

Drivers' Understanding of Artificial Intelligence in Automated Driving Systems: A Study of a Malicious Stop Sign

Katherine R. Garcia, Scott Mishler and Yanru Xiao, Old Dominion University, Norfolk, VA, USA, Cong Wang, George Mason University, Fairfax, VA, USA, Bin Hu, Jeremiah D. Still and Jing Chen , Old Dominion University, Norfolk, VA, USA

Automated Driving Systems (ADS), like many other systems people use today, depend on successful Artificial Intelligence (AI) for safe roadway operations. In ADS, an essential function completed by AI is the computer vision techniques for detecting roadway signs by vehicles. The AI, though, is not always reliable and sometimes requires the human's intelligence to complete a task. For the human to collaborate with the AI, it is critical to understand the human's perception of AI. In the present study, we investigated how human drivers perceive the AI's capabilities in a driving context where a stop sign is compromised and how knowledge, experience, and trust related to AI play a role. We found that participants with more knowledge of AI tended to trust AI more, and those who reported more experience with AI had a greater understanding of AI. Participants correctly deduced that a maliciously manipulated stop sign would be more difficult for AI to identify. Nevertheless, participants still overestimated the AI's ability to recognize the malicious stop sign. Our findings suggest that the public do not yet have a sufficiently accurate understanding of specific AI systems, which leads them to over-trust the AI in certain conditions.

Keywords: Malicious attack, artificial intelligence computer vision, artificial intelligence in automated driving systems, understanding of artificial intelligence, trust in artificial intelligence

Many components within an Automated Driving System (ADS) contribute to the

Address correspondence to Jing Chen, Department of Psychological Science, MS-25, Rice University, 6100 Main Street, Houston, TX 77005, USA.
Email: jingchen@rice.edu

Journal of Cognitive Engineering and Decision Making
Vol. 0, No. 0, ■■ ■, pp. 1-15
DOI:10.1177/15553434221117001
Article reuse guidelines: sagepub.com/journals-rmissions
© 2022, Human Factors and Ergonomics Society.

successful operation for Levels 3 to 5 driving automation systems, defined by the Society of Automotive Engineers (SAE International, 2021). In ADS, the vehicle is responsible for object and event detection, recognition, classification, and response (SAE International, 2021). Various sensors on the vehicle capture the roadway data and translate it into information that supports real-time decisions. Artificial Intelligence (AI) plays an important role in this process, and ultimately the safe and secure operation of the ADS.

An AI driven ADS must learn how to operate a car and monitor for potential hazards. Any error made by the AI at any step in the process could be hazardous to nearby humans and property. Currently, with SAE Level 3 ADS, humans are still required in the driver's seat as they might be asked to take over control from the ADS when the system fails or is about to fail (SAE International, 2021). Technically, the Level 3 ADS allows the driver to engage only when prompted by a takeover request. For the human drivers to quickly and safely take over, they are expected to understand the possible failure communicated by the vehicle before the failure causes harm. However, there is still a lack of understanding of users' perception and trust while partnering with ADS. This study measured participants' AI related knowledge, experience, understanding, and trust, and examined their perception of how the AI technology would classify original, as well as maliciously manipulated, stop signs in Level 3 ADS.

ARTIFICIAL INTELLIGENCE

AI is crucial for many systems people use today. From online facial recognition software on social media platforms to voice-activated

speech systems in homes, AI is used to gather, interpret, and make decisions in a similar way to humans (Cunneen et al., 2019; Kaplan & Haenlein, 2019). AI in a system can have very narrow and specific functions or broad and advanced capabilities that combine several complex processes. This new AI era is expected to result in faster and better services than humans can produce (Grace et al., 2018). However, the more complex an AI system, the greater the chance of erroneous conclusions or decisions. In the context of ADS, the erroneous conclusions or decisions can potentially harm the well-being of the driver and other road users, as well as property damages (Halim et al., 2016).

Artificial intelligence is vulnerable to adversarial inputs, and even minimally perturbed noise added to the images can easily lead the AI to wrong decisions (Goodfellow et al., 2014). These vulnerabilities have deep roots in the fundamental AI algorithms and span almost all AI applications. When an attacker slightly modifies the inputs (image pixels) in the directions of *maximizing* the loss function, the AI is bound to yield an incorrect decision as the original AI algorithms are designed to *minimize* a loss function by iterating through the training data. Research has further shown that these attacks can successfully transfer to an unknown (black box) AI model due to the similarities between their decision boundaries on the same task (Qiu et al., 2019). So far, it is still an open question why AI is robust to additive random noise (e.g., Gaussian white-noise) but susceptible to purposed perturbations, and how this contradiction connects to human vision given that humans can easily identify both images with random noise and those with perturbations (Yu et al., 2019).

Trusting Artificial Intelligence

For an automated system to function properly, a user's trust calibration is essential (Hoff & Bashir, 2015; Lee & See, 2004). Over-trusting the system could result in problematic errors going through uncorrected, but under-trusting the system could prevent the reaping of system benefits (Parasuraman & Riley, 1997). The collaboration between humans and AI to

holistically approach challenges is the key to developing human-AI trust relationships (Asan et al., 2020). An appropriate level of user trust is needed in order to fully gain AI's potential benefits; this can be accomplished by developing AI with bias detection and mitigation techniques, and the ability to explain their decision-making process (Rossi, 2018). Similar to interpersonal trust (i.e., trust between people), human-AI trust focuses on the vulnerability of the human user and their ability to anticipate the outcome of the AI's decision (Jacovi et al., 2021).

The difference between human-AI trust and human's trust in other technology lies in the new features, performance, process, and purpose of AI compared to other technologies (Siau & Wang, 2018). Human-AI trust initially builds through representation of the AI, the image or perception the human has of AI, reviews from other uses, transparency and ability of the AI to explain its behaviors and decisions, and the human's ability to try the AI before accepting or adopting it (Siau & Wang, 2018). Human-AI trust then continues to develop through usability and reliance of the AI, collaboration and communication between the human and AI, sociability and bonding between the human and AI, security and privacy protection of the user's information by the AI, interpretability of the AI's rationale, job replacement of human performance with AI, and goal congruence between the human and AI (Siau & Wang, 2018). With this aspect of usability and reliance, humans can trust AI to help aid them with important decisions such as medical decisions (Ferrario et al., 2021).

