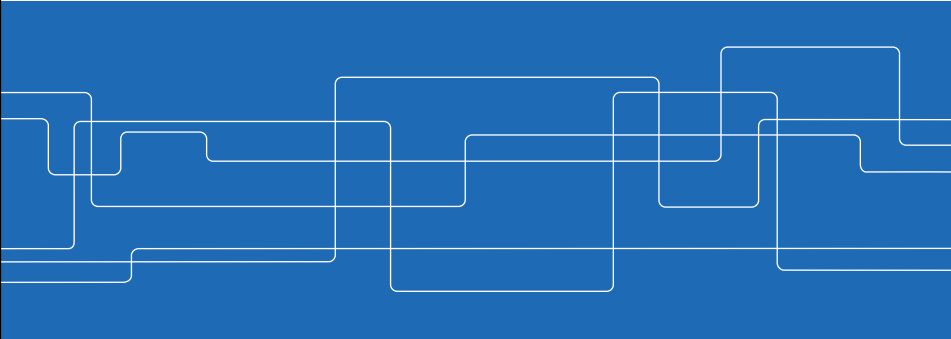

 **Security concerns and their impact on our understanding of Cyber-Physical Systems** KTH ROYAL INSTITUTE OF TECHNOLOGY


Panos Papadimitratos

Networked Systems Security Group  
[www.ee.kth.se/nss](http://www.ee.kth.se/nss)

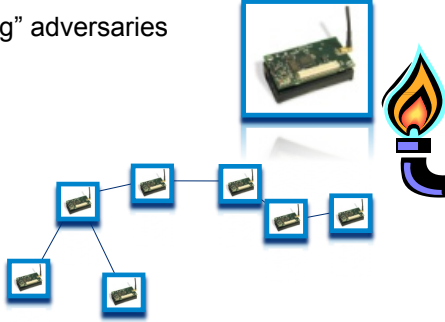


 **“Physical” can harm “cyber”**

Usually, we talk about the cyber-attacker harming the physical system



“Input-controlling” adversaries




[ESCAR'06]



### 'Pay attention to the context'

Cautionary tales: neighborhood, proximity, and location

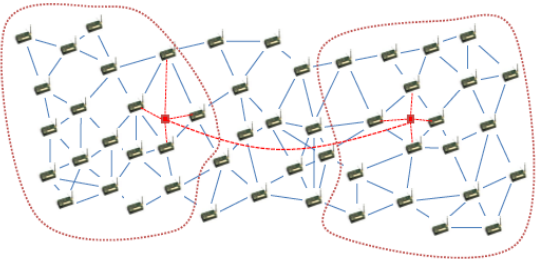
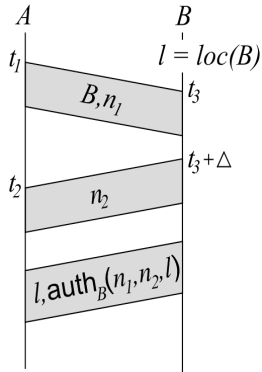


