# Security Issues of 4G Core Network

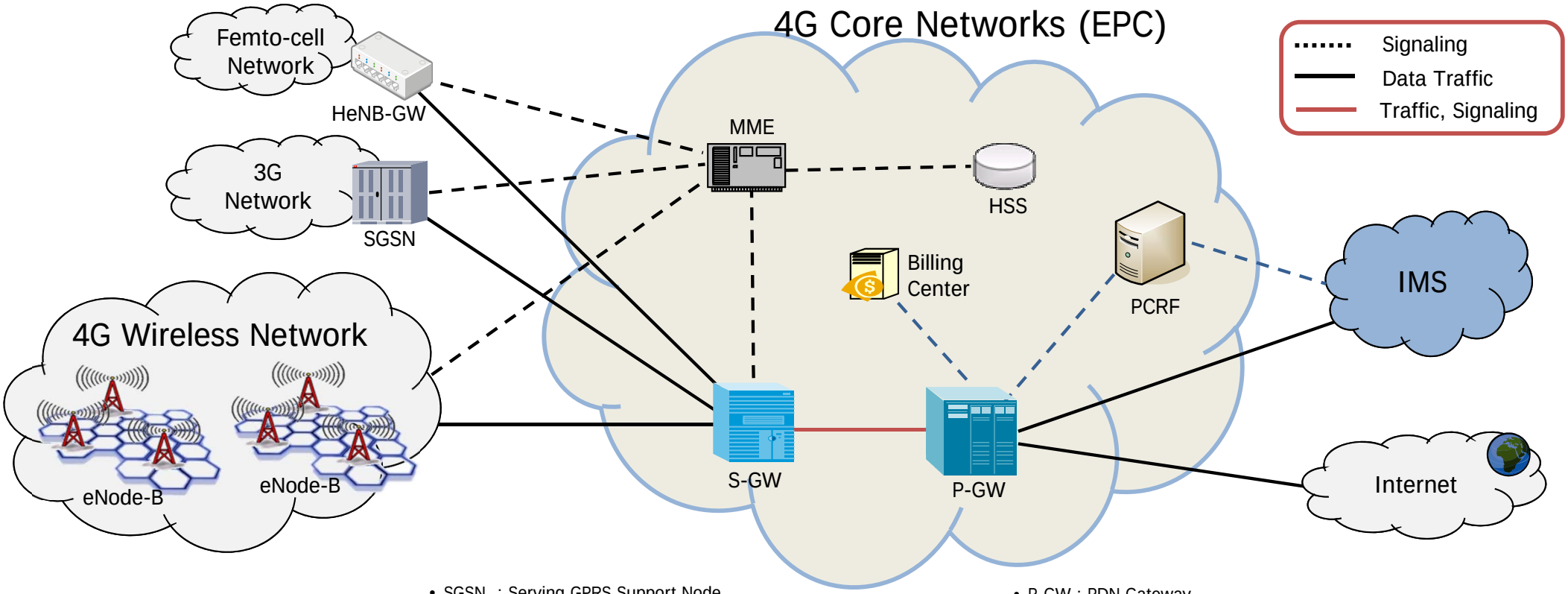

## Korea Internet Security Center

### Chaetae Im


# Table of Contents

# 1. Overview – 4G Mobile Network

- **4G Mobile Network is the mobile communication infrastructure that has evolved from 3G and supports high-speed data transfers**
  - 4G Network is a wireless network (E-RAN) that manages User Equipment (UE) and wireless resources.
  - It consists of core networks (EPC) that process data and handle authentication & billing.
  - The segment between UE and E-RAN is wireless, and the segment after E-RAN is the All-IP-based wired that is linked with 3G and Femto-cell networks.



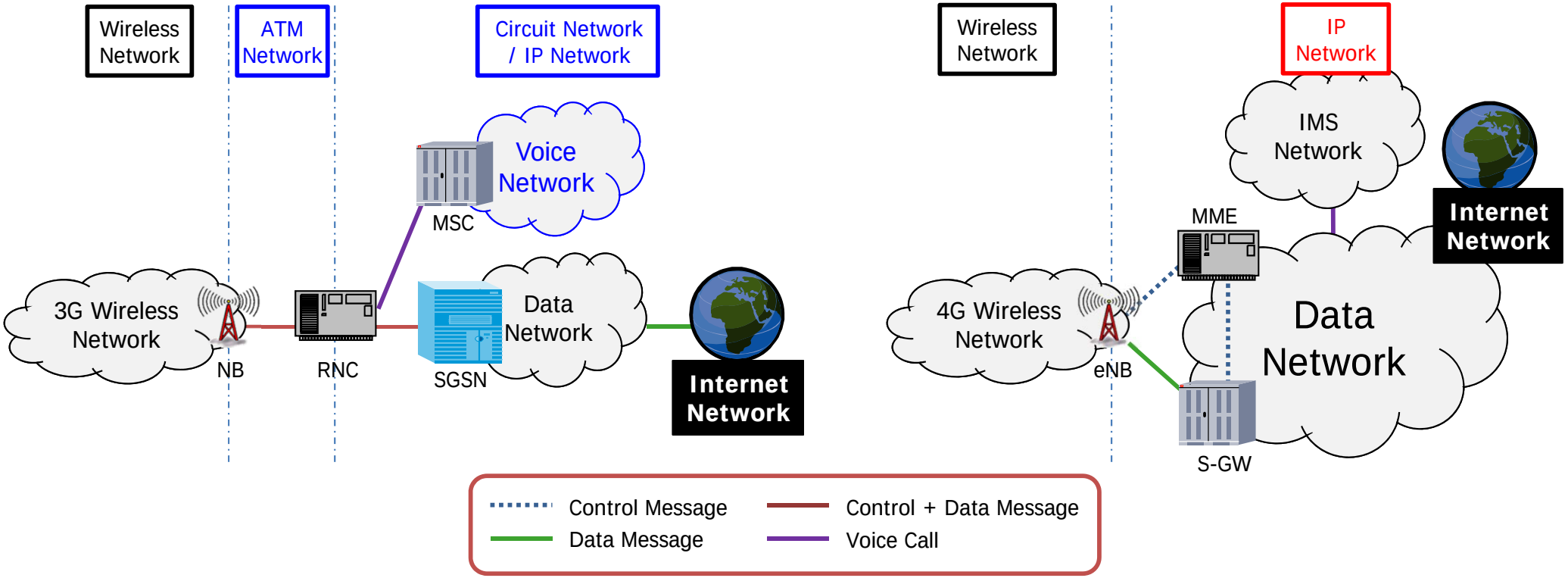

- SGSN : Serving GPRS Support Node
- HSS : Home Subscriber Server
- MME : Mobility Management Entity
- S-GW : Serving Gateway

- P-GW : PDN Gateway
- PCRF : Policy & Charging Rule Function
- HeNB-GW : Home eNodeB Gateway
- EPC : Evolved Packet Core

# 1. Overview – Comparison of 3G & 4G Mobile Networks

| Type | 3G Mobile Network | 4G Mobile Network |
|---|---|---|
| Message Delivery Path | The control & data message delivery paths match. | The control & data message delivery paths are different. |
| Network | ATM + IP + Circuit-based Network | All-IP-based Network |
| Voice Network (Circuit Network) | Yes | No (Integrated to Data Network) |

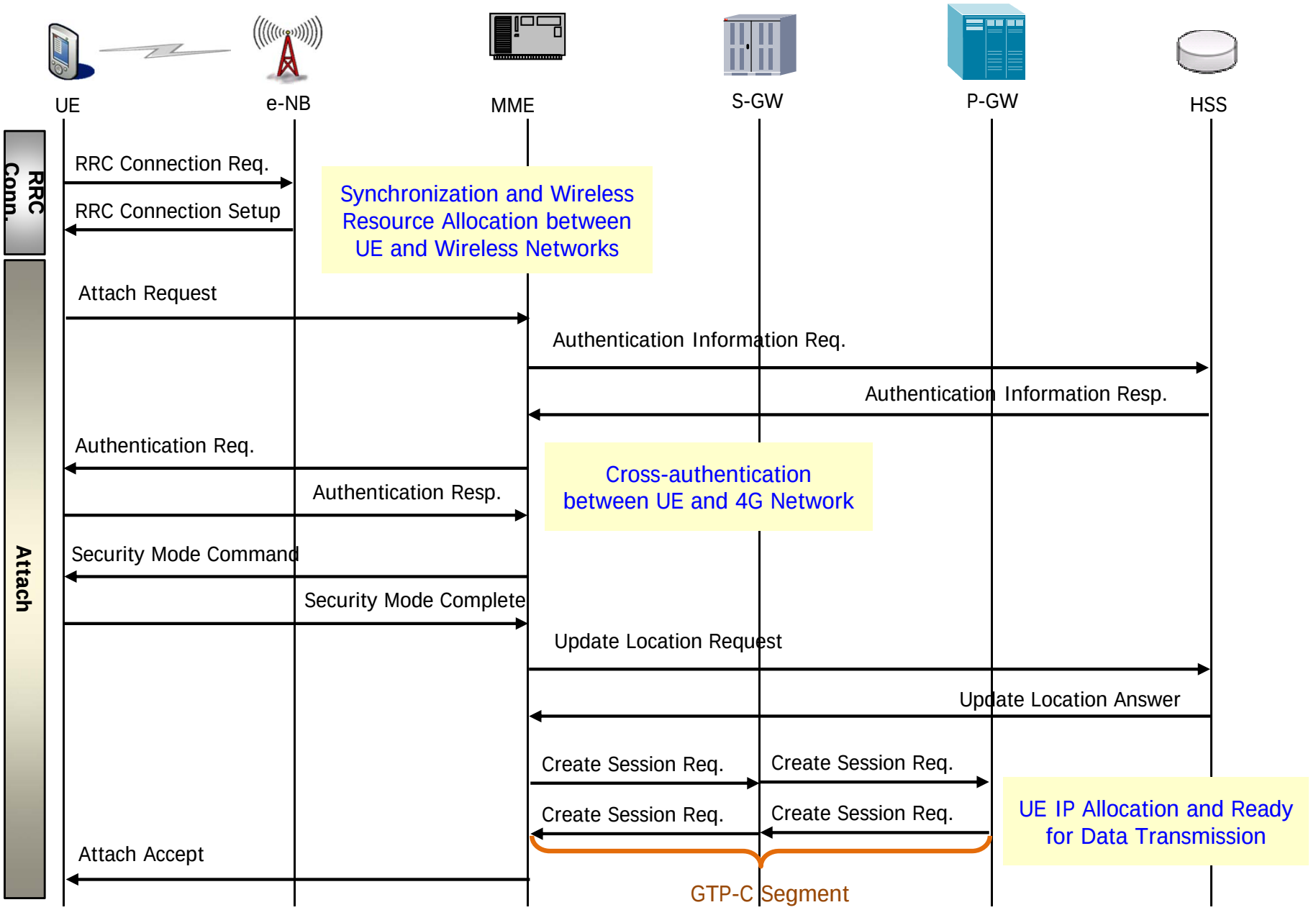
## <The Structural Differences of 3G & 4G Mobile Networks>



