.

[35] R. Lipovský M. Čermák, Š. Svorenčík and O. Kubovič. KR00K - CVE-2019-15126. https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf. [Online].

[36] Mahendra Data. The defense against arp spoofing attack using semi-static arp cache table. In *2018 International Conference on Sustainable Information Engineering and Technology (SIET)*, pages 206–210. IEEE, 2018.

[37] M. A. Hussain, H. Jin, Z. A. Hussien, Z. A. Abduljabbar, S. H. Abbdal, and A. Ibrahim. Dns protection against spoofing and poisoning attacks. In *2016 3rd International Conference on Information Science and Control Engineering (ICISCE)*, pages 1308–1312, 2016.

[38] Farmbeatslabs. farmbeatslabs/studentkit, Jun 2019.

[39] Matthew Gigli and Simon Koo. Internet of things: services and applications categorization. *Advances in Internet of Things*, 1(02):27, 2011.

[40] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347–2376, 2015.

[48] Manuel Díaz, Cristian Martín, and Bartolomé Rubio. State-of-the-art, challenges, and open issues in the integration of internet of things

[41] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[42] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7):1645–1660, 2013.

[43] Maanak Gupta and Ravi Sandhu. Authorization framework for secure cloud assisted connected cars and vehicular internet of things. In *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, pages 193–204, 2018.

[44] A. R. Biswas and R. Giaffreda. Iot and cloud convergence: Opportunities and challenges. In *Proc. of WF-IoT*, pages 375–376. IEEE, 2014.

[45] R. Lea and M. Blackstock. City hub: A cloud-based iot platform for smart cities. In *Proc. of CloudCom*, pages 799–804. IEEE, Dec 2014.

[46] A. Botta, W. de Donato, V. Persico, and A. Pescapé. On the integration of cloud computing and internet of things. In *Proc. of FiCLOUD*, pages 23–30. IEEE, Aug 2014.

[47] M. Aazam, I. Khan, A. A. Alsaffar, and E. N. Huh. Cloud of things: Integrating internet of things and cloud computing and the issues involved. In *Proc. of IBCAST*, pages 414–419, Jan 2014.
and cloud computing. *Journal of Network and Computer Applications*, 67(Supplement C):99 – 117, 2016.

[49] Alessio Botta, Walter de Donato, Valerio Persico, and Antonio Pescapé. Integration of cloud computing and internet of things: A survey. *Future Generation Computer Systems*, 56(Supplement C):684 – 700, 2016.

[50] M. Gupta, J. Benson, F. Patwa, and R. Sandhu. Secure V2V and V2I Communication in Intelligent Transportation using Cloudlets. *IEEE Transactions on Services Computing*, pages 1–1, 2020.

[51] Maanak Gupta, James Benson, Farhan Patwa, and Ravi Sandhu. Dynamic groups and attribute-based access control for next-generation smart cars. In *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*, pages 61–72, 2019.

[52] Baozhu Zuo. Grove base hat for raspberry pi.

[53] Terry Warwick. Overview of windows 10 iot core - windows iot.

[54] John Bellardo and Stefan Savage. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In *USENIX security symposium*, volume 12, pages 2–2. Washington DC, 2003.

[55] Joshua Wright. Weaknesses in wireless lan session containment. *White paper.[Online] Available: http://i. cmpnet.com/nc/1612/graphics/SessionContainment_file. pdf [Accessed: February 2010]*, 2005.

[56] Prabhaker Mateti. Hacking techniques in wireless networks hacking techniques in wireless networks. *Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management*, 3:83, 2006.

[57] Cisco Meraki. 802.11w Management Frame Protection MFP. https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/802.11w_Management_Frame_Protection_MFP. [Online].

[58] Scott Champion, Linsky, Peter Mutschler, Brian Ulicny, Thomson Reuters, Larry Barrett, Glenn Bethel, Michael Matson, Thomas Strang, Kellyn Ramsdell, and Susan Koehler. Threats to precision agriculture (2018 public-private analytic exchange program report), 02 2020.