"Challenges of **Secure Routing in MANETs**: A Simulative Approach using ***AODV-SEC***"

Analysis of a technical report from Stephan Eichler and Christian Roman, IEEE International Conference on Mobile Adhoc and Sensor Systems, 2006.

Presented by Martin Dimkovski
CSE 6950
November 8th, 2010

Agenda of the Presentation

1. ***Part I: Security in MANET Routing***
2. Part II: AODV-SEC as a Solution
3. Part III: Simulation and Results
4. Part IV: Conclusions and Ideas

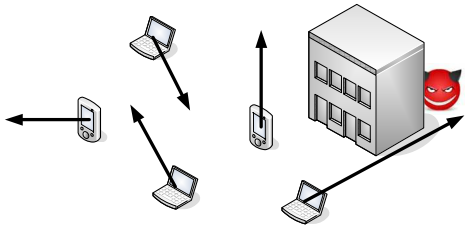
2

Part I: Security in MANET Routing

- Trouble for routing is a DoS
- MANETs are different:
  - Open air
  - Dynamic topology
  - Link breaks
  - Channel availability
- **Novel attack models**
- **= Novel security approach needed**

3

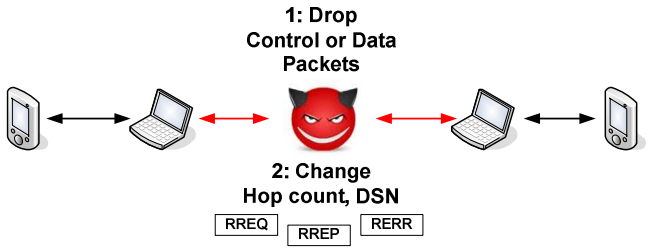
Easier Physical Access
=> Careful what is Shared



- The symmetric / asymmetric dilemma
  - Shared keys could compromise everyone
  - But asymmetric several times more expensive

4

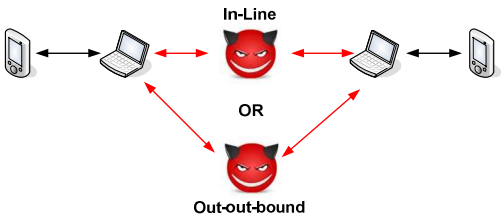
In-line Tampering



- Hop Count tampering:
  - Make itself the desired next hop
    - To eavesdrop
    - To drop packets
  - Invalidate routes
- DSN tampering:
  - Outdate good route
  - Wraparound numbering

5

Sybil Attack – Bad Identities



- Forged identities
  - Pretending to be someone else
  - Eavesdropping makes this easy
- Multiple identities
  - Causing confusion
  - Bypassing protocol logic

6

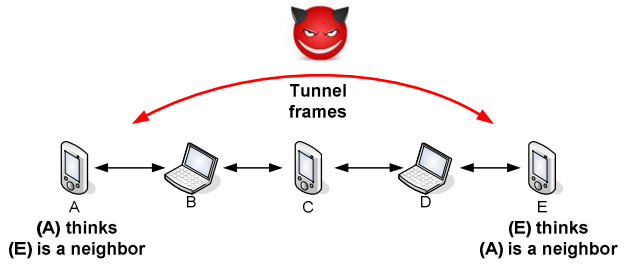
Blackhole and Greyhole Attacks

- **Blackhole** = Drop all packets
  - Drop them itself, or
  - Make them loop to max TTL
- **Greyhole** = Drop packets selectively
- Can be achieved with
  - Tampering

  And/Or
  - Bad identities

7

Wormhole Attack



- Invisible to higher layers
- Current solution = Add packet leashes (marks)
  - Time
  - Geographic

8

Previous Work on MANET Routing Security

- Any work on sensor networks applicable
- SEAD
- SRP
- ARIADNE (based on DSR)
- ARAN (based on AODV)
- SAODV

9

Agenda of the Presentation

1. Part I: Security in MANET Routing
2. ***Part II: AODV-SEC as a Solution***
3. Part III: Simulation and Results
4. Part IV: Conclusions and Ideas

10

Part II: AODV-SEC as a Solution

1. AODV-SEC Motivation
2. Public Keys Signed with External CA Certificates
3. Encryption and Signatures
4. Hash Chains on Hop Count
5. Compact New Certificate Type
6. AODV-SEC Implementation
7. Solved Problems
8. Open Problems

