

# Performance Evaluation of Security-Aware Routing Protocols for Clustered Mobile Ad Hoc Networks

**Gregory S. Yovanof - Kerem Ericsi**  
**Athens Information Technology**

Tel: +30 210 668 2772 Email: [gyov@ait.edu.gr](mailto:gyov@ait.edu.gr)

Int'l Workshop on Wireless Ad-Hoc Networks IWWAN'04, Oulu, Finland  
*1 June 2004*



# Outline

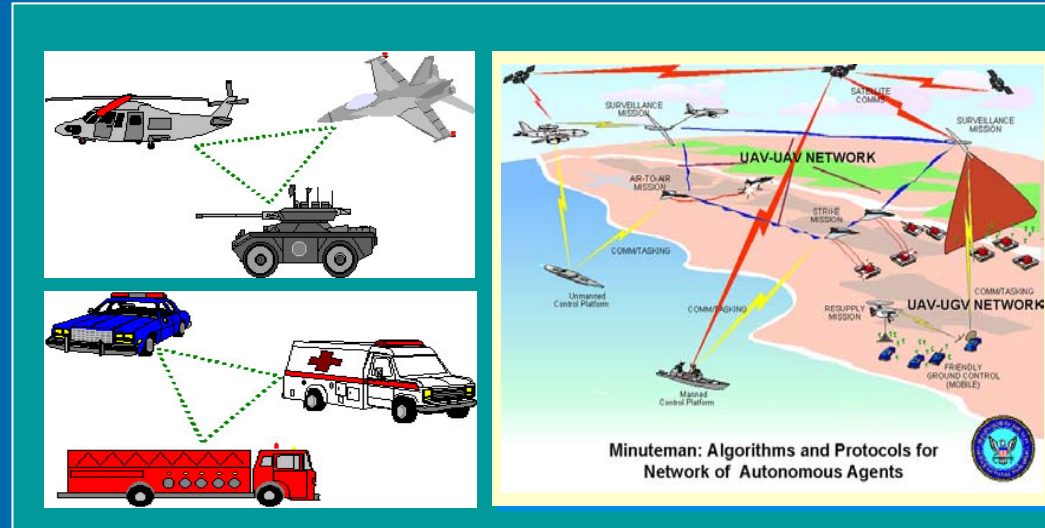
- Hierarchical Clustered Mobile Networks
- Secure Routing Protocols
  - Proactive (SEAD) vs. Reactive (ARIADNE) schemes
- System Design Parameters
  - Multimedia Data, Session Link, Motion Model
- Routing Protocol Performance Evaluation
  - Proactive vs. Reactive Schemes
  - Incremental Overhead due to Security Extensions
  - Effect of Queuing Buffer Size
- Conclusion



# Hierarchical Clustered Ad-Hoc Networks

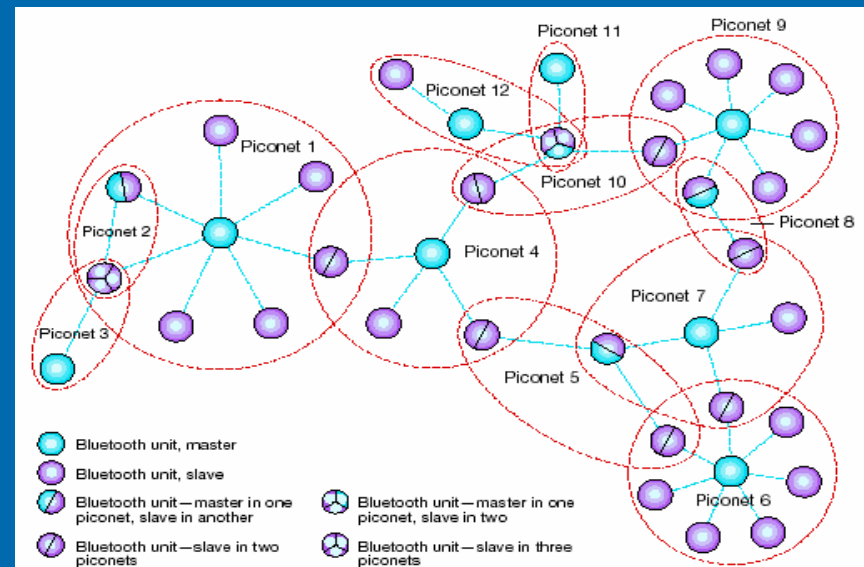
## 1) Heterogeneous (Non-Uniform) Hierarchical Clustered Mobile Nets

- Battle-field Communications
- Emergency and/or Rescue Operations



## 2) Homogeneous (Uniform) Hierarchical Clustered Mobile Networks

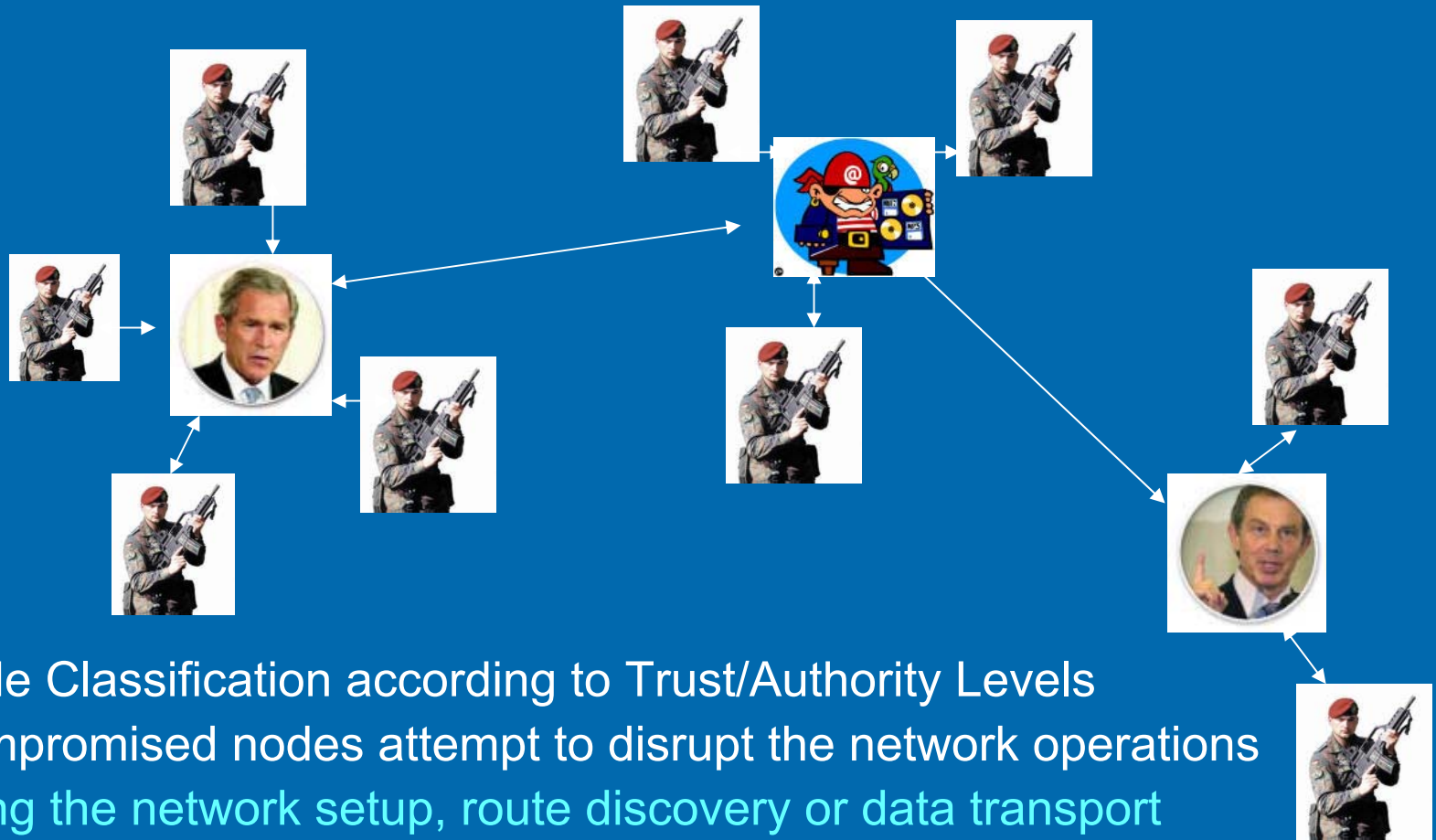
- Bluetooth scatternets
- Multihop Relay-Networks
- Nomadic computing





