Securing MANET Routing Protocols

Jared Cordasco, Werner Backes and Susanne Wetzel

Center for the Advancement of Secure Systems and Information Assurance (CASSIA)

http://www.stevens.edu/provost/research/securitycenter/

STEVENS Institute of Technology

Research & Entrepreneurship Day 2009

Introduction

What:

- Developed a comprehensive attacker model for analyzing and comparing routing protocols.
- Developed an implementation of AODV for TelosB sensor motes (MoteAODV) and PC's + PDA's (xAODV).

Why:

- Focus on categorizing attackers instead of attacks.
- Earlier attacker models did not allow comparison of protocols.
- Previous AODV implementations did not include security.

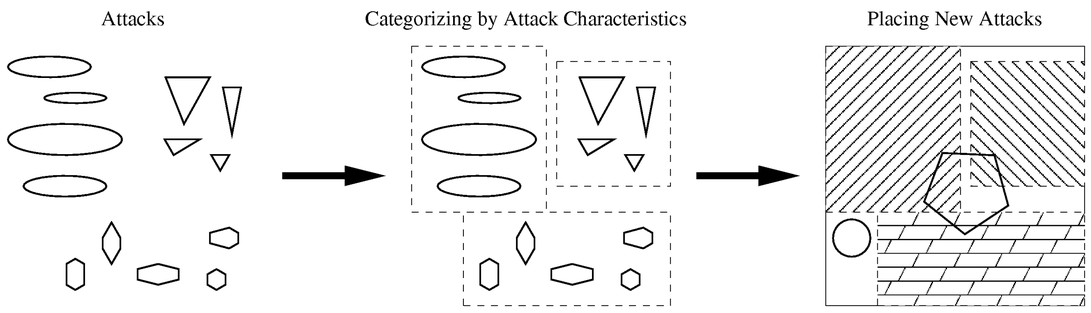
How:

- Attacker model focuses on categorizing attackers by capabilities.
- Attacker model is protocol and topology agnostic allowing comparison of routing protocols and their security.
- MoteAODV includes timer-based events in AODV and supports AES-128, hash functions (MD5, SHA-256), and trust mechanisms.
- xAODV includes an extensible framework for testing future protocol modifications.

Attacker Model

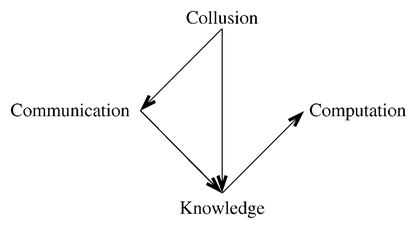
Existing Models:

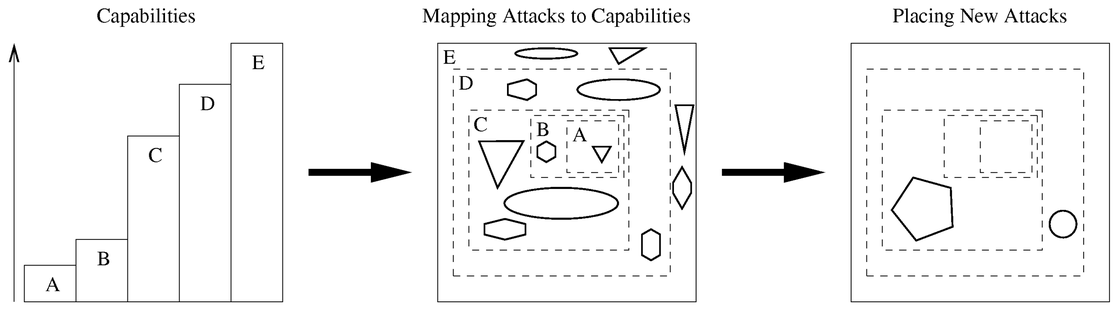
- Proposed for specific protocol, not general use.
- Categorize attacks, then transfer categorization to attackers.
- New attacks might require requiring new categorization.



Our New Model:

- Categorizes attackers based on their capabilities.
  - *Communication:*
    - Receive (passive) vs. send (active)
    - Single node vs. colluding attackers vs. Dolev-Yao equivalent
  - *Computation:*
    - Ability to encrypt/decrypt messages
    - Knowledge
    - Collusion





Advantages of New Model:

- Easier to model more general attacker.
- Yields necessary and sufficient capabilities for an attack.
- Easily evaluate new protocol for vulnerability to known attack.