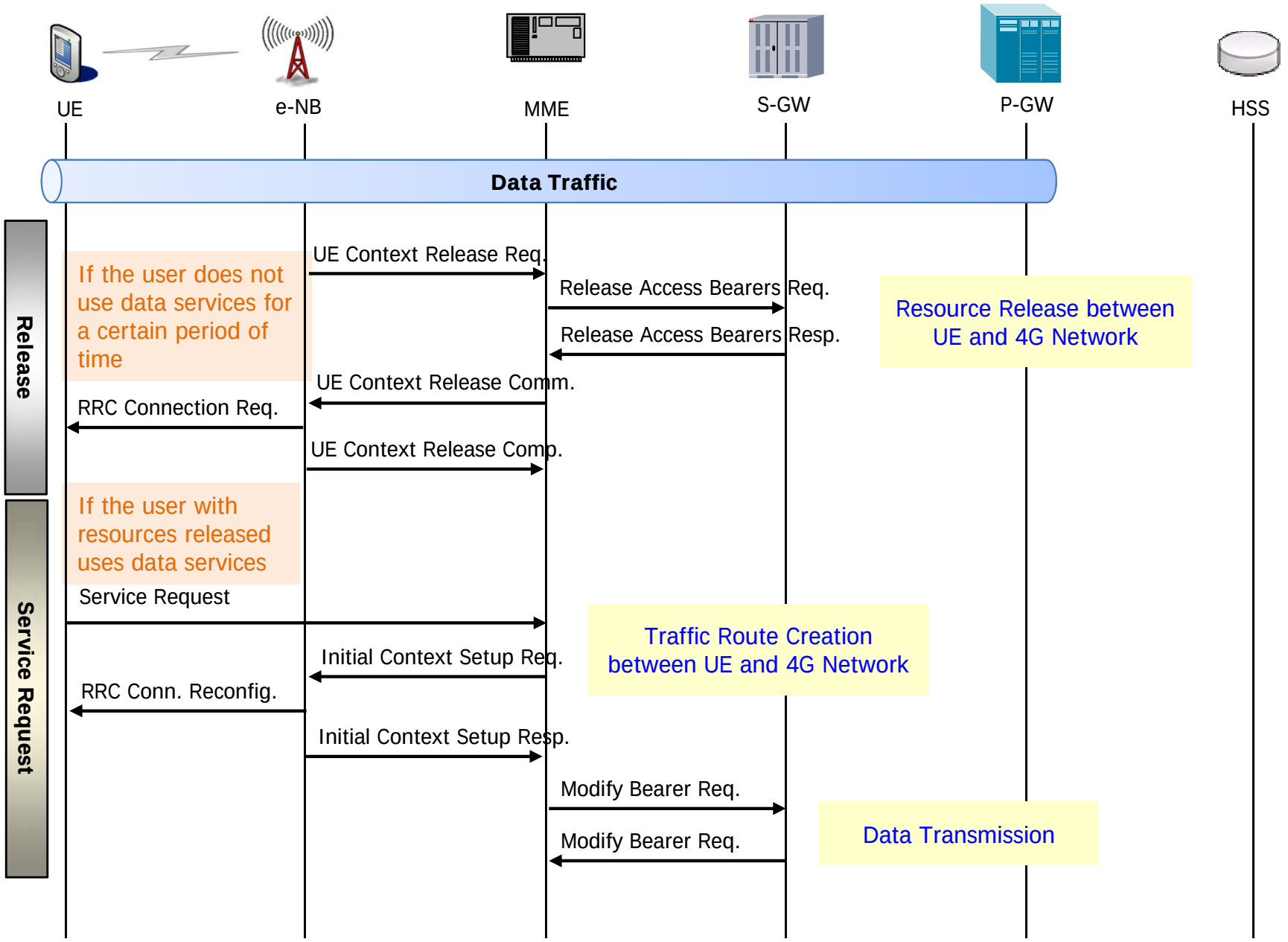
# 1. Overview – Features

| Type | 4G Mobile Network | Wired Network |
|---|---|---|
| Network Structure | A complex network consisting of wireless and wired (IP based) networks | IP based wired network |
| IP Address Allocation | After authentication is performed from a UE to wireless networks and from a UE to the core network, an IP address is allocated from mobile networks to the UE. | The user sets the authorized IP address manually or an IP address is allocated by DHCP. |
| IP Address Change | The allocated IP address is changed due to various factors such as rebooting UE, passing shadow areas, or switching back from flight mode. | Changed by the user or the IP address reallocated by DHCP (usually, fixed) |
| Data Routing | Hierarchical Route (4G: UE → S-GW → P-GW) | Dynamic Route |
| Communication Protocol | Utilizes communication protocols that are optimized for mobile networks such as GPRS Tunneling Protocol (GTP). | TCP/IP |

# 1. Overview – Call Flow - Attach

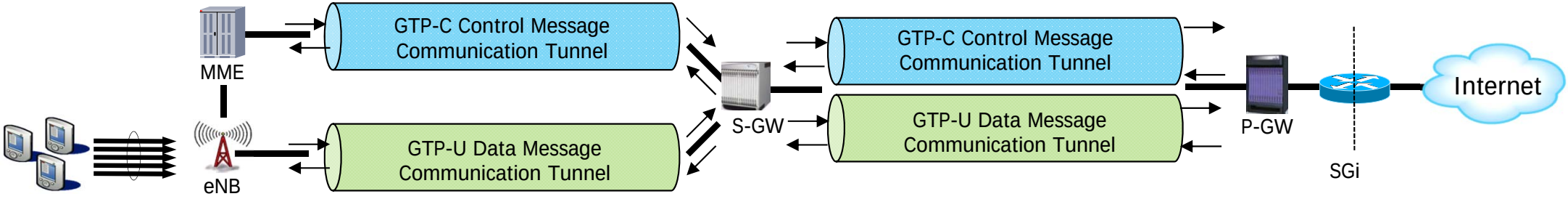


# 1. Overview – Call Flow - Release & Service Request

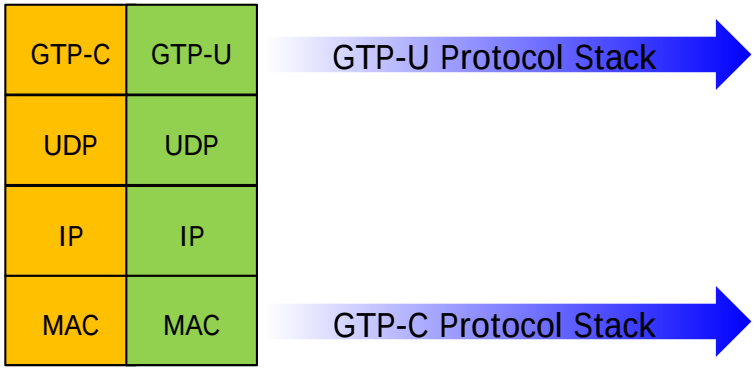


# 1. Overview – GPRS Tunneling Protocol (GTP)

- **Via the GTP(dedicated protocol for mobile networks), control & data messages are transferred within the network**
  - Consists of the GTP-C for data call setup/delete/update and the GTP-U for data delivery.
    ※ GTPv1 is used in the 3G Network, GTPv2 is used in the 4G Network.
  - User data is transferred via GTP-U packet, after the control & data channels allocated to each user.




Create a tunnel for transmission of control messages to each user




GTP-U Protocol Stack

| Version | IP Header Length | Type of Service | Total Length |
|---|---|---|---|
| Identification | | x D M | Fragment Offset |
| Time to live | Next Header Protocol | | Header Checksum |
| Source IP Address | | | |
| Destination IP Address | | | |
| Source Port | | | Destination Port |
| Length | | | Checksum |

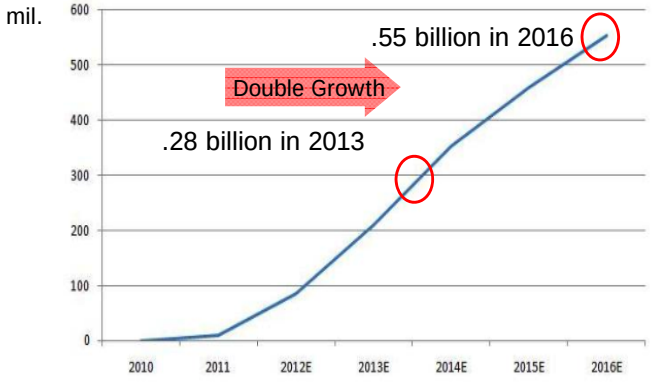
GTP-C Protocol Stack

| Version | Piggybacking flag | TEID flag | Spare | Message Type |
|---|---|---|---|---|
| Total length | | | | |
| Tunnel Endpoint Identifer | | | | |
| Sequence number | | | | Spare |

# 2. The Needs for Protection Tech. – Environmental Changes (1/2)

- **(Early diployment of the 4G network) The top 3 Korean mobile carriers implemented the nationwide LTE network early**
  - SKT, KT, LGU+ started the nationwide LTE service in the second half of 2012 (over one year earlier than expected)
  - Early network implementation and competitions lead to activation of the 4G service in 2013.
- **(Explosion of the 4G UE market) Main handset makers began to launch LTE devices aggressively**
  - In ’13, we expect about 280 million units of 4G LTE UE to be in the market and in ‘16, we expect it to increase by about two folds.
- **(Malicious mobile code) Sudden increase in the number of malicious mobile codes**
  - As malicious mobile codes are increased, malicious/abnormal traffics are entering the 4G Network.
  - Beside 4G, there are many security threats such as personal information leaks on the Internet, Smartphone data exposures, spams, and DDoS attacks.


