Journal of Medical Systems (2020) 44: 29
https://doi.org/10.1007/s10916-019-1489-9

MOBILE & WIRELESS HEALTH

Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles

Sibi Chakkaravarthy Sethuraman[1] · Vaidehi Vijayakumar[1] · Steven Walczak[2]

Received: 25 August 2018 / Accepted: 17 October 2019 / Published online: 14 December 2019

Abstract

The growing use of wireless technology in healthcare systems and devices makes these systems particularly open to cyber-based attacks, including denial of service and information theft via sniffing (eaves-dropping) and phishing attacks. Evolving technology enables wireless healthcare systems to communicate over longer ranges, which opens them up to greater numbers of possible threats. Unmanned aerial vehicles (UAV) or drones present a new and evolving attack surface for compromising wireless healthcare systems. An enumeration of the types of wireless attacks capable via drones are presented, including two new types of cyber threats: a stepping stone attack and a cloud-enabled attack. A real UAV is developed to test and demonstrate the vulnerabilities of healthcare systems to this new threat vector. The UAV successfully attacked a simulated smart hospital environment and also a small collection of wearable healthcare sensors. Compromise of wearable or implanted medical devices can lead to increased morbidity and mortality.

Keywords Mobile healthcare · Cyber threats · Drone · Body area network (BAN) · Implantable medical device (IMD) · Unmanned aerial vehicle (UAV)

Introduction

The healthcare industry, including providers and manufacturers, is embracing wireless technology. Wireless systems enable a cleaner and more mobile approach to healthcare information systems. However, due to the focus on patient wellbeing, wireless medical systems often have few or limited security features [1]. One wireless healthcare technology that has been advancing rapidly and enabling improved quality of care is mobile healthcare systems.

Mobile healthcare technology is rapidly advancing and providing improved outcomes across a wide range of economic and geographic backgrounds [2, 3]. Body area networks (BAN), such as Fitbits, pulse oximeters, and wearable blood pressure monitors [4], and implantable medical devices (IMD), such as insulin pumps and pacemakers, utilize wireless technology and are joining the growing number of devices associated with the Internet of Things (IoT). IMDs are currently available to assist in the treatment of numerous chronic conditions including: heart disease, diabetes, chronic pain, hearing loss, and sleep apnea [5]. An estimated 110 million wearable medical computing devices will be purchased in 2018 in the USA alone, with the number expected to increase significantly in the future due to ubiquitous Internet and ever-increasing healthcare needs of the population and information needs of medical providers [6, 7]. The term wearable IoT (WIoT) has been introduced to recognize the growing presence of this type of device in the IoT space.

Medical WIoT enables multiple benefits, including: rapid and comprehensive collection of medical data, and remote monitoring and treatment of chronic medical conditions [8–10], which can save patients time by reducing the need to be onsite for medical care as well as improve medical service delivery in areas with limited or low medical infrastructure [11]. However, the use of wireless technology to transmit medical data opens these devices up to potential cyber attacks [12, 13].

This article examines specific cyber threats to medical systems conducted using unmanned aerial vehicles (UAVs), more

This article is part of the Topical Collection on *Mobile & Wireless Health Provided*

✉ Steven Walczak
swalczak@usf.edu

[1] Vellore Institute of Technology, Amaravati, India

[2] School of Information & Florida Center for Cybersecurity, University of South Florida, 4202 E. Fowler Ave., CIS 1040, Tampa, FL 33620, USA

commonly called drones. A particular emphasis is focused on UAV cyber attacks against WIoT medical devises including BAN and IMD. Besides their military, government, and law enforcement uses for surveillance [14, 15], UAVs are widely used by hobbyists for entertainment purposes [16]. Recently, various organizations have announced potential product delivery via UAV [17] and this delivery method is a mechanism for improving pharmaceutical and other medical device delivery in remote areas [18]. Therefore, it can be reasonably expected that the presence of small UAVs will become ever more commonplace [19], enabling hostile UAVs to go unnoticed.

Background

Cyber attacks against medical devices have been widely researched. Attacks against BAN and IMD may be classified as either system attacks, including denial of service (DoS) attacks and other attacks corrupting the functionality of the system, and information attacks, which seek to obtain confidential medical data or alter the data [20, 21]. Data alteration may be accomplished by spoofing, which causes the sensor to accept an outside signal as part of the IMD system.

The most common form of attack against BAN and IMD type devices is an acoustic attack that uses ultrasonic or other audio frequencies at the resonant frequencies of WIoT devices to attack the devices [22]. Acoustic attacks have been shown to work against implanted cardiac defibrillators and pacemakers [23–25], insulin pumps [21, 26, 27], and activity monitors [28], among other medical devices. These attacks can acquire confidential medical information, alter information causing system malfunctions and delivery of inappropriate therapies, and cause the BAN or IMD to lose power so as to become unusable [29]. These attacks can be carried out inexpensively as shown by [28], who claim to be able to inject fake steps into a Fitbit using a US$5 speaker.

Security for BAN medical devices and IMD is a long standing issue, with many organizations providing various security measures [30]. Common security methods for BAN include encryption and biometric multi-factor authentication, however some controversy exists as these security protocols may limit necessary access to medical data during an emergency [23].

Cyber attacks using UAVs

As shown in the previous section, cyber attacks against medical BAN and IMD are possible. UAVs are an ideal platform for wireless and IoT cyber attacks due to their small size and ease of access over difficult or secured terrain [31]. Theoretically, a UAV could hover over a hospital or medical clinic and conduct malicious cyber attacks. Hence, UAVs carrying cyber attack tools pose a severe threat to medical devices since they can evade physical security controls and penetrate the target's territory surreptitiously to perform an attack with high precision. The theory behind developing UAV-based cyber attacks is reported in [32].