# Need for Secure Routing

- Security support is of grave importance to Military Communications



- Node Classification according to Trust/Authority Levels
- Compromised nodes attempt to disrupt the network operations (during the network setup, route discovery or data transport phases, e.g., packet littering, net partitioning, DoS attacks, etc)



# Prior Work – Our Contribution

- J. Broch, D. Maltz, Johnson et al. “Performance Comparison of Multihop Routing” MobiCom’98
  - No Secure Routing Schemes
- Hu, Perrig and Johnson, “ARIADNE ...” MobiCom’02, and “SEAD...” June 2002
  - Flat Network Topology, No Group Mobility
- **Our Contribution: Performance Evaluation of Security Aware Routing Protocols in the following scenario**
  - Clustered Mobile Network
  - Group Mobility - Reference Point Group Mobility (RPGM) Model
  - Session Level Link Formation Through Cluster-Heads
  - Security Aware Routing Protocols (SEAD and ARIADNE)
  - Multimedia Data: Delay-sensitive real-time data traffic



# Proactive vs. Reactive Routing Protocols

## ➤ Proactive:

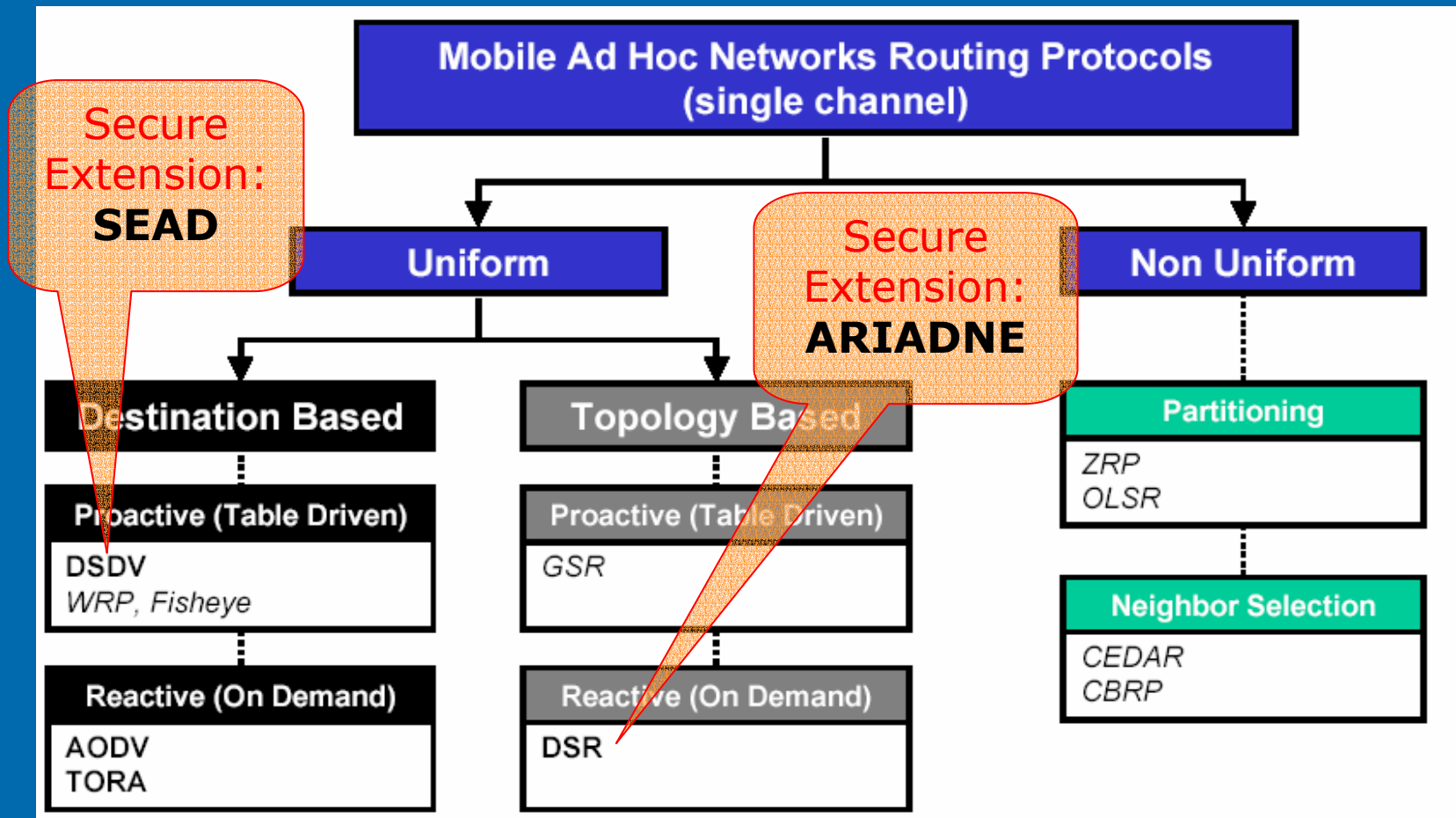
- Actively pursue route updates to destinations, even when route is not used
  - + Reduced communication latency
  - More overhead

## ➤ Reactive:

- Discover routes to destinations only when needed
  - + Less overhead
  - Increased latency



# Ad Hoc Routing Protocols Classification





# Proactive Protocol: DSDV

- DSDV – **Destination Sequenced Distance Vector**: Proactive scheme (table-driven)
- Uniform – No Hierarchical structure
  - Each node sends/responds to a routing message the same way
- A **routing table** is maintained at each node containing entries for all destinations:
  - **Next Hop**: the next intermediate node towards the destination
  - **Metric**: how many hops to reach the destination
  - **Sequence Number**: when this route was advertised
- Every node periodically broadcasts the state of its routing table
  - Periodic update interval: Tradeoff between latency of routing info and excessive communication overhead



