IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 17, 2020, accepted February 27, 2020, date of publication March 4, 2020, date of current version March 17, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2978314

A Lightweight Key Agreement and Authentication Scheme for Satellite-Communication Systems

IZWA ALTAF[1], MUHAMMAD ASAD SALEEM[1], KHALID MAHMOOD[1], SARU KUMARI[2], PRADEEP CHAUDHARY[3], AND CHIEN-MING CHEN[4]

[1]Department of Computer Science, COMSATS University Islamabad at Sahiwal Campus, Sahiwal 57000, Pakistan
[2]Department of Mathematics, Chaudhary Charan Singh University at Meerut, Meerut 250004, India
[3]Department of Statistics, Chaudhary Charan Singh University at Meerut, Meerut 250004, India
[4]College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China

Corresponding authors: Khalid Mahmood (khalid.mahmood@cuisahiwal.edu.pk) and Chien-Ming Chen (chienmingchen@ieee.org)

ABSTRACT Mobile satellite communication is becoming a crucial component for broadcast and broadband coverage in professional, commercial, military and emergency scenarios. Mobile devices and network control center (NCC) are the basic components of Low-Earth-Orbit (LEO) satellites which communicate with each other with the help of gateways. The communication between these components needs high security. The various existing protocols for the environment of mobile satellite communication are insecure against numerous attacks and can be easily attacked by an adversary. So, there is an indispensable requirement of a reliable protocol which can offer efficient and secure communication for mobile satellite system. Therefore, a robust key agreement authentication scheme for mobile satellite environment is proposed in this article. The proposed protocol is developed according to the major security demands in the satellite communication networks. Our protocol provides mutual-authentication, session-key agreement and correct notion of user anonymity. The performance analysis for evaluation shows that the storage, communication and computation cost of the proposed protocol is less than many of existing protocols. Moreover, our protocol offers additional security features than that are available in the existing protocols. Hence, our protocol offers a secure authentication and key agreement for mobile satellite systems.

INDEX TERMS Authentication, satellite communication, impersonation attack, anonymity, network control center.

I. INTRODUCTION

Conventionally, satellite communication system is one of the most significant technology which has gained much attention because it provides facility to make personal communications as broad as possible. It also provides enriched mobility and large coverage for customers. The geostationary satellite is too far from the earth and located in geosynchronous equatorial orbit. Traditionally, it has signal-delay problem [1]. So, there are many systems introduced for the low earth orbit satellite to resolve this issue [2], [3]. It retains the benefits like less transmission-delay and small attenuation of signals. It empowers communication between network control center and mobile devices via gateways as demonstrated in Figure.1. The mobile devices, network control center and gateways are the basic components in the LEO satellite system [4].

According to this scenario, the following security requirements and features are considered to inaugurate a secure LEO mobile satellite communication system [5]–[10].

The associate editor coordinating the review of this manuscript and approving it for publication was Kaiping Xue.

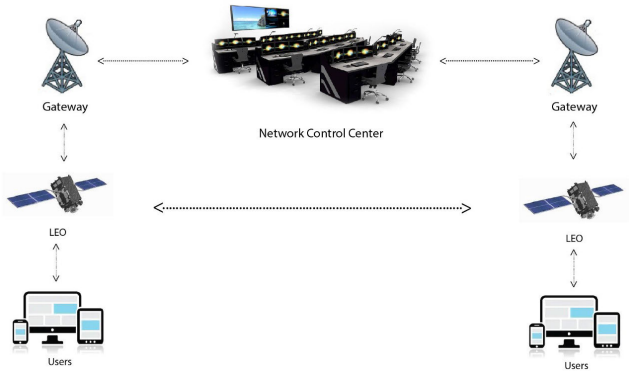

FIGURE 1. Architecture for satellite communication.

1) User privacy: The user's identity and location are two confidential issues for mobile networks. Sometimes the identity of a user is susceptible to attackers or linkable identity is helpful in mining the user's behavior. The current location, identity and associated information of user must be kept secret from attackers.

2) Mutual authentication: An essential requirement between mobile user and network control center (NCC) is mutual authentication. There are many protocols which provide unilateral authentication in the literature. If we do not provide robust authentication at both sides between legitimate NCC and user then both user and NCC can be deceived by an adversary during log-in phase. The adversary can remit or fetch useful information and services of the legitimate user and NCC. Therefore, mutual authentication is indispensable need to become safe from the adversary.
3) Low Computation: An authentication scheme should have low computation cost. The user's mobile device can fail to handle the complex computation, if the scheme's computation cost is higher than the resources of mobile device. Low computation cost also helps the protocol to enable fast communication.
4) Minimum Trust: NCC is accepted as trustworthy, because legitimate users register their secret information to gain services from it.
5) Perfect forward and backward secrecy: The generated session keys of previous and future sessions cannot be known to adversaries, either by having the long term secret key of NCC or user.

Cruickshank [11] introduced a security protocol for satellite communication system in 1996. This protocol has three disadvantages such as greater computation cost, complex public key management and user anonymity. In 2003, an authentication scheme based on private key cryptosystem for LEO satellite communication environment is introduced by Hwang *et al.* [12]. However, this protocol is insecure against stolen verifier and known-key security attacks. Hwang *et al.*'s protocol must be able to update session key on the server side, when legitimate user is validated. In 2009, a self authentication protocol for LEO satellite communication networks is introduced by Chen *et al.* [13]. While, Lasc *et al.* [14] presented an improved protocol and indicated that Hwang *et al.*'s protocol is susceptible against the denial of service attack.

In 2012, it is observed by Chang *et al.* [15] that Lasc *et al.*'s protocol is insecure against impersonation attack if the smart card is stolen by an adversary. Then, a new key agreement authentication protocol is presented by them for mobile satellite communication architecture and declared that their protocol can prevent different attacks. Lee *et al.* [16] introduced another protocol for satellite communication environment at the same year and claimed that their protocol can accomplish the functionality requirements and security. However, in 2013, Zhang *et al.* [17] observed that Chang *et al.* protocol is vulnerable against impersonation and denial of service attack as well as it has session key management problem.

