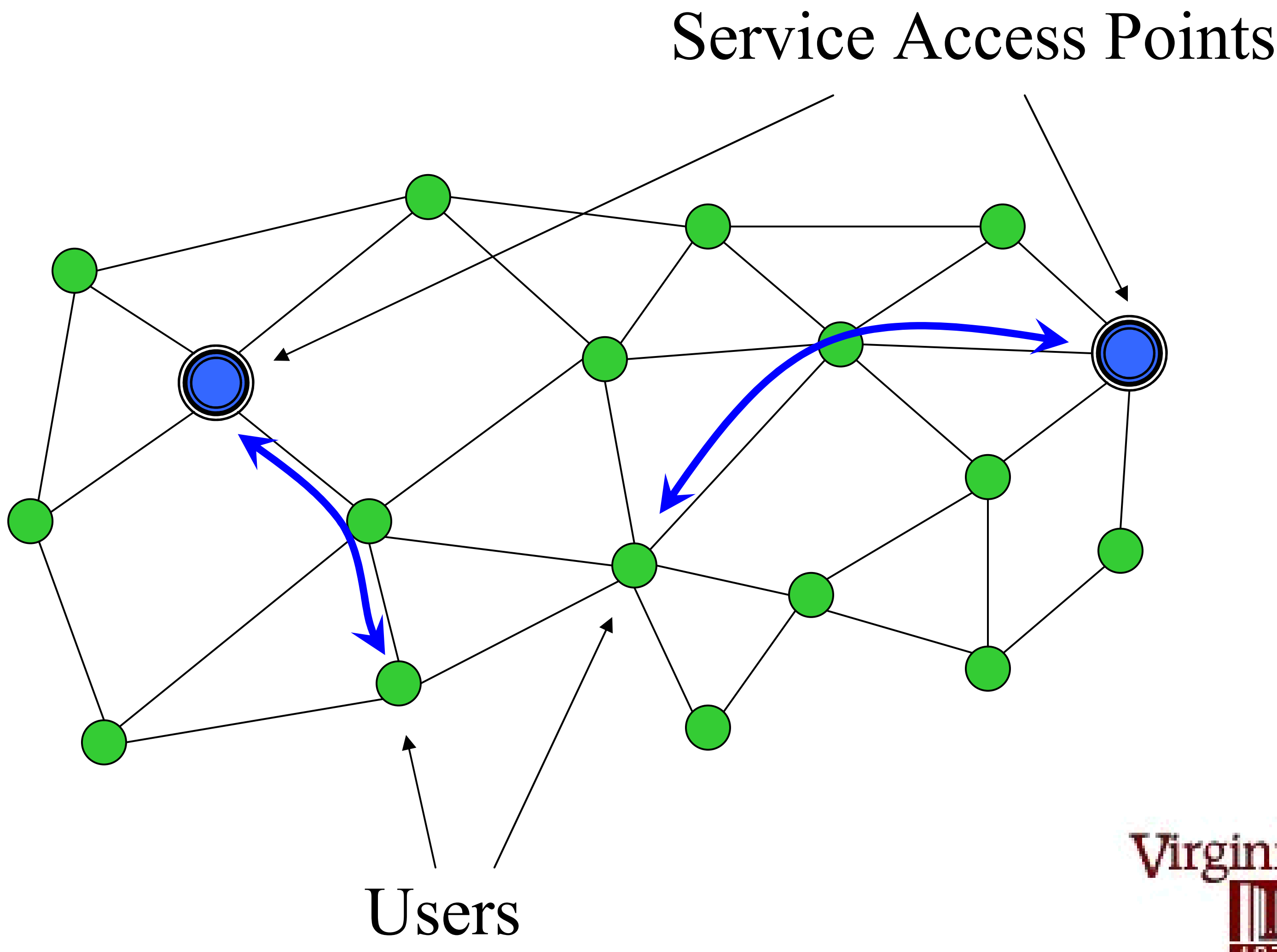
Safeguarding Wireless Service Access

Panos Papadimitratos

Electrical and Computer Engineering

Virginia Tech

Wireless Service Access



Wireless Service Access (cont'd)

