Evaluation of Authentication Signaling Loads in 3GPP LTE/SAE

Chan-Kyu Han, **Hyoung-Kee Choi**, Jung Woo Baek, Ho Woo Lee

Sungkyunkwan University

hkchoi@ece.skku.ac.kr

IEEE LCN 2009, Zürich, Switzerland, 20-23 October, 2009

SUNG KYUN KWAN UNIVERSITY

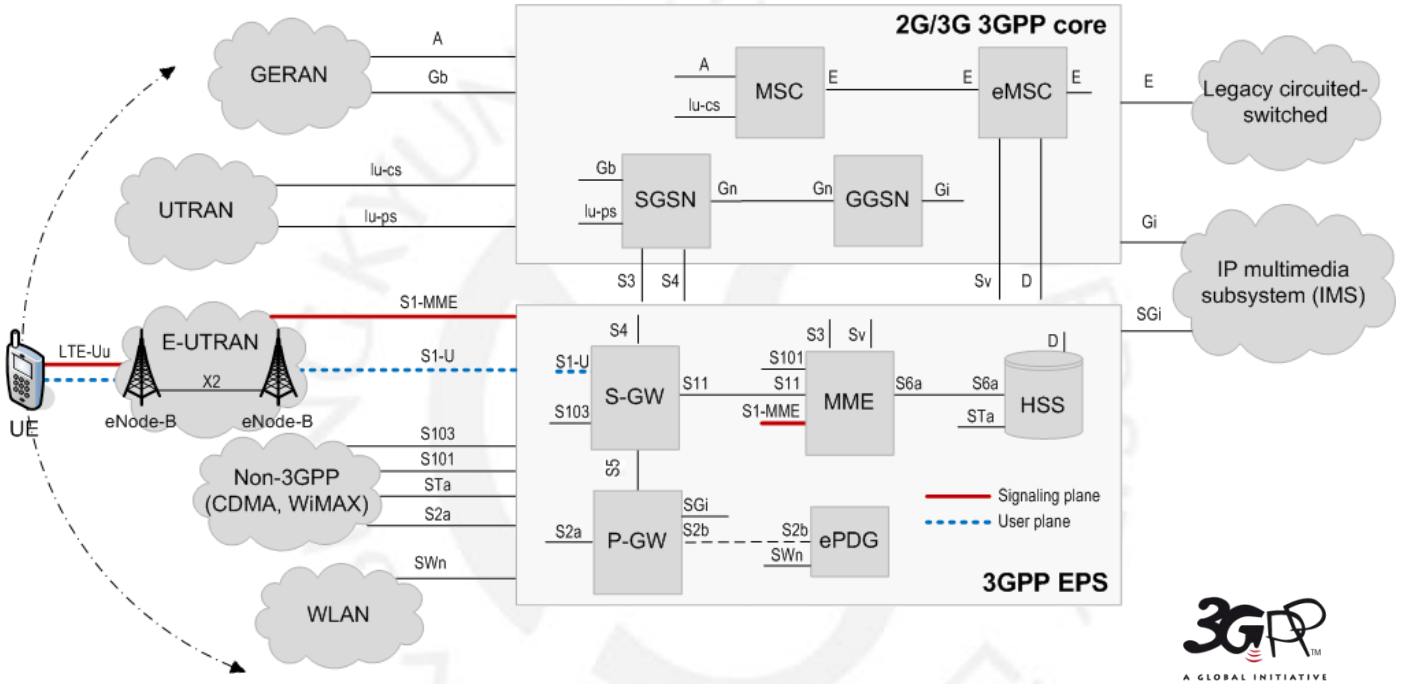
School of Information and Communication Engineering

Computer Engineering

In a Nutshell

- Introducing the revised security architecture in 3GPP LTE/SAE
- Relaxing the Poisson assumption in authentication request process
  - Renewal process and renewal reward theorem
- Exploring new authentication triggers
  - *e.g.* horizontal and vertical handover, multimedia requests
- Observing signaling cost of each authentication event
- Analyzing the effect of arrival rate, exceptional case, various random processes on signaling loads in mobile networks