Understanding Artificial Intelligence

Understanding how the AI works, what it is capable of, and maintaining a proper amount of trust is crucial for optimal system performance. AI systems are likely to make errors (Prahl & Goh, 2021; Russell et al., 2017). It is common to have a human providing oversight (Jarrahi, 2018). Humans monitor when the system fails to work as intended and interject to prevent or correct the error (Bansal et al., 2019). For example, consider a daily use case of a voice

recognition system on cellular phones. The voice recognition system often misunderstands the user and performs the wrong actions. However, the user can easily notice the error and act to quickly resolve it; sometimes, the user even modifies their future behavior in similar situations to avoid a repeat frustration. Many users still rely on the voice recognition system in most cases because it typically performs adequately. However, the user needs to understand the capabilities and limitations of the AI system to compensate when the AI makes errors.

There have been mixed findings of how the public perceive AI. Some people see AI as an adversary and challenge the idea of using it; some see it as a servant, built to follow orders; and others see AI as future cooperative partners and are willing to working together with it (Hengstler et al., 2016; Oh et al., 2017, 2018). Past experience with AI has also been found to impact the willingness to use it (Hengstler et al., 2016; Hoff & Bashir, 2015; Oh et al., 2017). For example, Wiegmann and colleagues (2001) found that trust in an automated diagnostic aid can be lost quicker than it can be regained. Examining how people perceive AI helps inform researchers about how much the users will trust, use, and rely on it.

Artificial Intelligence in Driving

ADSs are an open-loop process and requires the completion of complex tasks, which require the utilization of AI. The different functions include Adaptive Cruise Control, Lane Departure Sensor, Collision Avoidance, Parking Assist, and many others. The present study focused on the AI of computer vision that is essential for these functions. For example, computer vision and sensor data processing are used to represent the environment, plan routing, execute the path navigation, and monitor changing conditions to ensure everything is functioning appropriately (Halim et al., 2016; Ma et al., 2020; Zhang et al., 2016). This study focused on one specific task of AI employing computer vision to recognize road signs.

Computer vision is required to identify a wide variety of objects on the road, including road signs, road markings, other vehicles,

pedestrians, obstacles on the road, and so on. Critically, the system needs to operate within the rules governing roadway operations. For instance, it must recognize and identify a stop sign. The physical act of data collection through sensors and computer vision is noisy, which causes uncertainties for decisions and lowers the detection likelihood or successful categorization of objects (Kendall & Gal, 2017). Special weather conditions like fog or snow can obscure sensors, or signs can be obscured by markings and stickers or wear and tear (Ma et al., 2020). In addition, many road signs during a driving expedition may be defaced or altered in some way, such as a sticker placed on a stop sign beckoning the viewer to “Stop Eating Animals.” Alternatively, malicious attackers might exploit AI vulnerabilities and fool the AI to misclassify road signs, which impairs the ADS from functioning safely (Liu et al., 2021). Given that these malicious attacks do not usually affect human vision, a prompt takeover from the human driver can help ensure the safety of the ADS. However, the immediate takeover would require human drivers to be aware of these AI vulnerabilities to predict when the AI might fail.

Current Study

Understanding the public’s perception of general AI systems and those used in their vehicle is essential to designing a safe and secure system for them to use. Previous studies focused mainly on the AI’s ability to classify various images (Eykholt et al., 2017; Liu et al., 2021; Ma et al., 2020). However, little research has focused on human perception of the AI’s capabilities regarding these images in ADS. The current study aims to answer the question, are typical human drivers aware of the AI capabilities and vulnerabilities? The answer to this question sets the stage for future research to investigate how these AI characteristics should be conveyed to human drivers. We used a stop sign with a well-known malicious attack in the AI research community as a testbed and investigated participants’ perception of the AI’s capability of identifying the stop signs in comparison to their own ability. The malicious attack produced the worst classification

performance by current AI technology (Eykholt et al., 2017), which would lead to the most noticeable results compared to a stop sign without any attack with the best classification performance.

We measured potential factors that may affect the public's perception of the AI capabilities, including individuals' knowledge of AI, experience with AI, and trust in AI. Specifically, knowledge of AI measured how much the user knew about the uses and applicability of AI, experience with AI reflected how much the user had encountered and used AI, and trust was captured by employing the Jian and colleagues (2000) survey that evaluates a user's trust in an automated system.

We hypothesized that participants with a higher understanding of AI would be more trusting of AI than those with less knowledge (Shin, 2021). Participants who have more understanding of the concepts and technology that AI uses were predicted to have more trust in the AI since they understand the processes and rationale behind the AI's decisions and behaviors. And we expected exposure to AI and knowledge of AI, both in general and specifically for ADS, to be positively correlated (Holzinger et al., 2011; Reig et al., 2018). The more experience a user has with AI, the more likely they will know AI applications. Lastly, we expected participants to identify both the standard and altered stop signs because both images still resemble a stop sign. However, it was exploratory whether participants would report that an AI would identify the altered stop sign. The AI would have difficulties identifying the altered stop sign because the noise added to the image would disrupt the computer vision techniques (Kendall & Gal, 2017). Still, this knowledge may not be readily available to common drivers.

This manuscript contributes to the human-AI collaboration literature by adding a deeper understanding about human perception regarding AI capabilities. On the one hand, this study adds to the knowledge of how humans perceive, understand, and trust complex technologies like AI. On the other hand, this study highlights the importance of adequately relaying AI's capabilities to novice users properly.

The rest of this manuscript first introduces the methods used for this study including the participants, materials, experimental design, and procedures in the Method section. Following, the Results section describes the results from the study which were analyzed based on the participants' perception of human's and perceived AI's ability to classify stop signs, relations between AI knowledge, exposure and understanding, and lastly, relations between knowledge, understanding and trust. Finally, in the Discussion section we discuss the findings, implications of our study, and limitations and future research.

METHOD

Participants

Two hundred eighty-one participants were recruited through Old Dominion University's online research participation system (SONA; oduppsychology.sona-systems.com). The mean reported age was approximately 21 years ($N = 267$, $SD = 5.30$). Participants reported their gender as either female ($N = 205$), male ($N = 64$), or other ($N = 3$), or chose not to respond ($N = 9$). Participants reported their race as White ($N = 111$), Black or African American ($N = 104$), Asian ($N = 17$), Native Hawaiian or Pacific Islander ($N = 2$), American Indian or Alaska Native ($N = 1$), and Mixed/Other ($N = 37$), or chose not to respond ($N = 9$). All participants received credit towards a course research experience requirement.

