Performance Improvement of Chaos MIMO Transmission Scheme Using Space-Time Block Coding

Eiji Okamoto† and Yuma Inaba†

†Graduate School of Engineering, Nagoya Institute of Technology
Gokiso-cho, Showa-ku, Nagoya 466-8555, Japan.
okamoto@nitech.ac.jp

Abstract– In wireless transmission, an additional security or simplification of the conventional upper layer security protocols can be provided by ensuring physical layer security. To achieve not only this physical layer security but also channel coding gain, we have proposed a chaos multiple-input multiple-output (MIMO) transmission scheme in which chaos signals correlated by transmit bits are multiplied to each transmit symbols of MIMO. However, to make the chaos MIMO more effective, the error rate performance needs to be improved. In MIMO transmission techniques, a space-time block code (STBC) is proposed to obtain a space diversity gain and to improve the error rate performance, and is widely used. Therefore, in this study, we propose a chaos MIMO-STBC scheme applying the STBC into chaos MIMO scheme, and show that the improved error rate performance with a physical layer security is obtained.

1. Introduction

Wireless traffic is continuously increasing because of the spread of smartphones and the demand for higher capacity of wireless communication is still growing. In accordance with the traffic increasing, a wireless security is becoming more important. Currently, the wireless security is ensured mainly by the upper layer protocols such as public key encryption, IPSec, or scrambling. However, a physical layer security is recently drawing much attention as an additional or substitutional security scheme [1], too. As the scheme achieving both physical layer security and channel coding gain without rate-efficiency penalty, we have proposed a chaos multiple-input multiple-output (C-MIMO) transmission scheme [2]. It is a chaos-modulated MIMO multiplexing scheme where the transmit MIMO symbols are multiplied by the chaos symbols correlated by the transmit bit sequence, and the chaos encryption and rate-1 block channel coding effect are obtained. There are several conventional schemes using chaos modulation in MIMO transmission [3-5]. However, those schemes need frequency expanding because of a chaos spreading modulation and the rate-efficiency is decreased, while the proposed scheme uses rate-1 channel coding and the rate-efficiency degradation is avoided. In the receiver of C-MIMO, the demodulation and decoding cannot be correctly done without a common key shared by the transmitter and the receiver, and thus, the common key-based physical layer security is ensured. It is shown in [6,7] that the computational security is sufficiently ensured in C-MIMO. Furthermore, the bit error rate performance is improved by a maximum likelihood sequence estimation (MLSE) in the receiver in tradeoff with the decoding complexity increase. Because

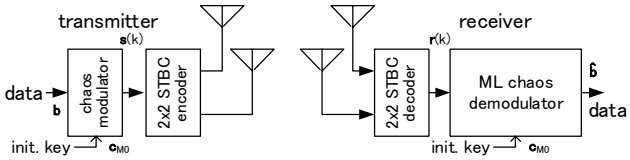

Fig. 1 space-time block coded chaos MIMO transmission system.

the transmit signal of C-MIMO is Gaussian, Shannon capacity will be achieved when the block length is expanded. The decoding complexity is, however, also exponentially increased and the block length of C-MIMO is restricted to some extent. Hence, an additional technique is required other than block length expansion to improve the error rate performance. Here, in MIMO transmission the space-time block coding (STBC) is proposed [8] to obtain the time-frequency diversity effect with linear decoding calculation. It is well-known that the full diversity effect is obtained when the number of transmit antenna is two. Therefore, in this paper, to improve the error rate performance of C-MIMO without exponentially increasing the decoding complexity, we propose a space-time block coded 2-by-2 chaos MIMO transmission scheme and show that the block error rate is superior to that of non-STBC C-MIMO at the same rate-efficiency.

In the following, the system configuration is introduced in Section 2. Numerical results are shown in Section 3 and the conclusion is drawn in Section 4.

