Machine Learning for Intrusion Detection in Modern Vehicles

By *Sanket Mehrotra*

Table of Contents

* [1  Introduction](https://colab.research.google.com/drive/1fb4oR7wuIJ1kaHShBGZnbxKuEyDOmdQ3#Introduction)
* [2  Why do we need it?](https://colab.research.google.com/drive/1fb4oR7wuIJ1kaHShBGZnbxKuEyDOmdQ3#Why-do-we-need-it?)
  + [2.1  The in-car network : the CAN](https://colab.research.google.com/drive/1fb4oR7wuIJ1kaHShBGZnbxKuEyDOmdQ3#The-in-car-network-:-the-CAN)
  + [2.2  CAN attacks](https://colab.research.google.com/drive/1fb4oR7wuIJ1kaHShBGZnbxKuEyDOmdQ3#CAN-attacks)
* [3  How do we do it? : different approaches](https://colab.research.google.com/drive/1fb4oR7wuIJ1kaHShBGZnbxKuEyDOmdQ3#How-do-we-do-it?-:-different-approaches)
  + [3.1  Metric Based](https://colab.research.google.com/drive/1fb4oR7wuIJ1kaHShBGZnbxKuEyDOmdQ3#Metric-Based)
  + [3.2  Machine Learning Based](https://colab.research.google.com/drive/1fb4oR7wuIJ1kaHShBGZnbxKuEyDOmdQ3#Machine-Learning-Based)
  + [3.3  DNN Based](https://colab.research.google.com/drive/1fb4oR7wuIJ1kaHShBGZnbxKuEyDOmdQ3#DNN-Based)
* [4  Reference Papers/ Bibliography](https://colab.research.google.com/drive/1fb4oR7wuIJ1kaHShBGZnbxKuEyDOmdQ3#Reference-Papers/-Bibliography)
* [5  Analysis of Papers](https://colab.research.google.com/drive/1fb4oR7wuIJ1kaHShBGZnbxKuEyDOmdQ3#Analysis-of-Papers)
* [6  Issues and Challenges](https://colab.research.google.com/drive/1fb4oR7wuIJ1kaHShBGZnbxKuEyDOmdQ3#Issues-and-Challenges)
* [7  Conclusion](https://colab.research.google.com/drive/1fb4oR7wuIJ1kaHShBGZnbxKuEyDOmdQ3#Conclusion)
* [8  References](https://colab.research.google.com/drive/1fb4oR7wuIJ1kaHShBGZnbxKuEyDOmdQ3#References)

Explicitly mention the topic you chose. Add a brief discourse of why your chosen topic is of interest to you. Discuss what you perceive as the historical and future importance of the topic.

Very briefly mention the **three papers** you selected and why. Highlight the research questions posed in the papers, and the objective goals of the research. What is the impact of solving the research problems that are common across the papers?

Here is an example of how to cite an item in your list of references that must appear at the end of this document: The AI field includes a variety of search algorithms [Russell and Norvig, 2010]. Perhaps some of these search algorithms could be used to support critical decision makers [Trump, et al., 2020].

Introduction

For this assignment, I chose to cover the need for machine learning for intrusion detection in modern vehicles, applicable for both autonomous and human-driven cars. With the rise of the internet of things, the cars we see on the streets are getting 'smarter' and more communicative.

Nowadays, there is a lot of research going on in Vehicle to Vehicle, Vehicle to Infrastructure and tons of other connected vehicle technology. V2X(vehicle-to-everything) tech is part of what makes Tesla, Nikola and Fisker so cool among other big names in industry. While you see all this technology pushing self-driving and autonomous cars closer to ubiquity, there’s work being done to revolutionize the insides of the car too!

There are dozens of electronic control units (ECUs) present in cars today, communicating information about engines, brakes, fuel, speed and even car temperature and window height. There is a lot you can do with that much information from that many sensors. For example, Tesla has a well-known ‘Dog-mode’ in its cars that keeps the temperature from getting too hot or too cold, comfortable to leave dogs or people in locked cars. Parking assist sensors and cruise control are more features that are part of advanced driver assistance systems being developed.

Why do we need it?

With so much information flowing through the internal processors of cars, there comes a huge potential for malicious interference. Attacks have been shown to be able to disable engines, display incorrect information and release brakes all just by plugging into a port on a car. [K. Koscher et al. (2010)]. A video released just a few days ago by the COSIC group at the University of Leuven, Belgium shows a wireless and wired attack to hack and drive away with a Tesla Model X in a few minutes [COSIC (2020)][L. Wouters, B. Gierlichs and B. Preneel. (2020)]. Daily updates for anti-virus software on PCs are common, but today this is true for cars as well.

Ye olde in-car network: The CAN

One of the reasons for these vulnerabilities in modern cars and trucks is because of the in-vehicle network, sometimes referred to as the CAN (controller area network). It is a fast, error-correcting, broadcast only network used to communicate within devices in cars. The CAN protocol, which runs on the internal network, was designed in 1985 by Bosch. It was made keeping speed and robustness in mind, not the CIA (confidentiality, integrity, availability) metrics used for modern computer networks.