- Ad Hoc Networking
  - No fixed infrastructure
  - Collaborative support of the network operation
  - Peer-to-peer interaction
  - Transient associations
  - No administrative boundaries

Wireless Service Access (cont'd)

- Stringent service level requirements
- Shared and limited network resources
- 'Quality' of the communication paths becomes important
  - Data rate
  - Delay
  - Path reliability
- Route discovery protocols that convey path attributes are necessary

Virginia Tech 1872

Problem and Challenges

- Seemingly legitimate users, with access privileges, can get high-quality service access while systematically depriving other users from their sought service level
  - Adversaries can mislead other nodes that the discovered routes are better or worse than they actually are
- Authentication cannot solve the problem

Problem and Challenges (cont'd)

- The ad hoc networking environment introduces vulnerabilities
  - Each and every node can disrupt the network operation
  - No central authority and monitoring facility
  - Difficult or impossible to distinguish between benign and malicious faults
  - Frequent network changes

Solution

- Secure Discovery of Route Attributes
- Secure Routing Protocol for QoS-aware routing (*SRP-QoS*) between a pair of communicating end nodes
  - Accurate quantitative description of the discovered path attributes
  - Wide range of route selection and traffic handling schemes is enabled to configure communication

Network Model

- Network node
  - Unique identity, V
  - Public/private keys E_V, D_V
  - Networking protocols module
  - Wireless communication module
- Primitives: $Send_L(V,m)$, $Bcast_L(m)$, $Receive_L(m)$
- Links: *Up*, *Down*

Network Model (cont'd)

- Each end node knows the identity and the public key of its peer end node
- All nodes know the identities and the public keys of their neighbors
- Benign nodes comply with the protocol rules
- Adversaries deviate or actively disrupt the network operation

Network Model (cont'd)

- *Definition 1*: Independent adversaries are network nodes that can modify, forge, or replay routing or data packets, but ignore received traffic that does not comply with the operation of the networking protocols
- *Definition 2*: Arbitrary adversaries deviate from the protocol execution in an arbitrary (Byzantine) manner

Secure Route Discovery Specification

- N: set of nodes
- E: set of unordered pairs of distinct nodes, i.e., links or edges
- Route: sequence of nodes $V_i \in N$ and edges $e_{i,i+1} = (V_i, V_{i+1}) \in E$
- $f : E \rightarrow M \subseteq \Re$ is function that assigns labels to edges, denoted as link metrics $m_{i,i+1}$
- Route metric: $g(m_{0,1}, \ldots, m_{n-1,n})$
- Actual metric: $g(l_{0,1}, \ldots, l_{n-1,n})$

Secure Route Discovery Specification (cont'd)

$S, T \in N$

Secure Routing Protocol

(S,T) - route and a sequence of labels

- Let t_1 and $t_2 > t_1$ two points in time
  - t_2 is the point in time at which the routing protocol discovers a route

Secure Route Discovery Specification (cont'd)

- *Loop-freedom*: an (*S*,*T*)-route is loop-free when it has no repetitions of nodes
- *Freshness*: an (*S*,*T*)-route is fresh with respect to the (t_1,t_2) interval if each of the route's constituent links is up at some point during the (t_1,t_2)
- *Accuracy*: an (*S*,*T*) route is accurate with respect to a route metric g and a constant $\Delta_{good}>0$ if:

$$|g(m_{0,1},\ldots,m_{n-1,n}) - g(l_{0,1},\ldots,l_{n-1,n})| < \Delta_{good}$$

Virginia Tech

SRP-QoS Operation

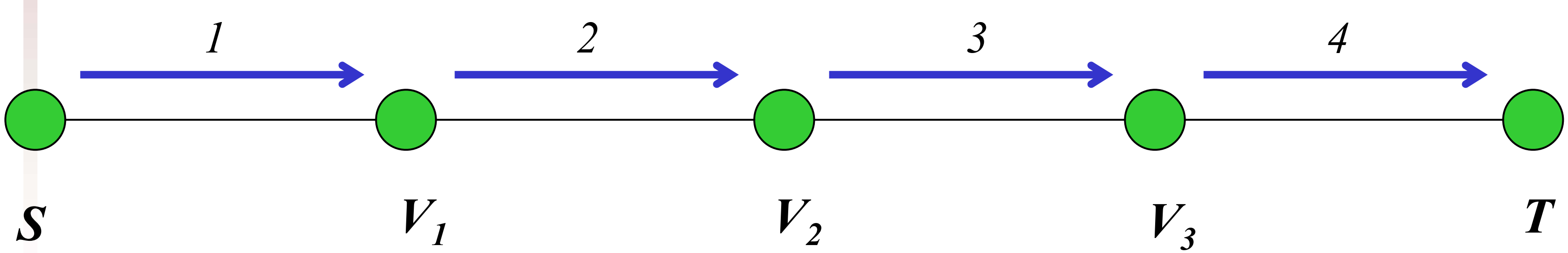
- Nodes estimate metrics for their incident links
  - For link (V_i, V_{i+1}), V_i calculates $m^{i}_{i,i+1}$ and V_{i+1} calculates $m^{i+1}_{i,i+1}$
  - For some $\varepsilon > 0$, $\left| m^{i}_{i,i+1} - m^{i+1}_{i,i+1} \right| < \varepsilon$
  - ε is a protocol-selectable and metric-specific threshold that allows for metric calculation inaccuracies
  - $\delta^{*} > 0$ is the maximum metric calculation error by a correct node

Virginia Tech 1872

SRP-QoS Operation (cont'd)

Route Request (*RREQ*): $S, T, Q_{SEQ}, Q_{ID}, MAC(K_{S,T}, S, T, Q_{SEQ}, Q_{ID})$

1. S broadcasts *RREQ*;
2. V_1 broadcasts *RREQ*, $\{V_1\}, \{m^1_{S,1}\}$;
3. V_2 broadcasts *RREQ*, $\{V_1, V_2\}, \{m^1_{S,1}, m^2_{1,2}\}$;
4. V_3 broadcasts *RREQ*, $\{V_1, V_2, V_3\}, \{m^1_{S,1}, m^2_{1,2}, m^3_{2,3}\}$;



SRP-QoS Operation (cont'd)

- *RREQ* processing
  - *PreviouslySeen*(*RREQ*) routine
  - For each relayed *RREQ*, V_i initializes a *ForwardList*
  - V_i adds a neighbor V_{i+1} to *ForwardList* iff V_{i+1} is overheard relaying *RREQ* with $NodeList = \{NodeList, V_{i+1}\}$ and $MetricList = \{MetricList, m_{i,i+1}^{i+1}\}$ and $\left| m_{i,i+1}^{i} - m_{i,i+1}^{i+1} \right| < \varepsilon$
  - Temporarily stores $m_{S,i}$

Virginia Tech
1872

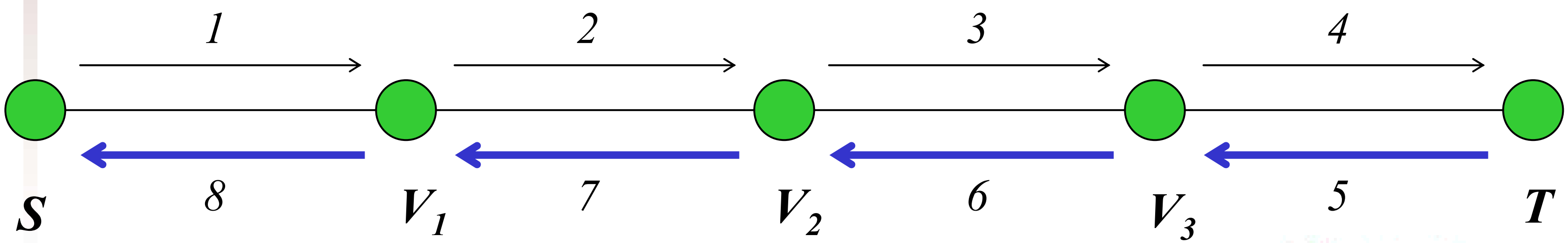
SRP-QoS Operation (cont'd)

