Practical MANET Routing Security

Jared Cordasco, Werner Backes, and Susanne Wetzel
Department of Computer Science

STEVENS Institute of Technology
Research & Entrepreneurship Day 2008

Overview

What:

- Develop balanced methods for securing MANET routing protocols.

Why:

- Original protocols were not designed to include security measures.
- Cryptographic protocols cause Denial of Service (DoS) attacks.

How:

- Evaluate less expensive cryptographic operations and trust mechanisms.
- Create appropriate combinations based on hardware availability, security requirements, and other scenario specific information.

Wireless Networks

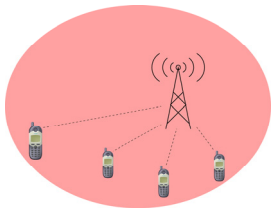
Traditional Wireless Networks

Pros:

- Reliability
- Speed

Cons:

- Infrastructure
- Single point of failure



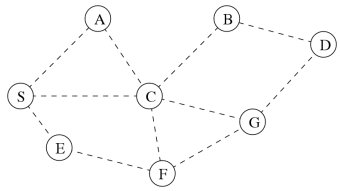
Ad-hoc Networks

Pros:

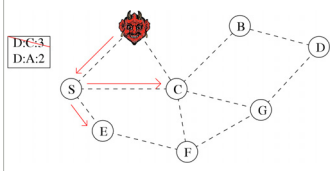
- No infrastructure
- Low cost

Cons:

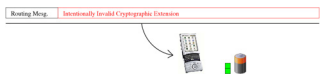
- Less reliable
- Complex communication



Attacks on Ad-Hoc Networks:



Stealth Attack: Impersonation



Denial of Service

Challenge: Finding suitable trade-off between vulnerability to stealth attacks and DoS.

Experiments

Hardware:

We use three different platforms for ad-hoc networks:

(A) TelosB Mote

(B) Sharp Zaurus SL-5500

(C) Everyday PC

	CPU	RAM	Storage	OS
A	8MHz 16-bit MSP430	10KB	48KB prog + 1MB data	TinyOS 2.x
B	206MHz SA-1110	32MB	16MB ROM + 32MB tmp	Linux 2.4
C	1.2GHz 32-bit x86	512MB	20+GB hdd	Linux 2.6

Cryptography vs. Trust:

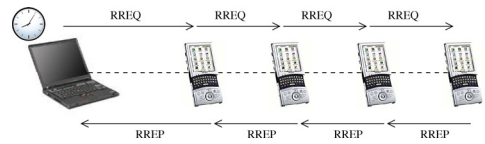
Implementation of

- AODV
- SAODV (cryptographically secured)
- TAODV (trust-based)

Overhead for cryptography/trust on Zaurus platform:

Protocol	Operation	Processing Time (ms)
SAODV (RSA)	SSE generation	30.8
	SSE validation	3.81
TAODV (Trust)	RREP/HELLO send	0.0453
	RREP/HELLO processing	0.0452
	R_ACK send	0.193
	R_ACK processing	0.297

Evaluation of round trip time for route discovery:



Protocol	Round Trip Time (ms)	Std. Deviation
AODV	138.177	0.765
SAODV	324.732	7.22
TAODV	152.780	0.863

Future Work

- Alternative cryptographic mechanisms.
- Alternative trust mechanisms.
- Finding combinations of the above mechanisms.
- Evaluating protocols in a malicious environment.