Evaluating Augmented Reality for Wireless Network Security Education

1st Martin Striegel
Fraunhofer AISEC
Garching near Munich, Germany
martin.striegel@aisec.fraunhofer.de

2nd Jonas Erasmus
Technical University Munich
Garching near Munich, Germany
jonas.erasmus@tum.de

3rd Parag Jain
Technical University Munich
Garching near Munich, Germany
parag.jain@tum.de

***Abstract*—In this innovative practice full paper, we investigate the benefits of using an augmented reality (AR) application in wireless network security education. For this purpose, we design and implement an AR application which passively captures wireless network traffic and superimposes the otherwise imperceptible network packets on the camera image of sending and receiving devices. We perform a user-study with 25 participants, who are provided with a laptop which runs our application. Students are tasked to spot *Evil Twin*, *Address-Resolution Protocol (ARP) Poisoning* and *Denial of Service (DoS)* attacks launched on a 802.11 Wi-Fi network by observing it with the AR application. We find that students were able to spot and describe those attacks intuitively. From those results we conclude that an AR-based approach is a valuable addition to wireless network security laboratory courses. Additionally, our results indicate, that our application provides access to this complex topic even for users without a technical background. To the best of our knowledge, this is the first experimental study, which shows the beneficial effects of using AR in wireless network security education.**

***Index Terms*—computer science, electrical engineering, laboratory, wireless communications, security education, augmented reality**

I. Introduction

Wireless network security is typically taught in university lectures and accompanying laboratory exercises using tools, which have a steep learning curve, such as `wireshark` or `tcpdump` [1], [2]. Those network monitoring tools merely provide an abstract view of the network by providing text, topological graphs or diagrams. However, effects of crafted network packets can alter the network topology and thus affect *all* machines in the network. If the network is inspected from a single machine, the overall impact of the attack might be shadowed by the perceived limited angle of view provided by central monitoring tools.

In contrast to that, *augmented reality (AR)* can provide a more immersive view of the network from a user-controlled birds-eye perspective. AR permits to join information from the visual world and the radio-frequency (RF) spectrum. In this case, a visualization of otherwise imperceptible network traffic can be superimposed on the camera image of the physical devices communicating with each other. The user can focus on selected parts of a wireless network by only capturing the devices of interest on camera, which provides a intuitive way of filtering information.

Studies on the use of AR in the classroom in other areas of application have shown, that this fosters both motivation and the student's understanding [3], [4], [5].

In this work, we show, that we can leverage these positive effects using AR in *wireless network security education*. We propose a laboratory setup and conduct a user study with 25 participants. They observe a Wi-Fi network through the AR application, while the common attacks *Evil Twin*, *Address-Resolution Protocol (ARP) Poisoning* and *Denial of Service* are launched on the network. Participants are tasked to detect and describe the attacks while they take place. This setup is highly interactive and provides a shared experience, as both attacker and defender act simultaneously and interact with the otherwise imperceptible network packets.

Remarkably, only by observing the changes in network topology, all participants were able to spot and describe the effect of all attacks. Hence, we conclude that AR is a valuable addition to traditional ways of teaching wireless network security. Furthermore, our results indicate, that AR-based network traffic visualization could permit access to the complex topic of wireless network security outside universities.

We make the following contributions:

- We design and implement an AR application tailored to wireless network security education, which helps users to spot attacks on a wireless network (Section III).
- We experimentally evaluate this application with 25 participants (Section IV).
- Based on our results, to the best of our knowledge, we are the first to demonstrate that AR-based traffic inspection can be of great benefit in wireless network security education.

II. Related Work

Our approach draws from previous work on AR-based visualization of networked devices, general engineering education and cybersecurity education.

a) AR-Based Device and Network Observation: In [6] and [7], the authors proposed AR interfaces to visualize sensor readings acquired by interconnected embedded systems. [8], [9], [10], [11] additionally visualized network links between devices. All of those solutions have in common, that they acquire information on devices and network links *actively*. Our AR application, in contrast, acquires network data passively.

This ensures, that we do not interfere with the attack we are observing.

[12] proposed an architecture and tool for AR-based network traffic visualization in 802.15.4-based wireless sensor networks. We leverage elements of this architecture such as passive traffic capturing, extraction of device addresses from Quick Response (QR) codes and the visualization of traffic. We extend their architecture by adding means to keep track of interrelated series of network packets. By doing so, our application is able to visualize roles of devices in the network and attacks, which consist of multiple packets. While their work lacks a study, which shows the usefulness of their approach, we conduct such a study and show, that this permits users to spot and describe the effects of attacks.

b) Engineering Education with AR: [4] found, that AR improves the learning experience by providing a high level of interactivity and a shared educational experience, while students interact with topics which can not be experienced in the real world.

[5] proposed an AR application to teach electromagnetism. The authors also found, that AR provides a positive shared interactive experience, as students exert control over the view and lets students manipulate objects AR.

[13] and [14] employed AR to visualize antenna radiation patterns in an overlay placed on the camera image of an antenna. This permits students to understand antenna characteristics and the effects of beamforming. They found that their approach increased the interest of students as well as reported learning gains.

c) Cybersecurity Education: Cybersecurity laboratory design and the use of AR in education have been discussed in several studies. However, none of those works has investigated the beneficial effects of AR in wireless network security education.

[1] and [2] have shown that a game of attacker and defender is motivating to students. However, in their works, the defender is the system administrator, who has to prevent attacks by securing the system *beforehand*, e.g., by configuring the firewall. In our work, the defender is provided with the AR application and tries to detect and describe attacks *while they happen*. This gives the defender a more active role during the attack and provides a close interaction between attacker and defender.