Materials

The study was presented through a Qualtrics survey (odu.qualtrics.com). This survey contained 62 questions in eight sections (see the Appendix). The first section, general AI knowledge, through the sixth section, trust in AI, were all on a 1 to 7 scale, where 1 represents low knowledge, exposure, understanding, and trust, and 7 represents high knowledge, exposure, understanding and trust. The seventh section, stop sign judgment, was on a 1 to 5 scale, where 1 represents low agreeance with the statement, and 5 represents high agreeance with the statement regarding the stop-sign image type

and agent type. Due to an oversight when implementing the survey, the scale of the questions in this section was not intentionally designed to match the earlier sections. The eighth section, descriptive information, had several answer choices the participant could choose from and some questions asking them to input a number. The sections were organized as follows.

- The first section was *the general AI knowledge section*, which asked about the participant's understanding of AI in general and contained ten questions. An example statement included in this section was, "AI is required for *conversation with Chatbots*."
- The second section was *the exposure to AI section*, which asked participants about their previous AI exposure in general and contained five questions. An example statement included in this section was, "I have seen AI discussed in social media."
- The third section was *the knowledge of AI in ADS section*, which asked participants about their general understanding of AI in the context of ADS and contained five questions. An example statement included in this section was, "I am aware of how autonomous driving systems use AI."
- The fourth section was *the applications section*, which asked participants about their understanding of the applications of AI in ADS and contained six questions. An example statement included in this section was, "For autonomous driving, AI is required for the detection of *road signs*."
- The fifth section was *the future prospects of AI in ADS section*, which asked participants about their understanding of AI in ADS for the future and contained six questions. A statement included in this section was, "AI will revolutionize driving in a good way."
- The sixth section was *the trust in AI section*, which asked participants about their opinions of AI and contained seventeen questions. These trust questions were adapted from [Jian and colleagues \(2000\)](#).
- The seventh section was *the stop-sign judgment section*, which contained two unique stop-sign images: an original stop sign and a stop-sign image with the malicious attack (see [Figure 1](#)).



Figure 1. Original (left) and malicious (right) images of a stop sign.

- The image with the malicious attack was generated using the algorithms [Eykholt and colleagues \(2017\)](#) proposed, which focused on how intentional perturbations for images can inhibit visual classification by an AI. The malicious stop sign was an intentionally perturbed image meant to prevent AI from properly classifying the sign, and the study showed a 0% accurate classification rate by the current AI technology ([Eykholt et al., 2017](#)). These two types of images were used because they were the types that produce the best and worst classification performance by the current AI algorithms, which would lead to the most dramatic results, if any, in this initial exploration of drivers' understanding of AI capabilities and vulnerabilities. Participants were asked to rate how much they agreed or disagreed with the statements that they thought the image is of a stop sign and if current AI technology would classify the image as a stop sign. This section contained four questions.
- The last section was *the descriptive information section*, which contained nine questions regarding the participant's technology familiarity, age, gender, race, education, and driving experience, derived from [Kyriakidis and colleagues \(2015\)](#). There was also a last open question asking participants if they had any comments regarding the survey.

Two attention checks were included in this study to ensure that participants were reading and comprehending the questions. The attention checks both stated, "For this question, you are required to choose the *strongly disagree* option below." If participants did not strongly disagree for both of these attention checks, their data were

excluded from the analyses. The first attention check was located at the end of the third section, knowledge of AI in ADS, and the other was located at the end of the fifth section, future prospects of AI in ADS.

Experimental Design

Each participant answered all the questions in all eight sections. For the stop-sign judgment section, two independent variables were manipulated within-subjects: agent type (humans vs. AI) and image type (original vs. malicious). In this seventh section, the dependent variable was the participants' agreement rating (1–5) on the humans and AI agent statements, given an image, that a human or an AI could identify or classify the image as a stop sign.

The first independent variable was the agent type. Participants reported their perception of how the agent would classify the images. The agent was either the participant themselves (i.e., humans) or the AI. For the humans, the statement asked how much the participant agreed with, "I think this image shows a stop sign." For the AI, the statement asked about their perception of the current AI technology's ability to classify the image, "I think the current AI technology will classify this as an image of a stop sign."

The second independent variable was the image type. The image type reflected whether the sign had been tampered with or not (original or malicious image; see [Figure 1](#)). For the original image, the image was a standard stop sign. For the malicious image, the image was the same stop-sign image, but it had been manipulated with a multicolor transparent film over the original image using the algorithm proposed in [Eykholt and colleagues \(2017\)](#). Participants were not told that the malicious image was "malicious" to keep their responses unbiased. They viewed one image of the stop sign (either original or malicious) with one agent statement (human or AI) a total of four times for all possible combinations.

Procedure

Upon beginning the online study, participants were welcomed and told they would answer

questions about their thoughts and opinions on Artificial Intelligence (AI) and related applications. Participants were told that the survey was about their opinions and personal ideas of AI, that it was not a test of their knowledge, and that there was no right or wrong answer. They were not provided with definitions regarding the survey or AI because this study was aimed to examine participants' understanding of AI. All participants completed the eight sections in the same order. After participants completed the last section of the survey, they would submit it and receive their SONA credit within the following few days.

RESULTS

Participants who missed at least one of the two attention checks were excluded from data analysis. Of the remaining 205 participants, 201 chose to report their age ($M = 21.67$, $SD = 5.74$); 151 indicated their gender as female, 51 as male, and three as other. When asked about race, 90 participants identified as White, 72 as Black or African American, 11 as Asian, and 32 as Mixed/Other. In the last open question, only one participant out of the 281 commented on possible safety and privacy concerns. The following analyses were performed on the remaining 205 participants that met the criteria of completing the survey and passing both attention checks.

Ability to Classify Stop Signs

A 2 (agent: humans vs. AI) x 2 (image type: original vs. malicious) within-subjects analysis of variance (ANOVA) was conducted to determine how these factors affected participants' ratings of whether the agent could successfully identify the stop-sign images. The assumption of sphericity was met. See [Table 1](#) for the full ANOVA results.