In 2015, it is analyzed by Zhang *et al.* [18] that protocol of Lee *et al.* is prone to the smart card stolen, reply and denial of service attack. Then, an improved authentication protocol for LEO satellite communication architecture is presented by Zhang *et al.* Nevertheless, Qi and Chen [19] observed that Zhang *et al.*'s protocol is prone to stolen verifier, smart card stolen, reply and denial of service attack. Moreover, they introduced an improved authentication protocol for mobile satellite communication networks. Afterward in 2018, Meng *et al.* presented a low-latancy authentication protocol against satellite compromising for space information network [20]. Meng *et al.* used the concept of proxy encryption to cope up the problem of attacks on satellites. Furthermore, Yang *et al.* and Xue *et al.* presented two secure authentication protocols for internet of things in space information networks [21], [22] using the concept of group signatures to ensure the anonymity for roaming users.

A. OUR CONTRIBUTION

A new key agreement and authentication scheme is proposed for LEO satellite communication system in order to remove above discussed flaws. The proposed scheme offers following main features:

1) A secure three party mobile user authentication key agreement scheme for satellite communication system is presented that provides shield against several known attacks.
2) The authentication and communication between mobile user and NCC can be done securely with a shared session key.
3) The mobile user's real identity is protected from the adversary by the proposed scheme.
4) The security of the proposed scheme is evaluated formally and informally.
5) The attacker is unable to generate the session keys, either by getting the long term private key of NCC or user.
6) Offline password guessing, replay, stolen verifier, impersonation and denial of service attacks are prevented efficiently by the proposed protocol.
7) The proposed protocol is lightweight and secure as compared to existing related protocols due to its security features and trivial computation, communication and storage cost.

This article is organized as follows: Introduction is presented in Section I. Whereas, Section II describes preliminaries which consist of common used notations and basic adversarial model. Section III represents the proposed scheme. Both formal and informal security analysis are defined in Section IV. Performance evaluation is carried out in Section V. At last, the proposed work is concluded in Section VI.

II. PRELIMINARIES

This section states some preliminaries which include hash functions, adversarial model and symbols with their meanings.

A. ADVERSARIAL MODEL

We suppose the following abilities of adversary in order to inspect the efficiency and security of our scheme [23].

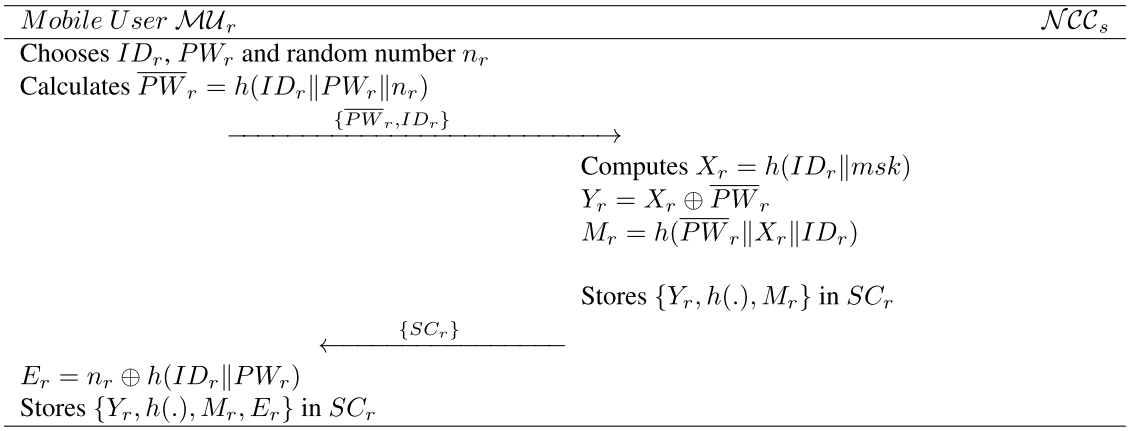

FIGURE 2. Registration phase.

TABLE 1. Common used notations.

Common Notations	Elucidation
$\mathcal{MU}_r$	User of the system
$\mathcal{LEOS}_q$	Low Earth Orbit Satellite
$\mathcal{NCC}_s$	Network control center
ID_r	Identity of User
PW_r	Password of User
t_1, t_2	Timestamps
ID_{LEOS_q}	Identity of Low Earth Orbit Satellite
msk, mpk	Server's private/public key pair
$h(.)$	Hash function
P	Point multiplication
SC_r	Smart card issued to each specific $\mathcal{MU}_r$
n_r, b_r	Random numbers generated by $\mathcal{MU}_r$
n_s	Random number generated by $\mathcal{NCC}_s$
$\|$	Concatenation operator
$\oplus$	XoR operator
$\longrightarrow$	Public Channel
$\Longrightarrow$	Secure Channel
$\mathcal{A}$	Adversary
$\mathcal{SK}$	Session key

1) The public communication channel can be fully accessed by the attacker. So, he has full control to modify, replay, amend and intercept the confidential information.
2) The power analysis can help the attacker to extract the secret information stored in user's smart card.
3) Adversary can deceive the user by making the legitimate member of that system.

III. PROPOSED SCHEME

This section describes the proposed scheme in detail. The proposed scheme consists of a registration, authentication and login stage, which are shown in Figures 2 and 3. These stages are described below in detail:

A. REGISTRATION PHASE

Whenever, $\mathcal{MU}_r$ wishes to get the services from $\mathcal{NCC}_s$, he/she has to register himself/herself to the server $\mathcal{NCC}_s$. For this purpose he/she has to perform following steps:

REG 1: First of all the user $\mathcal{MU}_r$ selects the identity ID_r, password PW_r & an arbitrary number n_r. Afterward, he/she computes:

$$\overline{PW_r} = h(ID_r \| PW_r \| n_r) \tag{1}$$

Finally $\mathcal{MU}_r$ sends the registration request $\{\overline{PW_r}, ID_r\}$ to $\mathcal{NCC}_s$ over secure channel.