3GPP LTE/SAE



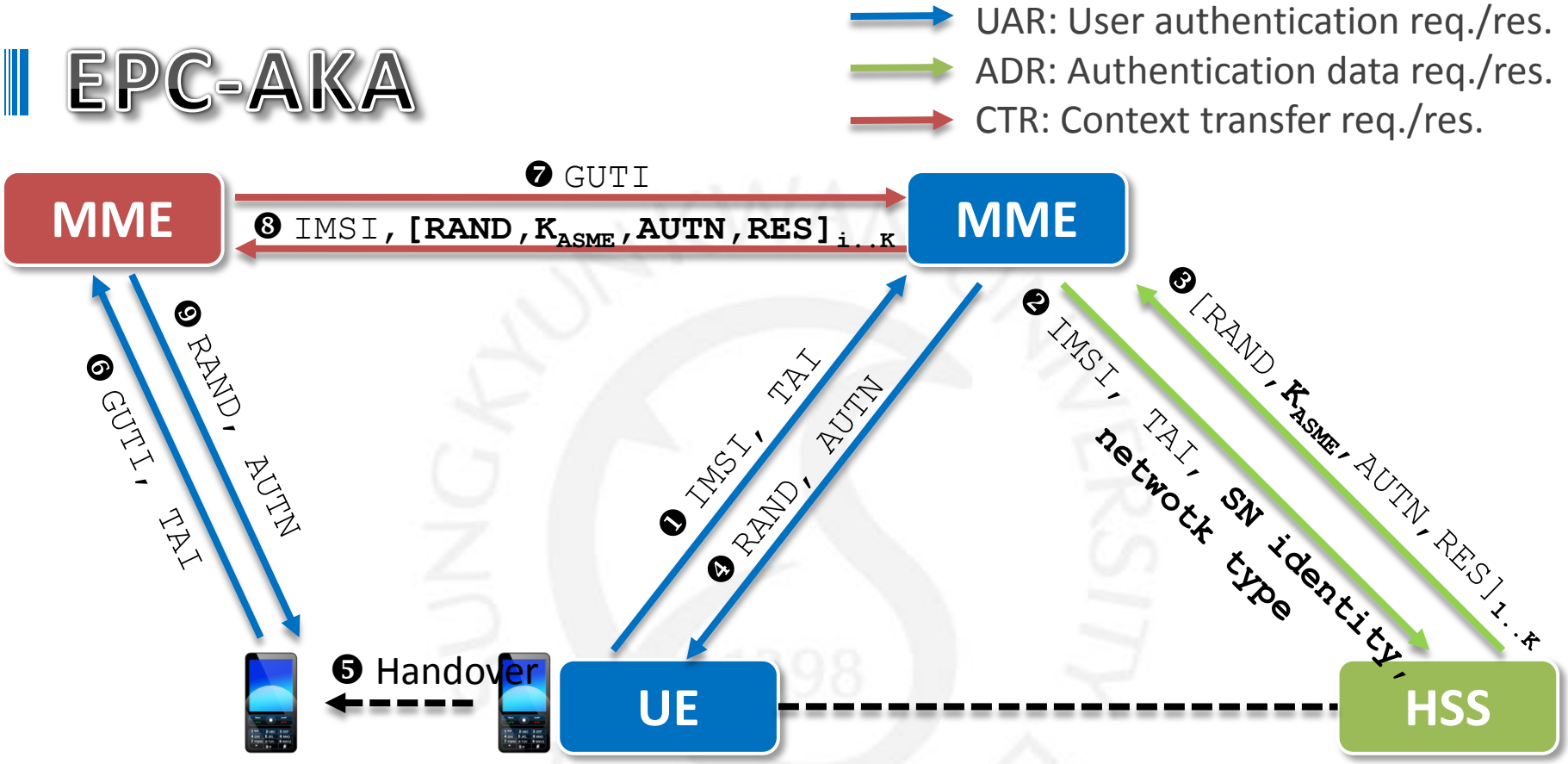
Multiple-access network	Heterogeneous mobility	All IP-based multimedia service	Revised UMTS-AKA

Long Term Evolution (Evolved-UTRAN)	**System architecture evolution** (Evolved Packet System)

