Software defined network architecture to improve security in a swarm of drones

C. Guerber, N. Larrieu, M. Royer
ENAC, Université de Toulouse
christophe.guerber@enac.fr

Journées Cloud 2019,
12 et 13 Septembre 2019 à Toulouse
Context

- A swarm of drones
- Shared/distributed mission
  - Sharing Information
- Secure the network
  - To complete the mission
Summary

• Problem statement and State of the art
• SDN-Based security architecture
• Security evaluation
• Conclusion
Summary

• Problem statement and State of the art
• SDN-Based security architecture
• Security evaluation
• Conclusion
Problem statement
State of the art

Security on UAVs

• Lots of security issues in commercial drones
• Threats identified for military UAVs
  – Eavesdropping
  – Zero day vulnerabilities
  – Replay attack, Spoofing, DoS/DdoS
  – Malicious Code, Subroutine Exploit
  – Virus, Worms, Malware, Trojans and Keyloggers
State of the art
Summary

• Problem statement and State of the art
• SDN-Based security architecture
• Security evaluation
• Conclusion
Architecture contribution 1/2

Inband control

Diagram showing the architecture with components such as Controller, OpenFlow, UDP, TCP, AODV, IP, GCS Host, Mission Host, SDN Switch, Inner port, and Outer port.
• Update neighborhood knowledge
• Loss of neighborhood = remove related flow entries
• Reactive = change only on deletion
• Proactive = change also on addition
• Alternate routes for redundancy
Summary

- Problem statement and State of the art
- SDN-Based security architecture
- Security evaluation
- Conclusion
How to improve security?

1. AODV Routing
2. Secured Connection
3. New Traffic
4. Monitor
5. Identify Anomalies
6. Deploy Defense Strategy

Data plane
Control plane

SDN switch
Control
Data

OpenFlow
Trustful
Mission
Flow entry
Flow Entry
Flow entry
Security model

• Infrastructure:
  – Limited network size, mission duration and key validity
  – A secure Public Key Infrastructure is available
  – TLS is secure and no 0day exploit considered

• Attacker
  – Does not already know a vulnerability
  – Has access to WAN channel (receive and transmit)
  – Cannot physically access the UAV
  – Has limited computation power
  – Does not have credentials for the GCS and UAVs
Security rules

- Two first very simple rules:
  - No ARP (included in flow definition)
  - New flows accepted only from inner ports

<table>
<thead>
<tr>
<th>Attack</th>
<th>AODV</th>
<th>SDN (with or without spoofing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP cache poisoning</td>
<td>Vulnerable</td>
<td>Not vulnerable</td>
</tr>
<tr>
<td>Port scanning</td>
<td>Vulnerable</td>
<td>Not vulnerable</td>
</tr>
<tr>
<td>OS fingerprinting</td>
<td>Vulnerable</td>
<td>Not vulnerable</td>
</tr>
<tr>
<td>SYN flood</td>
<td>Vulnerable</td>
<td>Not vulnerable</td>
</tr>
</tbody>
</table>
Injection on data plane

- Use SDN statistics, compare source and sink
- Change the flow on the fly when detected

Data traffic sent on the network (red) vs. received by the application (blue), 1s stats update period, injection of a single copy of the data, no mobility.

Detected and filtered after less than 2s.
Summary

• Problem statement and State of the art
• SDN-Based security architecture
• Security evaluation
• Conclusion
Conclusion

• SDN based architecture with mobility
• Basic network attacks can be blocked
• Can’t avoid injection but detected and blocked

• Future work:
  – Study round-robin obfuscation technique
  – Implement ML detection for complex attacks with additional statistics
    • Virus, Worms, Malware, Brute force attacks...