A Cost-Effective Simulation Testbed for Unmanned Aerial Vehicle Network Cyber Attack Analysis

Ahmad Javaid, Weiqing Sun, and Mansoor Alam

Safe & Secure Systems & Software Symposium (S5)
June 9-11, 2015
Background and Motivation

• UAVs
  – Unmanned Aerial Vehicles, more popularly known as Drones
    • being used extensively in Civilian, Military, Agriculture, Research
  – United States being the top manufacturer/user

• Recent Cyber Attacks Against UAVs
  – 2009 - Tapping of video-feed of a UAV by terrorist organizations using $21 Russian developed software called “SkyGrabber” which was meant for tapping free Satellite video feeds.
    • No encryption
  – 2010 – Mexican Drone (Israeli made) crashes in an El Paso backyard
    • No idea why it was flying in US Airspace
  – 2011, October - A “Keystroke” virus affecting control programs of US Predator and Reaper Drones
Background and Motivation

- **Security of UAVs urgent and important**
  - Attacks against UAVs are on the rise
  - Impact of losing control can be catastrophic

- **Cost-effective testbed needed to facilitate research in this area**
  - Unavailability of effective software based simulation testbed
  - Time sensitive nature of UAV Systems
  - Communication plays an important role in information transmission
Related Work

• Single UAV simulation
  - Visual simulator based on Matlab/Simulink and FlightGear
  - Some GUI based simulators were designed
    • Using actual hardware to mimic real UAVs
    • Using a right-angle robot to mimic an unmanned vehicle
  - Another work used JSBSim and FlightGear for finding vulnerabilities of the auto-pilot system.

• UAV Swarms simulation
  - LaBRI involves deployment of actual UAVs on a field for specific applications and check their survivability
  - SPEEDES (Synchronous Parallel Environment for Emulation and Discrete Event Simulation) - simulates a swarm of UAV on a high performance parallel computer
  - C3UV (Center for Collaborative Control of Unmanned Vehicles) - focuses on the fact that information acquisition through collaborative sensing and control are highly coupled
UAV Testbed Requirements

- Support various UAV models (including those developed from other sources)
- Support UAV network communication simulation
- Support attack and defense simulation
- Provide interactive GUI for users to control their experiments
- Provide users intuitive analysis results
Our Approach

- **UAVSim:**
  - Simulates UAVNet (UAV Network) based on OMNeT++
  - Incorporates UAV modeling
  - Develops attack library
  - Provides results analysis
  - Provides experimentation control through GUI
Design and Implementation

UAVSim
- Attack Library
  - Jamming Attack
  - DoS Attack
- UAV Network Module
- UAV Model Library
- Graphical User Interface
- Result Analysis Module
- UAV Model Browser
- Attack Hosts
  - UAV Host
    - Mobile Attack Host
    - Fixed Attack Host
    - Basic Model
    - Advanced Model
OMNeT++

- Freeware, open source
- Modular, uses C++ and NED
- Simulate network characteristics
- Additional module INET 2.0
  - Provides mobility, radio propagation, etc.
  - Wireless network simulation
- Multiple Node simulation
- Visual traffic animation
- Results
  - can be stored in log or separate files
  - can be used for result analysis using inbuilt Scave
UAV Communication Network Modeling

LOS Link
Ku Band, 1.5-50 Mbps
Satellite

UAV1
UAV2
UAV3

C-Band, 0.5-10 Mbps
BLOS Link

HQ Ground Control Station

LOS Link, 2-10 Mbps
Local Ground Control Station

Portable Ground Control Station

UAV4

LOS Link

Local Ground Control Station

HQ Ground Control Station
Security Threat Modeling and Attack Library

Confidentiality
- Attacks compromising Confidentiality

Integrity
- Attacks compromising Integrity

Availability
- Communication Interruption

Malicious Attacks
- Jamming
- DoS/DDoS

Unintended/Natural Events
- Falsifying Control Signal/Commands
- Spoofing/Smurfing
- Buffer Overflow
- Flooding
- UDP
- SYN
- ICMP
- Ping
Security Threat Modeling and Attack Library

Security
- Confidentiality
  - Attacks compromising Confidentiality
- Integrity
  - Attacks compromising Integrity
- Availability
  - Communication Interruption
- Malicious Attacks
  - Jamming
  - DoS/DDoS
- Unintended/Natural Events
  - Falsifying Control Signal/Commands
    - Buffer Overflow
    - Flooding
    - Spoofing/Smurfing
    - UDP
    - SYN
    - ICMP
    - Ping
Attack Selection

• **Availability attacks**
  – High resource consumption attacks

• **Confidentiality and Integrity attacks**
  – usually require low resources

• **Selected attack types**
  – Single Target
    • DDoS
    • GPS Spoofing
  – Multiple Target
    • Total Signal Jamming
    • Selective Jamming (GPS)
**Attack Anatomy**

- **DDoS**
  - Network Congestion for a single node
  - Buffer overflow, Flooding, etc.
  - Frequent requests resulting in ~100% packet drop
  - PING, SYN, etc can be used
  - Attack hosts indistinguishable from UAVs
    - Same IP range
  - Number of attack hosts varied to vary impact
  - Success in less than 2 seconds – 99.99% loss
  - Single frequency band used
Attack Anatomy

• **Signal Jamming**
  – Network Congestion for all nodes
  – Random noise and pulse transmission
  – All UAVs in the area affected
  – Signal transmitted to all hosts in round-robin
    • framework limitation
  – Multiple frequency bands used
  – Success in less than 5 seconds – 90+% average loss
  – High resource consumption attack
GUI

