



Information System Security Operation

Intrusion Detection for Mobile Ad-hoc Networks

A Cooperative Intrusion Detection Architecture for Tactical Wireless Networks

Problem

The Army's Future Force requires a fully-mobile, fully-communicating, agile, and situation-aware force that exploits net-centric distributed platforms to enhance its survivability and lethality. This force consists of a heterogeneous mixture of individual soldiers, manned and unmanned platforms, and sensors. All these components operate in a wireless, mobile, highly dynamic or ad hoc, networking environment (MANET). The information infrastructure that supports this force will be rapidly deployable, self-organizing, adaptive, self-contained, multi-layered, survivable, and interoperable with other military networks and with DoD's Internet-based Global Information Grid (GIG). Information throughout this infrastructure must be protected to ensure that it is authentic, accurate, secure, and available under a full range of threats. Survivability must be maintained in spite of the inherent vulnerabilities of standardized protocols and commercial technologies and techniques that will be leveraged by the military.

Approach

Information throughout this distributed infrastructure must be protected to ensure that it is authentic, accurate, secure, and available under a full range of threats. This is particularly challenging because these networks have limited resources; use wireless channels that are noisy and susceptible to attack; employ highly dynamic and self-configuring networking; do not have concentration points where traffic can be analyzed; and must support forward-deployed tactical military operations.

Our project, Intrusion Detection for Mobile Ad-hoc NETWORKS (ID-MANETS). It is intended to address these requirements. ID-MANET

focuses on distributed detection, particularly of insider threats. This architecture leverages recently published research, and goes significantly beyond previously published results in the following respects, as it is designed to:

- Meet the specific needs of tactical wireless networks, which are significantly different than their commercial counterparts.
- Provide a general foundation for *all* intrusion detection and supporting activities that can adapt to dynamic network conditions. These activities include detecting a broad spectrum of conventional attacks and MANET-specific attacks on routing and other infrastructure services; collecting, reducing, and correlating intrusion events; responding to intrusions; and managing intrusion detection and related functions.
- Address key enabling features for assigning and reassigning network monitoring and other responsibilities to nodes; facilitating seamless transition of these responsibilities among nodes; and enabling controlled sharing of cryptographic session keys to allow network monitors to decrypt and inspect encrypted packet payloads.

Solution

We analyzed the challenges confronting intrusion detection in MANETS and designed a cooperative intrusion detection architecture that enables the application of multiple, diverse, overlapping detection mechanisms for layered defense and broad spectrum protection; exploits clustering to provide efficient hierarchical communications and control while exploiting peer-to-peer communications for flexibility and resilience; and dynamically adapts its data collection, detection, aggregation, and correlation capabilities as topology, routing, and connectivity change.

This work was sponsored by Army Research Laboratory (ARL) through Telcordia Technologies, Inc., Contract Number DAAD19-01-C-0062, Subcontract Number 10084668, with McAfee Research, which is now the Security Research Division of SPARTA.

<http://www.isso.sparta.com/research>

Intrusion Detection for Mobile Ad-hoc Networks

A Cooperative Intrusion Detection Architecture for Tactical Wireless Networks

Future Research

Our work continues in two related areas:

Cooperative Intrusion Detection Architecture

- Evaluating alternative clustering algorithms in terms of bandwidth consumption during cluster establishment and maintenance; impact of cluster updates on detection latency; scalability; and potential to induce congestion and processing bottlenecks in intrusion detection reporting, aggregation, and correlation processing.
- Analyzing cost vs. benefit tradeoffs for using redundancy in the hierarchy including assigning two parents to each leaf node and providing backup nodes for the root node.
- Analyzing the effectiveness and costs of the en route detection strategy for 1) tracking the behavior of mobile nodes over time and 2) acquiring and aggregating reliable statistics on highly distributed attacks.

Intrusion Detection Algorithms

- Analyzing the reliability and utility of network data acquired by promiscuous eavesdropping in the presence of hidden

and exposed terminal effects, other interference phenomena, and noise.

- Developing, simulating, prototyping, and analyzing distributed algorithms for detecting misbehavior in MANET routing and infrastructure protocols, particularly in the situations where intermittent connectivity and noise require detection decisions to be made with incomplete or erroneous data.
- Improving techniques for formulating security specifications for specification-based detectors.
- Developing metrics and synthetic intrusions to assess performance and overhead of distributed detection systems for MANETs.

The results of this project, particularly if extended and amplified by investigation of these research topics, can strongly contribute to addressing the Army's critical need to protect tactical wireless networks from intrusions. Moreover, these efforts can play an important role in the development of the sophisticated intrusion detection capabilities that these networks must incorporate before they can be deployed operationally.