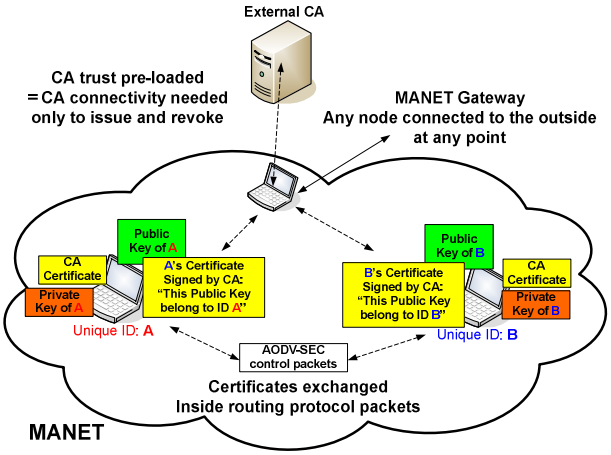
11

AODV-SEC Motivation

- Specific use case for vehicular networks
- Occasional fixed network connection
- Asymmetric cryptography (no shared keys)
- Central CA for subscription services
- Real cryptography simulation

12

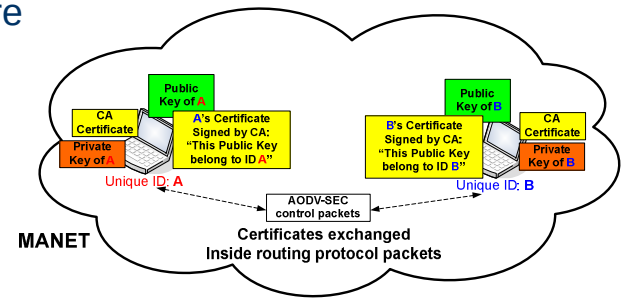
Public Keys Signed with External CA Certificates



13

Encryption and Signatures

- Senders use private keys to sign messages
- Receivers use certified public keys to verify signature



14

Encryption and Signatures (2)

- Public/Private key algorithm = RSA
- Private key signatures protect
  - Authenticity (origin)
  - Integrity of message
- 2 Signatures in each routing packet
  - Originator**, and**
  - Last hop

15

Hash Chains on Hop Count

- SHA-1 hash chains:
  - Provide a “chain of custody” on hop count
    - Going back to the originator
  - No intermediate node can lower the count
    - Even if a valid MANET member

16

Hash Chains on Hop Count (2)

- "Top Hash" field = h(h(..h(seed)..))
  - h applied Max_Hop_Count times
  - Set by originator
- "Hash" field
  - Start with h(seed)
  - Each node: Hash = h(Hash) AND Hop_Count++
- Receiver's verification: ? h(h(..(Hash)) = Top Hash
  - where h is applied Max_Hop_Count – Hop_Count

17

Compact New Certificate Type

- Bad performance with X.509 due to its size
  - Fragmentation on each control packet
- New certificate type created – mCert.
- mCert keeps only critical data and achieves a 50% size reduction (450 B vs ~1000 B).

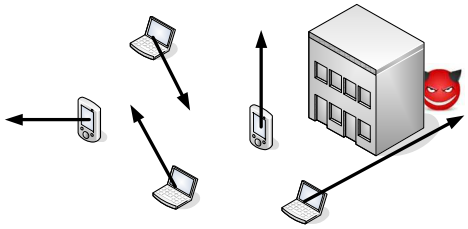
18

AODV-SEC Implementation

- Existing AODV extension options
- Existing AODV code from Uppsala University
- Only controller code module required mod.
  - Interoperable with insecure AODV

