ISSN 1392 – 124X INFORMATION TECHNOLOGY AND CONTROL, 2009, Vol. 38, No. 1

AN EXTENDED CERTIfiCATE-BASED AUTHENTICATION AND SECURITY PROTOCOL FOR MOBILE NETWORKS

Cheng-Chi Lee

Asia University, Department of Information and Communication Engineering
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan, R.O.C.
e-mail: cclee@asia.edu.tw

I-En Liao

National Chung Hsing University, Department of Computer Science
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.

Min-Shiang Hwang

National Chung Hsing University, Department of Management Information Systems
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.

Abstract. An optimized certificate-based protocol for mobile network with authentication and security has been proposed by Yi et al. This protocol allows efficient computation and less storage requirement in the mobile device. As a result, less power is consumed in the mobile device. However, in 1999, 2002, and 2003, Martin et al., Wong, and Laih et al. respectively showed that Yi et al.'s scheme is vulnerable to some attacks, but did not remedy these attacks. In this paper, we propose an improved protocol to remedy these attacks. Using the new protocol, the protection against attacks can be assured. The security of the key distribution on the mobile network is enhanced as well.

Key words: Authentication, key distribution, mobile communication, privacy, security.

1. Introduction

Nowadays, mobile communication is widespread in the world, and has become a necessity in our daily lives. Despite the convenience of mobile communication, an important issue, the security of communication, has drawn the attention of researchers and manufacturers. Mobile communication is vulnerable to data interception and unauthorized access than wired communication networks. Among these security threats, privacy of communication and authentication of the user are the two major security problems yet to be solved [4, 5, 10, 15, 22].

Privacy is the most obvious need for a cryptosystem. It ensures the private messages will not be disclosed to illegal users. When a message is transmitted through the networks, it is first encrypted and anyone who tries to read it has to have a secret key to decipher the information. Even if the message is intercepted on the network, no one can read it unless he/she is a legal receiver. In the mobile network, privacy involves ensuring that an eavesdropper cannot successfully decipher the information transmitted by mobile users [14, 17, 25].

Authentication is a mechanism to ensure only legal users can access the network. When a mobile user tries to setup a communication session with another user, he/she must verify the identity of the other. This is a mutual authentication process to prevent a fraudulent user from accessing the network [8, 13, 16, 24]. In the mobile network, authentication involves ensuring that the network services are not obtained fraudulently.

There have been many research efforts aiming at designing secure protocols for privacy and authentication on the mobile network [1–4, 10, 15, 23, 26]. In [23], Yi et al. proposed a certificate-based protocol which has the advantages of simpler algebraic computation and less storage space required in the mobile device, thereby, reducing the power consumption in the mobile device. In their method (called YOL protocol), the mobile user and the base station can easily achieve mutual authentication, and a more efficient scheme of key distribution is proposed. Despite the advantage of their method, it is obvious that their method cannot protect certificate against replaying attack [9, 18]. To resist the replaying attack, Hwang et al. proposed an extended version of YOL protocol using timestamp [9]. However, Wong pointed out that

Hwang et al.'s protocol is also vulnerable to the replaying attack [21]. In addition, Laih et al. and Wong respectively pointed out that the YOL protocol is vulnerable to an attack which allows an adversary to forge a mobile user to login [12, 21]. We will discuss the security flaws of YOL protocol in Section 3.

In this paper, a significant improvement of YOL protocol is proposed. We will show that the proposed protocol provides the ability to ensure privacy and authentication on mobile communication, and remedy the security flaw of YOL protocol. The rest of this paper is organized as follows: in the next section, we review the YOL protocol and point out its drawbacks in Section 3. Then our protocol is discussed in Section 4. In Section 5, we analyze the security of our protocol. Finally, we conclude this paper in the last section.

2. Review of YOL Protocol

Yi, Okamoto, and Lam proposed an optimized protocol for mobile network authentication and security [23]. It's a protocol which utilizes the ElGamal signature [7] and Diffie-Hellman's key distribution protocol [6]. This protocol can be divided into two phases: (1) certification and (2) mutual authentication and key distribution, as described in the following two subsections.