2. Proposed space-time block coded chaos MIMO system

Fig. 1 shows the proposed space-time block coded chaos MIMO transmission system, where the numbers of transmit antenna N_t and receive antenna N_r are N_t=N_r=2, one chaos modulation block length is B, and the transmit bits per symbol is q. The bit sequence $\mathbf{b}=\{b_0,\cdots,b_{qN_tB-1}\}, b_k\in\{0,1\}$ in one block is chaos modulated and the complex transmit symbol sequence $\mathbf{s}=\{s_0,\cdots,s_{N_tB-1}\}$ is generated (see Section 2.1). After that, every N_t symbols are transmitted by MIMO multiplexing transmission. When the transmitted symbol at time k from i_t-th antenna ($1\le i_t\le N_t$) is expressed as $s_{i_t}(k)$, MIMO transmit vector at time k becomes $\mathbf{s}(k)=[s_1(k),\cdots,s_{N_t}(k)]^T$ ($0\le k\le B-1$) and the one transmit block becomes $\mathbf{s}_B=[\mathbf{s}(0),\cdots,\mathbf{s}(B-1)]$, where T means the transpose. Then,

every $\mathbf{s}(k)$ is encoded to $\mathbf{s}'(k)$ by 2-by-2 Alamouti STBC and transmitted using two timeslot as,

$$\mathbf{s}'(k)=\begin{bmatrix} s_1(k) & -s_2^*(k) \\ s_2(k) & s_1^*(k) \end{bmatrix} \quad (1)$$

where * means the complex conjugate. It is assumed that the channel is two-symbol static, antenna- and time k-i.i.d. quasi-static Rayleigh fading, and the channel matrix is given by

$$\mathbf{H}(k)=\begin{bmatrix} h_{11}(k) & \cdots & h_{1N_t}(k) \\ \vdots & \ddots & \vdots \\ h_{N_r1}(k) & \cdots & h_{N_rN_t}(k) \end{bmatrix} \quad (2)$$

where $h_{i_r i_t}(k)$ is the complex channel coefficient from transmit antenna i_t to receive antenna i_r. The received matrix is given by

$$\mathbf{r}'(k)=\mathbf{H}(k)\mathbf{s}'(k)+\mathbf{n}'(k) \quad (3)$$

where the receive matrix $\mathbf{r}'(k)$ and the noise matrix $\mathbf{n}'(k)$ are given, respectively, by

$$\mathbf{r}'(k)=\begin{bmatrix} r_{11}(k) & r_{12}(k) \\ r_{21}(k) & r_{22}(k) \end{bmatrix} \quad (4)$$

$$\mathbf{n}'(k)=\begin{bmatrix} n_{11}(k) & n_{12}(k) \\ n_{21}(k) & n_{22}(k) \end{bmatrix} \quad (5)$$

In the receiver, the STBC decoding is conducted by

$$\begin{bmatrix} r_1(k) \\ r_2(k) \end{bmatrix}=\begin{bmatrix} h_{11}^*(k)r_{11}(k)+h_{21}(k)r_{21}^*(k)+h_{12}^*(k)r_{12}(k)+h_{22}(k)r_{22}^*(k) \\ h_{21}^*(k)r_{11}(k)-h_{11}(k)r_{21}^*(k)+h_{22}^*(k)r_{12}(k)-h_{12}(k)r_{22}^*(k) \end{bmatrix} \quad (6)$$

and the receive vector $\mathbf{r}(k)$ and receive block $\mathbf{r}_B$ are obtained as

$$\mathbf{r}(k)=\left[r_1(k),\cdots,r_{N_r}(k)\right]^T \quad (7)$$

$$\mathbf{r}_B=\left[\mathbf{r}(0),\cdots,\mathbf{r}(B-1)\right] \quad (8)$$

After that, the C-MIMO MLSE is conducted for the receive symbol sequence $\mathbf{r}=\{r_0,\cdots,r_{N_tB-1}\}$, which is the sorted sequence of $\mathbf{r}_B$. The chaos block modulation and demodulation are described in the following.

2.1 Configuration of chaos modulation

In chaos modulation, the bit sequence $\mathbf{b}$ is modulated to MIMO transmission block $\mathbf{s}_B$ [6]. First, the shared key signal among the transmitter and the receiver is set as

$$\mathbf{c}_{M_0}=[c_{00},\cdots,c_{0(M_0-1)}],\ 0<\mathrm{Re}[c_{0i}]<1,\ 0<\mathrm{Im}[c_{0i}]<1 \quad (9)$$

where each c_{0i} ($0\le i\le M_0-1$) is a random complex symbol and is used as an initial value of the chaotic system. By using M_0 independent initial values and averaging the processed chaos signals starting from those initial values, the transmit symbol $s_{i_t}(k)$ can have a Gaussian distribution, and the average squared Euclidean distances of neighboring sequences can be enhanced. When q-bit/symbol rate efficiency is adopted, the number of bits in one block $\mathbf{b}$ is qN_tB and the integer sequence $\mathbf{d}$ is composed by every q bit as

