SECURITY OF VEHICLE-TO-VEHICLE COMMUNICATION NETWORKS

Krishna Nikhila Kalinga
Daniel May

Introduction:

The future is all about "Driverless Cars", with the availability of vehicles with blind spot detection, cars that can brake automatically to avoid collisions, parking assistance etc. The next step towards driverless cars is vehicles that can communicate. Todays technology lets us browse Internet in vehicles, connect to our own vehicles Wi-Fi etc, which makes the taught of vehicle to vehicle communication possible. Wireless communication is the technology, which comes handy when trying to implement the proposed idea. All communication systems are vulnerable to security attacks and have implementation problems. In this paper we would like to present possible security attacks, issues of architectures along with possible solutions and available resources.

List of Security Services we are planning to explore:

- Authentication: To ensure all the communications are accurate and can't be spoofed.
- Replay Attack: To ensure that Data transmitted is not fraudulently repeated.
- Integrity: To manage vulnerability of wireless spectrum used for communication.
- Privacy: To ensure the vehicles are not tracked by any other except, government authorized authorities.

Detailed list of problems/hypotheses we are planning to investigate:

- Detection of impersonating vehicle.
- Comprehensive study on different type of attacks on V2V communication networks.
- Limitations in Security of Communication between Vehicles.
- Comprehensive study as well as comparison of different type of algorithms implemented.

A tentative list of questions we will be seeking an answer to:

- What is V2V communication?
- What is the architecture of V2V communication?
- What are the security issues and attacks?
- What are the types of encryption algorithms?

- What are the better methods to enhance present security methods?
- What are the scenarios in which the security algorithms can be applied?
- What are the pros and cons of current security algorithms?

Procedure used for verifying the result of investigation:

Detailed study of the available resources as well as opinions of experts in the field of security will help verifying the result of my investigation.

Tentative Time schedule:

- Oct 16-17:
- As most of the resources are gathered we will start analysis of V2V architecture, which includes: structure, implementation, issues of implementation etc.
- Analyzing security attacks and limitations of security.

- Nov 04-06:
- Will learn about different encryption algorithms implemented and try to find out pros and cons of algorithms.
- How has the algorithms evolved from the day this idea was proposed

- Nov 18-20:
- Analyzing algorithms for different scenarios
- Pros and cons of algorithms for different scenarios.

- Dec 02-04:
- First draft of the research paper.
- Come up with enhancements that can be done to current techniques.

Tentative table of contents:

- Introduction
- V2V communication
- Security issues of V2V communication
- Encryption algorithms
- Scenarios
- Comparison of algorithms
- Pros and cons of current security algorithms
- Enhancements
- Evaluation and analysis
- Conclusion
- References

List of literature:

[1] *GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications,* International Standard 0018-9545, 2007

[2] T. Zhang and L. Delogrossi, "Vehicle Safety Communications: Protocols, Security, and Privacy," in *Information and Communication Technology Series*, vol. 103, T. R. Hsing and K. N. Lau, Eds. Hoboken, NJ: Wiley & Sons, 2012, pp. 106-322.

[3] J. Harding et al. (2014, August). *Vehicle-To-Vehicle Communications: Readiness of V2V Technology for Application*, DC: National Highway Traffic Safety Administration, Washington, Rep DOT HS 812 014

[4] K. Lemke, M. Wolf, C. Paar, *Embedded Security in Cars,* Bochum, Germany, Springer-Verlag Berlin Heidelberg, 2006, pp. 17-111.

[5] *A Method of Preventing Unauthorized Data Transmission in Controller Area Network,* International Standard 1550-2252, 2012.

[6] A. Weimerskirch, "V2V Communication Security: A Privacy Preserving Design for 300 Million Vehicles," CHES, Busan, Korea, 2014

[7] T. Leithauser. (2014, Aug 25). *Data Security, Privacy Issues Loom Large as Officials Eye Vehicle-to-Vehicle Tech* [Online]. Available: http://www.exlibrisgroup.com

[8] M. Amoozadeh et al. *Security Vulnerabilities of Connected Vehicles Streams and their Impact on Cooperative Driving* [Online]. Available: http://rubinet.ece.ucdavis.edu

[9] *Security Credential Management System Design*. (2012, April 13). U.S. Department of Transportation [Online]. Available: http://www.its.dot.gov

[10] T. Hehn et al. "A Security Credential Management System for Vehicle-to-Vehicle Communications," in *IEEE VNC*, Boston, MA, 2013.

[11] F. Kargl. (2011, Mar 7). *23C3: Vehicular Communication and VANETs* [Video]. Available: https://www.youtube.com

[12] Security Innovation. (2014, Nov 20). *Webcast: Talking Cars - The Biggest Security Challenge Nobody has Heard About* [Video]. Available: https://www.youtube.com