中国移动
China Mobile

Signaling Protocol Security between Different Network

China Mobile

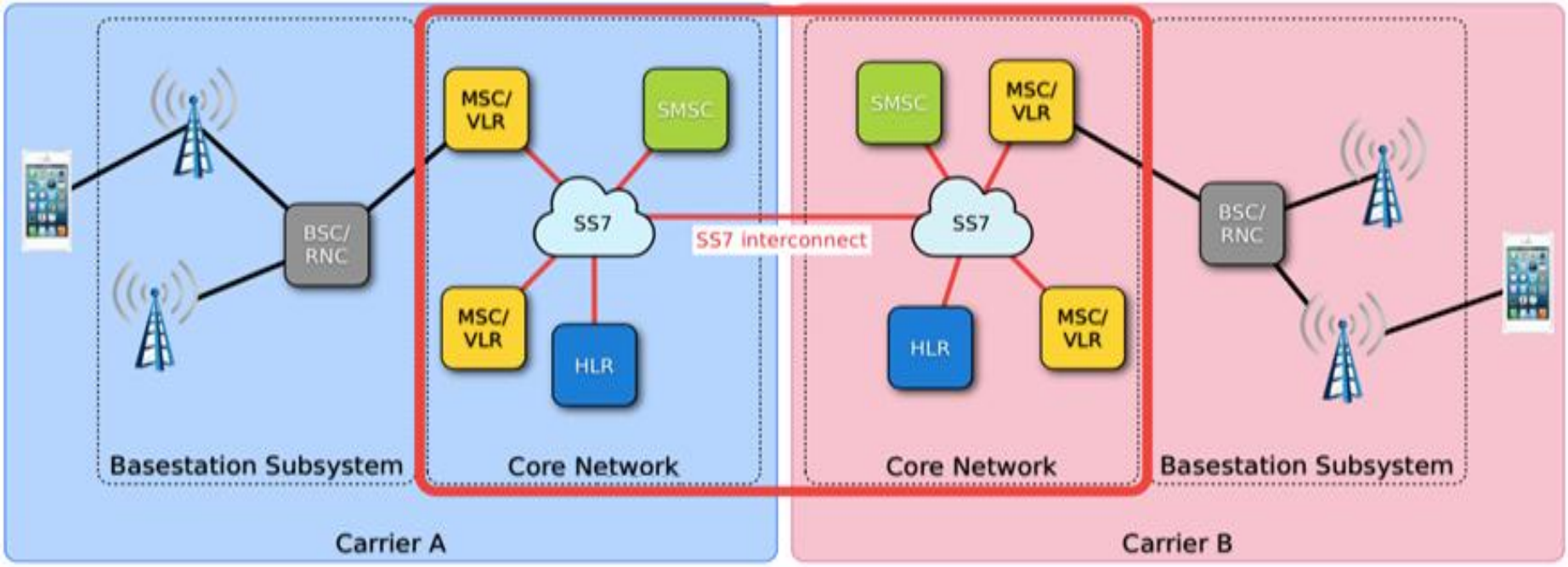
www.10086.cn

Content

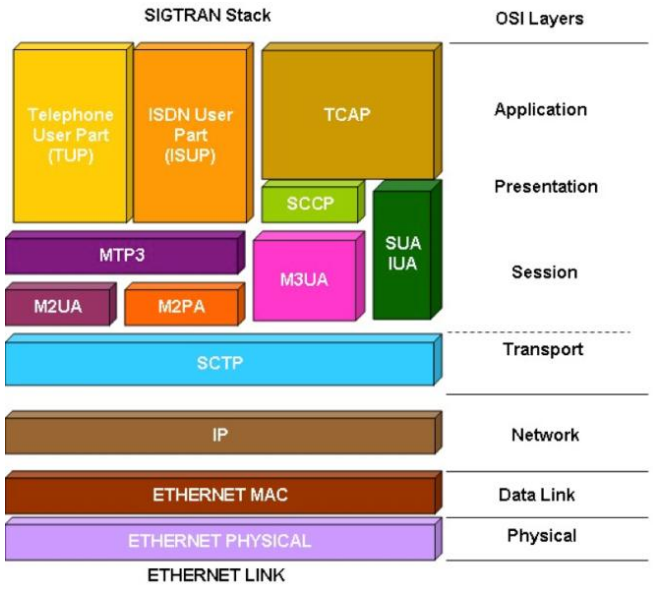
- Reason of interconnection security risk
- Evolution of interconnection protocols
- Common signaling attack scenarios
- China Mobile's experience in detection methods
- Use case of detection method
- High risk signaling of interconnection

