S3-030196

Kc security for the U-TDOA LCS method

SA3#28 - Berlin, Germany

May 6-9, 2003

TruePosition

Introduction

- Purpose of this presentation
  - **Propose encryption technique for the protection of Kc when used for U-TDOA**
  - **Propose physical security measures for the protection of Kc when used for U-TDOA**
- Goal
  - **Agree to suitable security measures**
    - Will be communicated to GERAN
    - Used to specify integrated U-TDOA solution

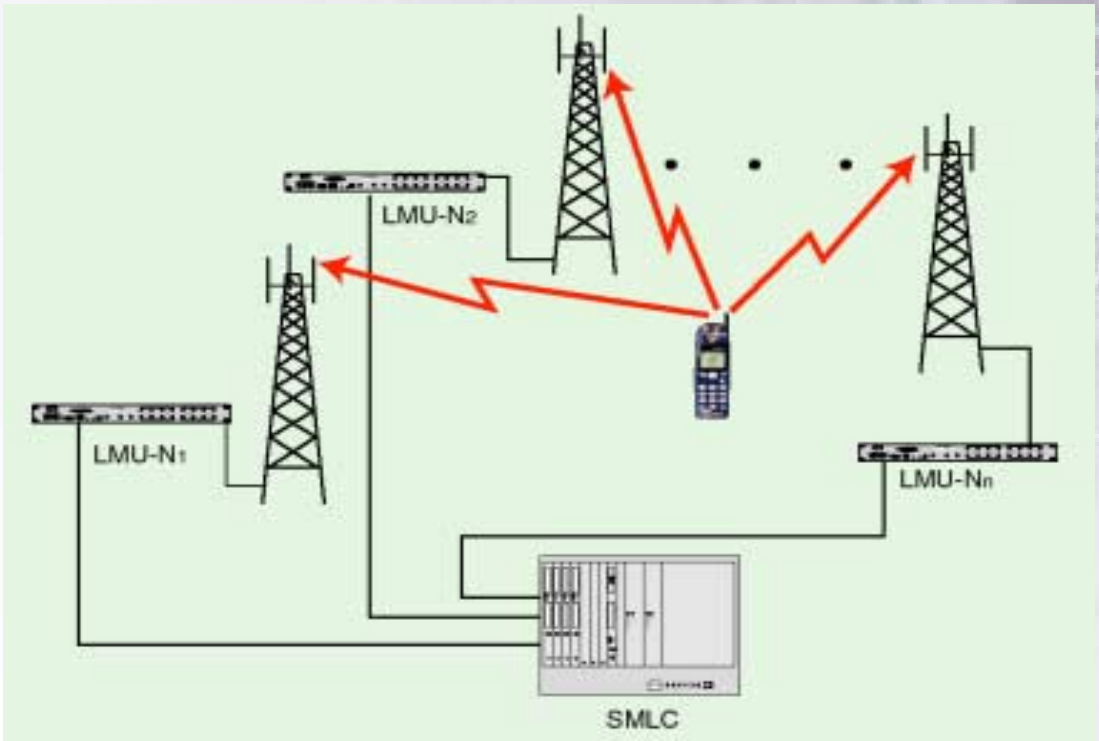
TruePosition

U-TDOA Fundamentals

- Uplink Time Difference Of Arrival (U-TDOA) uses MS transmit energy for location purposes
- Energy from an existing connection or from a dedicated channel (SDCCH or TCH) assigned for location purposes (i.e. previously idle mobile) is used
- The channel information (transmitted bits) is captured at the serving cell and used by the location receivers (LMU) at several other sites to identify the energy associated with the target MS
- The Time Of Arrival (TOA) of the MS signal at each LMU is then used to calculate the position of the MS
- Use of the information bits (actual subscriber or signaling information) between the LMU and the Stand-alone Mobile Location Center (SMLC) is preferable
  - **Provides least errored pattern for correlation which yields the highest performance (accuracy)**
  - **Results in the lowest possible amount of data transported for location purposes**

TruePosition

U-TDOA Architecture



TruePosition

Motivation for the use of Kc

- Higher accuracy, lower latency
  - **The accuracy of a TOA based location method is a function of the energy (bits) captured**
  - **Bit errors increase the amount of energy (bits) that must be captured for the same level of accuracy**
  - **The location system can take advantage of Forward Error Correction (FEC) to correct errored bits by applying the convolutional code**
  - **Decryption must be performed before this can occur**
- Lower impact on network interconnect facilities
  - **The acquisition of the reference information from the serving site and the distribution of the reference information to the cooperating LMUs utilizes the Abis and Lb (SMLC-BSC) interfaces**
  - **By decrypting and decoding the reference information, the volume of this data is reduced by ½ due to the half rate convolutional coding**

