Your Home is Insecure: Practical Attacks on Wireless Home Alarm Systems

Tao Li*, Dianqi Han†, Jiawei Li†, Ang Li†, Yan Zhang†, Rui Zhang‡, Yanchao Zhang†
* Indiana University-Purdue University Indianapolis, † Arizona State University, ‡ University of Delaware
tli6@iupui.edu, {dqhan, jwli, anglee, yanzhangyz, yczhang}@asu.edu, ruizhang@udel.edu

IEEE INFOCOM 2021 - IEEE Conference on Computer Communications | 978-1-6654-0325-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/INFOCOM42981.2021.9488873

***Abstract*—Wireless home alarm systems are being widely deployed, but their security has not been well studied. Existing attacks on wireless home alarm systems exploit the vulnerabilities of networking protocols while neglecting the problems arising from the physical component of IoT devices. In this paper, we present new event-eliminating and event-spoofing attacks on commercial wireless home alarm systems by interfering with the reed switch in almost all COTS alarm sensors. In both attacks, the external adversary uses his own magnet to control the state of the reed switch in order to either eliminate legitimate alarms or spoof false alarms. We also present a new battery-depletion attack with programmable electromagnets to deplete the alarm sensor's battery quickly and stealthily in hours which is expected to last a few years. The efficacy of our attacks is confirmed by detailed experiments on a representative Ring alarm system.**

I. Introduction

With people's increasing attention on home security and the development of IoT technology, home security devices—such as smart cameras, alarms, locks, and doorbells—are flooding into the market. Compared with traditional security devices, these smart devices can provide better protection for your home and are more user-friendly. The home security market is estimated to reach 74.75 billion dollars by 2023 from 45.58 billion dollars in 2018 [1].

The wireless home alarm system is a very popular home security product which has been provided by companies such as Ring (an Amazon company), Google, and Honeywell. Fig. 1 illustrates a typical home alarm system consisting of a base station, contact sensors, and extenders. Each contact sensor is associated with a magnet to monitor the OPEN or CLOSE state of the door or window.[1] For each pair of the contact sensor and magnet, one piece is installed on the door, and the other is installed on the door frame. When we open the door and then separate the contact sensor and magnet, the Reed switch in the contact sensor detects low magnetic field strength and then triggers an OPEN event report to the base station which in turn reports the event to the user's smartphone and the alarm service provider if any. The extender forwards packets between the base station and contact sensors when they are too far away from each other. Communications between the base station and contact sensors are usually based on some lightweight communication protocols such as Z-Wave, Bluetooth Low Energy, and Zigbee. Normally, contact sensors are powered by a small battery, and the base station and extenders are connected to outlets.

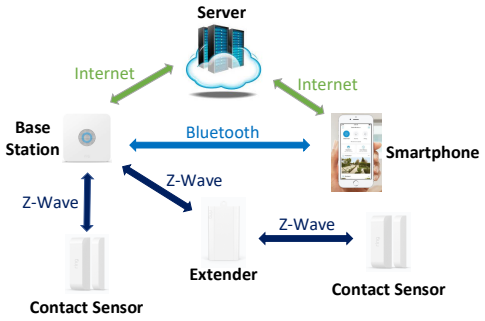


Fig. 1. A typical wireless home alarm system.

The security of home alarm systems has not been well studied. Most attacks reported so far only exploit vulnerabilities in the networking protocols. For example, Lamb [2] presented jamming and replay attacks to eliminate legitimate alarms and cause false alarms for multiple home alarm systems. Fouladi and Ghanoun [3] used a flaw in Z-Wave to reset the encryption key to a chosen value so that the attacker can inject unauthorized commands. The attacks in [4], [5] inject a fake base station into the network to control the home IoT devices. To the best of our knowledge, nobody has studied the security issues arising from the home alarm system's physical components such as the reed switch in contact sensors.

In this paper, we present new *event-eliminating* and *event-spoofing* attacks on commercial home alarm systems by interfering with the reed switch in almost all contact sensors. In both attacks, the adversary uses a magnet of its own—called a *malicious magnet* henceforth—to control the state of the reed switch. In the event-eliminating attack, the adversary makes the malicious magnet have the same polarity as the legitimate one so that their magnetic fields strengthen each other. When the adversary opens the corresponding door from outside, the interfered reed switch may not trigger any alarm because the magnetic strength around the contact sensor is still maintained by the malicious magnet. In the event-spoofing attack, the adversary makes the malicious magnet have the opposite polarity to the legitimate one so that their magnetic fields weaken each other. If the magnet field strength falls below a threshold, the reed switch can trigger a false alarm even though

[1]We use the door as an example in the rest of this paper.

978-1-6654-0325-2/21/$31.00 ©2021 IEEE

the door is still closed. Even worse, when receiving no alarm or too many annoying false alarms from a particular contact sensor, the user or base station may consider it faulty by mistake and temporarily disable it. The door with the disabled sensor thus can become the weakest entry point into the house until a field technician responds to the user's on-site service call, which may happen in a few days.

In addition to event-eliminating and event-spoofing attacks, we present a new *battery-depletion* attack to deplete the sensor battery quickly and stealthily. The basic idea is to force a contact sensor to generate large amounts of fake events and transmit continuously to consume energy without raising alarms. The contact sensor with low battery cannot provide any security alarm unless the user manually replaces the battery, which may be infeasible if the user has no backup battery at home or is traveling away from the home. Since the contact sensor will have to be temporarily disabled to avoid continuous low-battery warnings, attackers may have a long time window to illegally enter the house and an even longer time window if the home owner is on travel.[2]

To launch the above attacks, there are some critical challenges to solve. First, attackers are outside the target house and cannot see the interior contact sensor. Attackers may not be able to achieve their goal if they cannot accurately infer the sensor's location or magnet's polarity. To solve this challenge, we present techniques for attackers to localize the contact sensor and then determine the legitimate magnet's polarity with a smartphone. Second, it is impractical for attackers to manually generate a large amount of fake events to deplete the sensor battery with a permanent magnet. To tackle this challenge, we build a system with a programmable microcontroller and an electromagnet to attack the sensor automatically. The system can be programmed to transmit magnetic signals periodically to force the sensor to generate OPEN and CLOSE events continuously until the sensor battery is dead. Finally, the triggered fake events can be received by the base station which may report the anomaly to the service provider or the user (home owner). To launch the attack stealthily, we introduce novel jamming techniques to prevent the base station from receiving any packet while triggering the contact sensor to transmit continuously.