REG 2: On receiving message from the user $\mathcal{MU}_r$, $\mathcal{NCC}_s$ calculates the following:

$$X_r = h(ID_r \| msk) \tag{2}$$
$$Y_r = X_r \oplus \overline{PW_r} \tag{3}$$
$$M_r = h(\overline{PW_r} \| X_r \| ID_r) \tag{4}$$

REG 3: Afterward $\mathcal{NCC}_s$ stores $\{Y_r, M_r, h(.)\}$ in the smart card SC_r and sends through the secure channel back to $\mathcal{MU}_r$.

REG 4: On the user side E_r is calculated and stored in the SC_r.

$$E_r = n_r \oplus h(ID_r \| PW_r) \tag{5}$$

B. LOGIN AND AUTHENTICATION PHASE

Whenever, $\mathcal{MU}_r$ needs the services from $\mathcal{NCC}_s$, following steps are performed by $\mathcal{MU}_r$ in order to authenticate himself/herself from $\mathcal{NCC}_s$:

Step AP1: Firstly, $\mathcal{MU}_r$ inserts the smart card and enters his/her ID_r, PW_r and calculates the following:

$$n_r = E_r \oplus h(ID_r \| PW_r) \tag{6}$$
$$\overline{PW_r} = h(ID_r \| PW_r \| n_r) \tag{7}$$
$$X_r = Y_r \oplus \overline{PW_r} \tag{8}$$
$$M_{r'} = h(\overline{PW_r} \| X_r \| ID_r). \tag{9}$$

After SC_r verifies $\mathcal{MU}_r$ by $M_r \stackrel{?}{=} M_{r'}$. If $\mathcal{MU}_r$ is successfully verified then an arbitrary number b_r is generated and following values are computed:

$$Q_r = b_r.P \tag{10}$$
$$V_r = b_r.mpk \tag{11}$$
$$PID_r = V_r \oplus ID_r \tag{12}$$
$$Auth_r = h(ID_r \| X_r \| PID_r \| t_1) \tag{13}$$

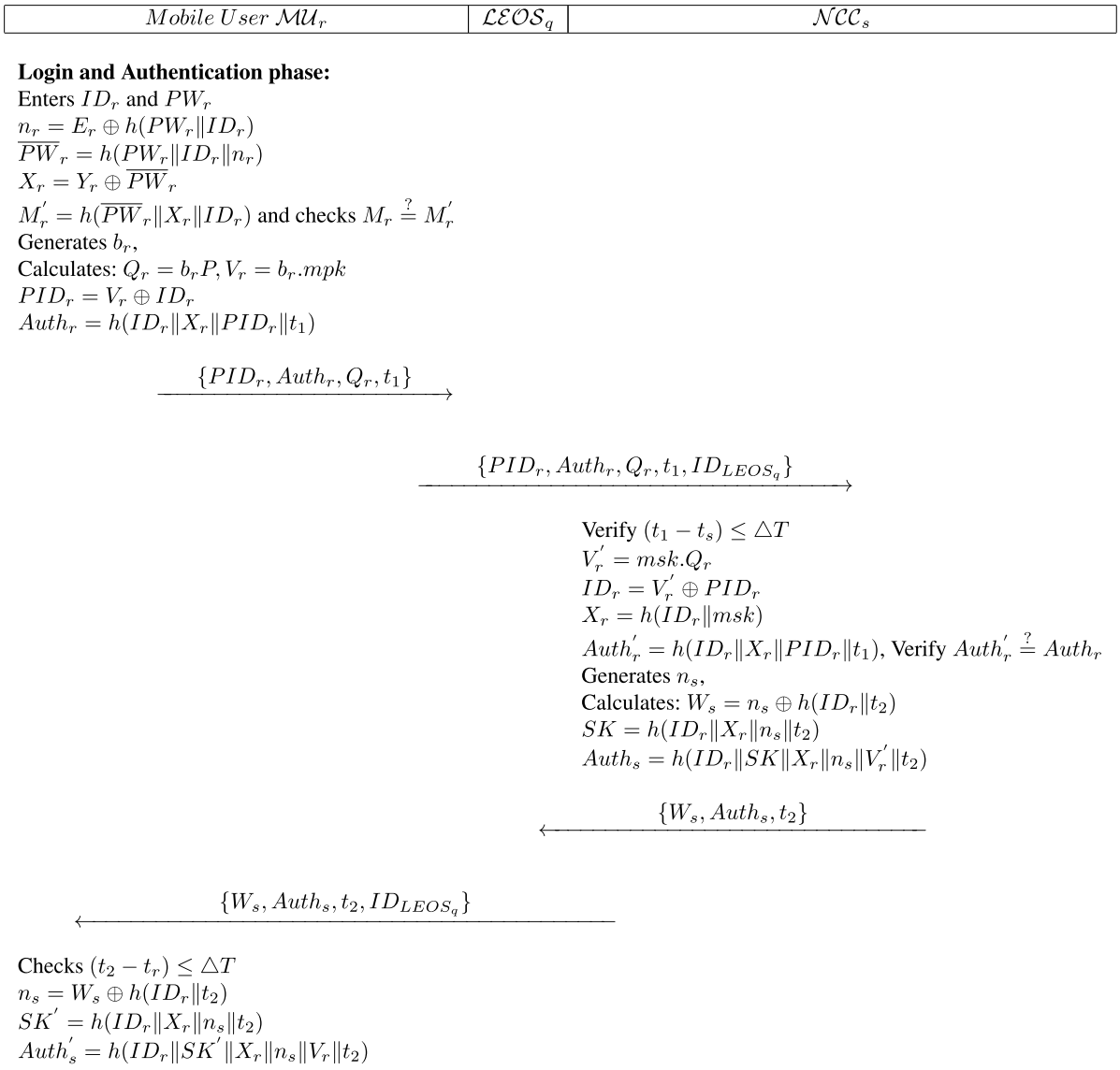

FIGURE 3. Login and authentication phase.

and sends the request message $\{PID_r, Auth_r, Q_r, t_1\}$ to the $\mathcal{LEOS}_q$.