### Tale 1: Secure neighborhood discovery

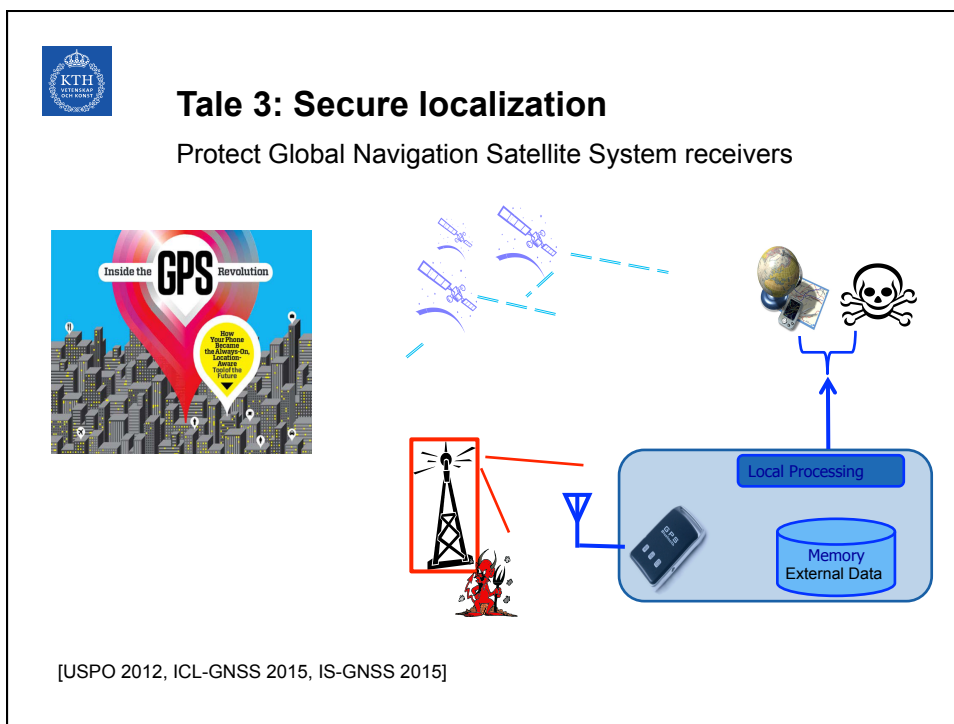
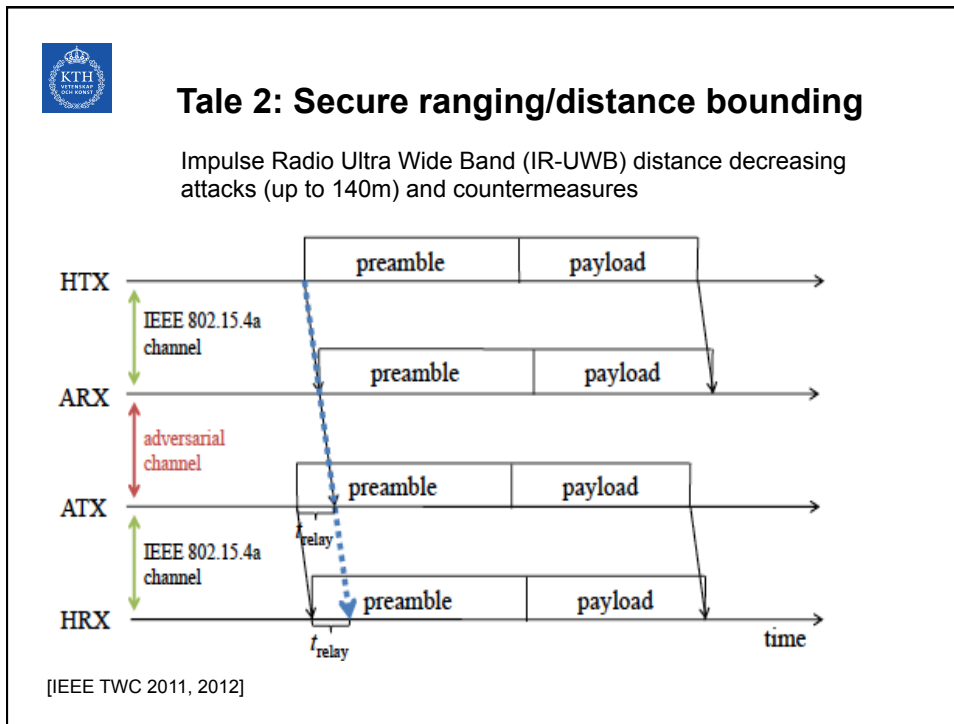
Secure neighbor discovery


- Impossibility result: no time-based solution
- Proven secure protocols
- Position and communication neighborhood

$t_2 - t_1 - \Delta = 2d(\text{loc}(A), l)v^l$   
 $\downarrow$   
 Neighbor(A, B, t<sub>1</sub>)  
 Neighbor(B, A, t<sub>2</sub>)

[IEEE TDSC 2013, IEEE TMC 2014]

