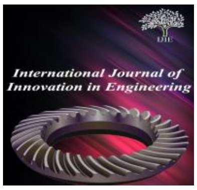
International journal of innovation in Engineering

journal homepage: www.ijie.ir



Research Paper

Security Analysis and Improvement of Wei-Chi Ku and Yi-Han Chen's RFID protocol

MohammadReza Mehrabani[1a], **Soosan Sadegha**[b]

[a] *Department of Electrical Engineering, Iran University of science and Technology, Tehran, Iran*

[b] *Pharmacy faculty, Tehran university of medical science, Tehran, Iran*

ARTICLE INFO

Received: 13 May 2021

Reviewed: 19 May 2021

Revised: 28 May 2021

Accepted: 9 June 2021

Keywords:
Radio frequency identification (RFID), security, privacy, authentication, confidentiality

ABSTRACT

RFID are small wireless devices that can be used for identification of objects and humans. With development of RFID technology and increasing the use of this technology in everyday life, the Security issues in these systems have been growing in terms of importance day by day. In 2012 Wei-Chi Ku and Yi-Han Chen Proposed a new efficient mutual authentication protocol for passive RFID that provides confidentiality, un-traceability and efficiency. This paper demonstrates that Wei-Chi Ku and Yi-Han Chen's protocol has a serious security problem and proposes a new protocol to prevent this security problem by some changes. Furthermore, the capability of our method for improving, confidentiality, untraceability, and data integrity is discussed.

1. Introduction

Systems based on radio frequency identification (RFID) in the past were used to identify physical objects. Due to the importance of RFID in everyday life, the need to maintain security and Privacy in these systems has been increasing day by day. To maintain the security and privacy, authentication protocols, as the core of secure communication in RFID systems, are used. RFID systems use radio frequencies to communicate themselves, and they were used on World War II to identify physical objects for the first time (Cole et al., 2008).

[1] Corresponding author
mrmehrabany@gmail.com

RFID system consists of three parts: RFID tags, RFID readers, and a back-end server. Communication between tag and reader is via radio waves through the wireless channel while the relationship between the reader and the server is through a wired channel. An RFID tag is embedded in an object and has an identification number that is used to identify an RFID-tagged object. Tags include a processor, antenna, and connection element. The reader is formed from a radio frequency unit (including a transmitter, and a receiver antenna) and a control unit (including CPUs, memory, and control circuits), (Yeh et al., 2011). The use of the authentication protocols for RFID systems is a safe way to protect privacy and eliminate the security threats to these systems. These protocols for performing valid and reliable authentication between RFID system components, and also covering the issue of identification, are steadily improving (Zuo, Y., 2010).

In 2008 Song and Mitchell classified the attacks to the RFID authentication protocols into two groups, weak attacks and strong attacks (Song and Mitchell, 2008).

Weak attacks: In this type of attack, the attacker can potentially benefit from two ability, One the capability of the listening to the communication channel between tag and reader (passive attack), and the other capability of changing the messages that are exchanged in the communication channel (active attack). The Attacker is able to use these two abilities, to attack the RFID systems protocols (Rizomiliotis et al., 2009). In the following, we will review the attacks that are in this group.

Impersonation attack: Attackers can masquerade as the reader or the tag to pass the authentication by garbling data and thereby earn illegal advantages (Aghili et al., 2018).

Replay attack: In this attack, an attacker uses a previous relationship between the label and card reader for successful authentication between tag and reader (Van Deursen et al., 2008).

De-synchronization attack: In this attack, the goal attacker is permanent down of the communication between tag and reader in the next contacts. For example, to perform operations that Cause the tag updates information shared with the server, while the server has not done this. In this case, the next contacts between the label and server However, both of which are valid but it will not be able to authenticate one another (Lo, N. W., 2011).

Strong attacks: In these attacks assume the attacker is able to gain confidential information of the tag with any way possible including physical attack, or possession of tag. This assumption is reasonable despite the cheap tags (Song and Mitchell, 2008).

Following instances of the attacks that are in this group are reviewed.

Forward tracing attack: In this attack, the attacker is assumed to have all the information of the tag at time t and all messages of the channel before the time t have been listened enough. Now it must be reviewed to know whether the attacker can track the tag at the arbitrary moment t' which $t' \langle t$ (Habibi and Aref, 2015).

