On Secure Inter- and Intra-Vehicle Communications

M. M. Hasan and H. T. Mouftah

uOttawa

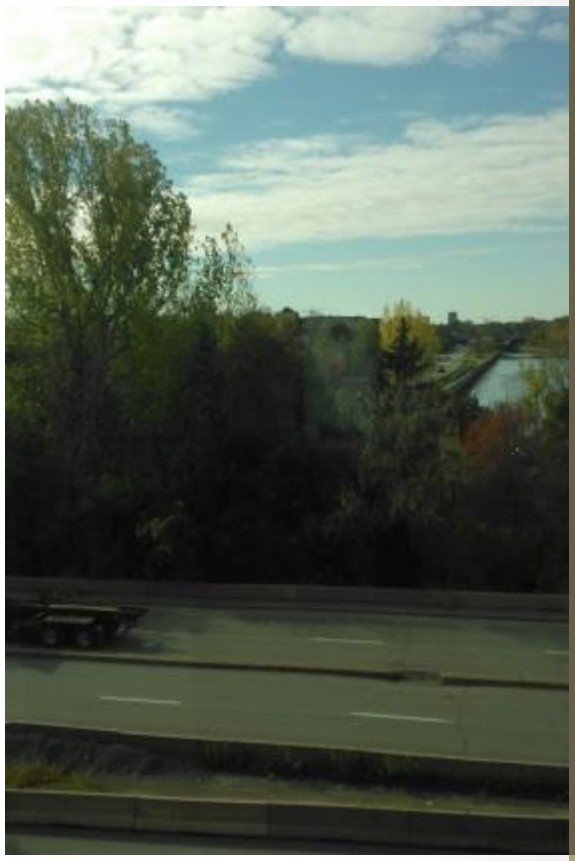
Presenter: Mahmud Hasan

October 23rd, 2013

The 31st Meeting of the WWRF, Vancouver, BC, Canada

Outline

- Introduction
- System Overview
- Proposed Techniques
- Numerical Results
- Conclusion



Introduction

- Vehicular Communications
  - Vehicle-to-anything (V2X): V2V, V2I, V2G
  - Intra-Vehicle Communications: sensors, controllers
- Applications
  - Intelligent Transport System (ITS): vehicle tracking, collision avoidance, roadside safety, congestion control
  - Smart Grid: EV discharging and charging schedule
  - Vehicular Sensor Networks: Sensing, monitoring

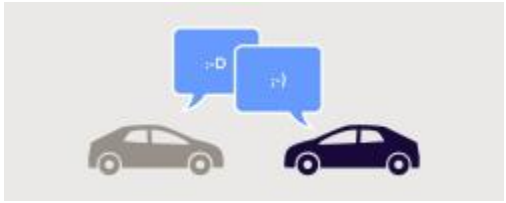
Introduction (cont.)

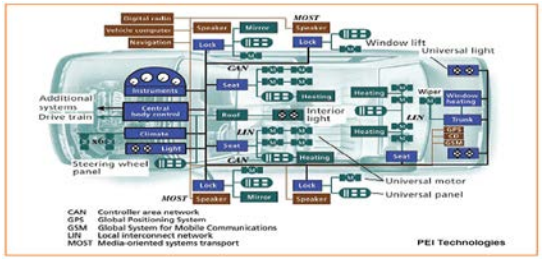
- Security Concerns
  - Sensitive information
  - Confidentiality
  - Integrity
  - Availability

- PHY layer Security
  - To boost up higher layer security mechanisms
  - Creation of additional layer of security

Introduction (cont.)

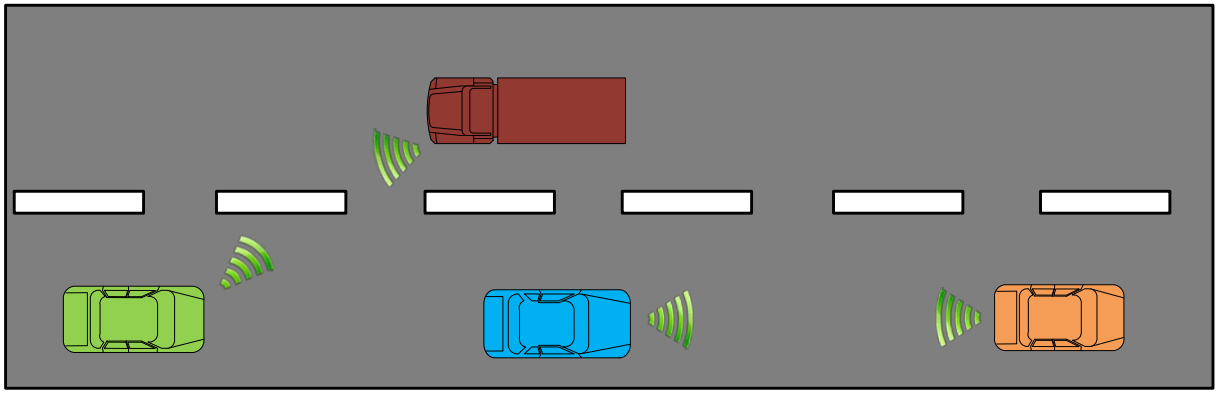
- Our current area
  - V2V communications
  - Intra-vehicle communications





