strict protection as assumed, it is infeasible for Eve to obtain $h(r \oplus PW_i)$ in this way. In addition, if Eve is a legal user and has stolen her TPW_e, it is still computational infeasible for Eve to retrieve x since $h(.)$ is a collision-resistant one-way hash function. That is, our proposed scheme can resist the stolen-verifier attack.

Claim 3. The proposed scheme can resist the server spoofing attack and registration center spoofing.

Proof: If Eve is a legal user, she cannot impersonate as any remote server S_j to cheat U_i, since she cannot construct the session key SK without the knowledge of PW_i, r. Even if Eve has stolen the TPW_i, she cannot obtain $h(r \oplus PW_i)$ as mentioned above. Thus, Eve cannot decrypt the transmitted messages from some legal user. After communicating with the masqueraded remote server, the legal user can detect immediately and terminates the session. Hence, our improved scheme can protect the user from being cheated by the masqueraded remote server.

Similarly, if Eve wishes to masquerade as the registration center to cheat the server, it is infeasible because each server S_j has a $V_j=h(SID_j, x)$. The server can use V_j and a nonce N_j to verify the registration center in Step V3 of the Authentication Phase.

Claim 4. The proposed scheme can resist the off-line password guessing attack.

Proof: Suppose an attacker Eve has the information of $\{h(r\oplus PW_i)\oplus rc, h(h(r \oplus PW_i))\oplus rs$ and $h(SK, rc)\}$. Eve first can guess a password PW_E to compute the corresponding $h(PW_E)$ and then finds ru = $ru\oplus h(r\oplus PW_i)\oplus h(PW_E)$ and $rs =rs\oplus h(r \oplus PW_i)\oplus h(PW_E)$. However, it is computationally infeasible, since Eve does not know ru, rs and SK. In addition, $h(.)$ is a collision-resistant one-way hash function. Hence, even if Eve has guessed the correct password, she cannot verify her guess by analyzing the scheme messages over the network. Obviously, off-line guessing attacks cannot be performed on our proposed scheme.

4. Conclusions

We have shown that our proposed scheme can withstand various attacks. As compared to the Lee et al.'s scheme, the proposed scheme inherits their merits, enhances their security. Therefore, the proposed scheme is well suited to the practical applications environment.

5. References

[1] W.S. Juang, Efficient password authenticated key agreement using smart cards, Computers and Security, vol. 23, pp. 167-173, 2004.

[2] W.S. Juang, Efficient multi-server password authenticated key agreement using smart cards, IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 251-255, 2004.

[3] L. Lamport, Password authentication with insecure communication, Communications of ACM, vol. 24, pp. 770-772, 1981.

[4] J.S. Lee, Y.F. Chang and C.C. Chang, A novel authentication protocol for multi-server architecture without smart cards, International Journal of Innovative Computing Information and Control, vol. 4, no. 6, pp. 1357-1364, 2008.

[5] I.C. Lin, M.S. Hwang and L.H. Li, A new remote user authentication scheme for multi-server architecture, Future Generation Computer Systems, vol. 19, pp. 13-22, 2003.

[6] W.J. Tsuar, An enhanced user authentication scheme for multi-server internet services, Applied Mathematics and Computation, vol. 170, pp. 258–266, 2005.