In [15], an AR-based game for teaching smartphone application security and privacy to high-school students was developed. In the game, common threats to social media "attack" the student, who chooses and wields an appropriate wooden shield with an AR marker to fend off the threat. In their study, the authors find that this serious game increases the self-awareness of students regarding cybersecurity and develops their critical thinking about technology.

[16] proposed a laboratory course, which leverages Software-Defined Radios (SDRs) to teach concepts related to wireless security such as eavesdropping and jamming . In a final competition, students tested their implementations by trying to eavesdrop on a IEEE 802.11 Wi-Fi (Wi-Fi) wireless link with different levels of protection. The authors found, that this is highly motivating for students. As their laboratory course is about SDR, they focused on attacks close to the physical layer, neither did they utilize AR.

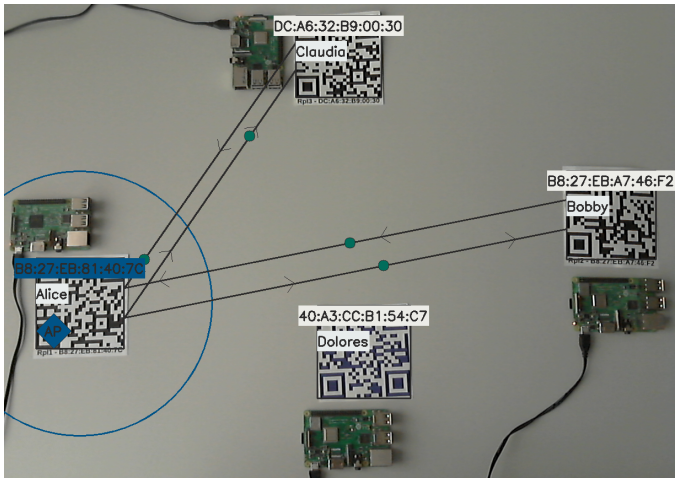

Fig. 1. Monitoring a network of four devices. All communicating devices are captured in the camera image. Claudia and Bobby exchange messages, which are routed by Alice. Alice transmits a beacon frame.

While the visualization benefits of AR in engineering education have been demonstrated in previous works, there is a research gap in the application of AR in wireless network security education with its particular need for *situational awareness*. Users must be trained to detect an attack, how the attack is conducted and the implications of the attack [17]. Due to the complexity of wireless network protocols, those goals are difficult to achieve by merely presenting, e.g., networking sequence diagrams in class. Thus we intend to utilize the motivating effects of AR in education [5], [13], [14] as well as the competitive aspects of attacker and defender games [1], [2], [15], [16] to provide a inciting way to wireless network security education, which, to the best of our knowledge, has not been studied before.

III. Augmented Reality Network Traffic and Attack Visualization

A. Overview

Figure 1 shows a screenshot of our AR application, the camera being pointed at a Wi-Fi network with four devices. Every networked device is identified by a QR code, which contains the Medium Access Control (MAC) address of the device. If the application captures a wireless packet, whose source and/or destination address correspond to a device visible in the camera image, the application superimposes traffic information on the camera image[1]. Here, the device to the top and the device to the right communicate with the access point (AP) on the left side of the figure. Every colored

[1]Our application assumes, that MAC addresses remain static, as randomization would cause a mismatch between identifiers derived from QR codes and those found in network packets. We consider this acceptable for the laboratory setup we are targeting

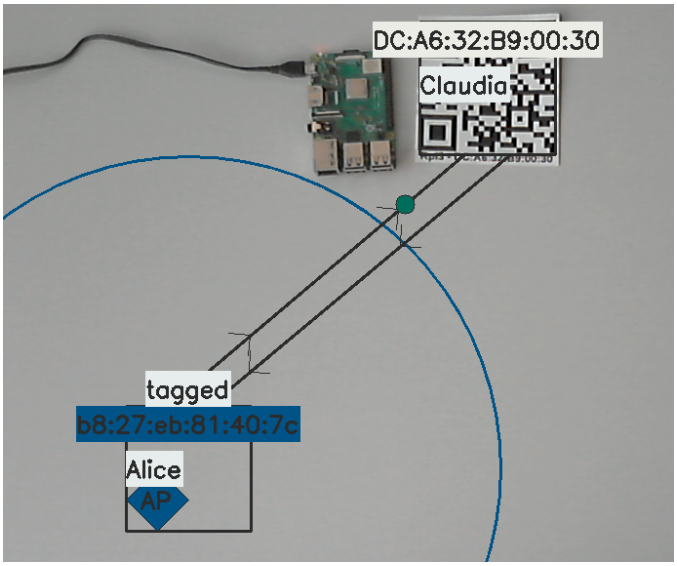

Fig. 2. Monitoring a single device (Claudia), whose communication partner (Alice) is not captured by the camera image and thus represented by a virtual device.

dot between devices corresponds to one Wi-Fi network packet using a unicast address, the arrows indicating the direction of data flows. The circle around the central device represents a packet using the broadcast address, e.g., a beacon.

A device of interest might not be captured by the camera image. In this case, the user can select the device from a list of known devices, which is composed of all known MAC addresses, and drag it into the camera image to an arbitrary location. It is then treated as a virtual device, as shown in Figure 2. Thus, the user is still able to inspect traffic flows from and to this device.