2.1. Certification

In this phase, each participant of the mobile network is assigned a certificate by a trusted certification authority (CA). The CA provides the public key certification service and is considered as a trusted third party.

1. Each participant has a triplet, (p, q, g), chosen by the CA, where p is a large prime number, q is a large factor of $(p-1)$, and $g = h^{(p-1)/q} \bmod p$ with h being an integer satisfying $(1 < h < p-1)$ and $h^{(p-1)/q} \bmod p > 1$.

2. Each participant uses the triplet to generate its public and secret keys. Let the public and secret keys of a mobile user be denoted by (y_m, x_m), where $(y_m = g^{x_m} \bmod p)$ and x_m is a secret number chosen randomly from $GF(q)^*$. When the mobile user completes the computation of x_m and y_m, he/she can remove q and g from the memory to save storage space. In a similar way, the pair of public and secret keys of a base station and CA are denoted by (y_b, x_b) and (y_{ca}, x_{ca}), respectively.

3. CA constructs C_x using standard X.509 [11]. For a mobile user m, C_m contains such information as the certificate serial number, validity period, the ID of m, the public key y_m of m, the ID of CA, and the public key y_{ca} of CA. For a base station b, CA also constructs C_b in the same way. Then, both the user and the base station compute the hash values $h(C_m)$ and $h(C_b)$, respectively, by the block cipher techniques (such as IDEA [20]).

4. Each participant has his/her certificate created by the CA: $Cert_{ca,b} \equiv (C_b, s_b, t_b)$ for the base station and $Cert_{ca,m} \equiv (C_m, s_m, t_m)$ for the mobile user. The certificate involves two numbers, s_b and t_b, where $s_b = g^{r_b} \bmod p$ with r_b being a random number chosen from $GF(p)^*$; and $(t_b = -s_b - h(C_b) \times r_b \times x_{ca}^{-1} \bmod q)$. In the similar way, $s_m = g^{r_m} \bmod p$ and $(t_m = -s_m - h(C_m) \times r_m \times x_{ca}^{-1} \bmod q)$.

2.2. Mutual Authentication and Key Distribution

When a mobile user and a base station try to communicate with each other, they use their certificates for mutual authentication. And then a session key is determined for communication between them. The detailed process is shown in Figure 1 and is described as follows.

1. When a mobile user wants to communicate with a base station, he/she sends a $SETUP$ signal and the certificate $Cert_{ca,m}$ to the base station.

2. When the base station receives the certificate, it can verify the validity of the mobile user by checking the equality of the following equation:

$$y_{ca}^{s_m+t_m} \times s_m^{h(C_m)} \bmod p = 1. \quad (1)$$

Then it sends $CONNECT$ signal, its certification $Cert_{ca,b}$, and $y_m^{-x_b} \times k \bmod p$ to the mobile user, where k is a random number working as a session key to communicate between the mobile user and the base station.

3. When the mobile user receives the certificate of base station, he/she can verify the validity of the base station by checking the equality of the following equation:

$$y_{ca}^{s_b+t_b} \times s_b^{h(C_b)} \bmod p = 1. \quad (2)$$

Then he/she can factor k out of $y_m^{-x_b} \times k \bmod p$ by computing:

$$y_b^{x_m} \times (y_m^{-x_b} \times k) \bmod p = k.$$

Consequently, they can use the session key k to encrypt and decrypt the transmitted message using a symmetric cryptosystem [20] between the mobile user and base station.

3. Cryptanalysis of YOL Protocol

In 1999, Martin and Mitchell proposed some comments on YOL protocol [18]. Later, in 2002,

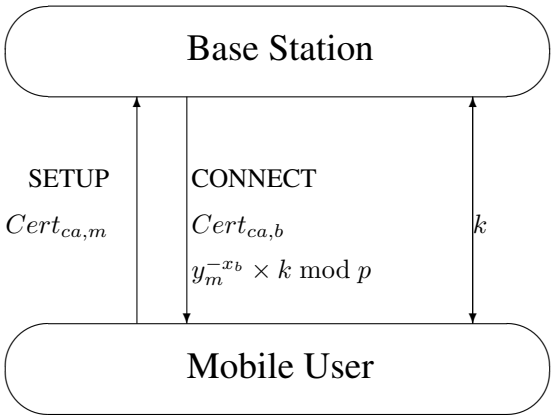

Figure 1. The YOL protocol

Wong proposed a forgery attack to YOL protocol [21]. In 2003, Laih et al. also proposed another forgery attack to YOL protocol [12]. We show their cryptanalysis of YOL protocol in the following three subsections.