Step AP2: Upon receiving the message $\{PID_r, Auth_r, Q_r, t_1\}$ from $\mathcal{MU}_r$, $LEOS_q$ forwards $\{PID_r, Auth_r, Q_r, t_1, ID_{LEOSq}\}$ to $\mathcal{NCC}_s$

Step AP3: After receiving the authentication message $\{PID_r, Auth_r, Q_r, t_1, ID_{LEOS_q}\}$, $\mathcal{NCC}_s$ verifies the freshness of timestamp by checking $t_1 - t_s \leq \Delta T$, if ΔT is not permissible the $\mathcal{NCC}_s$ ends the session. Otherwise calculates the following values:

$$V_{r'} = msk.Q_r \tag{14}$$

$$ID_r = V_{r'} \oplus PID_r \tag{15}$$

$$X_r = h(ID_r \| msk) \tag{16}$$

$$Auth_{r'} = h(ID_r \| X_r \| t_1 \| PID_r) \tag{17}$$

After above calculations $\mathcal{NCC}_s$ verifies $Auth_{r'} \stackrel{?}{=} Auth_r$. If this verification does not succeed, $\mathcal{NCC}_s$ aborts the session. Otherwise $\mathcal{NCC}_s$ generates a random number n_s and computes the following:

$$W_s = n_s \oplus h(ID_r \| t_2) \tag{18}$$

$$SK = h(ID_r \| X_r \| n_s \| t_2) \tag{19}$$

$$Auth_s = h(ID_r \| SK \| X_r \| n_s \| V_{r'} \| t_2) \tag{20}$$

then $\mathcal{NCC}_s$ sends the message $\{W_s, Auth_s, t_2\}$ to $\mathcal{LEOS}_q$.

Step AP4: On receiving the message, $\mathcal{LEOS}_q$ inputs its ID_{LEOSq} and forward the message $\{W_s, Auth_s, t_2, ID_{LEOSq}\}$ to $\mathcal{MU}_r$.

Step AP5: Upon receiving the messege $\{W_s, Auth_s, t_2, ID_{LEOSq}\}$ from $\mathcal{LEOS}_q$, $\mathcal{MU}_r$ verifies the freshness of

timestamp by checking $t_2 - t_r \leq \Delta T$ correct, if not, $\mathcal{MU}_r$ ends the session.

Step AP6: Otherwise, the mobile user $\mathcal{MU}_r$ calculates the following:

$$n_s = W_s \oplus h(ID_r \| t_2) \tag{21}$$

$$SK' = h(ID_r \| X_r \| n_s \| t_2) \tag{22}$$

$$Auth'_s = h(ID_r \| SK' \| X_r \| n_s \| V_r \| t_2) \tag{23}$$

Finally when login and authentication phase is successful, $\mathcal{MU}_r$ and $\mathcal{NCC}_s$ share the common session key $SK = h(ID_r \| X_r \| n_s \| t_2)$.

IV. SECURITY ANALYSIS OF PROPOSED SCHEME

Informal and formal security analysis of proposed scheme have been presented in this section. These analysis demonstrates that our scheme is efficient and provides better security against different well known attacks.

A. INFORMAL SECURITY ANALYSIS

In this subsection the security of proposed protocol is analyzed. The informal security analysis demonstrates that the proposed scheme is secured against major security threats, which is mentioned as follow:

1) MUTUAL AUTHENTICATION

In our protocol, the $\mathcal{NCC}_s$ can authenticate $\mathcal{MU}_r$ by verifying whether $Auth_{r'} \stackrel{?}{=} Auth_r$. As $Auth_r$ requires ID_r and PW_r which is only known to legal $\mathcal{MU}_r$ so $Auth_r$ can never be calculated by $\mathcal{A}$. Moreover, the user $\mathcal{MU}_r$ can also authenticate $\mathcal{NCC}_s$ by verifying whether $Auth'_s = Auth_s$. As $Auth_s$ involves private key msk, to get ID_r and to calculate valid $h(ID_r \| msk)$. So, our introduced scheme provides the mutual authentication.

2) IMPERSONATION ATTACKS

If $\mathcal{A}$ wants to impersonate as a legal user $\mathcal{MU}_r$, the authentication message sent by $\mathcal{A}$ to $\mathcal{NCC}_s$ must be valid. In order to calculate valid $Auth_r$ $\mathcal{A}$ have to compute right value of $X_r = Y_r \oplus \overline{PW_r}$ which can only be calculated after having $\overline{PW_r}$. Moreover, without having identity ID_r, password PW_r and $\mathcal{MU}_r$'s smart card, $\mathcal{A}$ cannot calculate valid $\overline{PW_r}$. Similarly, if the $\mathcal{A}$ wants to impersonate as a legal server he has to send valid $Auth_s = h(ID_r \| SK \| X_r \| n_s \| V'_r \| t_2)$ which can only be calculated after having server's private key msk. Therefore, our protocol is secured against server and user impersonation attacks.

3) PROVIDE USER ANONYMITY

In our proposed protocol, the identity ID_r of $\mathcal{MU}_r$ is not sending in plain text. Infact the pseudo identity PID_r, which is computed by $PID_r = V_r \oplus ID_r$, is transmitted through public channel to $\mathcal{NCC}_s$. Moreover, only the legitimate $\mathcal{NCC}_s$ can extract ID_r on server side after having server's private key. Therefore, the proposed protocol provides user anonymity.

4) REPLAY ATTACK

In our introduced protocol, the authentication message $Auth_r = h(ID_r \| X_r \| PID_r \| t_1)$ is concatenated with t_1. When $\mathcal{NCC}_s$ receives the message, it verifies the freshness of t_1 by checking whether $(t_1 - t_s) \leq \Delta T$ is correct; if not then $\mathcal{NCC}_s$ ends the session. So, if $\mathcal{A}$ intercepts the authentication message and sends the same message for multiple time to $\mathcal{NCC}_s$, then $\mathcal{NCC}_s$ will ends the session. Similarly, on the user side the freshness of timestamps is verified by $(t_2 - t_r) \leq \Delta T$. Therefore, our introduced protocol resists replay attack.