B. System Design and Data Flows

Figure 3 shows data flows in the framework, which are discussed in detail in the upcoming section. Our application is written in *Python3.7*, using *OpenCV*[2] for image acquisition and processing, *pyzbar*[3] for QR code detection and *scapy*[4] for capturing and manipulating network packets. It can hence be run on all devices, which support Python3 and which are capable of capturing a video stream and network traffic, either using the internal adapter or an external capturing device, e.g., connected via Universal Serial Bus (USB) or Ethernet.

a) Data Input: There are three sources of input: network traffic, camera images and user supplied information. Network traffic is captured passively to not interfere with the operation of the network, which is being observed by the application. Traffic is transformed in a data stream and forwarded to the application for processing. This modular architecture permits capturing different wireless protocols as well as wired protocols by adding a transceiver for that protocol. Additional packet sources, such as external traffic monitoring systems, can inject packets into this data stream to provide additional information.

Camera images are captured and fed into the application via an image stream. If desired, the user can input additional information such as friendly names and the roles of particular devices such as the APs using a configuration file. Furthermore, the user can also control the application by performing mouse clicks in the displayed video stream to open and close annotations. Those actions are written in the user input stream and fed into the application.

b) Processing: Device identifiers are extracted from the QR codes found in a camera image. Identifiers are also extracted from the source and destination fields of captured network packets. Thus, in general, all types of packets which include a source and a destination field can be processed by the application. A wireless protocol might use specific addresses, e.g., multicast or broadcast addresses in Wi-Fi. These protocol-specifics are stored in a protocol configuration file which tells the AR application how to handle the addresses. In case of, e.g., a broadcast packet, the application interprets the destination as a virtual broadcast-device and draws the overlay.

If a new device identifier is encountered, either in the network traffic or in an optical marker, the application adds this identifier to the list of known devices. If a known device identifier is found in the source or in the destination field of a captured network packet, traffic is drawn in the overlay. If both source and destination devices are visible in the camera image, a direct connection is drawn between them. If only either source or destination is seen, the invisible device is represented as a virtual device, so traffic flows can still be visualized.

By analyzing network traffic, the application can derive special roles of devices and keep track of events, which consist of multiple packets. For this, the application uses packet filtering and stateful decision trees, which encode network behavior. Packet filtering differentiates between control and data packets. For example, to find the AP in a Wi-Fi network, the application searches for Wi-Fi beacon frames. A device which sends a number of those frames is identified as an AP by the application. If multiple devices advertise the same network, this is fed into a decision tree, as it could indicate an *evil twin* attack. If, subsequently, a de-authentication packet is captured by the application, it is likely that an evil twin attack is taking place.

This straightforward classification is suitable for a wireless laboratory setting, where textbook attacks are being taught and experimented with. To be useful in a real-world setting, the modular architecture permits machine-learning based mechanisms for sophisticated network traffic analysis to be added in the processing routines.

c) Output: The application outputs a video frame, which consists of the original camera image with superimposed information on network traffic and attacks. The goal is to provide a clear, yet informative view on the network. Initially, the

[2]https://pypi.org/project/opencv-python/
[3]https://pypi.org/project/pyzbar/
[4]https://pypi.org/project/scapy/

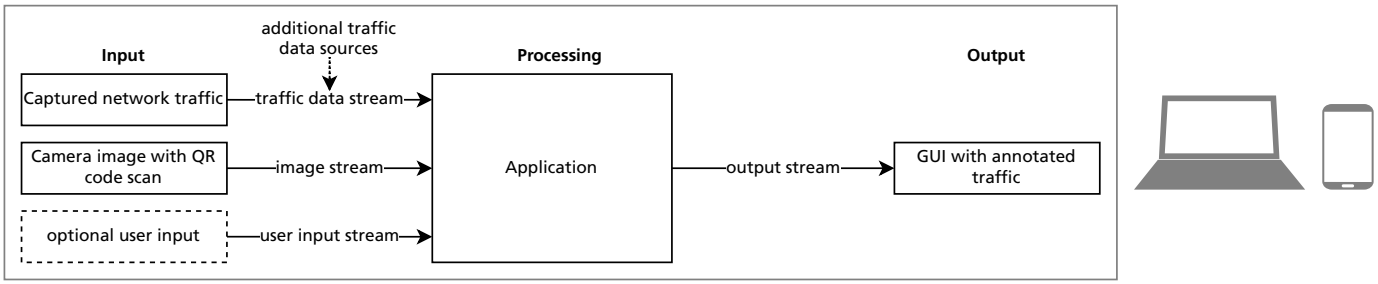

Fig. 3. Architecture: Data flows in the AR application

application displayed additional information about the packet content on every packet. As many devices might be captured by the camera simultaneously, the amount of information displayed needed to be balanced to not lose important information but also not to clutter the view. To find this balance, we conducted a pilot study with ten participants to understand which visualization of traffic is perceived most helpful. In result, every unicast packet is shown as one dot without additional information, as participants commented that more information clutters the view too much. Participants also liked that Wi-Fi packets, which are sent to the *broadcast address*, are shown as circles. They found the graphical distinction between unicast and broadcast traffic on logical layer helpful and precise, despite every wireless packet being broadcast in the air on the physical layer.

The application can provide various levels of visual guidance. By default, only network packets exchanged between devices are visualized as one white dot following a directed line to the destination device. The user can choose to activate filtering and the decision trees. Then, the application colors packets and annotates special roles of devices. For example, data packets are display in green, while Wi-Fi de-authentication packets are colored orange. Devices which the application found to have special roles, e.g., the Wi-Fi AP or a device having been subject to an attack, are marked by a colored diamond.

The user can also input additional information on devices. For example, in a known network, friendly names can be supplied to devices to easily distinguish them. Additionally, device roles can be made known to the application manually. This set of customization options permit the AR application to be tailored to the laboratory course and the varying skill levels of the students, e.g., by providing hints.