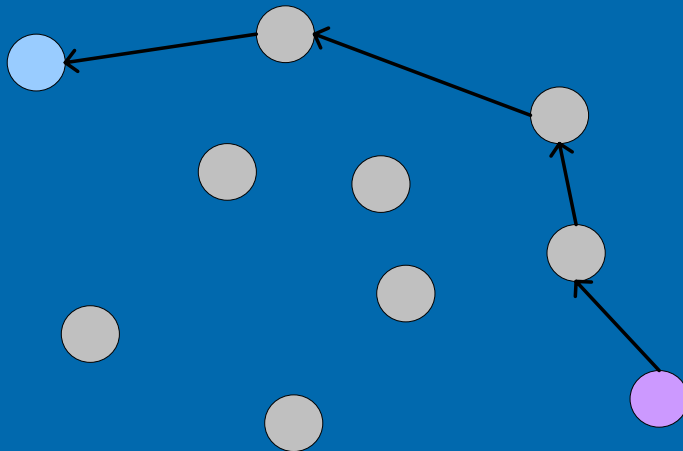
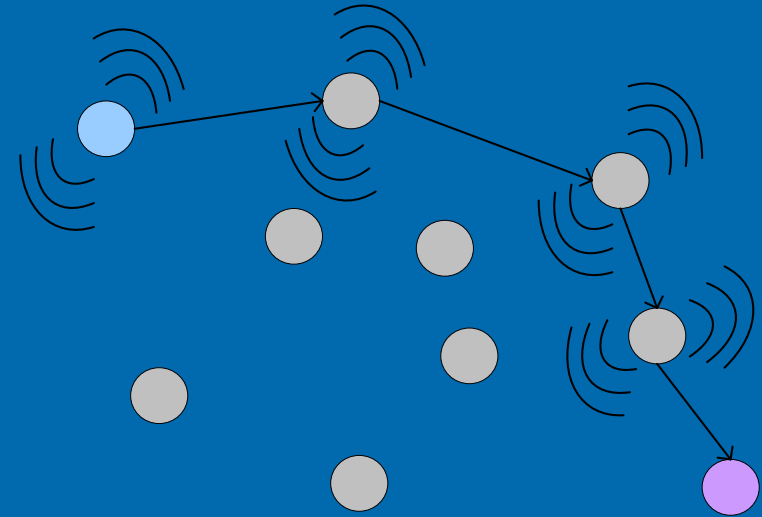
# SEAD – Secure Efficient Distance Vector Routing Protocol

- SEAD is based on DSDV – Proactive (Table Driven)
  - Easy to implement and efficient in terms of required memory and CPU processing capacity
  - Improvements on the original DSDV protocol
- Uses efficient one-way Hash Function but no symmetric key cryptography
  - Built in one-way hash function  $H:\{0,1\}^* \rightarrow \{0,1\}^p$
  - Simple to compute but infeasible to invert
- Robust against multiple uncoordinated attackers creating incorrect routing state
- Guards against DoS (Denial-of-Service)



# Reactive Protocol: DSR

- Dynamic Source Routing (DSR):  
On Demand (Reactive)
- If destination is unknown, the network is flooded with requests
- A node receiving the request re-broadcasts it
- Node address is appended to request



- Once destination is found, it replies through the same path
- Found route is placed in a cache
- Multiple paths possible



# ARIADNE – Secure on Demand Routing

- On Demand (Reactive) - DSR based
- Source Routing better suited for Security Aware Routing
  - Sender is able to authenticate every node in the route-reply phase - ensuring trustworthiness of entire route
- ARIADNE uses TESLA: an efficient **Broadcast Authentication** protocol
- Prevents large number of Denial-of-Service (DoS) type attacks
- ARIADNE is efficient, using only highly efficient **symmetric cryptographic** primitives



# Route Discovery (ARIADNE/TESLA)

Route Discovery

$$M = \langle \text{Request}, S, D, id, ti \rangle$$

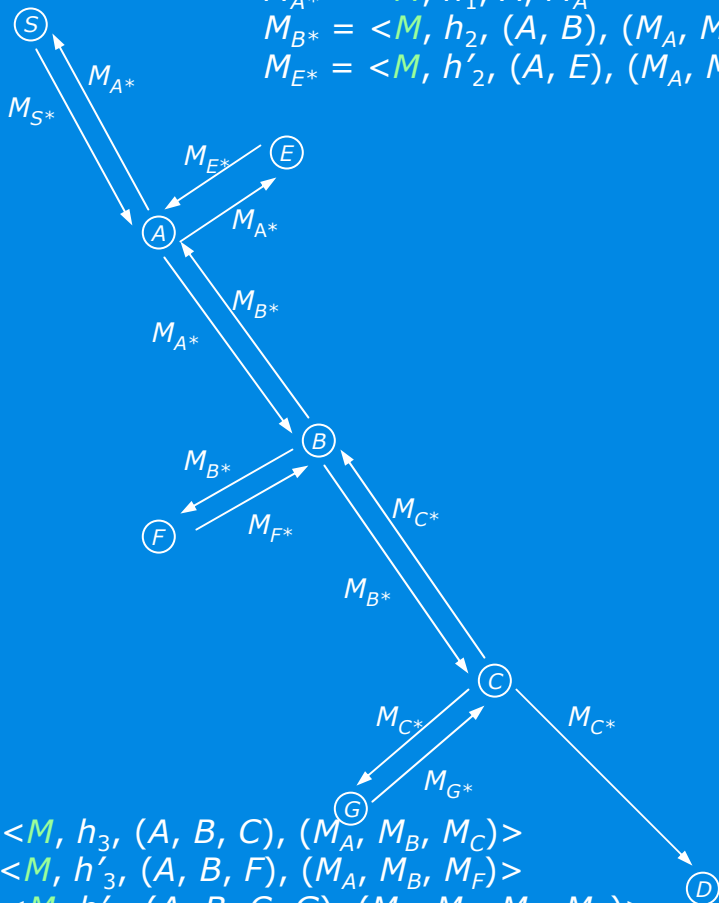
Route Request

$$M_{S^*} = \langle M, h_0 \rangle$$

$$M_{A^*} = \langle M, h_1, A, M_A \rangle$$

$$M_{B^*} = \langle M, h_2, (A, B), (M_A, M_B) \rangle$$

$$M_{E^*} = \langle M, h'_2, (A, E), (M_A, M_E) \rangle$$



$$M_{C^*} = \langle M, h_3, (A, B, C), (M_A, M_B, M_C) \rangle$$

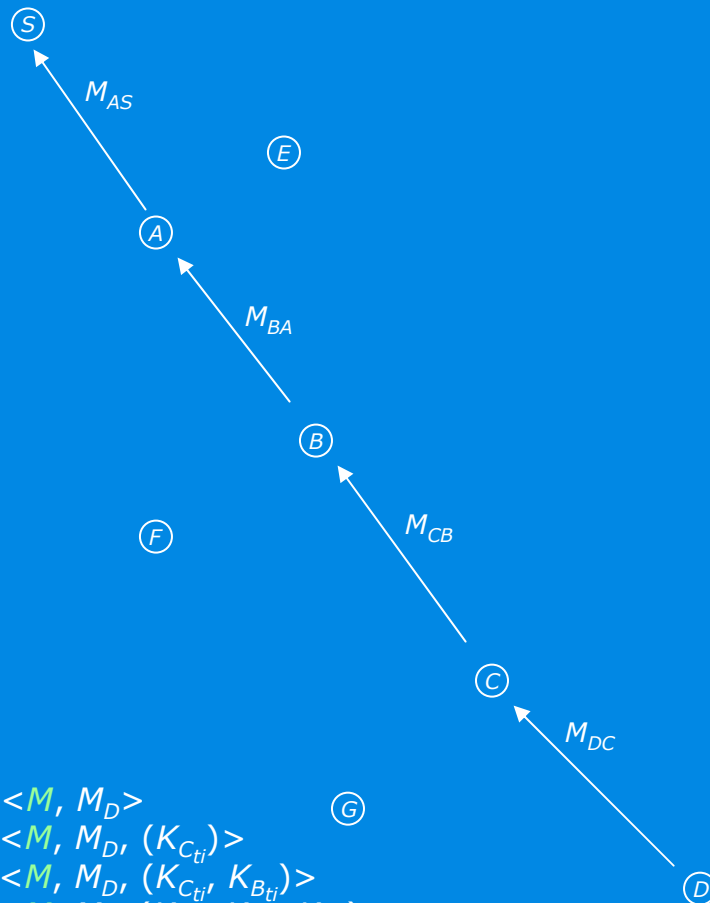
$$M_{F^*} = \langle M, h'_3, (A, B, F), (M_A, M_B, M_F) \rangle$$

