Research Portfolio

[7COM1084-0901-2021 - Advanced Research Topics in Computer Science](https://herts.instructure.com/courses/90051)

Name: SATYANARAYANA REDDY BOGGULA

Student ID:19050844

MSC DATA ANLYTICS WITH PLACEMENT YEAR

Research Specialisms:

1.Robotics and AI specialism paper

2.Cyber Security specialism paper

Table of Contents

Part 1 3

1. Introduction of research specialism 3

2. Open research question 3

3. Existing and related work 4

4. Research approach 5

5. Personal investment 6

6. References 7

Part 2 8

1. Introduction of research specialism 8

2. Open research question 8

3. Existing and related work 9

4. Research approach 10

5. Personal investment 11

6. References 12

Part 1: AI and Robotics

1. Introduction of research specialism

Introduction of AI and Robotics Specialism

Artificial intelligence (AI) and robotics is a specialism in computer science that links conceptual grounding in intelligent systems with theoretical knowledge in the practicing environment (Martinetti et al., 2021). The application of AI and robotics range from medicine to entertainment with significant expansion in the scope of practice. AI and robotics are two different concepts that are interdependent (Bicchi et al., 2009). For instance, artificial intelligence (AI) is a branch of computer science that involves the intention of developing computer programs that can complete tasks that require human intelligence. This is achieved by developing and programming AI algorithms that can tackle learning, problem-solving, perceptions, logical reasoning, and language understanding. On the other hand, robotics involved the development of physical robots (programmable machines that can undertake tasks autonomously or semi-autonomously (Menon & Holthaus, 2019). Robots can interact with the physical world via actuators and sensors and programmable algorithms. Artificial intelligence and robotics are mutually interdependent and influence each other (Ahmad et al., 2017). In some cases, robotics may require artificial intelligence, and in some other cases, they do not require artificial intelligence based on the complexity of tasks and the need for intelligent decisions using input and outputs.

1. Open Research Question: Safety and Human Interactions

The article by Holthaus et al. (2019) believes that safety and human interaction are some of the topics discussed. From the authors, safety and human interaction is important aspect to consider in robotics. AI and robotics require an assessment to evaluate their ability to alert users or act in coordination with a user about hazards and mitigation. In real-life applications, safety and human interaction capabilities are integrated into areas such as speed monitoring systems, sat-navs, cockpit monitoring systems, medical devices, and automated vehicle operational alerts. In all these real-life applications, there is a potential risk for disengagement of the user. If human engagement is not undertaken following an alert of potential hazards by these systems, there may be challenges in mitigating the hazard. Methods used for alert or interruption by these AI and robotics systems may influence the disengagement of the user. For instance, the authors identified that method of alert or interruption in sat-nav and speed monitoring systems on speed may be switched off due to irritation of the alerts despite the speed warning helping to improve safety.

In automotive domains, Holthaus et al. (2019) identified that there exists evidence of accidents that occur due to disengagement of the user with the system. Ignoring the alerts repeatedly may have negative impacts on the safety of users. This question is very critical to scientific evidence and provides an effective ground for the enhancement of safety and human interactions with AI and robotics systems. While artificial intelligence and robotics may provide a very effective alert system, there is a need to evaluate the interaction with the user to ensure potential risks in safety or hazards are minimized. AI and robotics interaction with human users offer a physical safety dimension linked to enhancing the safety of users. When the robotics and artificial intelligence systems have high predictive behavior for hazards, there is enhanced safety of users who interact effectively with the system alert during disengagements.

