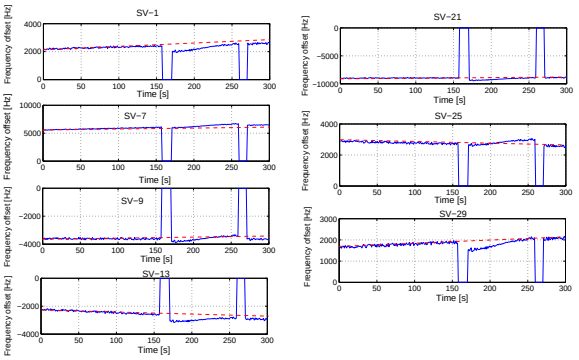

Figure 9: Doppler shift attack; sophisticated adversary. The dotted line represents the predicted and the solid line the measured frequency offset.

resilience to long unavailability periods without specialized equipment.

Our results are the first, to the best of our knowledge, to provide tangible demonstration of effective mechanisms to secure mobile systems from location information manipulation via attacks against the GNSS systems.

As part of on-going and future work, we intent to further refine and generalize the simulation framework we utilized here, to consider precisely the effect of counter-measures that only partially limit the attack impact. Moreover, we will consider more closely the cost of mounting attacks of differing sophistication levels, especially through proof-of-concept implementations.

References

[1] N. Bertelsen, K. Borre, *The GPS Code Software Receiver*, Aalborg University, Birkhauser, 2007

[2] W. Franz and H. Hartenstein, *Inter-Vehicle Communications, FleetNet project*, University Karlruhe, 2005

[3] *http://www.freepatentsonline.com/5036329.html*

[4] S. Godha, *Performance Evaluation of Low Cost MEMS-Based IMU Integrated with GPS for Land Vehicle Navigation Appplication*, University of Calgary, 2006

[5] G.W. Hein and F. Kneissl, *Authenticating GNSS Proofs Against Spoofs*, InsideGNSS, September/October 2007

[6] E.D. Kaplan, *Understanding GPS - Principles and Applications*, Artech House, 2006

[7] M. Kuhn, *An asymetric Security Mechanism for Navigation Signals*, Sixth Information Hiding Workshop, Toronto, Canada, 2004

[8] NAVSTAR GPS Joint Program Office, *NAVSTAR Global Positioning System - Interface Specification IS-GPS 200 Space Segment/Navigation User Interfaces*, SMC/GP, CA, USA, 2004

[9] P. Papadimitratos and A. Jovanovic, *Protection and Fundamental Vulnerability of GNSS*, IWSSC, Toulouse, 2008

[10] A.D. Rabbany, *Introduction to GPS*, Artech House, 2002

[11] L. Scott, *Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Signals*, ION-GNNS, Portand, Oregon, 2003

[12] J.A. Volpe, *Vulnearability Assesment of the Transportation Infrastructure Relying on GPS*, NTSC, NAVCEN draft report, 2001

[13] H. Wen, P. Huang, and J. Fagan, *Countermeasures for GPS signal spoofing*, The University of Oklahoma, 2004

[14] J. Zogg, *GPS Basics - Introduction to the System*, U-blox AG, 2002