19

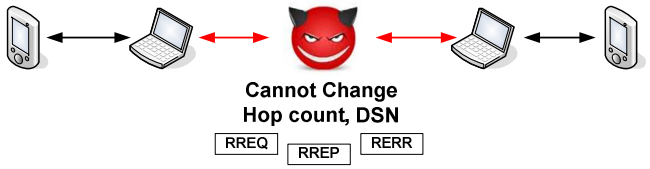
Improved: Physical Access Risks



- **No private keys are shared**

20

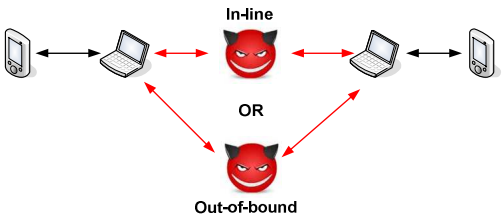
Solved: In-line Tampering



- All fields signed back to originator

21

Solved: Sybil Attack – Bad Identities



- Unique, centrally certified IDs

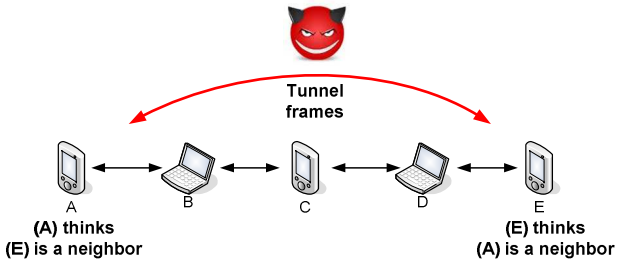
22

Solved:
Blackhole and Greyhole Attacks

- **Blackhole** = Drop all packets
  - Drop them itself, or
  - Make them loop to max TTL
- **Greyhole** = Drop packets selectively
- **Prevents sybil attacks and tampering**

23

Solved: Wormhole Attack

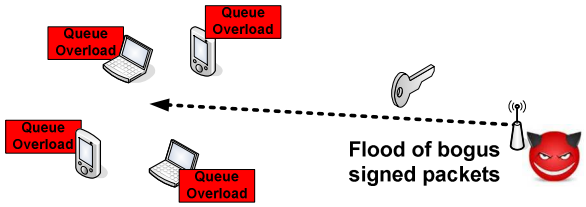


- **Packet leashes signed back to originator**

24

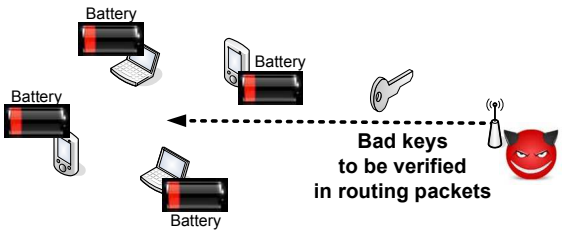
Open Problem:
DoS from Signed Control Packets

- If nodes cannot check signatures line speed:



25

Open Problem:
Sleep Deprivation Torture



26

Agenda of the Presentation

1. Part I: Security in MANET Routing
2. Part II: AODV-SEC as a Solution
3. ***Part III: Simulation and Results***
4. Part IV: Conclusions and Ideas

27

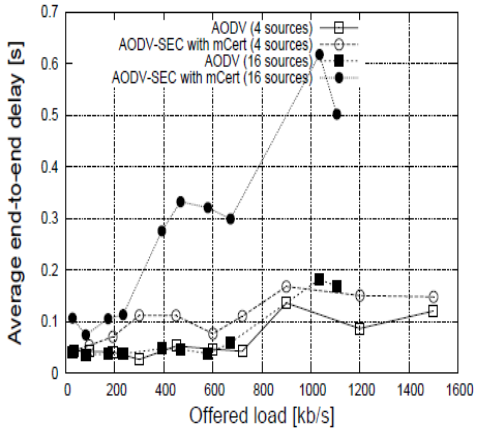
Simulation Environment

- NS-2 simulator
- DSSS, 11 Mbps, 170m range
- 802.11 DCF
- Random Waypoint Model (0 to 600 s)
- CBR, 512B packets, 25-50% of nodes as senders
- 2 scenarios:
  - 900 x 200 m, 20 nodes
  - 1500 x 300 m, 50 nodes

28

End-to-End Delay - Not Scalable

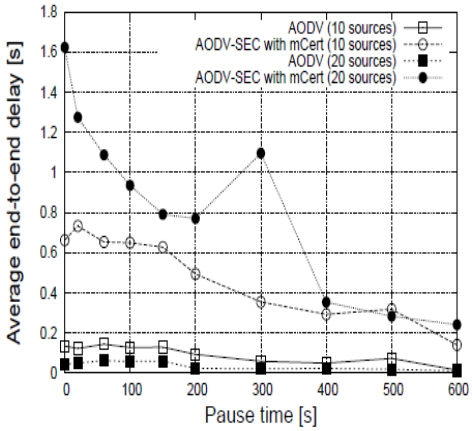
- With only 16 sources:
  - **Impractical** for **real-time** applications at moderate load
- Ex: ITU-T G.114: voice requires < 0.15 s



29

Larger Network Experiment Confirms Serious Scalability Issues

- Dramatic increase
  - Problem even for non-real-time applications



30

End-to-End Delay a Problem?