Our contributions can be summarized as follows.

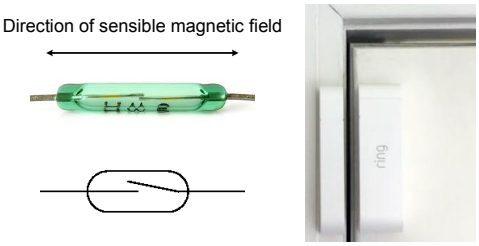
- We present practical event-eliminating and even-spoofing attacks on home alarm systems using security flaws of the reed switch which is commonly used for proximity detection in contact sensors. Attackers can eliminate true alarms and also generate false alarms with magnetic signals of different polarities. To make the attack practical, we introduce techniques to help external attackers localize interior contact sensors and infer their magnet polarity with a COTS smartphone.
- We build a system with a programmable microcontroller and an electromagnet to make a contact sensor continuously transmit to the base station so that its battery can be quickly depleted. We also propose novel jamming techniques so that the base station cannot receive any sign of the ongoing battery-depletion attack. Same as event-eliminating and even-spoofing attacks, the battery-depleting attack is generic and can apply to almost all home alarm systems using the reed switch.
- We conduct extensive experiments to evaluate the above attacks. Our evaluation results show that the attacks are highly practical and effective. In particular, the attacker can successfully deplete a new sensor battery in 43 hours which should work for years.

Our experiments use a popular Ring alarm system. We have reported our findings to the Ring company but have not received any response.

The rest of the paper is organized as follows. Section II introduces the background of home alarm systems and their communication protocols. Section III describes the adversary model. Section IV presents techniques to localize the legitimate magnet and infer its polarity. Section V introduces techniques to eliminate legitimate alarms and also trigger false alarms by manipulating the magnetic field strength. Section VI details how to launch the battery-depletion attack. Section VII points out some countermeasures. Section VIII evaluates the attacks on commercial home alarm systems. Section IX briefs the related work. Section X concludes the paper.

II. Background

A. Reed Switch and Contact Sensor



(a) Reed switch (b) Contact sensor

Fig. 2. Examples of reed switches and contact sensors.

A Reed switch is a contactless electrical switch which is widely used as a proximity sensor to activate or deactivate a circuit. We can easily find reed switches in computers, alarms, and a lot of other appliances. Fig. 2(a) shows a reed switch used in a contact sensor. It contains two ferromagnetic contacts which are sealed in a small glass envelope filled with unreactive gas. If there is a strong magnetic field parallel to the contacts, the two contacts are magnetized and snap together. Then the current flows through the closed reed switch to activate the circuit. When the magnetic field disappears, the two contacts are separated from each other so that the reed switch deactivates the circuit.

The contact sensor is installed on the interior of a door, and the associated magnet is installed on the interior of a door

[2]One of the authors had to remotely disable a contact sensor with low battery during his vacation to avoid continuous warnings sent to his phone and the alarm company, which motivates this work.

frame as illustrated in Fig. 2(b). When the door is closed, the sensor and magnet are very close to each other, so the reed switch keeps closed. When the door is open, the sensor and magnet are separated, so the reed switch is open and triggers an OPEN alarm to notify the base station and/or the user's smartphone app. Since each contact sensor is powered by a battery, it is normally in the sleep mode and does not respond to or forward any packet to save energy. Only some specific events (e.g., door OPEN or CLOSE) can switch the sensor into the active mode to transmit and receive messages. Since contact sensors have very limited computing resources and can be easily reached by malicious signals outside the house, they are the weakest points in the home alarm system.

B. Home Alarm System Demystified

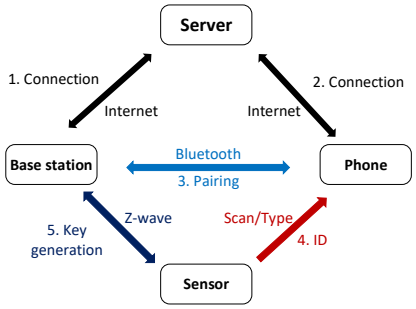


Fig. 3. The initialization of the Ring alarm system.

Most home alarm systems use low-power communication protocols such as ZigBee, Z-Wave, and Thread. This paper uses the Ring alarm system based on Z-Wave as an example, but our findings can be easily extended to home alarm systems based on other communication protocols. Z-Wave was developed by Zensys in 1999 targeting low-bandwidth communications between embedded devices such as security sensors, smart bulbs, controllers, and other home appliances. It can construct a mesh network composed of different home embedded devices. Z-Wave devices transmit on 868.42 MHz in Europe and both 908.4 MHz and 916 MHz in North America for different purposes. Z-Wave also uses Frequency-shift Keying (FSK) as the modulation method.

Now we describe the working principle of the Ring alarm system which normally consists of a base station, contact sensors, and range extenders. Contact sensors monitor the OPEN or CLOSE state of the door and report such events to the base station. The base station controls contact sensors in the range and reports events further to the user's smartphone and the alarm service company if any. It periodically broadcasts messages and is always ready to answer messages from contact sensors. After receiving an event from the contact sensor, the base station replies with an ACK. If no ACK is received in a certain period, the contact sensor retransmits the packet. The range extender serves as a signal repeater between the base station and sensors when they are far away from each other. In contrast to battery-powered contact sensors, the base station and range extenders are normally plugged to an outlet in the house, so they have no energy limitation when working.

Fig. 3 shows the system initialization steps of the Ring alarm system. The first step is to connect the base station to the Internet via Wi-Fi or Ethernet. Then the user installs a Ring app on the smartphone and also registers an account. The phone should keep the Bluetooth open for pairing with the base station. The user taps a button on the base station to start the pairing process. After the successful pairing, the user can manage the base station through the app. The fourth step is to add each contact sensor to the alarm system using the app. The user inputs each sensor ID to the system by scanning the QR code on the sensor using the smartphone. When the user installs the battery in the contact sensor, the sensor transmits a message to the base station to start the cryptographic key generation process. Based on the common initial key in firmware, the two devices generate two 128-bit keys for authentication and payload encryption, respectively. All the packets except the ACKs between the sensor and base station are encrypted using the 128-bit AES algorithm.