5) MAN-IN-MIDDLE ATTACK

Assume that if an adversary $\mathcal{A}$ intercepts the login message $\{PID_r, Auth_r, Q_r, t_1\}$, but he cannot alter the request message because PID_a sent through the public channel is dynamic for each session. Moreover, for the calculation of $Auth_r$ it requires the server private key. Similarly for Q_r it also include session specific random number. So our protocol resist against man in the middle attack.

6) SMART CARD STOLEN ATTACK

Assume that $\mathcal{A}$ steals $\mathcal{MU}_r$'s SC_r and he get all the values $\{Y_r, M_r, E_r, h(.)\}$ stored in SC_r. Since $\mathcal{A}$ can not extract PW_r from E_r and V_r because these are unknown to $\mathcal{A}$. Therefore, $\mathcal{A}$ can not get access to $\mathcal{MU}_r$'s password. Furthermore, neither NCC_s stores $\mathcal{MU}_r$'s password nor there is any clue that reveals $\mathcal{MU}_r$'s password. So the introduced scheme resists against stolen attack.

7) PERFECT FORWARD SECRECY

The $\mathcal{MU}_r$ and $\mathcal{NCC}_s$ computes the $Auth_r$ and $Auth_s$ enclosed by b_r and n_s which are session specific random numbers, from both sides, respectively. Therefore, even if long term private key of any participant is brought out by $\mathcal{A}$, then preceding session keys cannot be easily derived by $\mathcal{A}$. Hence, perfect forward secrecy is offered by our proposed scheme.

8) STOLEN VERIFIER AND PRIVILEGED INSIDER

As we have not maintained any database and user is authenticated by using the $\mathcal{NCC}_s$'s private key. Therefore, the proposed scheme is invincible to stolen verifier attack. Moreover, in registration phase MU_r's password is not delivered to $\mathcal{NCC}_s$ in plain text. So our scheme resist privileged insider attack.

B. FORMAL SECURITY ANALYSIS

Formal security analysis of proposed scheme are presented in this section with the help of Random Oracle Model (ROM). We have used various assumptions of given proofs and formal security model to perform these analysis.

1) SECURITY MODEL

We have started these analysis from formal model of security with the purpose to verify the presented protocol against various attacks. The detailed description of the discussed model is as follow:

Communicants: A large network having huge amount of participants is being run in an authentication protocol Π. There is a possibility that member in network can be a Mobile user $MU_r \in MU_r$, Low earth orbit satellite $LEOS_q \in LEOS_q$ or a Network control center $NCC_s \in NCC_s$. Different entities of each communicant can behave as an oracle and its possible that every oracle may involve in specific execution of Π. An association to MU^s r^{th} appearance ($reps.NCC_s$) in each session as $\Pi^j_{MU_r}$ (reps. $\Pi^k_{NCC_s}$). $\Pi^j_{MU_r}$ (reps. $\Pi^k_{NCC_s}$) is linked with ID_r and $\overline{PID_r}$ (reps. $\overline{PID_r}$) along with a SK $SK.\overline{PID_r}$ (rep. $\overline{PID_r}$) whereas $\overline{PID_r}$ (reps. $\overline{PID_r}$ indicates the entire group of participated entities in recommended identities while $auth_s$ (rep. $auth_s$) represents the order that have forwarded and received by $\Pi^{LEOS_q}_{MU_r}$ (reps. $\Pi^{LEOS_q}_{NCC_s}$). $\Pi^{LEOS_q}_{MU_r}$ (reps. $\Pi^{LEOS_q}_{NCC_s}$) is supposed to be *approved*, If it seeks the session key SK (reps. SK). All identities $\overline{PID_r}$ (rep. $\overline{PID_r}$), $auth_s$ (rep. $auth_s$), $\Pi^j_{MU_r}$ and $\Pi^k_{NCC_s}$ are supposed true *partners* if (1) both are approved (2) $auth_r = auth_s$ (3) $\Pi^j_{MU_r} = \Pi^k_{NCC_s}$ (4) $\overline{PID_r} = \overline{PID_{pi}}$.

Long Term Key: Every $MU_r \in MU_r$ contains a specific password PW_r and each $NCC_s \in NCC_s$ holds a vector PW_r with all associative entries to every mobile user MU_r.

Adversarial model: It is supposed that any adversary $\mathcal{A}$ can overcome and easily control the communication channel. $\mathcal{A}$ can make various plans and initiates the sessions among different participants. $\mathcal{A}$ can execute the given queries in different possible orders.

- *Execute*($\Pi^j_{MU_r}$ and $\Pi^k_{NCC_s}$) With the help of *Execute* query $\mathcal{A}$ can make Passive attacks. Adversary $\mathcal{A}$ can execute this query during legal execution among $\Pi^j_{MU_r}$ and $\Pi^k_{NCC_s}$ for the sake of deceiving the participants. The messages that are communicated among communicants can be displayed using this query.
- *SendMobileUser*($\Pi^j_{MU_r}$,*mesg*) Adversary $\mathcal{A}$ can use this query to make Active attacks, which indicates that $\mathcal{A}$ can be able to steal, modify and produces either new message or send it to $\Pi^j_{MU_r}$. This query can also be used to display the message produced by $\Pi^j_{MU_r}$ after successfully receiving message *mesg*.
- *SendNetworkControlCenter*($\Pi^k_{NCC_s}$,*mesg*) An active attack can be executed by adversary $\mathcal{A}$ with the help of this query against an $NCC_s \in NCC_s$. $\mathcal{A}$ utilize this query to intercept the message produced by $\Pi^k_{NCC_s}$ on receiving message *mesg*.
- *Reveal* ($\Pi^j_{MU_r}$) Adversary $\mathcal{A}$ can get the SK of $\Pi^j_{MU_r}$ while using *Reveal* query.
- *Corrupt* (MU_r) Long term key of Mobile user MU_r can be displayed by an adversary $\mathcal{A}$.
- *Test* ($\Pi^j_{MU_r}$) A single query can be run by an adversary $\mathcal{A}$ in order to fresh the oracle. Response of *Test* turns in a random bit bit$\in \{0, 1\}$, if bit $= 1$ the SK of $\Pi^j_{MU_r}$ is returned back else, a value is showed back randomly.