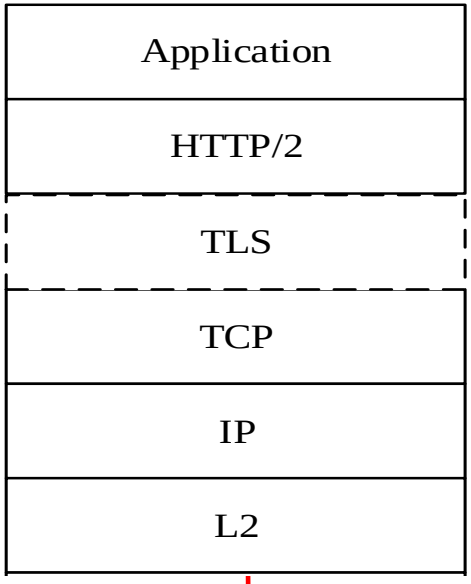
Reason of interconnection risk

At the beginning of SS7/Diameter signaling design, identity authentication mechanism was not considered. Since there is no identity authentication, once the attacker accesses the signaling system, the attacker can send malicious SS7/Diameter signaling to other operators, and the receiver operator will not identify the source and the intention of the signaling.



Evolution of interconnection protocols

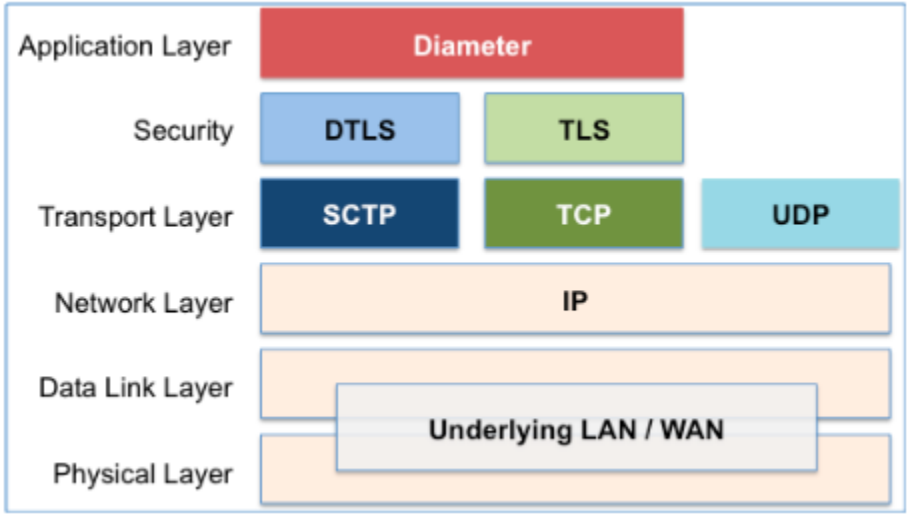




2/3G

4G

5G

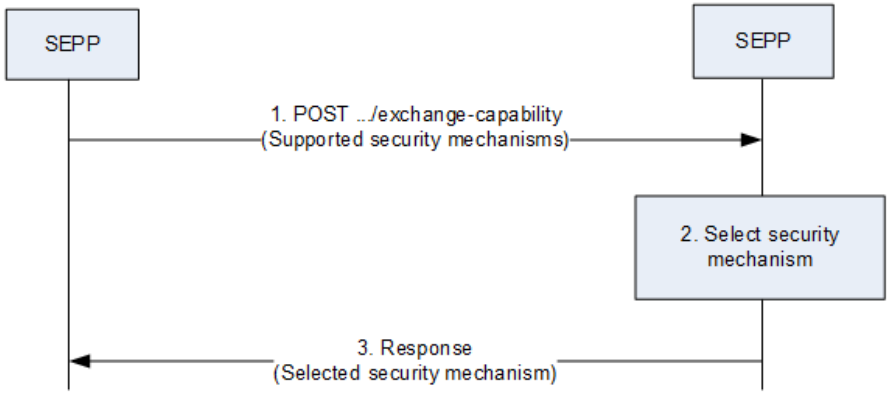


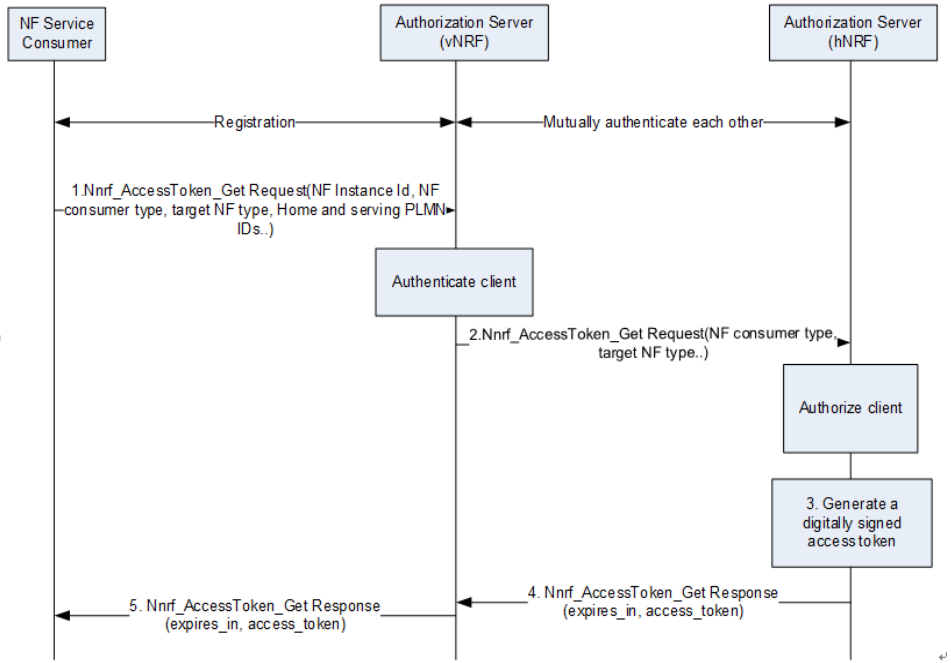
Evolution of interconnection protocols

5G interconnection security mechanism

- TLS/ALS
- Token based authorization

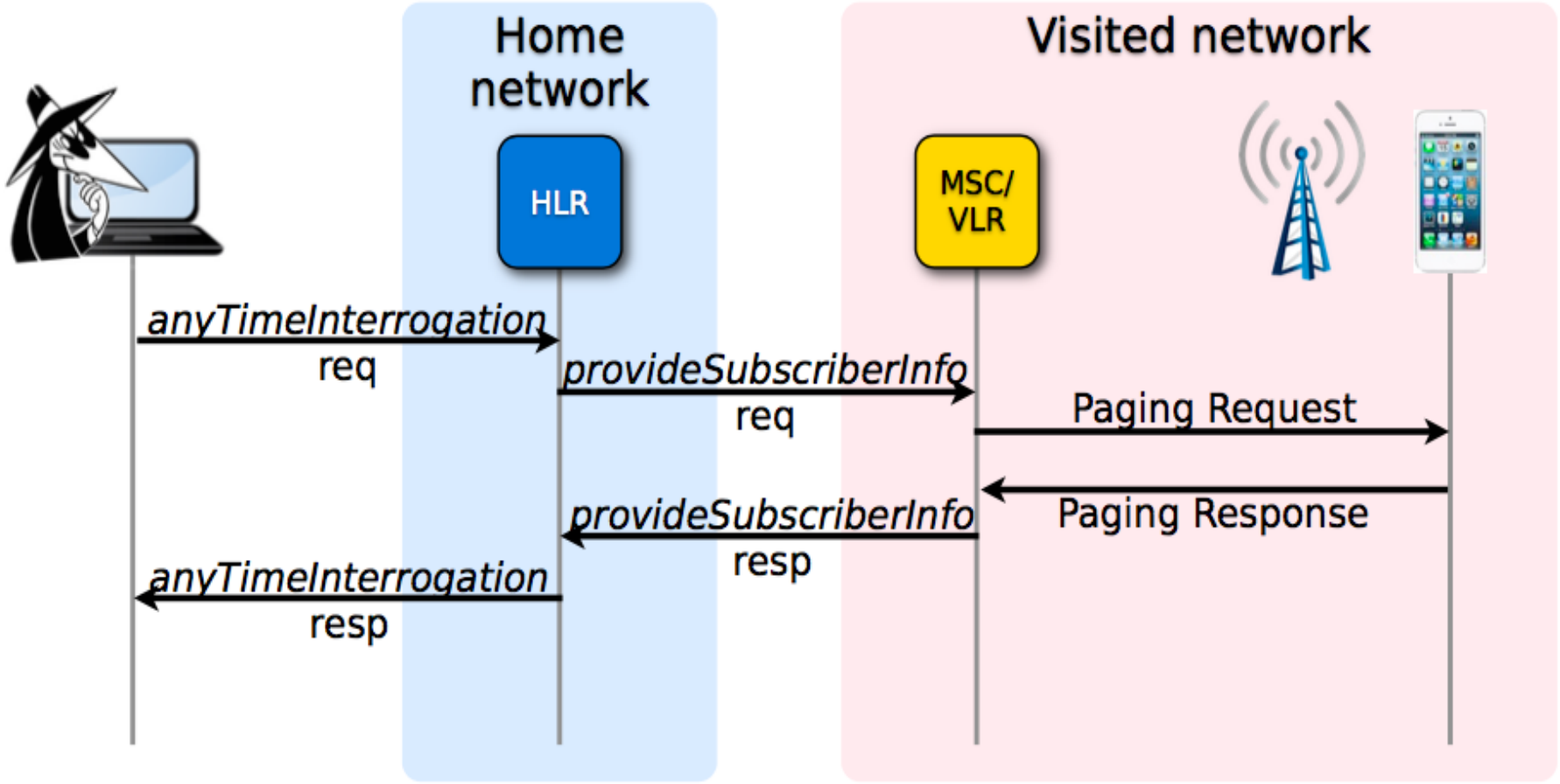
N32 protection mechanism	Description
Mechanism 1	N32 Application Layer Secuity
Mechanism 2	TLS
Mechanism n	Reserved





