Consider a disaster situation, a terrorist attack for example, in which a wireless network needs to be formed on an ad hoc basis, without the support of any fixed infrastructure, in order to interconnect all relevant computing and communication devices. The objective is to share information with the highest security possible, since no-one can guarantee that ‘high-tech’ terrorists/attackers won’t try to disrupt or intercept the rescue efforts. However since neither a certification authority nor a secure communication channel exists, attackers have the ability to eavesdrop and tamper with messages transmitted over the air. Additionally, since no Identification Authority is present, group members may easily be impersonated.

In the above scenario, the main problem involves group members establishing a secure wireless network and at the same time eliminating outside threats. Moreover, in the case where a new node arrives and wishes to become a member of an existing group, how can this particular node participate in the group session without distracting the initial group? Having entered the group session, how can this node then gain the same privileges as other group members? And of course, in a more general case where a whole group is formed from scratch, how can the network be extended to incorporate it?

In order to answer the above questions, the Telecommunications and Networks Laboratory (TNL) of FORTH-ICS has introduced a new family of security protocols for wireless ad hoc networks. The security problems addressed by our system are:

- **Contributory key establishment.** An ad hoc network is set when a session key is agreed to by all network entities. This session key is generated through a process where all participating entities contribute equivalently.
- **Secure authentication.** Strong authentication must be derived from a small password.
- **Resilience against attacks during the key formation:**
  - **Forward authentication.** If a malicious party manages to compromise a secure wireless ad hoc network and at the same time eliminating outside threats. Moreover, in the case where a new node arrives and wishes to become a member of an existing group, how can this particular node participate in the group session without distracting the initial group? Having entered the group session, how can this node then gain the same privileges as other group members? And of course, in a more general case where a whole group is formed from scratch, how can the network be extended to incorporate it?

In order to answer the above questions, the Telecommunications and Networks Laboratory (TNL) of FORTH-ICS has introduced a new family of security protocols for wireless ad hoc networks. The security problems addressed by our system are:

- **Contributory key establishment.** An ad hoc network is set when a session key is agreed to by all network entities. This session key is generated through a process where all participating entities contribute equivalently.
- **Secure authentication.** Strong authentication must be derived from a small password.
- **Resilience against attacks during the key formation:**
  - **Forward authentication.** If a malicious party manages to compromise a secure wireless ad hoc network and at the same time eliminating outside threats. Moreover, in the case where a new node arrives and wishes to become a member of an existing group, how can this particular node participate in the group session without distracting the initial group? Having entered the group session, how can this node then gain the same privileges as other group members? And of course, in a more general case where a whole group is formed from scratch, how can the network be extended to incorporate it?

In order to answer the above questions, the Telecommunications and Networks Laboratory (TNL) of FORTH-ICS has introduced a new family of security protocols for wireless ad hoc networks. The security problems addressed by our system are:

- **Contributory key establishment.** An ad hoc network is set when a session key is agreed to by all network entities. This session key is generated through a process where all participating entities contribute equivalently.
- **Secure authentication.** Strong authentication must be derived from a small password.
- **Resilience against attacks during the key formation:**
  - **Forward authentication.** If a malicious party manages to compromise a secure wireless ad hoc network and at the same time eliminating outside threats. Moreover, in the case where a new node arrives and wishes to become a member of an existing group, how can this particular node participate in the group session without distracting the initial group? Having entered the group session, how can this node then gain the same privileges as other group members? And of course, in a more general case where a whole group is formed from scratch, how can the network be extended to incorporate it?