The main effect of agent was significant, $F(1, 204) = 121.76$, $p < .001$, $\eta_p^2 = .37$, with the rating of the human agent ($M = 4.94$, $SE = 0.02$) being higher than that of AI ($M = 4.32$, $SE = 0.06$). The main effect of image type was also significant, $F(1, 204) = 41.15$, $p < .001$, $\eta_p^2 = .17$, with the rating of the original image ($M = 4.73$, $SE = 0.03$) being higher than that of the malicious image ($M = 4.53$, $SE = 0.04$).

Table 1. Analysis of Variance for Ratings by Agent and Image Type.

Source	SS	df	MS	F	η_p^2
Agent	78.68	1	78.68	121.76***	.37
Error	131.82	204	0.65		
Original image	44.02	1	44.02	70.73***	.26
Error	126.98	204	0.62		
Malicious image	123.32	1	123.32	118.85***	.37
Error	211.68	204	1.04		
Image type	7.81	1	7.81	41.15***	.17
Error	38.70	204	0.19		
User agent	0.31	1	0.31	4.06*	.02
Error	15.69	204	0.08		
AI agent	25.29	1	25.29	37.73***	.16
Error	136.71	204	0.67		
Agent x image	5.00	1	5.00	27.17***	.12
Error	37.51	204	0.18		

*** = $p < .001$, * = $p < .05$.



Figure 2. Ratings for each of the four stop-sign conditions. *Note.* Human Original = if the participant thinks the image is a stop sign; Human Malicious = if the participant thinks the malicious image is of a stop sign; Artificial Intelligence (AI) Original = if the participant thinks the AI could recognize the image as a stop sign; AI Malicious = if the participant thinks the AI could recognize the malicious image as a stop sign. Error bars are 95% confidence intervals.

In addition, the interaction between agent and image type was significant (see [Figure 2](#)), $F(1, 204) = 27.17, p < .001, \eta_p^2 = .12$. Follow-up tests of simple main effects revealed that, for the human agent, the ratings of the original image

($M = 4.96, SE = 0.02$) were significantly greater than the ratings for the malicious image ($M = 4.92, SE = 0.02$), $F(1, 204) = 4.06, p = .045, \eta_p^2 = .02$. For the AI agent, the ratings of the original image ($M = 4.50, SE = 0.05$) were

significantly greater than the ratings for the malicious image ($M = 4.15$, $SE = 0.07$), $F(1, 204) = 37.73$, $p < .001$, $\eta_p^2 = .16$. The significant results of interaction and the simple main effects showed that the participants rated both the AI and themselves to be less capable of identifying the image as a stop sign for the malicious image than for the original image, but the reduction for the AI was greater than that for themselves.

To test whether participants' perception of their and the AI's ability to identify the stop signs correlated with their understanding, knowledge, or trust in AI, we conducted Spearman's rank correlational analyses with a Benjamini–Hochberg alpha correction. The analyses included correlations between their ratings on the AI's capability of identifying the original and malicious stop signs and their self-reported understanding of AI in general and AI in ADS, knowledge of AI in general and AI in ADS, and trust in AI in general and AI in ADS. Self-reported general understandings of AI positively correlated with participants' ratings of how AI would classify the original stop-sign image ($M_s = 3.96$ and 4.50 , respectively), $r_s(203) = .17$, $p = .012$. Participants who had higher self-reported general understandings of AI rated higher that the AI could correctly identify the original image of a stop sign. Trust in AI was positively correlated with participants' ratings of how AI would classify the original stop-sign image ($M_s = 4.30$ and 4.50 , respectively), $r_s(203) = .30$, $p < .001$, and trust in AI in ADS was positively correlated with their ratings of how AI would classify the malicious stop-sign image ($M_s = 4.03$ and 4.15 , respectively), $r_s(203) = .27$, $p < .001$. Participants who had greater trust in AI and AI in ADS rated higher that the AI could correctly identify the original and malicious image of the stop sign, respectively. No other correlations were significant, $p > .05$.

Artificial Intelligence Knowledge, Exposure, and Understanding

Spearman's rank correlational analyses with a Benjamini–Hochberg alpha correction were conducted among knowledge of AI, exposure to AI, understanding of AI, knowledge of AI in

ADS, and understanding of AI in ADS. See Table 2 for the correlation coefficients. The results showed that general AI knowledge was positively correlated to exposure to AI ($M_s = 4.83$ and 4.82 , respectively), $r_s(203) = .28$, $p < .001$, and knowledge of AI in ADS ($M_s = 4.83$ and 4.35 , respectively), $r_s(203) = .45$, $p < .001$. Participants who had a greater general knowledge of AI tended to have more exposure to AI and greater knowledge of AI in ADS. Exposure to AI was positively correlated to self-reported understandings of AI ($M_s = 4.82$ and 3.96 , respectively), $r_s(203) = .34$, $p < .001$, self-reported understandings of AI in ADS ($M_s = 4.82$ and 3.87 , respectively), $r_s(203) = .33$, $p < .001$, and to knowledge of AI in ADS ($M_s = 4.82$ and 4.35 , respectively), $r_s(203) = .25$, $p < .001$. Participants who had more exposure to AI tended to have higher self-reported general understandings of AI, self-reported understandings of AI in ADS, and tended to have greater knowledge of AI in ADS. Self-reported general understanding of AI was positively correlated to self-reported understandings of AI in ADS ($M_s = 3.96$ and 3.87 , respectively), $r_s(203) = .69$, $p < .001$. Participants who had higher self-reported general understandings of AI tended to have higher self-reported understandings of AI in ADS. No other correlations were significant, $p > .05$.

Knowledge, Understanding, and Trust

Spearman's rank correlation analyses with a Benjamini–Hochberg alpha correction were also conducted among knowledge of AI, trust in AI in general, self-reported general understandings of AI, knowledge of AI in ADS, trust in AI in ADS, and self-reported understandings of AI in ADS. See Table 3 for the correlation coefficients. Trust in AI was positively correlated to general AI knowledge ($M_s = 4.30$ and 4.83 , respectively), $r_s(203) = .18$, $p = .011$, and self-reported general understanding of AI ($M_s = 4.30$ and 3.96 , respectively), $r_s(203) = .39$, $p < .001$. Participants who had higher levels of trust in AI in general tended to have greater general knowledge of AI and higher self-reported general understandings of AI. Trust of AI in ADS was also positively correlated to knowledge of

Table 2. Spearman's Rank Correlations of AI Related Questions.

