Dynamic Discovery and Configuration in Airborne Networks

N. Charbonneau, J. D'Amelia, E. Idhaw

The MITRE Corporation

MITRE

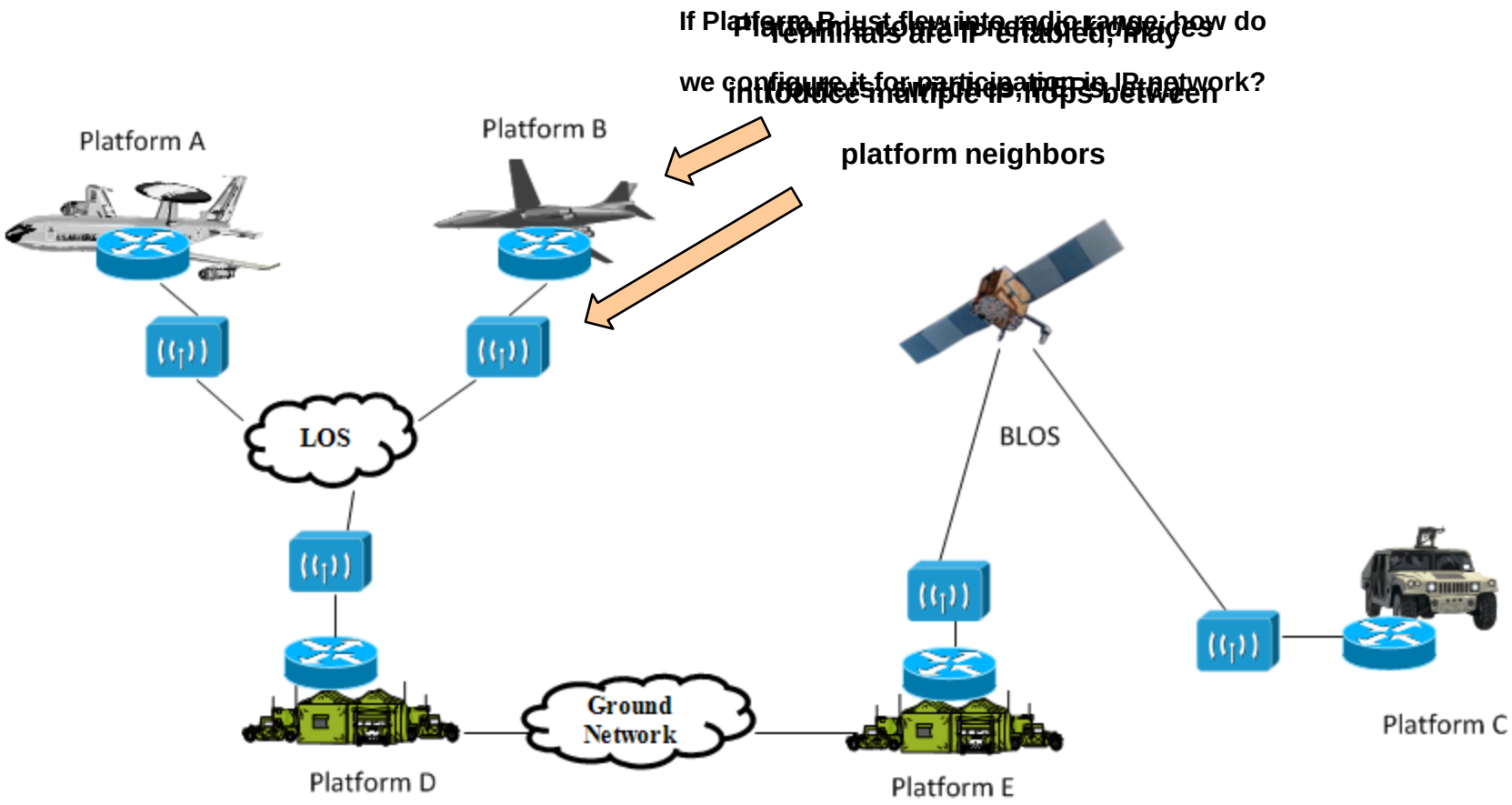
Overview

- Introduction
  - Problem definition
  - Assumptions
  - Device Discovery
  - Automated Configuration
- System Architecture
  - Discovery Protocol
  - Advertisement Protocol
  - Configuration Templates
- Evaluation
- Conclusion