In order to answer the above questions, the Telecommunications and Networks Laboratory (TNL) of FORTH-ICS has introduced a new family of security protocols for wireless ad hoc networks. The security problems addressed by our system are:

- **Contributory key establishment.** An ad hoc network is set when a session key is agreed to by all network entities. This session key is generated through a process where all participating entities contribute equivalently.
- **Secure authentication.** Strong authentication must be derived from a small password.
- **Resilience against attacks during the key formation:**
  - **Forward authentication.** If a malicious party manages to compromise a secure wireless ad hoc network and at the same time eliminating outside threats. Moreover, in the case where a new node arrives and wishes to become a member of an existing group, how can this particular node participate in the group session without distracting the initial group? Having entered the group session, how can this node then gain the same privileges as other group members? And of course, in a more general case where a whole group is formed from scratch, how can the network be extended to incorporate it?

In order to answer the above questions, the Telecommunications and Networks Laboratory (TNL) of FORTH-ICS has introduced a new family of security protocols for wireless ad hoc networks. The security problems addressed by our system are:

- **Contributory key establishment.** An ad hoc network is set when a session key is agreed to by all network entities. This session key is generated through a process where all participating entities contribute equivalently.
- **Secure authentication.** Strong authentication must be derived from a small password.
- **Resilience against attacks during the key formation:**
  - **Forward authentication.** If a malicious party manages to compromise a secure wireless ad hoc network and at the same time eliminating outside threats. Moreover, in the case where a new node arrives and wishes to become a member of an existing group, how can this particular node participate in the group session without distracting the initial group? Having entered the group session, how can this node then gain the same privileges as other group members? And of course, in a more general case where a whole group is formed from scratch, how can the network be extended to incorporate it?

In order to answer the above questions, the Telecommunications and Networks Laboratory (TNL) of FORTH-ICS has introduced a new family of security protocols for wireless ad hoc networks. The security problems addressed by our system are:

- **Contributory key establishment.** An ad hoc network is set when a session key is agreed to by all network entities. This session key is generated through a process where all participating entities contribute equivalently.
- **Secure authentication.** Strong authentication must be derived from a small password.
- **Resilience against attacks during the key formation:**
  - **Forward authentication.** If a malicious party manages to compromise a secure wireless ad hoc network and at the same time eliminating outside threats. Moreover, in the case where a new node arrives and wishes to become a member of an existing group, how can this particular node participate in the group session without distracting the initial group? Having entered the group session, how can this node then gain the same privileges as other group members? And of course, in a more general case where a whole group is formed from scratch, how can the network be extended to incorporate it?
Within this project, we have modified protocols for password authenticated multi-party Diffie-Hellman (DH) key exchange, to make them more resistant against dictionary attacks. Figure 1 presents the node algorithm for finding a partner and performing a DH two-party key exchange. Figure 2 depicts the 2-d case, which will be described below, and Figure 3 depicts the 3-d case of the general d-cube protocol.

In the 2-d case it is considered that node A is a faulty partner. Therefore, in round 1, node B will fail to complete the Diffie-Hellman key exchange with A. However (see Figure 1), instead of remaining idle during this round, node B will perform a new DH key exchange with node C. This exchange will be successfully completed resulting in a new key and at the same time informing that is faulty. Meanwhile, node C has already performed a successful key exchange with node D creating key. Round 1 will be concluded with the creation of the keys and . On the second round, node B will perform a DH key exchange with node D and the key will be created. This key will be the common session key for the entities . Node C can calculate the common session key for itself, since it has all necessary information needed from the previous round. The main point in this scenario is that during the second round node won’t have to perform any DH key exchange with the faulty node A, is being isolated because its neighbors in earlier rounds, than those foreseen by the d-cube algorithm, have performed extra DH key exchanges due to its behavior.

Additionally, we have also introduced new key establishment methods based on elliptic curve cryptography due to its lighter computational requirements, which is important for ad-hoc networks consisting mostly of thin clients. Finally we have proposed new faster protocols for the dynamic case, where the composition of the ad-hoc network changes in time with the arrivals and departures of nodes.

The current project was developed by TNL under the Information Security Program of FORTH-ICS.

Please contact: Ioannis G. Askoxylakis, ICS-FORTH
Tel: +30 2810 391723
E-mail: asko@ics.forth.gr