3GPP TSG SA WG3 Security — S3#32 **S3-040116**
09 - 13 February 2004
Edinburgh, Scotland, UK

Technical Specification Group GERAN **TSGG#18(04)0561**
Meeting #18, Reykjavik, Iceland, 2-6 February 2004

Title: ***Protection of Kc in the Uplink TDOA location method***

Release: Release 6

Source: GERAN

To: SA3

Contact Person:	Andrew Corporation	TruePosition
Name:	Oskar Magnusson	Robert Gross
Tel. Number:	+1 703 860 9700 x195	+1 610 680 1119
E-mail Address:	oskar.magnusson@andrew.com	rlgross@trueposition.com

Overview

The purpose of this liaison statement is to request SA3's recommendation for the protection of Kc during the transfer of the encryption key from the SMLC to the LMUs during the U-TDOA location process.

Use of Kc to enable location of AMR connections, increase accuracy and reduce data volume

It is necessary to decrypt each burst of an AMR based connection in order to locate the MS using the U-TDOA location method because the AMR vocoder rate may be continuously changed using in-band signalling (RATSCCH).

The ability to decrypt each burst of a target connection also enables significant efficiencies that increase capacity, reduce latency and improve the accuracy of the U-TDOA location method. These aspects were discussed in SA3 #27 and #28 in documents S3-030038 and S3-030196 respectively. These documents are attached for clarity.

Exposure of Kc

The use of Kc for U-TDOA LCS exposes the Kc on the links between the SMLC and the LMUs (location receivers). These links are coincident with the BSC-BTS links.

The GERAN specifications currently limit the provision of Kc to emergency services only. In GERAN #18, a proposal has been made to remove this restriction so that the Kc could be used for all U-TDOA location purposes.

2. Actions for the SA3:

GERAN seeks SA3's security recommendations when using the Kc for the purposes described above.

3. Date of Next TSG-GERAN Meetings:

Meeting	Date	Location
G2#18 bis	22-26 March, 2004	Phoenix, USA
GERAN#19	19-23 April, 2004	Cancun, Mexico

3GPP TSG SA WG3 Security — S3#26 **S3-030038**
25 - 28 February 2003
Sophia Antipolis, France

Technical Specification Group GERAN **TSGG#13(03)0451**
Meeting #13, San Antonio, USA, 3-7 February 2003

Title: ***Use of Kc in the Uplink TDOA location method***

Release: Release 6

Source: GERAN
To: SA3

Contact Person: TruePosition
Name: Rhys Robinson
Tel. Number: +1-610-680-2119
E-mail Address: Rrobinson@TruePosition.com

Overview

U-TDOA requires the transfer of information between the LMU (typically co-located with the BTS) and the SMLC (typically co-located with the BSC).

The LCS network architecture, as defined in 3GPP TS 43.059, transfers data between the SMLC and LMU via the BSC and BTS.

The purpose of this liason statement is to describe the transfer of the Kc encryption key and algorithm version to the LMUs during U-TDOA location, so that SA3 may advise TSG GERAN on any associated security impacts or risks.

Use of Kc to increase accuracy and reduce data volume

The U-TDOA methodology determines a MS location by capturing uplink RF bursts at multiple locations, establishing the Time Of Arrival (TOA) of these bursts as referenced to a highly accurate common clock and calculating the location by trilateration of the TOA values. In practice 20 to 100 bursts are required, depending on the desired level of accuracy and 10 to 20 Location Measurement Units (LMU) will participate in a location determination.

The general U-TDOA process can be summarized as follows:

- The BSC provides the SMLC with the identity of the serving cell as well as the time and frequency information necessary to identify the transmissions of the target MS
- The SMLC determines the appropriate LMUs for the location determination based on the cell identity, MS power and the required accuracy level.
- The SMLC tasks these LMUs to begin capturing and storing the uplink transmissions of the target MS.
- As directed by the SMLC, the information in 20-100 bursts (depending on the accuracy requirement) is captured at the visited LMU (primary LMU) and transferred to the SMLC
- The SMLC distributes this reference information to all LMUs participating in the location determination
- These Cooperating LMUs (Co-Ops) use the reference information to determine the TOA value at their location by correlating the reference information to the data previously captured and stored in their buffers
- This TOA information is returned to the SMLC
- The SMLC uses this TOA information to calculate the MS location

The resulting accuracy depends on the quality of the reference information used by the LMU to identify the transmissions from the target MS. The bit errors that normally occur during RF transmission can be corrected by decoding the bursts from the serving cell that will be used as the reference information. The decoding process invokes the Forward Error Correction (FEC) inherent in the convolutional coding. Using the most accurate possible reference information yields the highest correlation index in the LMUs that provide the most accurate TOA results. This increased accuracy is only

possible if the reference burst in the serving cell can first be decrypted so that the subsequent convolutional decoding can be performed.