1. Existing and Related Work

Research on Safety and Human Interactions in AI and Robotics

Different scholars have evaluated the issue of robots-human interaction on social behavior and safety functionality. In Lee et al. (2015) study, the author identified that physical interaction between human operators and robots results in physical safety dimensions associated with the protection of workers from harm through this form of interaction. Therefore, there is a need to focus on versatility and autonomy by identifying the less predictable robots for human operators to effectively collaborate for enhanced safety. From the author, the potential harm is not only linked to the potential for physical harm, but also social interactions that may lead to cognitive underload, passivity, and depression. In another study by Martinetti et al. (2021), the author identified social aspects of human-robot interaction on the issue of trust that may affect trust level. Under-trust in the robot-human interaction may result in high-risk behavior that compromises physical and mental safety. Additionally, the author noted that limited trust may result in collaboration and acceptance problems.

On the other hand, performance monitoring of workers may cause mental health harm due to anxiety, the overlap between work and life, and work surveillance. In Holthaus, et al.'s (2019) study, the interaction between humans and robots may result in different approaches associated with problems associated with safety if the alerts get ignored or result in disengagement. Findings revealed that intelligent assist devices (IADs) go beyond conventional notions for the safety of robots in the protection of human users from harm including cumulative trauma disorder. The findings further revealed that intelligent assist devices (IADs) and physical human-robot interaction may also lead to harm, which emphasizes the value of reliability and safety standards to be reevaluated.

From these studies, there is a further inquiry that is required in evaluating the concept of human-robot interaction and enhancement of safety. One emerging question is, what measures must be taken to improve psychosocial and physical safety in robot-human interactions? Another question is, what approaches should be undertaken to ensure robots are cognizant of human behavior when they provide alerts? Could improving the nature and forms of alerts result in increased safety by increasing compliance in disengagements and response to prevent harm? These fundamental components remain answered in the sources reviewed. Evaluating these questions or gaps may provide sufficient information on robot-human interaction and safety performance by evaluating the robot’s social actions and safety performance effectiveness (Giuliani et al., 2010). Therefore, the gaps can be sealed by identifying how social deficiencies of a robot may undermine perceived authority in alerting a user to hazards in the work environment.

1. Research Approach

In answering the questions identified, a quantitative research method is the most appropriate since most of the judgments and evaluations of the robot's social credibility and effectiveness of its authority to safety functions. To evaluate these aspects, an experimental design would be appropriate, which could evaluate the adherence of people to safety-related alerts by robots (Colgate et al., 2008). The approach will need an evaluation of circumstances and factors that influence adherence to the safety alerts by robots. Since the experimental will involve human participants, a full review may be required to ensure that there are minimal risks. This ensures that safety alerts do not lead to fateful or injuries when the participant ignores the safety alert. In the proposed research, the experiment would focus on the level of trust in robots and the response to safety alerts. The study is intended to evaluate the influence of the level of trust in robots and response to safety alerts (Bankins & Formosa, 2020). The question to be answered is, does the level of trust in robots influence the response to safety alerts during human-robot interaction?

First, the experiment will take the safety rating for the robots by the participants while the second approach will involve identification of reaction to safety or hazard alert. This research is meaningful since it would help in evaluating ways that level of trust in robots would have in adherence to safety or hazard alerts. Organizations that have deployed robots to automate or augment human operations may benefit from this research since they can base the findings in drafting their training to the teams on response to hazard or safety alerts by the robots. Addressing the issue of trust and elevating the understanding of staff on the value of assessing the level of trust would have in aligning them to respond to hazard or safety alerts (Ahmad et al., 2017). As a result, the workplace can be more secure by educating the staff working with robots on the need to adhere to hazard or safety alerts, which may help in preventing potential risks (Ahmad et al., 2017). Using the experimental design, one can identify the willingness and thoroughness to respond to robot safety or hazard alerts.

1. Personal Investment

To undertake the experiment, I believe I should be clear of the intended goals and practices that are required to make the experiment successful. A better understanding of AI and robotics coupled with computer science literacy maybe my biggest strength in the assessment of the potential risks involved in the experiment (Ahmad et al., 2017). Another strength is thorough research on previous studies to gain the knowledge for successful deployment of the experiment (Colgate et al., 2008). Submitting my experimental design to the Ethics Committee in the institutional could help in identifying the potential for harm or hazards in experimenting for the participants to ensure the safety and potential risks are minimized below the normal range (Ahmad et al., 2017). These measures may ensure that the experiment does not pose a significant risk to participants as an ethical requirement that I must fulfill.

