The Nucleus **49**, No. 3 (2012) 199-208

The Nucleus
A Quarterly Scientific Journal of Pakistan
Atomic Energy Commission
NCLEAM, ISSN 0029-5698

# ON CAPACITY TRADEOFFS IN SECURE DS-CDMA PACKET COMMUNICATIONS WITH QOS CONSTRAINTS

*F. SATTAR and M. MUFTI

Department of Electrical Engineering, University of Engineering and Technology, Taxila, Pakistan

(Received July 12, 2012 and accepted in revised form September 05, 2012)

This paper presents a mathematical framework for analysis of effect of counter mode (CTR) encryption on the traffic capacity of packet communication systems based on direct-sequence, code-division, multiple-access (DS-CDMA). We specify QoS constraints in terms of minimum acceptable mean opinion score (MOS) of voice payload, maximum permissible resource utilization for CTR-mode re-keying and DS-CDMA processing gain. We quantify the trade-offs in system capacity as a function of these constraints. Results show that application of CTR encryption causes error expansion and respecting the QoS constraints while satisfying the desired encryption parameters results in reduction of traffic capacity.

**Keywords:** CTR encryption, DS-CDMA, QoS, MOS, Capacity trade-off, Security design

## 1. Introduction

Wireless networks are intrinsically vulnerable to eavesdropping due to their inherent broadcast nature. The ubiquity and portable nature of wireless terminals and end user devices further exacerbates security problems. While application of encryption algorithms and cryptographic security protocols addresses the security vulnerabilities to some extent, the fact that wireless devices are typically resource constrained, makes the implementation of encryption challenging and results in trade-off in system performance. In [1] authors have shown that application of encryption in 3G wireless systems results in increased power budget, increased packet delay and decrease in bandwidth efficiency. In [2] authors show that maintaining confidentiality in real-time Voice over IP (VoIP) networks comes at a cost of error expansion and mitigating this error-expansion results in increased delay and reduced bandwidth efficiency. Similar studies on analysis of impact of encryption on system performance have been done in [3, 4].

In this paper we develop an analytical model to quantify the effect of counter mode (CTR) encryption on wireless system capacity constrained by quality of service (QoS) parameters. This model is most relevant to the dimensioning and planning of CTR based secure wireless systems.

CTR mode has been declared by the National Institute of Technology and Standards (NIST) as one of the standard modes of operation for block ciphers [5]. This mode is considered as an attractive security algorithm for use in high speed networking because of its significant efficiency advantages, its ability to be fully parallelized and its proven security [6].

We consider direct-sequence, code-division, multiple-access system (DS-CDMA) [7] as the underlying wireless primitive as almost all 3G mobile cellular systems use variants of DS-CDMA as their prime multiple access air-link architecture [8, 9].

This paper has following organization: Section 2 briefly describes the CTR mode encryption and decryption algorithms. It also defines the measure to quantify the re-keying effort in CTR encryption. Section 3 presents a packetized voice system model for a DS-CDMA communications system accommodating two categories of users: ones with confidentiality based on CTR encryption and others without any encryption. The QoS metrics to measure the desired level of voice quality of both profiles of users is also defined. Second 4 provides

* Corresponding author : fouz@ieee.org

a quantitative analysis of the impact of the CTR encryption on system traffic capacity with QoS constraints. Section 5 discusses the analytical and numerical results. Finally in Section 6, conclusions are given.

## 2. Counter Mode Operation and Re-keying Performance Quantification

CTR mode is based on the application of a block cipher to a set of input blocks, called counters, to produce a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext. Decryption process is identical to encryption with plaintext and ciphertext interchanged. The counter values can be explicitly communicated between sender and receiver or they can be maintained at each end with some kind of synchronization mechanism between sender and receiver. If $E_K(P)$ denotes a block cipher that takes a key $K$ and $n$-bit plaintext $P$ to return $n$-bit ciphertext $C$, then encryption of $L$-bit message $P$ using CTR mode with key $K$ and $n$-bit counter $ctr$ is processed as follows:

**Algorithm 1** $\mathcal{E}_K(ctr, P[0] \dots P[L-1])$

1: **for** $i = 1 \dots L-1$ **do**
2: $\quad C[i] \leftarrow E_K(ctr + i) \otimes P[i]$
3: **end for**
4: **return** $C[0] \dots C[L-1]$

Figure 1. CTR Encryption Algorithm.

where $f : B \leftarrow A$ denotes a function or mapping which assigns to each element $a$ in $A$ precisely one element $b$ in $B$. $|x|$ denotes the length of string $x$. If $|x|$ is multiple of $n$ then we view it as divided into sequence of $n$-bit blocks such that $x[i]$ denotes $i$-th block, $\forall i = 0,1 \dots L-1$ i.e. $x = x[0] \dots x[L-1]$ where $L = \frac{|x|}{n}$.