[4G LTE UE shipments for the entire networks]

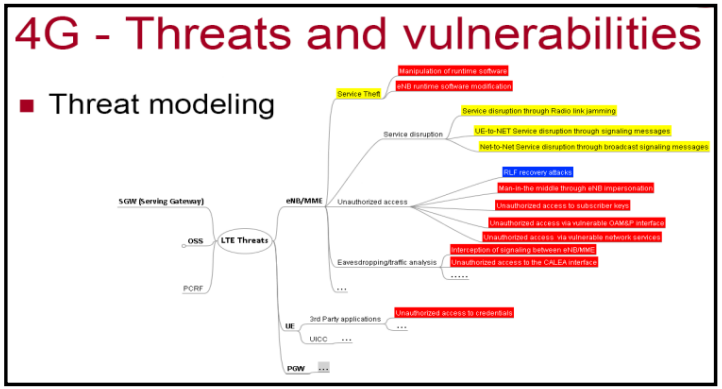


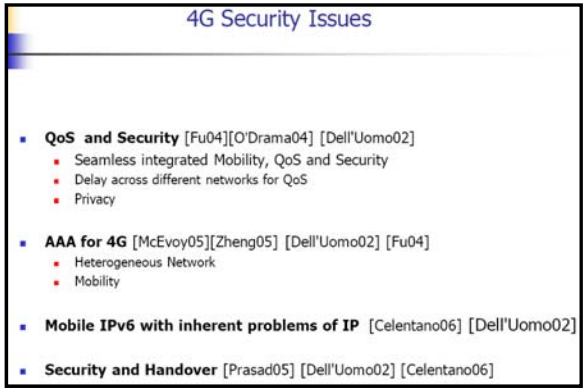

Source: IHS, 8/2012

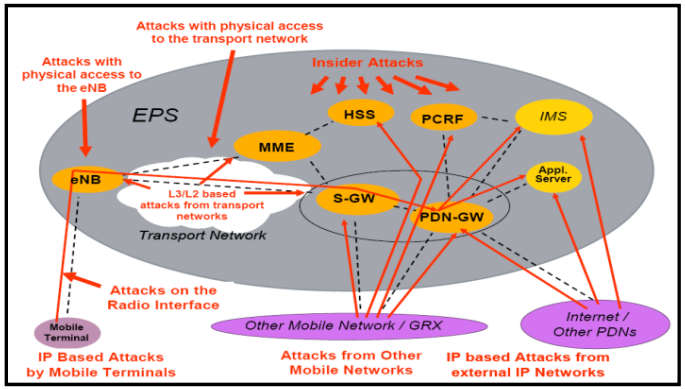
# 2. The Needs for Protection Tech. – Environmental Changes (2/2)

- **As the 4G network was implemented too early without considering security, we can expect lots of security threats**
  - Security threats that need to be considered when implementing the 4G LTE Network are announced by 3GPP, IEEE, and ITU.
  - There are ongoing projects to study how to remove security threats that can arise before implementing the LTE Network.

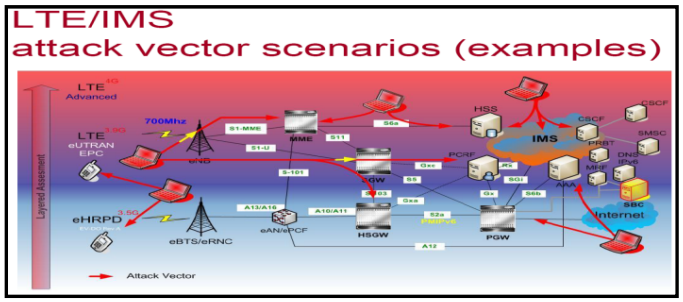
    ※ Germany's ASMONIA project ('10 Sep~'13 May, researches to define security threats that can occur in the 4G Network and to develop the technologies to respond to them.)






[The 4G LTE Network security threats disclosed internationally]

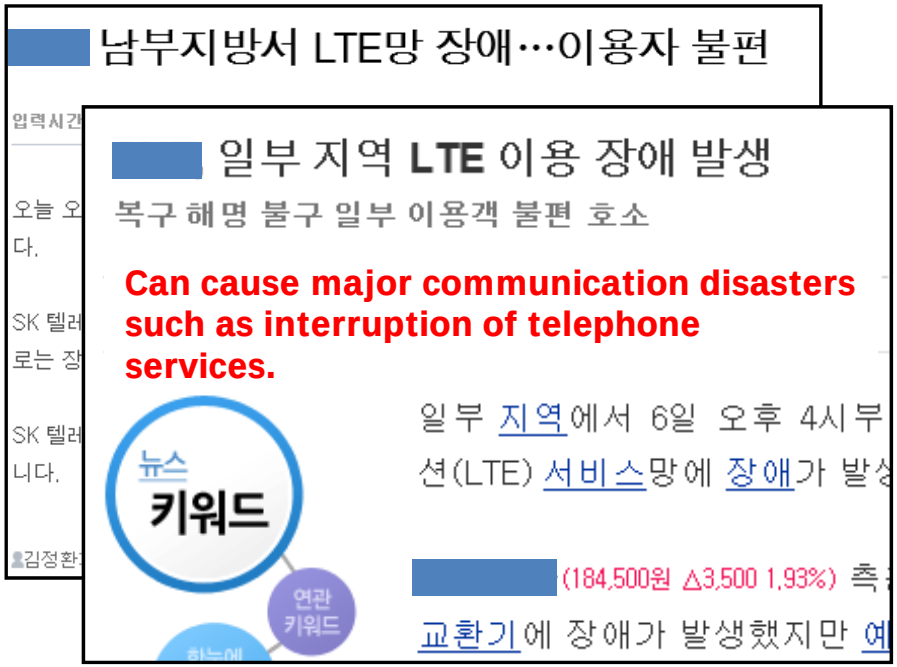
# 2. The Needs for Protection Tech. – Mobile Network Faults

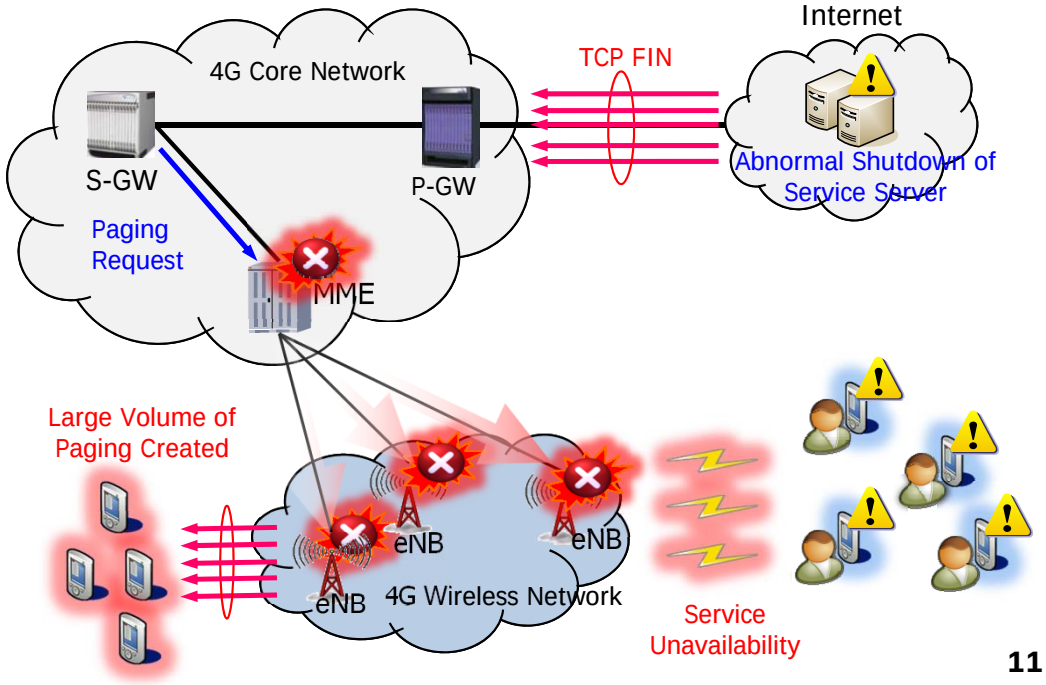
- **Due to abnormal behavior of the service server, a mobile carrier suffered from 4G NW failure('13.2)**
  - As the external service server shuts down abnormally, all the connected UEs received a large volume of TCP FIN messages.
  - From being idle with wireless resources released, a UE switches to the active state to receive data.

  ※ To ensure efficient management of wireless resources, mobile network release wireless resources from a UE that is idle for a certain period of time.
  - During this process, a large volume of paging messages were generated, causing failures of the 4G network equipment such as eNode-B and MME.

  ※ Paging messages repeatedly occur depending on the response from a UE, with expanding TA(Cell group) that controlled by MME.

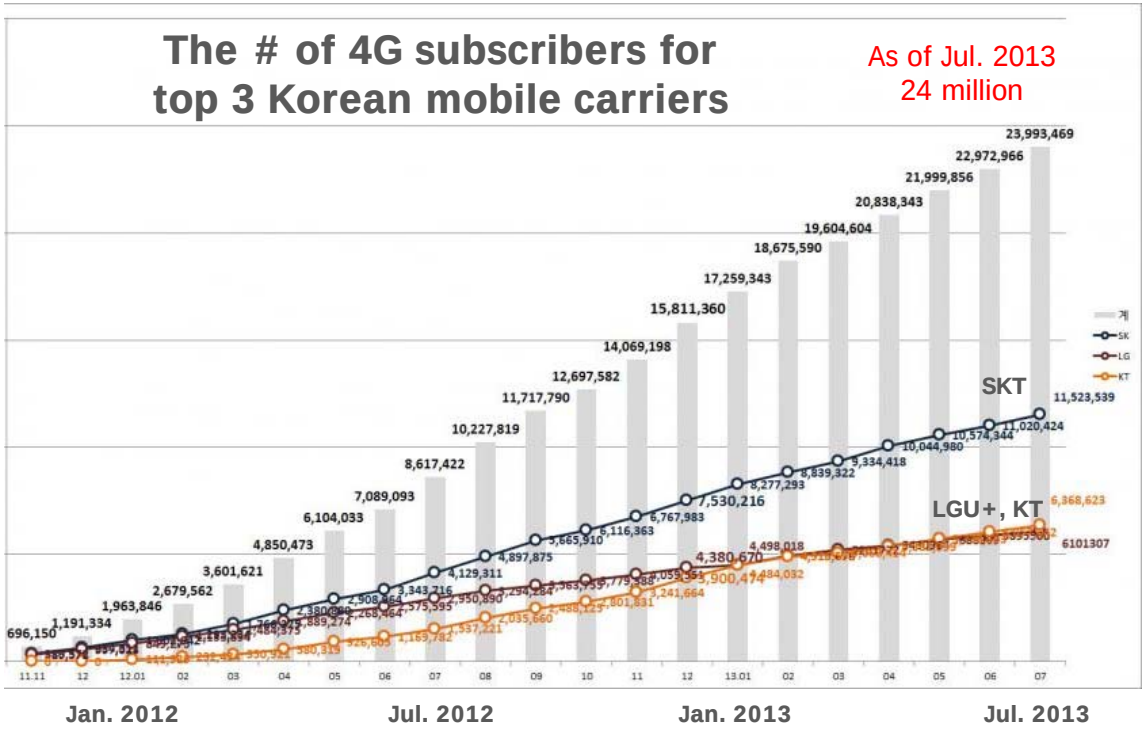
  **→ 4G Network failures can occur due to attacks against mobile service servers in the Internet.**