Variable	M	SD	1	2	3	4	5
1. Exposure to AI	4.82	1.31	-	-	-	-	-
2. Understanding of AI	3.96	1.68	.34***	-	-	-	-
3. Understanding of AI in ADS	3.87	1.63	.33***	.69***	-	-	-
4. Knowledge of AI	4.83	0.71	.28***	-.12	-.15	-	-
5. Knowledge of AI in ADS	4.35	0.44	.25***	.14	.06	.45***	-

Note. *** = $p < .001$.

Table 3. Spearman's Rank Correlation of Knowledge and Trust in General and Correlation of Knowledge of Artificial Intelligence in Automated Driving Systems and Trust in Artificial Intelligence in Automated Driving Systems.

Variable	M	SD	Trust in AI	Trust in AI in ADS
Understanding of AI	3.96	1.68	.39***	.36***
Understanding of AI in ADS	3.87	1.63	.39***	.41***
Knowledge of AI	4.83	0.71	.18*	.14
Knowledge of AI in ADS	4.35	0.44	.28***	.19**

Note. *** = $p < .001$, ** = $p < .01$, * = $p < .05$.

AI in ADS ($M_s = 4.03$ and 4.35 , respectively), $r_s(203) = .19$, $p = .006$, and self-reported understandings of AI in ADS ($M_s = 4.03$ and 3.87 , respectively), $r_s(203) = .41$, $p < .001$. Participants who had higher levels of trust in AI in ADS tended to have greater knowledge of AI in ADS and higher self-reported understandings of AI in ADS. The correlation between self-confidence in one's driving ability and trust in AI in ADS was not significant ($M_s = 5.36$ and 4.03 , respectively), $r_s(203) = -.13$, $p = .074$.

DISCUSSION

The present study investigated drivers' perception of the capabilities of AI in ADS by using the case of a maliciously manipulated stop sign. AI is critical to the proper functioning of ADS and provides executive oversight of the ADS at work. AI perceives the roadway environment and makes real-time decisions to guide the ADS on the road. Without AI, the ADS would no longer be able to regulate its interactions with the road or other road users. In this study, we found accurate perception of stop signs by participants for both the standard and malicious conditions. This result was expected because both images were recognizable by human eyes

as a stop sign even though the malicious sign was altered. For the question regarding the participant's perception of whether an AI in ADS would recognize the original stop sign, participants gave lower ratings than those reflected by their own ability, which indicates that people are likely to estimate an AI's abilities in this aspect less than those of their own. This result is similar to prior research that shows people are often likely to rely more on their abilities than that of a ADS or have higher self-confidence than confidence in automation (Hoff & Bashir, 2015; Kyriakidis et al., 2015; Röttger et al., 2009; Tenhundfeld et al., 2020).

Participants rated the AI's ability to detect the malicious stop-sign image as a stop sign lower than the original stop sign. However, the mean rating for the former was still high, 4.15 out of 5, and a large portion of the participants was fairly certain that the malicious image was identifiable by AI. The malicious stop-sign image was crafted so that the current AI computer vision system trained on stop signs would have a 0% probability of correctly categorizing this image as a stop sign (Eykholt et al., 2017). Therefore, our participants indeed had a much higher-than-expected belief that an AI would be able to identify the

malicious stop sign. The high ratings by the participants could be due to them having high predictions of the AI performance, a phenomenon called the perfect automation schema (PAS). PAS is a cognitive schema focusing on the high performance of automation (Tschopp, 2020). People with PAS have high performance expectations of the automation, which may lead to automation bias, or over-trusting of the automation (Lyons & Guznov, 2019; Parasuraman & Riley, 1997). Although a simple and straightforward result, it is quite informative because it demonstrates a potentially severe mismatch between an AI's capabilities and the beliefs that a user might have about that system.

Reflecting recent advances in technology, the knowledge ratings of AI showed participants self-reported to be, on average, quite knowledgeable about AI. They had a high amount of exposure to AI. However, participants' general understandings of AI, such as the concepts and technology that allows AI to work, were only slightly higher than the neutral rating. Since these measures were not manipulated in the study, correlations were used to assess the results. These three ratings were correlated, likely because the more time spent with a system, the greater understanding of what processes are involved in the system and knowledge of uses of AI. For example, the more a user uses a voice assistant such as Siri, the more they learn about it and its capabilities as well as the general tasks the AI can accomplish. They will see that the AI selects specific processes to use, such as the calculator for a math question or scouring the internet for a pop culture question, like a movie's name. Likewise, participants who had higher general understandings of AI correctly believe that the AI could detect the original stop-sign image as a stop sign. However, understandings of AI in AV were not strongly correlated with the ratings of the AI's ability to detect a malicious stop-sign image as a stop sign. These results indicate that the mere understanding of the general concepts and technology used by AI may not be sufficient for users to understand a specific function of AI, especially in the context of cyber-attacks.

Additionally, there was a positive correlation between the AI's ability to correctly identify the original stop-sign image and trust in AI, as well as between identifying the malicious stop sign and trust in AI in ADS. Those who trusted AI and AI in ADS more tended to believe the AI was more capable at identifying the signs. It is typical that systems of higher capability will lead to higher perceived capability and higher trust in the system (Sanchez et al., 2004). However, if the user does not have sufficient knowledge about how the system works, then their trust level will not match the system's actual capability (i.e., trust miscalibration; Lee & See, 2004).

In terms of knowledge and understanding of the more specific types of AI (i.e., those specifically used in ADS), participants had lower scores than the general knowledge and understanding AI questions. A possible reason for this result is that the participants had less direct experience with ADS because few were on the market. Another possibility is that the public lacks an understanding of how AI works to accomplish specific functions. For example, many people may know that AI is required for facial recognition but may not understand what particular features might make the AI struggle to function. Likewise, people may assume that high-resolution images are best for AI to identify. However, there is a tradeoff at specific resolutions between accuracy and the number of images that can be scanned at a time (i.e., speed; Sabottke & Spieler, 2020).

