



# A Secure Routing Protocol for Ad Hoc Wireless Networks

---

Pramod Gurunath

Xiong Yunli



# Outline

---

- Introduction to Ad-hoc wireless networks
- Routing Protocol
  - AODV
- Security concerns
- Authenticated Routing for Ad hoc Networks (ARAN)
- Summary



# Mobile Ad-hoc Network (MANET)

---

- There is no pre-deployed infrastructure
  - Nodes cooperatively form the network by agreeing to certain routing messages
- Nodes are resource constrained
  - Usually powered with batteries
- Communication medium can be easily eavesdropped
  - Radio waves etc.



# Vulnerabilities of Ad-hoc Network

---

- Open medium makes attacks easier
  - Don't need access to wires, Don't need to pass through firewalls or gateways
- Routing protocol controls the network but is based on cooperation among nodes
  - Malicious nodes can mislead other peers



# Two Important Routing Protocols

---

- Ad-hoc On-Demand Distance Vector (AODV)
  - Intermediate nodes keep routing table entries
- Dynamic Source Routing (DSR)
  - Route is contained in the packet's header



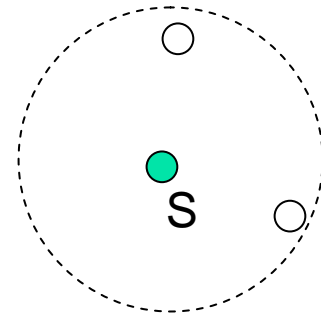
# AODV <sup>[1]</sup>

---

- Path discovery
  - Initiate routing request
  - Reverse path setup
  - Forward path setup
- Path maintenance

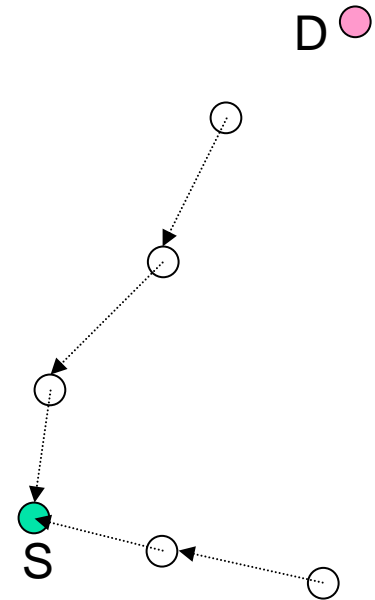
# AODV Path Discovery - Initiation

- Source node initiates path discovery
- Broadcast a route request (RREQ) to neighbors
- RREQ contains:
  - source\_addr,
  - source\_sequence\_#,
  - broadcast\_id,
  - dest\_addr, dest\_sequence\_#,
  - hop\_cnt



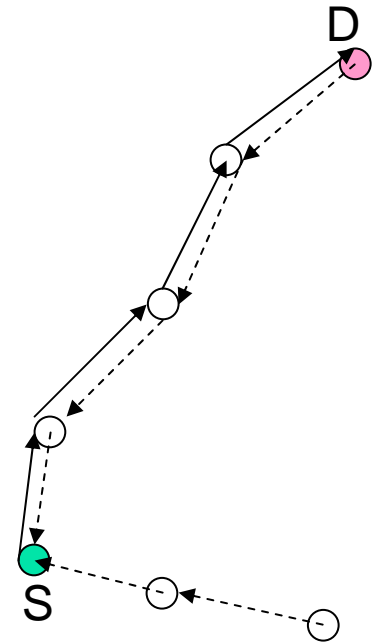
# AODV– Reverse Path Setup

- Reverse path is created automatically as RREQ travels to the destination.
- When RREQ is received, intermediate node records the address of the last hop.
- Expires after a period



# AODV– Forward Path Setup

- Destination or a node that has a route to the destination will send reply to source.
  - Compare dest\_sequence\_#
- Route Reply Packet (RREP)
  - <source\_addr, dest\_addr, dest\_sequence\_#, hop\_cnt, lifetime>
- Intermediate node sets up a forward pointer to the last hop of RREP





# AODV – Routing table

---

- Each routing table mainly contains :
  - Destination
  - Next hop
  - Number of hops (metrics)
  - Destination Sequence Number



# AODV - Path Maintenance

---

- Source moves
  - reinitiate the route discovery
- Destination or intermediate node move
  - special RREP to notify affected nodes
- Next hop becomes unreachable
  - RREP with  $\text{hop\_cnt} = \infty$
  - Source reinitiate a route discovery