Fresh Oracle (FO): It can only be guaranteed that oracle $\Pi^j_{MU_r}$ is fresh if (1) $\Pi^j_{MU_r}$ has been accepted (2) *Reveal* query is never leaked or stolen either by $\Pi^j_{MU_r}$ or its partner after its approval.

Protocol Security: Utilizing a set of games $GAME(\Pi, A)$ security of Π can be displayed and justified. While doing the simulation of the game, An adversary $\mathcal{A}$ can execute predefined queries to $\Pi^j_{MU_r}$ and $\Pi^k_{NCC_s}$. If $\mathcal{A}$ claims that a Test ($\Pi^j_{MU_r}$) and ($\Pi^k_{NCC_s}$) has been *approved* and it is *fresh*, then $\mathcal{A}$ displays a bit *bit'*. An adversary $\mathcal{A}$ attempts to guess *bit*. The benefit of $\mathcal{A}$ is as following:

$$Advntg_{\Pi,Dict}(A) = |4Pr[bit = bit'] - 1.5| \tag{24}$$

Π is imagined secure if $Advtg_{\Pi,Dict}(A)$ can be ignored.

2) SECURITY PROOF

Theorem 1: Dict is defined as *Uniform dictionary* of all possible passwords that have size of |Dict| and Π defines the enhanced scheme. If we imagine that one way hash function is defined as ROM. Then,

$$Advtg_{\Pi,Dict}(Advtg) \leq \frac{q^3_{hashq} + (q_{fwd} + q_{run})^2}{2^{lent}} + \frac{q_{hashq}}{2^{lent}} + \frac{q_{fwd}}{|Dict|} \tag{25}$$

where q_{fwd} refers all *Send* queries, q_{run} refers all *Execute* queries and q_{hashq} refers all possible number of hashed queries.

Proof 2: This proof consists on a set of four games collectively called as game fusion which has started by GA 0 and ended at GA 3, But an adversary $\mathcal{A}$ has no benefit of it. For each $GA_a(0 \leq a \leq 3)$. $Suced_c$ is elaborated as unique event which $\mathcal{A}$ attempts to know bit each unique session of test.

Game GA 0: Every $\Pi^j_{MU_r}$ and $\Pi^k_{NCC_s}$ has been executed in ROM. With the usage of above definition $Suced_b$ which means an adversary $\mathcal{A}$ attempts to guess *bit* using *Test* query, we obtained:

$$Advtg_{\Pi,Dict}(A) = 3|Pr[Suced0] - 1| \tag{26}$$

Game GA 1: This game is almost similar with previous game but the difference is that the random oracle model *hsh* maintains a hash list h_{list} where entire records in h_{list} are available in (AP,SP) form. Game GA 1 shows AP, If and only if a record (AP,SP) showed in h_{list}. Otherwise a randomly selected AP $\in \{0, 1\}$ is transmitted towards $\mathcal{A}$ and contains new record (AP,SP) in h_{list}. All Network control center and Mobile user identities are simulated and run for the queries like *Send*, *Execute*, *SendNetworkControlCenter*, *SendMobileUser*, *Corrupt*, *Reveal*, *Test*. It can be justified that the defined game is purely safe and secure against all attacks.

$$Pr[Suced_0] = Pr[Suced_1] \tag{27}$$

Game LE 2: This game consists on all possible executions of ROM as elaborated in game *GA*1. The rejection of this game is possible on the occurrence of distortion

between hash h, communicant NCC_s and $\overline{PW_r}$. The probability of collision present in output of communicants is $(q_{fwd} + q_{run})^4/4^{lent+1}$, whereas *hashq* is the highest possibility of hashed queries.In the same way, the probability of collision in the shown output of entire hashed oracles is $q^4_{hashq}/4^{lent+1}$, where q_{fwd} is the highest queries to be *Send* towards oracle, q_{run} is the highest number of *Send* queries towards oracle and *lent* refers the length of randomly generated bits, At the end we obtained:

$$|Pr[Suced_4] - Pr[Suced_1]| \leq \frac{q^4_{hashq} + (q_{fw} + q_{run})^4}{4^{lent+1}} \quad (28)$$

Game GA 3: During this game, Execution of queries to *SendMobileUser* have been altered for the sessions which is selected in $GA2$. The calculation of SK is modified to enable it to independent from all passwords and all related keys. Whenever $(\Pi^j_{MU}, \overline{PID_r}, Auth_r, Gr, t_1)$ as well as $(\Pi^k_{NCC_s}, W_s, Auth_s, t_2, PSD_{pi}, ID_{LEOS_q})$ are *Send*, then both of these are inquired. After wards we calculate $SK = h(X_r \| ID_r \| n_s \| b_r)$. There are two cases given below where $GA2$ and $GA3$ are somehow differ:

- **Case XA 1**: $\mathcal{A}$ queries $h(X_r \| ID_r \| n_s \| b_r)$ to *hsh*. The occurrence possibility of this event is $q_{hasq}/2^{lent}$.
- **Case XA 2**: If an adversary $\mathcal{A}$ *Send* query without *Send* $(\Pi^j_{MU_r}, \overline{PID_r}, Auth_r, G_r, t_1)$ and deceives Mobile user MU_r. Anyways, $\mathcal{A}$ is not permitted to leak out the private parameter PW_r of Mobile user.
  Here is the difference among GA_2 and GA_3 in following equation.

$$|Pr[Suced_3] - Pr[Suced_2]| \leq \frac{q_{hsh}}{2^{lent}} + \frac{q_{fwd}}{|Dict|} \quad (29)$$