Backward tracing attack: in this attack like backward tacking assume that the attacker has all the information of the tag at time t. The other assumption in this attack is that the attacker has listened all messages of the channel after the time t . Now it must be examined that whether the attacker can trace the tag at the moment $t' \rangle t$ or not (Habibi and Aref, 2015).

In this paper, we propose the improved version of Wei-Chi Ku and Yi-Han Chen's protocol that both preserves its features and solves its security problems. The remaining sections of the paper are organized as follows: Section 2 briefly reviews of Wei-Chi Ku and Yi-Han Chen's protocol. Section 3 gives a security problem of Wei-Chi Ku and Yi-Han Chen's protocol. The improved protocol is presented in Section 4, while Section 5 discusses the security and the performance of the proposed protocol. Some conclusions are presented in Section 6.

2. Review Wei-Chi Ku and Yi-Han Chen's protocol

In this Section, we review the notations used in Wei-Chi Ku and Yi-Han Chen's protocol (Ku and Chen, 2012).

The notation used in Wei-Chi Ku and Yi-Han Chen's protocol is defined as follows:

- N_T : The random number generated by tag
- N_R : The random number generated by reader
- K_i : The tags authentication key
- FLAG: represents whether the previous session is safely terminated (FLAG = 0) or not (FLAG = 1)

2.1 Initialization phase

In this phase, the system, makes a unique EPC code and k to each Tag, and store the corresponding information in the Database. EPC code and K can only be aware of the database and Tag, then reset the value of the Flag to zero (Flag=0).

2.2 The authentication phase

The detailed steps of the authentication phase are presented as follows.

Step 1.

Reader $\rightarrow$ Tag: N_R

The reader generates random number N_R and forwards it to the tag.

Step 2.

Tag $\rightarrow$ Reader: ($FLAG, A, M_1$)

Tag generates random number N_T , and generates A and M_1 as follow:

$$A = N_T \oplus PRNG(K_i)$$

$$\Delta N = N_R - N_T$$

$$M_1 = EPC_i \oplus PRNG(\Delta N) \oplus K_i$$

Tag sends massage $FLAG, A, M_1$ to reader and sets FLAG = 1.

Step 3. R forwards (FLAG, A, M1, NR) to DB.

Step 4. DB performs as follow

- **Case 1 (FLAG = 0):**

DB sequentially retrieves the stored $K_{new}{}^{*}$ and $EPC^{*}{}_{DB}$ in each record to compute

$$N_T{}^{*} = A \oplus PRNG(K_{new}{}^{*})$$

$$\Delta N^{*} = N_R - N_T{}^{*}$$

$$EPC^{*}{}_{DB} = M_1 \oplus PRNG(\Delta N^{*}) \oplus K_{new}{}^{*}$$

If none of the stored EPC_{DB} equals the retrieved $EPC^{*}{}_{DB}$, then DB keeps silent and terminates this protocol run. Otherwise, DB computes

$$N_T = N_T{}^{*}$$

$$\Delta N = \Delta N^{*}$$

$$Q = PRNG(N_T) \,||\, K_{new}$$

$$K_{old} \leftarrow K_{new}$$

Next, DB updates K_{new} with a random number, then computes

$$M_2 = Q \oplus (PRNG(\Delta N) \,||\, K_{new})$$

and then sends (M_2, B, Object-Data) to reader.

- **Case 2 (FLAG = 1):**

DB sequentially retrieves the stored K_{old}*, K_{new}*, and EPC_{DB}* in each record to compute

$$N_T{}^{*} = A \oplus PRNG(K_x{}^{*})$$

$$\Delta N^{*} = N_R - N_T{}^{*}$$

$$EPC^{*}{}_{DB} = M_1 \oplus PRNG(\Delta N^{*}) \oplus K_x{}^{*}$$

If the computed EPC_{DB}* equals the stored EPC_{DB}, X is set to either ‘old’ (if K_{old}* matches) or ‘new’ (if K_{new}* matches). If no match is found, then DB keeps silent and terminates this protocol run. Otherwise, if X = ‘old’, DB computes

$$N_T = N_T{}^{*}$$

$$\Delta N = \Delta N^{*}$$

$Q = PRNG(N_T) \| K_{old}$,

then updates K$_{new}$ with a random number, and computes

$M_2 = Q \oplus (PRNG(\Delta N) \| K_{new})$

$B = CRC(\Delta N \| K_{new})$.