6.References

Ahmad, M., Mubin, O. and Orlando, J., 2017. A systematic review of adaptivity in human-robot interaction. Multimodal Technologies and Interaction, 1(3), p.14.

Bankins, S. and Formosa, P., 2020. When AI meets PC: Exploring the implications of workplace social robots and a human-robot psychological contract. European Journal of Work and Organizational Psychology, 29(2), pp.215-229.

Bicchi, A., Peshkin, M. A., & Colgate, J. E. 2009. Safety for Physical Human-Robot Interaction. Springer Handbook of Robotics 57, p. 1335–1348. Doi: 10.1007/978-3-540-30301-5\_58

Colgate, E., Bicchi, A., Peshkin, M.A. and Colgate, J.E., 2008. Safety for physical human-robot interaction. In Springer handbook of robotics (pp. 1335-1348). Springer.

Giuliani, M., Lenz, C., Müller, T., Rickert, M. and Knoll, A., 2010. Design principles for safety in human-robot interaction. International Journal of Social Robotics, 2(3), pp.253-274.

Holthaus, P., 2021. How does a robot's social credibility relate to its perceived trustworthiness? arXiv preprint arXiv:2107.08805. https://arxiv.org/abs/2107.08805.

Holthaus, P., Menon, C. and Amirabdollahian, F., 2019. How a robot’s social credibility affects safety performance. In International Conference on Social Robotics (pp. 740-749). Springer, Cham.

Lee, J.G., Kim, K.J., Lee, S. and Shin, D.H., 2015. Can autonomous vehicles be safe and trustworthy? Effects of appearance and autonomy of unmanned driving systems. International Journal of Human-Computer Interaction, 31(10), pp.682-691.

Martinetti, A., Chemweno, P.K., Nizamis, K. and Fosch-Villaronga, E., 2021. Redefining safety in light of human-robot interaction: A critical review of current standards and regulations. Frontiers in Chemical Engineering, p.32.

Menon, C. and Holthaus, P., 2019. Does a loss of social credibility impact robot safety? PESARO 2019. http://uhra.herts.ac.uk/handle/2299/21473.

**Part 2: Cyber Security specialism paper**

## 1. **Introduction of research specialism**

The wireless technology is applied in different forms and providing solution in terms of security and availability (Abdallah, Abd Razak and Ghalib, 2019). The different risks are unmanaged and using of WLAN computer communication provide aid to maintain security standard. The attackers are monitoring network for learning vital network information. With the help of MAC address, it is easy to move forward. The different approach is applied to notice probe request attacks in context of IEEE 802.11 network. The study has analyzed genuine occasion transfer capture on wireless house system. The main aim is to detect attack at early phase by doing effective communication and accomplish better outcomes. From the experiment, it has experiential that WLAN transfer is applied in random and usage are depended and application of operating system for users and accomplish highest results. Moreover, WLAN traffic as well as parallel processing has known cause of significant quantity of overhead to monitor STA as well as know performance of it.

## 2. **Open research question**

The research specialism is based on a clever move towards for detect probe request attack in IEEE 802.11 systems. For this investigate work, open research query are framed. The open research questions are as follows:

* Is wireless local area network important for probe request as well as response manages?

The configuring wireless leads to access and enhances using of laptop computers as well as wireless access devices within business to rise in mobility of worker and meet with demand (Ahmadpour and Kabiri, 2020). The wireless technology has analysed incompatibility issues as well as vendor specific products. The slow in technology, reserved and expensive are for mobile situations or environments to know all impossible aspects. The industry standards lead to cause levelling point.

* What are the ways to detect probe request attacks (PRA)?