Also the lowest possible number of bits can be transferred between the LMU and the SMLC by reducing each burst to the core 57 bits of user/signalling data (CS-1). Without the ability to decrypt and decode at the serving cell, all 114 user bits in each burst must be transferred between the SMLC and the LMU. This also requires that all LMU are provided with the Kc so that the reference information can be encoded and encrypted for correlation to the target MS burst information received by each LMU.

Alternately, only the LMU in the serving cell could receive the Kc, perform the convolutional decoding to correct bit errors, encode, encrypt and transfer the resulting encrypted reference information to the SMLC. This approach has the advantage of providing the minimum exposure to Kc but has the disadvantage of requiring the transfer of all 140 payoad bits per burst.

The lower volumes of data transferred between the LMU and SMLC by utilizing the Kc also leads to improved latency (lower transfer time) and capacity.

Exposure of Kc

The use of Kc for U-TDOA LCS exposes the Kc on one additional link; the Lb interface between the SMLC and the BSC.

2. Actions for the SA3:

GERAN seeks SA3's analysis of security impacts when using the Kc for the purposes described above.

3. Date of Next TSG-GERAN Meetings:

Meeting	Date	Location
G2#13 bis	10-14 March, 2003	Winchester, UK
GERAN#14	7-11 April, 2003	Munich, Germany

S3-030038

Use of Kc in the Uplink TDOA location method

In reference to GERAN#13 LS TSGG#13(03)0451

TruePosition

Introduction

- Purpose of this presentation
  - **Provide overview of Uplink Time Difference Of Arrival (U-TDOA) location method**
  - **Describe advantages of using Kc with U-TDOA**
    - Performance advantage
    - Efficient use of system resources
  - **Discuss liaison statement**
- Goal
  - **GERAN seeks SA3's advice on the security impact of using the Kc for the described purpose.**