$$\mathbf{d}=[d_0,\cdots,d_{N_tB-1}],\ d_i\in\{0,1,\cdots,2^q-1\} \quad (10)$$

$$d_m=b_{qm}2^{q-1}+b_{qm+1}2^{q-2}+\cdots+b_{q(m+1)-1}2^0,\ 0\le m<N_tB-1$$

Using the bit sequence $\mathbf{b}$, the chaos modulation is conducted as follows. The real and imaginary parts of $c_{(k-1)i}$ are modulated by the different bits as

$$x_0=\{a+d_m/(2^q+1)\}\bmod 1 \quad (11)$$

Real part: $a=\mathrm{Re}[c_{(k-1)i}],\quad m=k$

Imaginary part: $a=\mathrm{Im}[c_{(k-1)i}],\quad m=(k+1)\bmod N_tB$

in the range of $0\le i<M_0-1$ and $1\le k\le N_tB$. When k=1, the initial key signal is modulated. When q=1, it is slightly changed to obtain better sequences as

$$x_0=\begin{cases} a & (b_m=0) \\ 1-a & (b_m=1,\ a>1/2) \\ a+1/2 & (b_m=1,\ a\le 1/2) \end{cases} \quad (12)$$

Then, the variable x_0 is processed as follows:

$$x_{l+1}=2x_l \bmod 1 \quad (13)$$

This (13) is the equation of the Bernoulli shift map. Then, after iterating (13) approximately *Ite* times, the M_0 processed chaos symbol c_{ki} is extracted by

$$\mathrm{Re}[c_{ki}]=x_{Ite+d_{(k+N_tB/2)\bmod N_tB}},\ \mathrm{Im}[c_{ki}]=x_{Ite+d_{(k+N_tB/2+1)\bmod N_tB}} \quad (14)$$

where the iteration number is shifted by the different bits of $\mathbf{b}$ from (11) and (12). By (11), (12) and (14), the chaos symbols correlated to the transmit bits can be generated. Finally, the transmit random Gaussian symbol $s_{Ite,k}$ is obtained by averaging all chaos element symbols c_{ki} ($0\le i\le M_0-1$) as

$$s_{Ite,k}=\frac{1}{M_0}\sum_{i=0}^{M_0-1}(\mathrm{Re}[c_{ki}]-\mathrm{Im}[c_{ki}])\exp\{j4\pi(\mathrm{Re}[c_{ki}]-\mathrm{Im}[c_{ki}])\} \quad (15)$$

The MIMO transmit block is composed as follows:

$$\mathbf{s}_B=\begin{bmatrix} s_{Ite,1} & \cdots & s_{Ite,(B-1)N_t+1} \\ \vdots & \ddots & \vdots \\ s_{Ite,N_t} & \cdots & s_{Ite,BN_t} \end{bmatrix} \quad (16)$$

Each MIMO antenna transmits the allocated symbols of (16) B times. The configurations of (11), (12), (14), and (15) are determined empirically so as to make the $s_{Ite,k}$ Gaussian signal having a large minimum squared Euclidean distance (MSED) between the neighboring sequences, and it is expected that this configuration can be flexibly changed to some extent.

In random sequence transmissions based on chaos, sometimes the MSED between neighboring sequences becomes small, and the error rate performance in the receiver is degraded. For this problem, it has been shown in [6] that an adaptive chaos iteration scheme of *Ite* is effective. Thus, this scheme is adopted in this paper. After $\mathbf{s}_B$ of (16) is generated with *Ite* iteration, $\mathbf{s}_B$ is again generated within the range of $I_0\le Ite\le I_0+M$, and the sequence with the largest MSED is selected. Then, this $\mathbf{s}_B$ is transmitted. By this scheme, the error rate performance can be improved when the receiver detects the correct *Ite*. Here, this iteration number is not transmitted in the proposed scheme, and the blind estimation of *Ite* is conducted in the receiver jointly with the decoding because this additional information decreases the rate efficiency. The transmit block $\mathbf{s}_B$ with *Ite* iteration is rewritten in vector form as