C. Laboratory Testbed

The testbed consists of four Raspberry Pi 3 (annotated Alice, Bobby, Claudia and Dolores for easier reference). Every device has a QR code optical marker that shows its MAC address. Alice acts as a Wi-Fi router and AP, while Bobby and Claudia are connected to the AP as clients. We use Wi-Fi in the testbed, as it is the prevalent wireless protocol and thus typically taught in university courses.

Bobby and Claudia exchange messages over User Datagram Protocol (UDP) once per second and those messages are routed

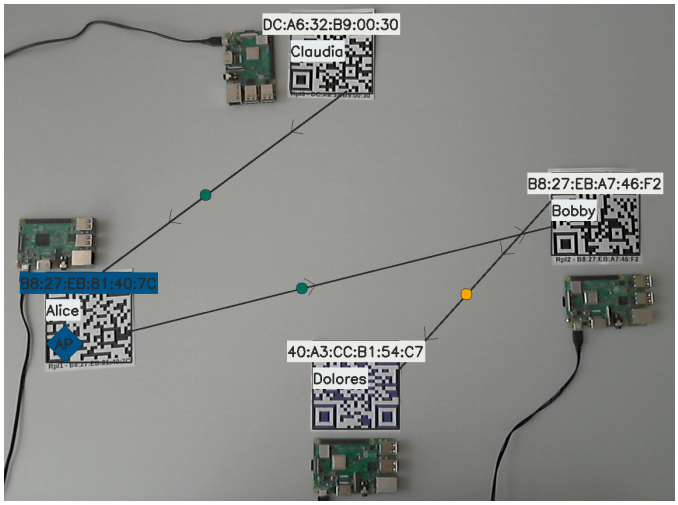

Fig. 4. Dolores performs an *Evil Twin* attack by de-authenticating Bobby from Alice's AP, then tricking Bobby into joining Dolores' malicious AP. Alice still considers Bobby to be part of its network. Bobby tries to send packets to Claudia, but Dolores does not forward packets. Due to having emitted a de-authentication request followed by Wi-Fi beacons, our application considers Dolores to be an attacker and thus colors the packets to and from Dolores orange.

by Alice. Every message is acknowledged by the peer. Dolores is the attacker and is also a client of the wireless network. The test supervisor, who takes the role of the attacker, can access her via Secure Shell (SSH) and launch attacks on the network. Using *scapy*, we implemented a set of attacks typically used in Wi-Fi network security laboratories [2].

- *Evil-Twin* attack: De-authenticating a device from a Wi-Fi network, advertising a malicious AP with high signal strength and tricking the de-authenticated victim into joining the malicious AP (Figure 4).
- ARP poisoning: Creating a mismatch between Internet Protocol (IP) and MAC addresses. This results in sending of packets to the attacker instead of the legitimate receiver (Figure 5).
- *DoS* attack: Overloading the victim device by sending packets at a very high rate. This might also overload the AP or prevent other devices in the network from sending packets, as the wireless channel is overloaded (Figure 6).

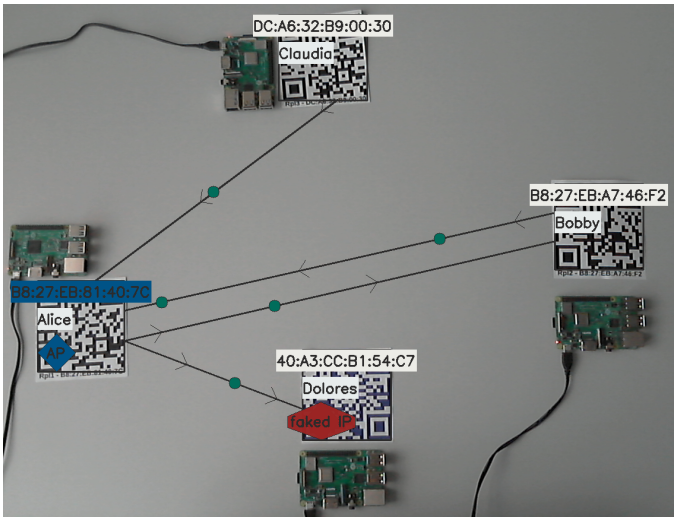

Fig. 5. Dolores performs *ARP* poisoning. Bobby takes Dolores' MAC address for Claudia's. As a consequence, Bobby sends packets destined for Claudia to Dolores instead.

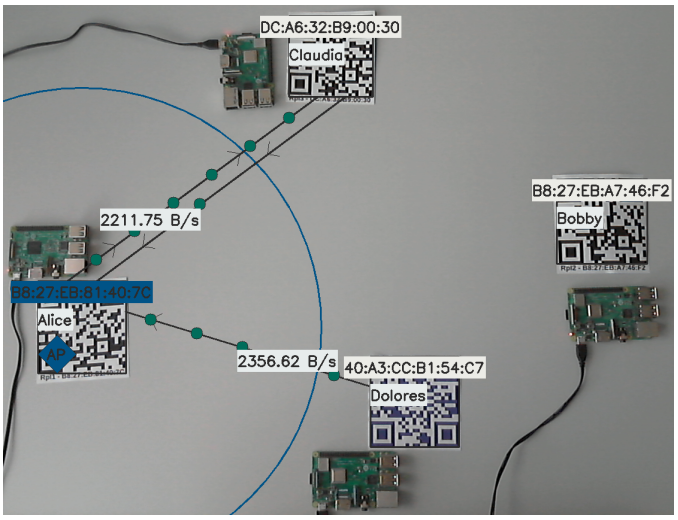

Fig. 6. Dolores performs a *DoS* attack against Claudia by sending packets at a high data rate. Alice is busy forwarding packets from Dolores to Claudia. In turn, Bobby does not receive packets and assumes, its connection to the AP is lost.

