Wireless Personal Communications (2020) 112:463–466
https://doi.org/10.1007/s11277-020-07038-2

Comments on "A Multi-factor User Authentication and Key Agreement Protocol Based on Bilinear Pairing for the Internet of Things"

Salman Shamshad[1] · **Khalid Mahmood**[1] · **Saru Kumari**[2]

Published online: 20 January 2020

Abstract
The Internet of Things (IoT) introduces a novel model for the future internet that aims to offer communication between numerous interactive objects via heterogeneous networks. The concept of IoT is that everything within the global network is interconnected and accessible. Although, the increasing use of IoT offers a lot of benefits but it also entails different privacy and security encounters which needs to be considered. One of the major security concerns is authentication of the user, which means that if a user wants to access IoT node then the user and IoT node must authenticate each other. Therefore, to ensure the security of the IoT paradigm, a number of multi-factor user authentication schemes have been proposed by many researchers. Very recently, Nikravan-Reza (Wirel Pers Commun, 2019. https://doi.org/10.1007/s11277-019-06869-y) proposed multi-factor user authentication and key agreement protocol for IoT environments. In their scheme, firstly the gateway authenticates the legitimacy of the user and then the user is authenticated by IoT node. In this comments paper, we reviewed their scheme and noticed that their scheme fails to withstand user and IoT node impersonation attacks. Moreover, their scheme does not offer security features that they have claimed in their paper. Since their scheme is vulnerable to various considerable security attacks, so it is not suitable for practical implementation.

Keywords Authentication protocol · Protocol · Security protocol

✉ Khalid Mahmood
khalid.mahmood@cuisahiwal.edu.pk

Saru Kumari
saryusiirohi@gmail.com

[1] Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus, Sahiwal, Pakistan

[2] Chaudhary Charan Singh University, Meerut, Uttar Pradesh 250004, India

1 Problem Statement

This comment is about "A Multi-factor User Authentication and Key Agreement Protocol Based on Bilinear Pairing for the Internet of Things", presented by Nikravan-Reza [1]. In this section, we cryptanalyse their scheme and highlight that their scheme is vulnerable to user and node impersonation attacks. Furthermore, we worried about storage and computation burden on gateway node side because Nikravan-Reza stores some values in database of gateway node. Hence, it is necessary to reduce the computation overhead for efficient communication, which will result in reduction of storage cost. The common notations used in this paper are listed in Table 1.

1.1 User Impersonation

The GW stores $\{MID_u, Y_u, FQ_u, PQ_u\}$ in its database during user registration process. Since all these parameters are used in the generation of request message. Therefore, using these parameters an adversary $\mathcal{A}_{adv}$ can easily masquerade to a legitimate user via stolen verifier attack. In order to impersonate as a legitimate user the adversary performs these steps as follow:

Step 1 Assume that $\mathcal{A}_{adv}$ extracts the parameters $\{C_1, e_{gw}, r, x, params\}$ and $\{H_4(B_u), K_u\}$ from permanent and temporary memory of user's smart device. After revealing these parameters from memory and $\{MID_u, Y_u, FQ_u, PQ_u\}$ from database, the adversary can send a valid request message to *GW*.
Step 2 First of all the $\mathcal{A}_{adv}$ randomly selects $N_u^{\mathcal{A}_{adv}}$, $d^{\mathcal{A}_{adv}}$ and computes: $e_u^{\mathcal{A}_{adv}} = d^{\mathcal{A}_{adv}} P$, $g_u^{\mathcal{A}_{adv}} = d^{\mathcal{A}_{adv}} FQ_{GW}$, $CID_u''^{\mathcal{A}_{adv}} = MID_u^* \oplus H_4(e_u^{\mathcal{A}_{adv}} \| g_u^{\mathcal{A}_{adv}})$, $msg_1^{\mathcal{A}_{adv}} = T_0 \| N_u^{\mathcal{A}_{adv}} \| MID_u^* \| Y_u^* \| IDN_j$, $C_1^{\mathcal{A}_{adv}} = Signcrypt(msg_1^{\mathcal{A}_{adv}}, PQ_{GW}, FQ_{GW}, H_4(H_1(B_u^*)))$
Step 3 After the above calculation $\mathcal{A}_{adv}$ sends the request message $\{CID_u''^{\mathcal{A}_{adv}}, C_1^{\mathcal{A}_{adv}}, e_u^{\mathcal{A}_{adv}}\}$ to *GW*.
Step 4 Upon receiving request message $\{CID_u''^{\mathcal{A}_{adv}}, C_1^{\mathcal{A}_{adv}}, e_u^{\mathcal{A}_{adv}}\}$, the *GW* first calculates $g_u = \alpha_{GW}.e_u$, $l = H_4(e_u \| g_u)$, $MID_u'' = CID_u''^{\mathcal{A}_{adv}} \oplus l$. Then *GW* retrieves FQ_u using MID'' and calculates: $msg_1 \stackrel{?}{=} Unsigncrypt(C_1, PS_{GW}, FS_{GW}, FQ_u)$, $msg_1 = T_o \| N_u \| MID^* \| Y^* \| IDN_j$. If $MID_u^* \stackrel{?}{=} MID_u''$ holds true value, the *GW* sends $\{CID_{GW}'', C_2, TU_{GW}\}$ to the IoT *Node* via public channel.
Step 5 On receiving message $< CID_{GW}'', C_2, TU_{GW} >$ from *GW*, the Node performs some necessary calculations. Finally the *Node* sends message $< CIDN_j'', FQ_j, C_3 >$ to user.