3.1. Martin et al. Attack

Martin and Mitchell proposed some comments on YOL protocol. We described their comments as follows.

1. The protocol cannot protect the certificate from replaying attack for mobile network. Although an attacker cannot obtain the session key to eavesdrop the communication, he/she can intercept the certificate $Cert_{ca,m}$ of the mobile user (or $Cert_{ca,b}$ of the base station) and replay it. An attacker can pass the authentication from the mobile user or the base station even though he/she cannot eavesdrop the communication between them, and both the mobile user and the base station would believe the attacker is a legal user.

2. There is no implicit key authentication from the mobile user to the base station, since the mobile user has to trust that the base station had generated the key on its own and by a suitable technique.

3. There is no mechanism for enabling the mobile user to check that the computed key is indeed correct.

4. In addition, if the session key, k, is known by an attacker one day, the other session key is derived. We explain as follows. If an attacker intercept $y_m^{-x_b} \times k \bmod p$ from the transmitted message, he/she can separate $y_m^{-x_b} \bmod p$ by computing:

$$\frac{y_m^{-x_b} \times k(\mathrm{mod}p)}{k(\mathrm{mod}p)} = y_m^{-x_b}(\mathrm{mod}p).$$

In next communication between the mobile user and base station, the attacker can derive this session key, k', from $y_m^{-x_b} \bmod p$ by computing:

$$\frac{y_m^{-x_b} \times k'(\mathrm{mod}p)}{y_m^{-x_b}(\mathrm{mod}p)} = k'.$$

3.2. Wong Attack

Without knowing the secret key x_{ca} of CA, any attacker can easily construct a forged certification (C', s', t') that could be verified successfully by all participants in the network and C' can be chosen arbitrarily to pretend a mobile user or a base station. We brief this attack as follows.

1. An intruder can intercept a valid certificate (C, s, t). The intruder computes $(s + t)h(C)^{-1} = -rx^{-1}(\mathrm{mod}q)$. Let $X = -rx^{-1}(\mathrm{mod}q)$.

2. The intruder can choose a message C' and then generate the corresponding (s', t'), where $s' = s$ and $t' = -s' + h(C')X(\mathrm{mod}q)$.

3. It can be seen that this (C', s', t') satisfies Equations (1) and (2).

3.3. Laih et al. Attack

Laih et al. proposed another forgery attack. An intruder can also construct a forged certification (C', s', t') without knowing the secret key x_{ca} of CA. The attack is briefed as follows.

1. An intruder randomly chooses an integer u and a message C'. The intruder computes $s' = (y_{ca}^u)^{-h(C')^{-1}}(\mathrm{mod}p)$.

2. Compute $t' = u - s'(\mathrm{mod}q)$.

3. It can be seen that this (C', s', t') satisfies Equations (1) and (2).

4. The Proposed Protocol

We have indicated the drawbacks of YOL protocol in the previous section. In the following, we describe a new protocol to remedy those shortcomings. The new protocol can also be divided into two phases: (1) certification and (2) mutual authentication and key distribution, described as follows:

4.1. Certification

In this phase, the first 3 steps are the same as those in the certification phase of YOL protocol. However, Step 4 in YOL protocol is modified as follows.

4'. The CA creates certificates $Cert_{ca,b} = (C_b, s_b, t_b)$ for the base station and $Cert_{ca,m} = (C_m, s_m, t_m)$ for the mobile user. Here, $s_b = g^{r_b} \bmod p$; r_b is a random number chosen from $GF(p)^*$; $t_b = -h(C_b) \times r_b \times x_{ca}^{-1} \bmod q$; $s_m = g^{r_m} \bmod p$; and $t_m = -h(C_m) \times r_m \times x_{ca}^{-1} \bmod q$.

4.2. Mutual Authentication and Key Distribution

When a mobile user and a base station try to communicate with each other, they use their certificates for mutual authentication. And then a session key is determined for communication between them. The detailed process is shown in Figure 2 and is described as follows.

