이동통신 네트워크 장비 프로토콜 상태 기계 추출 기반의 표준 위배 동작 검출

전기 및 전자공학부
황영빈

목차

- 연구 목적
- 배경 지식
- 연구 수행 방법
- 연구 결과
- 결론

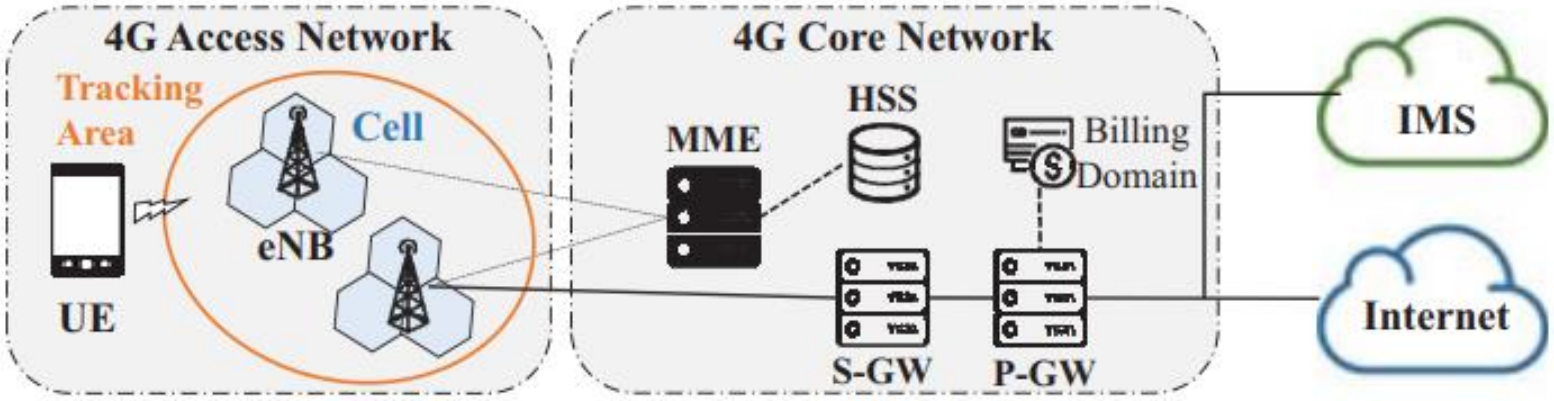
연구 목적

- 이동통신 기술의 빠른 성장
  - 보안 기술의 발전이 따라가지 못하고 있다.
- 이동통신 네트워크 장비에서 체계적인 보안 분석의 필요성
  - 통신사, 제조사별 구현이 다르다.
- LTE 네트워크 장비 보안성 분석의 부족
  - 대부분의 연구는 단말의 보안성을 분석한 연구이다.
- LTE 보안의 중요성
  - 5G가 도입되고 있지만 아직은 NSA(Non-Standalone)를 사용하기 때문에 코어 네트워크는 LTE 장비가 사용된다.

배경 지식

❖ LTE 네트워크 구조

– UE(User Equipment), ENB(Evolved Node B), MME(Mobility Management Entity)