HIT

SUNG KYUN KWAN UNIVERSITY

EPC-AKA



- One set of authentication vector for performance reason
  - Backward compatibility for vector-based UMTS-AKA
- Including network identity to prevent redirection attack
- Key hierarchy: (CK, IK) for HSS/AuC and K_{ASME} for MME

COMPARISONS

Criteria	UMTS-AKA	EPC-AKA
Vulnerability	Redirection, false BS attack [ZHANG05-IEEE Trans.Wcomm.]	Has not been reported
Authentication	Vector-based	Vector- or key reuse-based
ID protection	TMSI (*limited*)	GUTI(*limited*)
Key material	CK, IK (VLR, HLR/AuC)	K_{eNB}(eNodeB), K_{ASME}(MME), CK and IK (HSS)
Confidentiality	Only at the AS	AS and NAS (signaling only)
Integrity	Only at the AS	AS and NAS
Support	(1) Call origin./termin. (2) Location update	(1) Call origin./termin. (2) Multimedia service (3) Various location update

Challenges for mathematical analysis

- Various authentication request types
  - i.e., call origination/termination, multimedia service, X2/S1 handover and Inter RAT handover
- Various random processes rather than Poisson assumption
- Repeated ADR request every K UAR/CTR request
- Signaling cost for every repeated authentication cycle

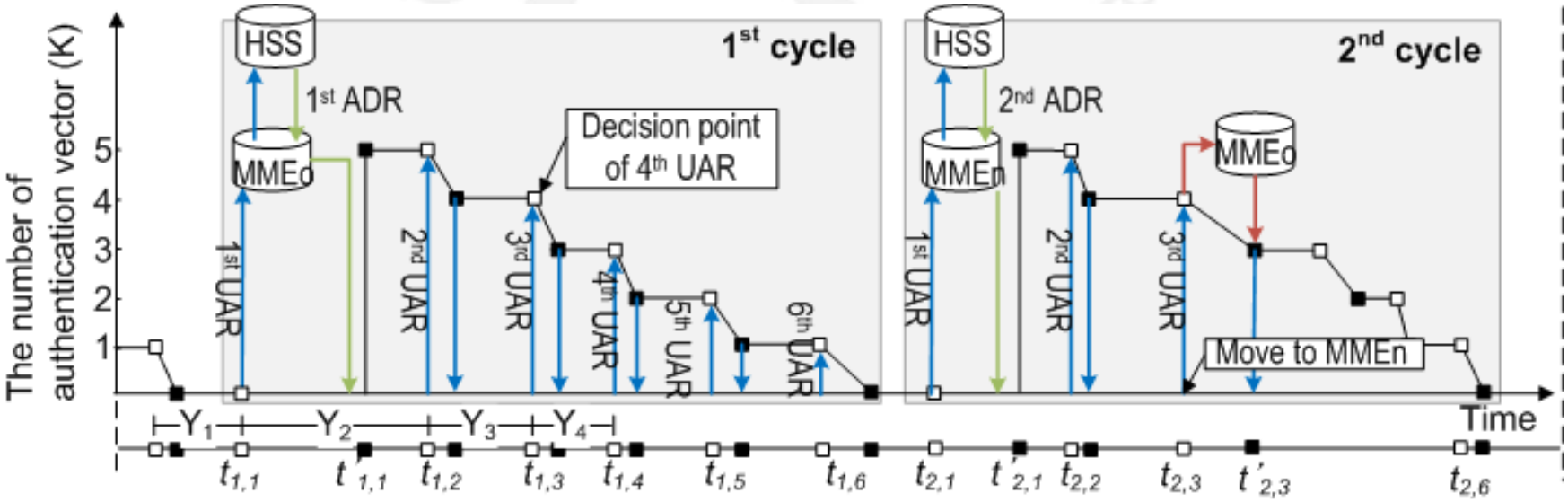
RENEWAL REWARD THEOREM

- R(t) : total reward earned by t
- N(t) : the counting process of renewal process X
- E[R] : expected reward (cost)
- E[X] : expected length of renewal process X

$$\lim_{t\to 0}\frac{R(t)}{t} = \lim_{t\to 0}\frac{\sum_{n=1}^{N(t)} R_n}{N(t)} \cdot \frac{N(t)}{t} = \frac{E[R]}{E[X]}$$

