Vien, Quoc-Tuan ORCID logoORCID: https://orcid.org/0000-0001-5490-904X, Le, Tuan Anh ORCID logoORCID: https://orcid.org/0000-0003-0612-3717, Yang, Xin-She ORCID logoORCID: https://orcid.org/0000-0001-8231-5556 and Duong, Trung Q. (2017) On the handover security key update and residence management in LTE networks. IEEE Wireless Communications and Networking Conference (WCNC 2017). In: IEEE Wireless Communications and Networking Conference (WCNC 2017), 19-22 Mar 2017, San Francisco, CA, USA. ISBN 978-1-5090-4183-1. ISSN 1558-2612 [Conference or Workshop Item] (doi:10.1109/WCNC.2017.7925678)

Final accepted version (with author's formatting)

This version is available at: https://eprints.mdx.ac.uk/21818/

On the Handover Security Key Update and Residence Management in LTE Networks

Quoc-Tuan Vien†, Tuan Anh Le†, Xin-She Yang†, Trung Q. Duong‡
†Middlesex University, London, United Kingdom. Email: {q.vien, t.le, x.yang}@mdx.ac.uk.
‡Queen's University Belfast, Northern Ireland, United Kingdom. Email: trung.q.duong@qub.ac.uk.

***Abstract*—In LTE networks, key update and residence management have been investigated as an effective solution to cope with desynchronization attacks in mobility management entity (MME) handovers. In this paper, we first analyse the impacts of the key update interval (KUI) and MME residence interval (MRI) on the handover performance in terms of the number of exposed packets (NEP) and signaling overhead rate (SOR). By deriving the bounds of the NEP and SOR over the KUI and MRI, it is shown that there exists a tradeoff between the NEP and the SOR, while our aim is to minimise both of them simultaneously. This accordingly motivates us to propose a multiobjective optimisation problem to find the optimal KUI and MRI that minimise both the NEP and SOR. By introducing a relative importance factor between the SOR and NEP along with their derived bounds, we further transform the proposed optimisation problem into a single-objective optimisation problem which can be solved via a simple numerical method. In particular, the results show that a higher accuracy of up to 1 second is achieved with the proposed approach while requiring a lower complexity compared to the conventional approach employing iterative searches.**

I. Introduction

The LTE network supports two types of handovers, i.e. intra and inter mobility management entity (MME) handovers [1]–[3]. In the intra MME handover, i.e. when a user equipment (UE) moves from a source to a target eNodeB[1] within the same MME, the source eNodeB provides the target eNodeB with a new session key[2] to be used after handover. The new key is generated from the current one by either utilising a one-way function, a.k.a. *backward key separation* process, or adding fresh materials to the process of generating the new one, a.k.a. *forward key separation* process. As eNodeBs are exposed to the public locations and the internet-protocol-architecture nature of the network, handover-key management process is vulnerable to attacks deployed by bogus eNodeBs [5]. Such attacks are referred to as desynchronization attacks [6], [7].

The aim of desynchronization attacks is to prevent target eNodeBs from adding the fresh materials thus breaking the forward key separation process. Consequently, attacker can either decipher the communications between a genuine eNodeB and a UE or compromise all future keys between specific UEs and eNodeBs for further active attacks. The effects of desynchronization attacks will be terminated at the next update of the root key when handover key materials are generated from scratch instead of deriving from previous keys. The root key update is requested by a UE or happens when a UE moves from one to another MME, i.e. inter MME handover [8], [9].

Determining the root key update interval (KUI) has been identified as an effective solution to tackle the desynchronization attacks, see e.g. [6], [10], [11]. In [6], a mathematical model was developed to represent the average number of exposed packages (NEP) between two root key updates and the average value of signaling overhead rate (SOR)[3]. A heuristic algorithm was also proposed in [6] to search for an optimal root KUI based on empirical data. However, such iterative search requires a high computational complexity causing a considerable handover processing delay, especially when considering a large network with a large number of nodes.

In this paper, we investigate the impacts of not only KUI but also MME residence interval (MRI) on the handover performance in terms of NEP and SOR. Specifically, in order to provide insightful meanings of the NEP and SOR expressions, we first derive their upper and lower bounds over the KUI and MRI. The derived bounds are helpful not only in capturing their behaviours at the boundary values of the KUI and MRI, but also in showing that there exists a trade-off between the NEP and the SOR. However, our aim is to minimise both of them. Therefore, as a second contribution of this paper, we propose a multiobjective optimisation problem to find the optimal KUI and MRI that minimise both the NEP and SOR. Due to the two objectives, i.e. NEP and SOR, are conflicting, a relative importance parameter is introduced to balance these two objectives with priority, and consequently allows us to convert the multiobjective optimisation problem to a single-objective optimisation problem which can be solved via a simple numerical method using the derived bounds of the NEP

[1] A node/access-point provides all radio access protocols.