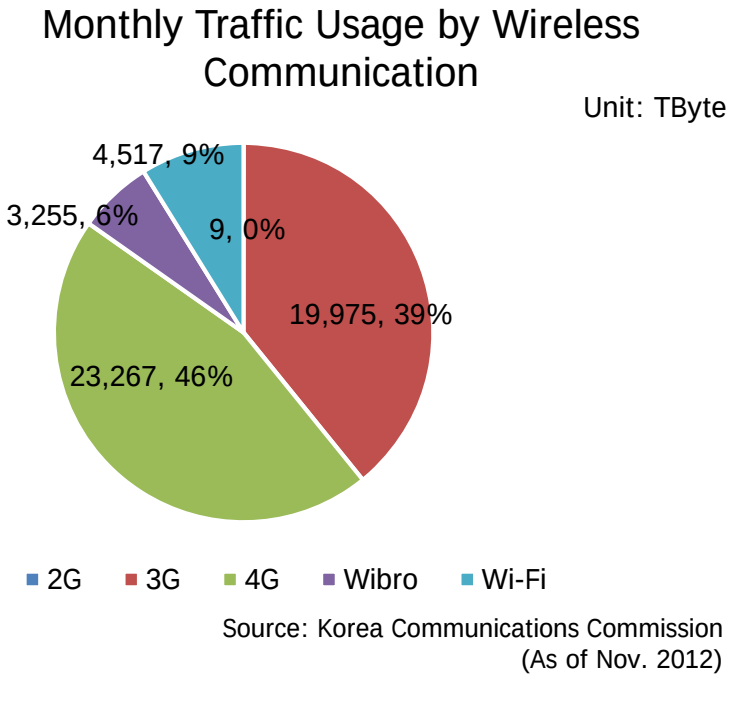


# 2. The Needs for Protection Tech. – Increased Potential Security Threats

- **As the 4G smart phone users and data traffic were increased significantly,**
  - The wireless network with the limited bandwidth was threatened.
    ※ In Korea, 64.6% of smartphone users are using the 4G Network and it reached about 24 million users within 20 months after the launching.
  - Massive allocation and de-allocation of wireless resources and consistently occupying the wireless resource can affect the availability of the 4G Network.
    ※ Compares to the 3G network, the 4G network can transmit data about 12 times faster.
    ※ 4G UE user uses data traffic of about 1.8GB in one month and it is 1.2 times the average of 3G UE users.

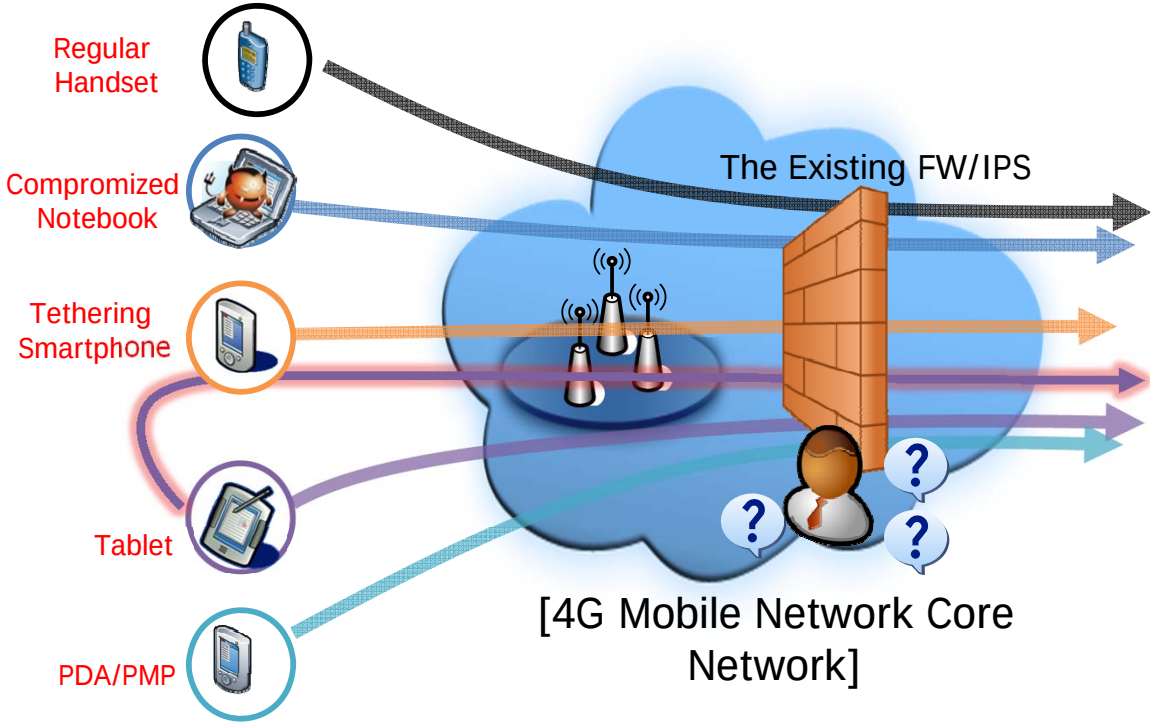


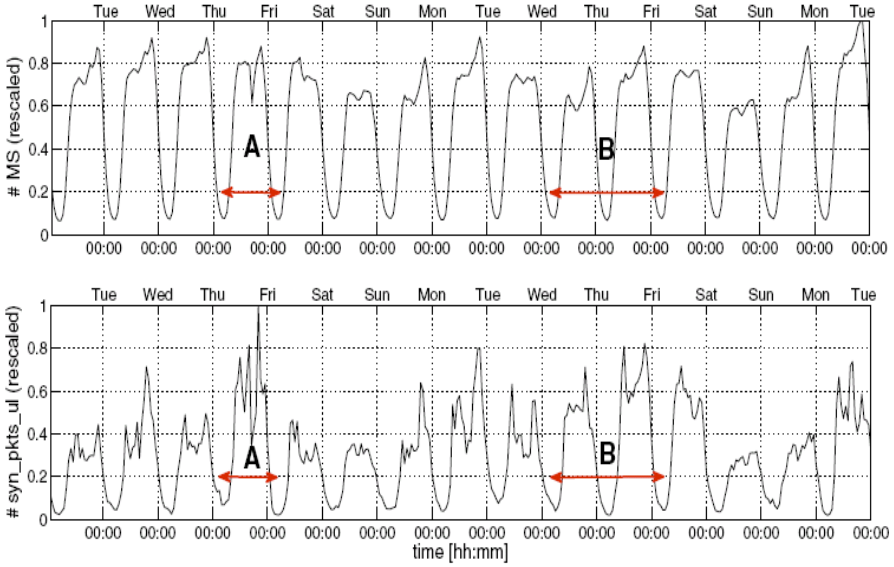

Source: Korea Communications Commission (As of Nov. 2012)

# 2. The Needs for Protection Tech. – Limitation of Existing Security Technologies

- **In the existing internet environment, security equipment such as IPS, Anti-DDoS**
  - Not able to analyze dedicated protocols for the 4G mobile environment, such as GTP, S1AP.
  - The pattern of traffic significantly differs from that of the existing internet environment. (Time/Day of Effect)
    - ※ At 8 AM, 7 and 11 PM, there is sudden change in the traffic. The traffic at specific time is similar to that of the same time on other days.
    - ※ There is a huge difference between the pattern of traffics on weekdays and weekend/holidays.




[4G Mobile Network Core Network]

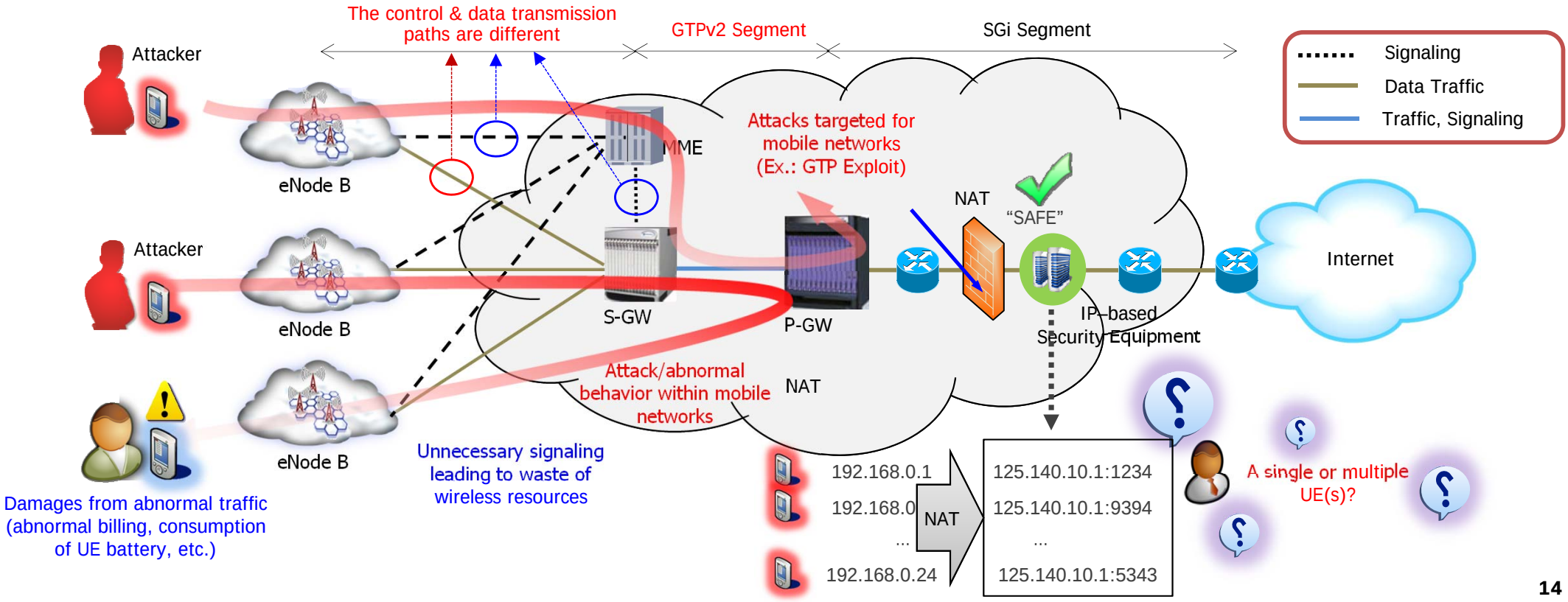



[4G Mobile Network Traffic Creation Patterns]

A. Although the # of UEs is similar to that of weekdays, traffic is rapidly growing.
B. The traffic creation patterns during weekends/holidays are highly fluid.