This article explores existing wireless network and device based attacks using UAVs with a practical demonstration of such attacks. The common attacks performed using the UAVs against the healthcare devices are specified in the following subsections.

Deauthentication attack

A deauthentication attack is a form of distributed DoS attack. This attack can be performed in two ways:

1) Against the authenticated Clients: The attacker sends a series of deauthentication frames to the clients requesting the clients to disconnect from the access point (AP).
2) Against the AP: The attacker sends a series of deauthentication packets to the AP to re-authenticate all the connected clients. This handshake takes place between legitimate clients and AP through re-authentication. This attack is launched to disconnect all of the connected clients [33].

Stepping stone attack

The stepping stone attack is an attack that uses multiple hosts (in this case UAVs) to launch an attack against the target. Figure 1 illustrates the stepping stone attack using multiple UAVs. The attacker initiates the UAV network connected to each other through a mobile hotspot. Next, the attacker sends the attack command as a request to the UAV which is directly connected to him. The attack request is forwarded through the intermediate UAVs (hops) until it reaches the destination UAV which is nearest to the target system. Once the target UAV receives the command from the attacker, it begins the attack on the target and returns any response data to the attacker via the intermediate hops or stores the response data in cloud storage.

Drone-in-the-middle (DitM) attack

The UAV or drone-in-the-middle (DitM) attack is used to take over the communication path between two devices, intercepting and re-directing all communications. Figure 2 illustrates the DitM attack. In the case of BAN and IMD, the target is the actual device and the Wi-Fi router would be replaced by the device's data receiver.

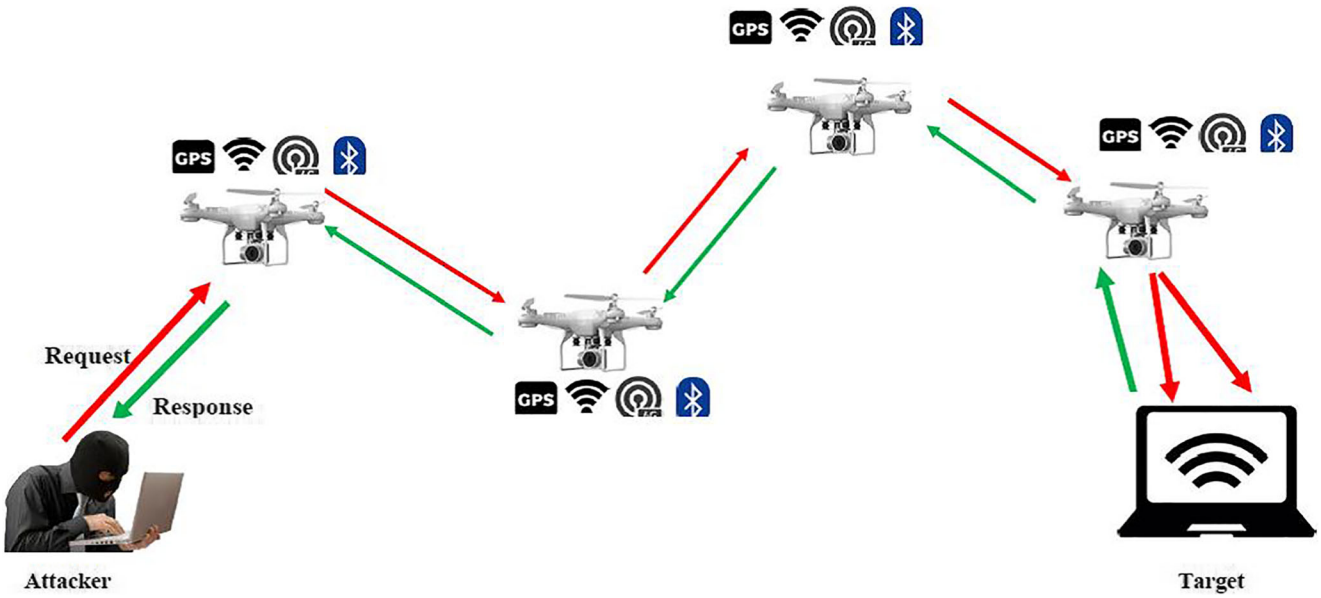


Fig. 1 Stepping stone attack using multiple UAVs

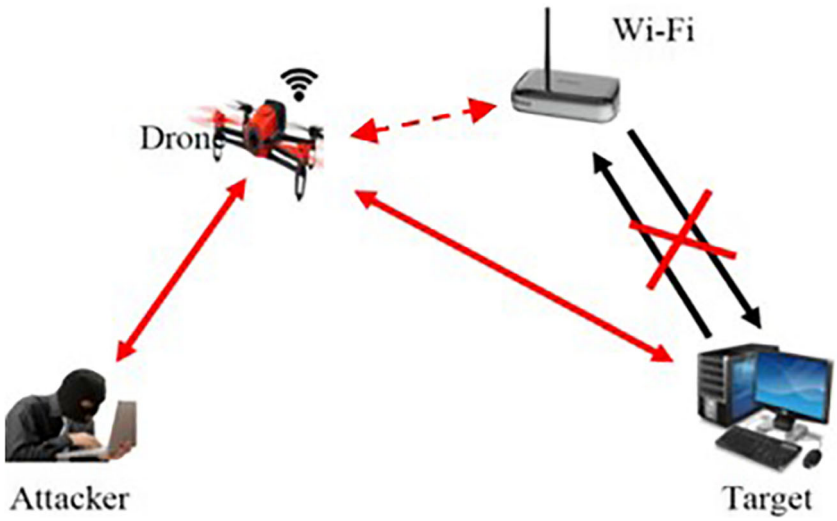
Cloud assisted UAV attack

Most of the UAV in today's market are designed with sophisticated capabilities including IoT, sensor cloud, and cloud. The UAVs with cloud capabilities are used by the attacker to store the hacked data remotely, so that the attacker can acquire the data at the time and location of his choosing. Generally, the data packets generated in the wireless network are huge and requires complex computation to retrieve vital information. UAVs with basic storage and limited battery backup cannot perform these complex computations. In order to avoid the storage burden and extend battery life, cloud assisted UAVs can be deployed, so that the data can be moved easily to the cloud with minimal battery usage (as shown in Fig. 3).