[2] Session keys are used to encrypted messages, i.e. user data and signaling packets, exchanged between a UE and its serving eNodeB [4].

[3] The SOR is defined as the average number of bits for individual authentication among the UEs, the MME and the home subscriber server/authentication centre during MME handover. The analysis of authentication transmission overhead as well as impacts of the handover process and security issues with encrypted keys can be referred to in [12]–[16].

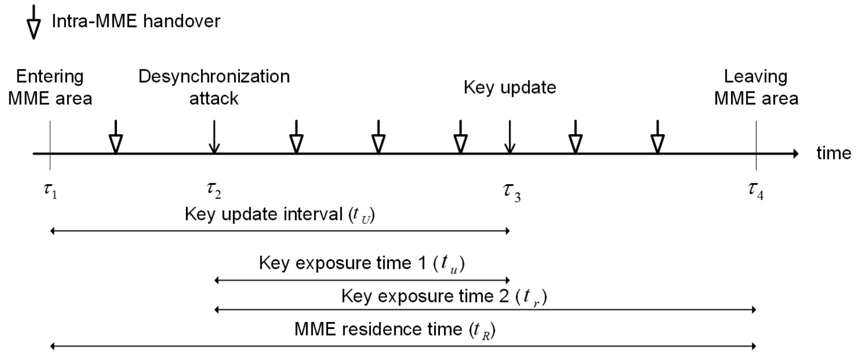


Fig. 1: Timing diagram of MME residence with key update and vulnerable attack periods [6].

and SOR. The proposed method can therefore avoid the conventional iterative searches in [6]; hence, it not only reduces the complexity but also improves the reliability, which in turns reflects the novelty of our work in deriving the aforementioned bounds.

II. System Model

Figure 1 illustrates the timing diagram of MME residence in a typical LTE network [6]. Consider the following times in a chronological order τ_1, τ_2, τ_3 and τ_4. At τ_1 and τ_4, a UE enters and leaves the MME area, respectively. Let $t_R = \tau_4 - \tau_1$ be a full MME residence time. At τ_2 and τ_3, there are a desynchronization attack and a root key update requested by the UE, respectively. The effect of a desynchronization attack will be eliminated at either the time of the update of the root key or the time when the UE leaves the MME. Let $t_U = \tau_3 - \tau_1$ be the interval time of the key update. Furthermore, let $t_u = \tau_3 - \tau_2$ and $t_r = \tau_4 - \tau_2$ denote the key exposure times. The vulnerable period t_c is defined as $\min\{t_u, t_r\}$ where $0 \leq t_u < t_R$ and $0 \leq t_r < t_R$. If $\tau_3 \leq \tau_2$, then $t_c = t_r$.

Following the same approach in [6], let us assume that KUI, i.e. t_U, follows an exponential distribution with mean of $T_U = 1/\mu_u$ where μ_u is the key update rate, and MRI, i.e. t_R, follows a gamma distribution [17] with a shape parameter of $k \geq 0$, mean of $T_R = k/\mu_r$ and variance of $\sigma_R^2 = k/\mu_r^2$ where μ_r represents the mobility rate.

III. Bounds of the NEP and SOR

During the vulnerable period, i.e. t_c, user data and signaling packets exchanged between the UE and eNodeB are exposed to eavesdroppers. The average number of exposed packets (NEP), i.e. $E[N]$, and the average signalling overhead rate (SOR), i.e. $E[S]$, can be expressed as in [6], i.e.

$$E[N] = \frac{\lambda_p}{\mu_u}\left(1 - \frac{\mu_r}{\mu_u k}\left(1 - \left(\frac{\mu_r}{\mu_u + \mu_r}\right)^k\right)\right), \quad (1)$$

$$E[S] = \frac{\rho}{\dfrac{1}{\mu_u} + \dfrac{k}{\mu_r}}, \quad (2)$$

where λ_p is the mean arrival rate of packets exchanged between the UE and eNodeB, and ρ is the number of bits in the messages for individual authentication among the UEs, the MME and the home subscriber server/authentication centre.

In order to provide insightful meanings of the above expressions, let us derive the limits of the average NEP and SOR as the average root KUI T_U and MRI T_R approach 0 and ∞. The findings are presented in the following three lemmas.