IV. User Study: Is AR Beneficial in Wireless Security Education?

a) Purpose and Scope: Students were given our AR application to observe a Wi-Fi network. They were tasked to spot attacks on the wireless network launched by the supervisor and to describe cause and effect of the attacks. The research questions investigated in this study are:

1) Does AR-visualization provide interesting information on a wireless network in a comprehensible manner?
2) Does visualization of wireless networks and attacks permit students to spot attacks?
3) Does the visualization enable them to explain the underlying mechanism of an attack?

b) Sample: We recruited a total of $N = 25$ participants. 19 participants were from computer science and electrical engineering study programs (9 CS, 10 EE), who already had taken a course related to wireless network security. To test if our application is useful to a person with no background in those topics, we recruited additional six participants.

c) Procedure: Prior to execution, the supervisor explained the test scenario, described the tasks to be performed and explained his own role as technical support. Next, participants were given a printed instruction sheet in English language. They were asked to read aloud the instruction sheet and ask any questions they may have.

Participants were provided with a switched-on laptop, to which a webcam was attached. On the laptop, the AR application was launched already. Initially, they were presented the view on the wireless network with no attacks being present. Participants were free to move the camera to explore the network and familiarize with the AR application. They were given time to ask questions about the general operation of the application. These were noted down by the supervisor and used as additional feedback.

Participants confirmed that they were ready to begin. Next, they were asked how many devices in the network were actively sending data, which device was the AP and at which interval it transmitted advertisement frames. Additionally, participants were asked to find out the name of the advertised Wi-Fi network and the IP address of network member Claudia. Answers to those closed questions were noted by the test supervisor.

After the participant had finished accessing the benign network, the supervisor, being in control of Dolores, launched an attack. Participants neither knew which attack they would encounter, nor which attacks were available in the test pool. After the participant confirmed that something in the network visualization had changed, the test supervisor asked the following open questions. Participants answered the questions orally. The test supervisor noted the answers word for word and also added hints given by them.

1) Did you notice the attack? How?
2) What effects does the attack have on the network?
3) Can you explain the attack in detail?

By using this three-stage questionnaire, we were able to differentiate between proficiency of the participants and test different parameters: Question one is intended to verify that the attack has been visualized by the application in a comprehensible way. Question two investigates whether the visual representation of the attack helps in explaining its *effect* on the network. Question three explores whether the visualization of the attack helps participants in explaining the *cause* of an attack. After participants had completed all three attacks, the supervisor asked them for qualitative feedback on their experience with the application.

Each of the three authors of this paper individually performed cluster analysis on the transcribed answers. We defined three clusters: (1): the question had not been answered or a wrong answer had been given; (2): some key concepts or

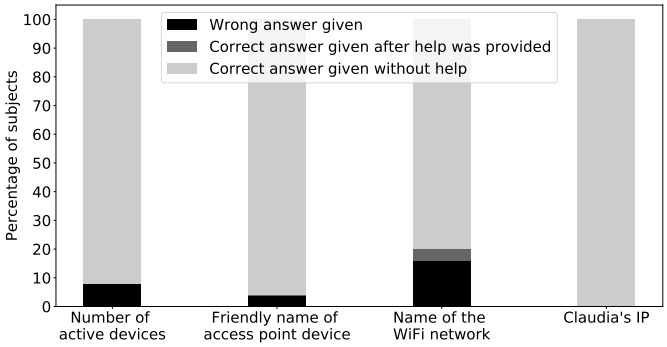

Fig. 7. Percentage of participants who were able to gather information indicated on the x-axis by inspecting the wireless network with the AR application.

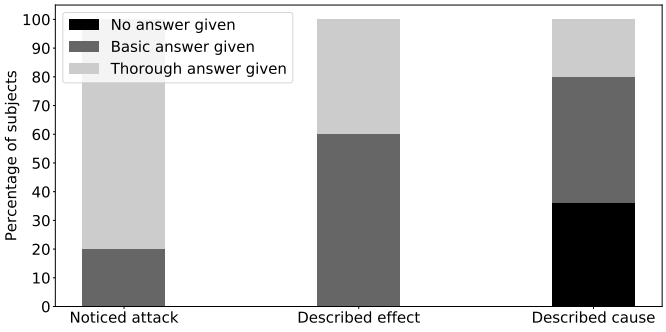

Fig. 8. Percentage of participants who noticed the *Evil Twin* attack; who could explain effect and cause.

a basic explanation were given, potentially, after the supervisor gave a hint; (3): all key concepts were mentioned or thorough answer was given without requiring a hint. Each author converted the transcripts individually, then the results were compared. In the case of discrepancies in the conversion, results were discussed among the authors until consensus was reached.

d) Limitations: This research is subject to limitations. As this study has been planned, executed and analyzed by the same group of people they were not "blind" and therefore a bias of the study results due to the expectations of these persons cannot be excluded. Due to the small sample size data were analyzed descriptively. As future work, the number of participants should be expanded significantly to be able to draw robust statistical conclusions.