Route Reply (*RREP*):

Q_{ID}, $\{T, V_3, V_2, V_1, S\}$, $\{m^{T}_{3,T}, m^{3}_{2,3}, m^{2}_{1,2}, m^{1}_{S,1}\}$,

$MAC\,(K_{S,T}, Q_{SEQ}, Q_{ID}, T, V_3, \ldots, V_1, S, m^{T}_{3,T}, \ldots, m^{1}_{0,1})$

5. $T \rightarrow V_3$: *RREP*;
6. $V_3 \rightarrow V_2$: *RREP*;
7. $V_2 \rightarrow V_1$: *RREP*;
8. $V_1 \rightarrow S$: *RREP*;



SRP-QoS Operation (cont'd)

- *RREP* processing
  - If V_i is T's predecessor, check $\left| m_{i,T}^{T} - m_{i,T}^{i} \right| < \varepsilon$
  - V_i checks if $m_{S,i} = m'_{S,i}$, where $m'_{S,i}$ is the aggregate of the links metric values reported in the *RREP* for links (V_k, V_{k+1}), $k<i$

Virginia Tech 1872

SRP-QoS Properties

- Metric types
  - Δ_{good}^{add} , $g_{add}\left(m_{0,1}^{1},\ldots,m_{k-1,k}^{k}\right)=\sum_{i=0}^{k-1} m_{i,i+1}^{i+1}$
  - If $m_{i,i+1}^{i+1} > 0$, $g\left(m_{0,1}^{1},\ldots,m_{k-1,k}^{k}\right)=\prod_{i=0}^{k-1} m_{i,i+1}^{i+1}$

    can be written as $g_{add}\left(\overline{m}_{0,1}^{1},\ldots,\overline{m}_{k-1,k}^{k}\right)$

    where $\overline{m}_{i,i+1}^{i+1} = \log(m_{i,i+1}^{i+1})$, for $0 \le i \le k-1$

SRP-QoS Properties (cont'd)

- Metric types
  - Δ_{good}^{max} , $g_{\max}\left(m_{0,1}^{1},\ldots,m_{k-1,k}^{k}\right)=\max_{0\le i\le k-1}\left\{m_{i,i+1}^{i+1}\right\}$
  - Δ_{good}^{min} , $g_{\min}\left(m_{0,1}^{1},\ldots,m_{k-1,k}^{k}\right)=\min_{0\le i\le k-1}\left\{m_{i,i+1}^{i+1}\right\}$

SRP-QoS Properties (cont'd)

Lemma: *Routes discovered by SRP-QoS in the presence of independent adversaries are accurate, with respect to (i)* g_{add} *and* $\Delta_{good}^{add} = \varepsilon k^2 + k\delta^*$, *(ii)* g_{max} *and* $\Delta_{good}^{max} = k\varepsilon + \delta^*$, *and (iii)* g_{min} *and* $\Delta_{good}^{min} = k\varepsilon + \delta^*$, *with k the number of route links,* $\varepsilon > 0$ *the maximum allowable difference between* $m_{i,i+1}^{i}$ and $m_{i,i+1}^{i+1}$, *and* $\delta^* > 0$ *the maximum error for a metric calculation by a correct node.*

Virginia Tech 1872

Conclusions

- Wireless ad hoc networking domains are a double-edged sword
- SRP-QoS enables a general QoS-based route selection even in the presence of adversaries
- More information: *papadp@vt.edu*