MoteAODV

Implementation:

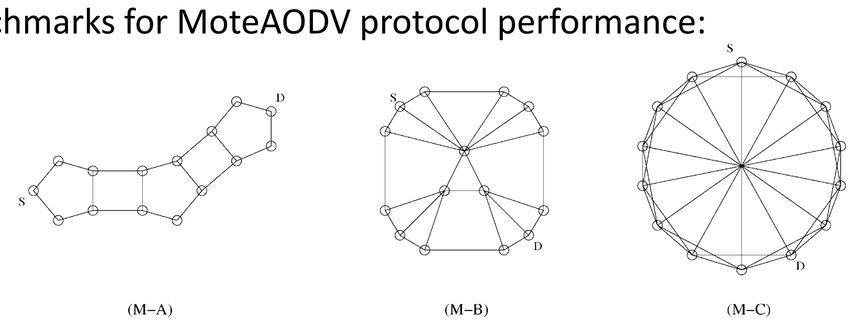
- Route expiry, HELLO message, micro-ack alternative.

Security Using Pre-Shared Keys and Trust:

- Implements AES-128, MD5, SHA-256, and trust mechanisms.
- Benchmarks for individual operations (AES-128):

Operation	Textbook	Improved	Assembler
Encryption	1.9944 ms	1.6377 ms	1.3001 ms
Decryption	2.3652 ms	1.9964 ms	1.6855 ms
Enc/Dec (CTR)	3.5411 ms	2.9000 ms	2.3769 ms

- Benchmarks for MoteAODV protocol performance:



Network	Protocol	Route Discovery (ms)	Route Recovery (ms)
(M-A)	MoteAODV	220.10	160.50 / 209.90
	MoteAODV+AES	642.30	425.70 / 601.00
	MoteTAODV+AES	714.10	-
(M-B)	MoteAODV	112.90	138.20
	MoteAODV+AES	333.00	382.60
	MoteTAODV+AES	431.20	-
(M-C)	MoteAODV	59.40	75.90
	MoteAODV+AES	223.10	201.50
	MoteTAODV+AES	317.60	-

xAODV

Implementation:

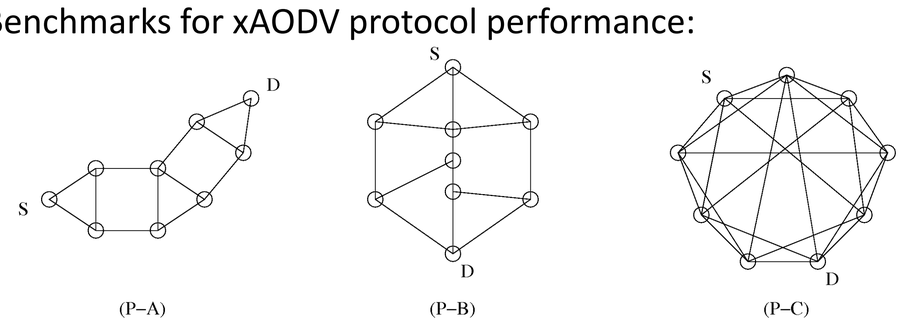
- Cross-platform runs on Zaurus SL-5500 and standard PC's.

Security Using ECC and Trust:

- Implements Elliptic Curve Cryptography and trust mechanisms.
- Benchmarks for individual operations (ECC):

Curve	Sig. Gen. w/o Opt. (ms)	Sig. Gen. w/ Opt. (ms)	Sig. Verif. (ms)
sect163k1	30.704	0.404	59.986
prime192v1	43.216	0.416	52.840
secp224r1	60.202	0.452	73.840
prime256v1	83.458	0.494	103.332

- Benchmarks for xAODV protocol performance:



Network	Protocol	Route Discovery (ms)	Route Recovery (ms)
(P-A)	xAODV	139.08	170.26
	ECC-xSAODV	491.85	637.52
	xTAODV	150.97	189.91
(P-B)	xAODV	99.78	100.32
	ECC-xSAODV	337.61	338.08
	xTAODV	120.62	119.97
(P-C)	xAODV	68.19	99.15
	ECC-xSAODV	186.38	336.20
	xTAODV	75.53	120.91

Future Work

- Analyze and compare various routing protocols in our new model.
- Test additional protocol extensions for MoteAODV and xAODV.