Evil twin attack

Evil twin attack (as shown in Fig. 4) is similar to a DitM attack, but instead of the UAV inserting itself into the middle of a data stream, it takes over as the receiver for the BAN or IMD. The evil twin attack is performed in two different phases. Initially, the attacker creates the deauthentication probes to deauthenticate the clients connected to the legitimate AP. Next, the attacker masquerades as the legitimate AP by launching a fake access point (spoofing the MAC address, reallocating the legitimate AP channels, and broadcasting the SSID) [33]. Finally, the clients are forced to re-authenticate with the UAV acting as the AP.

Fig. 2 UAV in the Middle attack



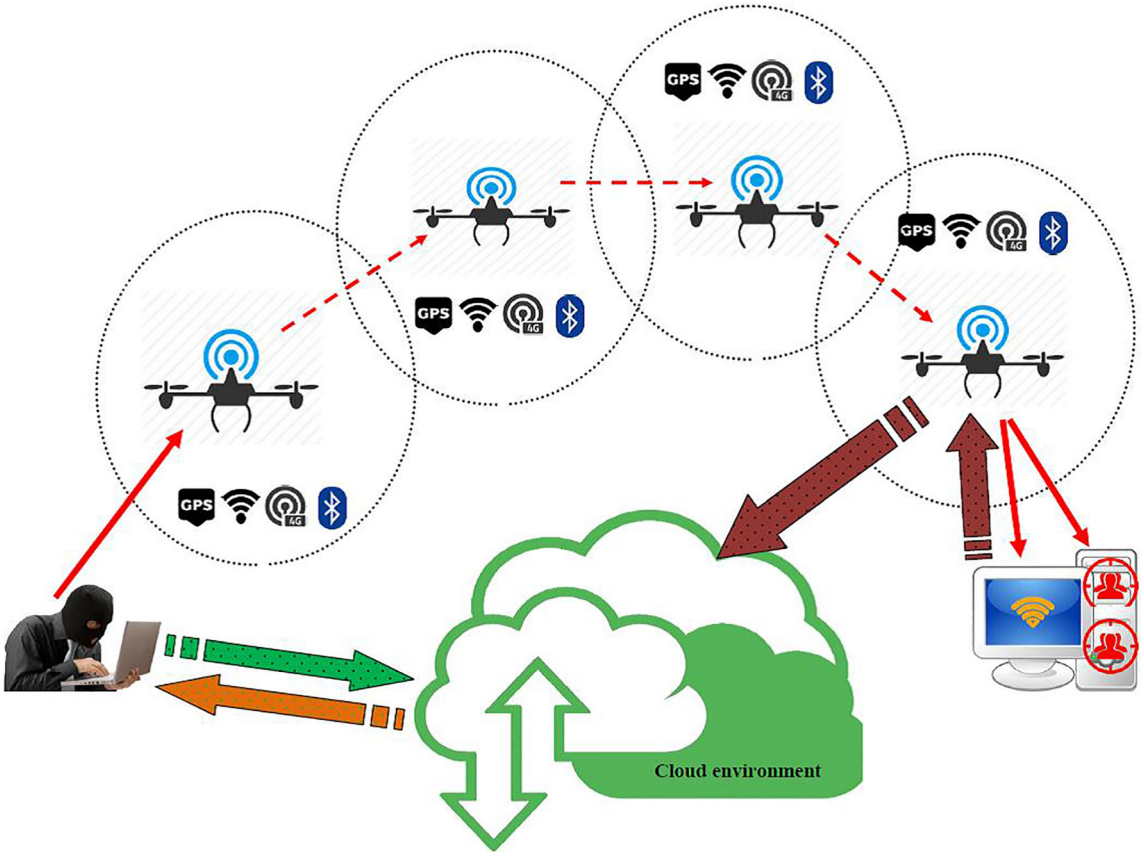


Fig. 3 Cloud assisted UAV Attack

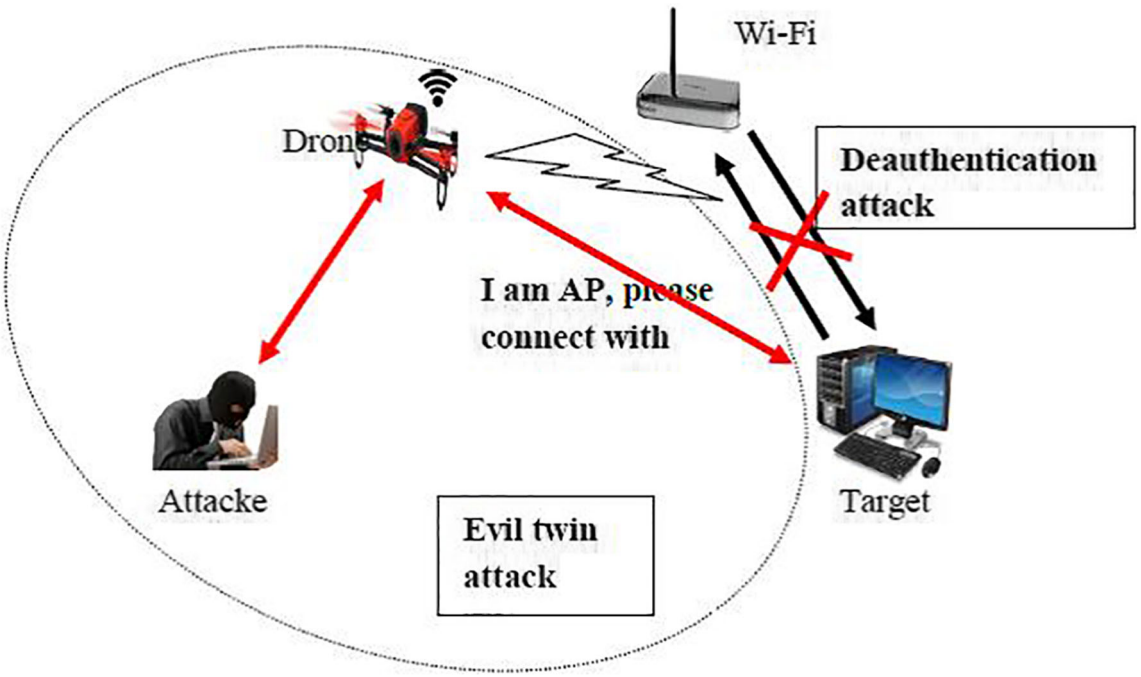


Fig. 4 Evil twin attack launched using UAV

Wifiphishing

Wifiphishing is a masquerading attack technique used on the Wi-Fi network to steal vital information like login passwords, medical account information, etc. Wifiphishing involves two phases. The first phase uses an evil twin attack whereas the second phase involves a fake login page which is forcibly displayed on the client side, prompting the clients to enter the valid credentials to re-connect with the AP. Likewise, the attacker can make use of any phishing pages to steal vital information like patient portal passwords.

UAV cyber attack experiment

The experimental setup for UAV based attack scenario is shown in Fig. 5. The devices used in the experiment setup are:

- Onida LEO40 SMART TV,
- Hacker UAV,
- Samsung android phone,
- NETGEAR wireless router and ASUS USB N13 wireless adapter,
- Alienware laptop,
- Zephyr Bioharness 3,
- Nonin Pulse Oximetry (SPO2) Sensor,
- MYTECH Blood Pressure Monitor sensor.

All the devices used for the experimentation are pre-configured to connect to the home (NETGEAR) router, except the Nonin SPO2 sensor, which is paired with the smart phone via Bluetooth.

Hacker UAV as shown in the Fig. 5 is used to carry a battery powered Raspberry Pi3. The average flight time of the Hacker UAV is 35 min. An external Wi-Fi adapter (ASUS 802.11 b/g/n USB N-13) is also configured and attached to the Raspberry Pi3 module to enable a Wi-Fi hotspot [34]. Monitor mode is enabled in all Wi-Fi adapters and a packet sniffer, Tshark, for displaying the network traffic, is installed to capture all the traffic at the monitor mode interfaces [35]. Various attack payloads including: Airmon-ng, Airodump-ng, Aireplay-ng, Aircrack-ng, Airbase-ng, Airdrop-ng