Table 1 Common used notations

Notation	Elucidation
ID_u	Identity of the user
ID_{GW}	Identity of the gateway
IDN_j	Identity of IoT node
SK	Session key
$\mathcal{A}_{adv}$	The adversary

Step 6 Once the adversary receives $< CIDN_j'', FQ_j, C_3 >$ against $\{CID_u''^{\mathcal{A}_{adv}}, C_1^{\mathcal{A}_{adv}}, e_u^{\mathcal{A}_{adv}}\}$ from *Node*, it means that $\mathcal{A}_{adv}$ has successfully authenticated by *GW* and *Node*. Afterwards, the $\mathcal{A}_{adv}$ calculates $SK = H_4(N_u^{\mathcal{A}_{adv}} \| N_n \| l \| T_0 \| T_2)$ and shares with *Node*.
Step 7 Hence, the $\mathcal{A}_{adv}$ has successfully shared *SK* with the *Node* and impersonated on behalf of legitimate user.

1.2 Node Impersonation

The *GW* stores J, IDN_j, FQ_j, PQ_j in database during *Node* registration process. Moreover, the *Node* uses all these parameters in the generation of request message. Therefore, an $\mathcal{A}_{adv}$ can easily masquerade as a legal *Node*. In order to impersonate as a legal *Node* the $\mathcal{A}_{adv}$ has to follow these steps:

Step 1 Suppose an $\mathcal{A}_{adv}$ extracts parameters
$PS_j, PQ_j, FQ_j, FS_j, params$ stores in *Node*'s memory and puts them back into the *Node*. Later he embeds them in a malicious node so that he can send message on the behalf of legal *Node*.
Step 2 Upon receiving the message
CID_{GW}'', C_2, TU_{GW} from *GW*, $\mathcal{A}_{adv}$ firstly selects $N_n^{\mathcal{A}_{adv}}$ randomly and computes:
$msg_3^{\mathcal{A}_{adv}} = T_0 \| T_2 \| N_u \| N_n^{\mathcal{A}_{adv}} \| MID_u^* \| IDN_j$, $C_3^{\mathcal{A}_{adv}} = Signcrypt(msg_3^{\mathcal{A}_{adv}}, PQ_u, FQ_u, SN_j)$,
$CIDN_j'' = IDN_j \oplus l$.
Step 3 Afterwards, $\mathcal{A}_{adv}$ sends message $\{CID_j'', FQ_j, C_3^{\mathcal{A}_{adv}}\}$ to user.
Step 4 Upon receiving the message $\{CID_j'', FQ_j, C_3^{\mathcal{A}_{adv}}\}$, the user first calculates:
$msg_3 = Unsigncrypt(C_3^{\mathcal{A}_{adv}}, PS_u, FS_u, FQ_j)$, $msg_3 = T_0 \| T_2 \| N_u \| N_n^{\mathcal{A}_{adv}} \| MID_u^* \| IDN_j$,
$IDN_j'' = CIDN_j'' \oplus l$. Afterwards the user verifies $IDN_j \stackrel{?}{=} IDN_j''$. If it holds true value the user agrees on common shared session key with *Node*.
Step 5 Hence, the $\mathcal{A}_{adv}$ can successfully impersonate on the behalf of legitimate *Node* and established session by sharing *SK* with user. Therefore, this scheme is vulnerable to *Node* impersonation attack.

2 Conclusion

This comment is about "A Multi-factor User Authentication and Key Agreement Protocol Based on Bilinear Pairing for the Internet of Things", proposed by Nikravan-Reza [1]. In this comment, we have mentioned out attacks in Nikravan-Reza's protocol. It is illustrated that their protocol has susceptibilities including user impersonation and node impersonation attacks.

Reference

1. Nikravan, M., & Reza, A. (2019). A multi-factor user authentication and key agreement protocol based on bilinear pairing for the internet of things. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-019-06869-y.

Salman Shamshad is currently pursuing his M.S. degree in Computer Science from COMSATS university Islapagnmabad, Sahiwal campus, Pakistan. He received his BS in Computer Science degree with distinction, from Bahauddin Zakariya University, Sahiwal campus, Pakistan in 2018. His research interests include Lightweight Cryptography, Healthcare Authentication and Authenticated Key Agreement Scheme.

Khalid Mahmood is currently working at COMSATS University Islamabad, Sahiwal Campus. He received his M.S. degree in Computer Science from Riphah International University, Islamabad, Pakistan in 2010. He received a Ph.D. degree in Computer Science from International Islamic University, Islamabad, Pakistan in 2018. The title of his Ph.D. dissertation is Secure Authenticated Key Agreement Schemes for Smart Grid Communication in Power Sector. His research interests include Lightweight Cryptography, Smart Grid Authentication, Authenticated Key Agreement Schemes, Design and development of Lightweight authentication protocols using lightweight cryptographic solutions for diverse infrastructures or systems like vehicular ad hoc network, smart grid and Telecare medical information system (TMIS) etc.

Saru Kumari received the Ph.D. degree in mathematics from Chaudhary Charan Singh University, Meerut, India, in 2012, where she is currently an Assistant Professor with the Department of Mathematics. She has published more than 133 research papers in reputed international journals and conferences, including 115 publications in SCI-indexed journals. Her current research interests include information security and applied cryptography. She is a Technical Program Committee Member for many international conferences. She is on the Editorial Board of more than 12 journals of international repute including seven SCI journals. She served as the Lead/Guest Editor of four Special Issues in SCI journals of Elsevier, Springer, and Wiley.