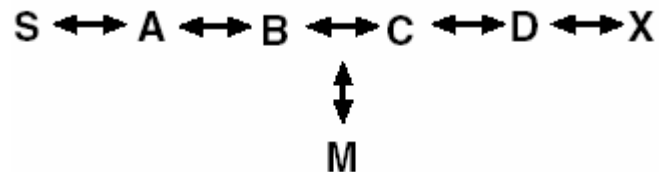
# Security Concerns

---

- Existing protocols (AODV, DSR) are vulnerable
- Attacks using
  - Modification
  - Impersonation
  - Fabrication

# Attacks using modification – False Sequence number

- AODV relies on `dest_sequence_num`
- 'M' advertises false sequence number



- All traffic to X now goes through M
- Time to correct: depends on the sequence num chosen by M



# Attacks using modification –

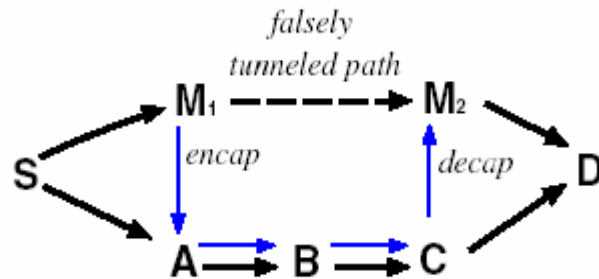
## False hop counts, False source routes

---

- AODV chooses route with least hop count
  - Malicious nodes can set hop count to zero
    - increases the chance that they are included
- DSR uses source routes in data packets
  - Can lead to DoS

# Attacks using modification – Tunneling

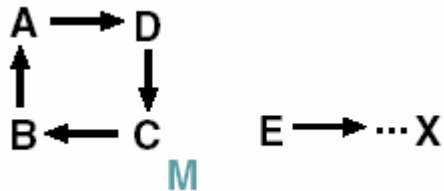
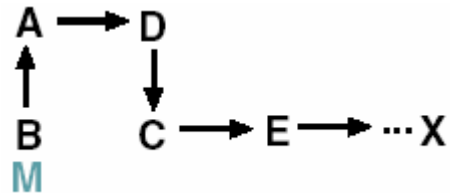
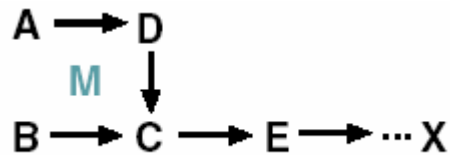
- Two/more nodes collaborate to exchange messages along the route
  - Spoofs path lengths – an important routing metric



- Exchange of messages destined for D

# Attacks using Impersonation

- Loops by spoofing
  - AODV/DSR are loop-free protocols
  - 'M' changes its MAC address

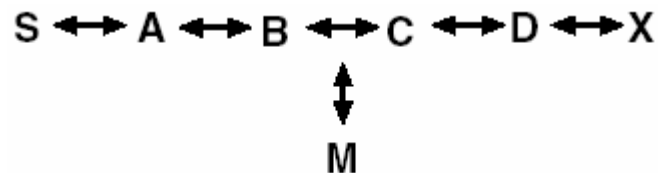




# Attacks using Fabrication

---

- Fabrication: false routing messages
  - Spoofing RERR messages



- DSR route cache corruption



# Enter ARAN...

---

- **A**uthenticated **R**outing for **A**d-hoc **N**etworks [2]
  - Uses cryptographic certificates
  - Exists as part of one-hop 802.11 networks
- Requires trusted certificate server T
  - Each node A gets a certificate from T after authentication

$$T \rightarrow A : \text{cert}_A = [IP_A, K_{A+}, t, e]K_{T-}$$



# Authenticated route discovery

---

- Source,  $A$ , broadcasts Route Discovery Packet (RDP)

$A \rightarrow \text{brdcast} : [\text{RDP}, \text{IP}_X, \text{cert}_A, N_A, t]_{K_A}$

- $N_A$  is monotonically increasing for each new RDP,  $t$  is timestamp
  - No hop count
- When node receives RDP
  - Sets up reverse path



## Authenticated route discovery - II

---

- Validates A's certificate
- Checks to see if  $(N_A, IP_A)$  is not processed already
- Broadcasts:

$B \rightarrow \text{brdcast} : [[\text{RDP}, IP_X, \text{cert}_A, N_A, t]K_{A-}]K_{B-}, \text{cert}_B$

- Thus creates complete authenticated path



# Authenticated route setup

---

- No shortest path
  - Considers only fastest path
- REP packet, X sends to D:

$X \rightarrow D : [\text{REP}, \text{IP}_a, \text{cert}_x, N_A, t]K_{X-}$

- Nodes forward back to the predecessor knowing reverse path
  - Each node verifies  $\text{cert}_x$ , signs and appends certificate