Now DB sends (M2, B, Object-Data) to reader. If X = ‘new’, DB computes

$N_T = N_T^*$

$\Delta N = \Delta N^*$

$Q = PRNG(N_T) \| K_{new}$

$K_{old} \leftarrow K_{new}$.

After that, updates K$_{new}$ with a random number, and computes

$M_2 = Q \oplus (PRNG(\Delta N) \| K_{new})$

and then sends (M_2, B, Object Data) to reader**.**

Step 5. Upon receiving Object-Data, reader forwards (M_2, B) to Tag.

Step 6. Up receiving (M_2, B), T computes

$Q = PRNG(N_T) \| K_i$

$PRNG(\Delta N)^* \| K_{new} = Q \oplus M_2$

If PRNG(ΔN)* equals PRNG(ΔN), then T computes

$B^* = CRC(\Delta N \| K_{new}^*)$.

If B* equals B, then T sets

$K_i \leftarrow K_{new}$

FLAG = 0.

3. Weaknesses of Wei-Chi Ku and Yi-Han Chen’s protocol

In this section, we show that Wei-Chi Ku and Yi-Han Chen’s protocol has the following security problem. This problem is as follows:

3.1 Forward security problem:

In this section, we provide Forward tracking attack on the W protocol and we will show that in this protocol tags are vulnerable to Forward tracking attack. The attack is provided by Oufi, and Phan's formal model (Phan et al., 2011).

Phase 1 (Learning):

At this phase, the attacker will choose two tags, T_0 and T_1 to engage with them, and sends corrupt query to gain T_0's i+1 session's secret values ($K_{i+1}^{T_0}, EPC_{i+1}^{T_0}$).

Phase 2 (Challenge):

At this phase challenger generates a random bit $b \in \{0,1\}$ and depending on what number is b, chooses the tag $T_b \in \{T_0, T_1\}$ and gives it to the attacker. After receiving T_b , attacker again sends Execute(R,T_b,i) query and gets ($A^{T_b}{}_i, M_1{}^{T_b}{}_i, B^{T_b}{}_i, M_2{}^{T_b}{}_i, N_R{}^{T_b}{}_i$).

Phase 3 (Guess):

With the information obtained from the learning and challenge phase, the attacker will perform these steps. He first calculates $\beta = M_2{}^{T_b}{}_i(96:191) \oplus K_{i+1}^{T_0}$ and $\alpha = A^{T_b}{}_i \oplus PRNG(\beta)$. Now attacker can easily detect which tag he has had Communicated in challenge phase. He guesses b' as follow:

$$b' = \begin{cases} 0 & if\ EPC_{i+1}^{T_0} = M_2{}^{T_b}{}_i \oplus PRNG(N_R{}^{T_b}{}_i - \alpha) \oplus \beta \\ 1 & otherwise \end{cases}$$

And so, the resulting advantage for attacker is equal:

$$Adv_A^{UPriv} = \left| p\left(T_b\, chosen\, at\, random\right) - p\left(T_b\, chosen\, correctly\right) \right| = \left| \frac{1}{2} - p\left(T_b\, chosen\, corectly\right) \right|$$

$$= \left| \Pr(b' = b) - \frac{1}{2} \right| = \left| 1 - \frac{1}{2} \right| = \frac{1}{2} \gg \varepsilon$$

Proof:

Because EPC is constant in all the sessions we have: $EPC_{i+1}^{T_0} = EPC_i^{T_b}$, according to this point, the proof is continued as follow:

If $T_0 = T_b$ we will have:

$$M_2{}^{T_b}{}_i(96:191) \oplus K_{i+1}^{T_0} = M_2{}^{T_0}{}_i(96:191) \oplus K_{i+1}^{T_0} = K_i^{T_0} \oplus K_{i+1}^{T_0} \oplus K_{i+1}^{T_0} = K_i^{T_0}$$

$$\Rightarrow \alpha = K_i^{T_0}$$

and

$$A^{T_b}{}_i \oplus PRNG(\alpha) = A^{T_0}{}_i \oplus PRNG(\alpha) = N_T^{T_0} \oplus PRNG(K_i^{T_0}) \oplus PRNG(K_i^{T_0})$$

$$\Rightarrow \beta = {N_T}^{T_0}$$

also, we have:

$${M_2}^{T_b}{}_i \oplus PRNG({N_R}^{T_b}{}_i - \alpha) \oplus \beta = {M_2}^{T_0}{}_i \oplus PRNG({N_R}^{T_0}{}_i - \alpha) \oplus \beta$$

$$= EPC_i^{T_0} \oplus PRNG({N_R}^{T_0}{}_i - {N_T}^{T_0}{}_i) \oplus K_i^{T_0} \oplus PRNG({N_R}^{T_0}{}_i - \alpha) \oplus \beta$$

$$\xrightarrow[2]{1} EPC_i^{T_0}$$

3.2 De-synchronization attack:

With a little attention to the messages M2 and B, the attacker can easily implement de-synchronization attack between tag and reader. The attacker allows to hold a session between the tag and reader. Now attacker blocks M2 and B messages in the fifth stage and stores them. We know that the length of $PRNG(N_T)$ and $PRNG(\Delta N)$ are equal, so M$_2$ is as follow:

$$M_2 = PRNG(N_T) \oplus PRNG(\Delta N) \,||\, K_i \oplus K_{i+1}$$

Therefore, the value of $K_i \oplus K_{i+1}$ is easily separable. Now the attacker can change the new sent key, which the tag cannot understand. The attacker can generate a random number like K' and XOR it with $K_i \oplus K_{i+1}$. Thus, the tag will receive $K_{i+1} \oplus K'$ as a new Key instead of K_{i+1}. The problem is that the tag will evaluate the correctness of new key by generating $B^* = CRC(\Delta N \,||\, {K_{new}}^*)$ and comparing it with received B. So, attacker should change an argument $\Delta N \,||\, K_{new}$ of massage B to $\Delta N \,||\, (K_{new} \oplus K')$. To achieve this goal, we use the lemma of CRC (Yi, X. et al., 2012), that is as follow:

$CRC(A||B)=CRC\ (A_{x<<n} \oplus B\ )=CRC\ (A_{x<<n}) \oplus CRC(B).$

So, we have:

$$B = CRC(\Delta N \,||\, K_{new}) = CRC(\Delta N_{x\ll n} \oplus K_{new}) = CRC(\Delta N_{x\ll n}) \oplus CRC(K_{new}) .$$

Now the attacker can compute $CRC(K')$ and XOR it with B:

$$B \oplus CRC(K') = CRC(\Delta N_{x\ll n}) \oplus CRC(K_{new}) \oplus CRC(K') = CRC(\Delta N_{x\ll n}) \oplus CRC(K_{new} \oplus K')$$
$$= CRC(\Delta N_{x\ll n} \,||\, K_{new} \oplus K')$$

Thus, tag will update its key with $K_{new} \oplus K'$, while the center has updated its key with K_{new} and the de-synchronization attack will happen.

4. Improved protocol

In this section we will propose the improvement of the Wei-Chi Ku and Yi-Han Chen's protocol. The main problem of Wei-Chi Ku and Yi-Han Chen's protocol is messages and B, that in this section we try to solve this problem. We improve protocol by define massage M$_2$ as follow:

$$M_2 = Rot((K_{old} \oplus K_{new}), \Delta N) \oplus PRNG(N_T)$$

4.1 Initialization phase

In this phase, the system, makes a unique EPC code and k to each Tag, and store the corresponding information in the Database. EPC code and K can only be aware of the database and Tag, Then reset the value of the Flag to zero (Flag=0)

4.2 The authentication phase

The detailed steps of the authentication phase are presented as follows.

Step 1.

Reader → Tag: N_R

The reader generates a random number N_R and forwards it to the tag.

Step 2.

Tag → Reader: ($FLAG, A, M_1$)

The tag generates random N_T , and generates A and M_1 as follow:

$$A = N_T \oplus PRNG(K_i)$$

$$\Delta N = N_R - N_T$$

$$M_1 = EPC_i \oplus PRNG(\Delta N) \oplus K_i$$

The tag sends massage $FLAG, A, M_1$ to reader and sets FLAG = 1.

Step 3. R forwards (FLAG, A, M1, NR) to DB.

