2016

Enabling Secure Group Communications for UAV Swarms using Distributed Key Management

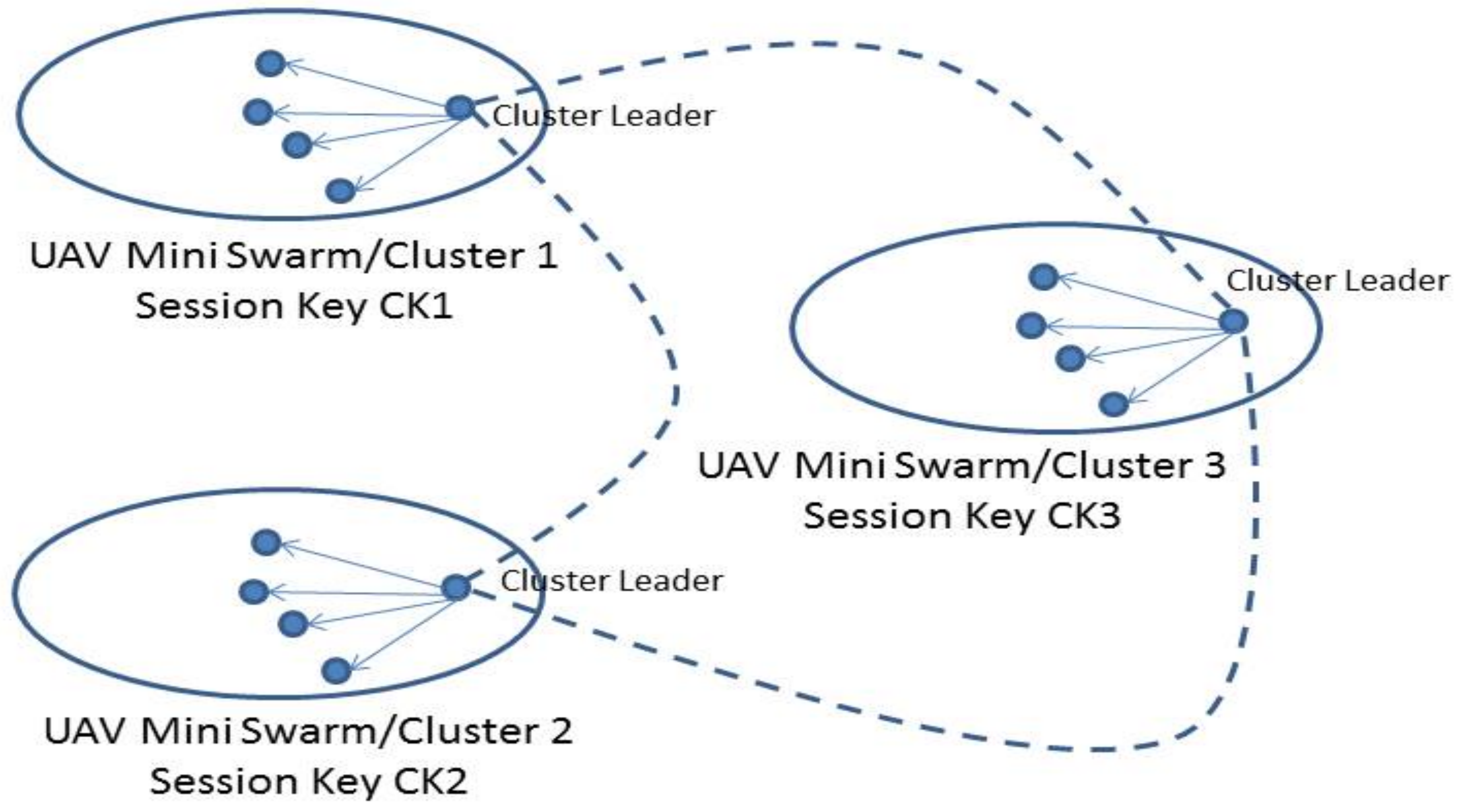
Thulasiraman, Preetha

Monterey, California: Naval Postgraduate School

http://hdl.handle.net/10945/57045

Enabling Secure Group Communications for UAV Swarms using Distributed Key Management

Naval Postgraduate School



A UAV swarm divided into mini swarms to facilitate security within group communications

- UAV swarm communications need security mechanisms.
- NSA has adopted the Advanced Encryption Standard (AES) as the cryptographic module for S/TS information.
- AES widely implemented because it is fast and has low ram requirements.
- AES needs key management protocol to facilitate key distribution and re-keying.
- UAVs swarms are cooperative and thus can be modeled using group communications protocols.
- Group Key Management (GKM) that is decentralized and can work in tandem with AES is necessary.

- GKM will be developed using dynamic K-means clustering algorithm.
- UAV swarm will be divided into K clusters with each cluster having a dynamically elected cluster leader (CL); all cluster members follow the CL.
- Each cluster leader generates a session key (CK) using the AES Pseudo Random Number Generator (PRNG) for encryption of data within the cluster.
- CL-X communicates to CL-Y as follows: 1) CL-X transmits CK-X to CL-Y; 2) CL-X transmits information to CL-Y which CL-Y decrypts using CK-X; 3) CL-Y encrypts data using CK-Y so that members within cluster X can decrypt information
- Rekeying only required within individual clusters when UAVs arrive or depart; only CK of one cluster is re-keyed as opposed to the whole network.

- Security is important in UAV swarm communications
- To this date very little work has been done on identifying feasible security algorithms for swarms.
- A straightforward encryption algorithm like AES combined with GKM will provide a stepping stone for further security research and collaboration
- This work will make an immediate impact by providing a preliminary solution to the lack of security in UAV deployment.
- This furthers the CRUSER mission
- Cybersecurity is an important research component at NPS and thus furthers the mission of the school, Navy and DoD.

CRUSER
Consortium for Robotics and Unmanned Systems Education and Research

Dr. Preetha Thulasiraman, PhD
Assistant Professor, ECE Dept
pthulas1@nps.edu, 831-656-3456