Similarly decryption process is identical to encryption and is described as:

**Algorithm 2** $\mathcal{D}_K(ctr, C[0] \dots C[L-1])$

1: **for** $i = 1 \dots L-1$ **do**
2: $\quad P[i] \leftarrow E_K(ctr + i) \otimes C[i]$
3: **end for**
4: **return** $P[0] \dots P[L-1]$

Figure 2. CTR Decryption Algorithm.

The ciphering and deciphering processes are depicted in Fig 3a and 3b. In practical usage scenarios, the same counter value is shared between the sender and receiver either by transmitting it along with each cipher text message or by incrementing it independently at sender and receiver sides after respective message transmittal or reception. This requires that both sender and receiver maintain state synchronization and communicate over a reliable channel. In this paper we focus on the the first case whereby complete or partial counter value is explicitly exchanged between the two parties. This synchronization mechanism is also followed in most of the system implementations such as [10, 11].

In practical CTR implementations, reusing a counter value (also called nonce) for more than one packet with the same key voids the confidentiality guarantees. Hence the size of nonce or counter determines the maximum number of packets that can be encrypted with a single block cipher key. If a counter value is ever used for more that one packet with the same key, then the same key stream will be used to encrypt both packets, and the confidentiality guarantees are voided. Therefore safe implementation of CTR necessitates that if nonce values are exhausted during communications; a fresh key must be established using a key exchange protocol. In other words small nonce size results in frequent re-keying and induces more key establishment overhead whereas large sizes of nonce reduces key establishment but at the same time consumes bandwidth. We quantify the re-keying effort $S_c$ as $log_2$ of the counter length $N_c = |ctr|$ normalized to maximum counter size $N_{c_{max}}$:

$$S_c = \frac{\log_2 N_c}{\log_2 N_{c_{max}}} \tag{1}$$

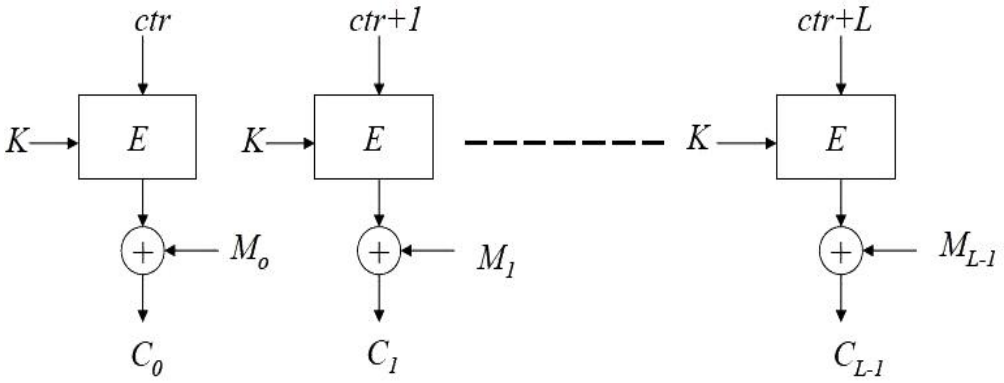


Figure 3a. CTR Encryption Operation .

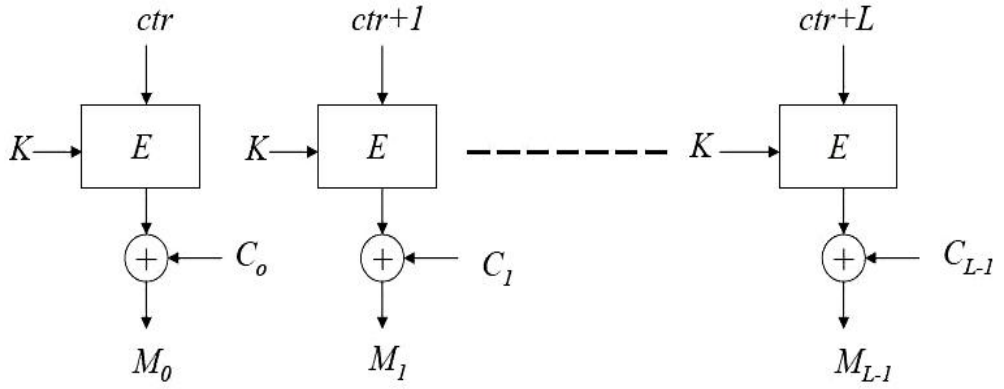


Figure 3b. CTR Decryption Operation.