- Authors see these results as promising
  - Maybe they are not considering real-time aspects in their specific scenario.
- They acknowledge cryptographic latency
  - **but not as a significant problem**

- We believe the results are concerning
- And that the main problem is cryptographic performance

31

Cryptography Performance Factor

- Per node crypto latency (in ms)
- Based on this – Authors say 60 ms average not a problem

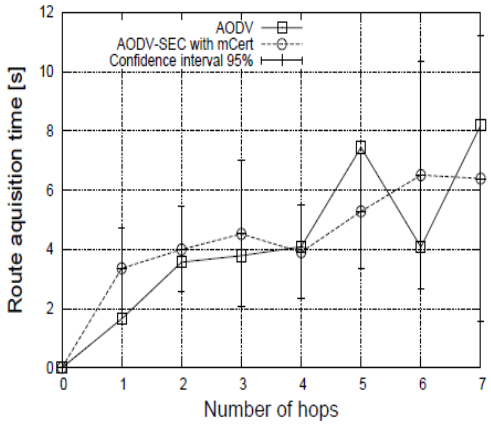
		System 1	System 2
RREQ [ms]	create	8.13	52.22
	forward	3.18	19.46
	verify	1.72	14.57
RREP [ms]	create	15.45	76.58
	forward	3.17	19.45
	verify	9.02	39.42
RERR [ms]	create	3.24	19.31
	verify	0.84	5.42

- However for an end-to-end total we need:
  - Times each node
  - For both the RREQ and RREP direction
- This can explain the delays in the results

32

Route Acquisition Times

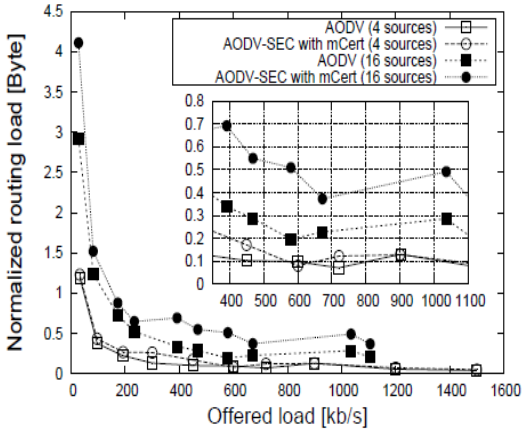
- Shows good results
- But for home many sources?
  - Inefficiency as per end2end delay comes with many sources
- And number of hops should go up to group size



33

Already Bad Overhead Can Get Much Worse

- With only 16 nodes
  - Overhead at 50% with moderate load
- Lighter cryptography (smaller packets) identified as a need



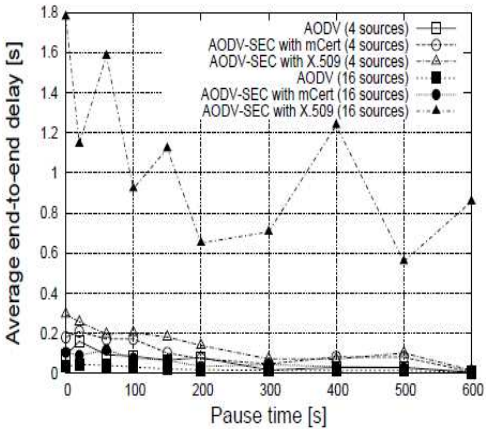
34

Mobile as Much as AODV
(but at what load?)

- Must be at low load
  - Based on previous
- Nevertheless, as such: *Maintains mobility excellence of AODV*

