Prospectus

Implementing the Kalman Filter Algorithm Using a Convolutional Neural Network
(Technical Topic)

Privacy Issues with Unwarranted Data Collection from Web and Mobile Applications
(STS Topic)

By

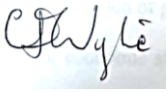
Akanksha Alok

March 30, 2019

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed:_____ Akanksha Alok ____ Date_____03/30/2019_____
Akanksha Alok

Approved: _____ Yuan Tian _____ Date_____03/30/2019_____
Yuan Tian, Assistant Professor of Computer Science

Approved: _____  _____ Date___03/30/2019_____
Caitlin Wylie, Assistant Professor of STS, Department of Engineering and Society

Introduction

My technical and STS thesis topics both involve the misuse or tampering of information collected from gadgets, such as sensors, cameras or other technological applications. As our society has the potential to progress towards "smart cities" with built-in sensors and technological components integrated in all aspects of our daily lives, there are high risks of these systems being hacked and the collected data to be compromised. Researchers have already developed algorithms and detailed networks that will be able to keep track of all vehicles based on traffic cameras and sensors on the roads (Khan, Sargento, & Luis, 2017), and the hacking of this system can potentially put every vehicle-owner at risk. Despite this fact, there is no mention of how their vehicle data will be secured or safeguarded, and this is a clear indication that as a society, we are moving towards extensive data collection without the proper safety measures in place. My technical thesis addresses the aforementioned problem of technical systems being hacked, and my project involves developing a solution that mitigates the effects of a hacked sensor or camera system employed on an autonomous car. It allows for the vehicle to continue on its normal trajectory without putting any lives in danger. My STS theses, on the other hand, deals with unauthorized data collection of human subjects. I will be exploring the ways in which a user's social media accounts, and web and mobile applications wrongfully elicit their personal information without their knowledge, and possible steps that we can take as a society to prevent this from happening. This breach of privacy affects almost every person on this planet, regardless of race, age, locality, or economic status, and can range from a person's name and email being stored in an external database to their entire identity being stolen (Irshad & Soomro, 2018). Extensive data collection and analysis will continue

to be a big part of our lives as we progress into the future, and it is time that we take the necessary precautions to ensure that the data is being collected and used rightfully.

Technical Topic

GPS Spoofing and the hacking of sensors and cameras has become a prevalent problem in our society, as expressed in detail by Humphreys (2016). He describes the large-scale operations that have been accomplished through GPS spoofing, such as the event in which Iran misguided several US ships and aircrafts into unknown territory, as well as his own attempt of successfully misguiding the White Rose cruise liner one kilometer astray without the crew noticing. In the case of autonomous vehicles, several researchers have already perfected an algorithm to trick current GPS navigation systems used in cars, deflecting vehicles thousands of meters from their intended destinations without the knowledge of the drivers (Zeng, Shu, Liu, Dou, & Yang, 2017). Any mishap with the gadgets used in an autonomous vehicle has the potential to put many lives in danger, whether it is the passengers in the autonomous car, passengers in the other cars on the road, or even pedestrians. I will try to tackle this problem in my technical project, so that even when a sensor, camera or navigation system of the car is hacked, the car will be able to tune out the exterior noise and continue functioning normally. In order to accomplish this, I will be implementing the Kalman Filtering algorithm. By training a neural network on input data from various cameras, sensors, and the GPS navigation system of the autonomous vehicle, it constructs a probabilistic model that is able to predict the next state of the vehicle based on the current state. When there is any external noise or extraneous data coming in from any of the hacked sensors, the algorithm will be able to tune out this noise and be able to continue on the rightful path. Researchers in the past have implemented this algorithm using a recursive

technique, and most of the research in this area has focused on finding a precise mathematical formula for the Kalman Filtering algorithm. For example, in the research paper by Li et. al (2015), they modify the coefficients of the formula using M-estimation in statistics and use a fading factor to procure a formula that yielded the most accurate results. However, in my research, I will be implementing the algorithm in a novel way, by using it in correspondence with a Convolutional Neural Network.

My research mentor, Dr. Yuan Tian, and I are working on this project in partnership with a Virginia Tech professor, whose team is trying to defeat our algorithm with their GPS hacking skills. The ultimate goal of this research project would be to train the Convolutional Neural Network in a way that is able to bypass their hacking techniques of the input sensors or systems of the autonomous car, and to ensure that the car maintains it correct path.

STS Topic

The STS topic that I want to explore is the invasion of privacy due to data collection performed through our social media accounts, web applications on the Internet and mobile applications on our phones. In this day and age, we extensively use applications or software that tracks our personal data on a daily basis - sometimes without our knowledge or permission. Users are often unaware of the potential consequences when they turn on their location settings while using navigation apps or social media accounts like Snapchat, making them vulnerable to personalized attacks at any given time (Fisher, Dorner, & Wagner, 2012). In fact, the user study done by Irshad and Soomro (2018) emphasized the fact that social media users do not realize that they are making themselves easy targets to crimes such as identity theft, when they irresponsibly and haphazardly share their information online. Similarly, Bilton (2010) published an article

about burglars using information from Facebook statuses that their neighbors had posted, in order to coordinate their crimes with their vacation times. While these incidents emphasize the lack of awareness and responsibility of the active users, a person who is not active online or on social media can have their information released through their friends' or family's accounts. For example, they can be tagged in a picture that a friend posted on Facebook or their information can be released to third parties when a friend's contact list is hacked. Several companies even use this public data from these applications for their own purposes and researchers can access this data easily for scientific study. The rise of data collection is inevitable in a society where technology is becoming increasingly integrated in our daily lives, and we need to ensure that our privacy is being upheld and that our information is not being collected wrongfully or without permission.