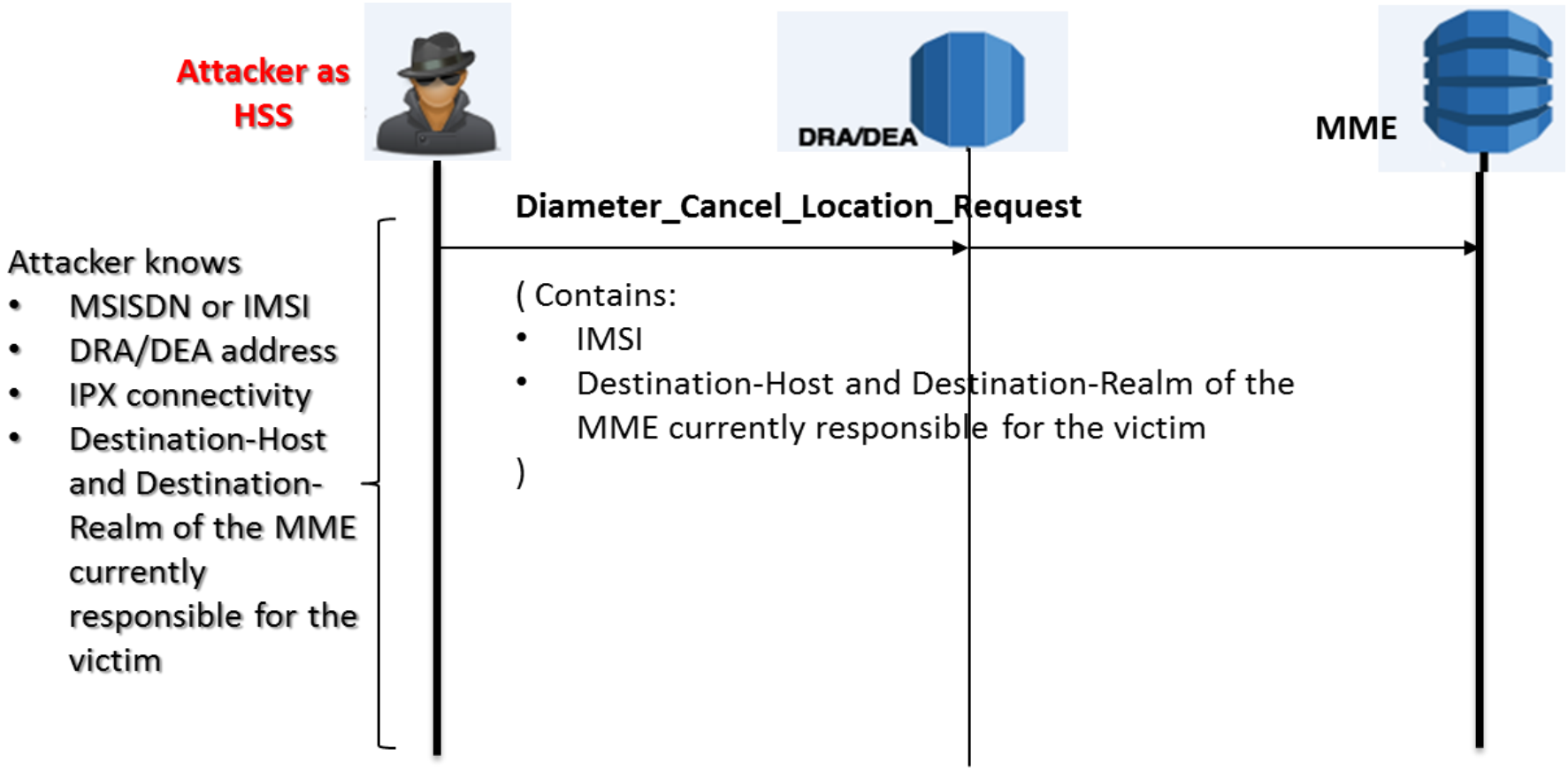
Attack scenario——Illegal localization

The attacker can obtain the user's current location information by sending an ATI message through ISTP.



Attack scenario——Denial of Service

The attacker imitates the HSS to send CLR messages to the MME/SGSN and deletes the user from the serving MME/SGSN, which can result the user in an unreachable state, interrupt the user data session, and fail to receive SMS.