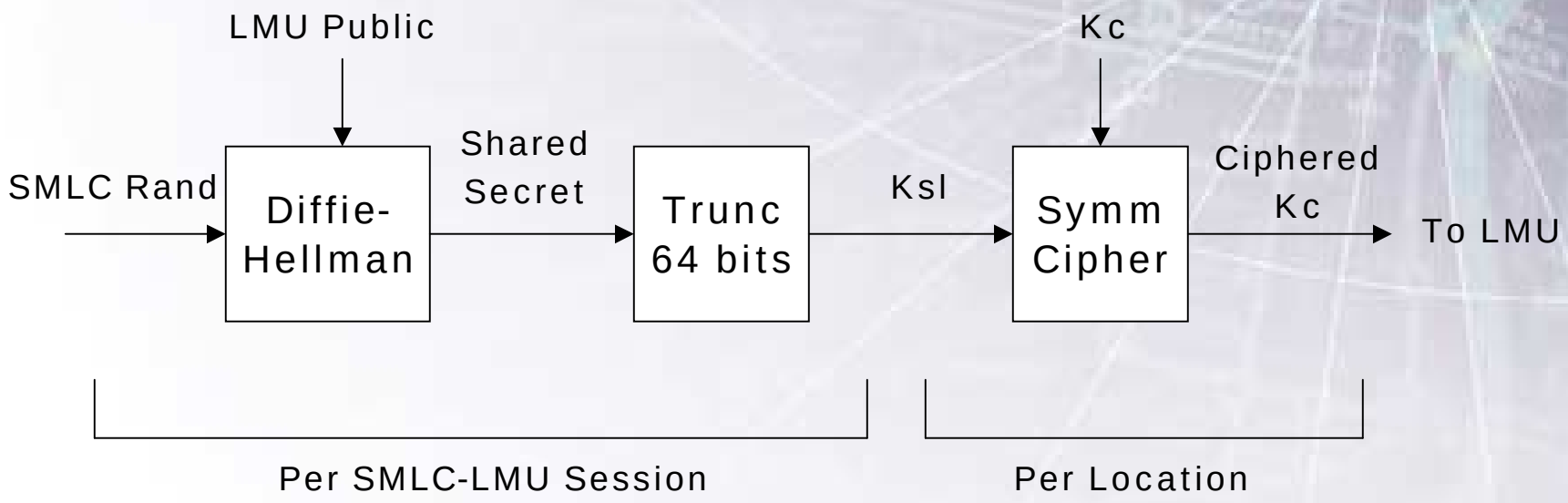
TruePosition

Proposed Kc Protection

- SMLC performs Diffie-Hellman key agreement protocol with each LMU at session establishment time
- Result is a key, Ksl, unique to each SMLC-LMU session
- SMLC encrypts Kc with symmetric encryption algorithm (via Ksl) to send to each LMU
- LMU decrypts Kc with symmetric algorithm via Ksl
- LMU decrypts MS bursts via Kc and recovers MS information bits for correlation
- Ksl kept in SMLC and LMU memory
  - **Never written to disk**

TruePosition

SMLC Perspective



TruePosition

Rationale

- Diffie-Hellman key agreement eliminates need for symmetric key management
  - **Provides unique key per LMU session**
  - **Key agreement computation is significant, so one symmetric key used for many locations**

TruePosition

Topics for discussion

- Physical Security
  - **Co-located LMU and BTS**
    - LMU not externally accessible
    - Kc only stored in memory
  - **Remote LMU (Type B) or Type A LMU (RF interconnect)**
    - Kc only stored in memory
- User data encryption
  - **Less than one second of user data exposed**
  - **Highly unlikely to be meaningful to an attacker**

TruePosition

Conclusion

- Encrypting Kc with unique SMLC-LMU session key maintains MS information privacy
- Kc protected from RF sniffing when sent to type A LMU (RF link)
- Next Steps
  - Communicate conclusions to GERAN
  - GERAN generate LS to SA3 as confirmation
  - Include agreed method in specifications

TruePosition