Our study focused on participants' knowledge and self-reported understandings related to things using AI rather than precisely how AI works. Participants accurately knew the types of technology that require AI, but might not understand how it works, which can be seen by the lower self-reported understanding ratings than the actual knowledge ratings. Clearly, participants over-trusted the AI's capabilities for identifying the malicious image because they may not understand how manipulating images can fool computer vision. Explainable AI, which describes the general AI model enough for the user to comprehend and trust the results, benefits trust in and usage of the AI system (Shin, 2021). Understanding the user's general and

specific knowledge and understanding of the given system, is a critical aspect for design. Moreover, how the AI characteristics should be conveyed to users is essential to increase the necessary knowledge of the user. The implications of this study may guide the explanation of AI for users to better calibrate their understanding of and trust in AI. Since users tend to over-trust and believe AI is more capable than it actually is, its restricted capabilities should be properly explained to the users. In addition, users should also be made aware of external factors, such as environment or hackers, that may hinder the AI's optimal operation.

Limitations and Future Research

There are some limitations in the current study. First, we only used one set of original and malicious stop signs for the participants to rate. This setting prevents us from discussing further implications of user's ratings of an AI's ability to detect the different road signs. Based on the current study, future studies can test various types of road signs and further systematically investigate the public's perception of AI's role in various ADS processes. Second, the present study used self-reported questionnaires, and humans cannot always judge themselves accurately through questionnaires. Based on the overconfidence bias (Moore & Healy, 2008), people tend to overestimate their own abilities and thus judge others to be less capable than themselves. It is likely that participants rated the AI in the way that they would rate other people, leading to a lower rating for AI than for themselves. Additionally, due to the timing of the implementation of this study during COVID 19, a questionnaire was the best method to collect the necessary data for our analyses. However, this limitation may account for the weak correlations we found, albeit significant. Lastly, the present study only tested one type of malicious attack (i.e., the physical attack) on the AI. The current AI technology has a 0% accuracy classifying the attacked image. This single attack type prevents us from discussing the implication of the AI's accurate classification rates at various levels, given that we only

included the images with 100% (the original image) and 0% (the attacked image) AI classification accuracy levels. In addition to the accuracy of AI classification, there are various types of attacks that can have different levels of visibility to human eyes (Qiu et al., 2019), which may affect how the human perceives an AI's judgment related to the attacks. Future research can examine how varying AI accurate classification rates for images and human's perception of the AI's capabilities differs under different malicious attacks and further guide the design of safe and secure ADS.

CONCLUSIONS

This study shows that humans can identify stop signs both before and after a malicious manipulation and how they perceive and trust an AI's ability to complete the same task. This study also demonstrates the close relationships among humans' knowledge, exposure, understanding, and trust related to AI. Participants could make accurate judgments of the road sign themselves and rated the AI as less able to identify the malicious sign than the original. However, participants highly overestimated the AI's ability to recognize the malicious stop sign. Our findings indicate that the public may not accurately understand specific AI systems, leading them to over-trust the AI in certain conditions.

ACKNOWLEDGMENTS

The authors thank Erin Fuller-Jakaitis for her assistance in preparing an earlier version of the study materials.

DECLARATION OF CONFLICTING INTERESTS

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

FUNDING

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the National Science Foundation award #2007386.

AUTHOR'S NOTE

Part of the reported data were presented at the 2021 Annual Meeting of Human Factors and Ergonomics Society and included as an extended abstract in the conference program.