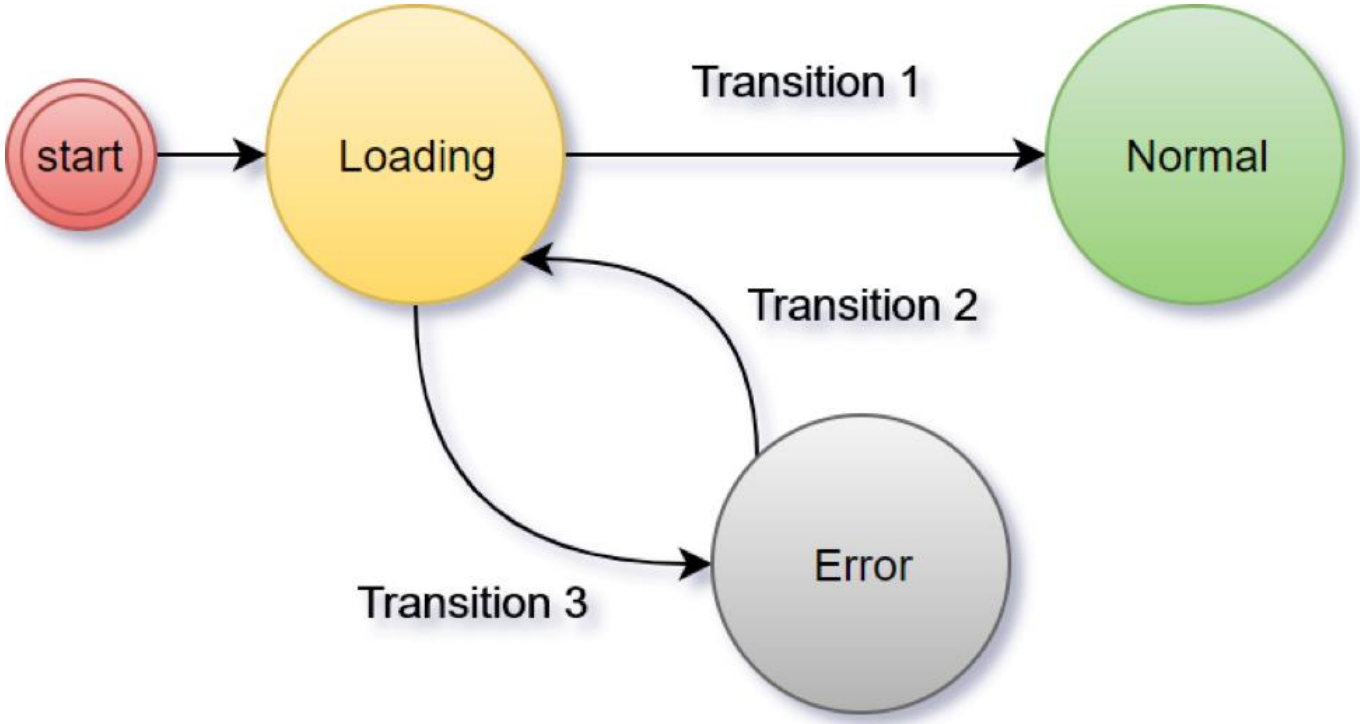


❖ LTE 제어 평면 프로토콜

– NAS(Non-Access Stratum)

배경 지식

- Finite state machine : 유한 개의 상태를 가지고 주어지는 입력에 따라 어떤 상태에서 다른 상태로 전환시키거나 액션이 일어나게 하는 모델.



배경 지식

❖ 선행연구: Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane

– Stateless fuzzer : 여러 state에 걸쳐 있는 취약점은 발견하기 어렵다.

--> state machine을 통해 숨겨진 취약점을 찾는 것이 목표.

Exploited NAS Messages	Implications		
	MME_1	MME_2	MME_3
Attach Request	DoS (**P**, **I**, **R**)	×	DoS (**P**, **I**, **R**)
TAU Request	DoS (**P**, **I**, **R**)	×	DoS (**I**), False location update (**R**)
Service Request	Spoofing (**R**)	×	Spoofing (**R**)
Uplink NAS Transport	DoS (**P**, **I**), SMS phishing (**R**)	SMS phishing (**P**, **I**, **R**)	-
PDN Connectivity Request	DoS (**I**)	×	DoS, DosS (**R**)
PDN Disconnect Request	DoS (**I**), DosS (**R**)	×	DosS (**R**)
Detach Request	DoS (**P**, **R**)	DoS (**P**, **I**, **R**)	DoS (**P**, **I**, **R**)

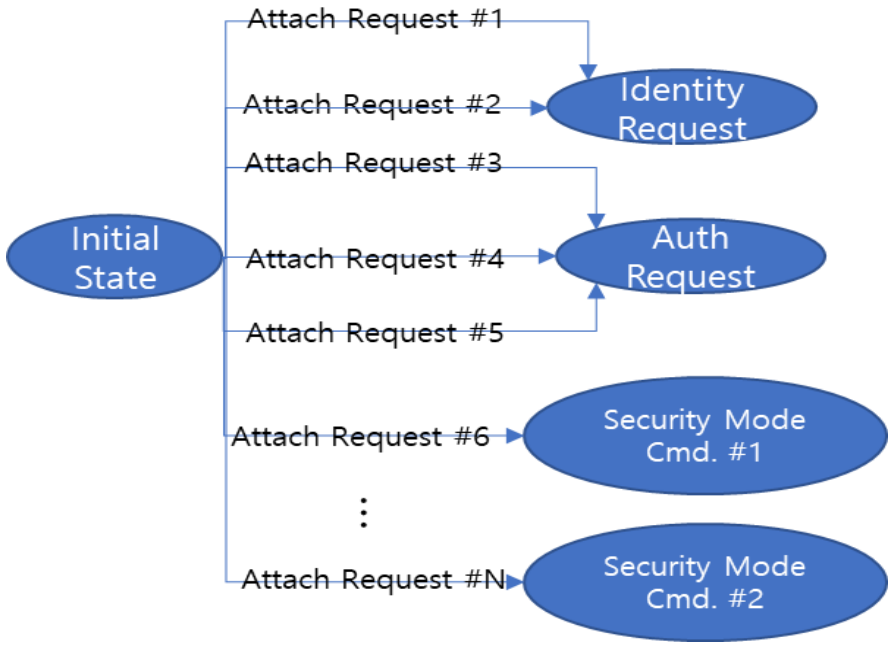
DosS: Denial of selective Service, **P:** Plain, **I:** Invalid MAC, **R:** Replay