Parameter Definition (Values shown are Defaults)

- Attack: DOS
- Maximum Transmission Range (mW): 10
- Attack host Transmission Range: 0
- UAV Host Transmission Range: 5
- Mobility Model: LinearMobility
- Attack host packet interval: 0.0001
- Channel Bitrate (Mbps): 2
- Number of Attack Hosts: 0
- Number of UAV Hosts: 4
- Radio Propagation Model: NakagamiModel
- UAV Model: Model1

Parameter Definition Preview

- Attack: DOS
- Tx Rng: 10
- Attack Tx Rng: 0
- UAV Tx Range: 5
- Mobility Model: LinearMobility
- Packet Interval: 0.0001 seconds
- BitRate: 2
- No. of Attack Hosts: 0
- No. of UAVs: 4
- Radio Propagation Model: NakagamiModel

X-47B

38.2 ft

62.1 ft
UAVSim Features

- Concurrent Multi-User Simulation
- User-friendly GUI
- Server Mode Simulation
- High Speed Simulation
- Swarm Simulation
### Default Values of Some parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Limit</strong></td>
<td>300 seconds</td>
</tr>
<tr>
<td><strong>Radio propagation model</strong></td>
<td>Nakagami model [20]</td>
</tr>
<tr>
<td><strong>Packet interval for UAVs</strong></td>
<td>0.05 seconds [21]</td>
</tr>
<tr>
<td><strong>Packet interval for attack hosts</strong></td>
<td>0.0001 seconds</td>
</tr>
<tr>
<td><strong>Number of UAV hosts</strong></td>
<td>10</td>
</tr>
<tr>
<td><strong>Number of attack hosts</strong></td>
<td>30</td>
</tr>
<tr>
<td><strong>Mobility model</strong></td>
<td>Linear mobility</td>
</tr>
<tr>
<td><strong>UAV transmission power</strong></td>
<td>5 Watts</td>
</tr>
<tr>
<td><strong>Attack host transmission power</strong></td>
<td>10 Watts</td>
</tr>
</tbody>
</table>
Hardware Setup

• **PC, Ubuntu 12.04 LTS**
  – Intel® CoreTM i7-3770 CPU
    • 1 x 3.40 GHz 4-core
    • L2/L3 Cache: 1 MB/8 MB
  – System memory: 8.0 GB

• **Server, Ubuntu 12.04 Server Edition**
  – Intel® Xeon® Processor E5-2630
    • 2 x 2.30 GHz 6-core
    • L2/L3 Cache: 1.5/15 MB
  – System memory: 64.0 GB
Results for DoS attack

- **Attack Host vs Average Loss**
  - Number of Attack hosts vs Average Loss (%)
    - Gauss Markov Mobility
    - Mass Mobility
    - Rectangle Mobility
    - Linear Mobility

- **Loss vs Attack Nodes**
  - Number of Attack Nodes vs Average Loss (%)
    - Mass Mobility
    - Linear Mobility

- **Loss vs UAV Hosts**
  - Number of Regular Nodes in the UAVNet vs Average Loss (%)
    - Attacked host-Mass
    - Regular host-Mass
    - Attacked host-Linear
    - Regular host-Linear

- **Average Loss for Linear Mobility**
  - Number of UAV Hosts vs Average Loss (%)
    - Attacked host - Host 1
    - Regular Host - Host 2
    - No Attack Loss - Host 1
    - No Attack Loss - Host 2
Results for Jamming Attack

**Loss vs Attack host TxRange**

![Graph showing Loss vs Attack host TxRange](image)

- Loss in Attack node
- Loss in regular node

**Average round trip time**

![Graph showing Average round trip time](image)

**Average Loss vs Attack Hosts**

![Graph showing Average Loss vs Attack Hosts](image)

- AvLoss1
- AvLoss2
- AvLoss3
- AvLoss4

- Case 1,2: where the communication range of the attack host is 10W and that of regular UAV host is 5W.
- Case 3,4: where the communication ranges for the attack host and regular UAV host are 5W and 10W, respectively.
Performance Evaluation

Time variation with Number of Attack Nodes

Number of Attack Nodes

Simulation Time (seconds)
Performance Evaluation

![Graph showing time variation due to GUI](image)

- **Simulation Time (s)** vs. **Number of Attack Nodes**
  - **GUI**
  - **Non-GUI**
  - **Percentage Change**

The graph illustrates the time variation due to GUI with an increasing number of attack nodes.
Performance Evaluation

![Graph showing time vs concurrent users for attack hosts]

- **Time vs Concurrent Users - Attack Hosts**

  - **Y-axis**: Simulation Time (5 Nodes)
  - **X-axis**: Number of Concurrent Users
  - **Legend**:
    - 5 Attacking Nodes
    - 10 Attacking Nodes
Conclusions

• **Software based Network Simulation - UAVSim**
  - UAVSim - A testbed for UAV system simulation was developed
  - Jamming and DDoS attacks were simulated and attack results were reported
  - Results show the real world simulation capability of the testbed as well as gives insights into the risk imposed by and impact of the simulated attacks
  - The usability of the testbed for lower end hardware has been proved through various performance tests.
Future Work

• **Improving the testbed**
  – Incorporating more UAV models
  – Adding more attacks in the attack library
  – Further enhancing its performance

• **Using the testbed**
  – Refining the testbed and packaging it to be available online for researchers
  – Perform research to secure UAV network based on the testbed
Publications


Questions?