A. Experiment: Basic Use and Information Presentation

a) Results: Figure 7 shows how participants dealt with the general presentation of information in the AR application. 92 % of participants were able to determine the number of active devices in the network and 96 % were able to obtain the friendly name of the AP device (Alice). 80 % of the participants were able to spot the name of the Wi-Fi network by clicking on Alice and reading the expanded information. 16 % needed a hint to click on the AP and found the requested information there, while 4 % were not able to find the name in the expanded view. All participants were able to obtain Claudia's IP address by clicking on that device.

b) Discussion: In average 92 % of participants were able to find requested information without needing help from the supervisor. This is especially remarkable, since 24 % of our participants had no background in computer science and electrical engineering and thus could not be expected to be familiar with Wi-Fi core concepts such as addressing. Information such as the number of active devices and the friendly name of the device hosting the AP could be seen at a single glance. Additional information requested in the experiment, such as the name of the Wi-Fi network and the IP address of device Claudia, could not be seen directly in the AR view. In those cases, participants clicked on a particular device, expecting that this would reveal additional information. Thus, we conclude that the combination of the AR view plus clickable devices is intuitive. All relevant information must be provided in those views, otherwise, information might be missed by the user.

Besides the AR view, our application also offers a network graph perspective on the network as well as a text-based packet log, similar to `wireshark`. In this study, we did not tell participants about their existence, as we wanted to evaluate how to present information in an optimal way in the AR view. Four curious participants discovered the existence of the packet log and used it to further investigate attacks. However, as they noted the similarity to `wireshark` and as our AR application is not intended to replace such text-based network inspection tools, we are going to remove the packet log in future versions of our application. We rather aim to improve the amount of information shown to the user and strive for a balance to not overwhelm the user, but nevertheless display relevant information. For example, more information could be displayed by default at the collapsed devices, e.g., their IP address or, in case of the AP, the name of the Wi-Fi network.

B. Experiment: Evil Twin

a) Results: Figure 8 shows that all participants noticed the *Evil Twin* attack and were able to give a basic or thorough answer. Basic notice means that the de-authentication packet was noticed and that Bobby now communicates with Dolores instead of Alice. 80 % of participants noted additionally that Dolores had sent broadcast frames before.

All participants were able to explain the effect of the attack. Among those, 60 % gave a basic explanation and described that Bobby now sends data directly to Dolores, while it previously had sent packets to Claudia via Alice. 40 % gave a thorough explanation and stated additionally that Bobby had left Alice's network and joined Dolores' network instead.

36 % of participants could not state the cause. 44 % could explain the cause of the attack in a basic way, describing that Bobby changed its communication behavior based on a broadcast frame emitted by Dolores. The thorough explanation given by 20 % of the participants additionally included that Bobby had left Alice's network and joined Dolores' network.

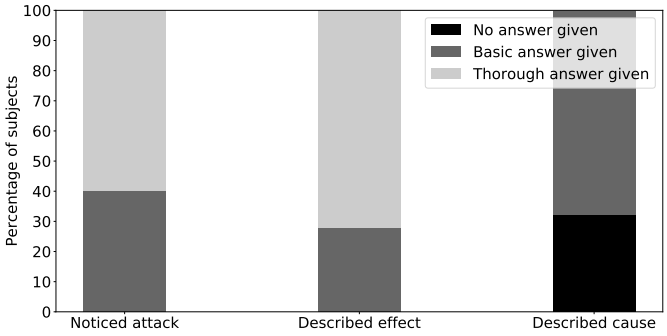

Fig. 9. Percentage of participants who noticed the ARP poisoning attack; who could explain effect and cause.

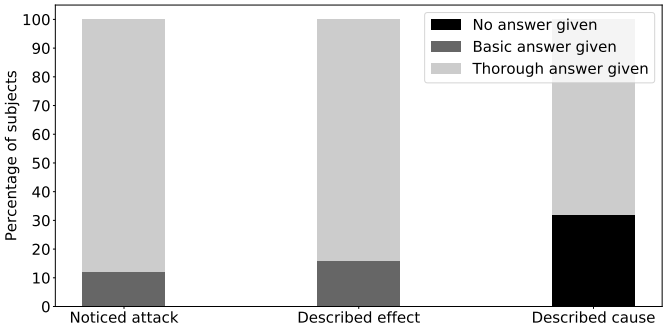

Fig. 10. Percentage of participants who noticed the DoS attack; who could explain effect and cause.

b) Discussion: Concerning the *Evil Twin* attack, the AR-based visualization of the wireless network permitted all participants, even those without a professional background, to *spot* that an attack had taken place. All participants were able to describe the *effects* an attack had on the network. Hence, we can conclude that the birds-eye view provided by AR is an intuitive way to visualize attacks.

Only 20 % gave a thorough description of the *Evil Twin* attack. To fully comprehend this attack, deep understanding of Wi-Fi networks is needed, especially the distinction between *Evil Twin*, where only beacons are forged, and *Impersonation* attacks, where the attacking device tries to mimic the legitimate network in all aspects. Participants who gave the correct explanation stated that they were able to do so based on their formal education or previous experience. Hence we noticed that currently, our application does not provide visual clues to foster this understanding. As a consequence, we plan to add additional information to the AR view, for example the frequency of occurrence and the signal strength of beacons as well as the announced Service-Set Identifier (SSID) of the wireless network. Such visual clues may indicate to the user that with high probability an *Evil Twin* attack is taking place.

C. Experiment: ARP Poisoning

a) Results: All participants noticed the attack. The basic explanation was that packets changed their route to Dolores. For a thorough answer the testees noticed that the data stream originally going from Bobby to Claudia is now routed through Dolores.

The effect could also be explained by all participants: 28 % stated that there is a new traffic stream to Dolores, which had not been there before. 72 % additionally pointed out that the missing data to Claudia and that it seemed as if the data stream from Bobby to Claudia had been rerouted.