and Wifiphisher are pre-configured into the Raspberry Pi3 [34]. The laptop acts as a command and control server to control the UAV and a remote Secure Shell (SSH) is used to connect the Raspberry Pi3 with the command and control (attacker) server. All captured traffic is saved both on the local hard drive as well as in Dropbox, an online cloud storage server.

UAV cyber attack scenarios

The research conducts two distinct experiments to demonstrate UAV cyber attack capabilities. The first shows how to compromise healthcare automation systems and the second demonstrates how to hijack and control BAN healthcare devices.

Smart hospital automation is an automated hospital control system that allows users to control various hospital appliances from Wi-Fi sensor devices [36]. Such applications include automatic identification of patients and healthcare personnel, RFID-based tracking of hospital resources, and control of lighting and televisions and other environment systems like HVAC [37]. At a wireless smart hospital, if an attacker is capable of breaking into any one of the gateway devices remotely, then it opens a channel to break into other smart devices associated with the compromised gateway device. This scenario explores how a UAV can hack smart hospital Wi-Fi routers and wireless devices and is demonstrated with a DoS attack. The UAV are designed to interrupt the wireless signal between the device controllers and the gateway device. Once the signals are interrupted, the connection will be lost and these UAVs take control of the entire hospital control system.

In the smart hospital scenario, a UAV is designed to execute a DoS attack against a SMART TV, simulating other possible connected devices within a hospital. The UAV flies over the experiment lab located within the hospital area of an Asian

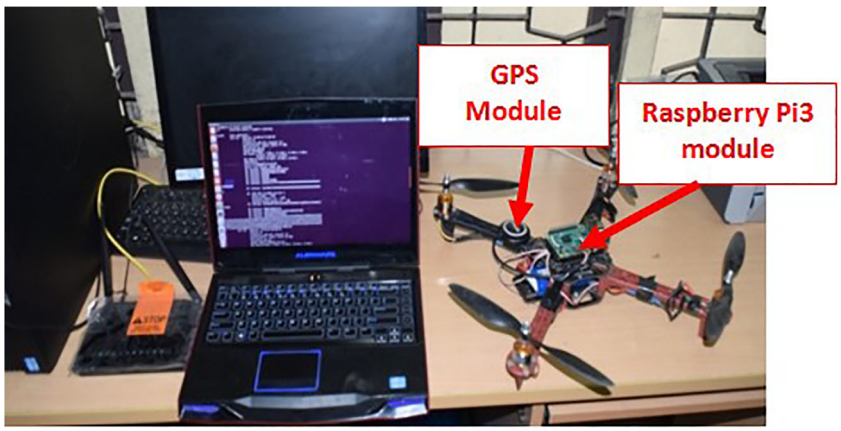


Fig. 5 Experimental Setup. (Hacker UAV, NETGEAR router and an Alienware laptop)

University. The UAV carries a pre-configured python script with the deauthentication payload. This payload is executed against the NETGEAR router, forcing all the connected devices to become disconnected. The payload executed using the UAV results in the disconnection of the SMART TV and the home router, thus resulting in a successful DoS attack. Figure 6 illustrates the flow graph of a deauthentication frame where the association table of the AP is filled with the SMART TV MAC address "E0:Cb:Ee:58:A8:21" in both source and destination leading the AP to confusion.