Step 4. DB performs

Case 1 (FLAG = 0):

DB sequentially retrieves the stored $K_{new}{}^{*}$ and $EPC^{*}{}_{DB}$ in each record to compute

$$N_T{}^{*} = A \oplus PRNG(K_{new}{}^{*})$$

$$\Delta N^{*} = N_R - N_T{}^{*}$$

$$EPC^{*}{}_{DB} = M_1 \oplus PRNG(\Delta N^{*}) \oplus K_{new}{}^{*}$$

If none of the stored EPC_{DB} equals the retrieved $EPC^{*}{}_{DB}$, then DB keeps silent and terminates this protocol run. Otherwise, DB computes

$$N_T = N_T{}^{*}$$

$$\Delta N = \Delta N^*$$

$$K_{old} \leftarrow K_{new}$$

Next, DB updates K_{new} with a random number, then computes

$$M_2 = Rot((K_{old} \oplus K_{new}), \Delta N) \oplus PRNG(N_T)$$

And then sends (M_2, B, Object-Data) to reader.

Case 2 (FLAG = 1):

DB sequentially retrieves the stored K_{old}*, K_{new}*, and EPC_{DB}* in each record to compute

$$N_T^{\ *} = A \oplus PRNG(K_x^{\ *})$$

$$\Delta N^* = N_R - N_T^{\ *}$$

$$EPC^*_{\ DB} = M_1 \oplus PRNG(\Delta N^*) \oplus K_x^{\ *}$$

If the computed EPC_{DB}* equals the stored EPC_{DB}, X is set to either 'old' (if K_{old}* matches) or 'new' (if K_{new}* matches). If no match is found, then DB keeps silent and terminates this protocol run. Otherwise, if X = 'old', DB computes

$$N_T = N_T^{\ *}$$

$$\Delta N = \Delta N^*$$

updates K_{new} with a random number, and computes

$$M_2 = Rot((K_{old} \oplus K_{new}), \Delta N) \oplus PRNG(N_T)$$

$$B = CRC(\Delta N \,||\, K_{new})$$

And then, DB sends (M_2, B, Object-Data) to reader. If X = 'new', DB computes

$$N_T = N_T^{\ *}$$

$$\Delta N = \Delta N^*$$

$$K_{old} \leftarrow K_{new}$$

updates K_{new} with a random number, and computes

$$M_2 = Rot((K_{old} \oplus K_{new}), \Delta N) \oplus PRNG(N_T)$$

And d then, DB sends (M_2, B, Object Data) to reader.

Step 5. Upon receiving Object-Data, reader forwards (M_2, B) to Tag.

Step 6. Up receiving (M_2, B), T computes

$M_2 \oplus PRNG(N_T) = Rot((K_{old} \oplus K_{new}), \Delta N)$

$K_{old} \oplus K_{new} = Rot(Rot((K_{old} \oplus K_{new}), \Delta N) \gg \Delta N)$

Now tag XOR $K_{old} \oplus K_{new}$ with K_{old} to obtain their new key.

then T computes $B^* = CRC(\Delta N \,||\, K_{new}{}^*)$, If B* equals B, then T sets

$K_i \leftarrow K_{new}$

FLAG = 0

5. Analysis

5.1 Confidentiality

Confidentiality means we must ensure that information is only available to those who are authorized to access this information (Shi, Z. et al. 2017). The EPC information of tag in this protocol will remain secret just like the Wei-Chi Ku and Yi-Han Chen's protocol. In fact, the only difference between our protocol and Wei-Chi Ku and Yi-Han Chen's protocol is in their fifth round while in our protocol the reader sends $M_2 = Rot((K_{old} \oplus K_{new}), \Delta N) \oplus PRNG(N_T)$, instead of $M_2 = Q \oplus (PRNG(\Delta N) \,||\, K_{new})$.

5.2 Untraceability

The problem of Wei-Chi Ku and Yi-Han Chen's protocol was M_2 that in improved protocol we defined the new massage that is secure against traceability.