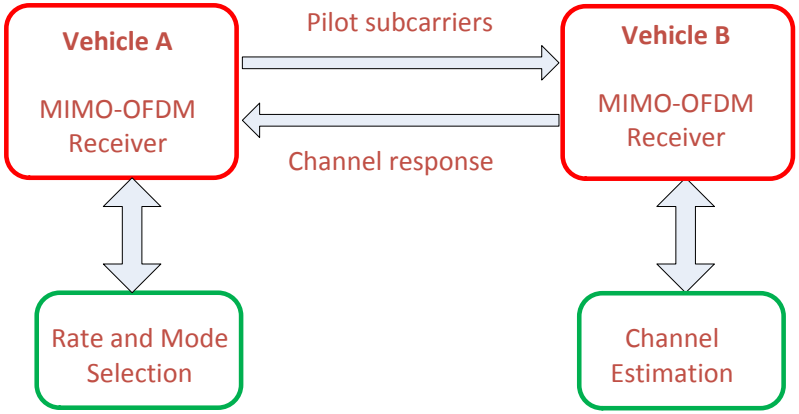
- Issues to be focused
  - V2V Authentication delay
  - V2V Eavesdropping
  - In-vehicle power line

System Overview (V2V)



- Vehicle-to-Vehicle Communications
  - IEEE 802.11p interface
  - Licensed band of 5.9 GHz
  - OFDM at the PHY layer
  - Adaptive MIMO antenna systems

System Overview (V2V Cont.)



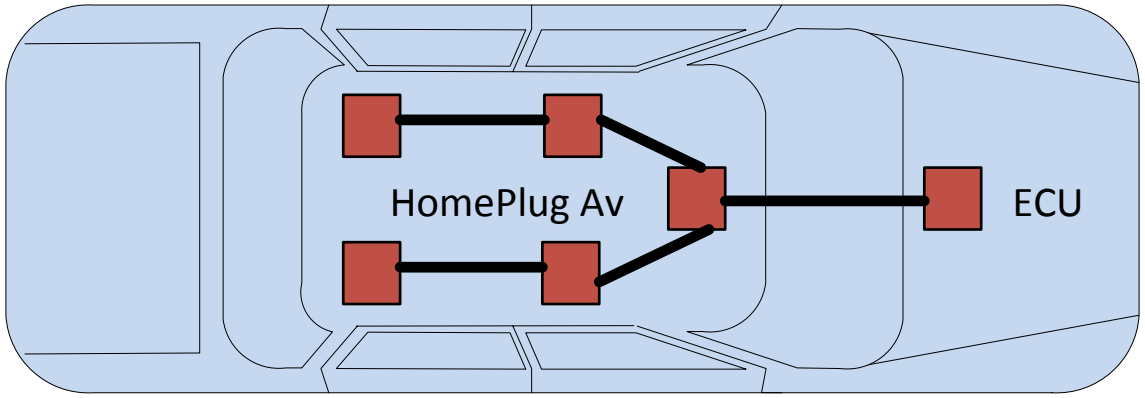
- Channel Estimation for V2V:

$$SNR_{adj,i} = (1-\alpha)SNR_{est,i} + \alpha SNR_{adj,i-1}$$

$$\alpha = f(v_R)$$

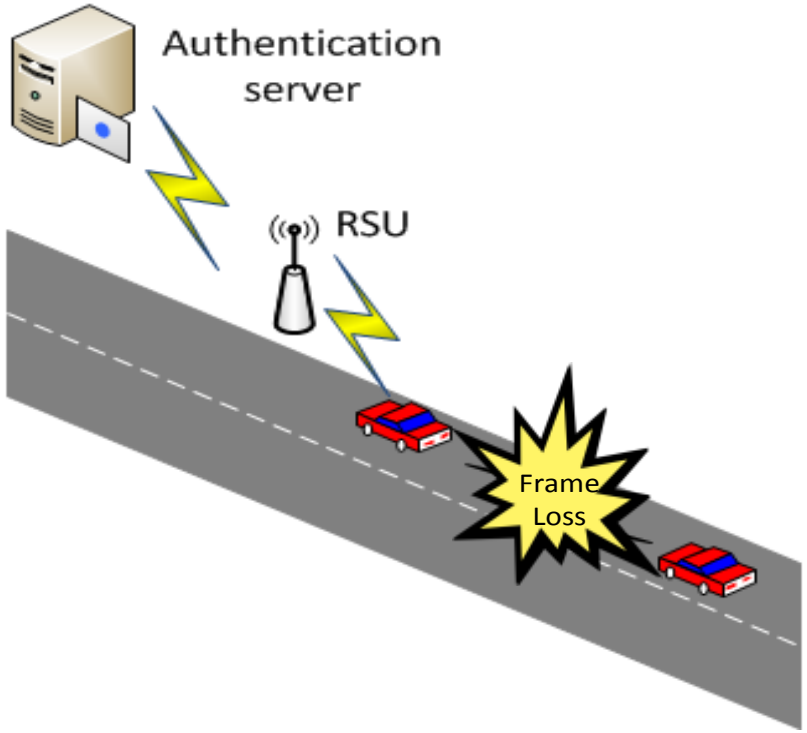
$$f_D = \pm \frac{v_R f_c}{c}$$

System Overview (Intra-Vehicle)



- HomePlug Av Interface
  - Power line communication (PLC)
  - 2-28 MHz band
  - OFDM
  - Communications between electric control units (ECUs)

Proposed Techniques (Adaptive ARQ)



- Number of Retransmission ↑ Authentication delay ↑
- Failed Authentication → Interruption of communications

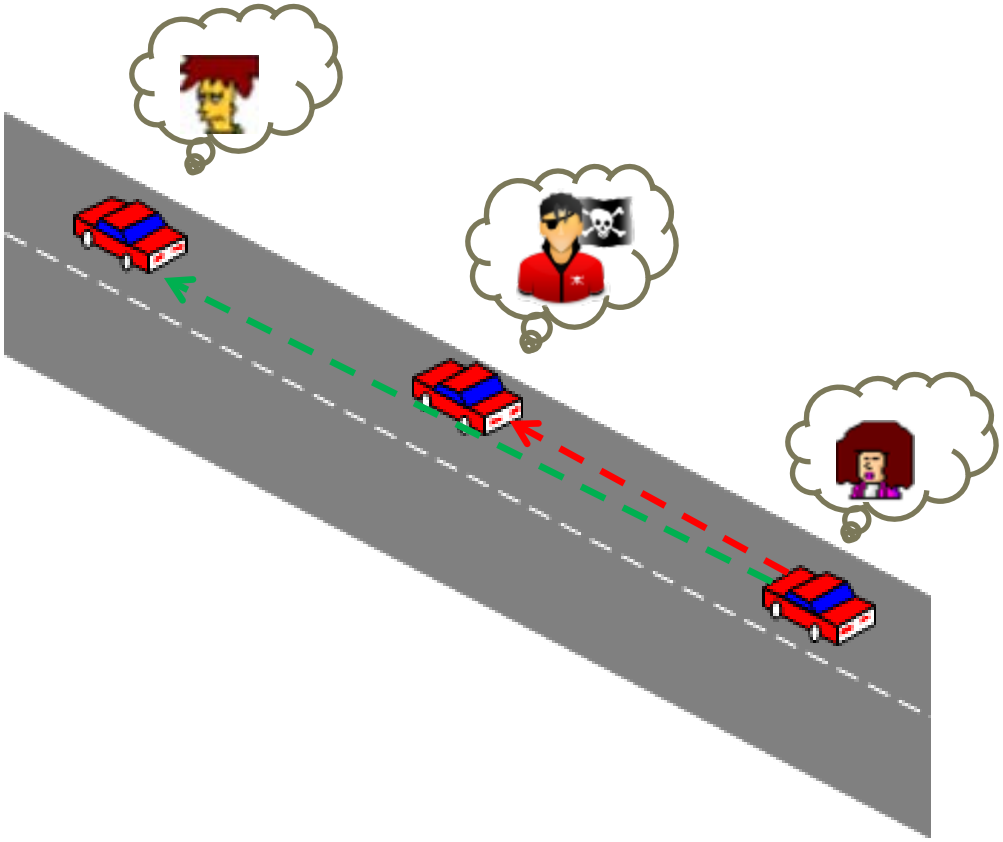
Proposed Techniques (Adaptive ARQ)