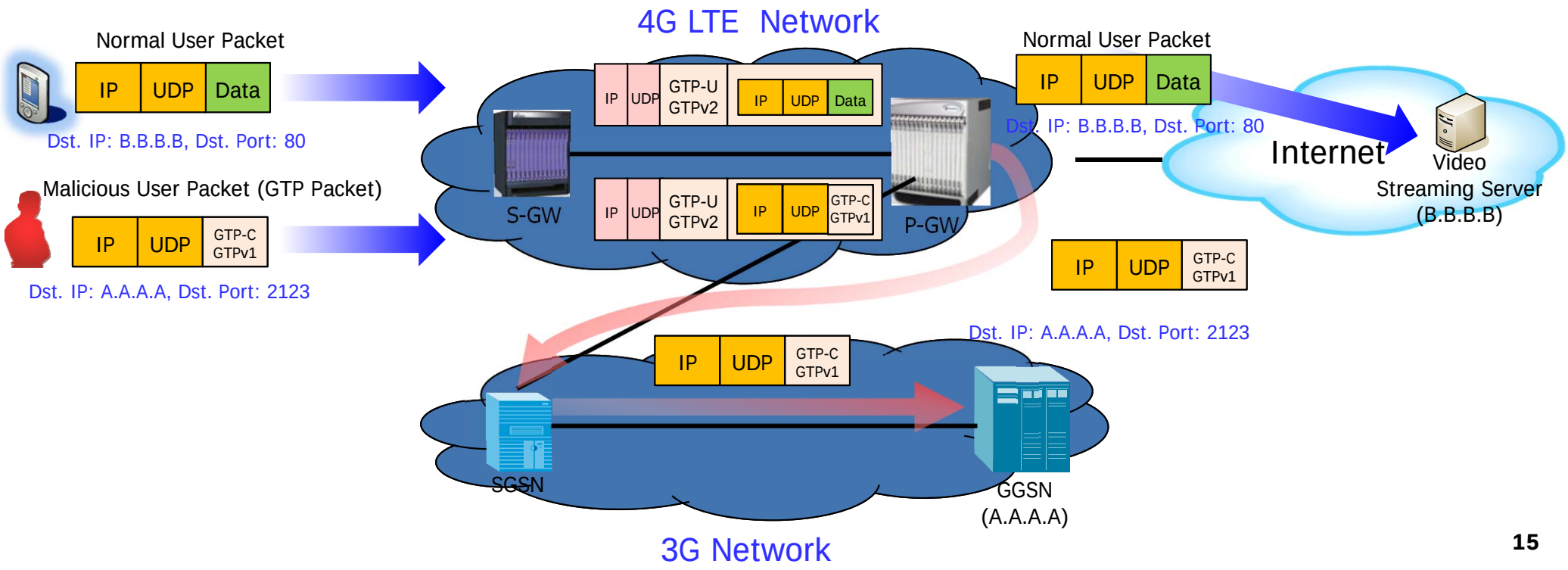
# 2. The Needs for Protection Tech. – Technical Issues Inside Mobile Networks

- **Need to develop security equipment that can be applied to the 4G Network.**
  - In the SGi section (P-GW↔internet), IP address based security equipment cannot distinguish abnormal traffics.
    - ※ Using the NAT, multiple UEs' IP addresses are converted into a single IP address(public).
    - ※ As a UE's IP address is frequently changed, it is difficult to track UE which use private IP address.
  - It is hard to detect attacking/abnormal traffics occurring inside the mobile Network(the front of P-GW).
  - As distinct protocol(GTPv2) is used and separate path for transferring control and data messages are used, it is hard to integrate session management.
    - ※ 3G Network has the same path for Control & Data message transmission and uses the GTPv1 Protocol.



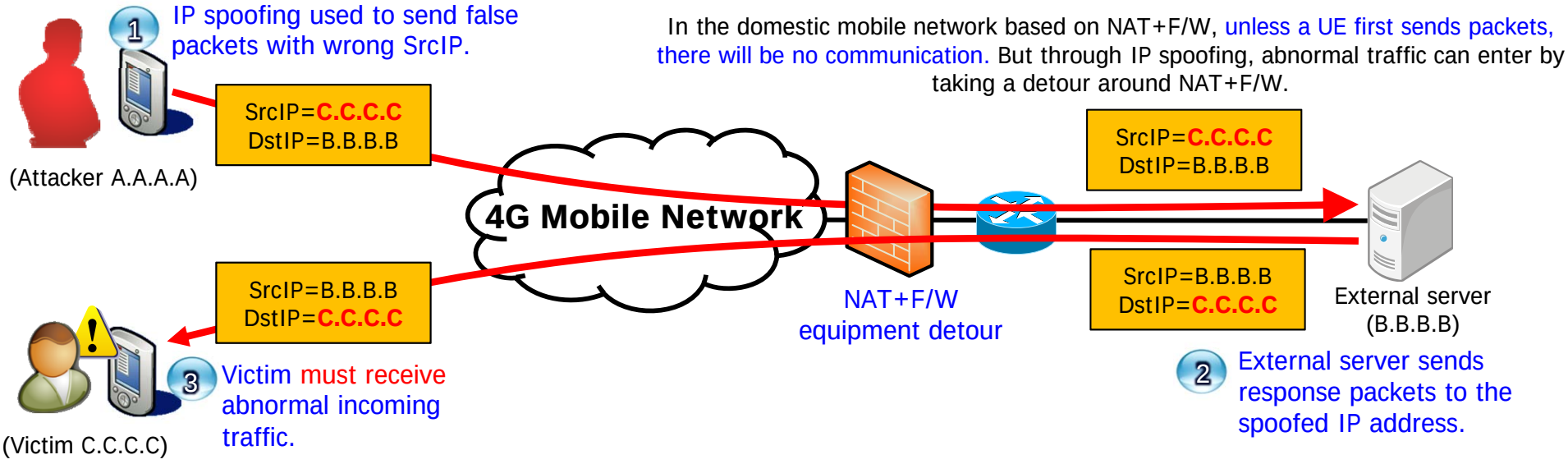
# 3. Security Issues – Security Vulnerabilities (1/4)

- **A LTE PGW equipment has vulnerability in processing the GTP-in-GTP Packets**
  - 4G LTE Network has the P-Gateway equipment that plays a similar roles as the GGSN of the 3G Network.
    ※ P-GATEWAY : Assigns IP addresses to mobile UEs and plays the role as a packet gateway in the 4G Network.
  - If LTE UEs transmit malicious GTP-C Messages, GTP-in-GTP type packets will be passed through the P-GATEWAY to the 3G Mobile Network.
    ※ Since the LTE Network uses GTPv2, GTPv1 is passed through GTPv2 to the 3G Network.(GTPv2-in-GTPv1 vulnerability).
  - The vulnerability is shared with the mobile carriers, now such traffics are all blocked off.



# 3. Security Issues – Security Vulnerabilities (2/4)

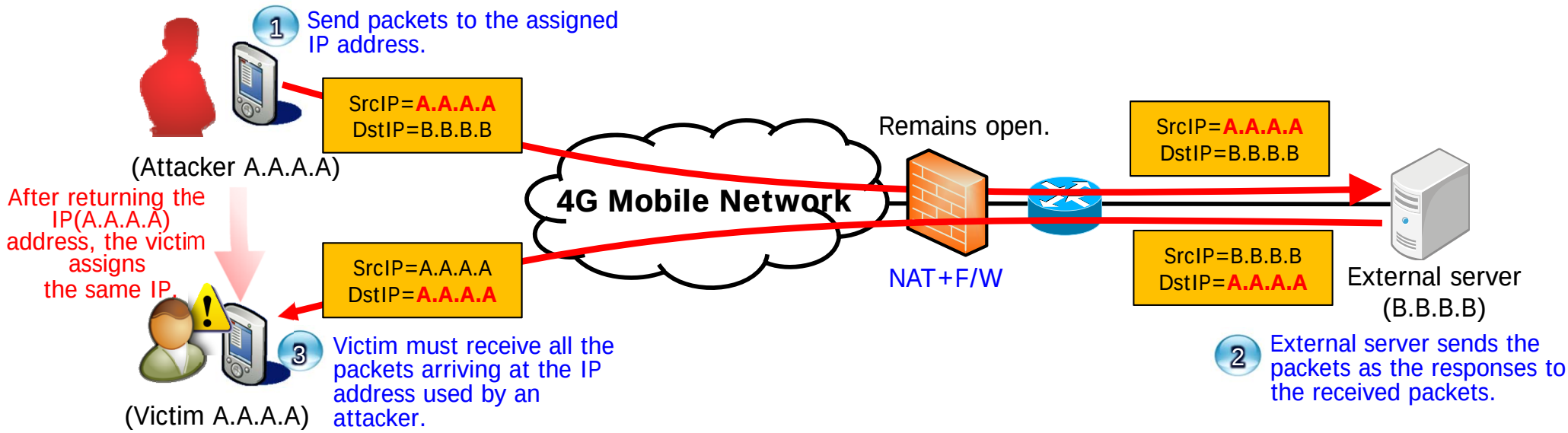
- **IP spoofing used to send abnormal traffic to the 4G Mobile Network from outside**
  - Attacker sends IP-spoofed packets with the IP address of a victim to the server of the external network.
    ※ IP spoofing : IP security vulnerability is exploited to falsify its own IP address.
    ※ NAT+F/W equipment in the 4G network creates communication paths to victim with spoofed IP address.
  - The external network server sends lots of abnormal data to the spoofed IP address (victim's IP address).
    ※ Using the communication path created in the FW+NAT equipment, lots of abnormal traffics are sent to the victim's UE.
  - Victim 's UE receive lots of abnormal traffic from the outside of the 4G Mobile Network.
- **Using the vulnerability, it can cause abnormal billing or loads/troubles in the 4G Mobile Network.**