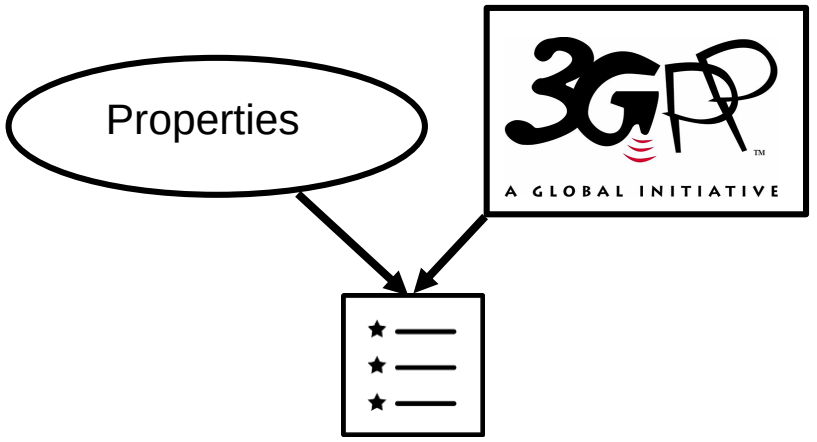
연구 수행 방법

- 이동통신 네트워크 장비 상태 모델(state machine) 추출
  - 상태 모델 추출 툴(Fuzzer) : 프로토콜 퍼징 기법을 이용해 다양한 메시지 형태를 네트워크 장비에 보내고 응답 기록.
  - 상태 모델 분석 툴(Analyzer) : 공통적인 응답을 유도하는 입력 메시지 형태들의 특징을 분석하여 state machine상의 transition을 구성한다.

