

Analysis and Evaluation of Key Management Protocols for Wireless Sensor Networks

Project Team: Sridhar Reddy Saran - ssarsan@gmu.edu
Venkata Gopal Krishna Addada – vaddada@gmu.edu

Introduction

Ad hoc networks are autonomous networks consisting of routing nodes (or some of the nodes may route and some cannot but just relay) that are mobile in nature. Ad hoc networks do not have a pre-defined infrastructure and topology. As ad hoc networks are mobile in nature, their topology varies randomly and unpredictably. Ad hoc networks may operate in standalone fashion, or may be connected to the large Internet.

Sensor networks are special case of ad hoc networks and can be widely used for military and weather monitoring applications. Each sensor node is equipped with a sensor, onboard processor, a transceiver and a low-powered battery. Sensor networks are self-organized as in case of ad hoc networks. The till to date research focuses only on static sensor networks, but mobility in sensor networks received less attention.

Security in sensor networks is very critical due to self-organization, low battery power, and low processing capability. Security requirements of sensor networks largely vary depending on the purpose of the application they are designed for and the environment in which they operate. For example, security requirement of military networks varies from that of a civilian network. All these constraints make it difficult to implement conventional security mechanisms to sensor networks.

Major security issues in sensor networks are secure routing, key management, intrusion detection, and broadcast authentication. Traditional key management protocols cannot be employed in their original form to wireless sensor networks due to their resource limitations. Hence, specific techniques, which are adaptable to sensor networks, are needed for key distribution, key exchange and key management. Sensor networks require different types of keys such as group keys, pair-wise keys, cluster keys etc based on specific requirements. Several keying protocols have been proposed to solve these requirements.

This project focuses on analyzing and evaluating some of the proposed key management protocols and identifying the future directions to this research.

Project Specification: -

1. Protocols to be Analyzed:
 - a.. Virgil Gligor proposed key management scheme
 - b. Adrian Perrig proposed random key pre-distribution scheme.
 - c. Wenliang, Jing proposed pairwise key pre-distribution scheme.
 - d. Roberto Di Pietro proposed random key assignment scheme
 - e. Donggang, Peng Ning proposed pairwise key establishment scheme
 - f. Donggang, Peng Ning proposed location based pairwise key establishment.

2. We are going to analyze based on following factors:
 - a. Security
 - Resiliency to node capture
 - Secure addition of Node (scalability)
 - Secure node revocation
 - b. Maximum Network size supported
 - c. Computational cost (key related) & Energy efficiency (Battery power)
 - d. Overhead (Memory utilization)

3. Tentative list of questions that we are seeking answer:
 - a. Are the proposed protocols sufficient to fulfill all the security (keying) requirements?
 - b. Can these protocols handle possible future attacks (new attacks) on keying infrastructure of sensor networks?
 - c. Can these protocols be implemented on largely resource constrained sensor network?
 - d. What are the aspects never handled by each protocol?
 - e. What are the issues that are not efficiently handled by the protocols?
 - f. What are the improvements that can be made to these protocols?
 - g. What future work can be done in this area?

4. Procedure for verifying the results of the investigation:
 - a. Analysis is based on the overhead of each protocol, complexity of keying mechanism and level of security it provides.
 - b. Consulting experts in this field.

5. Format and tentative table of content in final report:
 - a. Abstract of what we are trying to do.
 - b. Very brief description of protocols that are analyzed
 - c. Includes observations and critics of each protocol described in previous section
 - d. Conclusion and expected future work
 - e. References

6. Time schedule:
 - a. 10/04/2003: Submission of final project specification
 - b. 10/15/2003: Submission of first progress report, which includes Study and partial analysis of first set of protocols from the above list
 - c. 10/29/2003: Submission of second progress report, which includes study and partial analysis of second set of protocols from the list
 - d. 11/12/2003: Submission of third progress report, which includes final analysis and critic of each protocol.
 - e. 12/03/2003: Submission of final progress report submitted by e-mail
 - f. 12/06/2003: Submission of final project report in e-mail format
 - g. 12/09/2003: Discussion of project reports and view graphs with the instructor
 - h. 12/12/2003: Final oral presentation

** The above dates are tentative. We have to discuss with Instructor and fix the dates.

7. List of possible areas, where the specification can change:

Based on the progress of the project and availability of literature, new protocols can be added and existing protocols can be removed from the above protocol listing.

8. Literature:

- a. Laurent Eschenauer, Virgil D. Gligor. “[A key-management scheme for distributed sensor networks](#)”. Conference on Computer and Communications Security. Proceedings of the 9th ACM conference on Computer and communications security 2002 , Washington, DC, USA
- b. Haowen Chan, Adrian Perrig, Dawn Song “[Random Key Predistribution Schemes for Sensor Networks](#)” In 2003 IEEE Symposium on Research in Security and Privacy.
- c. Wenliang Du, Jing Deng, Yunghsiang S. Han and Pramod K. Varshney, Syracuse University, “A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks”
- d. Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei (University of Rome "La Sapienza", Italy), “Random Key Assignment for Secure Wireless Sensor Networks.”.
- e. Donggang Liu and Peng Ning, North Carolina State University , “Establishing Pairwise Keys in Distributed Sensor Networks “ .
- f. Donggang Liu and Peng Ning (North Carolina State University, USA), “Location-Based Pairwise Key Establishments for Relatively Static Sensor Networks”.
- g. Constraints and Approaches for Distributed Sensor Network Security, dated September 1, 2000. Network Associates Labs Technical Report #00-010
- h. The **Resurrecting Duckling**: Security Issues for Ad-hoc Wireless Networks by Frank Stajano, Ross Anderson
- i. Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar. “[SPINS: Security Protocols for Sensor Networks](#)”. MOBICOM, 2001.
- j. Donggang Liu and Peng Ning “[Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks](#)”. The 10th Annual Network and Distributed System Security Symposium. San Diego, California. February 2003

k. LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks
S. Zhu, S.Setia. S.Jajodia. To appear in the 10th ACM Conference on Computer and
Communications Security (CCS '03), Washington D.C., October, 2003.