ORCID iD

Jing Chen  <https://orcid.org/0000-0003-0394-0375>

REFERENCES

- Asan, O., Bayrak, A. E., & Choudhury, A. (2020). Artificial intelligence and human trust in healthcare: Focus on clinicians. *Journal of Medical Internet Research*, 22(6), Article e15154. <https://doi.org/10.2196/15154>
- Bansal, G., Nushi, B., Kamar, E., Lasecki, W. S., Weld, D. S., & Horvitz, E. (2019). Beyond accuracy: The role of mental models in human-AI team performance. *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing*, 7(1), 2–11. <https://ojs.aaai.org/index.php/HCOMP/article/view/5285>
- Cunneen, M., Mullins, M., & Murphy, F. (2019). Autonomous vehicles and embedded artificial intelligence: The challenges of framing machine driving decisions. *Applied Artificial Intelligence*, 33(8), 706–731. <https://doi.org/10.1080/08839514.2019.1600301>
- Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., Prakash, A., Kohno, T., & Song, D. (2017). Robust physical-world attacks on deep learning models. <https://doi.org/10.48550/arXiv.1707.08945>
- Ferrario, A., Loi, M., & Viganò, E. (2021). Trust does not need to be human: It is possible to trust medical AI. *Journal of Medical Ethics*, 47(6), 437–438. <https://doi.org/10.1136/medethics-2020-106922>
- Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. <https://doi.org/10.48550/arXiv.1412.6572>
- Grace, K., Salvatier, J., Dafoe, A., Zhang, B., & Evans, O. (2018). When will AI exceed human performance? Evidence from AI experts. *Journal of Artificial Intelligence Research*, 62, 729–754. <https://doi.org/10.1613/jair.1.11222>
- Halim, Z., Kalsoom, R., Bashir, S., & Abbas, G. (2016). Artificial intelligence techniques for driving safety and vehicle crash prediction. *Artificial Intelligence Review*, 46(3), 351–387. <https://doi.org/10.1007/s10462-016-9467-9>
- Hengstler, M., Enkel, E., & Duelli, S. (2016). Applied artificial intelligence and trust-The case of autonomous vehicles and medical assistance devices. *Technological Forecasting and Social Change*, 105, 105–120. <https://doi.org/10.1016/j.techfore.2015.12.014>
- Hoff, K. A., & Bashir, M. (2015). Trust in automation: Integrating empirical evidence on factors that influence trust. *Human Factors*, 57(3), 407–434. <https://doi.org/10.1177/0018720814547570>
- Holzinger, A., Searle, G., & Wembacher, M. (2011). The effect of previous exposure to technology on acceptance and its importance in usability and accessibility engineering. *Universal Access in the Information Society*, 10(3), 245–260. <https://doi.org/10.1007/s10209-010-0212-x>
- Jacovi, A., Marasović, A., Miller, T., & Goldberg, Y. (2021). Formalizing trust in artificial intelligence: Prerequisites, causes and goals of human trust in AI. *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 624–635. <https://doi.org/10.1145/3442188.3445923>
- Jarrah, M. H. (2018). Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. *Business Horizons*, 61(4), 577–586. <https://doi.org/10.1016/j.bushor.2018.03.007>
- Jian, J.-Y., Bisantz, A. M., & Drury, C. G. (2000). Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics*, 4(1), 53–71. https://doi.org/10.1207/S15327566IJCE0401_04
- Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, 62(1), 15–25. <https://doi.org/10.1016/j.bushor.2018.08.004>
- Kendall, A., & Gal, Y. (2017). What uncertainties do we need in bayesian deep learning for computer vision? *Proceedings of Advances in Neural Information Processing Systems*. arXiv preprint arXiv:1703.04977.
- Kyriakidis, M., Happee, R., & De Winter, J. C. F. (2015). Public opinion on automated driving: Results of an international questionnaire among 5000 respondents. *Transportation Research Part F: Traffic Psychology and Behaviour*, 32, 127–140. <https://doi.org/10.1016/j.trf.2015.04.014>
- Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors*, 46(1), 50–80. <https://doi.org/10.1518/hfes.46.1.50.30392>
- Liu, H., Wang, Y., Fan, W., Liu, X., Li, Y., Jain, S., Liu, Y., Jain, A. K., & Tang, J. (2021). Trustworthy AI: A computational perspective. <https://doi.org/10.48550/arXiv.2107.06641>
- Lyons, J. B., & Guznov, S. Y. (2019). Individual differences in human-machine trust: A multi-study look at the perfect automation schema. *Theoretical Issues in Ergonomics Science*, 20(4), 440–458. <https://doi.org/10.1080/1463922X.2018.1491071>
- Ma, Y., Wang, Z., Yang, H., & Yang, L. (2020). Artificial intelligence applications in the development of autonomous vehicles: A survey. *IEEE/CAA Journal of Automatica Sinica*, 7(2), 315–329. <https://doi.org/10.1109/JAS.2020.1003021>
- Moore, D. A., & Healy, P. J. (2008). The trouble with overconfidence. *Psychological Review*, 115(2), 502–517. <https://doi.org/10.1037/0033-295X.115.2.502>
- Oh, C., Lee, T., Kim, Y., Park, S. H., Kwon, S., & Suh, B. (2017). Us vs. them: Understanding artificial intelligence technophobia over the Google DeepMind Challenge match. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2523–2534. <https://doi.org/10.1145/3025453.3025539>
- Oh, C., Song, J., Choi, J., Kim, S., Lee, S., & Suh, B. (2018). I lead, you help but only with enough details: Understanding the user experience of co-creation with artificial intelligence. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–13. <https://doi.org/10.1145/3173574.3174223>
- Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. *Human Factors*, 39(2), 230–253. <https://doi.org/10.1518/001872097778543886>
- Prahl, A., & Goh, W. W. P. (2021). “Rogue machines” and crisis communication: When AI fails, how do companies publicly respond? *Public Relations Review*, 47(4), 102077. <https://doi.org/10.1016/j.pubrev.2021.102077>
- Qiu, S., Liu, Q., Zhou, S., & Wu, C. (2019). Review of artificial intelligence adversarial attack and defense technologies. *Applied Sciences*, 9(5), 909. <https://doi.org/10.3390/app9059099>
- Reig, S., Norman, S., Morales, C. G., Das, S., Steinfeld, A., & Forlizzi, J. (2018). A field study of pedestrians and autonomous vehicles. *Proceedings of the 10th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, 198–209. <https://doi.org/10.1145/3239060.3239064>
- Rossi, F. (2018). Building trust in artificial intelligence. *Journal of International Affairs*, 72(1), 127–134. <https://www.jstor.org/stable/26588348>
- Röttger, S., Bali, K., & Manzey, D. (2009). Impact of automated decision aids on performance, operator behaviour and workload in a simulated supervisory control task. *Ergonomics*, 52(5), 512–523. <https://doi.org/10.1080/00140130802379129>
- Russell, S., Moskowitz, I. S., & Raglin, A. (2017). Human information interaction, artificial intelligence, and errors. In W. F. Lawless, R. Mittu, D. Sofge, et al. (Eds.), *Autonomy and artificial intelligence: A threat or savior?* (pp. 71–101). Springer. https://doi.org/10.1007/978-3-319-59719-5_4

- Sabottke, C. F., & Spieler, B. M. (2020). The effect of image resolution on deep learning in radiography. *Radiology: Artificial Intelligence*, 2(1), Article e190015. <https://doi.org/10.1148/ryai.2019190015>
- SAE International. (2021). Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles (Publication No. J3016_202104). https://doi.org/10.4271/J3016_202104
- Sanchez, J., Fisk, A. D., & Rogers, W. A. (2004). Reliability and age-related effects on trust and reliance of a decision support aid. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 48(3), 586–589. <https://doi.org/10.1177/154193120404800366>
- Shin, D. (2021). The effects of explainability and causability on perception, trust, and acceptance: Implications for explainable AI. *International Journal of Human-Computer Studies*, 146, 102551. <https://doi.org/10.1016/j.ijhcs.2020.102551>
- Siau, K., & Wang, W. (2018). Building trust in artificial intelligence, machine learning, and robotics. *Cutter Business Technology Journal*, 31(2), 47–53. <https://www.cutter.com/article/building-trust-artificial-intelligence-machine-learning-and-robotics-498981>
- Tenhundfeld, N. L., de Visser, E. J., Ries, A. J., Finomore, V. S., & Tossell, C. C. (2020). Trust and distrust of automated parking in a Tesla Model X. *Human Factors*, 62(2), 194–210. <https://doi.org/10.1177/0018720819865412>
- Tschopp, M. (2020, May 7). *PAS - The perfect automation schema*. Influencing Trust. <https://www.scip.ch/en/?labs.20200507>
- Wiegmann, D. A., Rich, A., & Zhang, H. (2001). Automated diagnostic aids: The effects of aid reliability on users' trust and reliance. *Theoretical Issues in Ergonomics Science*, 2(4), 352–367. <https://doi.org/10.1080/14639220110110306>
- Yu, T., Hu, S., Guo, C., Chao, W.-L., & Weinberger, K. Q. (2019). A new defense against adversarial images: Turning a weakness into a strength. *Proceedings of the 33rd Conference on Neural Information Processing Systems*, 4(5), 1635–1646. <https://doi.org/10.48550/arXiv.1910.07629>
- Zhang, X., Gao, H., Guo, M., Li, G., Liu, Y., & Li, D. (2016). A study on key technologies of unmanned driving. *CAAI Transactions on Intelligence Technology*, 1(1), 4–13. <https://doi.org/10.1016/j.trit.2016.03.003>

APPENDIX

Questions Used in The Study

(Questions 20 and 32 are attention checks).