Fig. 4. The bar magnet.

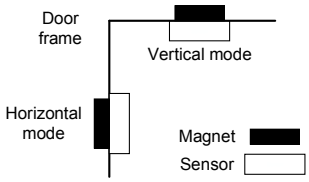


Fig. 5. Two installation modes of the contact sensor.

III. Threat Model

We consider a realistic threat model for alarm systems in daily life. The entire alarm system is installed inside the house, while attackers are outside and cannot physically access the devices. We do not consider attackers from the Internet who may hack the alarm service provider or the base station to disable the alarm system. These attacks deserve separate studies [6], [7]. Also, we assume that communications between devices are secure because the secret key is only known to the vendor. In our model, outside attackers use wireless signals to launch the attack in a short range.

There are three types of potential attackers. **Type-I** attackers want to open the door to illegally access the house without triggering any alarm. **Type-II** attackers do not want to enter the house but want to trigger false alarms just for fun. **Type-III** attackers want to quickly deplete the battery of a selected contact sensor without arousing the attention of the user, base station, or alarm service company if any. When the battery level of the contact sensor is below a threshold, a low-battery warning is periodically sent to the user's smartphone, the base station, and the alarm service company. If the user has no backup battery at home or is away from home, he usually just disables the involved contact sensor to avoid receiving too many low-battery warnings and also be able to activate other contact sensors. The door with the disabled sensor thus becomes the unguarded entry point into the house.

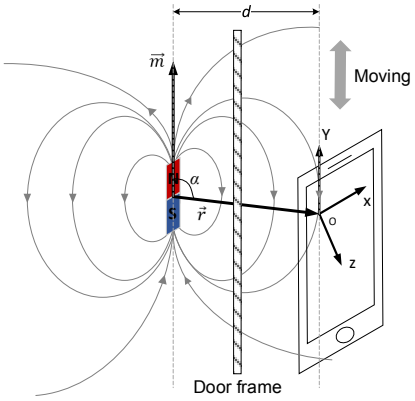


Fig. 6. Sensor localization using a smartphone.

IV. Inferring Location and Magnet Polarity of Contact Sensors

Outside attackers need to solve two challenges for a successful attack on the target door or window. First, they must infer the location of the contact sensor to launch the pinpoint attack. The magnetic field generated by the paired magnet is a good location indicator. Fig. 4 shows a bar magnet commonly used in alarm systems. The accuracy of localizing such a tiny magnet is critical to the success of the attack. Second, they need to determine the polarity of the magnet (the south or north magnetic pole), as incorrect magnet polarity may trigger unexpected alarms.

Attackers can localize the contact sensor by measuring the magnetic field generated by the legitimate magnet. The contact sensor and magnet are always installed in the horizontal or vertical mode on the door and frame, respectively, as illustrated in Fig. 5. In Fig. 6, the attacker moves his phone vertically along the door frame to collect the magnetic signal. O on the top left corner denotes the magnetometer's position in the smartphone. The magnetometer measures a 3-dimensional magnetic field vector (MFV) based on the phone's local coordinate system. According to the magnetic field theory, the MFV can be calculated as

$$H(\vec{r}) = \frac{K}{\|\vec{r}\|^3}\left[\frac{3\vec{r}(\vec{m}\cdot\vec{r})}{\|\vec{r}\|^2} - \vec{m}\right], \tag{1}$$

where K is a constant related to the magnetic moment which determines the magnetic strength of the magnet, $\overrightarrow{r} = (r_x, r_y, r_z)$ represents the 3D distance vector relative to the magnetometer, $\overrightarrow{m} = (m_x, m_y, m_z)$ is the directional unit vector of the magnet, and all the variables take values in the magnetometer's coordinate system shown in Fig. 6. Since K is approximately a constant for a given magnet, the measured MFV is only determined by the 3D relative position and orientation between the magnet and magnetometer.

When we move the phone along the frame, the bar magnet is always parallel with the smartphone, so the horizontal distance d and the vector $\vec{m} = (0, 1, 0)$ do not change. Therefore, the MFV only relates to vector $\vec{r}$, and its magnitude—called magnetic field strength (MFS)—is calculated as

$$\begin{aligned}\|H(\vec{r})\|^2 &= \frac{K}{\|\vec{r}\|^3}\left[\frac{3\vec{r}(\vec{m}\cdot\vec{r})}{\|\vec{r}\|^2} - \vec{m}\right]\cdot\frac{K}{\|\vec{r}\|^3}\left[\frac{3\vec{r}(\vec{m}\cdot\vec{r})}{\|\vec{r}\|^2} - \vec{m}\right] \\ &= \frac{K^2}{\|\vec{r}\|^6}\left[3\cos^2\alpha + 1\right].\end{aligned}$$

Since $\|\vec{r}\| = \frac{d}{\sin\alpha}$, we can substitute $\|\vec{r}\|$ and get

$$\|H(\vec{\alpha})\|^2 = \frac{K^2}{d^6}(4\sin^6\alpha - 3\sin^8\alpha),$$

where α is now the only variable in $\|H(\vec{\alpha})\|^2$. We then calculate the derivation as

$$(\|H(\vec{\alpha})\|^2)' = \frac{24K^2}{d^6}(\sin^5\alpha\cos^3\alpha).$$

We can see that $\|H(\vec{r})\|^2$ reaches the maximum when $\alpha = \pi/2$ and $\|\vec{r}\|$ reaches the minimum. So the phone can measure the maximum MFS when the magnetometer is in the same height with the magnet. Fig. 7 illustrates the MFS readings when we move the phone along the door frame at a uniform speed. The magnetometer reaches the same height with the magnet in the 60th sample. The experiment results are consistent with our above analysis. Note that we need to remove the background magnetic field from the readings before magnet localization.