Problem Definition

- Investigating tactical IP networks
- Today: tactical networks require significant pre-planning
  - Spreadsheets with IP addresses, configuration details
  - Very error-prone
- Adding a new node (e.g., Airborne Platform) to the network requires manual re-configuration
  - Operators in the field may not be networking experts so mis-configuration can occur
- Problem:
  - Pre-planning and potential for mis-configuration limits mission flexibility
  - Networks are rigid: difficult to reconfigure for new (unplanned) capability

Problem Definition: Example



Problem Definition

- **Goal: Automatically add nodes to the tactical network, or re-configure existing nodes, to quickly adapt to changing mission needs**
  - **Adding nodes to network means: configuring network devices to use proper routing protocols, DNS servers, and other configuration parameters**
- **Define two phases to the problem**
  - ***Device Discovery*: discover new nodes and establish initial connectivity**
  - ***Configuration Dissemination*: push the appropriate configuration to the new node so it can participate in network**

Problem Definition: Device Discovery

- Work under the assumption that a new node has no configuration (or invalid configuration for current network)
  - No configuration means no IP connectivity. An application-layer discovery solution will not work.
  - Typically, a routing protocol will discover neighbors, but will not work if not properly configured
  - IP-enabled radio terminals prevent link-local discovery
- Goal
  - Allow bidirectional communication between two nodes that do not have a valid configuration
  - Similar to the concept of an *orderwire*
  - Once this is established, can share configuration data

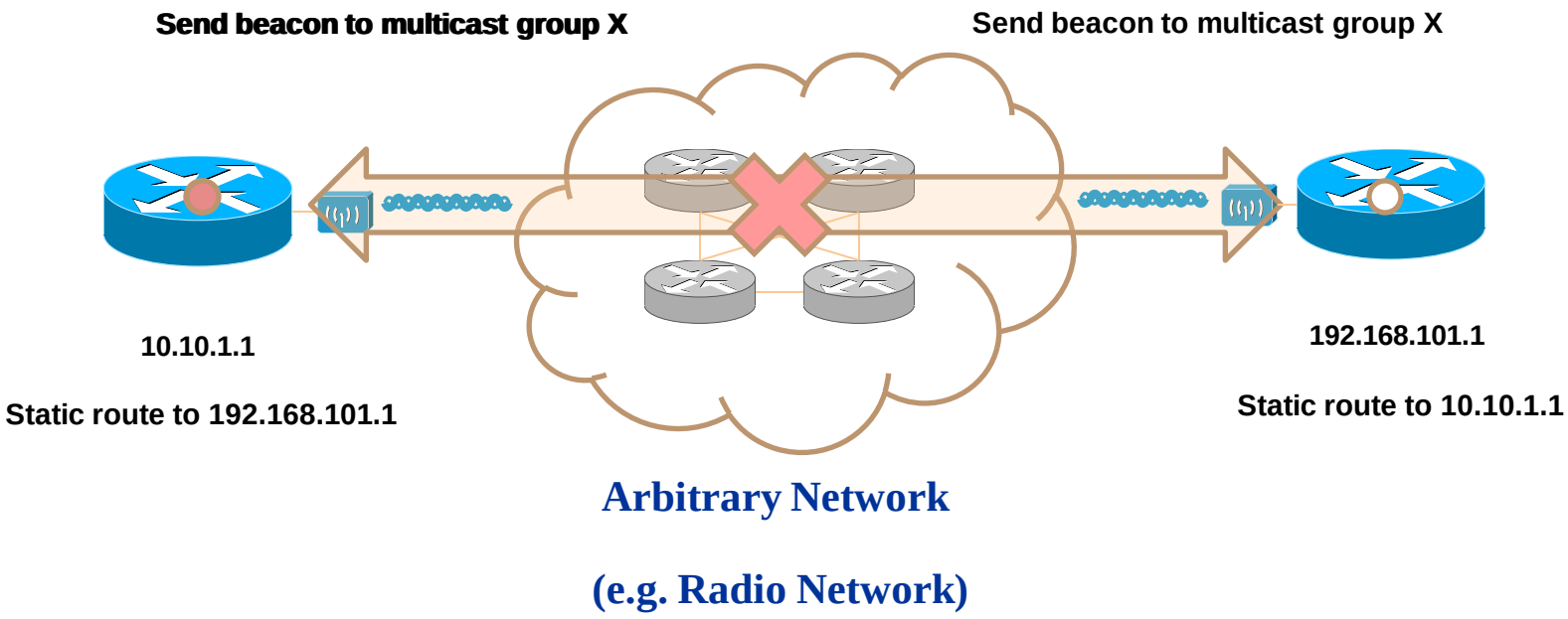
Problem Definition: Configuration Dissemination