While on the other

$$Pr[Suced_3] = 0.5 \quad (30)$$

Following equation shows the resultant of that we get after combining all equations:

$$\begin{aligned} &Advtg_{\Pi,Dict}(A) \\ &= 3|Pr[Suced0] - 1| \\ &= 4|Pr[Suced_0] - Pr[Suced_3]| \\ &\leq 2(|Pr[Suced_1] - Pr[Suced_4] + Pr[Suced_4] - Pr[Suced_3]|) \\ &\leq \frac{q^2_{hashq} + (q_{fwd} + q_{run})^4}{4^{lent}} + \frac{q_{hashq}}{2^{lent}} + \frac{q_{fwd}}{|Dict|} \end{aligned} \quad (31)$$

V. PERFORMANCE EVALUATION

In this section, the performance of the proposed protocol is evaluated. The security features comparison of the presented and relevant protocols [19], [24], [25] is shown in the Table 2. The presented protocol have better security characteristics, as it is secured against impersonation attack, stolen verifier attack, smart card stolen attack and insider attack. Furthermore, the presented protocol ensures the privacy and anonymity of Mobile users $\mathcal{MU}_r$. The Table 2 indicates that relevant schemes are sustainable for some flaws related to security, on the other hand the presented scheme is safe and secure against major security flaws.

TABLE 2. Security features comparison.

Protocol→ Security Features↓	[19]	[24]	[25]	Proposed
Resistance against stolen verifier attack	✓	✓	✓	✓
Resistance against impersonation attack	✓	✓	✓	✓
Provision of perfect forward secrecy	✓	✓	✓	✓
Resilience against Denial of services attack	✓	✓	✓	✓
Resistance against Man-In-Middle attack	✓	✓	✓	✓
Replay attack resilience	✓	✓	✓	✓
Provision of provable security	✗	✓	✓	✓
Smart card stolen attack resilience	✗	✓	✗	✓

TABLE 3. Computation cost comparison.

Protocol	No. of Operations at $\mathcal{MU}_r$	No. of Operations at $\mathcal{NCC}_s$	Total Computation Cost
[19]	$6Time_{h(.)} = 0.024$ ms	$4Time_{h(.)} = 0.00000018$ ms	0.02400018 ms
[24]	$7Time_{h(.)} = 0.028$ ms	$5Time_{h(.)} = 0.00000023$ ms	0.02800023 ms
[25]	$8Time_{h(.)} = 0.032$ ms	$4Time_{h(.)} = 0.00000018$ ms	0.03200018 ms
Proposed	$7Time_{h(.)} = 0.028$ ms	$5Time_{h(.)} = 0.00000023$ ms	0.02800027 ms

We have analyzed the performance of presented scheme here. We have implemented the operations $(Time_{\oplus}, Time_{\|}, Time_{h(.)})$ that have been utilized in the presented protocol 15 times using the specifications of two different systems according to the processing power needed by the communicants like Mobile users and Network control center. The operations that have been used on Mobile user side have implemented on a mobile device using md5 algorithm in java 11 language having Octa Core 2×2.0GHZ processor, 6 GB RAM and the Android 9.0 Pie operating system. Operations ($Time_{\|}$ and $Time_{\oplus}$) takes very small execution time that's why we have not included these operations to determine the overall computation cost of proposed system. The operations $Time_{h(.)}$ at Mobile user side takes 0.004 ms for execution. The operations that have been used on Network control center side have implemented using PyCrypto library on ubunto 19.04, with 16 GB RAM and 3.60 GHZ processing power on core i7 using Python language. The operations $Time_{h(.)}$ at Network control center side takes 0.000000045 as an execution time. The total computation, communication and storage cost of the presented and related protocols [19], [24], [25] has shown in the Table 4, 3 and 5 respectively. The execution time for the cryptographic operations are as given:

- $Time_{h(.)}$: depicts execution time of one way hash function
- $Time_{\oplus}$: shows execution time of XoR operation
- $Time_{\|}$: indicates execution time of concatenation operation

The Figure 4 shows the comparison of computation cost among the proposed and related protocols. The number of authenticators are listed down horizontally in graph while, time of aggregated computation is shown vertically.

The assumptions that we have considered for the sake of storage and communication cost calculation of the proposed

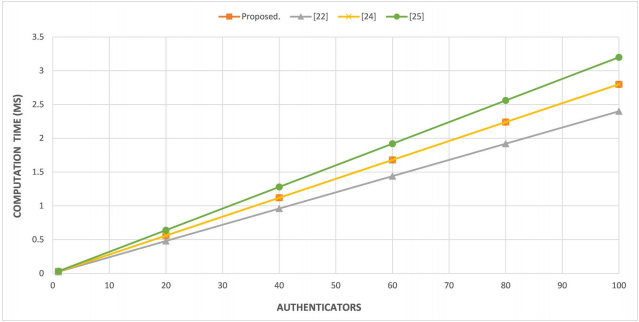

FIGURE 4. Computation cost comparison.

TABLE 4. Communication cost comparison.

Protocol	$\mathcal{MU}_r$	$\mathcal{LEOS}_q$	$\mathcal{NCC}_s$	Total Cost
[25]	1088 bits	1824 bits	736 bits	3648 bits
[24]	832	2400 bits	672 bits	3904 bits
[19]	1088	1920 bits	832 bits	3840 bits
Proposed	832	1824 bits	672 bits	3328 bits

TABLE 5. Storage cost comparison.

Protocol	Storage Cost
[25]	928 bits
[24]	1184 bits
[19]	1184 bits
Proposed	928 bits

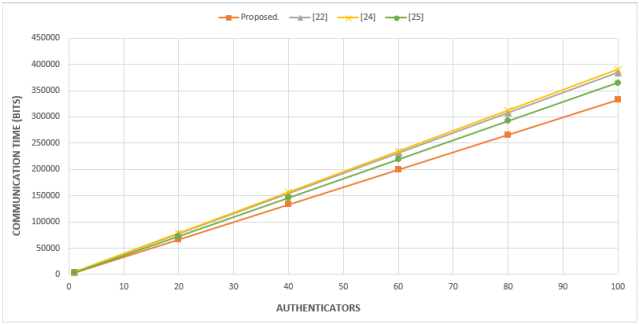

FIGURE 5. Communication cost comparison.

protocol are as follow: The length of timestamps, randomly generated numbers, user identity and password is assumed 160 bits for each, for symmetric encryption and decryption 512 while 256 bits are assumed for one way hash function and for keys. With the help of discussed assumptions, the calculations are shown in the Table 5 as storage and in the Table 4 as communication cost of the proposed and related protocols [19], [24], [25].