After we know the position of the magnet, it is straightforward to infer its polarity. We just need to place the phone along the door frame in the same height with the legitimate magnet and check the y-axis reading of the MFV. If the reading is negative, the south pole is at the bottom of the magnet, or the north pole is at the bottom.

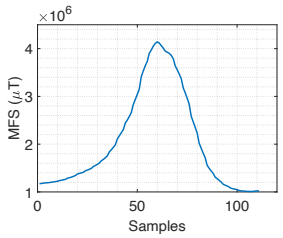
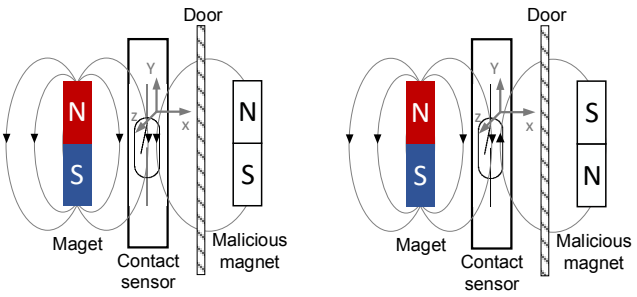


Fig. 7. MFS collected when moving magnetometer at a uniform speed.

V. Event Eliminating and Spoofing

Now we present two attacks to manipulate the reactions of contact sensors to the OPEN or CLOSE action. From Section II-A, the reed switch changes its state when the MFS along the contacts falls below or exceeds a threshold. So our basic idea is to influence the magnetic field along the reed switch in the contact sensor using a malicious magnet. The attacker can launch the event-eliminating attack to disable the contact sensor which then does not raise an alarm when the attacker opens the corresponding door. In addition, the attacker can use the event-spoofing attack to trigger false alarms, though the door stays closed.



(a) Event eliminating (b) Event spoofing

Fig. 8. Event eliminating and spoofing illustration.

A. Event-Eliminating Attack

The event-eliminating attack can enable the attacker to open the door "quietly" without triggering any alarm. In Fig. 8(a), the attacker moves a malicious magnet of the same polarity as the legitimate one around the contact sensor. The magnetic field vectors of the two magnets are approximately in the same direction when passing the reed switch, so the two magnetic fields are constructive to each other. At this time, if the attacker opens the door and separates the legitimate magnet from the sensor, the sensor (reed switch) reports nothing as long as the malicious magnet keeps the MFS along the reed switch above the default system threshold.

We now introduce the requirement for the malicious magnet to successfully disable the contact sensor. The contact sensor and the legitimate magnet in Fig. 8(a) are installed in the horizontal mode. To generate MFV that is parallel to the reed switch in the sensor, the attacker also needs to place the malicious magnet horizontally. The strength of the magnet that the attacker needs to generate the MFS above the threshold is related to the 3D distance $\vec{r}$ and orientation $\vec{m}$ of the magnet relative to the reed switch. Given the local coordinate system in Fig. 8(a), let (x, y, z) denote the position of the malicious magnet. Then we can get $\vec{r} = (-x, -y, -z)$ and $\vec{m} = (0, 1, 0)$. So the y-axis component H_y of the MFV that is generated by the malicious magnet along the reed switch can be written as

$$H_y = \frac{K(2y^2 - x^2 - z^2)}{(x^2 + y^2 + z^2)^{5/2}}. \tag{2}$$

Assuming that the magnetic strength threshold to change the reed switch's state is η, we can have

$$|H_y + E_y| > \eta,$$

where E_y is the y-axis component of the background MFV. This means that in addition to preserving certain orientation, the attacker needs a malicious magnet with a constant K, which depends on η, E_y, and the estimated location (x, y, z) of the malicious magnet relative to the sensor. Considering the above factors, the attacker can find an acceptable malicious magnet to launch the event-eliminating attack.

B. Event-Spoofing Attack

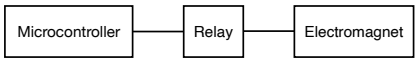
In addition to eliminating legitimate OPEN events, attackers can generate fake OPEN alarms using the malicious magnet. In Fig. 8(b), the attacker moves a malicious magnet of the opposite polarity close to the legitimate magnet and contact sensor. As the magnetic field generated by the malicious magnet is destructive to that of the legitimate magnet, the MFS at the reed switch decreases. If the MFS falls below the system threshold, the sensor triggers an OPEN alarm while the door is still closed. We assume that the y-axis component of the MFV generated by the legitimate magnet at the reed switch is $H_y^{'}$. To change the state of the reed switch, the malicious magnet should be able to generate an MFV with the y-axis component H_y satisfying $|H_y + H_y^{'} + E_y| < \eta$, where H_y and $H_y^{'}$ have different signs. If too many false alarms are generated, the user normally considers the contact sensor faulty and temporarily disables it until a technician comes for onsite diagnosis, which may take a few days. During the waiting period, the door with the disabled sensor becomes a vulnerable intrusion point.

VI. Battery-Depletion Attack

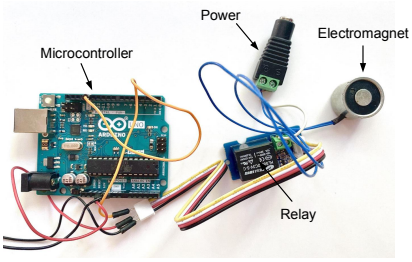
Each contact sensor is powered by a small battery which is expected to last a few years with the low-power communication protocols like Z-Wave. In this section, we present a battery-depletion attack that can deplete the sensor battery quickly and stealthily. The basic idea is to use an advanced event-spoofing attack to force the sensor to continuously generate and report a large amount of fake OPEN or CLOSE events without arousing the attention of the user, base station, or alarm service company. A contact sensor with a low battery level would periodically send low-battery warnings to the base station, the user's smartphone, and the alarm service company. To avoid receiving too many low-battery warnings pushed by the involved contact sensor, the user often chooses to temporarily disable the contact sensor. It may take the user many days to replace the dead battery, as he may not have a backup one at home or may be even on travel. So the attacker would have a longer time window to illegally enter the victim's home through the affected door.