- Once bi-directional communication is established, can share configuration information with a new, unconfigured node
- Major challenges:
  - Centralized configuration dissemination will not work, tactical networks may become partitioned
  - Support heterogeneous vendor networks
- Goal:
  - Define flexible, vendor-neutral configuration format
  - Define advertisement protocol to disseminate configurations

System architecture

- Software runs on the *controlling device*.
  - Has ability to intercept and inject packets
- Protocols use multicast
  - Single sender can send to group of destinations
  - Multicast has been deployed/demonstrated in tactical environments
- Components of architecture:
  - Discovery Protocol
  - Advertisement Protocol
  - Configuration format

System Architecture: Discovery Protocol



System Architecture: Discovery Protocol

- Use of multicast allows system to discover unconfigured neighbors as long as they join the multicast group
- Multicast not processed in typical way
  - Intercept packets before Reverse Path Forwarding (RPF) check is performed, otherwise packets would be dropped
  - Packets not forwarded beyond receiving host
  - Similar to a routing protocol

System Architecture: Configuration Dissemination

- Dissemination consists of
  - Configuration Advertisement Protocol
  - Configuration File format
- Requirement for distributed approach
  - Each node in the network stores network-wide configuration data (format show later)
  - When a new node is discovered, requests config from any neighbor
  - Configuration is distributed across entire network in hop-by-hop manner
  - If network partitions, new nodes can still get configuration data

System Architecture: Advertisement Protocol

- At this point, a configured device can send data to an unconfigured device using unicast
- Nodes advertise what configurations they have using an advertisement protocol
  - Multicast protocol (similar to discovery protocol)
  - Each node periodically advertises configuration data it has
  - When a node sees neighbor with newer config, requests it using unicast (which can now happen because of orderwire)
- Unicast transfer uses compression and diffs to reduce configuration size