1. **Mobile user to base station (m to b):**
When a mobile user wants to communicate with a base station, he/she sends a $SETUP$ signal, the certification $Cert'_{ca,m}$ and $T = (T_{1m}, T_{2m})$ to the base station, where $Cert'_{ca,m} = (C_m, z_m, t_m)$ with $z_m = s_m^{T_m} \bmod p$, and T_m is a time-stamp of mobile user. T_{1m} and T_{2m} are the signature of T_m. It is based on Nyberg-Rueppel signature scheme [19]. Mobile user generates a random number r. He/she then computes $T_{1m} = T_m g^r \bmod p$ and $T_{2m} = (x_m T_{1m} + r) \bmod q$.

2. **Base station to mobile user (b to m):**
When the base station receives T, and certification of the mobile user, (z_m, t_m), it extracts the time-stamp T_m from $T_m = g^{-T_{2m}} y_m^{T_{1m}} T_{1m} \bmod p$ and verifies the validity of time-stamp and certification of the mobile user as follows.

$$y_{ca}^{t_m \times T_m} \times z_m^{h(C_m)} \bmod p = 1. \quad (3)$$

If the validity of time-stamp and Equation (3) hold, the base station sends $CONNECT$ signal, the certification $Cert'_{ca,b} = (C_b, z_b, t_b)$ with $z_b = s_b^{T_b} \bmod p$, and $T' = (T_{1b}, T_{2b})$ to the mobile user, where T_b is a time-stamp of base station, T_{1b} and T_{2b} are the signature of T_b, $T_{1b} = T_b g^{r'} \bmod p$, $T_{2b} = (x_b T_{1b} + r') \bmod q$, and r' is a random number generated by base station. Next, the base station generates a session key, $K_c = f(K_i, T_b)$, for secure communication between the mobile user and the base station. Here, $K_i = y_m^{x_b} \bmod p$ is a secret parameter; $f(K_i, T_b)$ is a one-way hash function [20] with two parameters, K_i and T_b.

3. **Between mobile user and base station (m and b):**
When the mobile user receives T', and certification of the base station, (z_b, t_b), he/she extracts the time-stamp T_b from $T_b = g^{-T_{2b}} y_b^{T_{1b}} T_{1b} \bmod p$ and verifies the validity of time-stamp and certification of the base station as follows.

$$y_{ca}^{t_b \times T_b} \times z_b^{h(C_b)} \bmod p = 1. \quad (4)$$

If the validity of time-stamp, T_b, and Equation (4) hold, the mobile user uses the $K_i = y_b^{x_m} \bmod p$, a secret parameter, to derive the session key, $K_c = f(K_i, T_b)$. Finally, they can use the K_c to encrypt and decrypt the transmitted messages using the symmetric cryptosystem [20].

5. Cryptanalysis of The Proposed Protocol

The proposed protocol is based on the difficulty of solving discrete logarithms problem and the Diffie-Hellman key exchange scheme [6]. It is impossible for anyone to obtain the session key (K_c) and the secret parameter (K_i) without the knowledge of the secret key, either x_m of the mobile user or x_b of the base station, to eavesdrop the communication between the mobile users and base stations.

Five characteristics can be identified in our method:

1. An attacker cannot forge a valid signature pair (z, t) without knowing the secret key x_{ca} of CA. In addition, it is impossible to generate a correct pair of (z, t) because it is extremely difficult to solve for t (or z) using Equations (3) and (4).

The attacks proposed by Wang [21] and Laih et al. [12] cannot work successfully in our protocol. In Wong's attack: if an intruder intercepts a valid certificate (C, z, t), he/she computes $(z + t)h(C)^{-1} (\bmod q)$, which is not equal to $-rx^{-1} (\bmod q)$. Hence, the Wong's attack cannot work in our protocol. In Laih et al.'s attack: an intruder may randomly choose an integer u and a message C'. The intruder computes $s' = (y_{ca}^u)^{-h(C')^{-1}} (\bmod p)$. And then he/she computes $t' = u - s' (\bmod q)$. It can be seen that this (C', s', t') does not satisfy Equations (3) and (4) with s' and t' substituting for z and t, respectively. Therefore, our protocol is more secure than YOL protocol.