Hence $S_c$ ranges from 0 to 1. Smaller values of $S_c$ imply more re-keying effort while larger values of $S_c$ result in less frequency of re-keying.

## 3. Secure DS-CDMA Packetized Voice System Model

We consider DS-CDMA downlink transmitter system that supports variable QoS via the optimal power control algorithm as described [12]. We assume that the system can accommodate a total of $U$ users and each user is generating a single stream of packetized voice. We consider two profiles of users: $U_1$ users without confidentiality and $U_2$ users with confidentiality requirements i.e.

$$U = U_1 + U_2 \tag{2}$$

The traffic of users with confidentiality profile is encrypted with CTR encryption algorithm described in section 2.

Figure 4 shows the DS-CDMA system structure for downlink. As indicated in the figure, after packetization, each user stream then undergoes modulation and power control before being assigned a code and transmitted. The transmitter then performs power control over the aggregate of all users' streams at each time step, providing a global minimization of the total transmit power subject to each streams reliability requirement. Finally a spreading or direct sequence code is assigned to each stream before transmitting the DS-CDMA signal. For modulation, M-ary PSK modulation is considered hence the the power control layer remains transparent to the decoder.

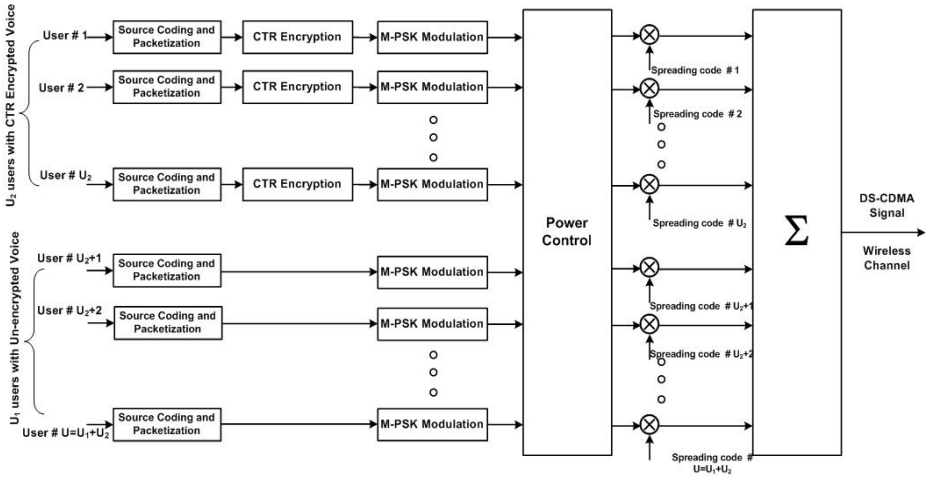


Figure 4. Secure DS-CDMA System structure for downlink.

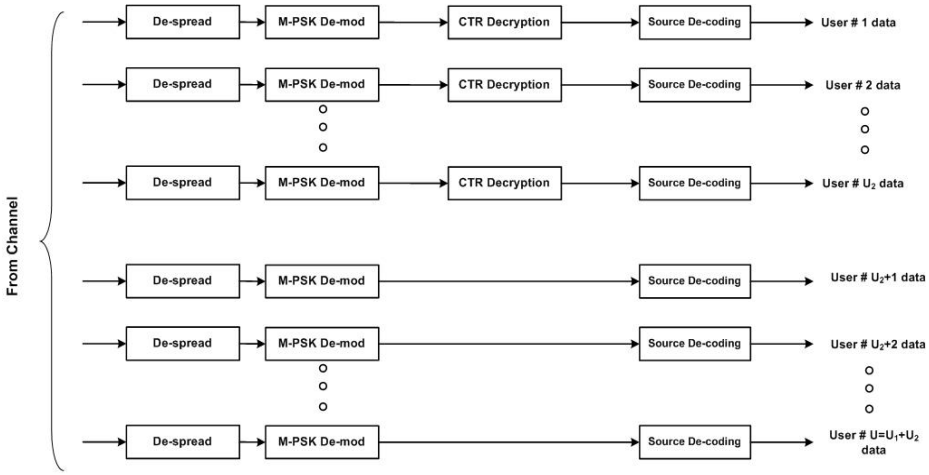


Figure 5. Receiver structure for downlink.