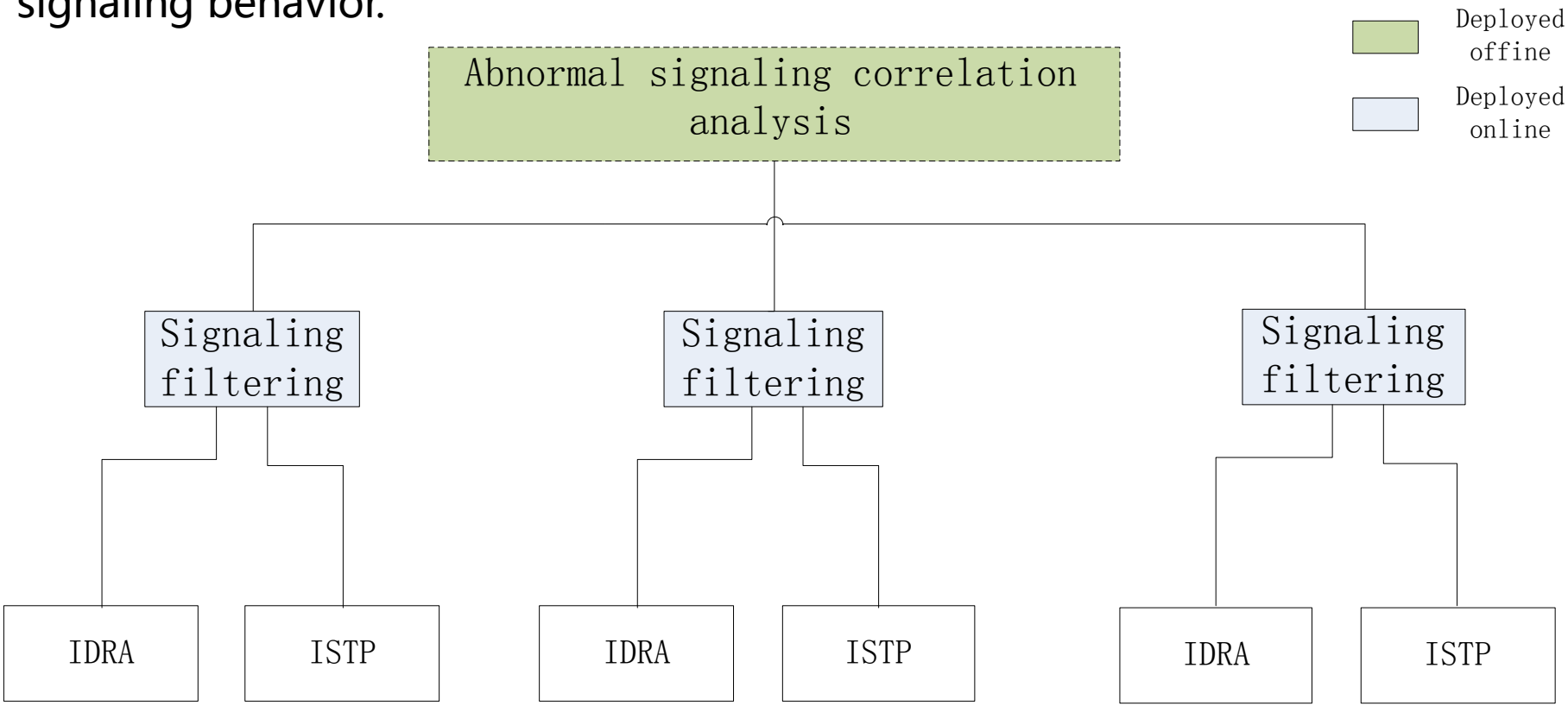


Detection Method—Architecture

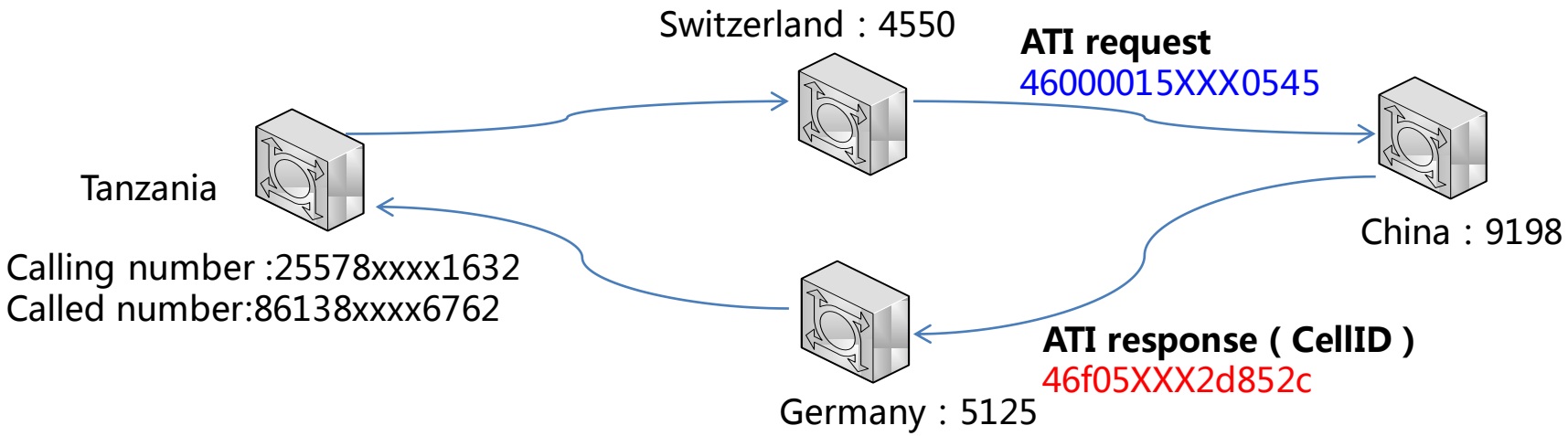
The detection method is composed of two parts: signaling filtering function and abnormal signaling correlation analysis function.

The signaling filtering function adopts online deployment to realize the identification and detection of illegal signaling according to the strategy;.

The abnormal signaling correlation analysis function adopts offline deployment. For abnormal signaling or attack events that cannot be discovered in real time, it can provide comprehensive analysis of abnormal signaling behavior.



Use case of illegal localization



Process of ATI illegal localization：

(1) The signaling point in Tanzania has obtained the IMSI corresponding to the number 86138xxxx6762 of China Mobile: **4600015XXX0545;**

(2) The calling number **25578xxxx1632** initiates ATI request signaling for IMSI: **46000015XXX0545**;

(3) The signaling is forwarded to China Mobile through the Swiss signaling link;

(4) China Mobile responds to CellID: 46f05XXX2d852c;

(5) The ATI response message is sent to Tanzania through the China-German signaling link.

