Secure Mobile UAV-MBN Network

Jiejun Kong, Kaixin Xu, Haiyun Luo, Daniel Lihui Gu, Mario Gerla, Songwu Lu

Challenges
† Current centralized solutions are incompatible with ad-hoc networks due to mobility, node failure and denial-of-service attack
† Provide a scalable and robust security solution for a potentially huge ad-hoc network with volatile members and heterogeneous mobile nodes

Fully Distributed Security Service
† Security services in mobile networks are supported at anywhere and anytime with a threshold based secret sharing mechanism
† Simple execution plan with one round-trip communication delay in each locality
† No single point of privilege and failure
† Works in very large mobile networks

Battle Ready Security for Multi-level UAV-MBN Mobile Networks
† Applicable to multi-level UAV-MBN network via damage control zone partitioning
† Capable of enemy identification
† Intra-zone and inter-zone security design
† Recursive SK-aggregation along the hierarchy
† Cascaded certification by routing gateways
† Secure zone composition in case of heavy battle loss

Implementation and Simulation
† Prototype implementation includes public key cryptosystem, Lagrange polynomial threshold secret sharing, and all novel algorithms doing fully distributed certificate renewal, self initialization, and proactive secret share update
† GloMoSim simulation on UAV-MBN network proves the solution is effective, scalable, and insensitive to mobility

UCLA CSD Network Research Laboratory
Supported by ONR’s MINUTEMAN project and NSF