Lemma 1. *The average NEP, i.e. $E[N]$, is an increasing function of $T_U \in (0, \infty)$, which is lower bounded by $N_{\min}^{(T_U)} = 0$ and upper bounded by*

$$N_{\max}^{(T_U)} = \frac{\lambda_p(k+1)}{2\mu_r}. \quad (3)$$

Proof. See Appendix A. □

Lemma 2. *The average NEP, i.e. $E[N]$, is an increasing function of $T_R \in (0, \infty)$, which is upper bounded by*

$$N_{\max}^{(T_R)} = \frac{\lambda_p}{\mu_u}, \quad (4)$$

while it is lower bounded by

$$N_{\min}^{(T_R)} = \frac{\lambda_p}{\mu_u}\left(1 + \frac{\mu_r}{\mu_u}\log\left(\frac{\mu_r}{\mu_u + \mu_r}\right)\right) \quad (5)$$

when $k \to 0$ and $N_{\min}^{(T_R)} = 0$ when $\mu_r \to \infty$.

Proof. See Appendix B. □

Lemma 3. *The average SOR, i.e. $E[S]$, is a decreasing function of both $T_U \in (0, \infty)$ and $T_R \in (0, \infty)$, in which both are lower bounded by 0, while they are upper bounded by*

$$S_{\max}^{(T_U)} = \frac{\rho\mu_r}{k} = \frac{\rho}{T_R}, \quad (6)$$

$$S_{\max}^{(T_R)} = \rho\mu_u = \frac{\rho}{T_U}. \quad (7)$$

Proof. (6) and (7) can be easily obtained from (2) with a notice that $T_U = 1/\mu_u$ and $T_R = k/\mu_r$. □

Lemmas 1, 2 and 3 indicate a fact that reducing either the KUI or MRI lowers the risk of security breaches, i.e. reducing NEPs, at the cost of an increase in signaling overhead. Hence, minimising the average NEP over either T_U or T_R is contradicting with minimising the average SOR. In the next Section, we introduce a method to find optimal values of T_U and T_R in order to balance between the two conflicting objectives.

IV. Optimal KUI & MRI

We first bring the average NEP and SOR into the same scale by defining the following normalised functions

$$\begin{aligned} S(x) &= E[S]/S_{\max}^{(x)}, && (8)\\ N(x) &= E[N]/N_{\max}^{(x)}, && (9) \end{aligned}$$

where $x \in \{T_U, T_R\}$, and $N_{\max}^{(T_U)}$, $S_{\max}^{(T_U)}$, $N_{\max}^{(T_R)}$ and $S_{\max}^{(T_R)}$ are given by (3), (6), (4), (7), respectively. From Lemmas 1, 2 and 3, one can show that $S(x)$ and $N(x)$ are decreasing and increasing functions, respectively, with respect to x. Since $S(x)$ and $N(x)$ are contradicting functions over x, finding an optimal x that minimises both functions is actually to solve the following multiobjective optimisation problem[4] [18]:

$$\min_{x\in[0,\infty)} \quad \mathbf{f}\left(x\right) = \min_{\mathbf{x}\in[0,\infty)} \left(S\left(x\right), N\left(x\right)\right). \qquad (10)$$

Generally, there is no single solution that simultaneously optimises the above two conflicting objectives. However, there exists a set of Pareto optimal solutions, i.e. Pareto frontier [18], [19]. The Pareto frontier is obtained by specifying the priority of each objective which is normally decided by the network operator. In the following, we address a typical scenario that the network operator would be using[5].

Let $\nu(x) = N(x)/S(x)$ denote the ratio of the normalised NEP to the normalised SOR. Furthermore let δ be the relative importance determined by the network operator as the ratio of NEP to SOR. We now introduce the following single-objective optimisation problem to find the optimal solution x while balancing the two conflicting objectives.

$$\begin{aligned} &\min_{x\in[0,\infty)} && x \\ &\text{s. t.} && \nu(x) \geq \delta. \end{aligned} \qquad (11)$$

Lemma 4. *The optimal solution to* (11) *can be obtained by*

$$x_{opt} = x | \nu(x) = \delta. \qquad (12)$$

Proof. It can be shown that $\nu(x)$, $x \in \{T_U, T_R\}$, is an increasing function with respect to x since $S(x)$ and $N(x)$ are decreasing and increasing functions, respectively, over x. Therefore, the optimal solution to (11) can be obtained by solving the equation $\nu(x) = \delta$. The Lemma is proved. □

Remark 1. *It can be noticed that, if $\delta \to 0$, then solving* (12)*, i.e. $\nu(x) \to 0$, means $N(x) \to 0$ and $S(x) \to 1$. Similarly, if $\delta \to \infty$, then we need to solve $\nu(x) \to \infty$, i.e. $S(x) \to 0$ and $N(x) \to 1$.*

In fact, as shown later in the numerical results, for every value of δ, the optimal values of T_R and T_U are the crossing points between the line $S(x) = N(x)/\delta$ and the curve $S(N(T_R))$ and $S(N(T_U))$, respectively.