Modeling of vector-based EPC-AKA

- $t_{x,y}$: x-th ADR within y-th UAR
- Y_i: duration of each authentication event
- $[t_{n,K}, t_{n+1,K}]$: The expected value of the renewal interval



Renewal process

- Recursive and reproductive process
- Renewal epoch: $[t_{n,K}]$

EXPECTED SIGNALING COST

- f(Y) : probability density function of renewal length Y
  - Bernoulli distribution with p_i for each authentication trigger X_i

$$f(Y) = \sum_{i=1}^{M} p_i \cdot f(X_i), \quad \text{where} \sum_{i=1}^{M} p_i = 1$$

  - X_i: i-th authentication trigger
    - call origination/termination, multimedia service, X2/S1 handover and Inter RAT handover
    - M: number of authentication trigger (=5)
- C_i : the total signaling cost of completion of X_i
  - K: the number of authentication vector

$$E[R] = C_0 + (K-1) \cdot E[Y] \cdot C_{i(1 \le i \le M)}$$

$$= C_0 + \sum_{j=1}^{K-1} j \cdot \left(\sum_{i=1}^{M} p_i \cdot E[X_i] \cdot C_i\right)$$

TOTAL AUTHENTICATION SIGNALING COST

- $C(K)$: normalized expected signaling cost
- p_ε: exceptional authentication trigger
  - $p_{\varepsilon,k} = p_\varepsilon \cdot (1 - p_\varepsilon)^k$
  - i.e., power-off, S1 handover to different domain, and Non-3GPP access
- D: SIP signaling load and processing time for generating authentication vector

$$C(K) = \frac{E[R]}{E[N]} = \frac{C_0 + \sum_{k=1}^{K-1} p_{\varepsilon,k} \cdot \left(\sum_{i=1}^{M} (K-1) \cdot p_i \cdot E[X_i] \cdot C_i \right) \cdot C_\varepsilon}{K \cdot \int_{t=1}^{\infty} Y \cdot f(Y) \cdot dt + E[D]}$$

Modeling of key reuse-based EPC-AKA

- Without multiple authentication vectors
  - Key revocation: K_{ASME} either is *compromised* or *reaches the period of* T

$$C(t) = \sum_{i=1}^{M} p_i \frac{E[R]}{E[N]}$$

- $T(x_i)$ /$t(x_i)$: the CDF/PDF of lifetime T of K_{ASME}

$$E[N] = \int_0^{\infty} E(Y \mid X = x) \cdot dT(x)$$

$$= \int_0^{T} x \cdot t(x) \cdot dx + \int_T^{\infty} T \cdot t(x) \cdot dx$$

- C_{-1}: rekeying cost for all EPS network entities
  - when K_{ASME} is compromised