5.3 Data integrity

Data integrity means that no person should be able to alter or manipulate the exchange information between parties of protocol (Su, W. et al. 2007). The new Protocol unlike Wei-Chi Ku and Yi-Han Chen's protocol that was very vulnerable to de-synchronization attack supplies data integrity and this is Because of changes in the last round of the Wei-Chi Ku and Yi-Han Chen's protocol. In the new protocol, adversary won't be able to change massage M_2 as he could change it in the Wei-Chi Ku and Yi-Han Chen's protocol, so the new protocol is secure against de-synchronization attack.

6. Conclusions

It is observed that with a little change in the Wei-Chi Ku and Yi-Han Chen's protocol we could promote this protocol and have an efficient mutual authentication protocol for passive RFID tags that provides data integrity, confidentiality, untraceability, mutual authentication, and efficiency. The improved protocol has all features of the Wei-Chi Ku and Yi-Han Chen's protocol in time complexity, space complexity, and communication cost.

References

- Aghili, S. F., Ashouri-Talouki, M., & Mala, H. (2018). DoS, impersonation and de-synchronization attacks against an ultra-lightweight RFID mutual authentication protocol for IoT. *The Journal of Supercomputing*, *74*(1), 509-525. doi: https://doi.org/10.1007/s11227-017-2139-y

- Cole, P. H., & Ranasinghe, D. C. (2008). Networked RFID systems and lightweight cryptography. London, UK: Springer. Doi: https://doi.org/10.1007/978-3-540-71641-9

- Habibi, M. H., & Aref, M. R. (2015). Attacks on recent RFID authentication protocols. *Journal of Signal Processing Systems*, *79*(3), 271-283. doi: https://doi.org/10.1007/s11265-013-0844-1
- Ku, W. C., & Chen, Y. H. (2012, August). Improvement of EPC-C1G2 RFID authentication protocols. In *2012 1st IEEE International Conference on Communications in China (ICCC)* (pp. 226-230). IEEE. doi: https://doi.org/10.1109/ICCChina.2012.6356882
- Lo, N. W., & Yeh, K. H. (2010, October). De-synchronization attack on RFID authentication protocols. In *2010 International symposium on information theory & its applications* (pp. 566-570). IEEE. Doi: https://doi.org/10.1109/ISITA.2010.5649726
- Phan, R. C. W., Wu, J., Ouafi, K., & Stinson, D. R. (2011). Privacy analysis of forward and backward untraceable RFID authentication schemes. *Wireless Personal Communications*, 61(1), 69-81. Doi: https://doi.org/10.1007/s11277-010-0001-0
- Rizomiliotis, P., Rekleitis, E., & Gritzalis, S. (2009). Security analysis of the Song-Mitchell authentication protocol for low-cost RFID tags. *IEEE Communications Letters*, *13*(4), 274-276. Doi: https://doi.org/10.1109/LCOMM.2009.082117
- Shi, Z., Chen, J., Chen, S., & Ren, S. (2017, March). A lightweight RFID authentication protocol with confidentiality and anonymity. In 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (pp. 1631-1634). IEEE. Doi: https://doi.org/10.1109/IAEAC.2017.8054290
- Song, B., & Mitchell, C. J. (2008, March). RFID authentication protocol for low-cost tags. In *Proceedings of the first ACM conference on Wireless network security* (pp. 140-147). Doi: https://doi.org/10.1145/1352533.1352556
- Su, W., Alchazidis, N., & Ha, T. T. (2007, October). Data Integrity in RFID Systems. In *MILCOM 2007-IEEE Military Communications Conference* (pp. 1-7). IEEE. Doi: https://doi.org/10.1109/MILCOM.2007.4455274
- Van Deursen, T., & Radomirović, S. (2009). Attacks on RFID protocols. *Cryptology ePrint Archive*, *2008*(310), 1-56.
- Yeh, T. C., Wu, C. H., & Tseng, Y. M. (2011). Improvement of the RFID authentication scheme based on quadratic residues. *Computer Communications*, *34*(3), 337-341. Doi: https://doi.org/10.1016/j.comcom.2010.05.011
- Yi, X., Wang, L., Mao, D., & Zhan, Y. (2012). An gen2 based security authentication protocol for RFID system. *Physics Procedia*, *24*, 1385-1391. Doi: https://doi.org/10.1016/j.phpro.2012.02.206
- Zuo, Y. (2010). Survivable RFID systems: Issues, challenges, and techniques. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *40*(4), 406-418. doi: https://doi.org/10.1109/TSMCC.2010.2043949