•X.509 results irrelevant after mCert introduction

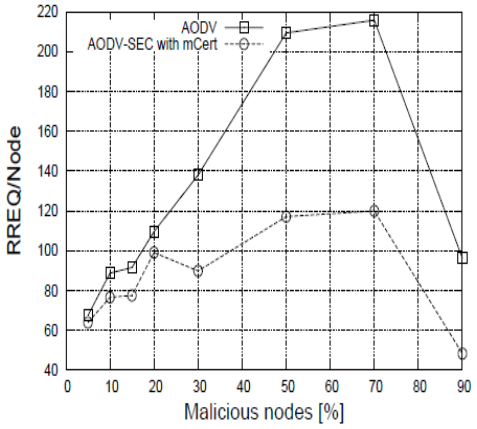
- Need load dependency



35

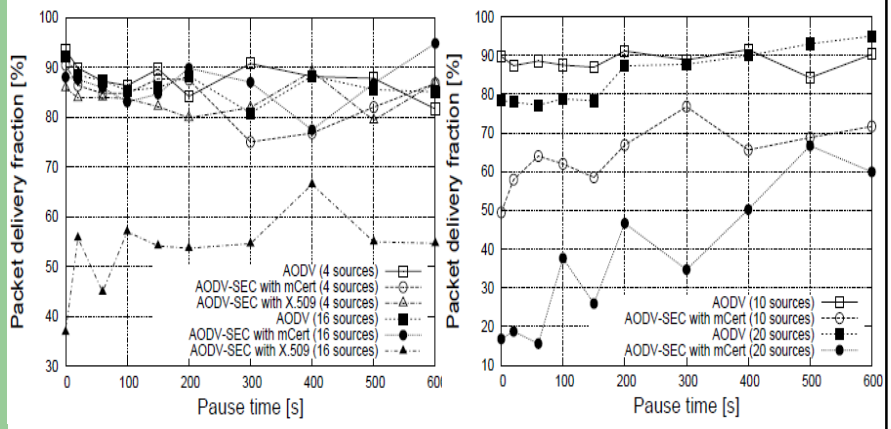
Succeeds in Blocking Malicious Nodes

- Attack scenario:
  - Attackers spoofing RREQs
  - No mobility / 16 sources
- AODV-**SEC** prevents the bad RREQs
- Peculiar why both drop above 70%?



36

Packet Delivery Ratio
Conflicting Results? (load data needed?)



37

Agenda of the Presentation

1. Part I: Security in MANET Routing
2. Part II: AODV-SEC as a Solution
3. Part III: Simulation and Results
4. ***Part IV: Conclusions and Ideas***

38

Part IV: Conclusions & Ideas

- Feasible protocol, especially for smaller, lighter scenarios
- We need to improve cryptography performance
  - Currently induced latency is concerning
- We need to improve cryptography efficiency
  - Large routing packet size is a problem
    - But probably not the main one

39

Future Improvement Ideas

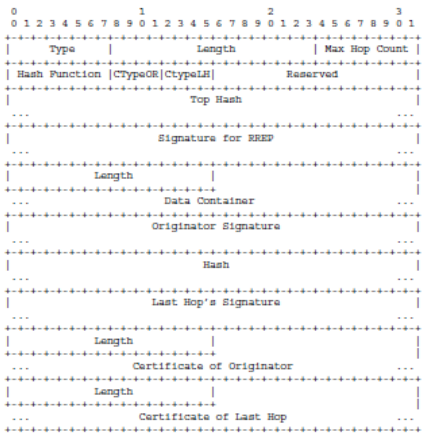
- Evaluate securing only replies
- Elliptic Curve Cryptography (ECC), would improve:
  - Certificate size / packet size
  - Calculation times
  - Better security
- More powerful simulation systems
- More efficient simulation models

40

Questions

41

Appendix 1:
Example Extension (RREP Single)



42

Appendix 2
Cryptography Library Selection

- Crypto++ and libcrypto benchmarked
  - libcrypto (OpenSSL) won

43

X.509 vs mCert

```
Certificate:
   Data:
       Version: 1 (0x0)
       Serial Number: 7829 (0x1e95)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Jul  9 16:04:02 1998 GMT
           Not After : Jul  9 16:04:02 1999 GMT
       Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                   33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                   66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                   70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                   16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                   c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                   8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                   d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                   e8:35:1c:9e:27:52:7e:41:8f
               Exponent: 65537 (0x10001)
   Signature Algorithm: md5WithRSAEncryption
       93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
       92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
       ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
       d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
       0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
       5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
       8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
       68:9f
```

Data field	Content description
type	Certificate type
h_func	Hash function type
ca_id	CA identification
serial	Certificate serial number
ip	IP address of the node
exp_time	Expiration date
exponent	exponent e (public key)
modulus	modulus n (public key)
signature	CA signature

TABLE III
DATA FIELDS OF THE MCERT CERTIFICATES

44