# 3. Security Issues – Security Vulnerabilities (3/4)

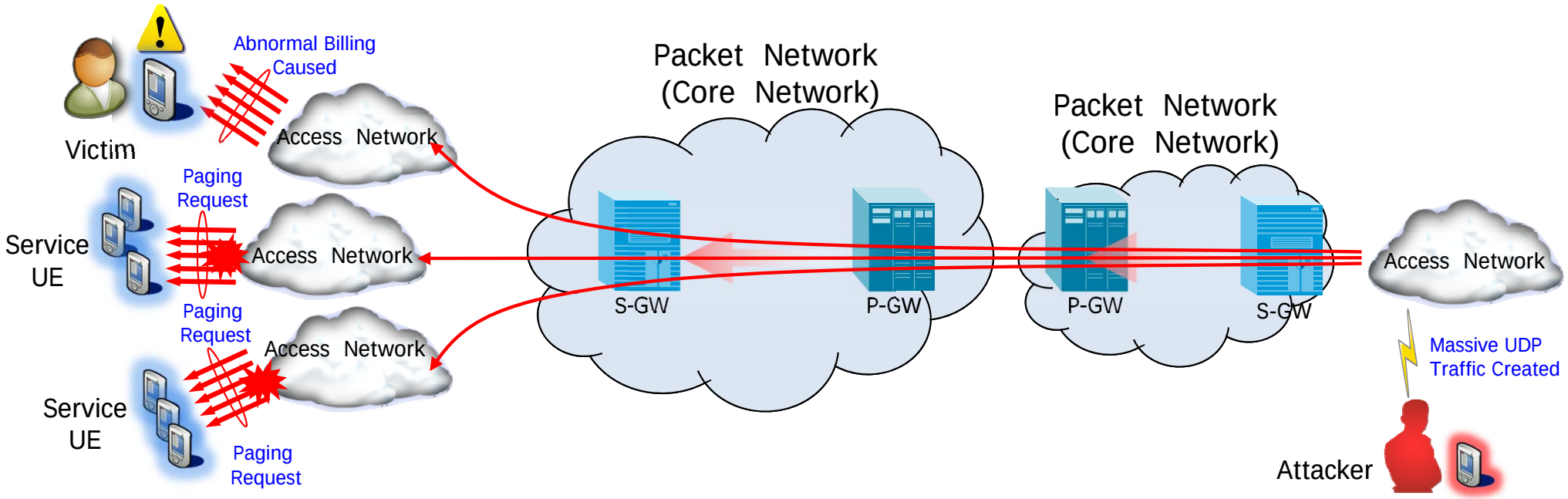
- **IP address re-using process misused to send abnormal 4G mobile traffic from outside**
  - Attacker tries to make a TCP connection to the malicious server, and returns the IP address by releasing a mobile network connection.
  - The malicious server periodically sends TCP ACK packets to the returned IP address to maintain the firewall opening.
  - A normal user who is assigned the IP address used by an attacker receive lots of dummy packets(TCP ACK, FIN and etc.) sent by the malicious server.

    ※ Normal User's mobile UE does not send TCP RST packets as the responses to TCP ACK Packets.
- **Using the vulnerability, it can cause abnormal billing or loads/troubles in the 4G Mobile Network**



# 3. Security Issues – Security Vulnerabilities (4/4)

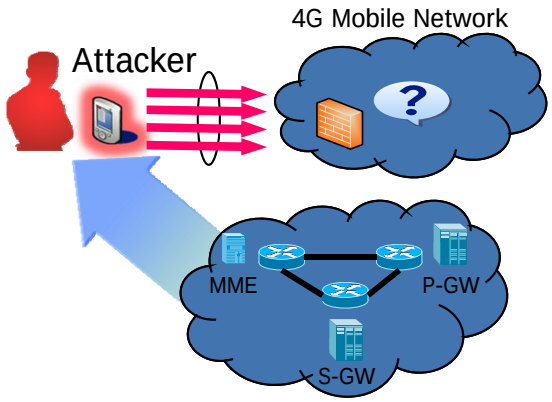
- **Mobile UE to mobile UE communication misused to send abnormal traffics in 4G mobile network**
  - Using UE tethering, repeatedly send UDP traffics to many other UE.
    ※ Korean mobile carriers such as SKT, KT are allowing UE to UE communication.
  - Victim UEs receive packets sent by the attacker.
- **Using the vulnerability, it can cause lack of wireless resources for normal UE.**



# 3. Security Issues – Cyber Attack Threats (1/2)

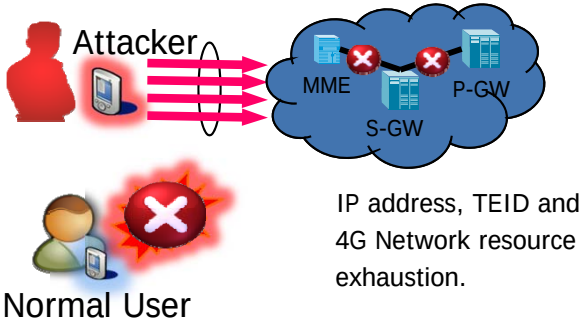
## 4G Network info leak

Using scan message transmission, collect the 4G mobile network components' IP address, MME, S-GW, P-GW.




## 4G Network resource exhaustion

Using the scan information, exhaust the resource of the main equipment of the 4G Mobile Network.

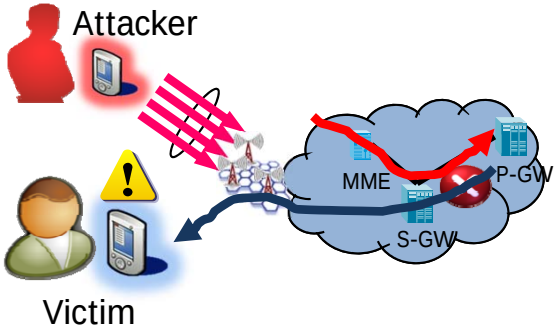



IP address, TEID and 4G Network resource exhaustion.

Data Communication Interrupted. (Insufficient IP,TEID)

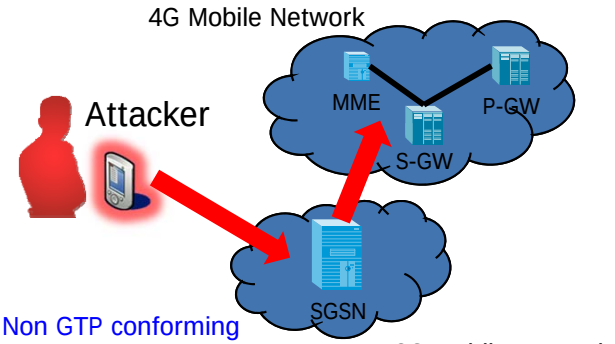
## 4G Network service interruption

Normal User's IP address, TEID assignment interrupted to forcefully terminate the Internet service in the 4G Mobile Network.




## DoS threats(GTP Fuzzing)

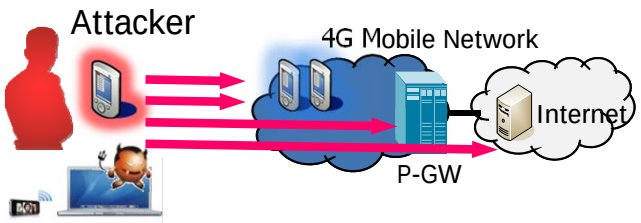
Through the 3G Linked Network, non standard GTP Message messages flow, causing malfunctions of the main equipments in the 4G Mobile Network .




Non GTP conforming Message sent.

## Network overloads(port scanning)

Scanning message for 4G UEs, network components or internet server's open ports or vulnerability transmission.



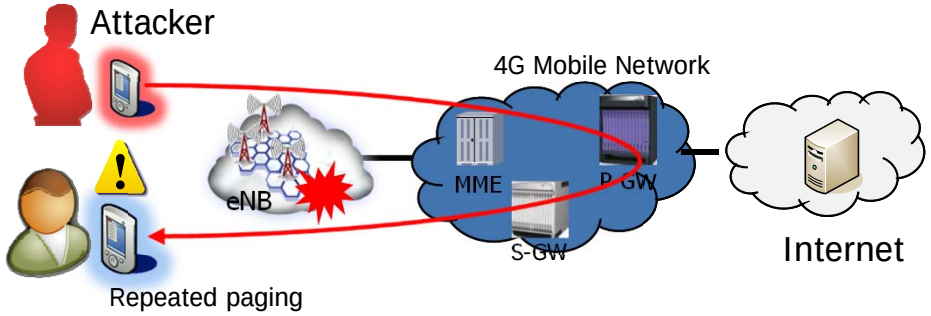

PC infected with malicious codes

4G Mobile Network or Internet Network port scanning traffic.

# 3. Security Issues – Cyber Attack Threats (2/2)

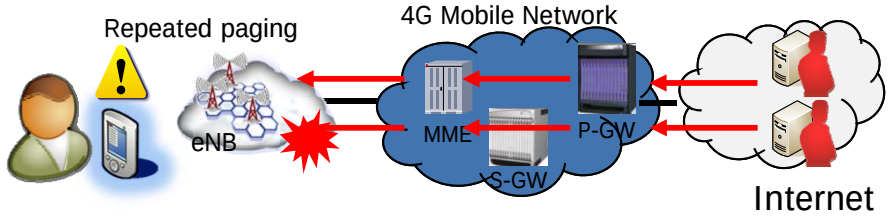
## Degradations of the service quality caused by wireless resource exhaustion - I

Via inter UE communication, small amount of traffic periodically arrives at the specific/non specific IP address, causing repeated paging and exhaust the wireless resource such as the paging channel.(service quality degradation)




## Degradations of the service quality caused by wireless resource exhaustion - II

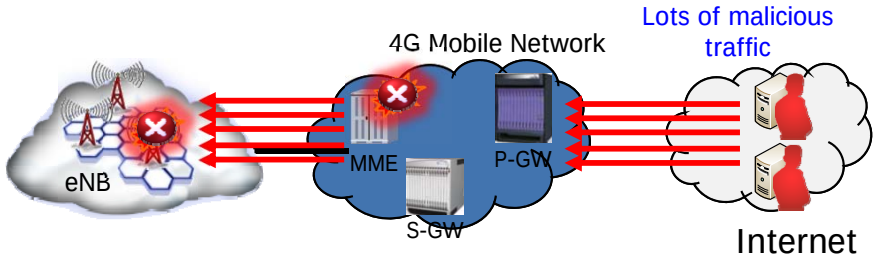
small amount of traffic periodically arrives at the specific/non specific IP address, causing repeated paging and exhaust the wireless resource such as the paging channel.(service quality degradation)




Wireless resource exhaustion causing
Degradation in the voice/mobile data service quality.