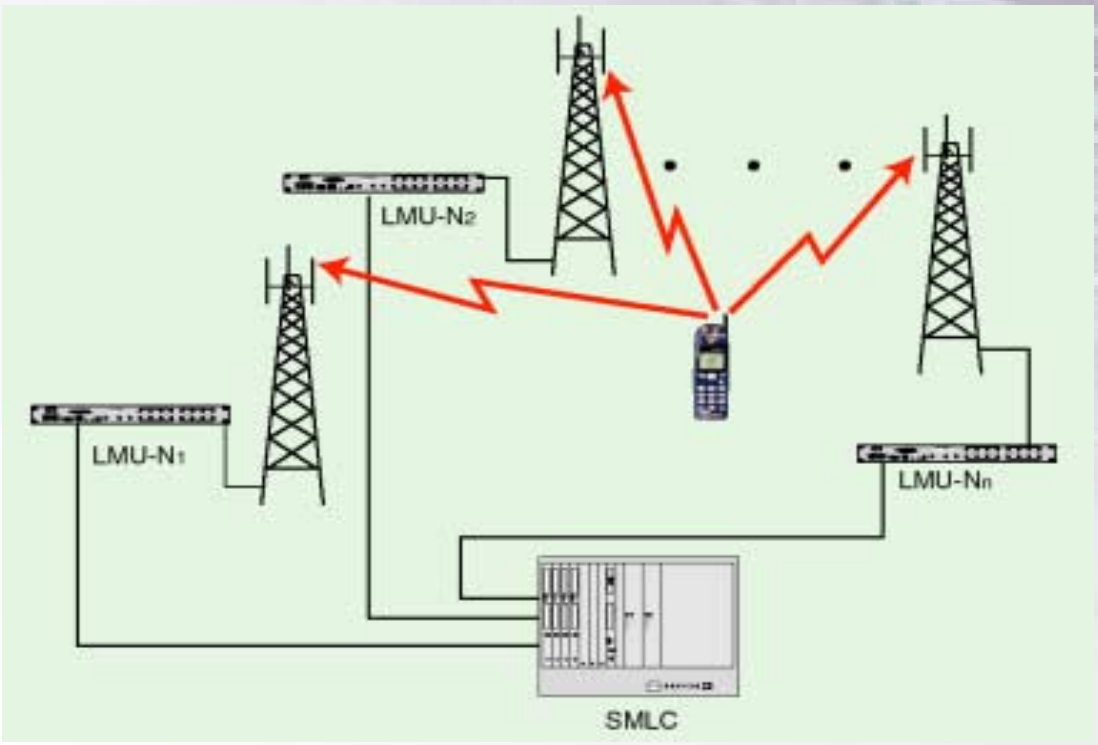
TruePosition

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

U-TDOA Signaling; LMU based TOA analysis

1. Following receipt of the Perform Location Request message from the BSC, the SMLC asks the BSC for MS channel assignment information using the U-TDOA Request message
2. The BSC provides the channel assignment information in the U-TDOA Response message
3. The SMLC uses the channel assignment information to task the cooperating LMUs (usually 10-20 LMU) to begin capturing and buffering RF information
4. The MS continues to transmits bursts on the SDCCH or TCH
5. The SMLC interrogates the LMU at the serving cell for the contents and timing of 20 to 100 bursts, depending the desired level of accuracy. This is the reference information

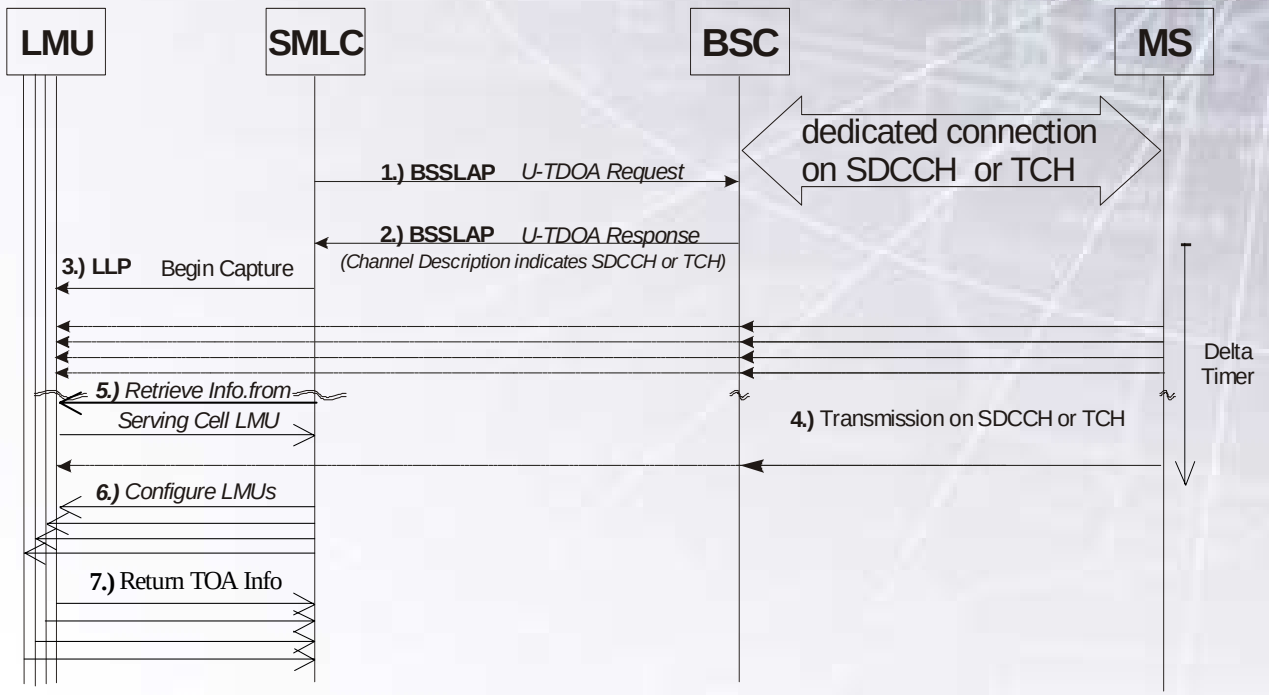
TruePosition

U-TDOA Signaling; LMU based TOA analysis

6. The SMLC distributes the reference and timing information information to all LMU participating in the location determination
7. The LMU correlate the RF information stored in their buffers to the reference information in order to determine the TOA.
8. The SMLC interrogates the LMU for their TOA value and uses this information to calculate the MS position