$$E[R] = (C_{-1} + C_i) \cdot \int_0^{T} t(x)dx + C_i \int_T^{\infty} t(x)dx$$

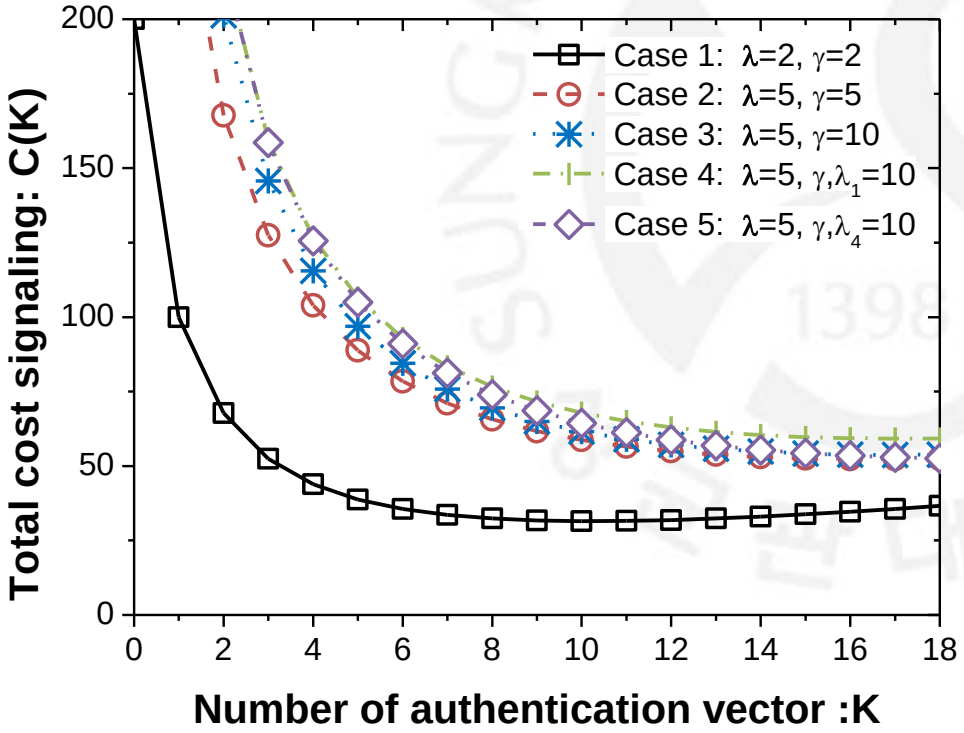
COST FUNCTION

Cost	Authentication event	Asymptotic signaling cost
C_0	Authentication vector fetch to HSS	$2\alpha+2\beta+4\gamma+K\ C_{SHA-1}$
C_1	Call origination	$4\alpha+9\beta$
	Call termination	$2\alpha+5\beta$
C_2	Multimedia request	$4\alpha+4\beta+4\gamma$
C_3	X2 handover	$4\alpha+10\beta+3\gamma$
C_4	S1 handover	$6\alpha+14\beta+21\gamma$
C_4	Inter RAT handover	$2\alpha+7\beta+13\gamma$
C_{TAU}	Tracking area update (TAU)	$4\alpha+6\beta+3\gamma$
C_{-1}	Revocation / Rekeying	$C_0+2\alpha+2\beta+2\gamma$

α: RTT between UE and eNodeB
β: RTT within the EPC core
γ: RTT across the serving domain

Effect of arrival rate

- λ_i: inter-arrival process for X_i
  - exponential distribution for all authentication triggers



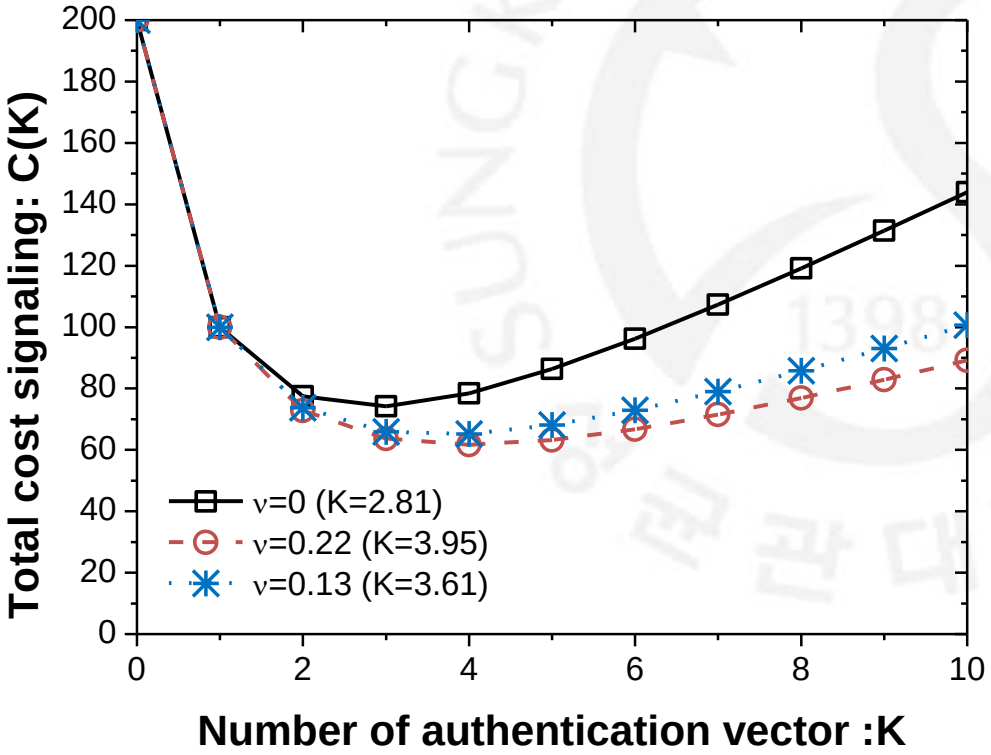
- Arrival rate (λ_i)
  -Increasing cost (Case 1 and 2)

