A Decision Framework for Enhancing Mobile Ad Hoc Network Stability and Security

LTC Mark E. Orwat, US Army
Naval Postgraduate School, Monterey CA
June 2008

Outline
I. Motivation / Introduction
II. Thesis Statement
III. Current MANET Management Techniques
IV. Contributions
V. Decision Framework
VI. Validation
VII. Conclusions
VIII. Future Work

Quote
Nothing is more difficult, and therefore more precious, than to be able to decide
Napoleon Bonaparte
Security Measurement

Effectively measuring the security of information systems is one of the eight information security (INFOSEC) technical hard problems identified by the INFOSEC Research Council (IRC).

Pervasiveness of the Handheld

United States Military

Bandia National Labs

Consolidated Biscuit Corporation

Loch Lomond & The Trossachs National Park

Emergence of MANETs in DOD

The ultimate goal of MANET network designers is to provide a self-protecting, "dynamic, self-forming, and self-healing network" for devices on the move.
Emergence of MANETs in DOD I

The ultimate goal of MANET network designers is to provide a self-protecting, "dynamic, self-forming, and self-healing network" for devices on the move.

- U.S. Special Operations Command (USSOCOM) early adopters of MANET technologies
- the Joint Tactical Radio System (JTRS): a "MANET-capable" radio for military and first responders
MANET Distributed Functions

<table>
<thead>
<tr>
<th>Distributed Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Head</td>
<td>Master routing decisions on behalf of network</td>
</tr>
<tr>
<td>User-specified Contact Point</td>
<td>The point where a specific user is tapped into the system</td>
</tr>
<tr>
<td>Lightweight Certificate Authority</td>
<td>(also called trust authority) manages the security certificates on behalf of the network</td>
</tr>
<tr>
<td>MANET Rally Point</td>
<td>Serves as an assembly point if network communications unexpectedly break down</td>
</tr>
<tr>
<td>Multi Service Gateway</td>
<td>Provides access to networks internal than current context</td>
</tr>
<tr>
<td>Language Communications Service Provider</td>
<td>Provides capability to transfer messages over large distances</td>
</tr>
<tr>
<td>Internet Service Provider</td>
<td>Provides access to network services without the ability to print</td>
</tr>
<tr>
<td>Photographic Service Provider</td>
<td>Provides the ability to take photos in silent that require a photo of a specific time outside of their location</td>
</tr>
<tr>
<td>Cross-realm Gateway</td>
<td>Serves as the communications link between MANETs at different classification levels</td>
</tr>
<tr>
<td>Multicast Service Connection Node</td>
<td>Provides the maximum flexibility to other MANETs of different security classification domains</td>
</tr>
<tr>
<td>Policy Enforcement/Policy Decision Point</td>
<td>(in p, it's non-essential) makes access control, authorization, authentication, and other security decisions related to the secure management of the MANET and its resources</td>
</tr>
</tbody>
</table>

MANET Dynamic Stability

The ability of a MANET to maintain its ad hoc virtual organizational structure as the underlying resources change and the physical topology varies

MANET Dynamic Stability

The ability of a MANET to maintain its ad hoc virtual organizational structure as the underlying resources change and the physical topology varies
MANET Security

Assignment of a network management function to a compromised or under-provisioned node could disrupt the functionality, efficiency, and security of the inter-device communications.

Thesis Statement

A MANET management process based on an ontological organization of network decision factors and device security characteristics can provide a decision framework for efficient, effective connectivity and security of inter-device communications.

Current MANET Management Techniques

- Active research in: Cluster-head, Trust Authority, Content Portal Functions
- Deployed selection technique ("in the field")
- Emerging selection techniques ("in the lab")
Current MANET Management Techniques

- Active research in:
  Cluster-head, Trust Authority, Content Portal Functions
- Deployed selection technique ("in the field")
- Emerging selection techniques ("in the lab")

MANET Cluster-Head Selection Criteria

<table>
<thead>
<tr>
<th>Single Node Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple Nodes Selection</td>
</tr>
<tr>
<td>Multi-Node and Multi-Node Selection</td>
</tr>
</tbody>
</table>

Contributions

- Presented a new method for incorporating security factors into the measurement of information systems security including a Value Focused Thinking (VFT) based process for the incorporation of subjective factors
- Developed a new conceptual framework to better manage network resources including:
  - The first domain ontology of MANET decision factors
  - The first to combine Value Focused Thinking (VFT) and a Network Flow Optimization Model for MANET decision-making
- Provided a worked example and an initial prototype of the new framework as a basis for the validation of our approach

The MDFO Management Mechanism (MMM)
Ontology I

"Two ... because there's Jacqueline
there at the back.

Ontology II

- "Ontology" has roots in philosophy...the study of existence
- W3C has made "Ontology" an explicit layer in the standards stack for the Semantic Web (web 3.0)
- We leverage the ability of an ontology to:
  ✓ conceptually characterize a domain
  ✓ normalize parameters into a common framework
  ✓ reason between objects via relationship rules and make inferences should items be unavailable or inconsistent
  ✓ Provide a canonical means to incorporate network and device security
- Terminology: Classes, Objects, Attributes, Relations

Ontological Class Descriptions I

Class I: MANET Function
Objects: function names
Attributes: categories
Values = parameters (partial listing)
Objects in the MANET Function Class

- Distributed Function Names
  - Gateways
  - Cluster-head
  - User-specific Context nodes
  - MANET Relay Points
  - Man-Machine Interface
  - Piggyback Service Provider
  - Policy Enforcement/Policy Decision Point

Fragment of the MANET Function Class

- Cluster-head
  - name: cluster-head
  - link QoS: (throughput, latency, mobility rate)
  - node capabilities: (processing capability, available memory, battery power, MI capability)
  - strength of security mechanism: (encryption method, existence of resource hosting hardware, authentication type, user qualification)
  - assurance of security mechanism: (EAL)