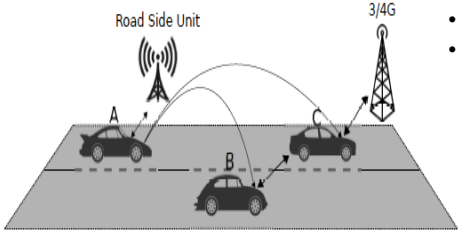


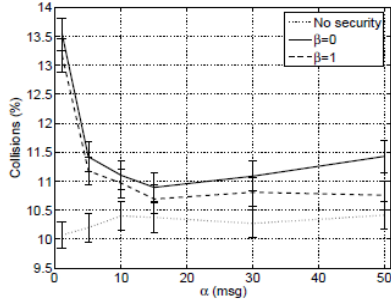


## ‘Security & Privacy can harm safety’

Architecture and protocols

- Large-scale, resource constraints
- Real-time and physical world challenges






<p>Vehicle A:</p> <ol style="list-style-type: none"> <li>1. Generate and sign message</li> <li>2. Encapsulate message</li> <li>3. Broadcast <math>\{Msg\}_{\delta(P_A)}, \{P_A\}_{\delta(PC_A)}</math></li> </ol>	<p>Vehicles B &amp; C:</p> <ol style="list-style-type: none"> <li>1. Validate the pseudonym, <math>\{P_V\}_{\delta(PC_A)}</math></li> <li>2. Verify the signature</li> <li>3. Validate message content</li> <li>4. Accept/reject the message</li> <li>5. Re-broadcast</li> </ol>
---	--

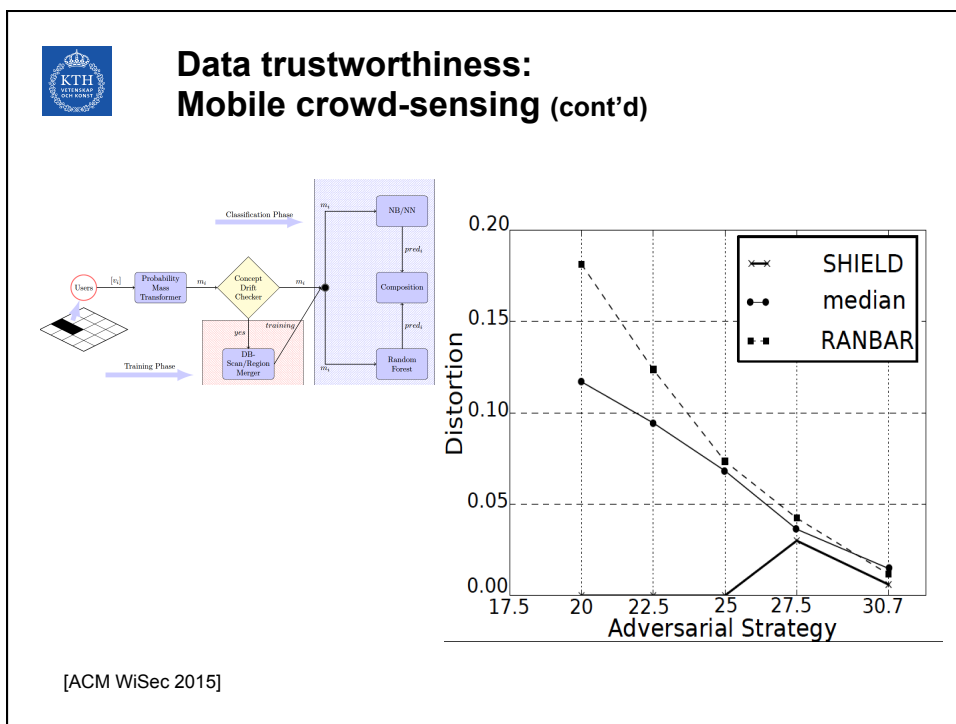
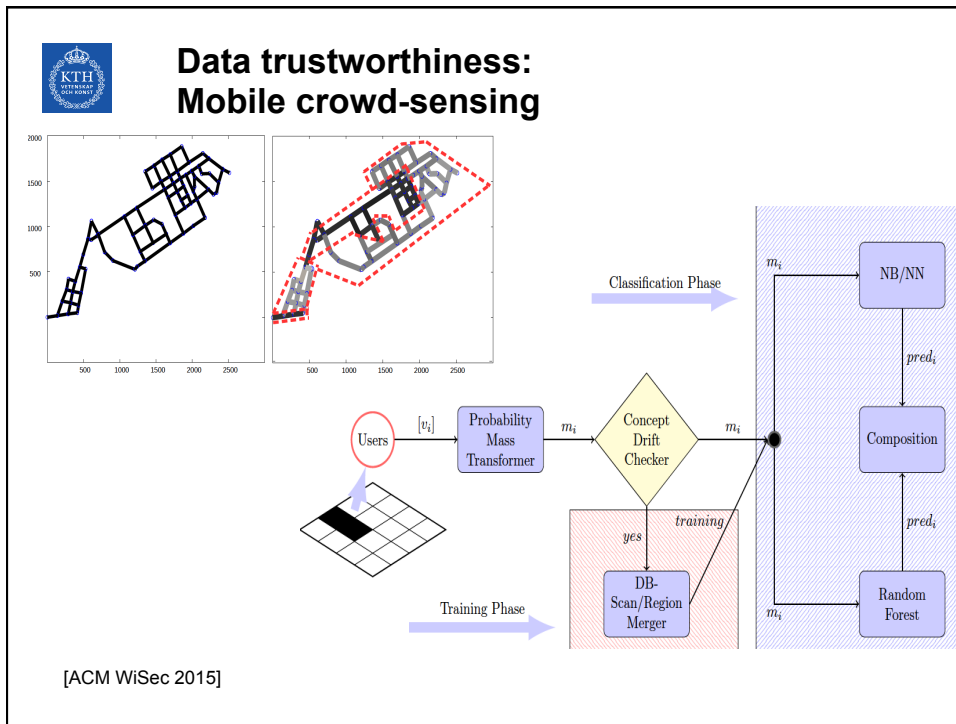
[IEEE TDSC 2011, IEEE VNC 2015, 2016]