32 % of participants could not give an explanation for the cause of the attack. 68 % gave the basic explanation that Dolores somehow managed to fool Bobby into sending data to her instead of Claudia. No participant gave the thorough explanation that traffic was redirected by a manipulation of Bobby's ARP table.

b) Discussion: All participants were able to notice and describe the effect of the attack, as the different traffic streams could be seen using the AR view. Explaining this attack, however, required participants to understand, how addressing in Wi-Fi-based wireless networks works and how the translation between MAC and IP addresses is done by ARP. To aid the user in understanding ARP, we plan to add a view filter to the application, letting users switch between IP-based and MAC-based addressing. By alternating between those views, participants could confirm that on the IP layer everything looks fine, while there has been a change in MAC-based addressing.

D. Experiment: DoS

a) Results: All participants noticed the DoS attack. 10 % only noticed that packets neither travel to, nor emanate from Bobby. 90 % additionally noticed that, unlike before the attack, a high number of packets go from Dolores to Claudia via Alice.

Concerning the effect of the attack, 16 % concluded that *Bobby* does not communicate any more and thus seems to have lost its connection. 84 % additionally stated that the traffic rate between Dolores, Alice and Claudia is much higher than before.

No explanation for the cause of the attack was given by 32 % of the participants. 64 % described that the attack caused *Bobby* to be disconnected due to an overload of the AP.

b) Discussion: The DoS attack was noticed and its effect could be described by all participants, as the high amount of packets and the disconnection of network participant Bobby was easily visible in the AR application. Especially in the case of DoS, the visual representation of the attack is able to precisely show its effect. While 30 % of the participants were not able to link Bobby being disconnected due to Alice being overwhelmed with packets, 70 % of the participants gave this correct explanation.

In this attack, Bobby seems to sit idle, which is not the case. Bobby is issuing requests to send (RTS), asking Alice to be given clearance to send regular message, i.e., re-join requests. As Alice does not answer Bobby's RTS, Bobby assumes he is not supposed to send packets and thus does not send the request to re-join Alice's network. Our application does not

show those low-level control frames, making it seem, that Bobby is not trying to reconnect to Alice' AP. As in a managed Wi-Fi network every regular frame is preceded by a RTS frame, we are convinced that visualizing those frames would clutter the AR view too much. Adding this, however, could be beneficial in a university course on Wi-Fi internals and we plan to add an option to enable and disable the visualization of those frames to our application.

E. Qualitative Feedback

All participants expressed that the AR-based visualization provided them with an intuitive visualization of the complex participants of Wi-Fi networks and attacks on those. They stated that visualizing each packet as one moving dot is clear. However, they wished that interrelated packets are visualized as such to make cause and effect of particular packets more clear. The use of QR codes was accepted for the university course setting. For a real-world application, they wished to be able to work without those.

Using the application in the laboratory setup sparked their interest, making them eager to investigate real-world setups. Participants with no background in wireless network security stated they would like to use the application to troubleshoot their Wi-Fi network at home. They pictured the scenario, in which they were able to connect their smart phone to the home router, but not their tablet computer. By seeing traffic being exchanged between the smart phone and the router, problems with the router can be ruled out and, with very high confidence, they can be narrowed down to the tablet computer.

Another proposed use case comprises investigating whether *seeing* a smart phone sending location and telemetry data has an influence on the participant's notice of privacy. As packet sniffing is rarely used on smart phones, the user could further observe whether his disabling of telemetry data yields the desired effect or whether there is a discrepancy between conceived privacy settings and real device behaviour.

Besides, it was suggested to make the effects of encryption and authentication visible, e.g., by letting participants observe the effects of attacks on a secure and an insecure connection.

Our results show that AR is a suitable approach for wireless network security education. It provides an easy to understand and clear visualization of complex attacks, permitting subjects to spot the attacks and describe their effect. Even participants with no background in engineering or computer science were able to spot attacks and give a description of its effect. The suggestion of new use cases shows, that observing a wireless network through the AR lens sparked the interest of participants.

Our application is designed to hide the complexity of wireless network security from the user, permitting access to the topic with a flat learning curve. Hence, we see the AR-based approach to be used in an introductory course or alongside text-based monitoring programs. This rationale is in line with 14 participants who expressed, that the AR application is useful for quick initial analysis. For an in-depth analysis, they would tools such as `wireshark`, which displays all information, however, in a less accessible manner. We conclude, that the AR application is a valuable supplementary tool, providing easy access to the complex matter of wireless network security, making hard-to-grasp concepts comprehensible and sparking student's interest.

While we suggest, that every student has their own handheld device in a laboratory, our approach could also be used within a wireless network security lecture. For this, the lecturer could place three to four laptops or low-cost single-board computers at their desk, capture those devices with a camera attached to their presentation laptop and display the network traffic visualization using a projector. This low-effort approach provides a shared and visually appealing experience for students, which fosters their motivation to explore the AR tool in the accompanying laboratory.

V. Conclusion

In this paper, we presented an augmented reality (AR) application tailored towards wireless network security education. The application visualizes network traffic flows and common attacks in wireless networks in an overlay placed over the camera image of networked devices.

