A few remarks on:

Security Analysis on a Group Key Transfer Protocol Based on Secret Sharing

M.Kim, N.Park, D.Won

The authors of [2] misunderstood some important aspects of our paper [3]. Please consider the following remarks:

- Paper [3] only aims to give a countermeasure for the particular attacks exposed against the original protocol. We do not claim that the improved version is secure - there is no formal security proof and therefore vulnerabilities may arise natural.
- The insider and outsider attacks against the improved version (Subsection 3.1, Methods 1 and 2; Subsection 3.2 Method 1) are limited by the success of a guessing attack against the hash function. We highlight that the attacks assume the guessing of a random number (not a password, which would have been feasible!). Hence, if the hash function is properly selected, the attacks are infeasible[1].
- The attacks mounted in Section 3.2, Method 2 and Section 3.3 are incorrect: the value α is chosen uniformly random for each session (see step 4 of the improved version) and therefore $\alpha_{(k_1)} \neq \alpha_{(k_2)}$.

References

[1] Mijin Kim, Namje Park, and Dongho Won. Cryptanalysis of an authenticated group key transfer protocol based on secret sharing. In *Grid and Pervasive Computing*, pages 761–766. Springer-Verlag, 2013.

[2] Mijin Kim, Namje Park, and Dongho Won. Security analysis on a group key transfer protocol based on secret sharing. In *MUSIC*, pages 483–488, 2013.

[3] Ruxandra F. Olimid. On the security of an authenticated group key transfer protocol based on secret sharing. In *Proceedings of the 2013 international conference on Information and Communication Technology*, ICT-EurAsia'13, pages 399–408, Berlin, Heidelberg, 2013. Springer-Verlag.

[1] The same remark applies to the attacks against the original protocol of Sun et al.'s that have been published in [1].