$$\mathbf{s}_{Ite}=[s_{Ite,1},\cdots,s_{Ite,N_tB}] \quad (17)$$

and the neighbor sequence corresponding to $\mathbf{b}'$ is denoted by

$$\mathbf{s}'_{Ite}=[s'_{Ite,1},\cdots,s'_{Ite,N_tB}]$$

Then, the squared Euclidean distance between two sequences is given by

$$d_s^2 = \sum_{k=1}^{N_t B} \left| s_{Ite,k} - s'_{Ite,k} \right|^2 \tag{18}$$

and the MSED becomes

$$\min_{\mathbf{b}' \neq \mathbf{b}} d_s^2 = \min_{\mathbf{b}' \neq \mathbf{b}} \sum_{k=1}^{N_t B} \left| s_{Ite,k} - s'_{Ite,k} \right|^2$$

Therefore, the transmitter selects the best *Ite* such that

$$Ite = \arg\max_{I_0 \le Ite \le I_0 + M} \left[\min_{\mathbf{b}' \neq \hat{\mathbf{b}}} \sum_{k=1}^{N_t B} \left| s_{Ite,k} - s'_{Ite,k} \right|^2 \right] \tag{19}$$

and the sequence of (17) with *Ite* iterations is transmitted. The drawback of this adaptive processing scheme is an increase in the computational complexity in the transmitter.

2.2 MLSE decoding

In the receiver, the joint MLSE in terms of MIMO detection and chaos demodulation is conducted. First, the MLSE result at each *Ite* among $I_0 \le Ite \le I_0 + M$ is calculated by

$$\hat{\mathbf{b}}_{Ite} = \arg\min_{\mathbf{b}} \sum_{k=1}^{N_t B} \left\| \mathbf{r}(k) - \mathbf{H}(k)\mathbf{s}(k) \right\|^2 \Big|_{Ite} \tag{20}$$

Then, the decoding candidate $\hat{\mathbf{b}}$ and the estimated *Ite* are determined by $\hat{\mathbf{b}}_{Ite}$ with the minimum distance in the right-hand side of (20). After that, the transmitter rule check is conducted, and if the check is not passed, that candidate is eliminated, and the decoding procedure is restarted. More specifically, whether the estimated *Ite* satisfies the generation rule of the transmitter

$$Ite = \arg\max_{I_0 \le Ite \le I_0 + M} \left[\min_{\mathbf{b}' \neq \hat{\mathbf{b}}} \sum_{k=1}^{N_t B} \left| s_{Ite,k} - s'_{Ite,1} \right|^2 \right] \tag{21}$$

or not is confirmed. If $\hat{\mathbf{b}}$ and *Ite* satisfy (21), $\hat{\mathbf{b}}$ is determined to be the decoded result. Otherwise, it can be determined as an incorrect sequence. In this case, $\hat{\mathbf{b}}$ is eliminated, and the decoding search is restarted. In the structure of the proposed scheme, user identification is conducted by the initial key value $\mathbf{c}_{M_0}$ in (9). However, if one or more parts of the chaos configurations, e.g., (11) to (15), are slightly changed, the transmission signals are drastically changed because of the initial value sensitivity of chaos. This property can be utilized for user identification, where each user has a slightly different C-MIMO configuration.

In the proposed chaos MIMO scheme, the decoding complexity is exponentially increased according to the block length *B* compared to the conventional MIMO-maximum likelihood decoding (MLD) scheme. Furthermore, the complexities at both the transmitter and the receiver are increased by the adaptive chaos processing. It is assumed that the calculations of the squared Euclidean distance between two sequences are counted as one search, and the total number of searches is derived. Table I shows a comparison of the computational complexities, where l_p denotes the number of sequence eliminations and re-decoding based on (21).

Table I Comparison of computational complexity.