$D \rightarrow C : [[\text{REP}, \text{IP}_a, \text{cert}_x, N_A, t]K_{X-}]K_{D-}, \text{cert}_D$

- C stores the info that it should forward packet to D to reach X (is known from reverse path info too)



# Note about errors

---

- Routes expire after certain time
- ERR generated is also signed. Packet also contains
  - source and destination IP
- ERR cannot be spoofed, but difficult to detect genuine ERR messages
  - Non-repudiation helps to eliminate 'M' nodes over time

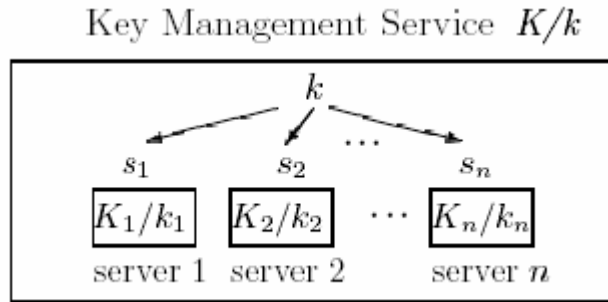


# Keys

---

- Protocol assumes trusted certificate server T
- Certificates issued and revoked by T
  - Revoke request is broadcast
- Multiple redundant authorities can be used [3]
  - Uses a key management service

# Keys - II



- $(n, t+1)$ , where there are 'n' servers and CA is stable until 't' servers are compromised
- Distribution of trust among 'n' servers is achieved through threshold cryptography



# Attacks solved by ARAN

---

- Unauthorized participation
- Spoofed route signaling
  - Prevents impersonation attacks
- Fabricated routing messages
  - Though not completely prevented, protocol offers non-repudiation
- Alteration of routing messages
  - Initial packet sent by source(RDP)/ destination(REP) cannot be changed by the intermediate nodes



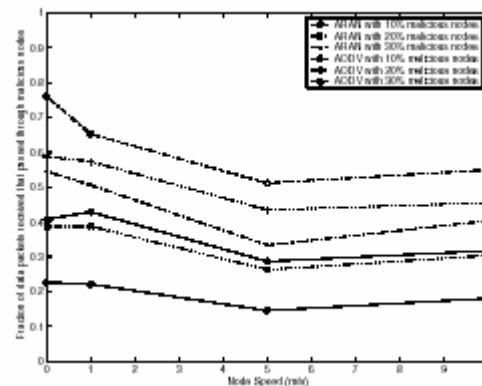
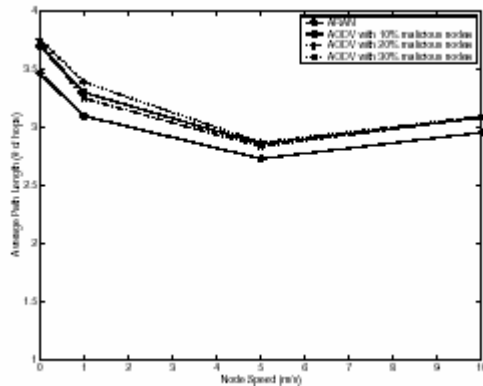
# Comparison

<i>Attack</i>	AODV	DSR	ARAN
Remote redirection			
modif. of seq. numbers	Yes	No	No
modif. of hop counts	Yes	No	No
modif. of source routes	No	Yes	No
tunneling	Yes	Yes	Yes, but only to lengthen path
Spoofing	Yes	Yes	No
Fabrication			
fabr. of error messages	Yes	Yes	Yes, but non-repudiable
fabr. of source routes (cache poisoning)	No	Yes	No

- ARAN is secure, but:
  - Requires CA
  - Computationally intensive – slower route discovery, larger packet size (greater routing load)
  - Not sure how it'll scale for less powerful wireless devices

# Some performance metrics... [2]

- ARAN simulation using 802.11 MAC, constant bit rate over UDP
- With malicious nodes 'M' altering path lengths; traffic through 'M's





# Summary

---

- Wireless Ad-hoc is still an active area for research – many aspects of security need to be addressed
  - Secure routing
  - Key management, Multicast security
- Found similar literature for secure routing
- As per IETF, experimental RFCs for AODV/DSR done
  - Nothing yet concrete on secure routing



# References

---

- [1] Perkins C.E. and Royer E.M. , "Ad-hoc On-Demand Distance Vector Routing,"  
Second IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, February 1999
  
- [2] Sanzgiri K, Dahill B, Levine B.N and Belding-Royer E.M, "A secure routing protocol for Ad-hoc networks," Proc. Of IEEE ICNP, 2002
  
- [3] Zhou L. and Haas Z.J, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, 1999