

PROJECT PROFILE

Distributed Sensor Network Security

Background

Battlefield constraints create daunting engineering challenges for sensor designers. Sensor packages will be small, lightweight, inexpensive, and low-power. Distributed in irregular patterns across remote and often hostile environments, sensor nodes will autonomously aggregate into collaborative, peer-to-peer networks. Sensor networks must be robust and survivable despite individual node failures and intermittent connectivity. Support for lengthy mission lifetimes constrains battery consumption to miserly rates when not in an energy conserving dormancy. High information assurance must be provided despite the use of unattended sensor packages with relatively weak resistance to tampering.

Providing confidentiality and authentication is critical to preventing an adversary from compromising the security of a distributed sensor network. However, providing key management for confidentiality and group-level authentication is difficult due to the ad hoc nature, intermittent connectivity, and resource limitations of the distributed sensor network environment. This DARPA-sponsored research addresses this problem by developing cryptographic protocols and mechanisms that efficiently provide key management security support services.

Objective

The primary objective of this research is develop a communications security architecture that incorporates cryptographic security mechanisms that efficiently support the provision of required integrity, authentication, and confidentiality security services within distributed networks of resource-limited sensors. The research has three underlying objectives:

- Identify practical cryptographic mechanisms and protocols that can be selectively employed by resource-limited sensor nodes;
- Design a communications security architecture suitable for use by distributed networks of resource-limited sensor nodes; and
- Implement a prototype system and simulation that can be used to demonstrate efficient and practical communications security for distributed networks of resource-limited sensors in a variety of environments and scenarios.

Approach

NAI Labs' approach has been to identify battlefield sensor network requirements and constraints, developing candidate protocols to solving our research problem, and analyzing the effectiveness of various methods. Since the most notable battlefield constraint affecting security is limited battery power, we have focused on developing protocols that minimize energy consumption.

Key management primarily consumes battery power in two ways: through the algorithm computations performed by the main processor and through the

Research Focus

Distributed Sensor Networks for Mission Critical Protection

Distributed sensor networks will be a mission critical component requiring commensurate communications security protection. Warfighters and sensors must be assured that received information is correct. Sensor network communications must prevent disclosure and undetected modification of exchanged messages.

This research addresses the problems of achieving sufficient "trust" among unattended sensor nodes to support key management, and efficiently performing cryptographic key computations for message privacy and authentication.

- David Carman
Principal Investigator,
Cryptographic Technologies
Group

Approach (continued)

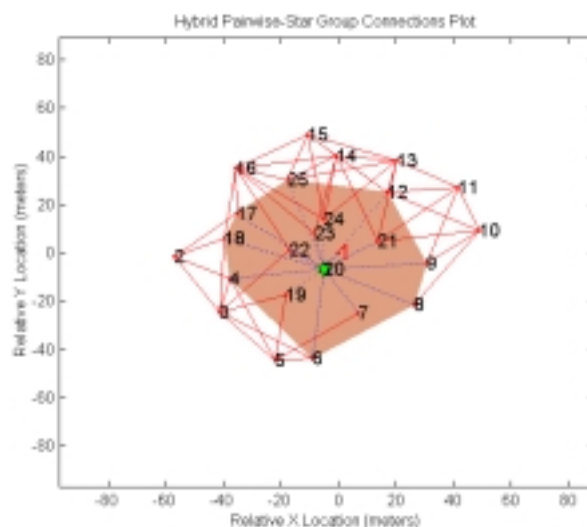
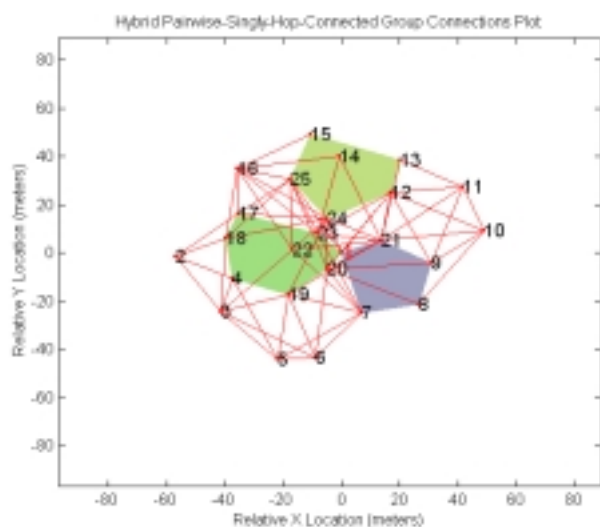
additional communications energy expended to transmit and receive key management information. Since the amount of energy consumed by different processors and communications systems varies widely, we have analyzed several popular embedded processors and communications subsystems.

Results

NAI Labs has developed key management protocols specifically designed for the distributed sensor network environment, including Identity-Based Symmetric Keying and Rich Uncle. We have analyzed both existing and NAI Labs-developed keying protocols for their suitability at satisfying identified requirements while overcoming battlefield energy constraints. Our research has focused heavily on key management energy consumption, evaluating protocols based on total system, average sensor node, and individual sensor node energy consumption.

Our examination of keying protocols has revealed that a single keying protocol will not be optimal for all sensor network topologies, densities, sizes, and scenarios. Protocols such as Identity-Based Symmetric Keying and Rich Uncle have limited application until the network's routing infrastructure has been sufficiently well established. Individually other protocols such as the public-key group and pairwise keying protocols consume too much energy. For significant sensor networks, a mix of public key-based protocols, including pairwise, group keying, and distribution keying, provide an energy-efficiency superior to using just a single protocol.

We have developed group determination algorithms and hybrid key management protocols to improve the energy efficiency of key management. The group determination algorithms find the largest non-overlapping singly-hop-connected and star groups within a given sensor network field such as those shown in the figures below. A singly-hop-connected group is a collection of sensor nodes that can each transmit and receive to every other group member. A star group is as a collection of sensor nodes that can each transmit and receive to a single "leader" node. The hybrid key management protocols perform various group keying protocols using either singly-hop-connected or star groups, and pairwise keying protocols for any remaining sensor nodes in the field.



Pairwise and Group Connections, Communications Range = 40 Meters

We have developed and analyzed a MATLAB-based simulation to assess the performance of our developed algorithms and protocols. Different communications ranges and different transmit power control methodologies were simulated for each of the different hybrid approaches. Our simulation-based analysis demonstrates that hybrid key management protocols provide significant advantages in performing key management.

Additional Information

For additional information about the Distributed Sensor Network Security project, email sensit@tislabs.com or visit our Web page at: <http://www.pgp.com/research/nailabs/cryptographic.asp>.

1/5/01



Who's watching your network

For more information on NAI Labs, contact your authorized NAI Sales Representative, or visit <http://www.nailabs.com>.

CORPORATE Headquarters

3965 Freedom Circle
Santa Clara, CA 95054-1203
Tel (800) 764-3337*
Fax (888) 203-9258

*Call for additional Worldwide Sales Offices