	MIMO-MLD	proposed adaptive C-MIMO
transmitter	0	$(2^{qN_t B} - 1)(M + 1)$
receiver	2^{qN_t}	$(2^{qN_t B+1} - 1)(M + 1)(l_p + 1)$
total	2^{qN_t}	$(M+1) \cdot \left\{ l_p (2^{qN_t B+1} - 1) + 3 \cdot 2^{qN_t B} - 2 \right\}$

As the conventional scheme, MIMO-MLD is compared. It can be observed that the sequence search of adaptive *Ite* is needed at the transmitter in proportion to its range *M* in the proposed scheme. Moreover, at the receiver, the calculation complexity is exponentially increased by the block length *B* and linearly increased by the adaptive range *M*. Because the elimination of (21) does not occur often in the higher receive SNR region, and the l_p term can be ignored, l_p=0 is satisfied at high SNR. Then, the computational complexity of the proposed scheme is increased by *B* and the *M* extension. In contrast, STBC decoding in (6) can be conducted with linear calculation, and it is expected that the bit error rate performance of C-MIMO will be improved by the STBC diversity effect only with the linear calculation increase of STBC decoding.

3. Numerical results

The block error rate (BLER) performance of the proposed scheme is calculated in the simulation condition listed in Table 1. The parameters of chaos modulation are the same as [6] in which the configuration is empirically searched. The chaos equation is Bernoulli shift map, the number of chaos multiplexing to make the transmit symbol Gaussian is M_0=10, the base iteration number of chaos is I_0=19, and the adaptive chaos processing range to enhance the MSED is *M*=2. It is assumed that the initial chaos vector (9) of common key is generated using a specific number such as receiver terminal ID and shared with the transmitter and the receiver. The performance is compared with unencrypted MIMO-MLD, MIMO-STBC, and encrypted C-MIMO without STBC which have the same rate-efficiency. The block length for calculating the block error rate is *B* for C-MIMO and 1 (that is one STBC block) for conventional MIMO.

Table II Simulation conditions.

	conventional	proposed
Modulation, bit/sym	BPSK,QPSK	q=1,2
PHY encryption	N/A	available
MIMO-STBC	(N_t,N_r)=(2,2)-Alamouti	
Channel	STBC block- and antenna-i.i.d. 1-path Rayleigh fading	
Receive channel estimation	perfect	
Decoding algorithm	MLD	MLSE
C-MIMO block length	-	B=2,3,4
Chaos	-	Bernoulli shift map
Num. of chaos multiplexing	-	M_0=10
Num. of chaos processing	-	I_0=19
Adaptive chaos processing range	-	M=2

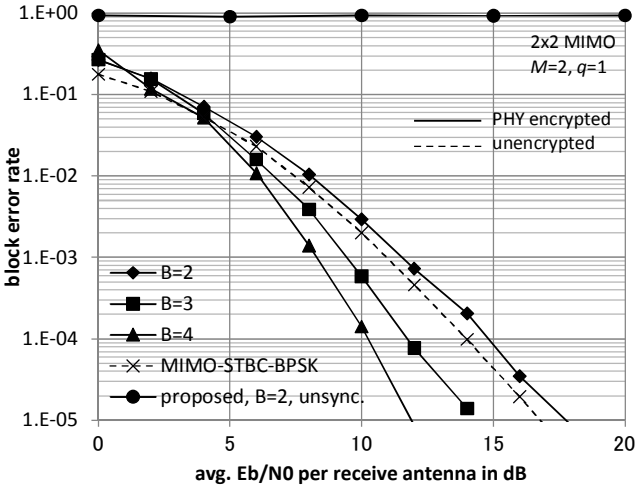

Fig. 2 Block error rate versus average E_b/N_0 at q=1.

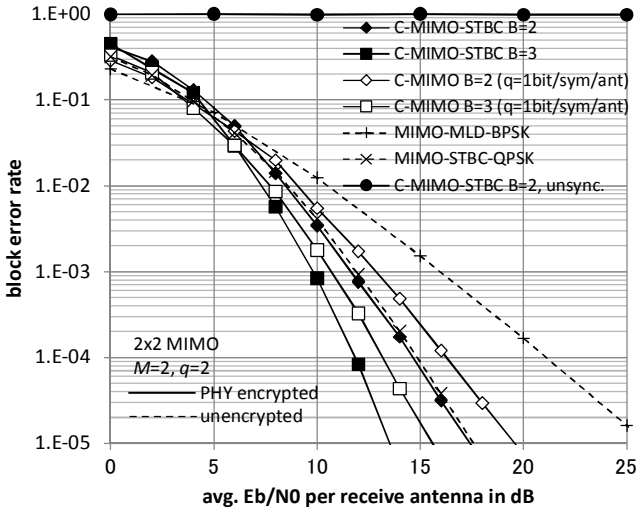

Fig. 3 Block error rate versus average E_b/N_0 at q=2.