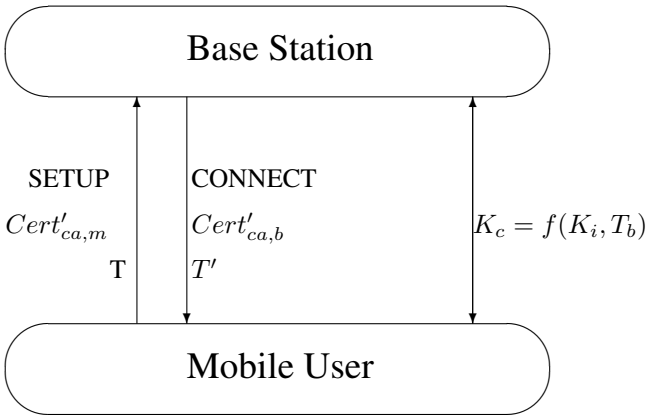

Figure 2. The propsed protocol

2. Time-stamps are used to prevent the certificate from replaying attack. By checking the validity of time-stamp, the system can prevent an attacker from replaying the messages. We use the Nyberg-Rueppel signature scheme [19] to sign the time-stamp. This technique can be used to prove that the time-stamp is sent from a particular mobile user or base station.

3. An attacker cannot eavesdrop the communication between mobile users and base stations without knowing the session key K_c. K_c is generated by a one-way hash function with two parameters, K_i and T_b. Since K_i is protected by the secret key of mobile user or base station, an attacker cannot derive K_c.

4. Since all session keys, K_c, are independent, an attacker cannot use the prior session key to derive the other session keys.

5. In our scheme, the session key, K_c, is generated by a one-way hash function, f, with two parameters, K_i and T_b. If the Equations (3) and (4) hold, the mobile user and the base station can confirm the time-stamp, T_b, and secret parameter, $K_i = y_m^{x_b} \bmod p = y_b^{x_m} \bmod p$. Therefore, our scheme can achieve key authentication [18].

With the aforementioned five properties, our protocol can achieve the requirements stated in Martin and Mitchell [18].

6. Conclusions

Although YOL's protocol has properties of simpler algebraic operations, less storage space, and less power consumption on the mobile device, it is still vulnerable to attacks as pointed out in [12, 18, 21]. In this paper, we propose an improvement to remedy the weaknesses of YOL protocol by using time-stamps. The improvements are three-fold:

- Our method is able to prevent an attacker from replaying or forging certificate.
- It is impossible to obtain the session key because it is protected by the secret keys of mobile user and base station. In addition, the session key is changed constantly, which makes it more difficult to be broken.
- It is harmless that the obsolete session key, K_c, is known by an attacker.

Acknowledgment

This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under the grant NSC 96-2219-E-009-013 and NSC 97-2218-E-468-010.

References

[1] **K. Al-Tawil, A. Akrami, H. Youssef**, "A new authentication protocol for GSM networks," *IEEE 23rd Annual Conference on Local Computer Networks (LCN'98)*, pp. 21–30, 1998.

[2] **A. Aziz and W. Diffie**, "Privacy and authentication for wireless local area networks," *IEEE Personal Communications*, vol. 1, no. 1, pp. 25–31, 1994.

[3] **M. J. Beller, L. F. Chang, and Y. Yacobi**, "Privacy and authentication on a portable communications system," *IEEE Journal on Selected Areas in Communications*, vol. 11, pp. 821–829, Aug. 1993.

[4] **C.-C. Chang, K.-L. Chen, and M.-S. Hwang**, "End-to-end security protocol for mobile communications with end-user identification/authentication," *Wireless Personal Communications*, vol. 28, no. 2, pp. 95–106, 2004.

[5] **C.-W. Chen, M.-C. Chuang, C.-S. Tsai**, "An efficient authentication scheme between MANET and WLAN on IPv6 based Internet," *International Journal of Network Security*, vol. 1, no. 1, 2005, pp. 14–23.

[6] **W. Diffie and M. E. Hellman**, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, Nov. 1976, pp. 644–654.