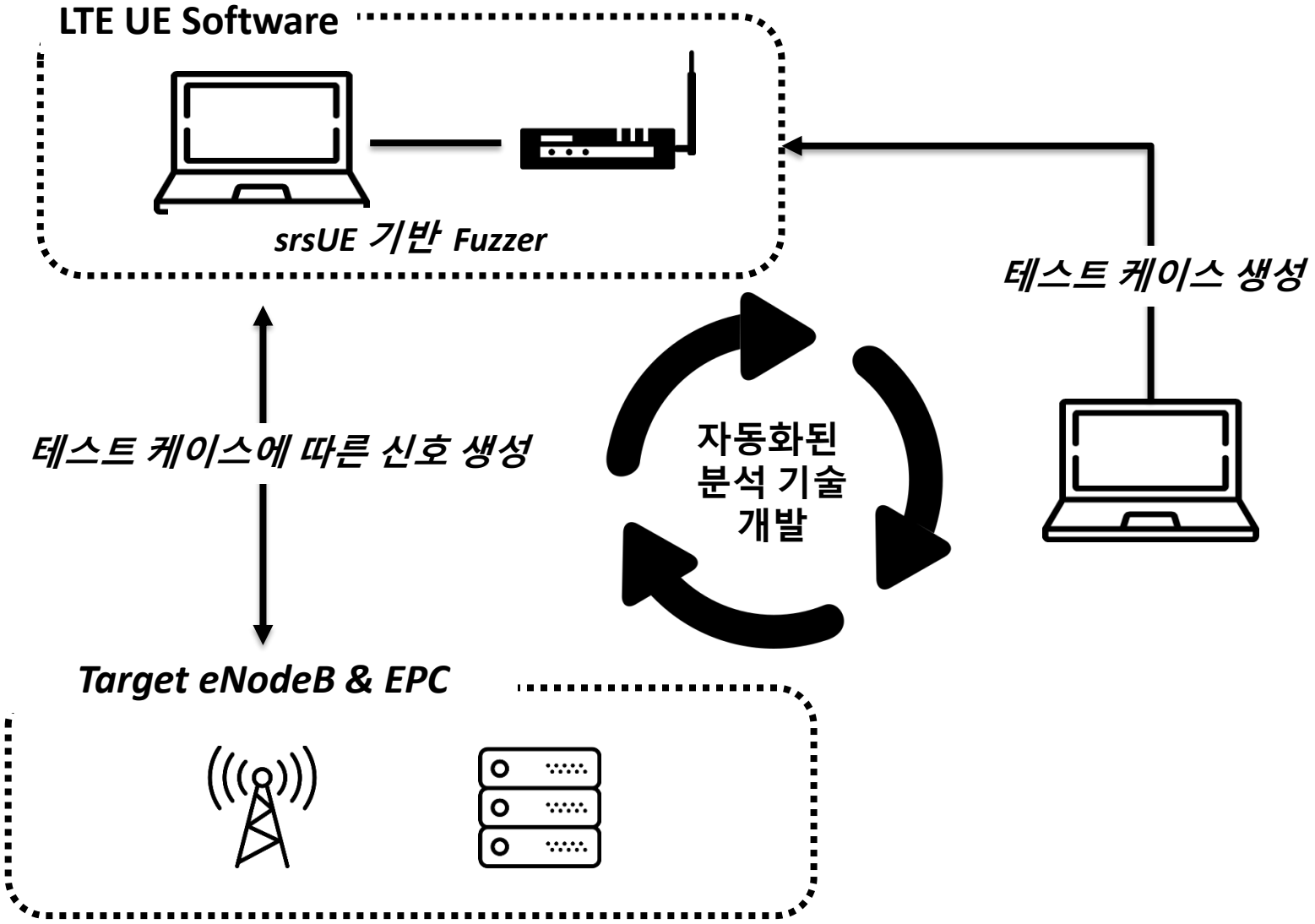
연구 수행 방법

- 표준 문서와 비교를 통해 취약점 찾기
  - 추출된 3사 state machine 중 상이한 부분을 중점적으로 표준 내용과 비교 분석





실험 환경



제어 가능한 LTE UE 소프트웨어
오픈소스 LTE S/W와 SDR를 활용한
다양한 동작 시나리오 테스트 가능한 단말

표준 분석 기반의 Testcase 생성
RRC/NAS 표준 분석을 통하여
표준 위배 메시지 (Testcase) 생성

Testcase 송신을 통한 네트워크 구현 검증
단말 로그 및 응답 메시지를 기반으로 결과 분석을
통해 Testcase를 올바르게 처리하는지 검증

구현

- State Machine Extractor (C++)
  - srsUE (open-source LTE stack) + 1800 LoC
- Test message generator (Python)
  - 1100 LoC
  - Message Type: Attach Request, Identity Response, Authentication Response, Security Mode Complete
  - # of test messages: 9498+
- Output Analyzer (Python)
  - 700 LoC

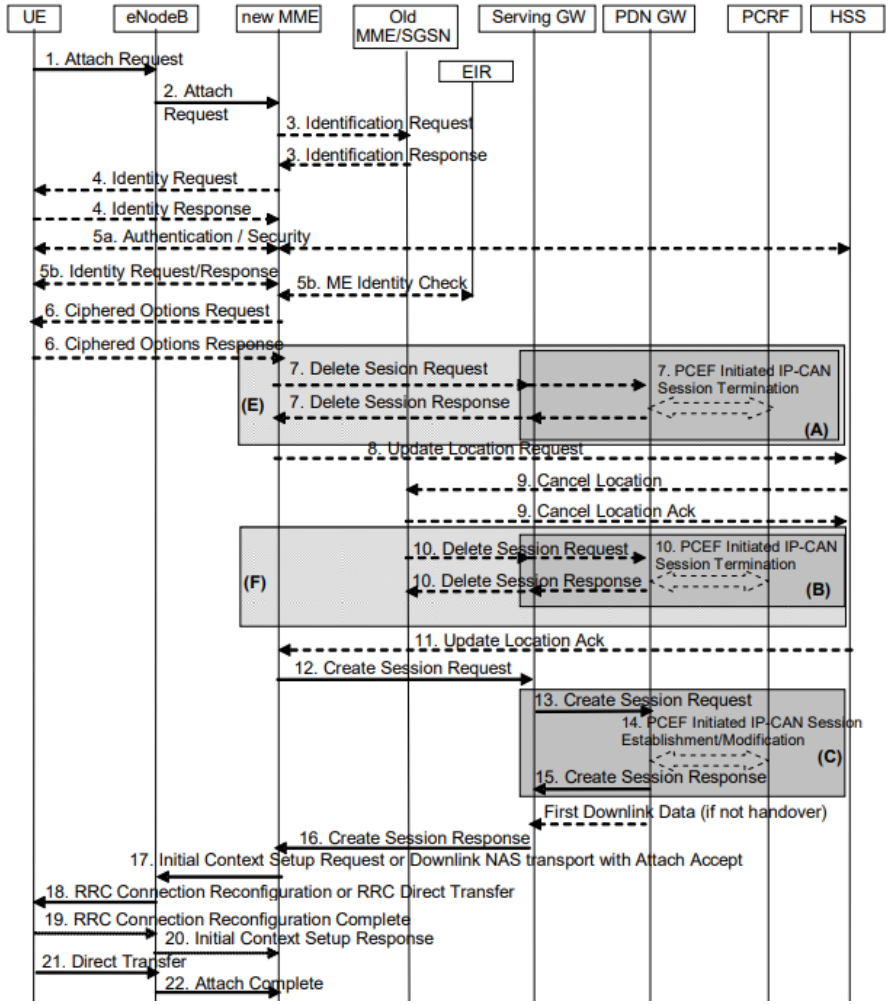
LTE 네트워크 프로토콜 상태 모델 추출 툴(FUZZER)

State machine 추출

❖ Step 1: 테스트하고자 하는 메시지 타입 선정

```
Target message: ATTACH REQUEST
Send: ATTACH_REQUEST (IV, ITP, Plain, MIN, Itp_as_EPS, Native_valid, IMSI_valid, NULL)
Recv: AUTHENTICATION_REQUEST (Plain, Native_valid)
Send: AUTHENTICATION_RESPONSE (IV, ITP, Plain, MIN, MIN)
Recv: AUTHENTICATION_REJECT (Plain)
```