I plan on researching how certain data-collecting apps operate, and how the companies design them in a way to be hidden by looking into the previous research done in these areas. I want to look into the existing rules and regulations provided by governing bodies of the United States on how data from these applications can be used and distributed. In order to further understand the relationship between these governing bodies, companies, and the users, I plan to use Actor-Network Theory. In fact, the study done by Acar et. al (2016) assigned each developer involved in the mobile application development cycle a specific role in implementing the security measure for ensuring user data safety, which already clearly defined several actors within the Actor Network. Through the Social Construct of Technology, I wish to explore how different groups of people are affected by the misuse of their personal data. For example, there are situations where people with secret clearances have had their identities stolen through the use of a seemingly harmless app, and others have unintentionally shared their information towards

studies or causes that they do not necessarily agree with. After thoroughly understanding the problem, I want to suggest ways in which we can solve this problem from a technical, legal, and social standpoint. There are already publications detailing the development of software that is attempting to stop applications from stealing information from the users, such as the TISSA software that counteracts malicious Android apps (Acar, et al., 2016), and there are safer alternatives to location-sharing, such as position-aware services, that can be used by mobile applications (Barkhuus & Dey, 2003). I will also try to suggest improvements to the laws in place for privacy in the technological realm, and will try to encourage the passing of legislation such as the General Data Protection Regulation made by the European Council. Most of all, I want to find a solution that raises awareness among users of the potential dangers of sharing too much information online or on other applications. As I am trying to find solutions to problems that will become more prevalent in our society as time passes and technology becomes more integrated in our lives, I will need to employ technological futurism to analyze if these techniques will be able to persist in the future and if these problems can change over time.

Conclusion

At the end of the Capstone project, I am hoping to create a fully-functional neural network that implements the Kalman Filter algorithm successfully. In the final testing stages, when the input data from the sensors and cameras is altered, the neural network should still be able to predict the next correct coordinates of the vehicle. Ultimately, the GPS spoofing attempts by the Virginia Tech team will not be able to misguide the neural network that is controlling the autonomous car system. While I am extensively using input data from various sensors on the car when working on my technical research and I realize the importance of having this data, I also want to make

sure that this data has been collected in a rightful manner, especially if it deals with human data. I want to have a better understanding of the laws and precautions that need to be taken in regards to data collection process of web and mobile applications. I want to discover the techniques that companies employ to steal a person's information, and want to encourage us, as a society, to take measures against this in order to maintain our own privacy. With my work on both the technical and STS thesis topic, I hope to find a way to maintain the integrity of the data that is being collected, especially as we move towards a future with a plethora of cameras, sensors, and technological applications that are going to be embedded in our daily lives.

References

Acar, Y., Backes, M., Bugiel, S., Fahl, S., McDaniel, P., & Smith, M. (2016). Sok: lessons learned from android security research for appified software platforms. 2016 IEEE Symposium on Security and Privacy (SP), 433–451. https://doi.org/10.1109/SP.2016.33

Barkhuus, L., & Dey, A. (2003, January). Location-based services for mobile telephony: a study of users' privacy concerns. Presented at the Human-Computer Interaction INTERACT '03: IFIP TC13 International Conference on Human-Computer Interaction, Zurich, Switzerland.

Bilton, N. (2010, September 12). Burglars said to have picked houses based on facebook updates. Retrieved March 30, 2019, from Bits Blog website: https://bits.blogs.nytimes.com/2010/09/12/burglars-picked-houses-based-on-facebook-updates/

Fisher, D., Dorner, L., & Wagner, D. (2012). Short paper: location privacy: user behavior in the field. Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM '12, 51. https://doi.org/10.1145/2381934.2381945

Humphreys, M. L. P. and T. E. (2016, July 29). Protecting gps from spoofers is critical to the future of navigation. Retrieved March 30, 2019, from IEEE Spectrum: Technology, Engineering, and Science News website: https://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation

Irshad, S., & Soomro, T. (2018). Identity Theft and Social Media. International Journal of Computer Science and Network Security, 18, 43–55.

Khan, M. A., Sargento, S., & Luis, M. (2017). Data collection from smart-city sensors through large-scale urban vehicular networks. 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), 1–6. https://doi.org/10.1109/VTCFall.2017.8288308

Li, K., Hu, B., Chang, L., & Li, Y. (2015). Robust square-root cubature Kalman filter based on Huber's M-estimation methodology. Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering, 229(7), 1236–1245. https://doi.org/10.1177/0954410014548698

Olson, P. (n.d.). Hacking a phone's gps may have just got easier. Retrieved March 30, 2019, from Forbes website: https://www.forbes.com/sites/parmyolson/2015/08/07/gps-spoofing-hackers-defcon/

Zeng, K. C., Shu, Y., Liu, S., Dou, Y., & Yang, Y. (2017). A practical gps location spoofing attack in road navigation scenario. Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications - HotMobile '17, 85–90. https://doi.org/10.1145/3032970.3032983