TECHNOLOGY

Key-Management Scheme and Apparatus for Distributed Sensor Networks

OVERVIEW

The increased utilization of Distributed Sensor Networks (DSNs), for security and military purposes, poses a huge challenge in providing such networks with strong security measures in terms of confidentiality, authentication, data integrity, key distribution, and network administration. On the other hand, the typical constraints for power consumption, communication, and computational capabilities inherent to DSN sensor nodes must be considered as part of the design problem.

DSNs are ad-hoc mobile networks that include arrays of sensor nodes that are battery powered, have very limited computational and memory capabilities, and rely on intermittent wireless communication via radio frequency. Typically a DSN may have tens of thousands of sensor nodes, and those nodes are usually deployed in hostile areas where communication is monitored and nodes are subject to capture and surreptitious use by an adversary. Hence DSNs require cryptographic protection of communications, sensor capture detection, key revocation, and sensor disabling.

Researchers at the University of Maryland, College Park, have developed a key-management scheme designed to satisfy both the operational and computational requirements of DSNs. It relies on probabilistic key sharing among the nodes of a random graph and uses simple protocols for shared-key discovery, path-key establishment, key revocation, re-keying, incremental addition of nodes, and deletion of nodes. The scheme is suitable for large-scale DSNs and simple enough given the sensor node computation and communication limitations. This approach is scalable and flexible; trade-offs can be made between sensor-memory cost and connectivity, and the design parameters can be adapted to fit the operational requirements for a particular environment. The results of the investigation indicate that this scheme is superior to the traditional key pre-distribution schemes.

For further information, please contact the Office of Technology Commercialization, (301) 405-3947 E-mail: otc@umd.edu.

CONTACT INFO

UM Ventures
0134 Lee Building
7809 Regents Drive
College Park, MD 20742
Email: umdtechtransfer@umd.edu
Phone: (301) 405-3947 | Fax: (301) 314-9502

Additional Information

INSTITUTION

University of Maryland, College Park

PATENT STATUS

Patent(s) pending

LICENSE STATUS

Available for exclusive or non-exclusive license

CATEGORIES

- Microelectronics
- Information Technology

EXTERNAL RESOURCES

- US Patent 7,486,795

IS-2003-065