TruePosition

U-TDOA Signaling; LMU based TOA analysis



TruePosition

Effect of errors on TOA performance

- 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
  - **Errors in the reference information reduce the correlation coefficient between the captured RF energy and the reference information.**
- The formula for the effect of bit errors on the correlation integration time is:

$$T_1/T_0 = 1/(1 - 2*BER)^2$$

where: T_1= integration time with errors

T_0= integration time without errors

TruePosition

Effect of errors on TOA performance

- For 1% BER
  - $T_1/T_0 = 1.041$
- For 5% BER
  - $T_1/T_0 = 1.235$
- For 10% BER
  - $T_1/T_0 = 1.5625$
- As the BER increases, more burst must be captured for a given level of accuracy
  - **1% BER requires only 4% more bursts to obtain the non-errored level of accuracy**
  - **5% BER requires 23% more bursts to obtain the non-errored level of accuracy**
  - **10% BER requires 56% more bursts to obtain the non-errored level of accuracy**
- This could impact RF resource availability in systems with a high level of location activity

TruePosition

Use of Kc to improve performance

- For example, a location accuracy requiring 60 bursts in an error free environment would require the following volume of reference information from the serving cell without error correction:
  - **60 error free bursts x 1.04 (T_1/T_0 for 5% BER) = 62.4 -> 63 bursts**
  - **60 error free bursts x 1.23 (T_1/T_0 for 5% BER) = 73.8 -> 74 bursts**
  - **60 error free bursts x 1.56 (T_1/T_0 for 10% BER) = 93.6 -> 94 bursts**
- The location system can take advantage of Forward Error Correction (FEC) to correct errored bits by applying the convolutional code
- The FEC associated with the convolutional code will typically yield less than a 1% BER
- Decryption must be performed before this can occur