Use case of illegal localization

MAP(ati/imsi:46000015XXX0545)

TCAP(otid: 2bdeee3a)

SCCP(CdPA:86138XXXX6762,CgPA:25578XXXX16322)

MTP3(DPC:9198,OPC:4550)

ATI request signaling

- MTP3

DPC：9198

Country: China (People's Republic of)
Signalling Point Name: Guangzhou ISC
Signalling Point Operator: China Mobile

OPC：4550

Country: Switzerland (Confederation of)
Signalling Point Name: Basel
Signalling Point Operator: Belgacom International Carrier

- SCCP

CdPA（SSN：HLR/GT：86138XXXX6762）

Country Code: 86 China (People's Republic of)
Carrier: China Mobile

CgPA（SSN：MSC/GT：**25578XXXX16322**）

Country Code: 255 Tanzania (United Republic of)
Carrier: Airtel (T) Ltd

- TCAP(otid: 2bdeee3a)
- MAP

opCode: anyTimeInterrogation
subscriberIdentity: imsi（46000015XXX0545）

MAP(ati/cellGlobalIdOrServiceAreaId:46f05XXX2d852c)

TCAP(dtid: 2bdeee3a)

SCCP(CdPA:25578XXXX16322,CgPA:861381XXX000)

MTP3(DPC:5125,OPC:9198)

ATI response signaling

- MTP3

DPC：5125

Country: Germany (Federal Republic of)
Signalling Point Name: Frankfurt Stand Alone STP/SPR
Signalling Point Operator: Deutsche Telekom AG

OPC：9198

Country: China (People's Republic of)
Signalling Point Name: Guangzhou ISC
Signalling Point Operator: China Mobile

- SCCP

CdPA（SSN：MSC/GT：25578XXXX16322）

Country Code: 255 Tanzania (United Republic of)
Carrier: Airtel (T) Ltd

CgPA（SSN：HLR/GT：861381XXX000）

Country Code: 86 China (People's Republic of)
Carrier: China Mobile

- TCAP(dtid: 2bdeee3a)
- MAP

opCode: anyTimeInterrogation
cellGlobalIdOrServiceAreaIdFixedLength: 46f05XXX2d852c

SS7 signaling examples

Sender	Receiver	Messagse	risk
GMSC	HLR	SRI(SendRoutingInfo)	Location leakage
HLR	VLR	PSI(ProvideSubscriberInfo)	Location leakage
gsmSCF	HLR	ATI(AnyTimeInterrogation)	Location leakage
GMLC	VMSC	PSL(ProvideSubscriberLocation)	Location leakage
HLR	VLR/SGSN	cancelLocation	Denial of service
HLR	VLR/SGSN	DSD(deleteSubscriberData)	Denial of service

Diameter signaling examples

Sender	Receiver	Message	Risk
HSS	MME	IDR(Insert Subscriber Data Request)/IDA(Insert Subscriber Data Answer)	Location leakage
MME	HSS	AIR(Authentication Information Request)/AIA(Authentication Information Answer)	Authentication vector leakage
MME	HSS	ULR(Update Location Request)	Denial of service
HSS	MME	IDR(Insert Subscriber Data Request)	Denial of service
HSS	MME	CLR(Cancel Location Request)	Denial of service
MME	HSS	Purge UE Request	Denial of service
HSS	MME	DSR(Delete Subscriber Data Request)	Denial of service
HSS	MME	NOR(Notification Request)	Denial of SMS service
HSS	MME	RSR(Reset Request)	Denial of service

5G signaling examples

Sender	Receiver	Message	Risk
AMF	UDM	3GppRegistration Non3GppRegistration	Malicious NF register
SMF	UDM	3GppRegistration	Malicious NF register
SMSF	UDM	3GppSmsfRegistration Non3GppSmsfRegistration	Malicious NF register
UDM	AMF	ProvideLocationInfo	Location leakage
AMF	SMSF	SendSMS	Denial of service
NEF	UDR	QueryAuthSubsData	Subscription message leakage

中国移动
China Mobile

Thank you !