A. Automatic Event Spoofing using an Electromagnet

In Section V-B, we use a permanent magnet to manually generate fake OPEN events. It is, however, impractical to



(a) The block diagram



(b) The circuit

Fig. 9. The system for the battery-depletion attack.

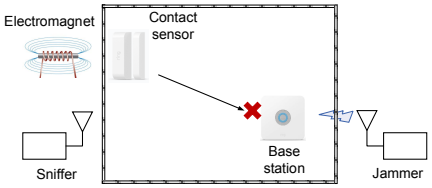


Fig. 10. Battery-depletion attack.

generate a large amount of events to deplete the battery in a short period. To enable automatic event spoofing, we design a system that can generate magnetic signals automatically to control the reed switch's state, as illustrated in Fig. 9. The microcontroller can be programmed to generate the ON-OFF square wave which is then used by the relay to control the power supply to the electromagnet. In the ON state, the current goes through a coil of copper wire in the electromagnet and creates a magnetic field; in the OFF state, the electromagnet is turned off to make the magnetic field disappear. In this way, the attacker can trigger the contact sensor to generate OPEN or CLOSE events with any time interval.

B. Stealthy Battery Depletion with Jamming

To deplete the sensor battery, attackers need to trigger the contact sensor to generate a large amount of OPEN or CLOSE events which are normally immediately reported to the base station, the user's smartphone, and the alarm service company. Abnormal alarms during a certain period would arouse the attention of the user and alarm service company. Therefore, it is necessary for the attacker to jam the channel between the sensor and base station to achieve quick and stealthy battery depletion, as shown in Fig. 10.

The reactions of contact sensors to jamming signals depend on the MAC (medium access control) protocol and the specific system implementation. If the system adopts CSMA (carrier-sense multiple access), the sensor waits for a clear channel after detecting the high energy noise before transmitting and may abandon the packet if the channel is always noisy in a certain duration. In contrast, if no CSMA strategy is used in the system, the sensor keeps transmitting regardless of jamming signals in the channel. The contact sensor is not programmable, and the vendor does not want to disclose implementation details. So it is difficult for attackers to infer the specific MAC strategy used in the alarm system when jamming signals exist. Therefore, we aim to devise a generic attack that can work on most alarm systems which may or may not use the carrier-sense MAC strategy. Also, attackers should be able to observe the triggered packets from the contact sensor during jamming so that they can evaluate the effect of the attack in real time.

To achieve the above goals, the attack in Fig. 10 should meet three requirements. First, the base station cannot decode the packets from the contact sensor to keep the user and the alarm service provider unaware of the ongoing attack. Second, the noise energy level should be below a threshold so that the sensor can keep transmitting to consume energy even if it uses the carrier-sense MAC strategy. Finally, the attacker's sniffer can decode the packets from the sensor, so the SNR at the sniffer should not be too low. So we need to put the jammer as close as possible to the base station and as far as possible from both the targeted contact sensor and the sniffer.

The attacker achieves the above goals in two steps. **First**, the attacker walks around the house with a handheld sniffer to measure the signals broadcast by the base station around doors and windows.[3] The contact sensor around the location with the minimum signal strength is considered the farthest away from the base station and chosen as the targeted sensor to attack; the sniffer is finally placed there as well. Also, the location with the maximum signal strength is considered closest to the base station and is chosen as the jammer's location. **Second**, the attacker gradually decreases the jammer's transmission power from the maximum until the sniffer can receive packets from the sensor, which indicates that the sensor starts to consume energy. If the attacker continues decreasing the jamming power, the base station may start to respond with an ACK; the previous jamming power level is thus chosen as the optimal one. The attacker can use a non-optimal power level which costs him more energy without triggering any alarm; or he can use the optimal power level with less energy consumption while triggering one or a few alarms. In the latter case, the attacker may wait sufficiently long before proceeding to the next step; in this way, one or a few alarms may be mistaken for accidental system faults by the user or alarm service company.

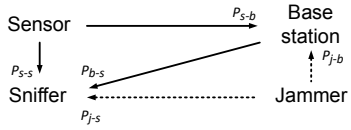


Fig. 11. Power of received signals in battery-depletion attacks.

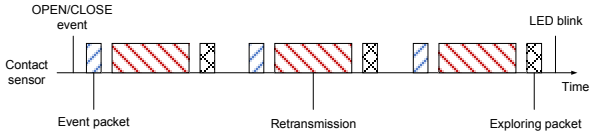


Fig. 12. Retransmission when no ACK is received from the base station.

We now prove that the above methods can attack the system stealthily. In Fig. 11, the sniffer is close to the contact sensor, and the jammer is close to the base station. P_{s-s}, P_{b-s}, and P_{j-s} represent the power of signals received by the sniffer from the contact sensor, base station, and jammer, respectively. P_{s-b} and P_{j-b} represent the power of signals received by the base station from the contact sensor and jammer, respectively. Then we can calculate SNR at the sniffer as $\text{SNR}_{s-s} = \frac{P_{s-s}}{P_{j-s}}$ and $\text{SNR}_{b-s} = \frac{P_{b-s}}{P_{j-s}}$ for the signals from the sensor and base station, respectively. Also, the SNR at the base station can be calcuated as $\text{SNR}_{s-b} = \frac{P_{s-b}}{P_{j-b}}$. According to relative positions, we can know $P_{j-b} > P_{j-s}$, $P_{s-s} > P_{s-b}$, and $P_{s-b} \approx P_{b-s}$.

[3] A drone can be used for this purpose as well.

As a result, we can get $\text{SNR}_{s-s} > \text{SNR}_{b-s} > \text{SNR}_{s-b}$. Now we can draw two conclusions. First, when the attacker's sniffer starts to receive packets from the contact sensor, the base station can decode nothing. Second, once the base station can decode packets from the contact sensor, the sniffer must know that by decoding the ACK from the base station.