결정된 메시지 타입 예시



State machine 추출

❖ Step 2: 선정한 테스트 메시지의 다양한 변종 생성

```
Target message: ATTACH_REQUEST (IV, EPS, Plain, MIN, EPS, Native valid, IMSI valid, NULL)
Send: ATTACH_REQUEST (IV, ITP, Plain, MIN, Itp_as_EPS, Native_valid, IMSI_valid, NULL)
Recv: AUTHENTICATION_REQUEST (Plain, Native_valid)
Send: AUTHENTICATION_RESPONSE (IV, ITP, Plain, MIN, MIN)
Recv: AUTHENTICATION_REJECT (Plain)
```

생성된 메시지 변종 예시

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Attach request message identity	Message type 9.8	M	V	1
	EPS attach type	EPS attach type 9.9.3.11	M	V	1/2
	NAS key set identifier	NAS key set identifier 9.9.3.21	M	V	1/2
	EPS mobile identity	EPS mobile identity 9.9.3.12	M	LV	5-12
	UE network capability	UE network capability 9.9.3.34	M	LV	3-14
	ESM message container	ESM message container 9.9.3.15	M	LV-E	5-n

State machine 추출

❖ Step 3: 생성된 테스트 메시지 송신 및 응답 로깅

- Stage 0: 4400개의 데이터를 저장.
- Stage 2: 5098개의 데이터를 저장.

```
Target message: ATTACH_REQUEST (Plain, MIN, Itp_as_EPS, Native_valid, IMSI_valid, NULL)
Path length: 0
```

송신한 메시지

```
Target message: AUTHENTICATION_RESPONSE
Send: ATTACH_REQUEST (IV, ITP, Plain, MIN, Itp_as_EPS, Native_valid, IMSI_valid, NULL)
Recv: AUTHENTICATION_REQUEST (Plain, Native_valid)
```

수신한 메시지

LTE 네트워크 프로토콜 상태 모델 분석 툴(ANALYZER)