CAN Vulnerability and Attacks

There is a plethora of attack surfaces to target in the CAN protocol and many companies have hidden specific details of CAN implementations in commercial cars. However, there are features of the protocol that can be universally exploited to hack, get information, or impair the functioning of vehicles. For example the protocol handles physical faults in sensors by keeping an error count of bad messages sent or received by a particular node(sensor), if this counter exceeds a particular value, the node is put in a passive state(kicked off the network). Getting access to the network is easy using on board wired ports and wireless connection technology like Bluetooth. It is possible to overload this counter for any one module, say the electric windows and prevent them from being opened or closed [T. Hoppe, S. Kiltz, and J. Dittmann (2008)].

[M. Bozdal, M. Samie and I. Jennions. (2018)] classify CAN attacks into three types: eavesdropping, data insertion and denial of service (DoS). [H. Lee, S. H. Jeong and H. K. Kim (2017)] explore a variant of DoS called fuzzy attack and also talk about Impersonation attacks. I briefly describe them below to understand how the papers I have reviewed try to detect each attack.

**Eavesdropping** is exploiting the broadcast nature of the CAN protocol to listen in and gather information. Any node can listen in on network traffic and gather information about the location, engine RPM, fuel levels and even the driver’s phone information through Bluetooth pairing. It is a passive attack, but can be used to initiate an active attack.

**Data Insertion/manipulation** is defined by [M. Bozdal, M. Samie and I. Jennions. (2018)] as the insertion of unauthorized data packet into the CAN network.

**Denial of Service**(DoS) is the prevention of use of the CAN network by flooding it with packets, this attack also exploits the broadcast nature of the CAN to send packets to overwhelm any one sensor node or to block the whole network.

**Fuzzy Attack** is a sort of misdirection attack in which sends random spoofed node identifiers arbitrary instructions, since there’s no verification of who sent the message, the receiving nodes obey and paralyze the car with random actions.

CANs today - Avoiding or Evading attacks?

IDSs and authentication within real-time latencies and low power requirements. Online not offline training and inference. Mitigation and Amelioration

Metric Based [H. Lee, S. H. Jeong and H. K. Kim (2017)]

Classic Machine Learning Based [Tomlinson, Andrew & Bryans, Jeremy & Shaikh, Siraj. (2018)]

DNN [V. K. Kukkala, S. V. Thiruloga and S. Pasricha. (2020)]

Analysis of Papers

For each paper:

* Explain your personal understanding of the methods and approaches used. Do not quote verbatim from the paper.
* Discuss your opinion of how well the methods achieved the goals of the paper.
* Describe which parts of the paper are the most difficult to understand and what aspects of the methods are not specified with sufficient detail to allow the reader to write their own implementation.

Compare the papers by describing similarities and/or differences in the goals, methods, and results of the papers. As an optional addition to this section, discuss which presented methods you think would be most easily combined and/or translated to real-world applications.

Issues and Challenges

What are the major issues and challenges present across all methods in the papers? When presenting an issue/challenge, give examples based on the methods which have those issues. Speculate on possible ways to deal with them.

Conclusion

Give your opinion of how well the work presented in the collection of papers have advanced the state-of-the-art in their field. What remaining issues must be addressed in future work to make further significant advances?

References

1. **[V. K. Kukkala, S. V. Thiruloga and S. Pasricha. (2020)]**, *INDRA: Intrusion Detection Using Recurrent Autoencoders in Automotive Embedded Systems* in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 11, pp. 3698-3710, Nov. 2020, doi: 10.1109/TCAD.2020.3012749.
2. **[Tomlinson, Andrew & Bryans, Jeremy & Shaikh, Siraj. (2018)]**, *Using a one-class compound classifier to detect in-vehicle network attacks.* 1926-1929. 10.1145/3205651.3208223.
3. **[M. Bozdal, M. Samie and I. Jennions. (2018)]**, *A Survey on CAN Bus Protocol: Attacks, Challenges, and Potential Solutions*, 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, United Kingdom, 2018, pp. 201-205, doi: 10.1109/iCCECOME.2018.8658720.
4. **[H. Lee, S. H. Jeong and H. K. Kim. (2017)]**, *OTIDS: A Novel Intrusion Detection System for In-vehicle Network by Using Remote Frame* 2017 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB, 2017, pp. 57-5709, doi: 10.1109/PST.2017.00017.
5. **[K. Koscher et al. (2010)]**, *Experimental security analysis of a modern automobile*, in Proceedings - IEEE Symposium on Security and Privacy, 2010, pp. 447–462
6. **[COSIC (2020)]**, COSIC researchers hack Tesla Model X key fob - Computer Security and Industrial Cryptography Group, University of Leuven, Belgium - <https://www.youtube.com/watch?v=clrNuBb3myE> (Accessed on 30th Nov 2020)
7. **[L. Wouters, B. Gierlichs and B. Preneel. (2020)]**, Belgian security researchers from COSIC and IMEC steal a Tesla model X in minutes - <https://www.esat.kuleuven.be/cosic/news/belgian-security-researchers-from-cosic-and-imec-steal-a-tesla-model-x-in-minutes/> (Accessed on 30th Nov 2020)
8. **[T. Hoppe, S. Kiltz, and J. Dittmann (2008)]**, “Security Threats to Automotive CAN Networks -- practical Examples and Selected Short-Term Countermeasures,” in SAFECOMP 2008 : 27th International Conference on Computer Safety, Reliability, and Security, 2008, pp. 235–248