

# The Philadelphia Area Urban Wireless Network Testbed

Gustave Anderson  
gus@minerva.ece.drexel.edu

Gaurav Naik  
gnaik@minerva.ece.drexel.edu

William C. Regli, Ph.D.  
regli@drexel.edu

Moshe Kam, Ph.D.  
kam@minerva.ece.drexel.edu

## 1 Introduction

Mobile Ad-hoc NETWORKS (MANETs) represent the integration of many subsystems. Security on a MANET is therefore multi-level, and while each subsystem may be classified as secure by some local performance index, the integrated plant does not necessarily inherit the security properties of its components. The most obvious vulnerability is “at the seams,” between subsystems. However, it is also possible that architectural weaknesses and intercommunication gaps would provide a potential attacker with opportunities that were not obvious during the design of the separate components. In general, one must assume that the integrated system is more vulnerable than each one of its components.

We describe a research and development effort to secure the integration of applications in a mobile computing environment. Our system addresses the need for robust and secure information distribution solutions in infrastructure-free environments. Applications built as part of this solution may then support users in communicating and transferring information more effectively and in ways not possible with existing technologies. A variety of real-world applications exist which would greatly benefit from such distributed, mobile tools. They have the potential to improve information flow between users in environments where power, networks, and other computing resources do not exist or have been damaged. These environments include coordinated police forces at large public events, medical personnel at an accident scene, and emergency responders to a natural disaster.

## 2 System Architecture

In this study we focus on the secure integration of mobile agent applications using agent technology

(COUGAAR or EMAA) in a mobile environment. In the development of this integrated architecture we focused on maintaining the following:

- Security - application layer Information Assurance.
- True distributed computing - no online central entity or authority.
- Revocation - the ability to dynamically remove users whose access privileges have changed.
- Efficiency - resources are limited in the mobile environment, therefore we need to maintain a high ratio of useful bandwidth to maintenance and security overhead.
- Stability - the system must be able to handle internal faults gracefully, and to allow reduced-level operation and regrouping after widespread failures.
- Survivability - the system must be able to handle a wide repertoire of external faults, and be able to operate in parts, and under islanding conditions.

In secure networks (mobile and static) it is useful for several hosts to share a single symmetric encryption and decryption key, where each group has its own unique key, though members may belong simultaneously to several groups. This key can be used to authenticate nodes throughout the integration of the system. MANETs provide an environment that has intermittent connectivity with changing topology and there can be no central point of authority. Classic cryptographic methods, such as pairwise keys [1] and public key infrastructures, are not suitable for this environment.

In these circumstances it is not only necessary to provide the network with a secure protocol for generating and distributing keys; the network should also react purposefully to changes in network topology. The CLIQUES protocol suite [4] addresses the membership problem of key agreement in a group setting with highly dynamic group member population. We selected two specific protocols from within CLIQUES: the Group Diffie-Hellman (GDH) and Tree Group Diffie-Hellman (TGDH) algorithms. In order to provide an efficient method of revocation we integrated the key generation protocols in CLIQUES with an implementation of mediated RSA known as the Security Mediator (SEM)[2].

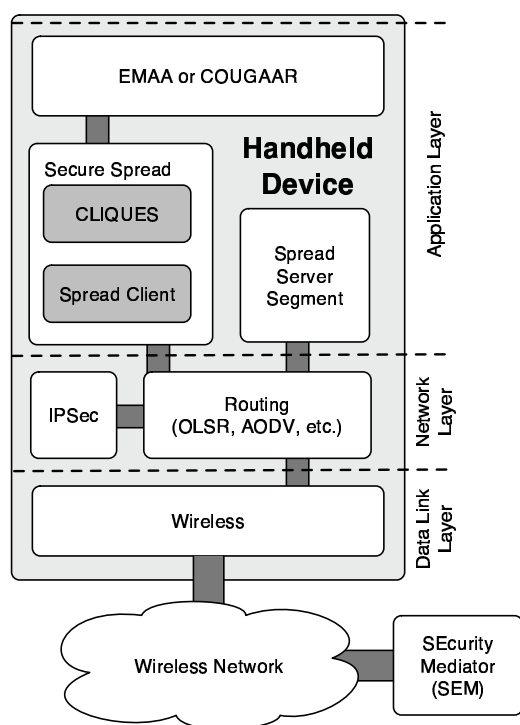


Figure 1: System architecture

The system (Figure 1) employs various security mechanisms at the application layer, the network layer and the data-link layer to ensure that the resultant system is not weakened by integration. The security objectives are to prevent passive attacks (i.e., eavesdropping) and active attacks including man-in-the-middle attacks and damage from malicious insiders. On the application layer the agent library (e.g., [3]) encrypts all agents and agent messages using the group keys generated by Secure Spread. Also on the application layer is the SEM which enables the

Certificate Authority (CA) to revoke any member of any group. On the network layer, IPSec encrypts and decrypts all data packets between hosts. On the data-link layer, at present, WEP/WPA encrypts each datagram.

### 3 Conclusion

We present a scalable system for real-world applications in a mobile environment. This system retains the security of its integrated components and further provides security measures for inter-component interaction. We have tested this system on real handheld PDAs and Tablet PCs on the Philadelphia Area Urban Wireless Testbed (PA-UWT). We have used several testing locations in the Philadelphia area, including urban canyons, urban caves, open areas and public parks, and city streets. These tests have provided diverse environments which demonstrated the versatility and adaptability of our architecture.

### References

- [1] Y. Amir, Y. Kim, C. Nita-Rotaru, and G. Tsudik. On the performance of group key agreement protocols. *Tech. Rep. CNDS 2001-5, Johns Hopkins University Center of Networking and Distributed Systems*, pages 339–408, 2001.
- [2] Dan Boneh, Xuhua Ding, Gene Tsudik, and Chi Ming Wong. A method for fast revocation of public key certificates and security capabilities. In *10th Usenix Security Symposium*, pages 297 – 308, 2001.
- [3] R. P. Lentini, G.P. Rao, J.N. Thies, , and J. Kay. Emaa: An extendable mobile agent architecture. *Fifteenth National Conference on Artificial Intelligence (AAAI '98)*, Madison, Wisconsin, Technical Report WS-98-10: Software Tools For Developing Agents, ISBN 157735 -063-4, 1997.
- [4] M. Steiner, G. Tsudik, , and M. Waidner. Cliques: a new approach to group key agreement. *Proceedings of the Conference on Distributed Computing Systems (IEEE)*, pages 380–387, May 1998.