The second research scenario experiment demonstrates how UAVs can hijack BAN and IMD devices. Because BAN and IMD use wireless technologies including Bluetooth and Wi-Fi to facilitate data transmission, UAVs can interrupt the wireless communication causing a DoS leading to service unavailability, intercept data transmissions causing the compromise of protected health information, and insert themselves into the communication path enabling data corruption leading to inappropriate or incorrect treatments causing increased morbidity or death.

This UAV experiment is carried out remotely in the hospital area of the university. The wearable sensors (as shown in the Fig. 7) are activated and the vital signs are continuously monitored and stored in the cloud server. Figure 8 depicts the experimental setup for the remote health monitoring system and the attack scenario for hijacking the healthcare devices using the UAV. In this experiment, two attacks are performed. First, the gateway (router or smart phone) is disconnected by performing a DoS attack. Second, an evil twin attack is performed and forcibly connects all the healthcare devices to the UAV's fake AP. All the traffic captured are stored in Dropbox. The attack leads to a successful disconnection of wearable sensors from the legitimate AP and gains a successful connection with the fake AP. Connecting to a fake AP enables a DitM attack for reading and changing the sensor information.

The system health parametric check is carried out for the victim network (NETGEAR- home router), the UAV network (fake AP - created by the UAV) and monitored using a self-developed visualization tool. The response is deliberated for the vital parameters like incoming byte rates, incoming packet rates, outgoing byte rates, outgoing packet rates, deauthentication frame rate and fake AP frame rate for the victim network and the UAV network. Figure 9 shows the comparison plot for normal traffic (legitimate AP) and UAV generated traffic (fake AP). The blue line shows the normal traffic (legitimate AP), whereas the red line shows the UAV generated traffic for the fake AP. From the graph it can be confirmed that the deviation in the outgoing packet and byte rate is very high for the UAV generated traffic when compared to the legitimate AP. It is observed during the experimental trials that the Deauthentication and Fake AP are the most successful attacks, which are used to interrupt the connection and to make the simulated hospital resource unavailable.

During the attack scenario the sensor devices connected to the hospital gateway (Wi-Fi network) exhibit a normal behaviour and the traffic is recorded for 45 min. In order to test the proposed UAV based attack models, payloads such as Wifiphishing/Eviltwin deauthentication are executed and recorded for the span of 15 min. The UAV sends deauthentication frames to all the clients connected to the target AP and waits for the successful disconnection. The UAV then sniffs the target AP for information such as ESSID (an electronic identifier of a device used to connect to a wireless router), and creates a fake AP pretending to be the legitimate one, forcibly making the clients connect to the fake AP. Once the clients get connected to the Fake AP, a set of phishing pages are displayed at the client interface, forcing the client to connect using phishing pages. These forged data frames only have a fixed (static) time stamp field and a different range of values when compared to legitimate AP data. The forged frames from the UAV usually have a higher signal