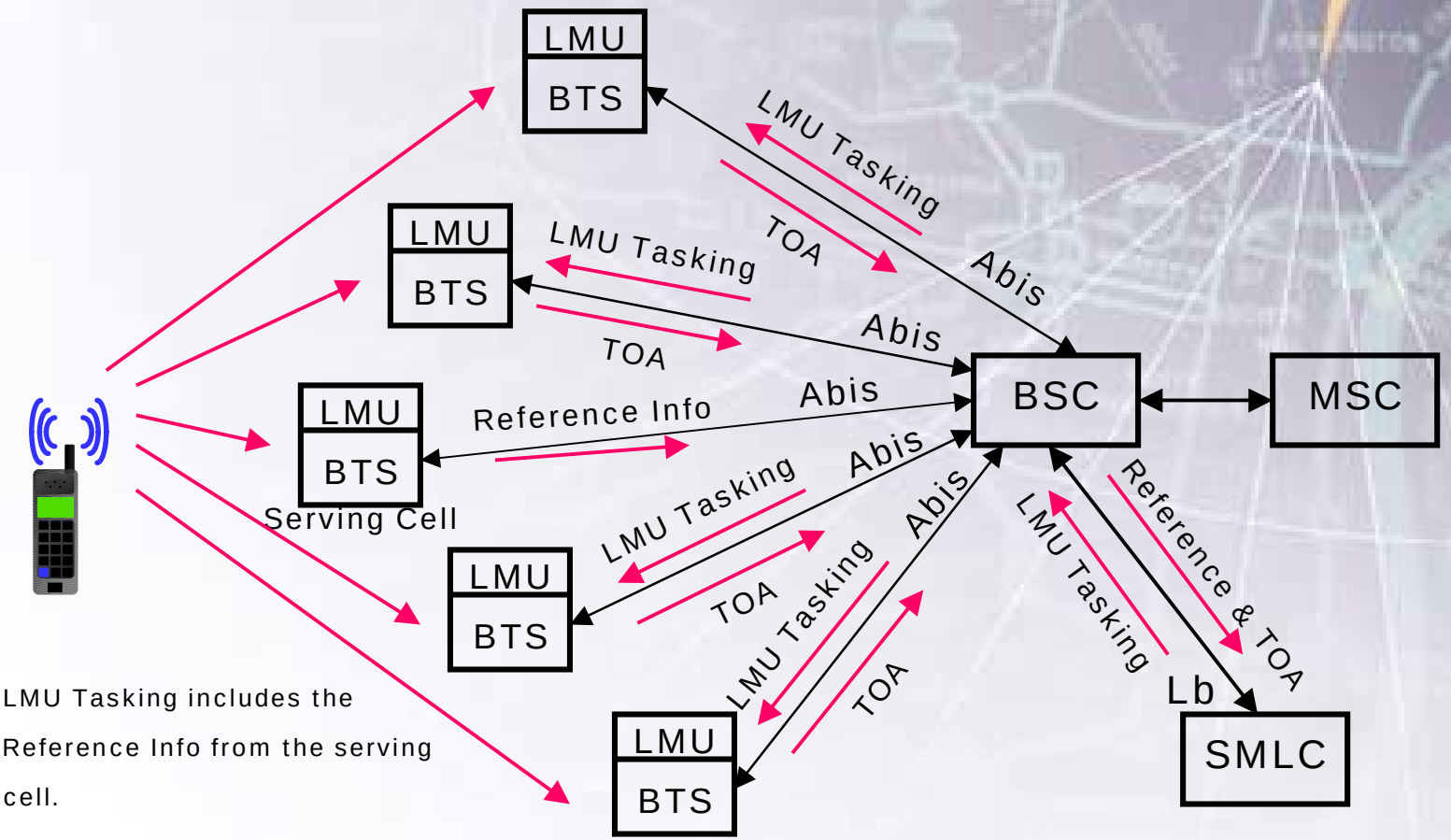
TruePosition

Use of Kc to reduce data volume

- 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
- In order to derive the RF signature, each co-operating LMU must recode, encrypt and modulate the reference information
- System capacity can be maximized, latency minimized and the volume of data transiting the BSS infrastructure can be reduced by decrypting and decoding
- Each LMU would require the Kc for this functionality

TruePosition

U-TDOA Information Flow Overview



Notes:

1. LMU Tasking includes the Reference Info from the serving cell.
2. LMU = LCS Measurement Unit
3. TOA= Time Of Arrival

TruePosition

Use of Kc to reduce data volume

Location related data transport, per location event	Number of bursts for same accuracy	Reference Info (LMU to SMLC)		LMU Tasking for 15 Co-Op LMU	
		On Abis	On Lb	On Abis	On Lb
With decryption and decoding	60	3420	3420	3420	51.3k
5% BER (without decryption or decoding)	74	8436	8436	8436	126.54k
10% BER (without decryption or decoding	94	10.716k	10.716k	10.716k	160.74k

Notes:

1. Message formatting and overhead is assumed to be the same for both methods
2. 60 bursts of reference information and 15 cooperating LMU are assumed for this calculation
3. 57 bits per burst are transported with Kc, 114 bits per burst without Kc

TruePosition

Security Risks discussed at GERAN

- Kc exposed on the Lb interface
  - **SMLC is usually at the same location as the BSCs and is in a controlled environment**
  - **The Lb interface does not utilize subscriber identifiers (IMSI/TMSI)**
    - SMLC identifies user by the SCCP connection identifiers
    - Mapping the Kc to a particular MS would be difficult
- The Lb interface will expose unencrypted user information
  - **Segments of subscriber information are short (fractions of a second in duration) and do not contain subscriber identifiers**
  - **The SMLC and LMU have no capacity to demodulate user information and provide it to an external interface**
- Type A LMU (connected to SMLC via RF) expose the Kc and unencrypted subscriber information
  - **The air interface between the Type A LMU and the serving BTS is encrypted**

TruePosition

Conclusion

- Kc is exposed on an additional interface (Lb) but the risk is mitigated by:
  - **Subscriber identity is not known**
  - **The SMLC and LMU are typically located in controlled environments**
  - **The Kc is not retained by either the SMLC or the LMU**

- Significant advantages can be realized
  - **Lower impact on RF resources for a given level of accuracy (QoS) and volume of location activity**
  - **Lower impact on interconnect facilities (SMLC <-> BSC <-> BTS <-> LMU)**