After determining the optimal jamming power, the attacker uses the programmed circuit and the retransmission strategy to trigger the contact sensor to transmit as many event packets as possible. Fig. 12 illustrates the retransmission strategy used in the Ring alarm system. When an OPEN or CLOSE event is triggered, the contact sensor first transmits a packet to report the event. Then it retransmits the original packet eight times if no ACK is received from the base station in a specific period. If still no ACK is returned, it transmits an exploring packet to indicate that it may have lost connection with the base station. The contact sensor repeats the whole process three times, and the LED light blinks after the sensor finishes the whole retransmission process. It takes the sensor about 18 seconds to transmit all the 30 packets in the retransmission process. So we let the microcontroller automatically change the ON-OFF state of the electromagnet every 18 seconds to induce the energy-consuming retransmission process. The battery of the contact sensor failed in 43 hours in contrast to the expected battery lifetime of a few years.

With the presence of jamming signals, the base station cannot receive any event report from any sensor instead of just the one targeted by the attacker. Since the user may notice missing events from the sensor on his smartphone, the attacker can launch the attack in multiple noncontinuous periods, e.g., at late night or when the user is not at home.

VII. Defenses

We can have the following countermeasures to thwart the above attacks. First, the attacks are based on the reed switch's vulnerability that it cannot differentiate the MFS changes caused by the real OPEN or CLOSE action from the attacker's interference. Therefore, we can add an accelerometer to the contact sensor to detect the continuous OPEN or CLOSE action. In particular, we assume that the accelerometer is static and that the reed switch is in the CLOSE state at t_1. After a time delay δ, the reed switch transfers to the OPEN state. We can calculate the sensor's displacement as $\vec{D} = \int_{t_1}^{t_1+\delta} \vec{v}(t)dt = \int_{t_1}^{t_1+\delta} \int_{t_1}^{t_v} \vec{a}(t_a)dt_a dt_v$, where $\vec{v}(t)$ and $\vec{a}(t)$ denote the sensor's speed and acceleration at time t. Since the displacement is very small, the sensor-magnet distance $d_{\text{s-m}} \approx \|\vec{D}\|$. We claim that the sensor has been separated from the magnet if $d_{\text{s-m}}$ exceeds a critical value that determines the reed switch's state change. If the reed switch triggers an OPEN event while the accelerometer cannot detect the corresponding action, the event may be fake. If the reed switch does not trigger any event while the accelerometer detects the action, an event may have been eliminated by attackers.

Second, the attacker cannot launch the attacks stealthily if the base station can detect the jamming signals. There are some techniques [8], [9] to detect continuous jamming signals.

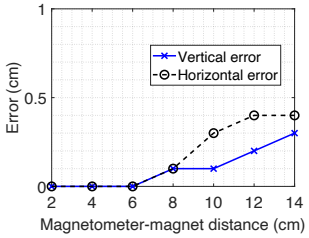


Fig. 13. Magnet-localization error.

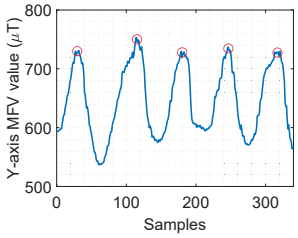


Fig. 14. Threshold η that changes the reed switch's state.

One simple solution is that the base station continuously monitors the energy level in the frequency range. In each time period, if the base station detects a large percentage of time with the energy level above a threshold, there can be an ongoing jamming attack. This defense can limit the impact of the attack but would fail if the attacker knows the jamming-detection parameters of the system.

VIII. Evaluation

In this section, we evaluate the efficacy of the proposed attacks with a popular Ring home alarm system.

A. Localization Accuracy

We use iPhone 6S as a magnetic signal detector to localize the legitimate magnet paired with the contact sensor. The magnetometer in iPhone 6S is 2.2 cm from the left frame and 1.6 cm from the upper frame. In addition, the Ring system uses a 3 cm $\times$ 0.35 cm $\times$ 0.8 cm bar magnet in the contact sensor illustrated in Fig. 4.

We first evaluate the horizontal and vertical localization accuracy of the magnet with different distances between the reed switch in the contact sensor and the magnetometer in the phone, as shown in Fig. 13. For each distance configuration, we measure the magnet's position three times and then calculate the average. We get localization errors of under 0.5 cm for all the distance settings and higher precision when the magnetometer is close to the magnet. Then we test the localization accuracy when there is a plank of 3.2 cm thick acting as a window or door between the magnet and magnetometer. We get localization errors of 0.1 cm for both horizontal and vertical accuracy. Therefore, the wood material between the magnetometer and magnet has little impact on the localization error.

B. Event-Eliminating and Event-Spoofing Attacks

We now evaluate the MFS threshold η that changes the reed switch's state because η is used to find acceptable malicious magnets in both event-eliminating and event-spoofing attacks. We measure η by attaching the reed switch to the magnetometer along the y-axis and then use a bar magnet to trigger the reed switch. The bar magnet is placed parallel to the reed switch as illustrated in Fig. 8(a) so that it can generate the MFV along the y-axis.

Fig. 14 illustrates the y-axis MFV component generated by the bar magnet at the reed switch. Initially, the magnet is far

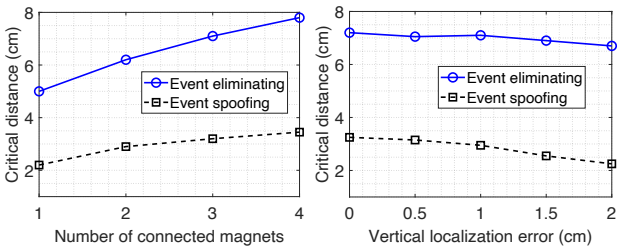


Fig. 15. Critical distance with magnets of different strength.

Fig. 16. Critical distance with localization errors.

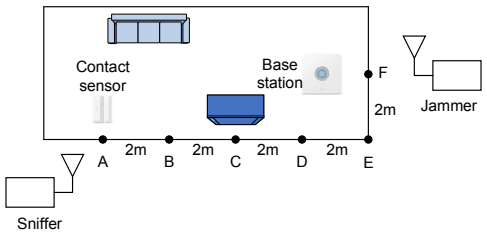


Fig. 17. Experiment scenario for the battery-depletion attack.

away from the reed switch; so the reading is small, and the reed switch is open. Then we move the magnet close to the reed switch until hearing a click which indicates that the two contacts have snapped together. At this time, the y-axis reading of the magnetometer reaches the maximum which represents the threshold η as the red circle in Fig. 14. When we move the bar magnet away, the reading decreases, and the contacts are separated from each other. We repeat the above process six times and get an average threshold $\eta = 735.74\ \mu T$. We also use a magnet with an opposite polarity and get an average threshold $\eta = 696.7\ \mu T$. The difference may be caused by measurement errors. When we place the bar magnet vertical to the reed switch, it cannot activate the reed switch because it cannot generate the MFV parallel to the reed switch.

