IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 27 September 2022, accepted 27 September 2022, date of current version 10 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3210727

COMMENTS AND CORRECTIONS

Corrections to "A Verifiably Secure ECC Based Authentication Scheme for Securing IoD Using FANET"

SAEED ULLAH JAN[1,2], IRSHAD AHMED ABBASI[3,5], (Member, IEEE), FAHAD ALGARNI[4], AND ADNAN SHAHID KHAN[5], (Senior Member, IEEE)

[1]Department of Computer Science, Government College Wari (Dir Upper), Khyber Pakhtunkhwa, Wari 18200, Pakistan
[2]Department of Computer Science & IT, University of Malakand, Chakdara 18800, Pakistan
[3]Department of Computer Science, Faculty of Science and Arts Belqarn, University of Bisha, Sabt Al-Alaya 61985, Saudi Arabia
[4]Faculty of Computing and Information Technology, University of Bisha, Bisha 67714, Saudi Arabia
[5]Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan 94300, Malaysia

Corresponding author: Irshad Ahmed Abbasi (aabasy@ub.edu.sa)

This work was supported in part by the University of Bisha and in part by the Research, Innovation and Enterprise Centre (RIEC), Universiti Malaysia Sarawak.

In the above article [1], the following corrections are necessary: Section II, preliminaries, subsection E Adversary Model – This model is based on [2], suppose the proposed protocol is denoted by $\prod$, entities involved are Mobile-Device (M), Drone (D), ground-control-station (GCS) and many instances are π means an ith instance of $\prod$. GCS has a confidential key s; suppose the drone has its identity ID_D, nonce, N_D, and public key R_D; mobile-device (M) has ID_M, nonce N_M, publicly known key R_M. Drone (D) stores (R_D, S_D, PK_D, SK_D), and Mobile-Device (M) stores (R_M, S_M, PK_M, SK_M) parameters in their memories. Adversary interacts with $\prod$ to represent themselves as a malicious drone with D, M, or GCS in the following manner.

Similarly, in [1], Section IV, subsection C, Authentication Phase, duplicate occurrence of **MODULE II(c)** must be removed. It should be kept once instead of two times in the paper.

REFERENCES

[1] S. U. Jan, I. A. Abbasi, F. Algarni, and A. S. Khan, "A verifiably secure ECC based authentication scheme for securing IoD using FANET," *IEEE Access*, vol. 10, pp. 95321–95343, 2022, doi: 10.1109/ACCESS.2022.3204271.

[2] Q. Do, B. Martini, and K.-K. R. Choo, "The role of the adversary model in applied security research," *Comput. Secur.*, vol. 81, pp. 156–181, Mar. 2019.