Proposal for MobiSys Demonstration
Secure Vehicle Communication (SeVeCom)

Frank Kargl (Ulm University), Panagiotis Papadimitratos (EPFL)

Inter-Vehicular Communication (IVC) systems become increasingly popular among researchers while at the same time groups like IEEE, ISO, or ETSI prepare their market introduction by working on standards documents, which commercial products will become available in 5 to 10 years. One widely acknowledged issue with IVC systems are the security and privacy problems that occur in such cooperative and ubiquitous systems. Between Jan. 2006 and March 2009, the EU ICT FP6 project SeVeCom has addressed those issues, designed an extensive security system for IVC, and developed a corresponding prototype for secure and privacy-preserving vehicular communication. See http://www.sevecom.org/ for project details.

The SeVeCom implementation is based on the ACUp communication system provided by BMW and runs on PC hardware as well as on dedicated vehicular communication subsystems - called Denso Wireless Safety Units (WSUs) (see Fig.1). Wireless communication uses IEEE 802.11p.

The SeVeCom demonstrator features two application scenarios: a cooperative awareness application where a vehicle „sees“ other vehicles by exchange of periodic beacon messages and can e.g. display warnings if there is a risk for collision. Second, an application features a road hazard warning based on road-side units (RSUs) sending a road condition warning to approaching vehicles. This includes multi-hop forwarding of warning messages between vehicles to reach larger coverage.

Those applications are running on notebooks connected to the WSUs. In-vehicle system provides positions from mobility traces pre-recorded in real driving situations to emulate vehicle movements when being demonstrated in a desktop setting. See Fig. 2 for overall setup. The applications visualize positions of vehicles and warnings graphically on maps. The SeVeCom security system [1,2] that is integrated with the communication stack features among others:

- Identity management with back-end certification authority to allow long-term identification of vehicles. Also included is certificate management and revocation.
- Privacy protection by means of changing pseudonyms. This includes change of cryptographic material and addresses used by the communication system, e.g. MAC addresses.
- Secure communication mechanisms based on cryptographic protection (ECC-based signatures) plus consistency checks, e.g. based on time and position where messages have been received.
- Emulation of a hardware security module that is responsible for secure storage of secret key material, signature generation, and time stamping.
- In-Vehicle gateway that protects connections to in-vehicle busses by means of a firewall and intrusion detection component.

The operations of the security system are primarily demonstrated based on attacker simulations. One can activate different forms of attacks, where e.g. invalid signatures are generated or earlier packets from a remote location are replayed. The security system reacts in all cases by detection and marking those data packets. It is then up to the application to handle those packets. In case of our demonstration, the information (like vehicle positions or warnings) are displayed, but marked as invalid by different colors.

Many features demonstrated - like secure multi-hop communication or MAC changes - have not been demonstrated at previous occasions [3,4,5]. Regarding the demo booth, we need enough space to put 3 computer systems side-by-side.

Fig. 1: Denso WSUs

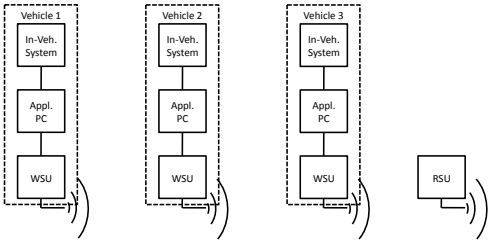

Fig. 2: Demonstration Setup

Additional authors (in order of affiliation):
Tamás Holczer (BUTE), Stefano Cosenza (CRF), Albert Held, Michael Müter and Naim Asaj (Daimler AG), Petra Ardelean (EPFL), Danny de Cock (KU Leuven), Michel Sall (Trialog), Björn Wiedersheim (Ulm Univ.)

References:

[1] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communications: Design and Architecture," IEEE Communications Mag., Nov. 2008

[2] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, B. Wiedersheim, E. Schoch, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communications: Implementation, Performance, and Research Challenges," IEEE Comm. Mag., Nov. 2008

[3] M. Gerlach, F. Friederici, P. Ardelean, P. Papadimitratos, "Security Demonstration" C2C-CC Forum and Demonstration, Dudenhofen, Germany, October 2008

[4] P. Ardelean, P. Papadimitratos, "Secure and Privacy-Enhancing Vehicular Communication," Demo, IEEE WiVeC, Calgary, AL, Canada, September 2008

[5] E. Schoch, F. Kargl, F. Wolf, M. Weber, "U2VAS: A Research Communication Stack for Vehicular Networks", Demo, IEEE WiVeC, Calgary, AL, Canada, Sept. 2008