We also evaluate the critical distance between the reed switch and malicious magnets of different strength to change the state in both event-eliminating and event-spoofing attacks. In particular, we build magnets of different strength by connecting different numbers of cylinder magnets together. As demonstrated in Fig. 15, the distance increases with the strength of the magnet so that the stronger magnet can interfere with the reed switch from a position farther away. Fig. 15 also shows that in the event-spoofing attack, the malicious magnet needs to be closer to the reed switch to cause its state changes, as the malicious magnet needs to generate a stronger magnetic field to offset the one generated by the legitimate magnet. This means that the required magnetic strength for the reed switch's state change is low, but the cost to offset the legitimate magnetic field is high.

We then evaluate the impact of the sensor localization error on the critical distance. Fig. 16 shows that the critical distance in both event-eliminating and event-spoofing attacks decreases slowly with the localization error. Therefore, the attacker needs to bring the malicious magnet closer to generate a stronger magnetic field when he cannot determine the sensor's location accurately. Also, the small errors in Fig. 13 have little impact on the critical distance. Similar to Fig. 15, the critical distance in event-spoofing attack is smaller as well.

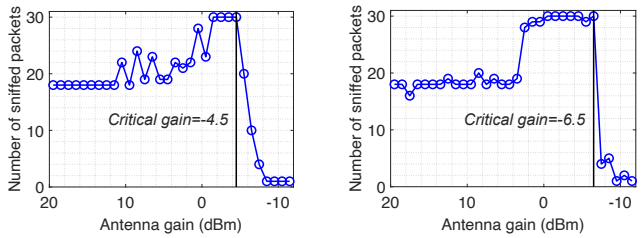
C. Battery Depletion Attack

We evaluate the battery depletion attack with a fully furnished 10 m $\times$ 4 m apartment room as illustrated in Fig. 17. Initially, the base station is close to position F, and the target contact sensor is close to position A. We use a USRP N210 as the jammer to transmit Gaussian noise in the same Z-Wave communication frequency. The actual distance between the base station and the jammer is about 2 meters. We use a commercial Z-Wave Toolbox [10] as a sniffer which is placed close to position A to measure the communication between the contact sensor and base station.

We first set both the jammer's initial transmission power and antenna gain to its maxima. Then, we decrease the jammer's antenna gain gradually and monitor the number of packets transmitted by the contact sensor when triggering an OPEN event, as illustrated in Fig. 18(a). At the beginning, only the sniffer can receive the packets because it is far away from the jammer. Note that the sensor transmits 30 packets if no ACK is received from the base station, but the sniffer only receives about 18 packets. The sniffer may fail to decode the rest packets because of low SNR or because the sensor may not transmit when detecting high energy in the channel. With the decrease of the antenna gain, the sniffer starts to receive more packets from the sensor with a maximum of 30. When the antenna gain falls below -4.5 dBm in Fig. 18(a), the base station starts to receive packets from the sensor after a few retransmissions. When the antenna gain is even lower, the communication between the base station and contact sensor returns to normal.

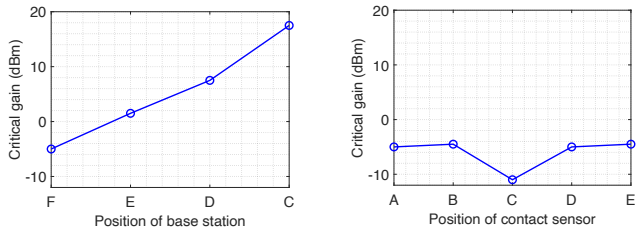
We use the *critical gain* to represent the minimum gain that can interrupt the communication between the sensor and base station. For example, the critical grain in Fig. 18(a) is -4.5 dBm. All the critical gains in the range of [-4.5, 20] dBm are feasible to launch the battery-depletion attack without alarming the base station. The critical gains between [-4.5, -1.5] are optimal because the attacker can trigger the sensor to generate more packets with less energy. We can observe similar results in Fig. 18(b) when CLOSE events are triggered. When the antenna gain is set to the optimal range, we can deplete the sensor battery in about 43 hours.

We also evaluate the impact of the relative positions of the jammer, base station, and contact sensor. From Fig. 19(a), we can see that the critical gain increases when we move the base station away from the jammer and keep others unchanged. Therefore, it is important to place the jammer close to the base station to achieve good jamming performance. Fig. 19(b) illustrates the critical gain when we move the contact sensor and sniffer close to the jammer and keep the base station in position A. We can see that the change of critical gain is very small when the relative position between the base station and



(a) (b)

Fig. 18. (a) Number of packets transmitted by the sensor when the attacker triggers an OPEN event. (b) Number of packets transmitted by the sensor when the attacker trigger a CLOSE event.



(a) (b)

Fig. 19. Critical gain (a) when moving the base station away from the jammer and (b) when bringing the contact sensor close to the jammer.

jammer is fixed. The channel between position C and position F is almost blocked by a piece of metal furniture, so the critical gain is low when the sensor is in position C.

IX. Related Work

This section first discusses some most germane work on the security of smart home devices including home alarm systems. Then we introduce some prior work on battery-depletion attacks and jamming attacks in wireless sensor networks (WSNs).

There are some attacks on home IoT systems using RF techniques. Picod *et al.* [11] presented a software-defined radio framework *Scapy* for packet manipulation and security assessment and test it in a Z-Wave network. Lamb [2] proposed jamming and replay attacks to eliminate legitimate alarms and cause false alarms for multiple home alarm systems. Fouladi and Ghanoun [3] used a flaw in Z-Wave protocol to reset the encryption key to a chosen value so that the attacker can inject unauthorized commands. In [12], the authors launched a sinkhole attack by deploying a malware to a legitimate device of a home Zigbee network. Rouch *et al.* [4] and Fuller and Ramsey [5] designed techniques to inject a fake controller (base station) to the network to control home IoT devices. Badenhop *et al.* [13] provided attacks on routing protocols of Z-Wave networks. None of the above work considers possible attacks utilizing magnetic interference with the reed switch in home IoT systems.

