

Ad-Hoc networks and Broadcast Encryption

Presented by Ash

Introduction

- How to Broadcast to a group of users
 - Certain Schemes.
 - Easiest one is to give each user a key and individually send messages to each users.

Drawbacks:

Long transmissions.
and overhead in computation of encryptions and storage of keys.

K-resiliency is defined as: for a given parameter k the scheme must be resilient to any subset of k users who collude to break the scheme.

Results

- **Assumptions:**
 - The device memory is tamper proof.
 - If the user has to break the system, then he has to perform an exhaustive search of keys or derive a probabilistic model for determine the keys.
 - The privileged set is known. And the number of bits to represent the users is fixed.
 - Each user is assigned an unique key, i.e.. No 2 users picked at random will have the same 2 keys in each of its column.
 - This algorithm does not deal with detection of traitors. It is assumed that there are mechanisms to detect traitors.
- **Advantages:**
 - The user will need to store only one key. Thus aiding in reduced memory requirements.
 - The algorithm is k-resilient, i.e.. Any coalition of k users cannot collude to break the system.
 - Revocations schemes which the most important in combat environment is simple and on-the-fly, hence very effective in this scheme.
 - This algorithm performs well when the privileged set is large.
- **Disadvantages:**
 - As members increase, the rows increase, the matrix grows, thus effecting the transmission rates of the key management block.
 - Max $2^{128} \times 128$ users allowed with this current design.

Model

- Each device is assigned a key of 1×128 column matrix or a vector. Each column is 128 bits; These are known as user-keys. An permutation function is also associated with the device and is stored on the device.
- The key to encrypted in the key management block; it's the repeated encryption of the key using the device keys.
- The key management block is a $(n \times 128)$ column matrix transmitted at the beginning of the transmission.
- The device knows its row position in the matrix. It reads its row, and uses its permutation function to get the column; then uses its user-keys to decrypt the management key from the block.
 - All Columns have to be matched to get the key;

Revocation scheme

- Revocations are simple and on the fly;
- With large number of users, and an hostile environment and sensitive nature of the data and messages, this algorithm provides a effective and easy way to revoke users from the broadcast session.
- Simply, delete the row of the device from the matrix, fill its row with dummy keys, called detractor keys. Thus rendering the device un-usable.