(a) Collisions as a function of  $\alpha, \beta$ ; 8-lane highway; comparison with unsecured VC.



## ‘Experience teaches’

- CPS security **not** by obscurity
  - Open standards, ensure no obscurity on the physical part
- Policies
  - Formalisms
  - Certification for components and platforms
- Automation of processes makes security all the more important
  - Proactive mitigation
- Human can still be the weakest link
  - Physical perception manipulation can induce behaviors





## References

- [TWC11] M. Poturalski, M. Flury, P. P., J.-P. Hubaux, and J.-Y. Le Boudec, "Distance Bounding with IEEE 802.15.4a: Attacks and Countermeasures," *IEEE Transactions on Wireless Communication (IEEE TWC)*, Vol. 10, No. 4, pp. 1334–1344, April 2011
- [TWC12] M. Poturalski, M. Flury, P. P., J.-P. Hubaux, and J.-Y. Le Boudec, "On Secure and Precise IR-UWB Ranging," *IEEE Transactions on Wireless Communications (IEEE TWC)*, Vol.11, No.3, pp. 1087–1099, March 2012
- [USPO12] P. P., and A. Jovanovic, "Method to secure GNSS based locations in a device having GNSS receiver," *US Patent 8,159,391*, April 2012
- [IS-GNSS 2015] K. Zhang and P. P., "GNSS Receiver Tracking Performance Analysis under Distance-Decreasing Attacks," *International Conference on Localization and GNSS (ICL-GNSS)*, Gothenburg, Sweden, June 2015
- [KL-GNSS 2015] K. Zhang, R. A. Tuhin, and P. P., "Detection and Exclusion RAIM Algorithm against Spoofing/Replaying Attacks," *International Symposium on GNSS*, Kyoto, Japan, November 2015
- [NordSec 2015] H. Jin and P. P., "Resilient Collaborative Privacy for Location-Based Services," *Springer Secure IT Systems*, NordSec conference, pp. 47-63, October 2015
- [IEEE TDSC 2014] R. Shokri, G. Theodorakopoulos, P. P., E. Kazemi, and J.-P. Hubaux, "Hiding in the Mobile Crowd: Location Privacy through Collaboration," *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*, Vol. 11, No. 3, pp. 266 – 279, May-June 2014
- [IEEE TDSC 2013] M. Poturalski, P. P., and J.-P. Hubaux "Formal Analysis of Secure Neighbor Discovery in Wireless Networks," *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*, Vol. 10, No. 6, pp. 355 - 367, November-December 2013



## References (cont'd)

- M. Fiore, C. Casetti, C.-F. Chiasserini, and P. P., "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing (IEEE TMC)*, Vol. 12, No. 2, pp. 289–303, February 2013
- P. P. and A. Jovanovic, "Protection and Fundamental Vulnerability of GNSS," *IEEE International Workshop on Satellite and Space Communications (IEEE IWSSC)*, Toulouse, France, October 2008
- P. P. and A. Jovanovic, "GNSS-based positioning: Attacks and Countermeasures," *IEEE Military Communications Conference (IEEE MILCOM)*, San Diego, CA, USA, November 2008
- [IEEE VTMag 2015] M. Khodaei and P. P., "The Key To Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems," *IEEE Vehicular Technology Magazine*, Vol. 10, No. 4, pp. 63-69, December 2015
- [IEEE T-ITS 2015] S. Gisdakis, V. Manolopoulos, S. Tao, A. Rusu, and P. P., "Secure and Privacy-Preserving Smartphone-based Traffic Information Systems," *IEEE Transactions on Intelligent Transportation Systems (IEEE ITS)*, Vol. 16, No. 3, pp. 1428-1436, June 2015
- [IEEE IoT 2016] S. Gisdakis, A. Giannetsos, and P. P., "Security, Privacy & Incentive Provision for Mobile Crowd Sensing Systems," *IEEE Internet of Things Journal (IEEE IoT)*, 2016
- H. Jin, M. Khodaei, and P. P., "Security and Privacy for Vehicular Social Networks," *Vehicular Social Networks*, A. M. Vegni, V. Loscri, A. V. Vasilakos, Eds., CRC Taylor & Francis Group, 2016