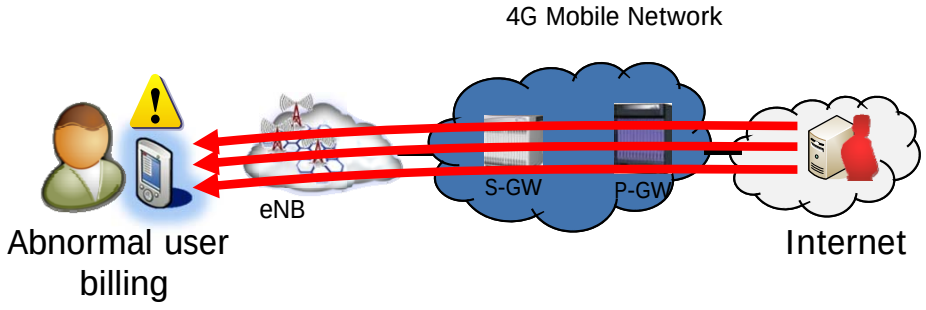
## Network overloads and failure

Using the internet server, send lots of malicious traffic to the 4G Mobile network, causing eNB, MME loads and exhaustion of the mobile communication network band, that in turn causes network failures.



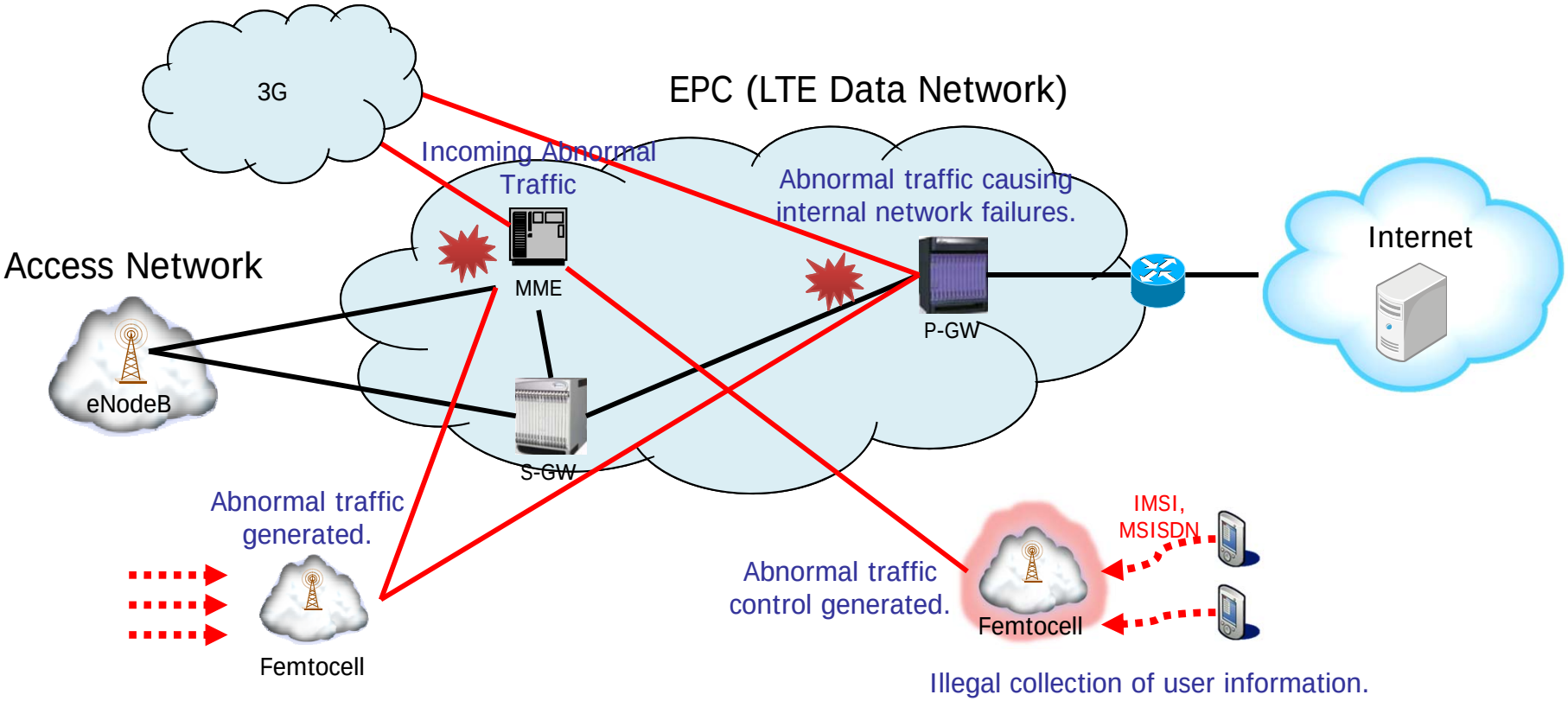

## Abnormal billing

Make a user receive lots of abnormal traffic to cause abnormal billing



# 3. Security Issues – Potential Security Threats

- **Security threats on interconnecting point with 3G Mobile Network**
  - Abnormal traffic from the 3G or other Mobile Network can enter LTE Network.
  - By misusing the management protocols such as SNMP, expose the equipment information (routing information, service lists and etc.)
- **Security threats on Femto-cell link in 4G Mobile Network**
  - Abnormal traffic inflow through Femto-cell.
  - Illegal collection of other users' IMSI, MSISDN through hacked Femto-cell.



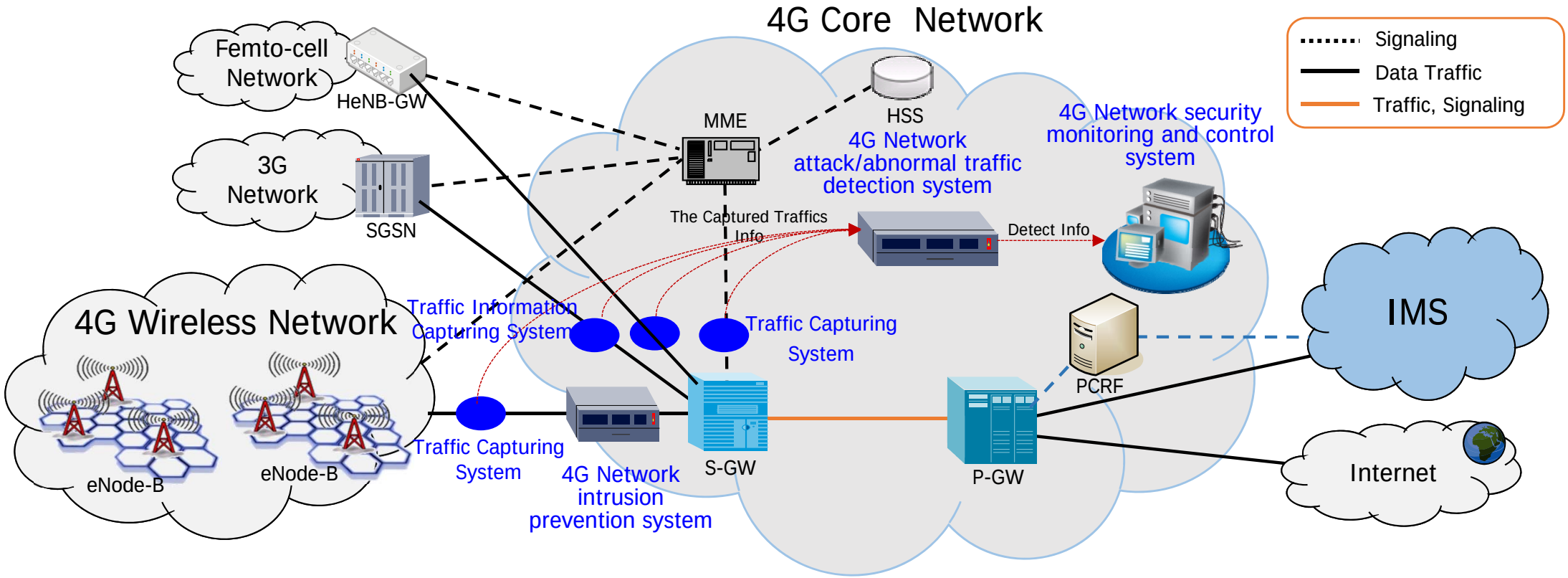
# 4. Countermeasures – 4G Mobile Network Protection Technologies