Probe requests mainly promote mobile station that are support through data tax as well as 802.11 capabilities like 802.11n (Mohammadnia and Slimane, 2020). They have compatible rate of data where probe response is provided to advertising SSID and supported through data tax, encryption kinds if needed and other 802.11 and capability of AP. The probe response is providing required information which device are required to trigger authentication procedure on wireless network.

* What is the usage of IEEE 802.11 networks?

It is highly used in office as well as home network that allow to printers, smartphones and laptops and other device for communicating one another and access internet without doing any connection (Bayrakdar, 2019). It is regarded as collection of standards to connect LAN and provide to consumers and accomplish desired outcomes in effective way. The 802.11b has transmitted in 2.4 GHz to know frequency brand of radio spectrum and handle 11megabits to enhance speeds and other aspects and gain outcomes. It is highly used to make work easier and simple and accomplish desired results.

## 3. **Existing and related work**

From the provided research paper, it has found that intrusion detection is identifying unauthorized users for gaining to access and compromised computer network (Chatzisofroniou and Kotzanikolaou, 202). The researchers need to look for several solutions. For instance, there is need to review non-intelligent methods to detect and prevent DoS attack in MAC coating and assess non-cryptographic ways for send-up detection in WLANs. This is expensive and required protocol repair and knows DoS target for improving in organization frame through joint key. The answer required modification in wireless card and hardware upgrade in context of providing unrealistic solution to know changes. The detection of frames is playing effective role in detection of attacks which include probe request attacks. The introduction has algorithm for detect MAC spoofing that is focused on figure gap through leveraging performance as well as arrangement of meadow It has utilized combination for sequence of window along with knowing traffic inter-arrivals statistics to detect traffic and spoof in context of wireless networks. The WIDs methods is applied to use, rule based and statistical for recognized pattern approach for knowing all types of attack signatures and lack of time, flexibility to adopt change environment and accomplish desired outcomes.

It has also presented that there is analysis of comparative of IDS approaches (Korolkov and Kutsak, 2021). The ANN is rising and established approach for IDS to know unpredictable behavior for several attacks and networks. The high intelligent is needed for IDSs for using TCP to know self-organizing maps. There is usage of different aspect and knowing Fuzzy inference system as well as using of hybrid models. It has introduced prototype of standalone WID as well as response on basis of Net Stumbler attacks. The solution is to detect attacks through calculation of probe needs for each moment. This also responds to assailant with help of DoS assault in term of return that leads to attack possess users. This is presenting business uncovering architecture which is based on clever agents with authority of auto-learning, Fuzzy logics and incorporate NN. This is large and complex system to implement as per knowledge and distribute with usage of IDS agents and falling shorts of implementations. It proposes comparative complex architecture to apply WIDs and using ANNs that is focused on genuine occasion information and using transporter intelligence, deluge and de-authentication for knowing all types of attacks. The main solution is to focuses on behavior of finish network that is challenging aspect in context of real network that consists of a greater number of users. (Satam and Hariri, 2020).

## 4. **Research** **approach**

The research approach is based on philosophy which has defined three kinds of frames namely control, measurement and data (Sethuraman, Dhamodaran and Vijayakumar, 2019). In case of management, it is made establish as well as maintain communications, control has helped in context of data delivery and each are consisting of MAC slogan, corpse and border check sequence. The MAC slogan leads frame manage, period, series manage, address and control information. There is also need of QoS data frame, QoS manage in order. There is frame that is applied for several information ton frame type as well as subtype. There is usage of FCS in context of IEEE 32-bit cyclic unemployment make sure to accomplish better results. Moreover, series number of MAC border that is 12-bit counter which has started from zero and starting of other aspect to wraps overflow. The parallel sequence has pattern and generated with same MAC address.