$$M_{G^*} = \langle M, h'_4, (A, B, C, G), (M_A, M_B, M_C, M_G) \rangle$$

Route Discovery

$$M = \langle \text{Reply}, D, S, ti, (A, B, C), (M_A, M_B, M_C) \rangle$$

Route Reply



$$M_{DC} = \langle M, M_D \rangle$$

$$M_{CB} = \langle M, M_D, (K_{C_{ti}}) \rangle$$

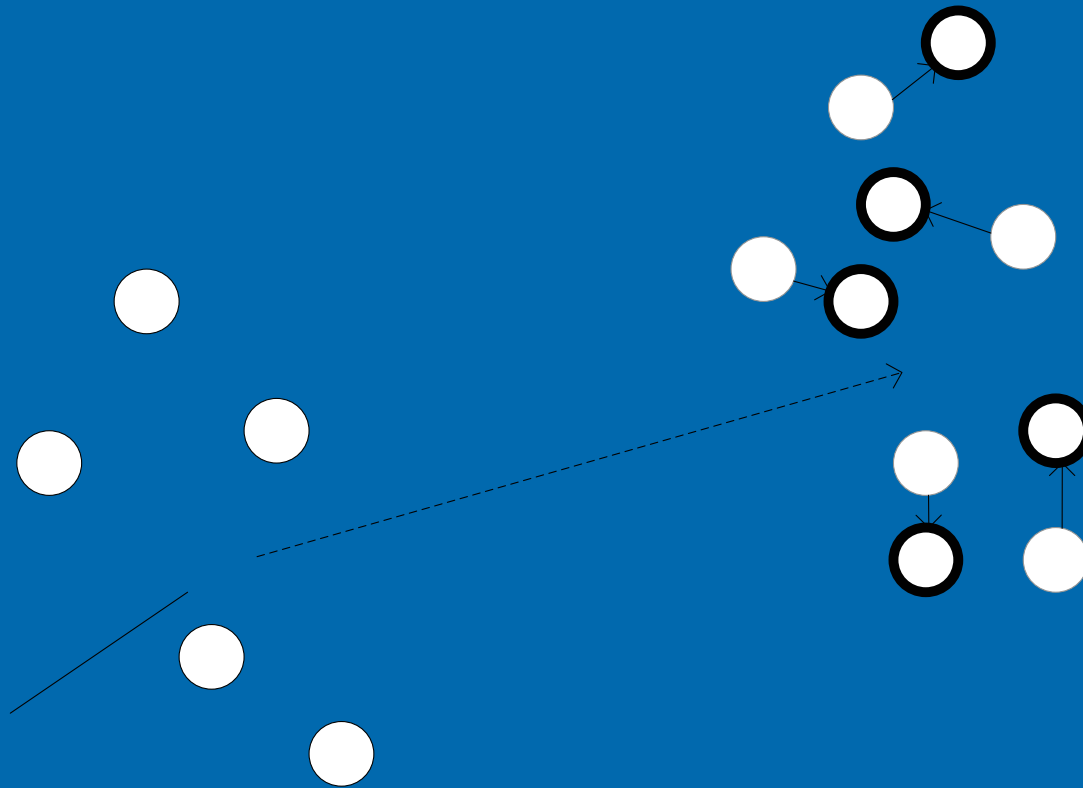
$$M_{BA} = \langle M, M_D, (K_{C_{ti}}, K_{B_{ti}}) \rangle$$

$$M_{AS} = \langle M, M_D, (K_{C_{ti}}, K_{B_{ti}}, K_{A_{ti}}) \rangle$$



# RPGM Movement Model

- Reference Point Group Mobility (RPGM) Model

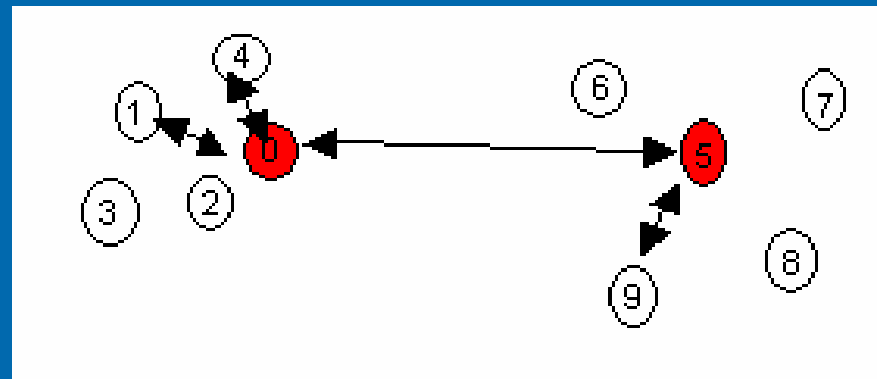


- Node motion is sum of two vectors: Group Vector GM - Individual Vector RM (GM is the dominant one)
- At each intermediate location the Group waits for Pause Time then selects random destination and starts to move again



# Session Level Link Formation

- At the Session Layer traffic flows are formed to emulate CGSR (Common Gateway Switch Routing) traffic patterns
  - Similar to Data Traffic flows in Bluetooth Scatternets
  - Fits Logical Hierarchy imposed by Military structure
- A single node is elected to serve as the **Cluster-Head** within each Cluster
- Traffic is routed through Cluster-Heads
- Cluster members cannot talk directly to each other
- Deviation from Flat Routing



Communication from node 4 to 9:  
**Session-Link**  $4 > 0 > 5 > 9$

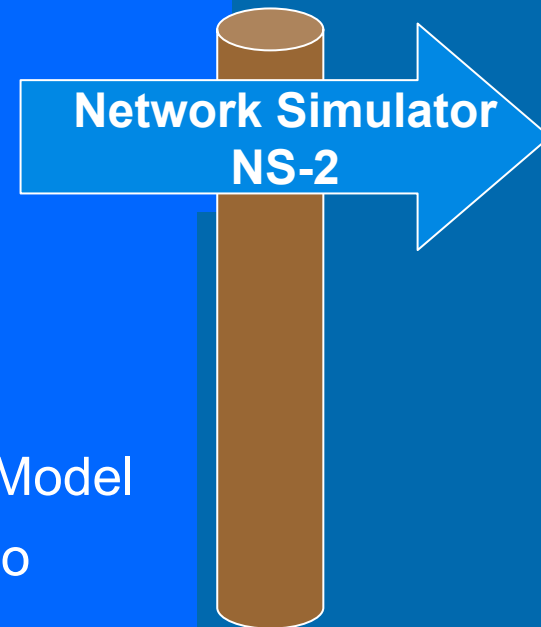
Communication from node 0 to 5:  
**Session-Link**  $0 > 5$