As shown in Figure 5, the receiver (for donwlink) performs the reverse of these functional blocks i.e. received signal is de-spread and de-modulated and encrypted traffic is decrypted using the CTR decryption described in section 1. For users without confidentiality, decryption stage is by-passed.

We consider the power control algorithm presented in [12] which is based on the principle of minimizing the interference each user experiences from other users within a given cell, while satisfying each user's reliability requirement.

As in [12], a feasible solution for this power control algorithm exists and this solution is unique and optimum if and only if:

$$\sum_{m=1}^{U} \beta_m \alpha_m < 1 \tag{3}$$

where:

$$\beta_m(\gamma) \approx \begin{cases} 1 & \text{if user } m \text{ is transmitting} \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

$$\alpha_m = \frac{\xi_m}{G + \xi_m} \tag{5}$$

$\xi_m$ is the energy per bit to interference for user *m* and *G* is the spread spectrum processing gain.

The feasibility condition given by equation (3) is identical for both uplink and downlink cases. It is a tight upper bound on user capacity $U$ because in order for system to accommodate as many users as possible, it only need add users until the addition would cause the summation in equation (3) to exceed unity.

To benchmark the acceptable level of voice quality, we use ITU-T predictive computational model [13]. This model uses the subjective metric called Mean Opinion Score (MOS) to predict the quality of packetized voice on a scale from a best case of 5 to a worst case of 1, as a function of transmission parameters:

$$MOS = \begin{cases} 1 & \text{for R} \le 0 \\ 1 + 0.035R + R(R-60)\cdot(100-R)\cdot 7\times 10^{-6} & \text{for } 0 < \text{R} < 100 \\ 4.5 & \text{for R} \ge 100 \end{cases} \quad (6)$$

Using the default values in [13], the R-factor $R$ can be computed as:

$$R = 93.2 - \left( I_e + (95 - I_e)\cdot \frac{PER}{\frac{PER}{BurstR} + B_{pl}} \right) \quad (7)$$

where $I_e$ is codec specific value for the Equipment Impairment Factor. $B_{pl}$ is Packet-loss Robustness Factor and is defined as codec specific value. $PER$ is the packet loss probability and $BurstR$ is the Burst Ratio, defined as:

$$BurstR \begin{cases} = 1 & \text{when packet loss is random} \\ > 1 & \text{when packet loss is bursty} \end{cases} \quad (8)$$

Hence if acceptable level of MOS for each user is $MOS_{target}$ and $R_{target}$ is the corresponding R-factor, the we can compute the required PER $P_{target}$ as:

$$P_{target} = \frac{B_{pl} BurstR (I_e - 93.2 + R_{target})}{(93.2 - R_{target} - I_e) - B_{pl}(95 - I_e)} \quad (9)$$

We will use the condition in equation (3) along with the QoS constraint (9) to quantify the trade-off between confidentiality and traffic capacity in the next section.

## 4. Capacity Tradeoff Analysis

We assume each user transmits continuously, then, for each user, $\beta_m$ is unity. Furthermore we assume that both user profiles (i.e. users with and without encryption) have same MOS requirement dictated by $R_{target}$. We suppose that $P_{target}$ is the corresponding PER and $P_e$ is the bit error probability required to achieve $P_{target}$ . With these assumptions, equation (3) results in:

$$\sum_{m=1}^{U_1} \alpha_1 + \sum_{n=1}^{U_2} \alpha_2 < 1 \quad (10)$$

where

$$\alpha_1 = \frac{\xi_1}{G + \xi_1} \quad (11)$$

$$\alpha_2 = \frac{\xi_2}{G + \xi_2} \quad (12)$$

$\xi_1$ is the energy per bit to interference requirement for user without encryption to maintain $P_e$ whereas $\xi_2$ is the energy per bit to interference requirement for user with encryption to maintain same value of $P_e$.

Expanding the summations:

$$U_1\alpha_1 + U_2\alpha_2 < 1 \quad (13)$$

or

$$(U - U_2)\alpha_1 + U_2\alpha_2 < 1 \quad (14)$$

Let $\rho = U_2/U$ denote fraction of the total users with confidentiality. Then in terms of $\rho$ equation (14) can be written as:

$$U(\alpha_1 + (\alpha_1 - \alpha_2)\rho) < 1 \quad (15)$$

or

$$U < U_{max} \tag{16}$$

where:

$$U_{max} = \frac{1}{\alpha_1 + (\alpha_1 + \alpha_2)\rho} \tag{17}$$

Substituting the values of $\alpha_1$ and $\alpha_2$ from equations (11) and (12):

$$U_{max} = \frac{(G + \xi_1)(G + \xi_2)}{\xi_1(G + \xi_2) + G(\xi_2 - \xi_1)\rho} \tag{18}$$

Throughout this paper we will use $U_{max}$ as a measure of maximum permissible system traffic capacity.