Remark 2. *It can be observed that, by deriving the bounds of the average NEP and the average SOR in Section III, the optimisation problem in* (11) *can be easily solved numerically (see Lemma 4), rather than performing iterative searches as in the conventional approach, e.g. [6]. This not only helps reduce the complexity in finding the optimal solutions, but also improves the reliability with numerical approach, which accordingly reflects the novelty of our work in finding the bounds for the NEP and SOR in Section III.*

V. Numerical Results

In this section, we present numerical results of two performance measures, including NEP and SOR, along with the optimisation of the KUI and MRI for the handover security key management.

A. Impacts of KUI and MRI on NEP Performance

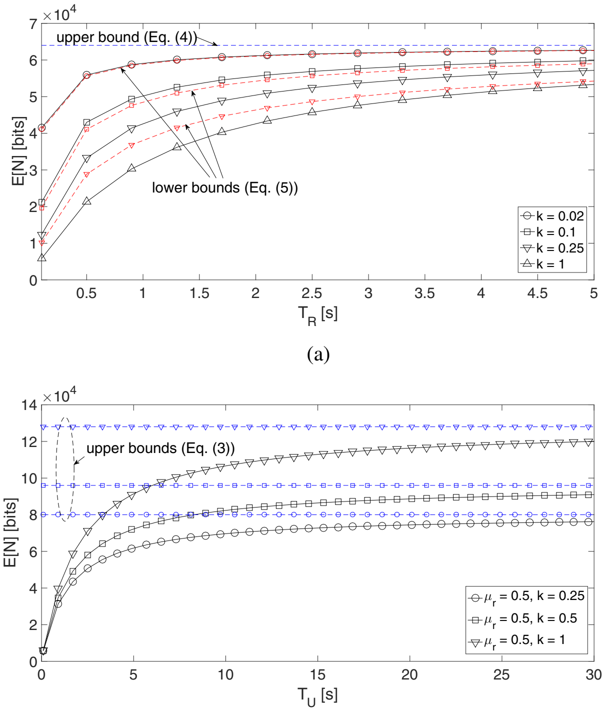
Figure 2 plots the average NEP, i.e. $E[N]$ [bits], as a function of MRI, i.e. T_R [s], and KUI, i.e. T_U [s], for various scenarios of mobility rate, i.e. μ_r, and shape parameter, i.e. k, of the gamma distribution. It is assumed that the mean arrival rate of packets exchanged between the UE and eNodeB is $\lambda_p = 64$ kbits/s. In Fig. 2(a), T_U is set to be 1 s and k varies in $\{0.02, 0.03, 1\}$, while three pairs of $\{\mu_r, k\}$, including $\{\mu_r = 0.5, k = 0.25\}$, $\{\mu_r = 0.5, k = 0.5\}$ and $\{\mu_r = 0.5, k = 1\}$, are considered in Fig. 2(b) to represent various scenarios of $T_R = k/\mu_r = \{0.5, 1, 2\}$ s. The upper and lower bounds are plotted using (3), (4) and (5) derived in Lemmas 1 and 2. It can be observed in both Figs. 2(a) and 2(b) that all the simulation results approach the derived bounds and the average NEP increases as either T_U or T_R increases. This accordingly verifies the statements in Lemmas 1 and 2 regarding the monotonic increasing property of $E[N]$ over T_U and T_R.

B. Impacts of KUI and MRI on SOR Performance

Investigating the impacts of KUI and MRI on the SOR performance, Fig. 3 plots the average SOR, i.e. $E[S]$ [bits/s (bps)], versus T_R [s] and T_U [s]. In Fig. 3(a), T_U is assumed to vary in $\{1, 5, 10\}$ s, while in Fig. 3(b), various scenarios of the pair $\{\mu_r, k\}$ are similarly considered as in Fig. 2(b). The number of bits for authentication between entities in the

[4] Note that optimising the KUI and MRI are two separate optimisation problems of T_U and T_R, respectively. Here, for brevity, let us group these two problems into one as shown in (10) when $x = T_U$ or $x = T_R$.

[5] Other techniques used to map the multiobjective optimisation problem to a single-objective optimisation can be referred to in [18].



