Presentation by RC B

"Towards Resilient Security in WSN"
Yang, Ye, Yuan, Lu & Arbaugh, MobiHoc '05

Problems with Pairwise (Symmetric) Keys?

MAC?

what if a node join after Bootstrapping period?

Only the node being deployed need
master key.

En-Route Filtering of Malicious Messages (P eroski)?

How dense the network should be?
ScientificMerit?
- Didntcompare to Pairwise scheme
- Only simulation results?

Mobility is not supported.

Scalability?

How upperbound h' in Thm 2 was computed?

Contributions?
- Soln for Insider Attack.

What if nodes in cell fail (e.g. near sick)?
Feasible?

What is the Trust Model?  
Attack Model?

Applications?

Try to work out an example to illustrate the idea.