- Setup delay
  -Insignificant (Case 2 and 3)

- Signaling cost (X_4): greater effect on increasing signaling cost (Case 4 and 5)
  C_4: 6α+14β, C_4: 4α+14β+21γ

Effect of authentication probability

- p_i: the probability of each authentication trigger X_i
- v: the distribution pattern of p_i (variance)

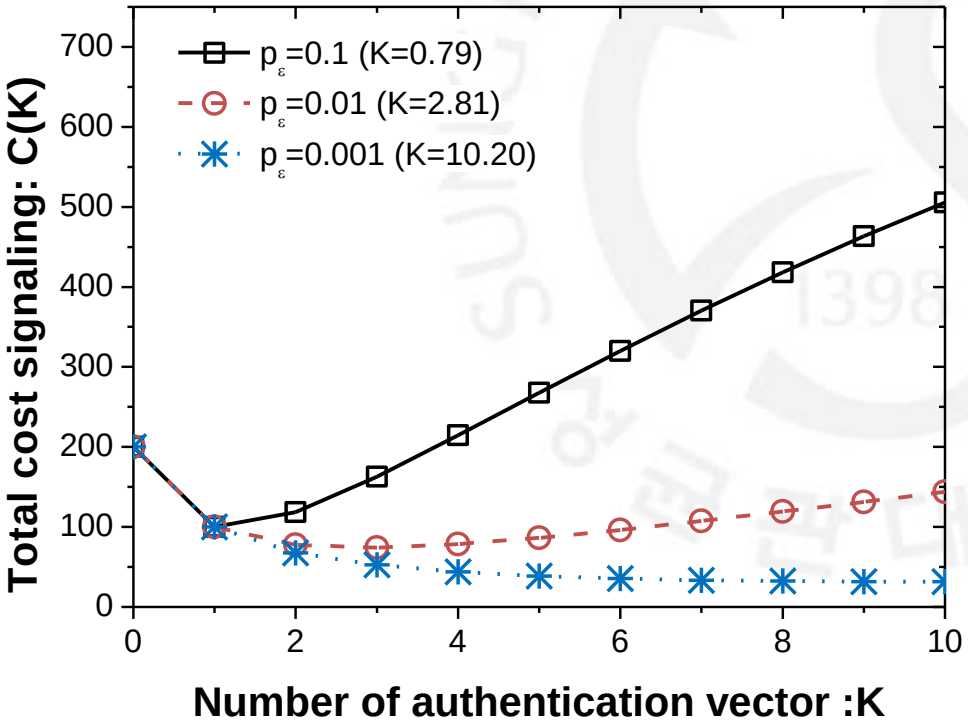


• lower variation
- decreasing the optimal K
- Minimizing C(K)

• propensity to be incline to a certain event
- *e.g.*, teen-ager, business man
- less agitates system