Fig. 2 shows the BLER versus average E_b/N_0 per receive antenna when q=1. Compared to MIMO-STBC-BPSK with the same rate-efficiency, the channel coding gain is obtained at B=3 and more. When the M_0 initial key symbols have slightly an error of 10^{-3} distance, the BLER becomes near 1 and the transmit bits cannot be correctly decoded. Hence, it is shown that the proposed scheme achieves both channel coding gain and physical layer security.

Next, the BLER performance versus average E_b/N_0 per receive antenna when q=2 is shown in Fig. 3. It is shown that the proposed scheme has performance improvement by STBC effect. At BLER of 10^{-4}, the proposed scheme with B=2 and 3 has around 1.5 dB coding gain for C-MIMO without STBC at the same rate-efficiency. Furthermore, compared to the unencrypted MIMO transmission, the proposed scheme achieves physical layer security and larger coding gain, especially with B=3. Compared to MIMO-BPSK-MLD and MIMO-STBC-QPSK, the proposed scheme at B=3 has around 9 and 2.5 dB gains, respectively. In comparing the decoding complexity as the tradeoff of the channel coding gain, the number of decoding search of the conventional unencrypted MIMO with BPSK and QPSK is 4 and 16, respectively, while that of the proposed scheme with q=1 and M=2 is 48 at B=2 and 192 at B=3. When q=2, it becomes 768 and 12288 at B=2 and 3, respectively. Thus, the further reduction of decoding complexity will be needed in the proposed scheme and the application of M-algorithm for MLSE is considered. Also, the complexity-reduced block length B expansion scheme will be considered.

4. Conclusions

In this paper, we proposed a space-time block coded chaos MIMO transmission scheme to achieve physical layer security and channel coding gain with restricted decoding complexity. As a results, the improved channel coding gain is obtained with the additional linear calculation of STBC, though the complexity of chaos modulation is not changed. The improved BLER performance was confirmed by numerical results.

In future studied, the reduction of decoding complexity, the block length expansion, and the outer channel code concatenation will be considered.

Acknowledgments

This research was partially supported by Strategic Information and Communications R&D Promotion Programs (SCOPE) in the Ministry of Internal Affairs and Communications, the KDDI foundation, and the Scientific Research Grant-in-aid of Japan No. 26420355. The authors wish to thank all of them for their support.

References

[1] Y.-S. Shiu, S.-Y. Chang, H.-C. Wu, S.C.-H. Huang, H.-H. Chen, "Physical layer security in wireless networks: a tutorial," IEEE Wireless Communications, vol. 18, no. 2, pp .66-74, Apr. 2011.

[2] E. Okamoto, "A chaos MIMO transmission scheme for channel coding and physical-layer security," IEICE Trans. Commun., vol. E95-B, no.4, pp.1384-1392, Apr. 2012.

[3] S. Wang and X. Wang, "M-DCSK-based chaotic communications in MIMO multipath channels with no channel state information," IEEE Trans. Circuits & Systems II: Express Briefs, vol. 57, no. 12, pp. 1001-1005, Dec. 2010.

[4] G. Zheng, D. Boutat, T. Floquet, J.-P. Barbot, "Secure Communication Based on Multi-input Multi-output Chaotic System with Large Message Amplitude," Chaos, Solitons & Fractals, Vol. 41, No 3, pp. 1510-1517, 2009.

[5] G. Kaddoum and F. Gagnon, "Performance analysis of STBC-CSK communication system over slow fading channel," Signal Processing, vol. 93, no. 7, pp. 2055-2060, 2013.

[6] E. Okamoto and Y. Inaba, "Multilevel Modulated Chaos MIMO Transmission Scheme with Physical Layer Security," Nonlinear Theory and Its Applications, IEICE, vol. E5-N, no. 2, Apr. 2014.

[7] Y. Inaba and E. Okamoto, "Multi-User Chaos MIMO-OFDM Scheme for Physical Layer Multi-Access Security," Nonlinear Theory and Its Applications, IEICE, vol. E5-N, no. 2, Apr. 2014.

[8] S. Alamouti, "A simple transmit diversity technique for wireless communications," IEEE Journal on Selected Areas in Commun., vol. 16, no. 8, pp. 1451-1458, Oct 1998.