Demo Abstract: Distance Enlargement and Reduction Attacks on Ultrasound Ranging

Sahar Sedighpour
Networked & Embedded Systems Lab,
56-125B, EE-IV,
University of California Los Angeles
+1 310 8257707
sahar60@yahoo.com

Srdjan Čapkun
Informatics & Mathematical Modeling,
Technical University of Denmark,
R. Petersens Platz, Building 322,
DK-2800 Kongens Lyngby, Denmark
+45 4525 3645
capkun@ucla.edu

Saurabh Ganeriwal,Mani Srivastava
Networked & Embedded Systems Lab,
56-125B, EE-IV,
University of California Los Angeles
+1 310 8257707
{saurabh,mbs}@ee.ucla.edu

Categories and Subject Descriptors
C.3 [**Special-purpose and application-based systems**]:*Real-time and embedded systems*

General Terms
Experimentation, Security

Keywords
Ultrasonic ranging, Wormholes, Attacks on ranging, Security

DEMO DESCRIPTION
Recently, researchers have proposed a number of ranging and positioning techniques for wireless networks. However, they all studied these techniques in non-adversarial settings. Distance estimation and positioning techniques are, nevertheless, highly vulnerable to attacks from dishonest nodes and malicious attackers [2]. Internal attackers can report false position and distance information in order to cheat on their locations and external attackers can modify the measured positions and distances of wireless nodes.

In this work, we demonstrate two attacks on ultrasonic ranging systems: the *wormhole attack* [3], by which the attackers reduce the distance measured between two honest nodes, and the *pulse-delay attack* [4], by which the attackers enlarge the measured distance. With these attacks, we show that the attackers can arbitrarily modify distances measured with ultrasonic ranging, despite the authentication and integrity protection of the messages used in the ranging protocol.

Our implementation is based on Cricket nodes developed at MIT [1] (software v2). The experiment is performed as follows. Two Cricket nodes (A and B) are placed at distance *d*. This distance is then measured using ultrasonic ranging: an ultrasonic signal and a radio signal are sent at the same time from node A to node B; node B then measures the difference between the reception time of the ultrasonic signal and the reception time of the radio signal; based on this difference, B estimates its distance to A.

SenSys'05, November 2–4, 2005, San Diego, California, USA.
ACM 1-59593-054-X/05/0011.

To demonstrate the wormhole attack, we placed attacker node M1 close to node A, and attacker node M2 close to node B. The node M1 was programmed to register the ultrasound signal sent by node A, and repeat this signal over its radio interface. The node M2 was programmed to listen to the communication from M1 on its radio receiver and to repeat this message on its ultrasound transmitted. As the speed of radio transmission (the speed of light) is much higher than the speed ultrasonic messages (the speed of sound), the attackers will succeed to speed-up the transmission of the ultrasound message from A to B. This will result in B under-estimating its distance to A.

To demonstrate the pulse-delay attack, we place a single attacker node M1 close to node B. M1 is programmed to jamm the reception of the ultrasound signal at node B, as soon as it receives the radio signal from A. M1 then replays the ultrasound signal to node B, after an arbitrarily delay, which results in node B over-estimating its distance to node A. Message jamming is emulated through the absence of the original signal, to cope with Cricket sound signal thresholding.

Our experimental setup allows the audience to observe distances being enlarged and reduced "on the fly" on the computer display. First, our nodes (A and B) measure their distance repetitively and the measured values are displayed on the computer display (corresponding to the actual distance). Second, the attackers are activated and the audience can observe the measured distance being reduced/enlarged as a consequence of the wormhole/pulse-delay attack.

REFERENCES
[1] Nissanka B. Priyantha, Anit Chakraborty, Hari Balakrishnan, *The Cricket Location-Support system*, In Proceedings of the 6th ACM MOBICOM, Boston, MA, August 2000.

[2] S. Capkun, J.P. Hubaux**,** *Secure positioning of wireless devices with application to sensor networks***,** In Proceedings of IEEE INFOCOM 2005.

[3] Yih-Chun Hu and Adrian Perrig and David B. Johnson, *Packet Leashes: A Defense against Wormhole Attacks in Wireless Network*, in Proceedings of IEEE INFOCOM 2003.

[4] S. Ganeriwal, S. Capkun, S. Han, M. Srivastava, *Secure Time Synchronization Service for Sensor Networks***,** In Proceedings of Wireless Security Workshop (WiSe) 2005.