(a)

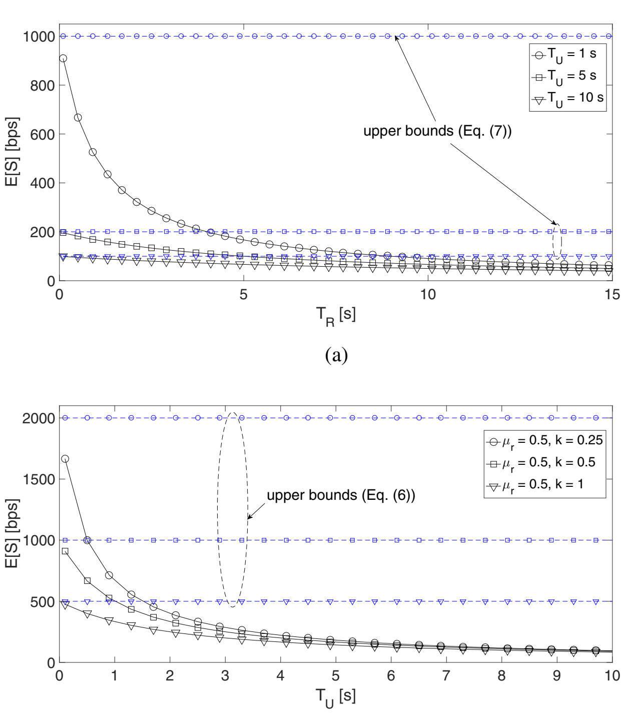
(b)

Fig. 2: (a) $E[N]$ versus T_R w.r.t. k; (b) $E[N]$ versus T_U w.r.t. μ_r and k.

network is set as $\rho = 1000$ bits. As shown in Figs. 3(a) and 3(b), the average SOR decreases to 0 as either T_U or T_R increases and they are all bounded by (6) and (7) when T_U and T_R approach to 0, respectively. These verify the findings in Lemma 3 about the monotonic decreasing property of $E[S]$ over T_U and T_R as well as confirming the derived upper and lower bounds of $E[S]$.

C. Optimal KUI and MRI

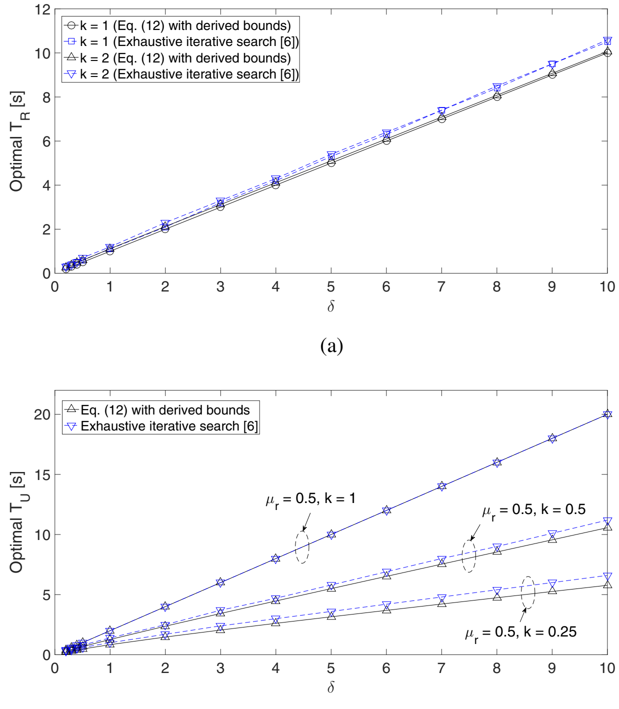
In order to validate the effectiveness of the derived bounds in finding the optimal KUI and MRI, Fig. 4 plots the optimal values of T_R and T_U versus the relative importance ratio between NEP and SOR, i.e. δ, using the proposed solution and the iterative search approach in [6]. In the iterative search approach, a running step size of 0.1 second is assumed, while in the proposed solution, by exploiting the bounds of $E[N]$ and $E[S]$ in Figs. 2 and 3, the normalised NEP and SOR can be determined, and thus the optimal T_R and T_U, i.e. $T_{R,opt}$ and $T_{U,opt}$, can be solved numerically in MATLAB. With the same settings as in Figs. 2 and 3, Fig. 4(a) shows $T_{R,opt}$ w.r.t. different values of k, while in Fig. 4(b), $T_{U,opt}$ w.r.t. various scenarios of μ_r and k. The relative importance ratio, i.e. δ, is assumed to vary in the range from 0.2 to 10 to reflect a variety of requirements in practice. It can be observed in Fig. 4 that there is a gap



(a)

(b)