In order to determine $\xi_1$, we consider that for a DS-CDMA system the sum of interference from other users and along multiple propagation paths can be approximated as being additive white, Gaussian noise (AWGN) [14]. We also assume that the impact of fading channel and interference from adjacent cells is mitigated to achieve an error performance that approaches an AWGN approximation using interleaving or any other diversity techniques. With these assumptions we can use the invertible BER expression for M-ary PSK in [15] as follows:

$$\text{BER}_{\text{MPSK}} = 0.2 \exp\left(\frac{-7k\xi}{2^{1.9k} + 1}\right) \tag{19}$$

where

$$k = \log_2(M) \tag{20}$$

Using equation (19), the $\frac{E_b}{N_o}$ $\xi_1$ required to maintain $P_e$ for each user without encryption can be determined as:

$$\xi_1 = -\frac{2^{1.9k} + 1}{7k} \ln(5P_e) \tag{21}$$

where:

$$P_e = 1 - \exp\left(\frac{\ln(1 - P_{target})}{N_c + L}\right) \tag{22}$$

$N_c = 0$ for users without encryption. To determine $\xi_2$, we first analyze the BER expansion caused by CTR encryption and then use equation (19) to determine the corresponding $\frac{E_b}{N_o}$ requirements. To this end, we first model the post decryption process of each secure user as in [1] and [16]. We consider fixed packet lengths for each user such that the length of counter block in each packet is $N_c$ and length of the ciphertext block is $L$. At the receiver side the decryption is performed by the exclusive-OR of the ciphertext with the generated key stream. Hence if bit errors occur in the ciphertext, then the recovered plaintext will have the same number of bit errors in the same bit positions as in the ciphertext and the decryptor will be in the state of preserving bit errors.

Similarly, if there is a bit error in the transmitted counter block, then a bit error may occur independently, in any bit position of the decryption of the corresponding ciphertext, with an expected error rate of fifty percent and decryptor will be in the state of expanding errors.

Bit error expansion is because of the fact that the underlying block cipher is assumed to adhere to strict avalanche criterion (SAC) [17] implying that each bit of its output function changes with probability one half, whenever an input bit is complemented.

In brief, we can associate four possible events with the reception of ciphered message:

- Event *D*: when both counter block and ciphertext block are in error.
- Event *C*: when ciphertext block is correct while counter block is in error.
- Event *B*: when counter block is correct while ciphertext block is in error.
- Event *A*: when both counter block and ciphertext block are correct.

When event *D* or *C* happens, the decryptor is in the state of error expansion. When event *B* takes place, preservation of bit errors occurs. When event *A* happens, the decryptor is free of errror expansion and error preservation. If the states corresponding to occurrence of events $A, B, C$ and $D$ are respectively referred to as 0 , 1 , 2 and 3 respectively, then we can model the decryption operation as a stochastic error model as illustrated in Figure 6.

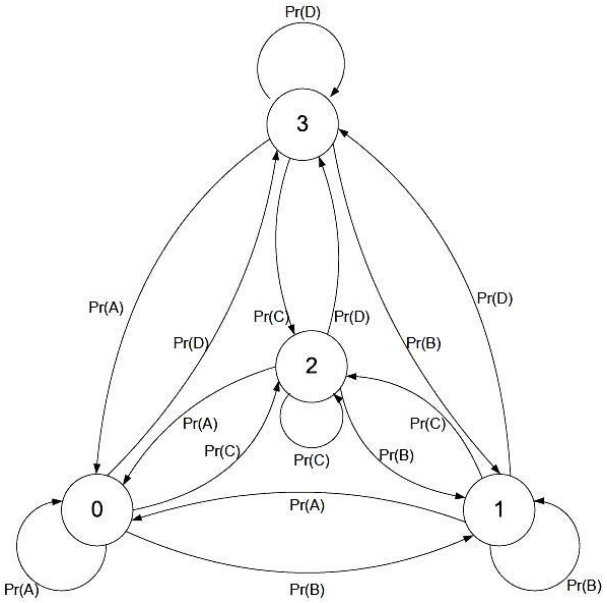


Figure 6. State diagram of the decryption process.