Effect of exceptional case

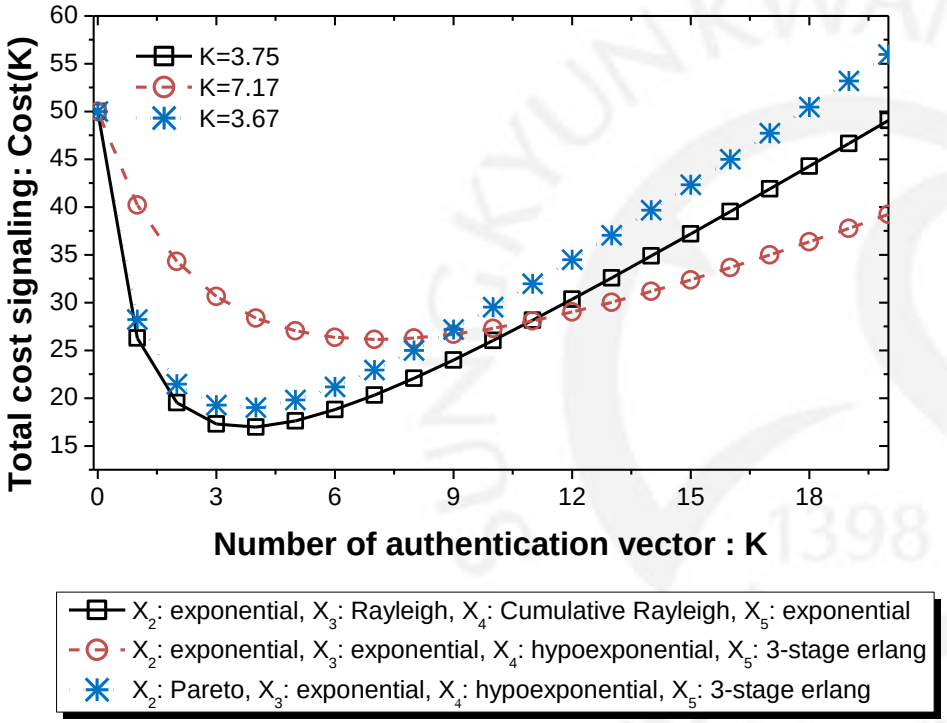
- p_ε: exceptional authentication trigger
  - i.e., power-off, S1 handover to different domain, and Non-3GPP access



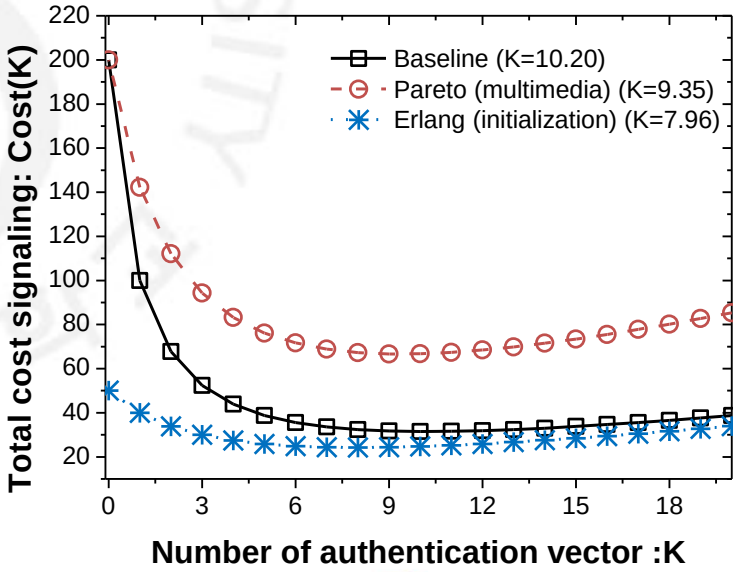
- Higher p_ε
  -increasing the total signaling cost
  -Decreasing the optimal K value

- Optimal K value < 1 (p_ε =0.1)
  - vector-based EPC-AKA is meaningless

EFFECT OF VARIOUS RANDOM PROCESSES



- Rayleigh distribution
  - Two-dimensional vector
  - suitable for handover (the subscriber's velocity and cell coverage by eNodeB)



- Pareto distribution
  - suitable for multimedia services
- The baseline without Pareto
  - Suffers from Underestimation

HIT

SUNG KYUN KWAN UNIVERSITY

SUMMARY

- An introduction of security in 3GPP LTE/SAE
  - Authentication procedures
  - Type of handovers
- Mathematical framework for analyzing authentication signaling load
- Numerical results: the effects of
  - Various random processes,
  - Examined the arrival rate,
  - Exceptional case, etc.
- Our result establishes the necessity of studying mobility management, security policy, and various random arrival processes

Questions?

- For more information:
  - http://hit.skku.edu/~hedwig/