[7] **T. ElGamal**, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, pp. 469–472, July 1985.

[8] **M.-S. Hwang, C.-C. Lee, S.-K. Chong and J.-W. Lo**, "A Key management for wireless communications," *International Journal of Innovative Computing Information and Control*, vol. 4, issue 8, pp. 2045–2056, August 2008.

[9] **M.-S. Hwang, Y.-L. Tang, and C.-C. Lee**, "A new protocol using time-stamp for mobile network authentication and security," *Technical Report (CYUT-IM-TR-2000-01)*, Department of Information Management, Chaoyang University of Technology, Taiwan, November 2001.

[10] **M.-S. Hwang and W.-P. Yang**, "Conference key distribution schemes for secure digital mobile communications," *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 2, pp. 416–420, 1995.

[11] **ITU.** "ITU-T recommendation X.509: Information technology – open systems interconnection – the directory: Authentication framework,". tech. rep., ITU, 1997.

[12] **C. S. Laih and S. Y. Chiou**, "Cryptanalysis of an optimized protocol for mobile network authentication and security," *Information Processing Letters*, vol. 85, no. 6, pp. 339–341, 2003.

[13] **C.-C. Lee, M.-S. Hwang, I-E. Liao**, "A new authentication protocol based on pointer forwarding for mobile communications," *Wireless Communications and Mobile Computing*, vol. 8, no. 5, pp. 661–672, June 2008.

[14] **C.-C. Lee, M.-S. Hwang, I-E. Liao**, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683–1687, Oct. 2006.

[15] **C.-C. Lee, C.-C. Yang, and M.-S. Hwang**, "A new privacy and authentication protocol for end-to-end mobile users," *International Journal of Communication Systems*, vol. 16, no. 9, pp. 799–808, 2003.

[16] **I-E. Liao, C.-C. Lee, M.-S. Hwang**, "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, vol. 72, no. 4, pp. 727–740, June 2006.

[17] **C.-Y. Liu**, "A lightweight security mechanism for ATM networks," *International Journal of Network Security*, vol. 1, no. 1, pp. 32–37, 2005.

[18] **K. M. Martin and C. J. Mitchell**, "Comments on an optimized protocol for mobile network authentication and security," *ACM Mobile Computing and Communications Review*, vol. 3, no. 2, p. 37, 1999.

[19] **K. Nyberg and R. A. Rueppel**, "A new signature scheme based on the DSA giving message recovery," *In: Proceedings of the 1st ACM Conference on Computer and Communications Security*, Fairfax, Virginia, Nov. 1993, pp. 58–61.

[20] **B. Schneier**, *Applied Cryptography, 2nd Edition*. New York: John Wiley & Sons, 1996.

[21] **D. S. Wong**, "An optimized authentication protocol for mobile network reconsidered," *ACM Mobile Computing and Communications Review*, vol. 6, no. 4, pp. 74–76, 2002.

[22] **C.-C. Yang and K.-H. Chu and Y.-W. Yang**, "3G and WLAN Interworking Security: Current Status and Key," *International Journal of Network Security*, vol. 2, no. 1, pp. 1–13, 2006.

[23] **X. Yi, E. Okamoto, and K.Y. Lam**, "An optimized protocol for mobile network authentication and security," *ACM Mobile Computing and Communications Review*, vol. 2, no. 3, pp. 37–39, 1998.

[24] **S. Wang, Z. Cao, and H. Bao**, "Efficient certificateless authentication and key agreement (CL-AK) for grid computing," *International Journal of Network Security*, vol. 7, no. 3, 2008, pp. 342–347.

[25] **J. Zhan, L. Chang, and S. Matwin**, "Privacy preserving K-nearest neighbor classification," *International Journal of Network Security*, vol. 1, no. 1, 2005, pp. 46–51.

[26] **Y. Zheng**, "An authentication and security protocol for mobile computing," *In: Mobile Communication - Technology, Tools, Applications, Authentication and Security (Proceedings of IFIP World Conference on Mobile Communications), Edited by J. L.Encarnacao and J. M.Rabaey,Chapman and Hall,Canberra, Australia.*, Sep. 1996, pp. 249–257.

Received November 2008.

DOI: 10.5755/j01.itc.38.1.11914