SSI has made frame to capture Wireshark to provide indication of received transmission power of NI and provide indication of location. SSI consists of patterns that are useful to detect spoofed attacks and leads to accomplish desired outcomes in effective way. The delta time value of wireless need to capture from all time and possess previous packet and useful in order to identify attacks and know attendant reply time and system around journey occasion and delay with the analysis of WLAN test bed, it is easy to statistically and detect to provide attack that are likely because of controlled nature. WIDS is clever to imprison and examine frame and know attack in live environment that is not predictable through help of nature.

With the consideration, it is easy to know dissimilar model and possible sensible as well as well-organized request on discovery of probe request attacks (Sontowski and et. al., 2020). The research needs to utilized and feed forward NN to move with architecture with input neurons and others.

## 5. **Personal investment**

From this research work, I have learned that it is important to identify external attacker with analyses of traffic generation from consumer MAC to speak to in solitary incidence for wireless local area network (Kutsak, 2021). The supervise has moved presumptuous for neural net within separate input in terms of delta-time, sequence number, frame and sign power and consists of sub-type that is applicable to identify as well as make differentiation from several rogue frame. The experimental provides results to apply neural system to notice search ask for that attack in case of lofty accuracy. With the adoption of new aspect, it is easy to allow WLAN users to move from one place to another in provided signal area. The research has enhanced my skills and knowledge to get more information of assigned topic and accomplish desired outcomes. Moreover, it enhances experiment with help of monitoring to coordinate several stations.

## 6. **References**

Abdallah, A. E., Abd Razak, S. and Ghalib, F. A., 2019, September. Deauthentication and disassociation detection and mitigation scheme using artificial neural network. In International Conference of Reliable Information and Communication Technology (pp. 857-866). Springer, Cham.

Ahmadpour, D. and Kabiri, P., 2020. Detecting forged management frames with spoofed addresses in IEEE 802.11 networks using received signal strength indicator. Iran Journal of Computer Science, pp.1-7.

Bayrakdar, M. E., 2019. Priority based health data monitoring with IEEE 802.11 af technology in wireless medical sensor networks. Medical & biological engineering & computing. 57(12). pp.2757-2769.

Chatzisofroniou, G. and Kotzanikolaou, P., 2021. Association Attacks in IEEE 802.11: Exploiting WIFI Usability Features. In Socio-Technical Aspects in Security and Trust: 9th International Workshop, STAST 2019, Luxembourg City, Luxembourg, September 26, 2019, Revised Selected Papers 9 (pp. 107-123). Springer International Publishing.

Korolkov, R. Y. and Kutsak, S. V., 2021. ANALYSIS OF ATTACKS IN IEEE 802.11 NETWORKS AT DIFFERENT LEVELS OF OSI MODEL. Natsional'nyi Hirnychyi Universytet. Naukovyi Visnyk. (2). pp.163-169.

Kutsak, S. V., 2021. ANALYSIS OF ATTACKS IN IEEE 802.11 NETWORKS AT DIFFERENT LEVELS OF OSI MODEL. Scientific Bulletin of National Mining University, (2).

Mohammadnia, H. and Slimane, S. B., 2020, April. IoT-NETZ: Practical spoofing attack mitigation approach in SDWN network. In 2020 Seventh International Conference on Software Defined Systems (SDS) (pp. 5-13). IEEE.

Satam, P. and Hariri, S., 2020. WIDS: An anomaly-based intrusion detection system for Wi-Fi (IEEE 802.11) protocol. IEEE Transactions on Network and Service Management, 18(1), pp.1077-1091.

Sethuraman, S. C., Dhamodaran, S. and Vijayakumar, V., 2019. Intrusion detection system for detecting wireless attacks in IEEE 802.11 networks. IET networks. 8(4). pp.219-232.

Sontowski, S., Gupta, M., Chukkapalli, S.S.L., Abdelsalam, M., Mittal, S., Joshi, A. and Sandhu, R., 2020, December. Cyber-attacks on smart farming infrastructure. In 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC) (pp. 135-143). IEEE.