The stochastic process updates its state every decryption cycle with the transition probabilities indicated in figure 6 whereby $Pr(X)$ denotes the probability of occurrence of event $X$. If $P_b$ represents the channel bit error probability after all the error control then we can express $Pr(A)$, $Pr(B)$, $Pr(C)$ and $Pr(D)$ in terms of $P_b$ as [16]:

$$Pr(A) = (1-P_b)^{N_c} \cdot (1-P_b)^{L} \quad (23)$$

$$Pr(B) = (1-(1-P_b)^{L}) \cdot (1-P_b)^{N_c} \quad (24)$$

$$Pr(C) = (1-P_b)^{L} \cdot (1-(1-P_b)^{N_c}) \quad (25)$$

$$Pr(D) = (1-(1-P_b)^{L}) \cdot (1-(1-P_b)^{N_c}) \quad (26)$$

The mean probability of error can be calculated as:

$$P_{decrypt} = Pr(A) \cdot e_0 + Pr(B) \cdot e_1 + Pr(C) \cdot e_2 + Pr(D) \cdot e_3 \quad (27)$$

where $e_v$ denotes the bit error rate associated with state $v \quad \forall k = 0,1,2,3$.

As the underlying block cipher is assumed to adhere to SAC, $e_2 = \frac{1}{2}$.

Also, the bit error rates in states **0** and **1** are $e_0 = 0$ and $e_1 = P_b$ respectively.

If we assume that the residual channel bit errors and the errors introduced by the block cipher avalanche effect occur independently, the bit error rate in state **3** can be expressed as:

$$\begin{aligned} e_3 &= 1-(1-\frac{1}{2}) \cdot (1-P_b) \\ &= \frac{1}{2}(1+P_b) \end{aligned} \quad (28)$$

Substituting these values of bit error rates in (27) along with the event probabilities from equations (23) to (26), the post decryption error probability can be written as:

$$\begin{aligned} P_{decrypt} &= \frac{P_b}{2}(1-(1-P_b)^{L})(1+(1-P_b)^{N_c}) \\ &\quad + \frac{1}{2}(1-(1-P_b)^{N_c}) \end{aligned} \quad (29)$$

Since $L > N_c$, for small values of $P_b$ $(<10^{-3})$ the first term in above summation becomes negligible and approximating second term in the summation results in:

$$P_{decrypt} \approx \frac{N_c}{2} P_b \quad (30)$$

In summary, the CTR encryption / decryption process amplifies the channel bit error probability by a factor $\frac{N_c}{2} P_b$. Hence if system BER requirement is $P_e$, then in order to compensate for

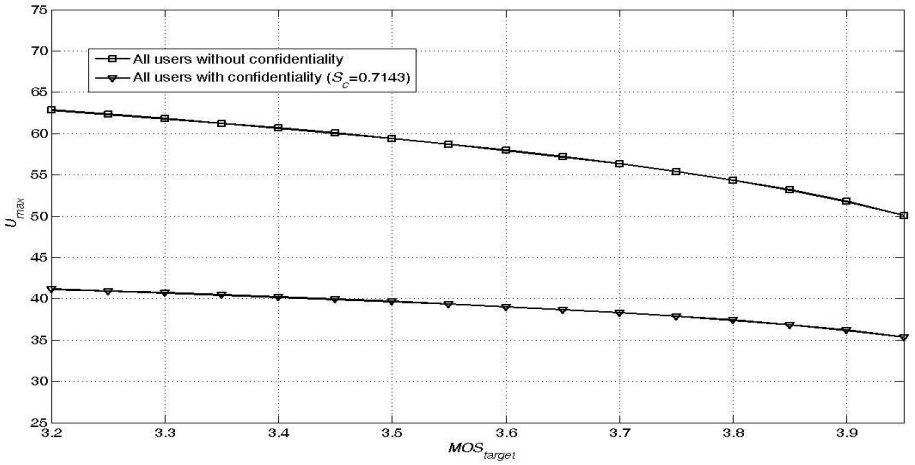


Figure 7. Capacity vs. MOS requirements

the effect of CTR encryption, the corresponding $\frac{E_b}{N_o}$ $\xi_2$ requirement from (19) and (30) is given as:

$$\xi_2 = -\frac{2^{1.9k}+1}{7k}\ln(\frac{10}{N_c}P_e) \quad (31)$$

In above derivation we have interchangeably used the terms BER and probability of error. This is because BER is actually the empirical probability of bit error, differing from the axiomatic approach to probability [14] and hence can be interchanged for all practical purposes.

Finally using relations in equations (1), (21) and (31):

$$\xi_2 = \frac{\ln\left(\frac{10}{S_c \log_2 N_{c_{max}}} P_e\right)}{\ln(5P_e)}\xi_1 \quad (32)$$

We will now use the relations (18), (21) and (32) to determine the numerical results summarized in next section.