# Design Parameters - Simulation

## *Examined Protocols:*

- ➤ DSDV - SEAD
- ➤ DSR - ARIADNE
- Lucent waveLAN DSSSS
  - Tx power: 24.5 dBm
  - Rx threshold: -94.4dBm
  - Two-ray Ground Reflection Radio Propagation Model
- Movement model: RPGM
  - variable pause times
- Simulation Time: 500 seconds





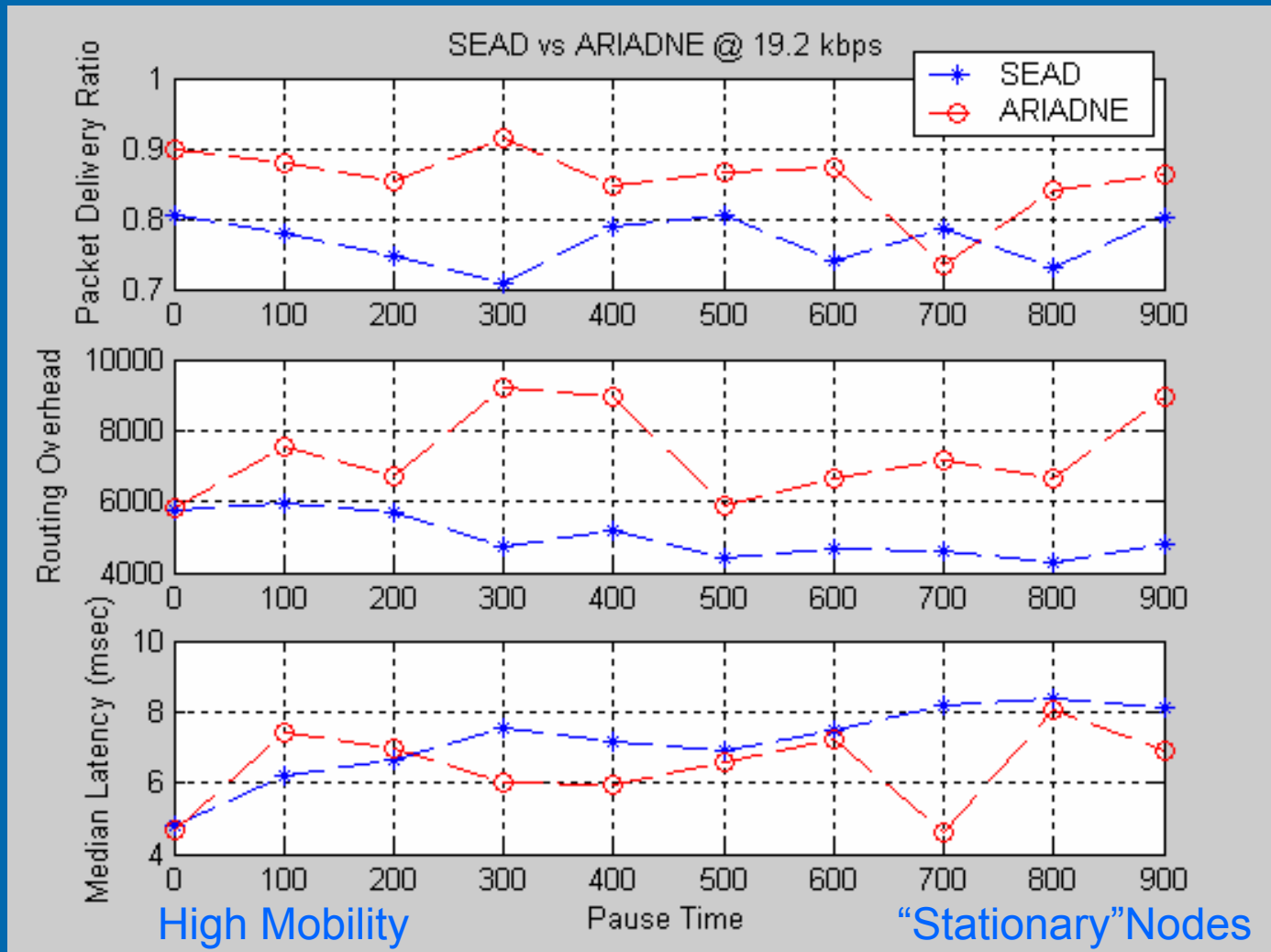
# Performance Metrics

- **Packet Delivery Ratio (PDR)**
  - Packets sent / Packets received, [%]
- **Median Latency (ML)**
  - Packet end-to-end Delay, [seconds]
- **Routing Overhead (RO)**
  - Total routing traffic generated, [bytes]
- **Target values for Real-time Interactive Multimedia Traffic**
  - PDR better than 75%
  - One-way, end-to-end Delay up to 250-300 msec



# SEAD vs ARIADNE @ 19.2 Kbps

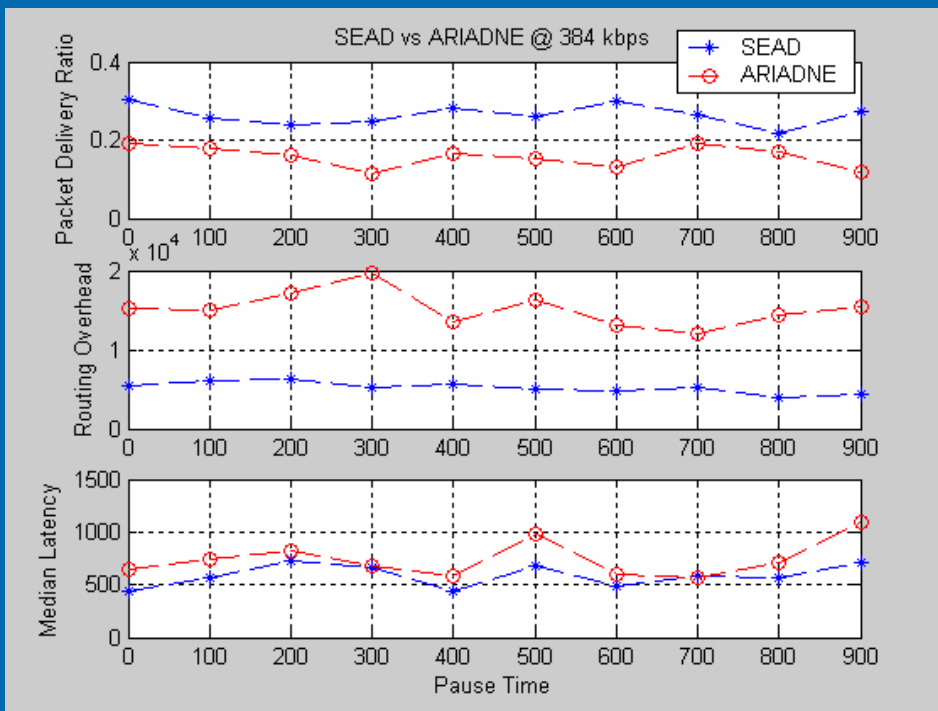
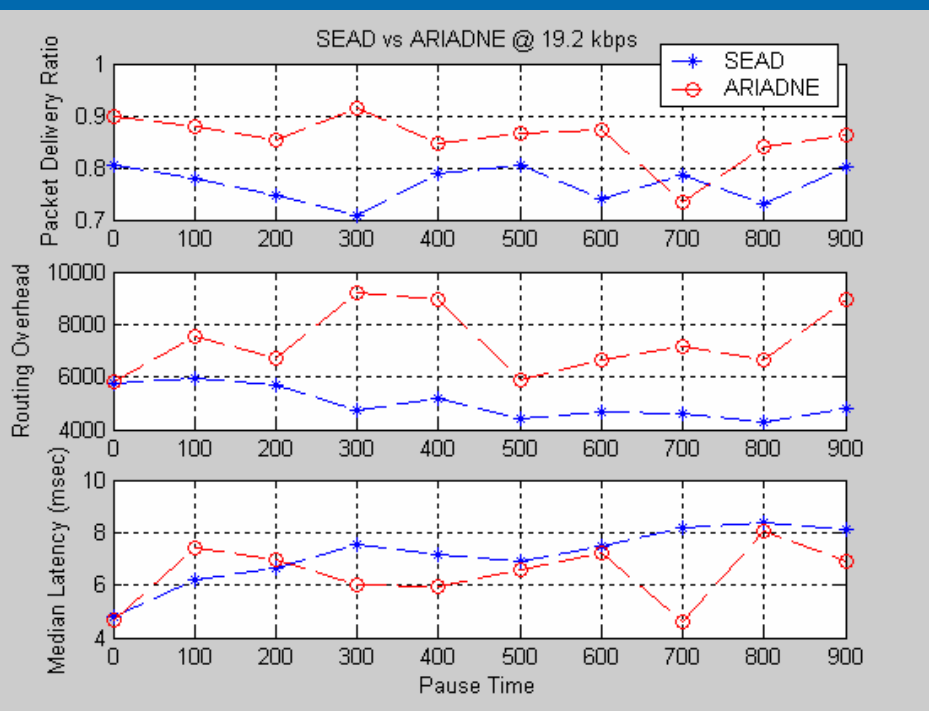
- ARIADNE (reactive) outperforms SEAD @ 19.2 kbps
  - More than 70% PDR, Low Overhead, 5-8 msec Latency