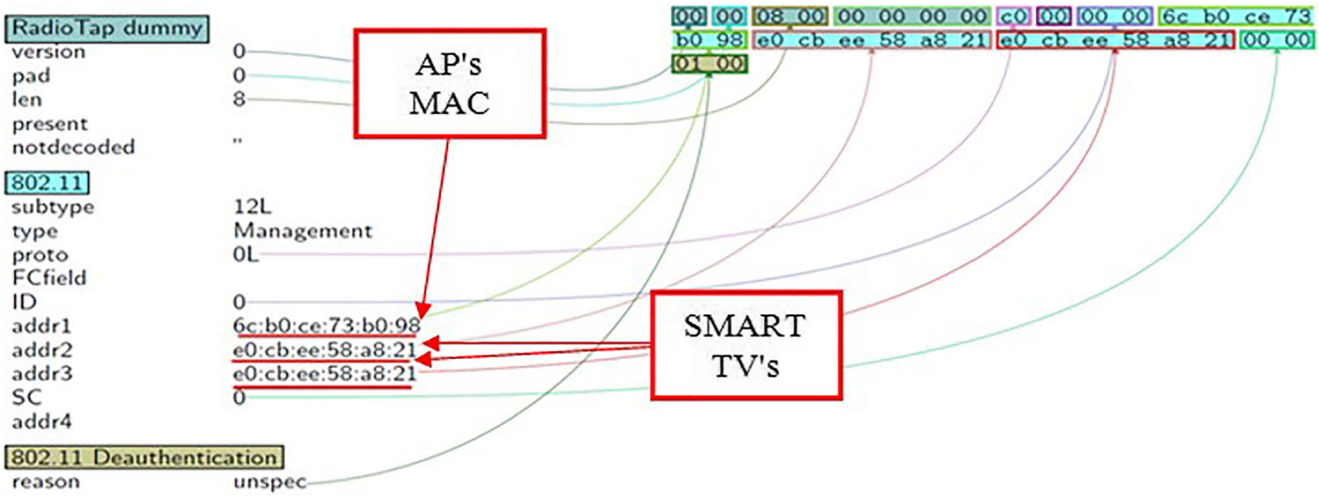


Fig. 6 Flow graph of the UAV's deauthentication attack

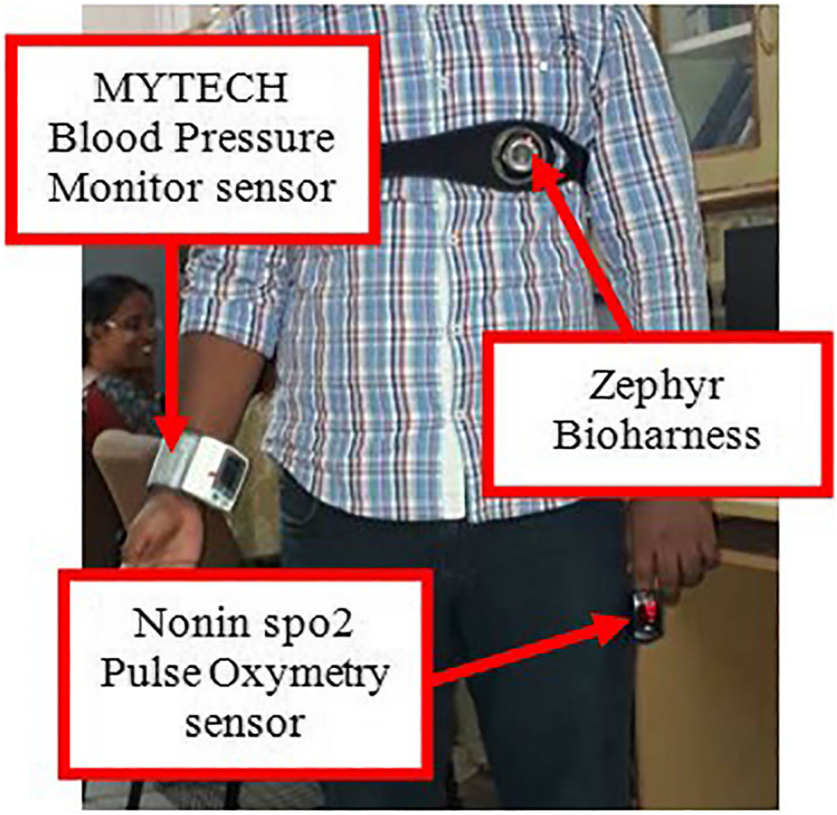


Fig. 7 Patient with BAN sensor devices

strength. Further these forged frames don't exhibit different behaviour in the network traffic and UAV produces forged frames which are nearly 90% valid.

The two research scenarios demonstrate the use of UAVs to perform attacks against both hospital systems and WIoT medical devices. The experimental validation of the attacks listed in this paper clearly reveals that, healthcare devices are prone to a multitude of threats some of which are severe while others are merely troublesome. For example, attacks on exposed services of these devices can be done with several underlying vulnerabilities, such as Fuzzing, where sending malformed data to characteristics IDs will cause misbehavior of the device. Also, some of the tested devices allow the attacker to directly connect to the device interface, through which the unauthenticated attacker can change the module's configuration, which can cause the device to function abnormally and even in some cases damage it.

Possible mitigation techniques

The vulnerabilities tested and reported in this paper are dangerous for both daily healthcare consumers and practitioners reliant on the medical condition measurements and subsequent treatment decisions afforded by BAN and IMD systems.