- Adaptive ARQ
  - Estimates SNR in each frame → Initial Selection
  - If the previous frame is lost → lower Rate

    Else

    Initial Selection is Final

Proposed Techniques (Adaptive MIMO)



- Eavesdropping can be active or passive
- Eavesdropping can initiate the MITM or replay attack

Proposed Techniques (Adaptive MIMO)

- Adaptive MIMO
  - Switches transmission mode between STBC and SM based on CSI
  - Mode switching occurs based on post-detection SNR instead of Demmel condition
  - Improves reliability between legitimate vehicles
  - Eavesdropper experiences very high BER

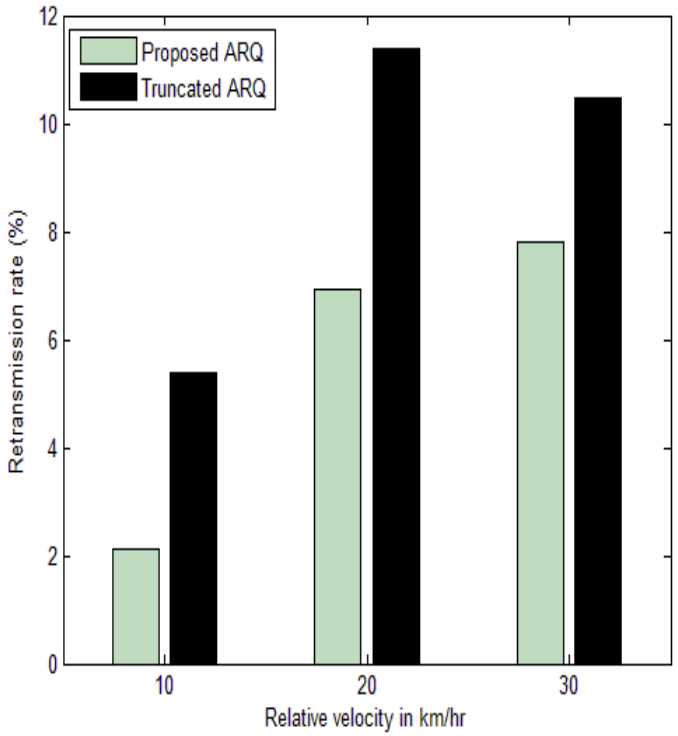
Proposed Techniques (In-Vehicle Power Line)

- Security of the Wired Networks
- Channel Capacity and Secrecy Capacity
- Design considerations: Signal-to-noise-ratio (SNR)
  - Attenuation ↑ Signal degradation ↑
  - Group delay ↑ Inter-symbol interference (ISI) ↑