Ontological Class Descriptions II

Class I: MANET Function
- Objects: function names
- Attributes: categories
  (Values = parameters (partial listing))

Class II: Network Component Profile
- Objects: device identification (IDs)
- Attributes: parameters (full listing)
  (Values = measured levels)
Fragment of the Network Component Profile Class

- Device 1499965
  - name: device 1499965
  - connections: (long-range, wifi, bluetooth)
  - bandwidth: (11 Mbps)
  - mobility rate: (10 m/s)
  - clock speed: (33 MHz)
  - available memory: (50 MB)
  - authentication type: (biometrics)

Ontological Class Descriptions III

Class I: MANET Function
- Objects: function names
- Attributes: categories
  (Values = parameters (partial listing))

Class II: Network Component Profile
- Objects: device identification (IDs)
- Attributes: parameters (full listing)
  (Values = measured levels)

Class III: Parameter
- Objects: categories
- Attributes: parameters
  (Values = measured level allowable range)

Fragment of the Parameter Class

- Link QoS
  - name: link QoS
  - throughput: (0, 248 Mbps)
  - latency: (1, 500 ms)
  - mobility rate: (0, 250 m/s)
  - jitter: (0, 50 ms)
  - Mean Opinion Score (MOS): (0, 5)
**VFT Swing Weight Matrix Method IV**

**Normal Mode**

<table>
<thead>
<tr>
<th>Contribution to Strength</th>
<th>Non-Security Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>Higher</td>
<td>Lower</td>
</tr>
<tr>
<td>Variability</td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>among</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>Devices</td>
<td>Low</td>
</tr>
<tr>
<td>Encrypt</td>
<td>Authent</td>
</tr>
<tr>
<td>100</td>
<td>73</td>
</tr>
<tr>
<td>ThruPct</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Latency</td>
<td></td>
</tr>
<tr>
<td>MobRate</td>
<td>25</td>
</tr>
<tr>
<td>ProcCap</td>
<td></td>
</tr>
<tr>
<td>AvMem</td>
<td>30</td>
</tr>
<tr>
<td>MLS Cap</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>

**VFT Swing Weight Matrix Method V**

The Normalized Global Weight Function:

\[ w_i = \frac{f_i}{\sum_{i=1}^{n} f_i} \]

- \( i \) = the index of the individual attribute being considered, up to \( n \) attributes here, \( i = [1, \ldots, n] \)
- \( f_i \) = the matrix swing weight assigned to the individual attribute \( (i) \)
- \( w_i \) = the relative weight assigned to the individual attribute \( (i) \)
- \( \sum_{i=1}^{n} w_i = 1 \)

**VFT Composition Function**

The Preference Value Composition Function:

\[ v(x) = \sum_{i=1}^{n} w_i k_i(x) \]

- \( f \) = the index of the individual attribute being considered, up to \( n \) attributes
- \( x \) = the single pair link being evaluated
- \( k_i(x) \) = the individual attribute \( (i) \) preference value assignment for the evaluated node-pair link \( (x) \)
- \( w_i \) = the relative weight assigned to the individual attribute \( (i) \)
- \( v(x) \) = the preference value assignment for the node-pair link being evaluated \( (x) \)
Network Optimization I

The Objective Function:

\[ \text{min} \sum_{l \in J} x_l + \sum_{i \in K} p_i y_i \]

Constraints:

\[ x_j + \sum_{k \in K} y_{k,j} = d_j + \sum_{k \in K} x_{k,j} \quad \forall j \in J \]
\[ 0 \leq x_j \leq 1 + \sum_{k \in K} y_{k,j} \quad \forall (i,j) \in A \]
\[ x_j \text{ = unit flow from node } j \]
\[ y_{k,j} \text{ = penalty for node } j \text{ in the considered node } k \]
\[ d_j \text{ = demand at node } j \]
\[ (i,j) \text{ = demand } (i,j) \]

Network Optimization II

Parameters:
- cost \( c_{ij} \)
- flow \( x_{ij} \)
- penalty \( p_i \)
- flow limit \( b_i \)
- demand \( d_j \)
- capacity \( a_{ij} \)

Supply at node 1:
- \( s_1 = 5 \) units

Demand at node 3:
- \( t_3 = 5 \) units

Graphical representation of network flow.
Network Optimization Results

<table>
<thead>
<tr>
<th>Context</th>
<th>Node ID</th>
<th>Score</th>
<th># of Arcs Reused</th>
<th>Node Choice</th>
<th>Connectivity Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Mode</td>
<td>1</td>
<td>55.4</td>
<td>4</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>38.3</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>20.2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>24.7</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>47.8</td>
<td>4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The MDFQ Management Mechanism (MMM)

Validation

- Translational Validation
  - Face Validation
  - Content Validation
- Criterion-Based Validation:
  - Discriminant Validation
- Security Case Study
- Complex Scenario
Conclusions

- A new method for incorporating security factors into the measurement of information systems security
- A new conceptual framework to better manage network resources including:
  - The first domain ontology of MANET decision factors
  - The first to combine Value Focused Thinking (VFT) and a Network Flow Optimization Model for MANET decision-making
- A worked example and an initial prototype of the new framework as a basis for the validation of our approach
Future Work

1. Develop extensions to framework applying it to other security scenarios
2. Apply the framework to network science problems
3. Demonstrate the applicability of the optimal connectivity map for MANETs and other network situations that can be depicted a network
4. Integrate the framework into the development of a lightweight version of the DoD's Global Information Grid (GIG) Risk Adaptive Access Control (RAAC)

Summary

Questions?

morwst@mns.edu