CipherJudge

Enables UE signal identification during over the air analysis of LTE mobile devices in encrypted high-traffic wireless networks

SIM
PWR
CipherJudge
SANJOLE
SAMSUNG
1:40 PM
www.sanjole.com/new-cip
SANJOLE
Wireless Network Test and Measurement Equipment
HOME
COMPANY
PRODUCTS
SOLUTIONS
SUPPORT
CONTACT
New CipherJudge product introduced
Sanjole introduces another exciting product called

An add-on to the WaveJudge 5000, Sanjole's CipherJudge enables

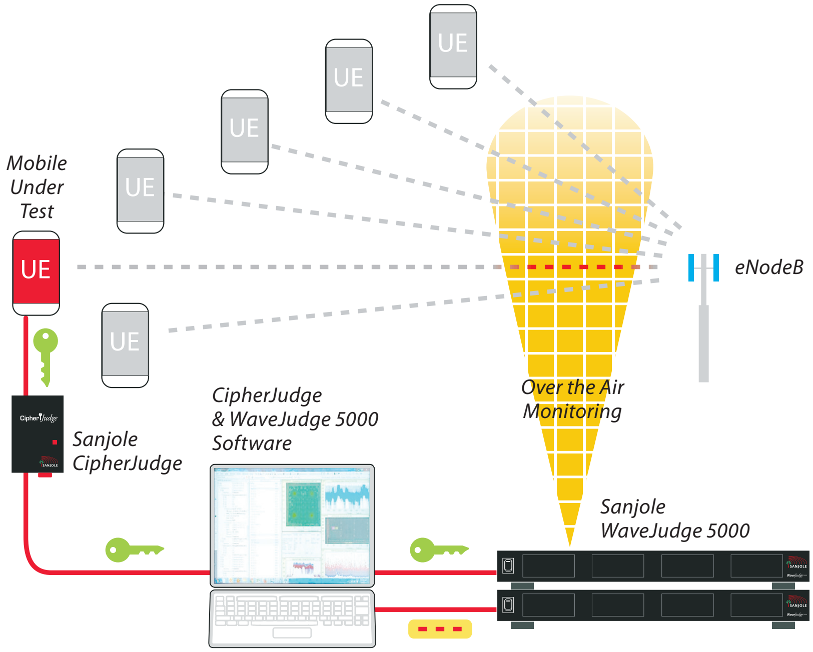
- **Real-time SIM key retrieval and parsing of ciphered traffic**
- **Identify and track UE's within commercial LTE networks**
- **Test UE's from lab to field environment**
- **Capture/decode/trigger off ciphered control messages such as handovers**

LTE takes great measures to protect the mobile's identity and the data packet payloads sent over the air. While important for mobile users, these privacy measures create challenges for testing a specific or groups of UEs.

Over the air analysis and monitoring is very effective for testing wireless devices and networks, saving hours if not days of time. Sanjole's powerful air monitor WaveJudge 5000 test system provides real-time visibility into the interaction between protocol and physical layers in wireless transmissions, thus facilitating identification of root causes of problems. Thanks to the CipherJudge, the WaveJudge's analytical power can now be extended with ease to test a UE operating in a live, high-traffic network. There is no longer a need to create special test setups, turn encryption off, or guess which messages are from the UE of interest.

The CipherJudge is a first to market, pocket-sized device that physically connects to a mobile of interest, and functions as an add-on to the WaveJudge 5000. By intercepting the messages between the ME (Mobile Equipment) and USIM (Universal Subscriber Identity Module), the CipherJudge allows the WaveJudge 5000 to uniquely identify a UE, and decode all messages between the lab- or field-located UE and the eNodeB. In doing so, the CipherJudge enables engineers to benchmark network attach, debug handover issues and contribute to QoE analysis in deployed networks.

This ability to diagnose problems of a unique UE operating in a network serving hundreds of other users while encryption is enabled makes Sanjole's CipherJudge a powerful tool in any engineer's arsenal.



Understanding LTE UE Security

At the time the UE is provisioned, both USIM and the HHS (Home Subscriber Server) are given the IMSI (International Mobile Subscriber Identity, a unique number identifying the user) and a secret number K (magic number used to derive encryption key set material).

When the UE wants to enter the network, it initiates the NAS attach procedure. The purpose of the NAS attach procedure is to mutually authenticate the UE and LTE network, register the UE on the network and establish encryption key set material.

Normally, USIM will store a valid GUTI (Global Unique Temporary ID) and key set from the last time the UE was connected to the network. This information is used in the ATTACH REQUEST message sent by the UE. Without external knowledge, the association between GUTI and IMSI is unknown and the user's identity is protected. If USIM contains an invalid GUTI or key set, the UE will be forced to transmit its IMSI without encryption turned on. Once done, the UE will revert to the default behavior of sending the GUTI and key set stored by USIM. This design protects the user's identity (IMSI) by limiting its Over the Air (OTA) transmission.

Almost every OTA packet is encrypted using the key set derived from K. Only the first few messages of the NAS attach procedure are sent without encryption turned on. K is never sent OTA, can never be read from the UICC "SIM" card and is never sent by the HHS.

Without diving too deeply into the details of encryption, by the time the AUTHENTICATION RESPONSE message is sent by UE, both the UE and network have authenticated each other and have independently calculated identical key set material to be used for encrypting data packets.

Once the UE has been validated on the network, the ATTACH ACCEPT message is sent by the MME. Its importance is the new GUTI which will be used to identify the user moving forward. This message is encrypted, and without the keyset, tracking the UE is impossible.

The CipherJudge intercepts communication between the ME and USIM. When the WaveJudge 5000 captures and processes data, the CipherJudge will provide a key set (CK, IK and KASME) that can be used to decrypt and identify all packets from a specific ME.

Call for Information

For more information about the CipherJudge, please call Sanjole at 1-808-457-1452 or email sales@sanjole.com.

About Sanjole

Sanjole is a leader in LTE and WiMAX testing with expertise in innovative wireless technology. Sanjole provides problem solving capabilities from inside the wireless network through over-the-air analysis tools that provide visibility into events spanning multiple layers.

Sanjole has been involved from the very beginning of LTE as a test vendor in the LTE/SAE Trial Initiative (LSTI) events for both fixed and wireless devices. Our work with the WiMAX Forum and 3GPP, participation in the Small Cell Forum, TETRA, and extensive experience in interoperability trials, enable deep insight into the complex technical issues specific to the LTE and 4G community.

Sanjole Inc.

Pacific Park Plaza | 711 Kapiolani Blvd,
Ste 1050 | Honolulu HI 96813-5285 USA
sales@sanjole.com | 808-457-1452
www.sanjole.com

CipherJudge Specifications

Included with CipherJudge

- USB cable
- CipherJudge FFC cable to SIM interface (4 orientations)
- Nano to Micro SIM card adapter
- Nano to Standard SIM card adapter
- Micro to Standard SIM card adapter
- Standard SIM to Nano with FFC cable
- Standard SIM to Micro with FFC cable
- Orientation change extension FFC for Standard SIM

SIM cards supported

- Nano, Micro and Standard

USIM parameters captured

- ICCID
- IMSI
- GUTI
- Kasme, NAS algorithms, NAS Counter values, key set id
- CK, IK, RAND, AUTN, RES

Protocol decodes

- MAC, RLC, PDCP, RRC, NAS, TCP/IP, VOIP