Locking Out The Evil Guys ... Without Using Keys

The use of wireless networks is increasing despite the risk of attack. Traditional access control precautions are based on keys and cryptography.

This approach is problematic:

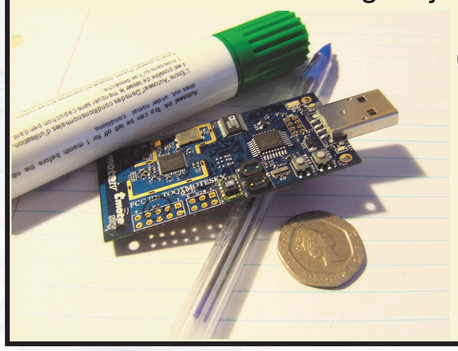
- Keys can be stolen or hacked.
- Cryptography costs energy.
- Denial of service can target the cryptography itself and waste energy.

Distance-Based Message Authentication, or DBMA, uses physical boundaries and the laws of physics to lock out attackers without using keys.

We proposed, implemented and evaluated DBMA. As far as we know, we are the first to use RF distance for access control.

Wireless Sensor Networks

Characterised by a low-cost, low-power, design. Can be especially vulnerable to energy-draining attacks and false message injection.



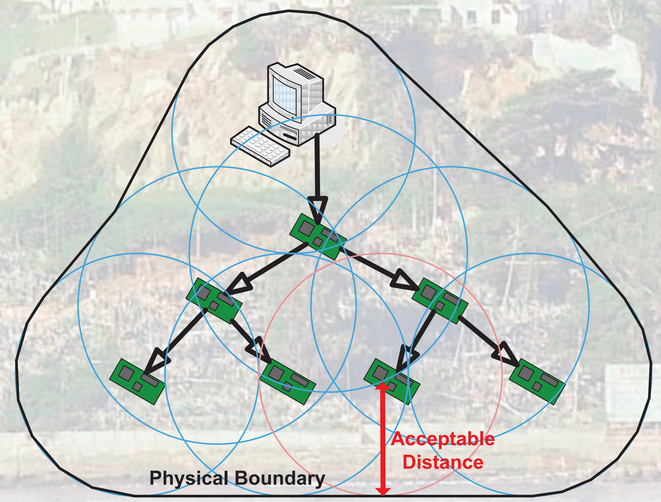
Common uses:

- Factories
- Healthcare
- Security
- Logistics

DBMA Concept

1. Chose intended node positions and links.
2. Carry out trial distance measurements on those links to identify accuracy.
3. Enable suitable links.
4. Check, or erect, physical boundary:

The physical boundary must prevent an attacker from being within an acceptable radius of a node.



Every time a message is sent between nodes:

- Measure the distance whilst **receiving**.
- Reject if the measurement result is too high.

If a message is discarded, it does not need to be forwarded or processed any further. This avoids further resource wastage, false message injection and energy denial attacks.

PUBLICATIONS

1. Chung, A. and Roedig, U., "Implementation and Evaluation of Distance-Based Message Authentication," IEEE WSNS/MASS 2010.
2. Chung, A. and Roedig, U., "Poster-Abstract: Implementation of Distance-Based Message Authentication for WSNs," EWSN 2010.
3. Chung, A. and Roedig, U., "On The Feasibility of a New Defense Layer for Wireless Sensor Networks using RF Ranging," IFIP N2S 2009.

Project Overview

DBMA requires that measurements are taken at the same time as message exchange:

- Round-Trip-Time was selected as it measures the propagation delay of a message.
- This delay can be converted into a distance.
- An attacker cannot `accelerate' a message.
- The attacker is therefore left with a very hard engineering challenge instead of `hacking'.
- Round Trip Time Message Authentication Protocol (RTTMAP). See [3].

RTTMAP was implemented using real devices to obtain energy performance and accuracy data:

- The Nanotron NA5TR1 chipset was chosen.
- Chirp Spread Spectrum modulation (2.4 GHz).
- Achieves an accuracy of +/- 1 metre. See [1].

The measured propagation delay is not ideal:

- The RF path may not be `direct' since signals can `bounce' around the site.
- Bad links involve paths that are too long.
- Extending the boundary to compensate for this may be infeasible and expensive.
- Some links therefore have to be disabled.
- We propose methods to chose suitable links.
- These methods exploit link redundancy but must maintain network connectivity.

LANCASTER UNIVERSITY

Tony Chung - School of Computing and Communications

4th Year PhD under supervision of Dr Utz Roedig

Faculty of Science and Technology Research Conference, 14th December 2010

School of Computing and Communications