# SEAD vs ARIADNE @ 384 Kbps

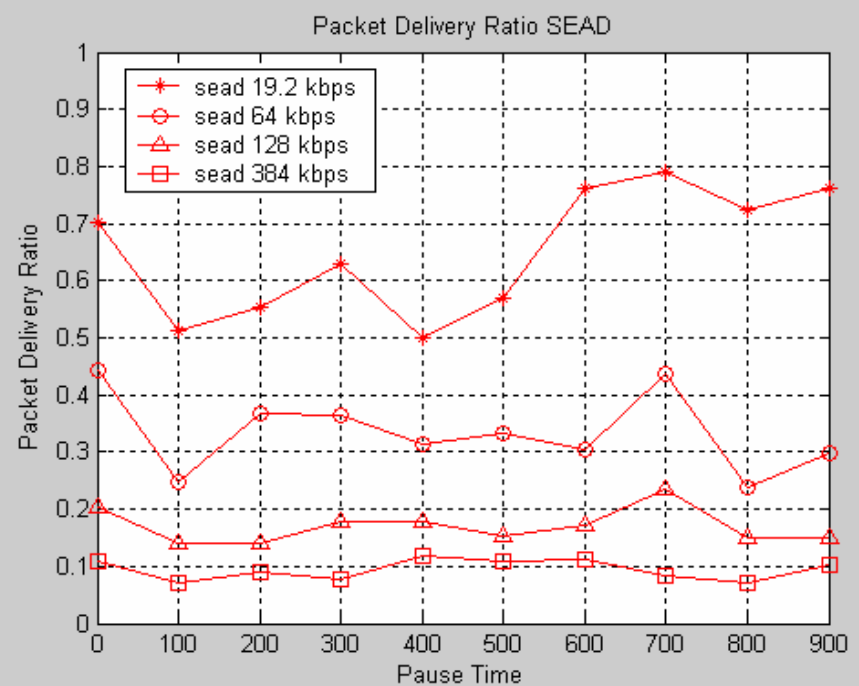
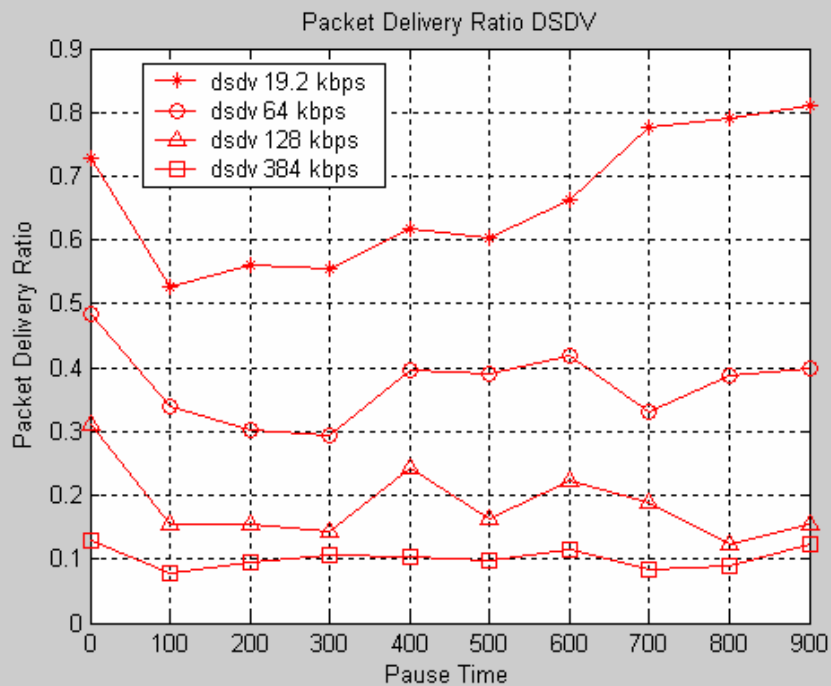
- Protocol behavior changes with the data rate
- SEAD (proactive) outperforms ARIADNE @ 384kbps, but:
  - Very Low PDR (20-30%), Unacceptable Latency (~500msec)
  - Fails to Accommodate Real-time Multimedia Traffic
  - Could that be due to the incremental overhead induced by the Security Extensions?





# DSDV vs SEAD - PDR

- Both DSDV and SEAD exhibit similar performance w.r.t. Packet Delivery Ratio over the entire range of Pause times and Data Rates
- SEAD slightly better only at 384 kbps
- Acceptable PDR levels (>70%) achieved only at 19.2 kbps and in the case of low mobility