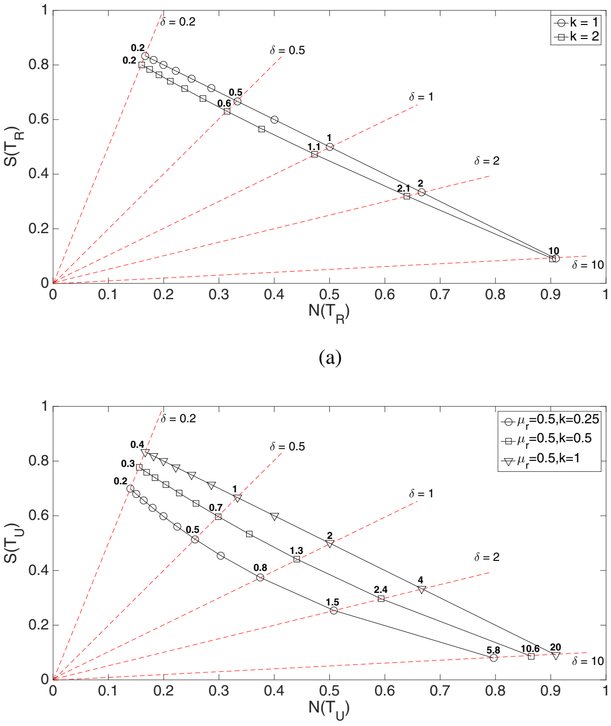
Fig. 3: (a) $E[S]$ versus T_R w.r.t. T_U; (b) $E[S]$ versus T_U w.r.t. μ_r and k.



(a)

(b)

Fig. 4: (a) Optimal T_R versus δ; (b) Optimal T_U versus δ.



(a)

(b)

Fig. 5: (a) $S(T_R)$ versus $N(T_R)$ w.r.t. k and (b) $S(T_U)$ versus $N(T_U)$ w.r.t. μ_r and k.

of up to 1 second between the optimal values of T_U and T_R in the proposed solution compared to those in the conventional iterative search approach. This accordingly verifies the statement in Remark 2 regarding the effectiveness of the proposed solution in finding the exact optimal values of T_R and T_U over the conventional approach which relies solely on the use of empirical data.

The findings of $T_{R,opt}$ and $T_{U,opt}$ are further illustrated in Figs. 5(a) and 5(b) where the optimal T_R and T_U are determined for every value of δ (see Lemma 4). It can be observed in both Figs. 4 and 5 that $T_{R,opt}$ and $T_{U,opt}$ increase as δ increases. In fact, a higher NEP is required over the SOR to achieve a higher δ. This means the security is of lower priority compared to the signalling overhead. Therefore, the optimal intervals $T_{U,opt}$ and $T_{R,opt}$ must be long enough to provide a lower $E[S]$ while sacrificing the cause of a higher $E[N]$. This observation verifies the notice in Remark 1 regarding the impact of δ as δ varies from 0 to ∞. This also reflects the observations in Figs. 2 and 3 regarding the contradictory between $E[N]$ and $E[S]$ when increasing either T_U or T_R.

VI. Conclusions

In this paper, the bounds of NEP and SOR have been first derived to not only facilitate the normalisation functions in the optimisation problem but also characterise the monotonicity properties of the NEP and SOR over the KUI and MRI. It has been shown that the NEP and SOR are respectively increasing and decreasing functions of both the KUI and MRI. A multiobjective optimisation problem has been accordingly proposed to find the optimal KUI and MRI that minimise NEP and SOR in MME handover. By specifying a relative importance parameter to balance two conflicting objectives NEP and SOR, the multiobjective optimisation problem has been converted to a single-objective optimisation problem where the optimal solutions can be found via a simple numerical method with a lower complexity and a higher accuracy of up to 1 second rather than performing iterative searches as in conventional approach.

Appendix A
Proof of Lemma 1

From (1), it can be easily shown that $E[N]$ decreases as μ_u increases, and thus $E[N]$ is an increasing function over T_U since $T_U = 1/\mu_u$. The lower bound of $E[N]$ can thus be determined when $T_U \to 0$, i.e. $\mu_u \to \infty$, as

$$\lim_{\mu_u \to \infty} E[N] = 0. \tag{13}$$

The upper bound of $E[N]$ can be computed by applying L'Hospital's Rule when $T_U \to \infty$, i.e. $\mu_u \to 0$. Let us define

$$\begin{aligned} f_1(\mu_u) &\triangleq 1 - \frac{\mu_r}{\mu_u k}\left(1 - \left(\frac{\mu_r}{\mu_u + \mu_r}\right)^k\right), && (14)\\ g_1(\mu_u) &\triangleq \mu_u. && (15)\end{aligned}$$

Substituting (14) and (15) into (1), we have

$$\begin{aligned} \lim_{\mu_u \to 0} E[N] = \lambda_p \lim_{\mu_u \to 0} \frac{f_1(\mu_u)}{g_1(\mu_u)} &= \lambda_p \lim_{\mu_u \to 0} \frac{f_1'(\mu_u)}{g_1'(\mu_u)}\\ &= \lambda_p \lim_{\mu_u \to 0} f_1'(\mu_u). \qquad (16)\end{aligned}$$