## References (cont'd)

- [IEEE IT 2017] M. Mirmohseni and **P. P.**, "Secrecy Capacity Scaling in Large Cooperative Wireless Networks," *IEEE Transactions on Information Theory (IEEE TIT)*, 63(3), 1923-1939, March 2017
- [IEEE JSAC 2006] **P. P.**, and Z.J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications (IEEE JSAC)*, Special Issue on Security in Wireless Ad Hoc Networks, Vol. 24, No. 2, pp. 343-356, February 2006
- [IEEE ISIT 2014] M. Mirmohseni and **P. P.**, "Active Adversaries from an Information-Theoretic Perspective: Data Modification Attacks," *IEEE International Symposium on Information Theory (IEEE ISIT)*, Honolulu, HI, USA, July 2014
- [IEEE INFOCOM 2014] W. Galuba, **P. P.**, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: Scalable Secure Routing for Ad-hoc Networks," *IEEE Conference on Computer Communications (IEEE INFOCOM)*, San Diego, CA, USA, March 2010
- P. P.**, Z.J. Haas, and J.-P. Hubaux, "How to Specify and How to Prove Correctness of Secure Routing Protocols for MANET," *International Conference on Broadband Communications, Networks, and Systems (IEEE-CS BroadNets)*, San Jose, CA, USA, October 2006
- [IEEE TDSC 2011] G. Calandriello, **P. P.**, A. Lioy, and J.-P. Hubaux, "On the Performance of Secure Vehicular Communication Systems," *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*, Vol. 8, No. 6, pp. 898-912, November - December 2011
- [ACM WiSec 2015] S. Gisdakis, T. Giannetsos and **P. P.**, "SHIELD: A Data Verification Framework for Participatory Sensing Systems," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec)*, New York, NY, USA, June 2015
- [ACM WiSec 2014] S. Gisdakis, T. Giannetsos and **P. P.**, "SPPEAR: Security & Privacy-Preserving Architecture for Mobile Crowd-Sensing Applications," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec)*, Oxford, UK, July 2014



## References (cont'd)

- [IEEE VCN 2016] H. Jin and **P. P.**, "Proactive Certificate Validation for VANETs," *IEEE Vehicular Networking Conference (IEEE VNC)*, Columbus, OH, USA, December 2016
- [IEEE VNC 2015] H. Jin and **P. P.**, "Scaling VANET Security Through Cooperative Message Verification," *IEEE Vehicular Networks Conference (IEEE VNC)*, Kyoto, Japan, December 2015
- [ACM CCR 2017] M. Hollick, C. Nita-Rotaru, **P. P.**, A. Perrig, S. Schmid, "Toward a Taxonomy and Attacker Model for Secure Routing Protocols," *ACM SIGCOMM Computer Communication Review*, 47, 1, 43-48, 2017
- [iNetSec 2015] **P. P.**, "Specification for secure routing: towards formal reasoning," *IFIP WG 11.4 Workshop -iNetSec*, October 2015
- [IEEE INFOCOM 2014] M. Mirmohseni and **P. P.**, "Scaling Laws for Secrecy Capacity in Cooperative Wireless Networks," *IEEE Conference on Computer Communications (IEEE INFOCOM)*, Toronto, Canada, April 2014
- [IEEE T-ITS 2017] M. Khodaei, H. Jin, and **P. P.**, "SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems," *IEEE Transactions on Intelligent Transportation Systems (IEEE ITS)*, in revision
- H. Jin and **P. P.**, "Resilient Privacy Protection for Location-Based Services Through Decentralization," *ACM WiSec*, Boston, MA, USA, July 2017



# Security concerns and their impact on our understanding of Cyber-Physical Systems

KTH ROYAL INSTITUTE  
OF TECHNOLOGY

Panos Papadimitratos

Networked Systems Security Group

[www.ee.kth.se/nss](http://www.ee.kth.se/nss)