State machine 추출

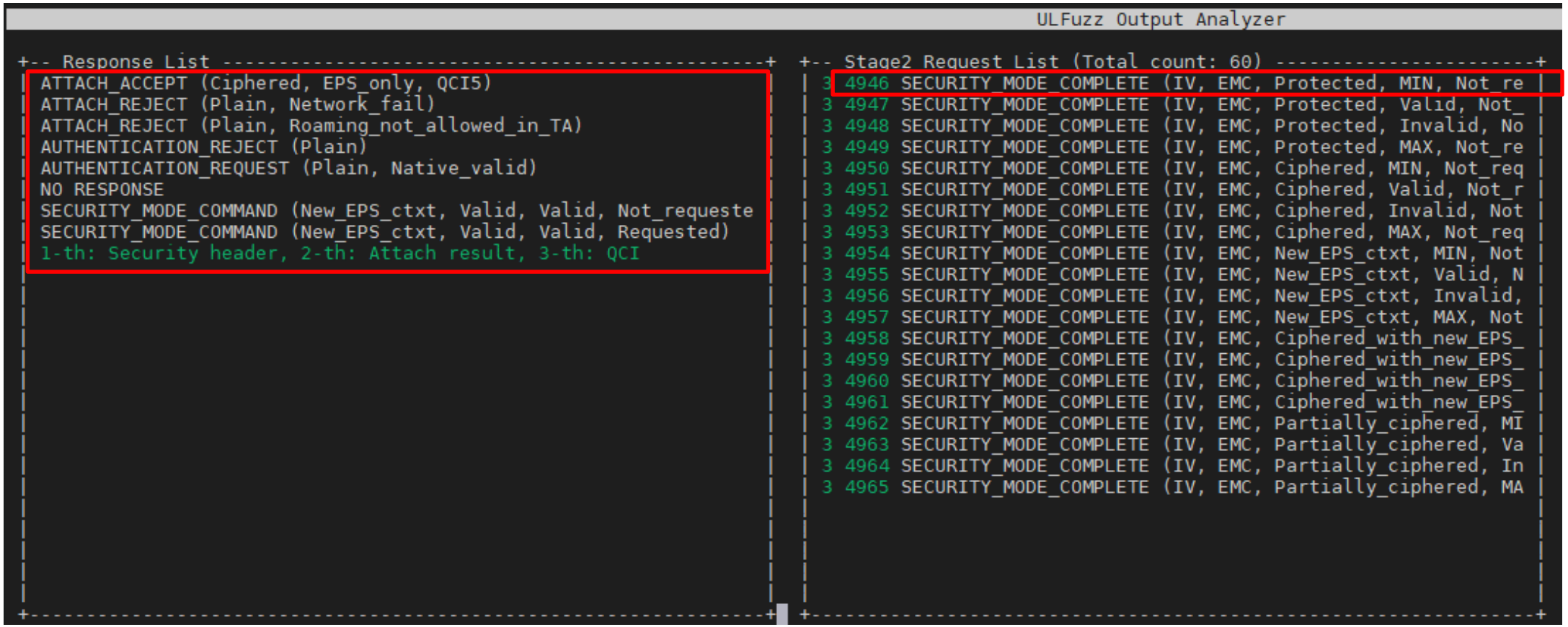
❖ Step 4: 응답결과 분석 후 중복 transition으로 추정되는 transition 선별

```
ULFuzz Output Analyzer

+-- Response List ----------------------------------------------+  +-- Stage2 Request List (Total count: 60) -----------------------+
| ATTACH_ACCEPT (Ciphered, EPS_only, QCI5)                      |  | 3 4946 SECURITY_MODE_COMPLETE (IV, EMC, Protected, MIN, Not_re |
| ATTACH_REJECT (Plain, Network_fail)                           |  | 3 4947 SECURITY_MODE_COMPLETE (IV, EMC, Protected, Valid, Not_ |
| ATTACH_REJECT (Plain, Roaming_not_allowed_in_TA)              |  | 3 4948 SECURITY_MODE_COMPLETE (IV, EMC, Protected, Invalid, No |
| AUTHENTICATION_REJECT (Plain)                                 |  | 3 4949 SECURITY_MODE_COMPLETE (IV, EMC, Protected, MAX, Not_re |
| AUTHENTICATION_REQUEST (Plain, Native_valid)                  |  | 3 4950 SECURITY_MODE_COMPLETE (IV, EMC, Ciphered, MIN, Not_req |
| NO RESPONSE                                                   |  | 3 4951 SECURITY_MODE_COMPLETE (IV, EMC, Ciphered, Valid, Not_r |
| SECURITY_MODE_COMMAND (New_EPS_ctxt, Valid, Valid, Not_requeste |  | 3 4952 SECURITY_MODE_COMPLETE (IV, EMC, Ciphered, Invalid, Not |
| SECURITY_MODE_COMMAND (New_EPS_ctxt, Valid, Valid, Requested) |  | 3 4953 SECURITY_MODE_COMPLETE (IV, EMC, Ciphered, MAX, Not_req |
| 1-th: Security header, 2-th: Attach result, 3-th: QCI         |  | 3 4954 SECURITY_MODE_COMPLETE (IV, EMC, New_EPS_ctxt, MIN, Not |
|                                                               |  | 3 4955 SECURITY_MODE_COMPLETE (IV, EMC, New_EPS_ctxt, Valid, N |
|                                                               |  | 3 4956 SECURITY_MODE_COMPLETE (IV, EMC, New_EPS_ctxt, Invalid, |
|                                                               |  | 3 4957 SECURITY_MODE_COMPLETE (IV, EMC, New_EPS_ctxt, MAX, Not |
|                                                               |  | 3 4958 SECURITY_MODE_COMPLETE (IV, EMC, Ciphered_with_new_EPS_ |
|                                                               |  | 3 4959 SECURITY_MODE_COMPLETE (IV, EMC, Ciphered_with_new_EPS_ |
|                                                               |  | 3 4960 SECURITY_MODE_COMPLETE (IV, EMC, Ciphered_with_new_EPS_ |
|                                                               |  | 3 4961 SECURITY_MODE_COMPLETE (IV, EMC, Ciphered_with_new_EPS_ |
|                                                               |  | 3 4962 SECURITY_MODE_COMPLETE (IV, EMC, Partially_ciphered, MI |
|                                                               |  | 3 4963 SECURITY_MODE_COMPLETE (IV, EMC, Partially_ciphered, Va |
|                                                               |  | 3 4964 SECURITY_MODE_COMPLETE (IV, EMC, Partially_ciphered, In |
|                                                               |  | 3 4965 SECURITY_MODE_COMPLETE (IV, EMC, Partially_ciphered, MA |
+---------------------------------------------------------------+  +----------------------------------------------------------------+
```