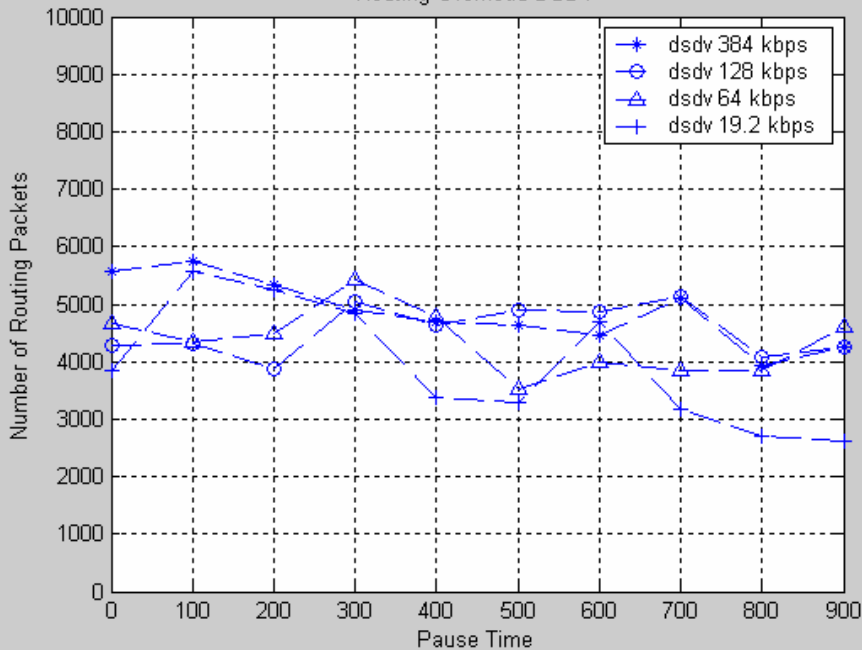




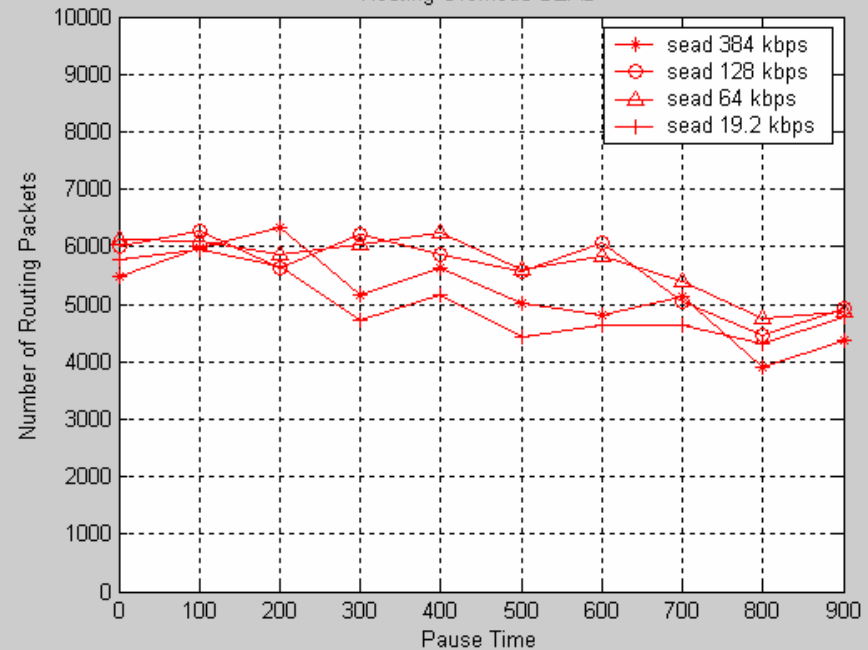
# DSDV vs SEAD - RO

- Routing Overhead is insensitive to traffic load (proactive scheme)
- SEAD exhibits slightly higher RO
  - Due to an optimization feature of SEAD that discards weighted settling time (more routing packets hence more overhead)

Routing Overhead DSDV



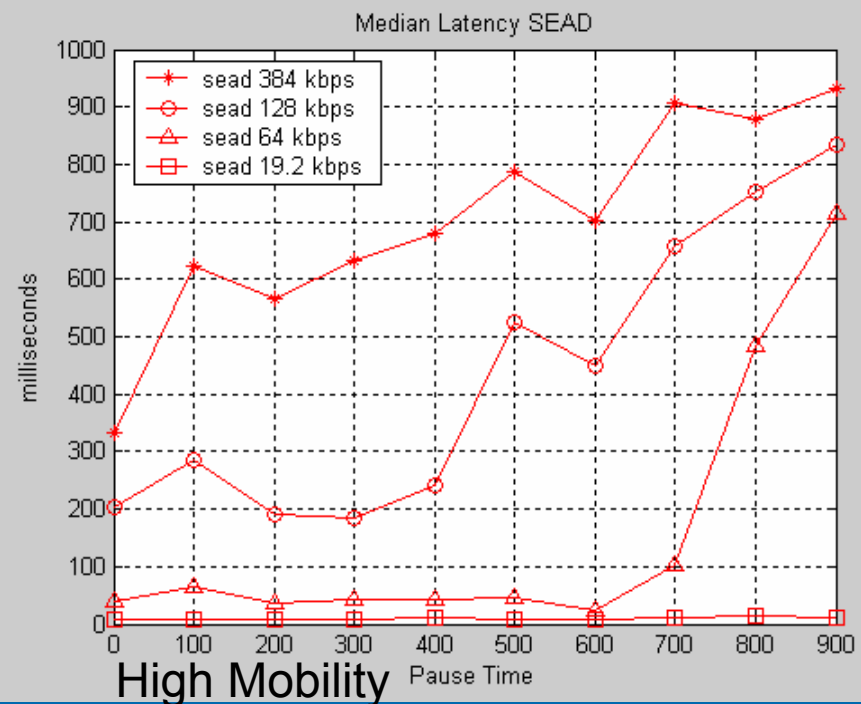
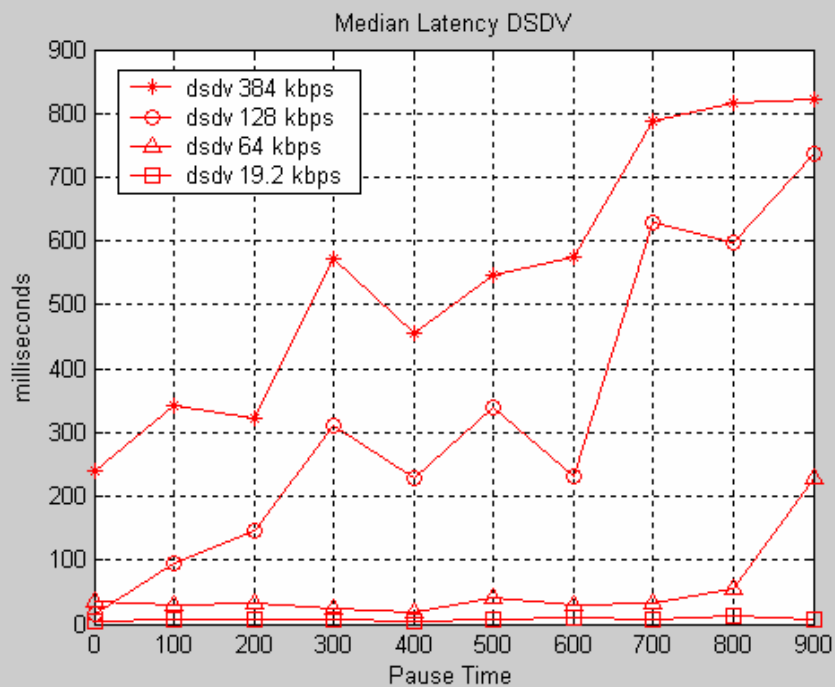
Routing Overhead SEAD