## 5. Numerical Results

We first analyze the variation of DS-CDMA system traffic capacity with the MOS requirement $MOS_{target}$ for the two profile of users. For both profiles we consider the processing gain *G*=30*dB* and 8-PSK modulation i.e. *k=3.*

Furthermore we assume that packets carry voice payload compressed with G.729A and VAD and ROHC [19,20] so that $L$ = 272 bits, $I_e$ = 11, $B_{pl}$ = 19 and *BurstR* = 4.

For users with confidentiality ($\rho$ = 1), we consider AES CTR encryption [18] with $N_{cmax}$ = 128 and $N_c$ = 32 and $S_c$ = 0.7143. Figure 7 shows the variation in system traffic for the two cases. At any value of $MOS_{target}$ the vertical distance between two curves gives the trade-off in system capacity due to confidentiality or CTR encryption e.g. with $MOS_{target}$ = 3.8 the system capacity degrades by 26%, dropping from 54 to 38 users when CTR encryption is applied on all users.

Hence application of CTR encryption on all users, while maintaining the accpetable level of MOS, results in significant de-gradation in system capacity.

For the same values of $G$ and $k$ and same codec specifications as above, we now fix the MOS requirement to $MOS_{target}$ = 3.9 and vary the counter size $N_c$ from 0 to $N_{cmax}$ = 128 in steps of 16 bits and analyze the impact on system with CTR encryption applied on all users ($\rho$ = 1).

Figure 8 shows the results for different values of as $S_c$ increases from 0.5714 to 1 (corresponding to $N_c$ increasing from 0 to $N_{cmax}$ = 128).

Hence, as we fix the MOS requirement, and attempt to decrease the re-keying overhead by increasing the value of $S_c$ the system traffic capacity drops considerably.

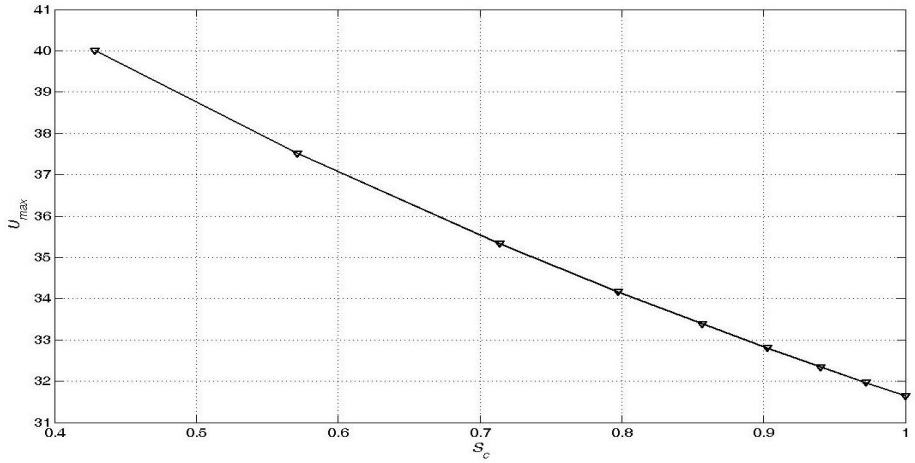


Figure 8. Effect of decreasing re-keying overhead on secure system capacity with fixed MOS.

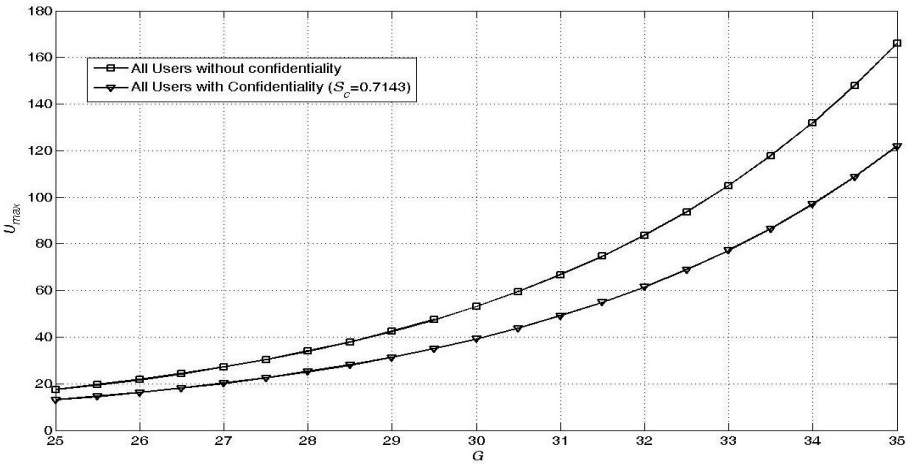


Figure 9. Secure system capacity vs bandwidth.