We continue by calculating $f_1'(\mu_u)$ as follows:

$$\begin{aligned} f_1'(\mu_u) &= \frac{\mu_r}{k\mu_u^2} - \frac{\mu_r^{k+1}}{k}\frac{1}{\mu_u^2\left(\mu_u + \mu_r\right)^k} - \frac{\mu_r^{k+1}}{\mu_u\left(\mu_u + \mu_r\right)^{k+1}}\\ &\triangleq \frac{f_2(\mu_u)}{g_2(\mu_u)}, \end{aligned} \tag{17}$$

where

$$f_2(\mu_u) = \mu_r\left(\mu_u + \mu_r\right)^{k+1} - \mu_r^{k+1}\left(\mu_u + \mu_r\right) - k\mu_u\mu_r^{k+1}, \tag{18}$$

$$g_2(\mu_u) = k\mu_u^2\left(\mu_u + \mu_r\right)^{k+1}. \tag{19}$$

Substituting (17) into (16), we then have

$$\lim_{\mu_u \to 0} E[N] = \lambda_p \lim_{\mu_u \to 0} \frac{f_2'(\mu_u)}{g_2'(\mu_u)} = \lambda_p \lim_{\mu_u \to 0} \frac{f_3(\mu_u)}{g_3(\mu_u)}, \quad (20)$$

where

$$f_3(\mu_u) \triangleq (k+1)\mu_r(\mu_u + \mu_r)^k - \mu_r^k, \quad (21)$$

$$g_3(\mu_u) \triangleq k\mu_u(\mu_u + \mu_r)^k \left[2(\mu_u + \mu_r) + (k+1)\mu_u\right]. \quad (22)$$

Similarly, we can arrive at

$$\lim_{\mu_u \to 0} E[N] = \lambda_p \lim_{\mu_u \to 0} \frac{f_3'(\mu_u)}{g_3'(\mu_u)} = \lambda_p \lim_{\mu_u \to 0} \frac{f_4(\mu_u)}{g_4(\mu_u)} \quad (23)$$

where

$$f_4(\mu_u) \triangleq (k+1)\mu_r(\mu_u + \mu_r)^{k-1}, \quad (24)$$

$$\begin{aligned} g_4(\mu_u) \triangleq\ & (\mu_u + \mu_r)^k \left[(k+3)\mu_u + 2\mu_r\right] \\ & + k\mu_u(\mu_u + \mu_r)^{k-1} \left[(k+3)\mu_u + 2\mu_r\right] \\ & + \mu_u(\mu_u + \mu_r)^k (k+3). \end{aligned} \quad (25)$$

Finally, we obtain

$$\begin{aligned} \lim_{\mu_u \to 0} E[N] = \lambda_p \lim_{\mu_u \to 0} \frac{f_4'(\mu_u)}{g_4'(\mu_u)} &= \lambda_p \frac{(k+1)\mu_r \mu_r^{k-1}}{2\mu_r^{k+1}} \\ &= \frac{\lambda_p (k+1)}{2\mu_r}. \end{aligned} \quad (26)$$

Equivalently, (13) and (26) can be stated as

$$N_{\min}^{(T_U)} = \lim_{T_U \to 0} E[N] = 0 \quad (27)$$

and

$$N_{\max}^{(T_U)} = \lim_{T_U \to \infty} E[N] = \frac{\lambda_p (k+1)}{2\mu_r}. \quad (28)$$

Hence, the Lemma is proved.

Appendix B
Proof of Lemma 2

From (1), it can be shown that $E[N]$ increases as either k increases or μ_r decreases. Therefore, $E[N]$ is an increasing function over T_R since $T_R = k/\mu_r$.

Considering both k and μ_r, we have the following cases:

i) $k \to \infty$ or $\mu_r \to 0$: we have $T_R \to \infty$, and thus

$$N_{\max}^{(T_R)} = \lim_{k \to \infty} E[N] = \lim_{\mu_r \to 0} E[N] = \frac{\lambda_p}{\mu_u}. \quad (29)$$

ii) $k \to 0$: we have $T_R \to 0$ and

$$N_{\min}^{(T_R)} = \lim_{k \to 0} E[N] = \frac{\lambda_p}{\mu_u} \left(1 - \frac{\mu_r}{\mu_u} \lim_{k \to 0} \frac{f_5(k)}{g_5(k)}\right), \quad (30)$$

where

$$f_5(k) \triangleq 1 - \left(\frac{\mu_r}{\mu_u + \mu_r}\right)^k, \quad (31)$$

$$g_5(k) \triangleq k. \quad (32)$$

It can be seen that $f_5(k) \to 0$ and $g_5(k) \to 0$ as $k \to 0$. By taking the derivative of both $f_5(k)$ and $g_5(k)$ as in the L'Hospital's Rule, we can obtain $N_{\min}^{(T_R)}$ as in (5).