The access point in the home IoT system also provides opportunities for attackers. After gaining access, the attacker may control the whole network. Crowley *et al.* [6] found several vulnerabilities that expose sensitive information from a Z-Wave gateway controller. By using these vulnerabilities, the attacker can create a backdoor account on the gateway. Barcena and Wueest [7] poisoned the gateway Address Resolution Protocol to redirect gateway firmware update requests to their own malicious server. After modifying the firmware, the gateway receives the malicious firmware as a legitimate update giving the attacker full control.

There are also some research on protecting smart home devices. Homonit [14] monitored the encrypted network traffic to detect anomaly for Samsung SmartThings. Brown *et al.* [15] jammed unsolicited messages for a home automation system without impairing legitimate transmissions in neighbouring houses. We can find some countermeasures for the packet injection attack on Z-Wave in [16].

Battery-depletion attacks have received attention in WSNs. In [17], the authors presented routing-layer attacks which exhaust energy by specifying far longer routing paths and forcing packet processing at remote network positions. Ghost-in-ZigBee [18] depletes nodes' energy in a ZigBee network by constructing bogus messages to lure nodes to do superfluous security-related computations. Raymond *et al.* [19] analyzed the effects of Denial-of-Sleep attacks in WSNs by considering the attacker's knowledge about the MAC protocol. In contrast, since the packets are triggered by reed switches in the home alarm network, we use magnetic signals to interfere with the reed switch to generate more communications and deplete the sensor battery.

There is also extensive research [9] on jamming techniques and countermeasures in WSNs. Xu *et al.* [20] studied the feasibility of launching and detecting jamming attacks at the MAC layer. Li *et al.* [21] investigated the optimal jamming and defense techniques under energy constraints in WSNs. We jam the base station from the physical layer so that the alarm service provider and the system user are unaware of the battery-depletion attack.

X. Conclusion

In this paper, we presented new attacks targeting home alarm systems by using malicious magnetic signals to interfere with the reed switch commonly employed in the alarm sensor. By generating specific magnetic signals, the attacker can eliminate the legitimate alarms and cause false alarms. We also demonstrated a new attack to successfully and stealthily deplete the alarm sensor's battery in 43 hours in contrast to the expected lifetime of a few years. In addition, we provided potential countermeasures against the attacks. Extensive experiments with a popular Ring alarm system confirmed the efficacy of our attacks. We have reported our findings to the Ring company but have not received any response.

XI. Acknowledgement

This work was supported in part by the US National Science Foundation under grants CNS-1933069, CNS-1824355, CNS-1619251, CNS-1933047, CNS-1718078, and CNS-1651954 (CAREER).

REFERENCES

[1] "Home security system market." [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/home-security-system-market-205573901.html.

[2] L. Lamb, "Home insecurity: No alarms, false alarms, and sigint," in *Black Hat USA*, Las Vegas, NV, Aug. 2014.

[3] B. Fouladi and S. Ghanoun, "Security evaluation of the z-wave wireless protocol," in *Black Hat USA*, Las Vegas, NV, July 2013.

[4] L. Rouch, J. François, F. Beck, and A. Lahmadi, "A universal controller to take over a z-wave network," in *Black Hat Europe*, London, United Kingdom, Dec. 2017.

[5] J. Fuller and B. Ramsey, "Rogue z-wave controllers: A persistent attack channel," in *IEEE LCN*, Clearwater Beach, FL, Oct. 2015.

[6] D. Crowley, D. Bryan, and J. Savage, "Home invasion v2.0-attacking network-controlled hardware," in *Black Hat USA*, Las Vegas, NV, July 2013.

[7] M. Barcena and C. Wueest, "Insecurity in the internet of things," *Security Response*, Mar. 2015.

[8] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: a survey," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, Dec. 2014.

[9] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, Dec. 2009.

[10] "Z-wave toolbox." [Online]. Available: https://www.zwaveproducts.com/products/zwp-tbx-z-wave-toolbox.

[11] J. Picod, A. Lebrun, and J. Demay, "Bringing software defined radio to the penetration testing community," in *Black Hat USA*, Las Vegas, NV, Aug. 2014.

[12] L. Coppolino, V. DAlessandro, S. DAntonio, L. Levy, and L. Romano, "My smart home is under attack," in *IEEE CSE*, Porto, Portugal, Oct. 2015.

[13] C. Badenhop, S. Graham, B. Ramsey, B. Mullins, and L. Mailloux, "The z-wave routing protocol and its security implications," *Computers & Security*, vol. 68, pp. 112–129, July 2017.

[14] W. Zhang, Y. M. Y. Liu, X. Zhang, Y. Zhang, and H. Zhu, "Homonit: Monitoring smart home apps from encrypted traffic," in *ACM CCS*, Toronto, Canada, Oct. 2018.

[15] J. Brown, brahim Bagci, A. King, and U. Roedig, "Defend your home! jamming unsolicited messages in the smart home," in *ACM HotWiSec*, Budapest, Hungary, Apr. 2013.

[16] J. Fuller, B. Ramsey, M. Rice, and J. Pecarina, "Misuse-based detection of z-wave network attacks," *Computers & Security*, vol. 64, pp. 44–58, Oct. 2017.

[17] E. Vasserman and N. Hopper, "Vampire attacks: draining life from wireless ad hoc sensor networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 318–332, Feb. 2011.

[18] X. Cao, D. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, "Ghost-in-zigbee: Energy depletion attack on zigbee-based wireless networks," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 816–829, Oct. 2016.

[19] D. Raymond, R. Marchany, M. Brownfield, and S. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network mac protocols," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 1, pp. 367–380, Jan. 2009.

[20] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *ACM MobiHoc*, Urbana-Champaign, IL, May 2005.

[21] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attack strategies and network defense policies in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 8, pp. 1119–1133, Aug. 2010.