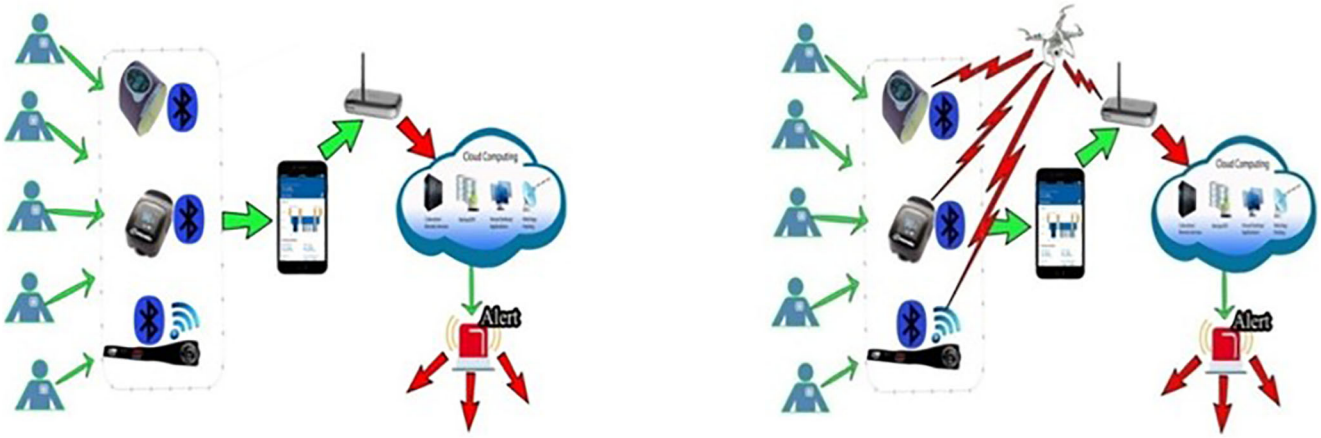


Fig. 8 Remote health (BAN) monitoring system and UAV attack scenario

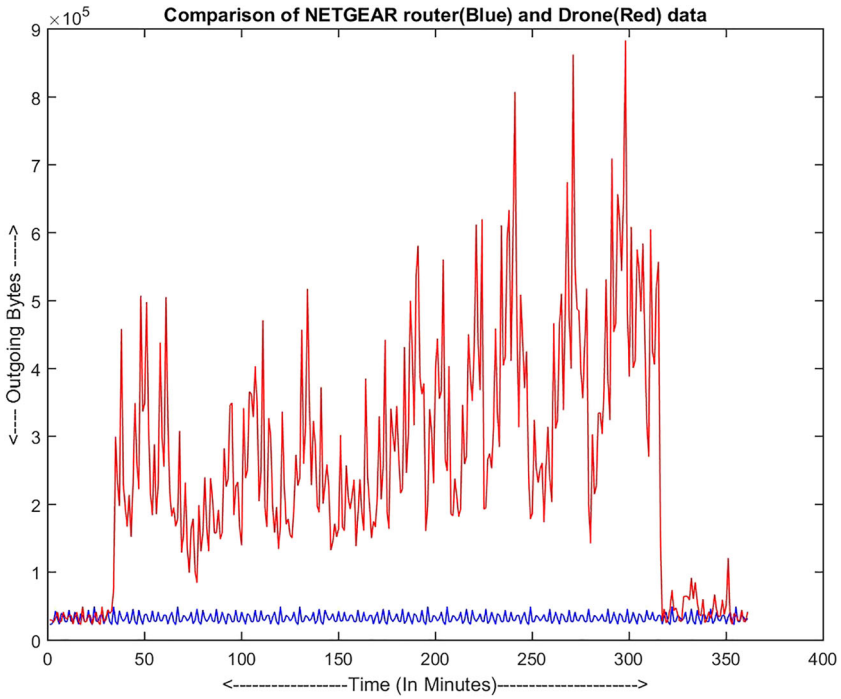


Fig. 9 NETGEAR router data vs. UAV data

Potential hackers can sneak into the device anonymously and listen to all the traffic and also obtain any personal data of the user and exploit it for several hazardous crimes.

Kintzlinger and Nissim [5] performed a literature review of wireless medical device security measures and reported 21 security methods reported between 2007 and 2015. The techniques reported were primarily of two types: the first requiring the BAN or IMD user to carry another device that would perform security scanning on the BAN or IMD device with some of these secondary security devices also being implantable, and new programming added to the device or reader to better secure the device.

We recommend four possible security risk mitigation techniques to safeguard medical BAN and IMD devices and other hospital Wi-Fi enabled devices from any external agent using the vulnerabilities determined in the UAV experiments. These four mitigation techniques fall into the latter type of security approach and involve implementation via device programming of new security features. Some of these feature are already present on some devices, but are underused. Educating consumers and practitioners would be necessary to gain the full security benefits afforded by these recommended techniques.

1. Key PIN protection [38, 39]
    a. Avail an option to set a custom PIN for the device on the initial setup.
    b. The changing of this PIN should be done only when the wearable device (consumer device) is connected to the app on the mobile device.
2. Admin device connection mode [38, 39]
    a. The wearable device remembers the MAC address of the parent/admin device (phone) and connects to only the admin device's MAC address and none other.
    b. Further, it refuses connection when any external device that does not match with the admin MAC address.
3. Device on screen notification when new device is connected
    a. This helps the user to know that a new unrecognized device is connected and the user can manually turn off Wi-Fi/Bluetooth on the device to stop the communication.
4. Discoverability mode locked to single device
    a. Once connected to the app from a particular MAC address (the phone/parent), the wearable device's discoverability is turned off and it looks only for the previously connected MAC address.

Conclusion

The research presented in this article demonstrated how UAVs may be used to conduct targeted attacks against healthcare facility wireless systems and personal medical devices including BAN and IMD. Prior research has already demonstrated

the vulnerability of IMDs to cyber attacks, especially acoustic-based attacks, but this article identifies a new and growing platform for discretely carrying out such attacks. Advancing technology enables modern BAN and IMD to communicate wirelessly to external devices over distances ranging from 5 m [22] to over 30 m [11], making UAV-based cyber attacks a reality. New UAV based attacks namely stepping stones attack and cloud assisted UAV attack are presented and the cloud assisted security threat was experimentally verified.

The attack patterns presented in this paper provides useful guidelines for healthcare device manufacturers to design proper security schemes for protection of BAN and IMD healthcare platforms. As UAVs become ever more available and present in society, the UAV based attacks will become more common and a device level security solution is desirable to combat these attacks.

Acknowledgements This research is supported by the Department of Science and Technology under the scheme 'DST PURSE II'. Author SCS would like to extend their sincere thanks to DST for supporting the research.

Compliance with Ethical Standards

Ethical Approval No human subjects were used outside of the researchers themselves. Informed consent was not required for this research. All procedures performed in studies involving human participants (the researchers) were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Conflict of Interest SCS was partially funded for this research from an internal university grant from the Department of Science and Technology. All authors confirm that there is no conflict of interest.