System Architecture: Configuration Format

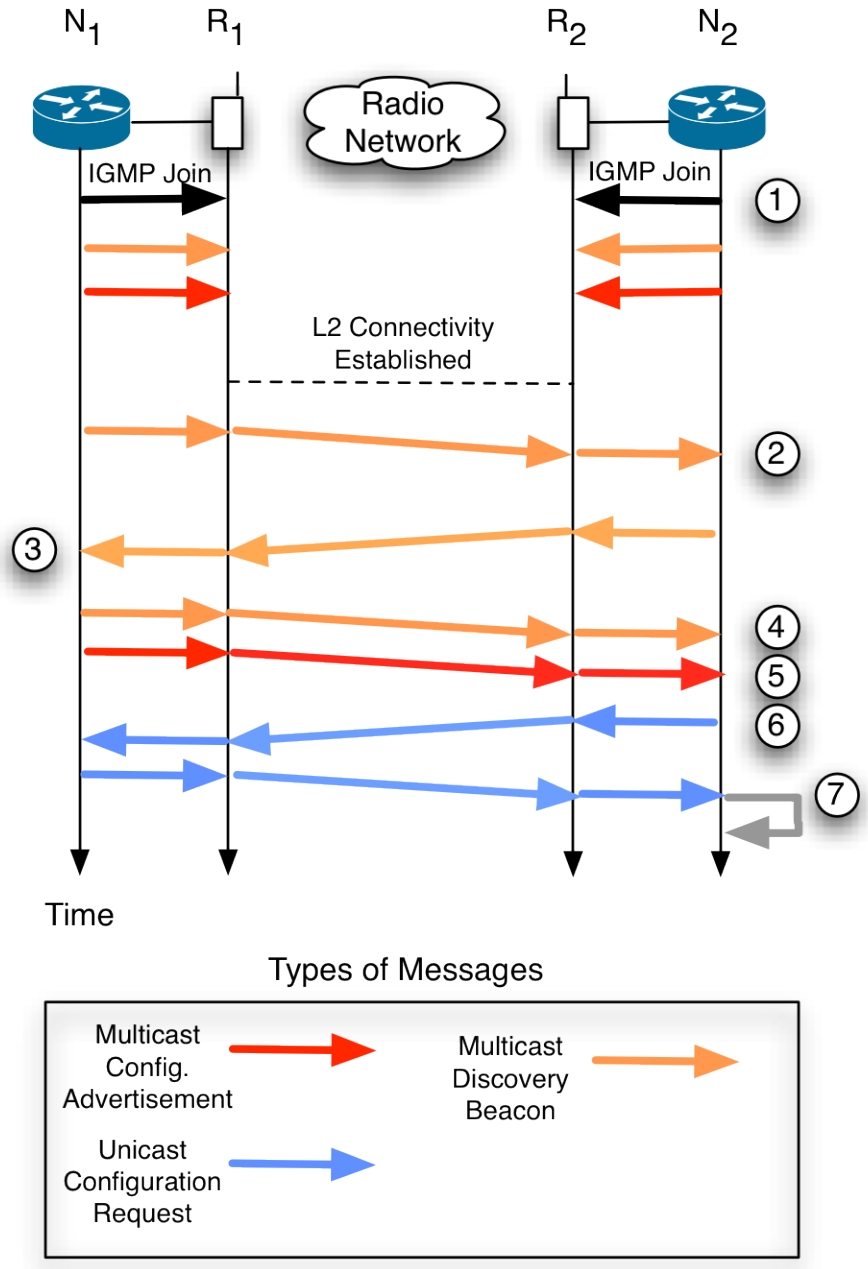
- Configuration represents network-wide configuration
- Pieces of configuration target individual devices or interfaces
- Targeting done using *roles*
  - E.g. AirborneNode, GatewayRouter
  - Roles can be applied to a device or an interface
- Configuration broken down into *requirements*
  - Configuration is a list of requirements, each requirement targets a role
- Define a high-level configuration format that is translated to device-specific configuration commands
- Format allows substitutions

Configuration Format Example

```
<xml>
  <Req name="MCast" version="1"
       targets="device=*">
    <Config>
      <MulticastRouting/>
    </Config>
  </Req>
  <Req name="OSPF" version="1"
       targets="device=*, interface=*">
    <Config>
      <OSPFRouterID>
        <Id>$ReversePathIP</Id>
      </OSPFRouterID>
    </Config>
    <Config target="*">
      <OSPFNetArea>
        <Addr>$IntIP</Addr>
        <Mask>$IntMask</Mask>
        <Id>0</Id>
      </OSPFNetArea>
    </Config>
  </Req>
  <Req name="Intervals" version="2"
       targets="device=*,interface=Radio">
    <Config target="Radio">
      <OSPFIntervals>
        <Interface>$IntName</Interface>
        <Hello>10</Hello>
        <Dead>20</Dead>
      </OSPFIntervals>
    </Config>
  </Req>
</xml>
```

Complete Example

1. Join multicast group
2. Receives discovery beacon, add static route
3. N1 adds static route to N2
4. Sees N1 has added route to N2, orderwire established
5. Sees N1 advertising a configuration
6. Requests configuration
7. Receives, translates, and applies configuration



Related Work

- **Commercial / Open Source discovery tools:**
  - **Cisco CDP**
  - **IETF ZeroConfig (e.g. Bonjour, mDNS)**
  - **Various MANET protocols**
- **Why don't commercial discovery solutions work?**
  - **Only work on a single broadcast domain (e.g. use link-local multicast address)**
  - **Vendor specific**
  - **Cannot travel through multiple IP hops that tactical radios may introduce**

Evaluation

- Prototype to test feasibility
- No existing software to make direct comparison
- Compared human operator (novice to experienced) re-configuration time to our software's reconfiguration time

Conclusion

- Current tactical networks are pre-planned: adding new nodes requires manual re-configuration
- We defined a device discovery protocol:
  - Allows an unconfigured node to establish bi-directional connectivity to an already configured node
- Defined configuration dissemination protocol:
  - Once initial connectivity is established, configuration data can be pushed to allow the new node to fully join the network
- Automated process allows tactical networks to be more adaptable to changing mission needs
- System can also be used to distribute new network configurations automatically (not just for discovery)