Securing Information through Trust Management in Wireless Networks

Mohit Virendra, Shambhu Upadhyaya
Computer Science and Engineering
The State University of New York at Buffalo
Buffalo, NY
Sep 24, 2004
Trust Schemes: Wireless Domain

Wireless Network Classification

1. Independent Ad-hoc
2. Central Authority

Trust-based Security Schemes

a. **Independently**
   Mutual information exchange between the nodes

b. Using a **Trusted Central Authority**
Overview

**Problem Statement:**

Defining trust schemes for securing information in WLANs and Ad-hoc networks

**Contributions:**

<table>
<thead>
<tr>
<th>Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust based Admission Control scheme with a <em>first yes</em> policy for WLANs</td>
</tr>
<tr>
<td>Trust monitoring through Intent Graphs in wireless domain</td>
</tr>
<tr>
<td><em>Actual Condition Review</em>-based Peer Monitoring Scheme</td>
</tr>
<tr>
<td>Trust based security scheme for ad-hoc networks: <em>Physical and Logical Security Domains</em></td>
</tr>
<tr>
<td>Trust management through <em>Domain Heads</em> in ad-hoc networks</td>
</tr>
</tbody>
</table>
CA Assisted Scenario: WLAN model

WLAN Architecture: Two servers on the Distribution System: (a) Admission Controller (AC), (b) Global Monitor (GM)

Trust Based Admission Control
- admission time trust establishment
- Admission decision depends on “trust value” and “intent” of the new node

Intent query scheme between AC and the new node
- Perfunctory check policy for node with unknown trust

Optimistic Approach: Trust everyone until misbehavior detected

“First Yes Policy”: Node proves and maintains trust value to be in session. Trust verified while node is in the system

Looks Naïve!
But very effective in selective admission control
WLAN model: Trust Establishment

Nodes use symmetric key pairs for communication with AP, key duration dependent on trust value and “incrementing” trust also

Trust Levels: Used to (dis)allow a node to perform certain operations
Three Trust Levels: Low, Medium and High

Intent Map (Graph) Generation: models node’s intended behavior
FSM based on resources required & steps to be followed

During the operation, AC/GM monitors node using GHMS [10], checks against Intent Map and builds its Trust History

Benign transactions increase node’s trust value

Relationship between transactions completed and trust value depicted by graph on next slide
Trust Value vs. Operations

- High
- Medium
- Low/Unknown

(Malicious)       Operations       (Benign)

Misbehavior Threshold (Intrusion Flagged)
## Intent Graphs and ACR generation

<table>
<thead>
<tr>
<th>Tolerance in Intent Graphs</th>
<th>Tolerance Level and Misbehavior Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dealing with excess data rates: calculating threshold as an incremental percentage or probability as a function of data rates [11]</td>
<td></td>
</tr>
<tr>
<td>Each deviation $\Rightarrow$ closer to threshold $\sim$ severity of misbehavior</td>
<td></td>
</tr>
<tr>
<td>Flagging an intrusion $\Rightarrow$ premature expiration of the session key between node and AP</td>
<td></td>
</tr>
<tr>
<td>Trust Values help in Leader Selection</td>
<td></td>
</tr>
<tr>
<td>Peer Trust Monitoring: Actual Condition Review (ACR) report generation scheme</td>
<td></td>
</tr>
<tr>
<td><strong>FORWARD MONITORING:</strong> APs generate ACRs about nodes</td>
<td></td>
</tr>
<tr>
<td><strong>REVERSE MONITORING:</strong> Nodes generate ACRs about APs</td>
<td></td>
</tr>
<tr>
<td><strong>SELF MONITORING:</strong> Nodes forced to submit their own progress report</td>
<td></td>
</tr>
</tbody>
</table>

**Result:** A self correcting trust monitoring system
Node Requests Admission

Query Intent

NO

Admitted

YES

Intent Graph Generation

Key Generation

YES

Granted

NO

Request Key Regeneration

Key Valid

NO

Request Key Regeneration

YES

Node perform next operation

Conforming to Intent Graph

NO

Crossed Threshold

NO

Node Done with all Tasks

YES

Flag Intrusion

NO

YES

STOP
Independent Ad-hoc Networks

**Mutual Information Exchange Based Trust**

**Trust Based Domains**

- Grouping nodes with similar trust parameters and interests
- Defining Qualitative Trust Parameters and Quantifying Trust

- $A \sim B$ and $B \sim C$, then $A \sim C$ using B’s trust as a verifier
- More comprehensive schemes if A and C don’t trust a common node

- Node may share trust interests with nodes belonging to two or more domains: “Border Nodes”

- Membership in a domain a collective decision (e.g. secure polling)

- Encryption Schemes proposed by Zhou et al. [17], [18]
Domains

Nodes preloaded with keying material: establish pair-wise symmetric keys on the fly with domain members

Nodes in a Domain share a common DOMAIN KEY

Domain Heads: Election and Rotation

Domain Heads can establish pair-wise symmetric keys with each other on the fly for trust negotiation

All inter and intra-domain communication uses symmetric pair-wise keys

Physical Trust Domains (PTDs) and Logical Trust Domains (LTDs)

Overlapping PTDs
Non-overlapping PTDs

Overlapping LTDs
Non-overlapping LTDs
Overlapping PTDs

PTD A

Na

Nab

PTD B

Nbc

PTD C

Nc
Overlapping PTDs

- Nodes in LTD A
- Nodes in LTD B
- Other Nodes
Non Trusted Regions and Hierarchical Trust

- Communication between non-trusted regions: End to end tunnels
- Tradeoff between: Information Security and Information Relevance Lifetime
- Sending information along multiple routes: Minimum Trust Value of a route

Hierarchical Trust and Super Domains

- Addressing Scalability and Reduce Control Overhead of Head Nodes

Hierarchical Trust:

- Would help if a domain head (hence all domain members) are compromised
- But, requires extra degree of protection for domain heads and super domain heads against attacks targeted at Central Authority
Conclusion and Discussion

Introduced trust based schemes for wireless networks

Trust based security model for WLANs

Idea of Physical and Logical Trust Domains in ad-hoc networks

Conceptual paper: describes new paradigms and concepts, require deeper investigation

Continuing Research:

Studying control overheads of the schemes introduced by us

Formalizing the “first yes” admission control scheme

Extending the ACR generation scheme to ad-hoc networks
References

Questions?

Email: \{virendra, shambhu\}@cse.buffalo.edu

www.cse.buffalo.edu/~virendra