References

1. Park, J., and Tyagi, A., Using power clues to hack IoT devices: The power side channel provides for instruction-level disassembly. IEEE Consum Electron Mag 6(3):92–102, 2017.
2. Nilsen, W., Kumar, S., Shar, A., Varoquiers, C., Wiley, T., Riley, W. T., Pavel, M., and Atienza, A. A., Advancing the science of mHealth. J Health Comm 17(sup1):5–10, 2012.
3. Steinhubl, S. R., Muse, E. D., and Topol, E. J., Can mobile health technologies transform health care? *JAMA* 310(22):2395–2396, 2013.
4. Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., Saleem, S., Rahman, Z., and Kwak, K. S., A comprehensive survey of wireless body area networks. J Med Syst 36(3):1065–1094, 2012.
5. Kintzlinger, M., and Nissim, N., Keep an eye on your personal belongings! The security of personal medical devices and their ecosystems. J Biome Inform 95:103233, 2019.
6. Piwek, L., Ellis, D. A., Andrews, S., and Joinson, A., The rise of consumer health wearables: Promises and barriers. PLoS Med 13(2):e1001953, 2016.
7. Thibaud, M., Chi, H., Zhou, W., and Piramuthu, S., Internet of things (IoT) in high-risk environment, health and safety (EHS) industries: A comprehensive review. Decis Support Syst 108:79–95, 2018.
8. Hiremath S, Yang G, Mankodiya K (2014) Wearable internet of things: Concept, architectural components and promises for person-centered healthcare. In *EAI 4th International Conference on Wireless Mobile Communication and Healthcare* (pp. 304-307), IEEE.
9. Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., and Kwak, K. S., The internet of things for health care: A comprehensive survey. IEEE Access 3:678–708, 2015.
10. Otto, C., Milenkovic, A., Sanders, C., and Jovanov, E., System architecture of a wireless body area sensor network for ubiquitous health monitoring. J Mobile Multimed 1(4):307–326, 2006.
11. Li, M., Lou, W., and Ren, K., Data security and privacy in wireless body area networks. IEEE Wireless Comm 17(1):51–58, 2010.
12. Al, T. R., and Youssef, A. M., Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. IEEE Access 4:959–979, 2016.
13. Camara, C., Peris-Lopez, P., and Tapiador, J. E., Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of Biomedical Informatics 55:272–289, 2015.
14. La Bella, L., UAVs and law enforcement. New York: The Rosen Publishing Group, 2016.
15. Loukas, G., Gan, D., and Vuong, T., A review of cyber threats and defence approaches in emergency management. Future Internet 5(2):205–236, 2013.
16. Lidynia, C., Philipsen, R., and Ziefle, M., Droning on about UAVs—Acceptance of and perceived barriers to UAVs in civil usage contexts. In: *Advances in Human Factors in Robots and Unmanned Systems*. Cham: Springer, 2017, 317–329.
17. Dorling, K., Heinrichs, J., Messier, G. G., and Magierowski, S., Vehicle routing problems for UAV delivery. T Syst Man Cy A 47(1):70–85, 2017.
18. Scott, J. E., and Scott, C. H., Models for UAV delivery of medications and other healthcare items. Int J Inform Syst Informatic 13(3):20–34, 2018.
19. Javaid AY, Sun W, Devabhaktuni VK, Alam M (2012) Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In *2012 IEEE Conference on Technologies for Homeland Security* (pp. 585-590), IEEE.
20. Al Ameen, M., Liu, J., and Kwak, K., Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst 36(1):93–101, 2012.
21. Leavitt, N., Researchers fight to keep implanted medical devices safe from hackers. Computer 43(8):11–14, 2010.
22. Fu, K., and Xu, W., Risks of trusting the physics of sensors. Commun ACM 61(2):20–23, 2018.
23. Denning T, Borning A, Friedman B, Gill BT, Kohno T, Maisel WH (2010) Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 917-926), ACM.
24. Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T., and Maisel, W. H., Security and privacy for implantable medical devices. Pervasive Comput 7(1):30–39, 2008.
25. Sametinger, J., Rozenblit, J., Lysecky, R., and Ott, P., Security challenges for medical devices. Commun ACM 58(4):74–82, 2015.
26. Klonoff, D. C., Cybersecurity for connected diabetes devices. J Diabetes Sci Technol 9(5):1143–1147, 2015.
27. Li C, Raghunathan A, Jha NK (2011) Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In *13th IEEE International Conference on e-Health Networking Applications and Services* (pp. 150-156), IEEE.

28. Trippel T, Weisse O, Xu W, Honeyman P, Fu K (2017) WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 3-18), IEEE.
29. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, Fu K, Kohno T, Maisel WH (2008) Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *IEEE Symposium on Security and Privacy* (pp. 129-142), IEEE.
30. Maisel, W. H., and Kohno, T., Improving the security and privacy of implantable medical devices. New England J Med 362(13): 1164–1166, 2010.
31. Salmon, P. C., and Meissner, P. L., Mobile bot swarms: They're closer than you might think! IEEE Consum Electron Mag 4(1): 58–65, 2015.
32. Hanspach, M., and Goetz, M., On covert acoustical mesh networks in air. J Comm 8(11):758–767, 2013.
33. Kolias, C., Kambourakis, G., Stavrou, A., and Gritzalis, S., Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. IEEE Comm Surv Tutorial 18(1): 184–208, 2016.
34. Saad A, Amran AR, Hasan MNA (2016) WarBox: Portable wardriving over raspberry PI. In *International Conference on Information and Communication Technology* (pp. 227-235), IEEE.
35. Gandhi, D. C., Suri, G., Golyan, R. P., Saxena, P., and Saxena, B. K., Packet sniffer–a comparative study. Int J Comput Network Info Sec 2(5):179–187, 2014.
36. Yu, L., Lu, Y., and Zhu, X., Smart hospital based on internet of things. J Network 7(10):1654, 2012.
37. Catarinucci, L., De Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M. L., and Tarricone, L., An IoT-aware architecture for smart healthcare systems. IEEE Internet Things J 2(6):515–526, 2015.
38. Haus, M., Waqas, M., Ding, A. Y., Li, Y., Tarkoma, S., and Ott, J., Security and privacy in device-to-device (D2D) communication: A review. IEEE Comm Surv Tutorial 19(2):1054–1079, 2017.
39. Zheng, G., Shankaran, R., Orgun, M. A., Qiao, L., and Saleem, K., Ideas and challenges for securing wireless implantable medical devices: A review. IEEE Sensor J 17(3):562–576, 2017.