**Target**

**The Development of 4G Network Protection Technology**

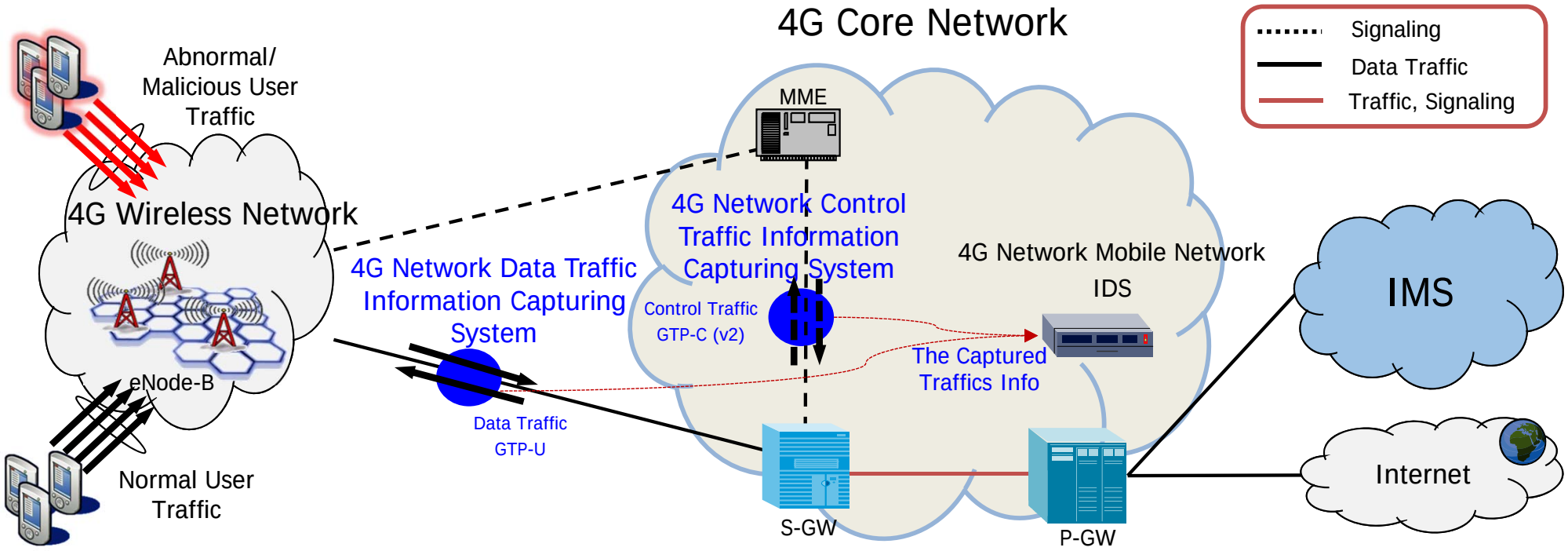
**Deliverables (2016)**

- **4G Network Traffic Information Capturing System(control, data traffic)**
- **4G Network attack/abnormal traffic detection system, 4G Network intrusion prevention system**
- **4G Network security monitoring and control system**



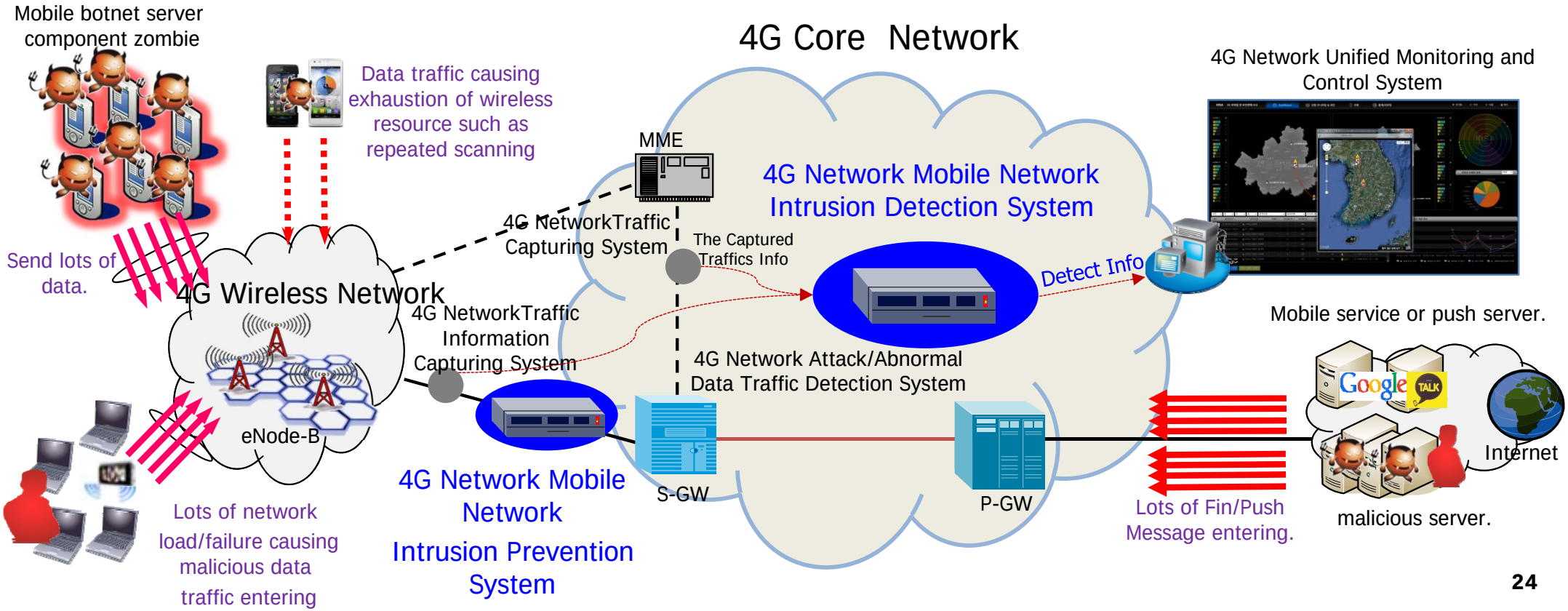
# 4. Countermeasures – 4G Network Traffic Information Capturing Technology

- **4G Mobile Network Traffic Information Capturing Technology**
  - 4G Network control and data traffic (GTP-C/GTP-U) collection technology.
  - Control and data traffic relevancy analysis technology for analysis of 4G mobile user sessions information.
  - Control and data traffic information capturing light transmission technology.



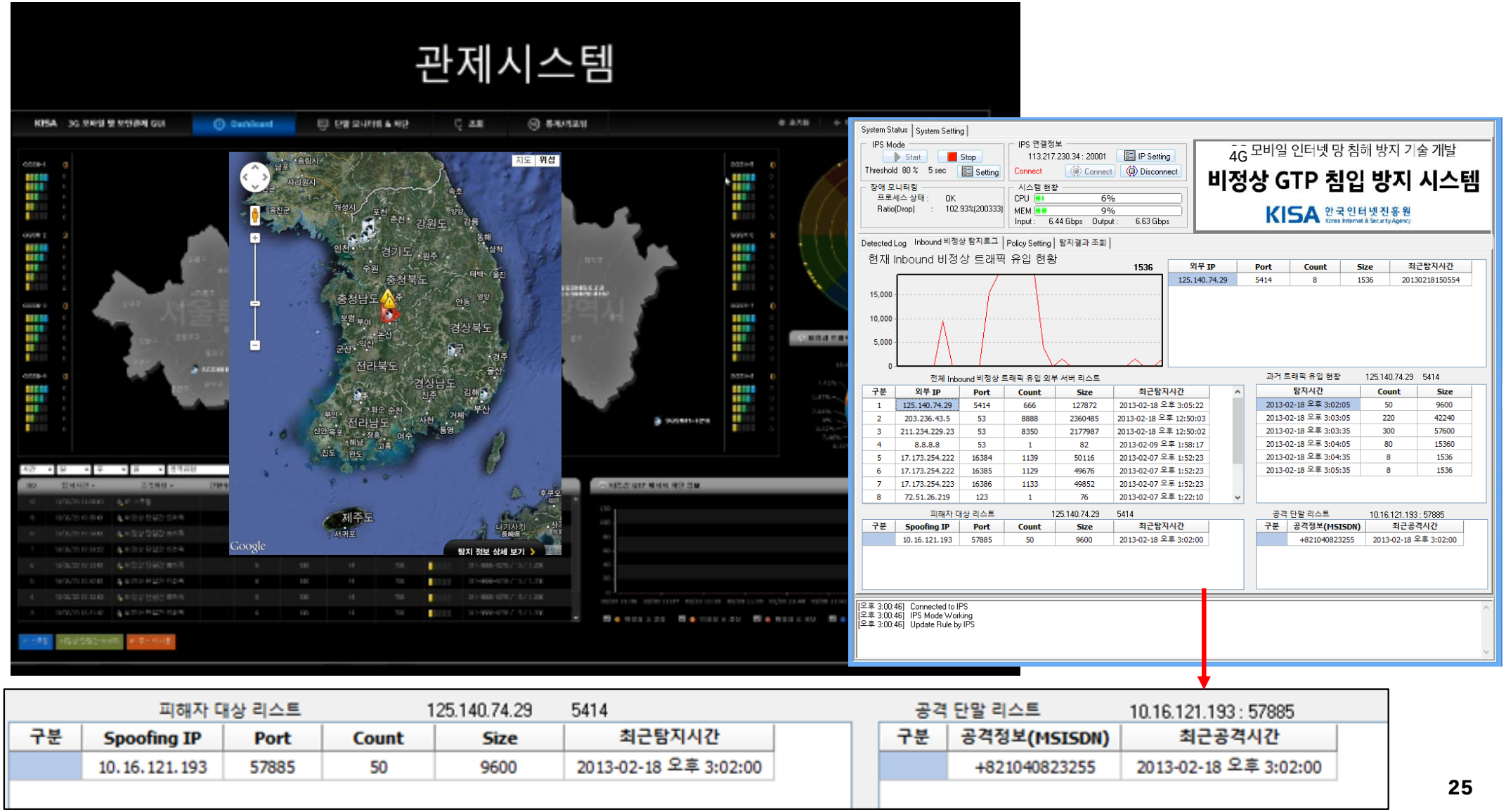
# 4. Countermeasures – 4G Network Intrusion Detection & Prevention Technologies

- **4G Mobile Network Intrusion Detection System**
  - 4G Network's internal information scanning detection, UE loads and abnormal billing causing attacks/abnormal data traffic detection.
  - 4G Network wireless resource exhaustion, main equipment resource exhaustion and load causing attacks/abnormal data traffic detection.
- **4G Mobile Network Intrusion Prevention System**
  - The real-time intrusion prevention technology for abnormal control & data messages (GTP) in 4G Mobile Network
  - IP spoofing and GTP-in-GTP data service based attacks/abnormal traffic blocking.



# 4. Countermeasures – 4G Network Unified Monitoring and Control Technologies

- **4G Mobile Network abnormality sign integration monitoring technology**
  - 4G Network attack/abnormal UE information (phone number/IP address) monitoring and attack/abnormal detection status visualization.




피해자 대상 리스트 125.140.74.29 5414

| 구분 | Spoofing IP | Port | Count | Size | 최근탐지시간 |
|---|---|---|---|---|---|
| | 10.16.121.193 | 57885 | 50 | 9600 | 2013-02-18 오후 3:02:00 |

공격 단말 리스트 10.16.121.193 : 57885

| 구분 | 공격정보(MSISDN) | 최근공격시간 |
|---|---|---|
| | +821040823255 | 2013-02-18 오후 3:02:00 |

# Thank You!