To investigate whether such AR-based traffic monitoring is beneficial in wireless network security education, we conducted a user study with 25 participants. 19 of those participants had received education in the fields of computer science or electrical engineering, 6 participants didn't. Participants were to observe an IEEE 802.11 Wi-Fi (Wi-Fi) network using our AR application while the test instructor launched common attacks on the network. Using the application, they were tasked to spot and explain the effects and causes of the attacks. All participants were able to spot all attacks and explain their effects on the network, while 66 % were able to explain the underlying mechanisms of the attack. Remarkably, even students with neither a background in computer science nor in electrical engineering, were able to spot the attacks and at least describe the effects on network topology. This shows that the AR-based approach is a suitable tool to be used in wireless communications security education, as it fosters the understanding of the otherwise hard-to-grasp attacks. Hence, we conclude that using AR-based traffic visualization is a valuable addition to wireless network security laboratories and, due to the flat learning curve, could also be used outside university courses.

References

[1] P. J. Wagner and J. M. Wudi, "Designing and Implementing a Cyberwar Laboratory Exercise for a Computer Security Course," *Proceedings of the 35th SIGCSE Technical Symposium on Computer Science Education, SIGCSE 2004, Norfolk, Virginia, USA, March 3-7, 2004*, pp. 402–406, 2004.

[2] M. Malekzadeh, A. A. Abdul Ghani, and S. Subramaniam, "Design of Cyberwar Laboratory Exercises to Implement Common Security Attacks against IEEE 802.11 Wireless Networks," *Journal of Computer Systems, Networks, and Communications*, vol. 2010, pp. 1–15, 2010.

[3] M. McGrath and J. Brown, "Visual Learning for Science and Engineering," *IEEE Computer Graphics and Applications*, vol. 25, no. 5, pp. 56–63, Sep. 2005.

[4] M. Billinghurst and A. Duenser, "Augmented Reality in the Classroom," *IEEE Computer*, vol. 45, no. 7, pp. 56–63, 2012.

[5] M. B. Ibánez, Á. Di Serio, D. Villarán, and C. Delgado Kloos, "Experimenting with electromagnetism using augmented reality: Impact on flow student experience and educational effectiveness," *Computers & Education*, vol. 71, pp. 1–13, Feb. 2014.

[6] M. Rauhala, A.-S. Gunnarsson, and A. Henrysson, "A Novel Interface to Sensor Networks Using Handheld Augmented Reality," in *Proceedings of the 8th Conference on Human-computer Interaction with Mobile Devices and Services*, ser. MobileHCI '06. New York, NY, USA: ACM, 2006, pp. 145–148, event-place: Helsinki, Finland.

[7] D. Goldsmith, F. Liarokapis, G. Malone, and J. Kemp, "Augmented Reality Environmental Monitoring Using Wireless Sensor Networks," in *2008 12th International Conference Information Visualisation*, Jul. 2008, pp. 539–544, iSSN: 1550-6037.

[8] N. Sakamoto, H. Shimada, and K. Sato, "Design and Implementation of Sensor Network Device Control System with AR Technology," in *Mechatronics and Information Technology*, ser. Advanced Engineering Forum, vol. 2. Trans Tech Publications, 2011, pp. 131–134.

[9] K. Sato, N. Sakamoto, S. Mihara, and H. Shimada, "CyPhy-UI: Cyber-Physical User Interaction Paradigm to Control Networked Appliances with Augmented Reality," *The Sixth International Conference on Advances in Computer-Human Interactions (ACHI)*, 2013.

[10] K. Sato, N. Sakamoto, and H. Shimada, "Visualization and Management Platform with Augmented Reality for Wireless Sensor Networks," *Wireless Sensor Network*, vol. 07, no. 01, pp. 1–11, 2015, publisher: Scientific Research Publishing, Inc,.

[11] T. Ohta, R. Ito, and Y. Kakuda, "Design of a Node Status Visualizing Software Utilizing the AR Technology for Multihop Wireless Networks," in *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, vol. 2, Jul. 2017, pp. 270–271, iSSN: 0730-3157.

[12] M. Striegel, C. Rolfes, J. Heyszl, F. Helfert, M. Hornung, and G. Sigl, "EyeSec: A Retrofittable Augmented Reality Tool for Troubleshooting Wireless Sensor Networks in the Field," *Proceedings of the 2019 International Conference on Embedded Wireless Systems and Networks (EWSN '19)*, vol. Junction Publishing (USA), pp. 184–193, 2019.

[13] C. Sahin, D. Nguyen, S. Begashaw, B. Katz, J. Chacko, L. Henderson, J. Stanford, and K. R. Dandekar, "Wireless communications engineering education via Augmented Reality," in *2016 IEEE Frontiers in Education Conference (FIE)*. Erie, PA, USA: IEEE, 2016, pp. 1–7.

[14] D. H. Nguyen, L. Henderson, J. Chacko, C. Sahin, A. Paatelma, H. Saarnisaari, N. Kandasamy, and K. R. Dandekar, "BeamViewer: Visualization of dynamic antenna radiation patterns using Augmented Reality," in *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Apr. 2016, pp. 794–795.

[15] M. Salazar, J. Gaviria, C. Laorden, and P. G. Bringas, "Enhancing cybersecurity learning through an augmented reality-based serious game," in *2013 IEEE Global Engineering Education Conference (EDUCON)*, 2013, pp. 602–607.

[16] C. Sahin, D. Nguyen, J. Chacko, and K. R. Dandekar, "Wireless cybersecurity education via a software defined radio laboratory," in *2015 IEEE Frontiers in Education Conference (FIE)*, Oct. 2015, pp. 1–8.

[17] G. P. Tadda and J. S. Salerno, "Overview of Cyber Situation Awareness," in *Cyber Situational Awareness*, S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds. Boston, MA: Springer US, 2010, vol. 46, pp. 15–35, series Title: Advances in Information Security. [Online]. Available: http://link.springer.com/10.1007/978-1-4419-0140-8_2