Section 1: Knowledge

This section asks about your understanding of artificial intelligence (AI).

- AI is required for *Deep Blue, a chess-playing computer developed by IBM*.
- AI is required for *conversation with Chatbots*.
- AI is required for *personalized feeds on social media*.
- AI is required for *digital voice assistants such as Alexa and Siri*.
- AI is required for *product recommendations for online shopping*.
- AI is required for *vending machines that sell drinks and snacks*.
- AI is required for *inputting a passcode to unlock a cellphone*.
- AI is required for *broadcasting cable TV shows*.
- AI is required for *personal reminders from a calendar*.
- AI is required for *electronic toothbrushes*.

Section 2: Exposure

This section asks about your previous exposure to artificial intelligence (AI).

- I am aware that AI is used in other applications like speech-/text-recognition, spam-filters, and recommendation algorithms.
- I have seen AI discussed in the media (TV/print/online).
- I have seen AI discussed in social media.
- I have seen AI discussed in school lectures or class material.
- I have seen AI discussed by friends or family.

Section 3: Artificial Intelligence in Automated Driving Systems

This section asks about your general understanding of artificial intelligence (AI) in the context of automated driving.

- Autonomous driving requires the use of AI.
- I am aware of how autonomous driving systems use AI.
- I have a basic understanding of the concepts and technology that allow AI to work.
- I have a basic understanding of the concepts and technology that allow automated driving to work.
- For this question, you are required to choose the *strongly disagree* option below.

Section 4: Applications

This section asks about your understanding of the applications of artificial intelligence (AI) in autonomous driving.

- For autonomous driving, AI is required for the detection of *road signs*.
- For autonomous driving, AI is required for the detection of *pedestrians*.
- For autonomous driving, AI is required for the detection of *other objects on the road*.
- For autonomous driving, AI is required for *lane-keeping*.
- For autonomous driving, AI is required for *auto-braking*.

26. For autonomous driving, AI is required for *cruise control*.

Section 5: Future

This section asks about your understanding of artificial intelligence (AI) in autonomous driving.

27. AI will revolutionize driving in a good way.
 28. AI will improve driving safety.
 29. Driver training will eventually need to involve discussion of AI.
 30. I am comfortable with the rising use of AI in driving.
 31. Human drivers will eventually be replaced with AI.
 32. For this question, you are required to choose the *strongly disagree* option below.

Section 6: Human versus Artificial Intelligence

This section asks about your opinions of artificial intelligence (AI).

33. I can trust AI in general.
 34. I am wary of the use of AI in general.
 35. The use of AI in general is dependable.
 36. The use of AI in general is reliable.
 37. I am confident in the use of AI in general.
 38. I am familiar with AI in general.
 39. If I knew more about how AI works in general, I would trust it more.
 40. I can trust AI in autonomous driving.
 41. I am wary of the use of AI in autonomous driving.
 42. The use of AI in autonomous driving is dependable.
 43. The use of AI in autonomous driving is reliable.
 44. I am confident in the use of AI in autonomous driving.
 45. I am familiar with the use of AI in autonomous driving.
 46. If I knew more about how AI works in autonomous driving, I would trust it more in autonomous driving.
 47. I drive more safely than AI.
 48. I am confident that I can make correct decisions for driving.
 49. I am confident in my driving ability.

Section 7: Stop Sign Questions

Please rate how much you agree or disagree with the following statement: (Strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree)

36. I think this image shows a stop sign. (Original Stop)
 48. I think this image shows a stop sign. (Malicious Stop)
 50. I think the current **AI technology** will classify this as an image of a stop sign. (Original Stop)
 52. I think the current **AI technology** will classify this as an image of a stop sign. (Malicious Stop)

Section 8: Demographics (age, gender, tech savvy vs. not tech savvy)

Questions 51, 52, 53, 54 responses are number entries.

Question 55 responses are: Male, Female, Other

50. I consider myself a tech-savvy person.
 51. How many years of driving experience do you have?
 52. At what age did you first receive your driver's license?
 53. About how many miles have you driven in the past 12 months?
 54. What is your age in years?
 55. What is your gender? (Female, Male, other)
 56. Race (White, Black or African American, American Indian or Alaska Native, Asian, Native Hawaiian or Pacific Islander, Other)
 57. What is the highest level of school you have completed or the highest degree you have received? (Less than high school degree, High school graduate (high school diploma or equivalent including GED), Some college but no degree, Associate degree in college (2-year), Bachelor's degree in college (4-year), Master's degree, Doctoral degree, Professional degree (JD, MD)).
 58. Do you have any comments regarding this survey?

Katherine R. Garcia is a doctoral student in Human Factors Psychology at Old Dominion University. She

received her bachelor's degree in Psychology at Rice University in 2020.

Scott Mishler is a doctoral student in Human Factors Psychology at Old Dominion University. He received his master's degree in Psychology at Old Dominion University in 2019.

Yanru Xiao is a doctoral student in Computer Science at Old Dominion University. He received his bachelor's degree in Computer Science and Technology at Central South University in 2017.

Cong Wang is an Assistant Professor of Cybersecurity Engineering at George Mason University. He received his Ph.D in Electrical and Computer Engineering at Stony Brook University in 2016.

Bin Hu is an Assistant Professor of Engineering Technology at Old Dominion University. He received his Ph.D. in Electrical Engineering at the University of Notre Dame in 2016.

Jeremiah D. Still is an Associate Professor of Human Factors Psychology at Old Dominion University. He received his Ph.D. in Human Computer Interaction at Iowa State University in 2009. ORCID ID: <https://orcid.org/0000-0002-3060-4417>

Jing Chen is an Assistant Professor of Human Factors Psychology at Old Dominion University. She received her Ph.D. in Cognitive Psychology and M.S. in Industrial Engineering at Purdue University in 2015. ORCID ID: <https://orcid.org/0000-0003-0394-0375>