SNR↓

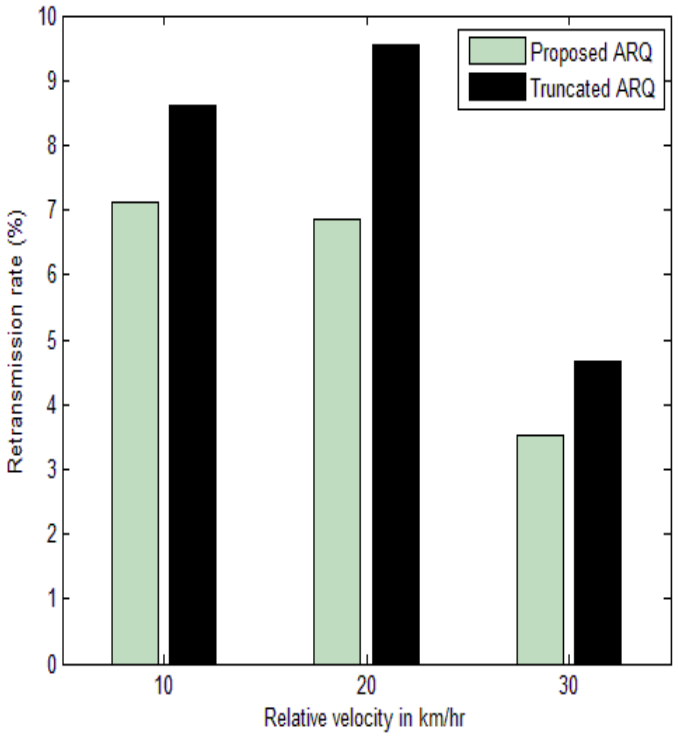
Numerical Results: V2V Authentication

Decremental Distance



- Imperfect CSI
- Initial distance 50m
- Variable power settings

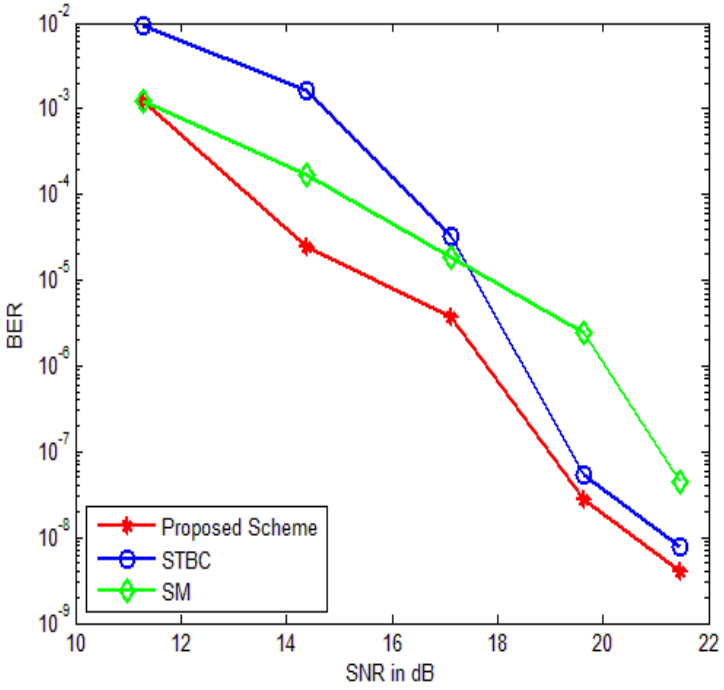
Incremental Distance



- Imperfect CSI
- Initial distance 150m
- Variable power settings

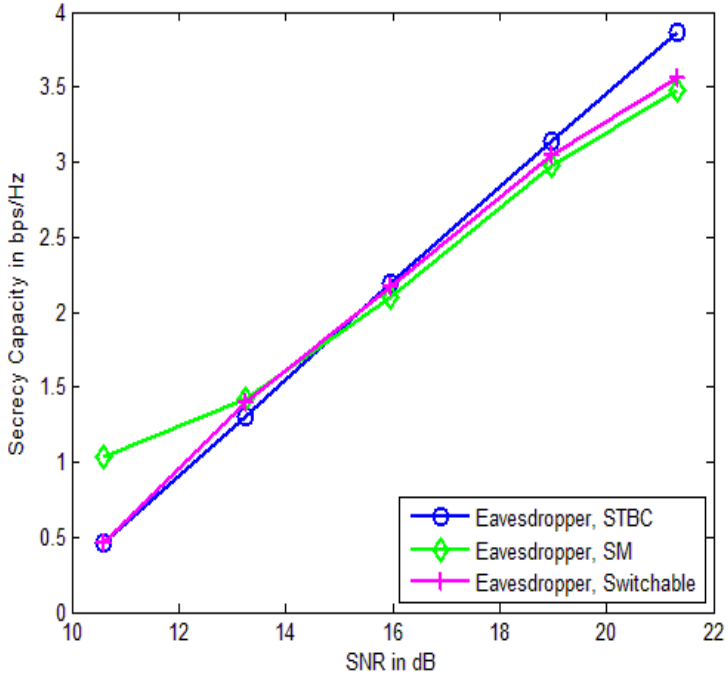
Numerical Results: V2V Security Against Eavesdroppers

BER for Legitimate Users



Improved reliability between legitimate vehicles

Secrecy Capacity



Enhanced secrecy capacity against eavesdropping

Numerical Results: Intra-Vehicle Cables

Manufacturer's Data

Cable Type	Nominal Cross Section (mm2)	Nominal Diameter (mm)	Insulation Thickness (mm)
1	1	1.13	0.7
2	1.5	1.38	0.7
3	2.5	1.78	0.8

Approximate Expressions

Cable Type	Attenuation Constant (Nepers/meter) for (MHz)	Group Delay (ns/meter)
1	$0.0020\,f$	6.162
2	$0.0018\,f$	6.072
3	$0.0017\,f$	6.096

Conductor diameter ↑ **Attenuation ↓ Group delay ↓**

Insulation thickness ↑ **Group delay ↑**

Conclusion

- PHY layer techniques can boost up higher layer security mechanisms
- Mobility awareness is a key factor in designing V2V security protocols
- Hybrid network can be used for secure Intra-vehicle communications

Thank you!

And

Questions?