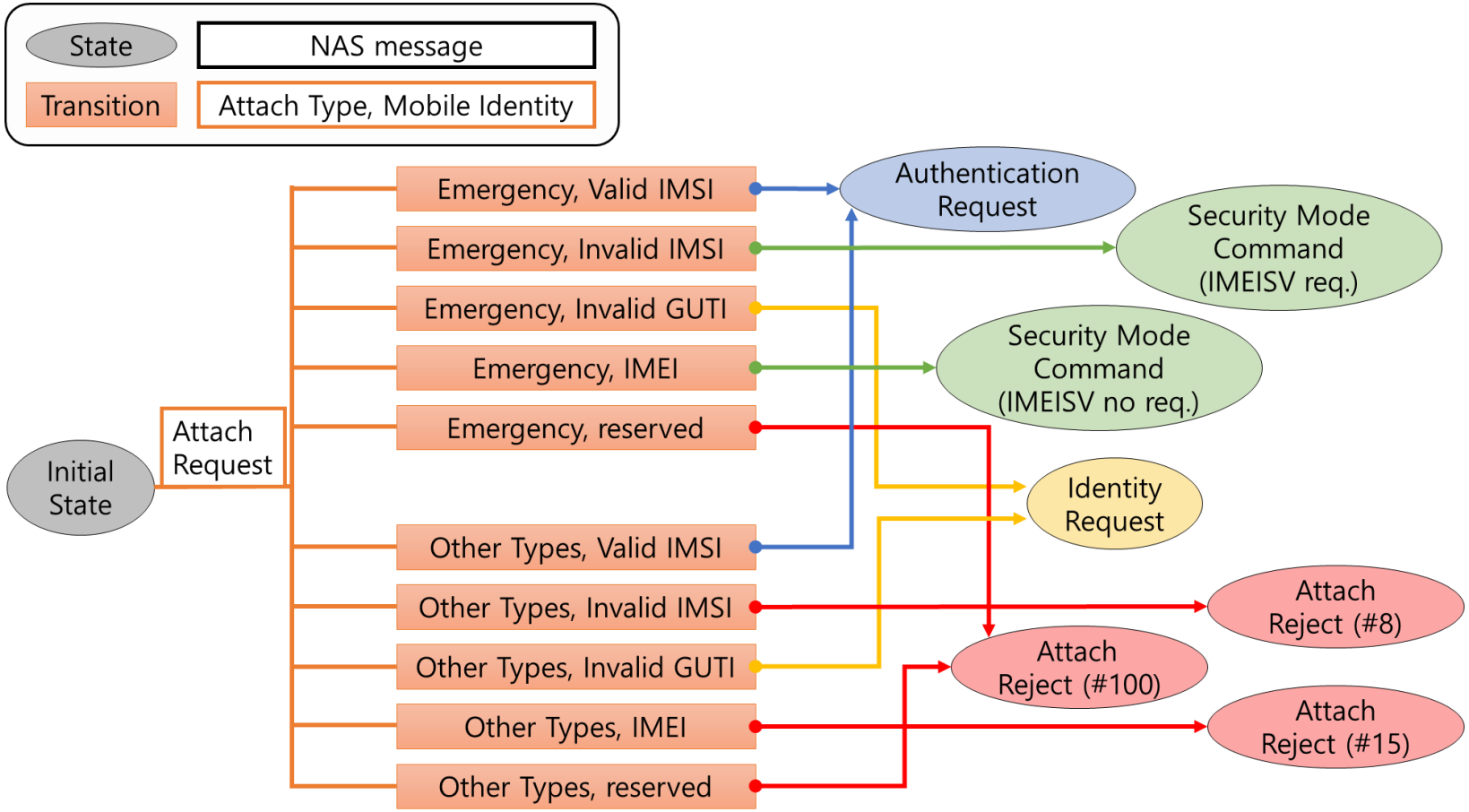
State machine 추출

❖ Step 4: 응답결과 분석 후 중복 transition으로 추정되는 transition 선별



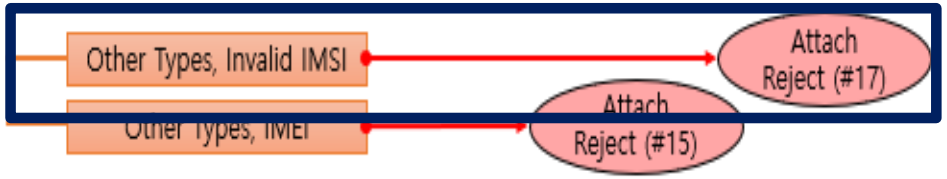
연구 결과

❖ 추출된 State machine – Stage 0



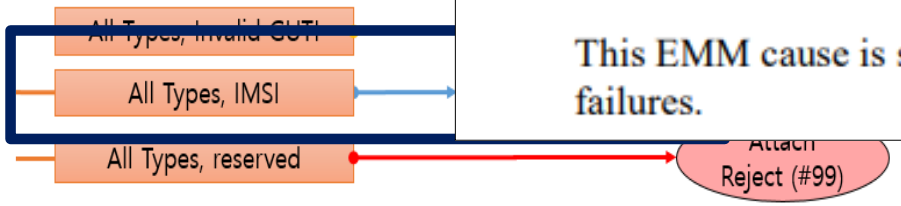
연구 결과

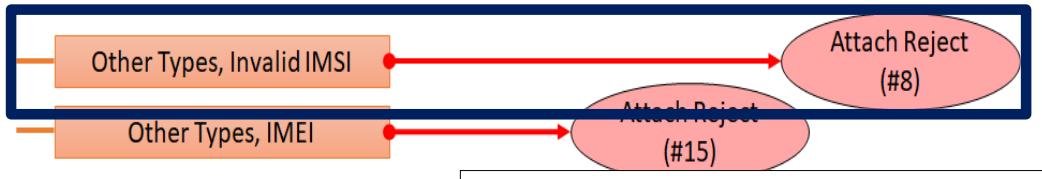
❖ 추출된 State machine – Stage 0



Cause #17 – Network failure

This EMM cause is sent to the UE if the MME cannot service an UE generated request because of PLMN failures.