Finally, we analyze the impact of processing gain *G* on the system capacity for the two user profiles for same codec specifications as above. To this end, we set $MOS_{target}$ = 3.9 and increase *G* from 25*dB* to 35*dB*. We determine the system capacity for cases when $\rho$ = 0 i.e. all users without confidentiality and when $\rho$ = 1i.e. all users with CTR encryption for $S_c$ = 0.7143. The results are shown in Figure 9. For a fixed system capacity, the horizontal distance between the curves gives the additional requirements for processing gain *G* to maintain that capacity. As system bandwidth is a linear function of process gain [21], we deduce that for a given capacity and BER requirement, application of CTR encryption results in a bandwidth penalty.

## 6. Conclusions

We have developed a mathematical framework for analysis of effect of counter mode (CTR) encryption on the traffic capacity of packet communication systems based on a direct-sequence, code-division, multiple-access (DS-CDMA).

We have quantified the trade-offs in system capacity as a function of different QoS constraints including minimum acceptable mean opinion score (MOS) of voice payload, maximum permissible resource utilization for CTR-mode re-keying and DS-CDMA processing gain. The analytical model and results presented in this paper provide an important contribution to the accurate design and dimensioning of secure packet DS-CDMA systems.

**References**


[1] F. Sattar and M. Mufti, Lecture Notes in Computer, Springer-Verlag, Berlin Heidelberg (2008) p. 507-516.

[2] J. M. Reason and D. G. Messerschmitt, Proceedings of the 4th IFIP/IEEE International Conference on Management of Multimedia Networks and Services: Management of Multimedia on the Internet Springer-Verlag, 2001, Berlin Heidelberg (2001) p. 175-192.

[3] Olteanu, Alina, Yang Xiao, Proceedings of the 2009 IEEE International Conference on Communications, IEEE Press, Piscataway, NJ, USA (2009) p.575-579.

[4] W. Liang and W. Wang, INFOCOM, 24th Annual Joint Conference of the IEEE Computer and Communications Societies IEEE Proceedings, Vol.2 (2005) p. 1478-1489.

[5] M. Dworkin, NIST Special Publication 800-38A, Computer Security Division, ITL NIST, Gaithersburg (2001) p.15-16.

[6] H. Lipmaa, P. Rogaway and D. Wagner, Comment to NIST concerning AES Modes of operations: CTR-Mode Encryption (January 2001) p.2-3.

[7] S. Moshavi, IEEE Communications Magazine **34**, No.10 (1996) 124.

[8] W.C.Y. Lee, IEEE Transactions on Vehicular Technology **40**, No.2 (1991) 291.

[9] R.L. Pickholtz, L.B. Milstein, D.L. Schilling, IEEE Transactions on Vehicular Technology **40**, No.2 (1991) 313.

[10] Housley, IETF RFC 3686, Network Working Group, The Internet Society (January 2004).

[11] IEEE Std 802.11i, IEEE Standard for Information Technology - Telecommunication and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Media Access Control (MAC) Security Enhancements (July 2004).

[12] L. Yun and D.G. Messerschmitt, Proceedings of IEEE Military Communications Conference MILCOM '94, Fort Monmouth, NJ (Oct. 2-4, 1994) p. 178 -182.

[13] International Teleommunication Union, Telecommunication Standardization Sector of ITU, ITU-T Recommendation G.107 (March 2005).

[14] J. Reason, Ph.D. dissertation, University of California, Berkeley (Dec. 2000) p. 72-98.

[15] S. T. Chung and A. J. Goldsmith, IEEE Transactions on Communications (September 2001) p. 1561-71.

[16] F. Sattar and M.Mufti, International Journal of Network Security **8**, No.2 (2009) 119.

[17] R. Forre, Proceedings on Advances in Cryptology, Springer-Verlag, New York, NY, USA, August 21-25 (1988) p.450-468.

[18] National Institute of Standards and Technology, FIPS Pub 197: Advanced Encryption Standard (AES) (Nov. 2001).

[19] A. Benyassine, E. Shlomot, H.-Y. Su, D. Massaloux and C. Lamblin, J.-P. Petit, IEEE Communications Magazine **35**, No. 9 (1997) 64.

[20] C. Bormann et al., IETF RFC 3095, Network Working Group (July 2001).

[21] R. C. Dixon, Spread Spectrum Systems with Commercial Applications, Wiley & Sons, (1994).