iii) $\mu_r \to \infty$: we have $T_R \to 0$ and

$$N_{\min}^{(T_R)} = \lim_{\mu_r \to \infty} E[N] = \frac{\lambda_p}{\mu_u} \left(1 - \frac{1}{k\mu_u} \lim_{\mu_r \to \infty} \frac{f_6(\mu_r)}{g_6(\mu_r)}\right), \quad (33)$$

where $f_6(\mu_r)$ has the same form as $f_5(k)$ in (31) and

$$g_6(\mu_r) = 1/\mu_r. \quad (34)$$

It can be seen that $f_6(\mu_r) \to 0$ and $g_6(\mu_r) \to 0$ as $\mu_r \to \infty$. Similarly, using the L'Hospital's Rule, we can show that $N_{\min}^{(T_R)} = 0$ as $\mu_r \to \infty$.

Summarising the above cases, the Lemma is proved.

References

[1] F. Khan, *LTE for 4G Mobile Broadband: Air Interface Technologies and Performance*. Cambridge University Press, Apr. 2009.

[2] Q. Xiao, W. Zhou, B. Cui, and L. Li, "An enhancement for key management in LTE/SAE X2 handover based on ciphering key parameters," in *Proc. 3PGCIC 2014*, Guangdong, China, Nov. 2014, pp. 256–261.

[3] M. Gohar and J. G. Choi, "Enhanced mobility management scheme in PMIP-SAE-based mobile networks," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1160–1163, Jun. 2016.

[4] D. Forsberg, "LTE key management analysis with session keys context," *Elsevier Comput. Commun.*, vol. 33, no. 16, pp. 1907–1915, Oct. 2010.

[5] C. B. Sankaran, "Network access security in next-generation 3GPP systems: A tutorial," *IEEE Commun. Mag.*, vol. 47, no. 2, pp. 84–91, Feb. 2009.

[6] C.-K. Han and H.-K. Choi, "Security analysis of handover key management in 4G LTE/SAE networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 457–468, Feb. 2014.

[7] P. K. Reddy and B. R. Chandavarkar, "Mitigation of desynchronization attack during inter-eNodeB handover key management in LTE," in *Proc. IC3 2015*, Noida, India, Aug. 2015, pp. 561–566.

[8] D. Forsberg, G. Horn, W.-D. Moeller, and V. Niemi, *LTE Security*, 2nd ed. Wiley, Dec. 2012.

[9] M. Song, J. Y. Choi, J. D. Cho, J. Jeong, B. h. Song, and H. Lee, "Reduction of authentication cost based on key caching for inter-MME handover support," in *Proc. HPCS 2014*, Bologna, Italy, July 2014, pp. 885–892.

[10] S. Pack and W. Lee, "Optimal binding-management-key refresh interval in mobile IPv6 networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 7, pp. 3834–3837, Sep. 2009.

[11] A. De Gregorio, "Cryptographic key reliable lifetimes: Bounding the risk of key exposure in the presence of faults," in *Proc. FDTC'06*, Yokohama, Japan, Oct. 2006, pp. 144–158.

[12] Y. Zhang, "Authentication overhead in wireless networks," in *Proc. IEEE ICC'08*, Beijing, China, May 2008, pp. 1505–1509.

[13] J. Al-Saraireh and S. Yousef, "Analytical model for authentication transmission overhead between entities in mobile networks," *Elsevier Comput. Commun.*, vol. 30, no. 8, pp. 1713 – 1720, Jun. 2007.

[14] R. Trestian, Q.-T. Vien, P. Shah, and G. E. Mapp, "Exploring energy consumption issues for multimedia streaming in LTE HetNet small cells," in *Proc. IEEE LCN 2015*, Florida, USA, Oct. 2015, pp. 498–501.

[15] R. Trestian, Q.-T. Vien, H. X. Nguyen, and O. Gemikonakli, "ECO-M: Energy-efficient cluster-oriented multimedia streaming in a LTE D2D environment," in *Proc. IEEE ICC 2015*, London, UK, Jun. 2015, pp. 55–61.

[16] Q.-T. Vien, T. A. Le, H. X. Nguyen, and H. Phan, "A secure network coding based modify-and-forward scheme for cooperative wireless relay networks," in *Proc. IEEE VTC 2016-Spring*, Nanjing, China, May 2016, pp. 1–5.

[17] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, 4th ed. Mc-Graw Hill, 2002.

[18] M. Ehrgott, *Multicriteria Optimization*, 2nd ed. Springer, Jun. 2005.

[19] P. N. Ngatchou, A. Zarei, W. L. J. Fox, and M. A. El-Sharkawi, *Pareto Multiobjective Optimization*. John Wiley & Sons, Inc., Jun. 2007, pp. 189–207.