TruePosition

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

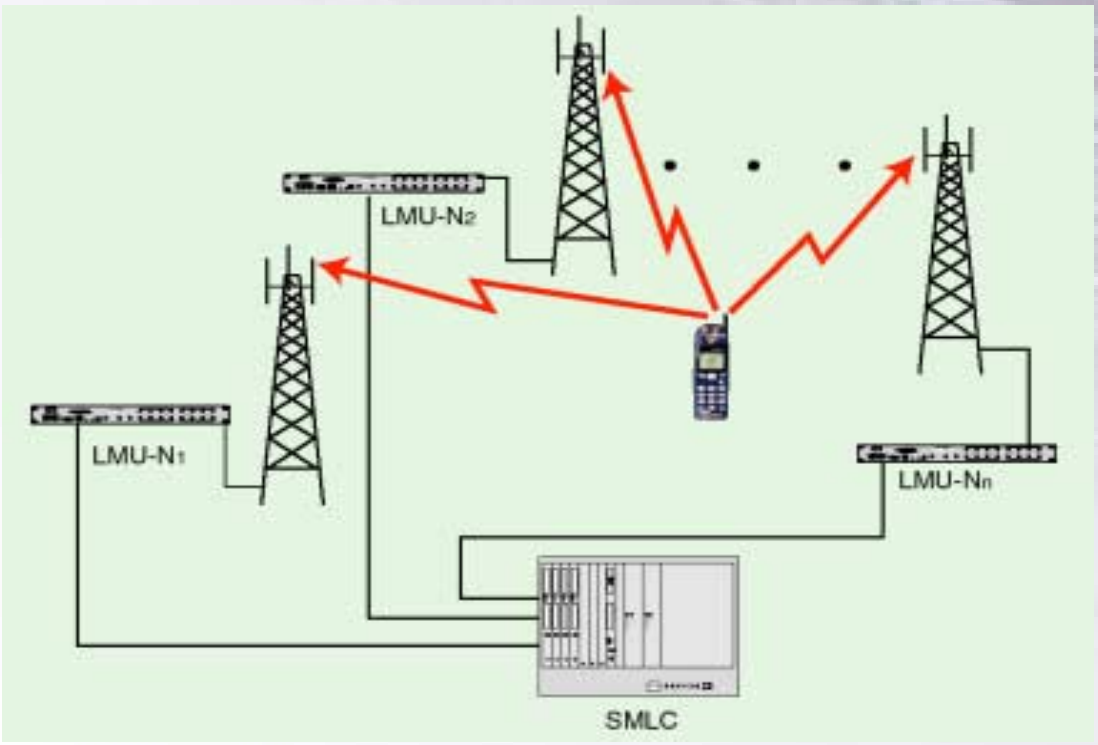
TruePosition

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**

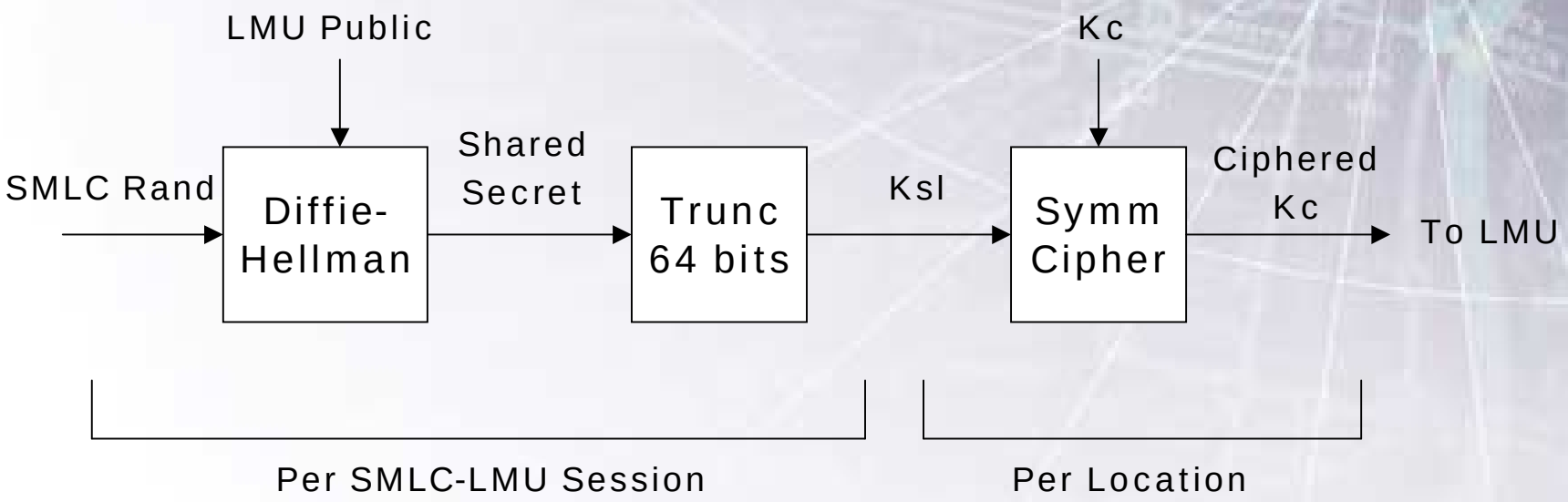
TruePosition

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