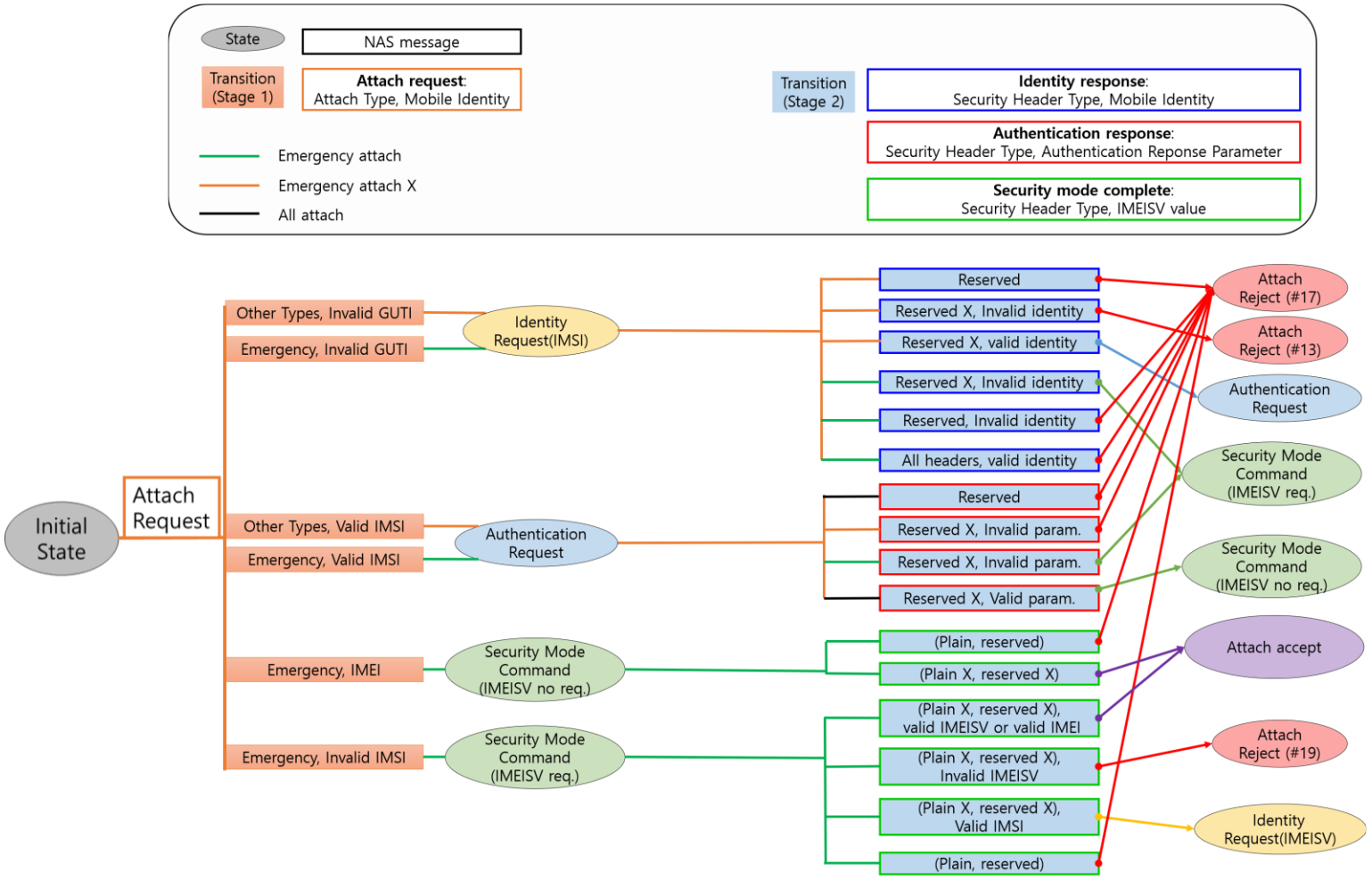


Cause #8 – EPS services and non-EPS services not allowed

This EMM cause is sent to the UE when it is not allowed to operate either EPS or non-EPS services.

연구 결과

❖ 추출된 State machine – Stage 2



결론

- 이동통신 네트워크 장비 제어 평면의 동작 State machine을 추출하기 위해 Fuzzer, Analyzer 2개의 툴을 개발.
- 3GPP 표준 문서와 각 통신사별 장비의 비교를 통해 총 7개의 이상 동작을 발견.
- 다른 시나리오로 진행되는 NAS 메시지에 대한 state machine 확장을 통해 추가적인 이상 동작을 확인할 수 있을 것이다.