# DSDV vs SEAD - ML

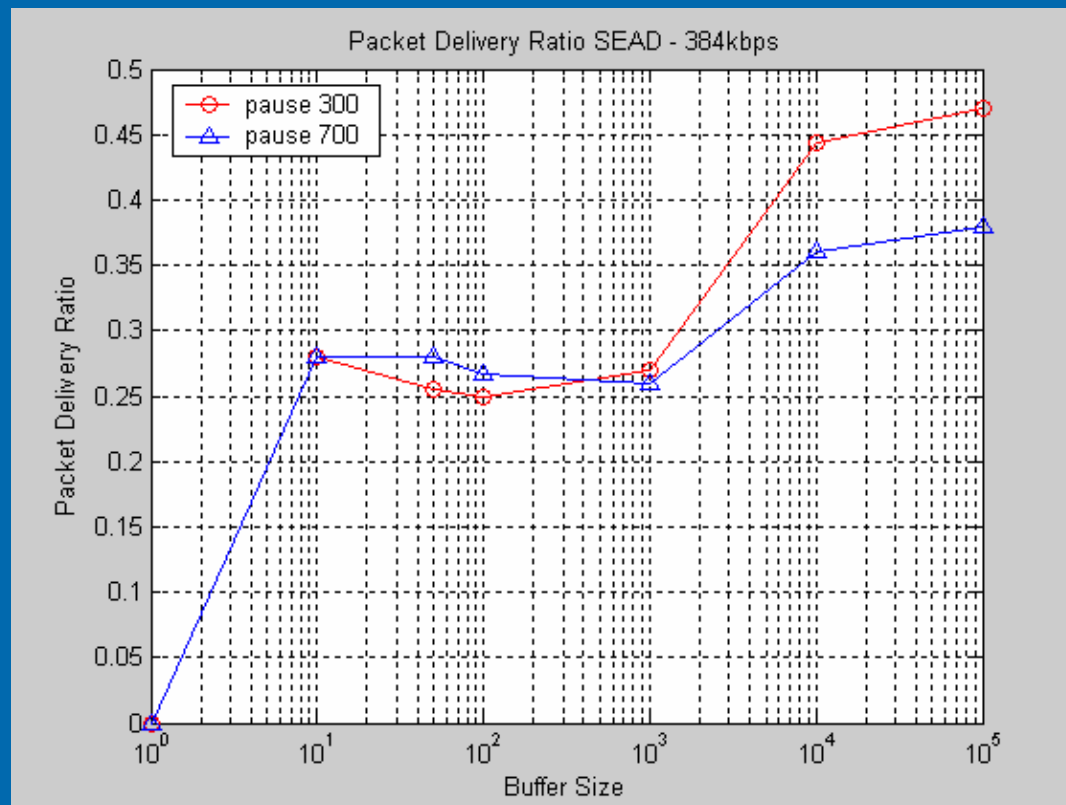
- SEAD exhibits overall longer ML than DSDV
- Median Latency better in High Mobility
  - Acceptable ML levels for up to a data rate of 128 kbps





# Impact of Buffer Size on SEAD - PDR

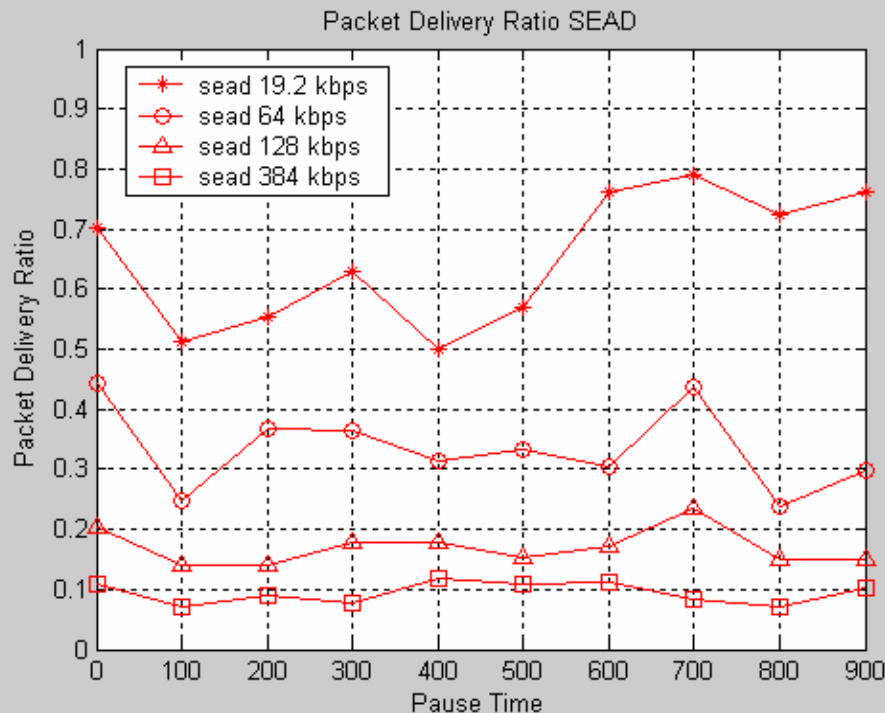
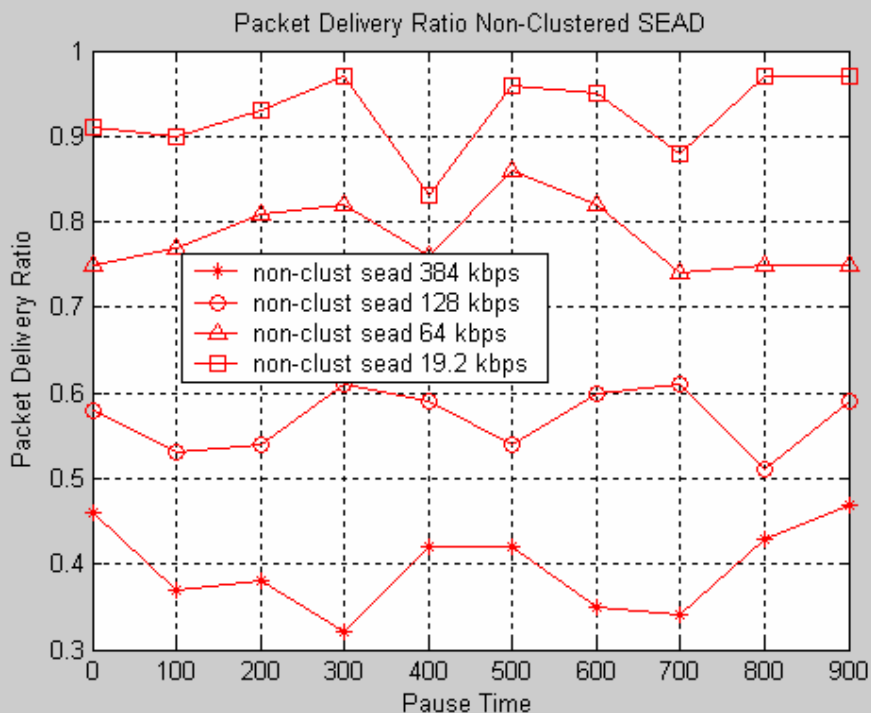
- For a wide range of values varying the size of the Queuing Buffer has a minimal effect on the Packet Delivery Ratio
  - Default Buffer size in ns-2: 50 pckts/buffer





# How Data-Flow Scenario Affects SEAD - PDR

- Flat topology. No Data-Flow constraints. Clusterheads are removed
  - Dramatic increase in Packet Delivery Ratios
  - Clusterheads are bottlenecks!





# Performance Summary

➤ No single winner ...

**Mobility**

72 Km/hr

*ARIADNE*  
*(reactive)*

*SEAD*  
*(proactive)*

*ARIADNE*

*SEAD*

19.2kbps

**64 kbps**

384 kbps

**Data Rate**

Acceptable  
Multimedia Performance



# Conclusion

- SEAD (proactive) performs better than ARIADNE at higher data load in the tested:
  - Clustered, Group Mobile and Constraint Traffic (Hierarchical) environment
- Minimal incremental overhead due to the Security extensions
- Both schemes fail to accommodate the stringent requirements of real-time interactive multimedia communications in the examined application scenario
- QoS constraints demand cross-layered optimized protocols (Hierarchical routing, Traffic/Resource driven cluster formation, Hot-spot mitigation, Load balancing ...)

# Thank You!

Q&A?