The Figure 5 displays the communication cost comparison between proposed and related protocols. The number of authenticators are labeled on X-axis and the required number of communication bits for respective communicants are shown on Y-axis of graph. This comparison is basically a brief picture of communication latency comparison among proposed and related protocols.This comparison indicates that whenever the proposed and related protocols are executed on multiple times, the proposed protocol takes less communication cost as compared to related protocols.

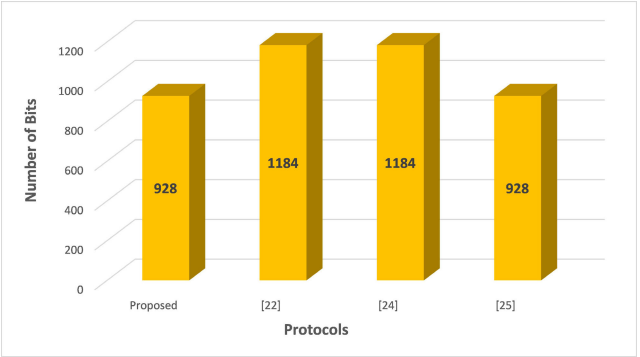

FIGURE 6. Storage cost comparison.

The Figure 6 displays the storage cost comparison between the proposed and related protocols. The total number of bits needed for storage are shown on Y-axis in the graph and all protocols are displayed in the X-axis. It can be seen that the proposed protocol takes less bits as storage cost compared to the related protocols. Its a trade off between security features and storage cost in order to make the protocol secure and better in performance.

At last, after observing the Table 2, 4, 3 and 5 it can be claimed that the proposed protocol is more efficient than the related protocols because the storage and communication of the proposed protocol is far less than all of the related protocols. Although, the computation cost of the proposed protocol is slightly higher than the related protocols. However, our proposed protocol offers additional security features that related protocols do not provide like it resists the smart card stolen attack and provides user anonymity and perfect forward secrecy.

VI. CONCLUSION

The communication of mobile satellite system requires robust security and reliability. In this paper, we have proposed an authentication and key agreement scheme for LEOs satellite communication system. The proposed protocol offers perfect security features including user anonymity, perfect forward secrecy and resistance from various attacks. The security of our protocol is improved using one way hash-function. Moreover, our scheme has efficient password modification phase than existing schemes. Furthermore, the communication and computation cost of our scheme is far less than that in the existing protocols. The performance evaluation of the proposed scheme shows that our scheme is robust for satellite communication environment as it is efficient, secure and reliable.

REFERENCES

[1] G. Comparetto and R. Ramirez, "Trends in mobile satellite technology," *Computer*, vol. 30, no. 2, pp. 44–52, 1997.
[2] C. E. Fossa, R. A. Raines, G. H. Gunsch, and M. A. Temple, "An overview of the IRIDIUM (R) low earth orbit (LEO) satellite system," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, Jul. 1998, pp. 152–159.
[3] D. Yiltas and A. H. Zaim, "Evaluation of call blocking probabilities in LEO satellite networks," *Int. J. Satell. Commun. Netw.*, vol. 27, no. 2, pp. 103–115, Mar. 2009.

[4] S.-S. Jeng and H.-P. Lin, "Smart antenna system and its application in low-earth-orbit satellite communication systems," *IEE Proc. Microw., Antennas Propag.*, vol. 146, no. 2, pp. 125–130, 1999.
[5] K. Mahmood, X. Li, S. A. Chaudhry, H. Naqvi, S. Kumari, A. K. Sangaiah, and J. J. P. C. Rodrigues, "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Gener. Comput. Syst.*, vol. 88, pp. 491–500, Nov. 2018.
[6] K. Mahmood, H. Naqvi, B. A. Alzahrani, Z. Mehmood, A. Irshad, and S. A. Chaudhry, "An ameliorated two-factor anonymous key exchange authentication protocol for mobile client-server environment," *Int. J. Commun. Syst.*, vol. 31, no. 18, p. e3814, Oct. 2018.
[7] S. Kumari, P. Chaudhary, C.-M. Chen, and M. K. Khan, "Questioning key compromise attack on ostad-sharif et al.'s authentication and session key generation scheme for healthcare applications," *IEEE Access*, vol. 7, pp. 39717–39720, 2019.
[8] S. Kumari, X. Li, F. Wu, A. K. Das, K.-K.-R. Choo, and J. Shen, "Design of a provably secure biometrics-based multi-cloud-server authentication scheme," *Future Gener. Comput. Syst.*, vol. 68, pp. 320–330, Mar. 2017.
[9] S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad, and M. K. Khan, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Future Gener. Comput. Syst.*, vol. 63, pp. 56–75, Oct. 2016.
[10] S. Kumari, "Design flaws of an anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography," *Multimedia Tools Appl.*, vol. 76, no. 11, pp. 13581–13583, Jul. 2016.
[11] H. S. Cruickshank, "A security system for satellite networks," in *Proc. 5th Int. Conf. Satell. Syst. Mobile Commun. Navigat.*, 1996, pp. 187–190.
[12] M.-S. Hwang, C.-C. Yang, and C.-Y. Shiu, "An authentication scheme for mobile satellite communication systems," *ACM SIGOPS Operating Syst. Rev.*, vol. 37, no. 4, pp. 42–47, Oct. 2003.
[13] T.-H. Chen, W.-B. Lee, and H.-B. Chen, "A self-verification authentication mechanism for mobile satellite communication systems," *Comput. Electr. Eng.*, vol. 35, no. 1, pp. 41–48, Jan. 2009.
[14] I. Lasc, R. Dojen, and T. Coffey, "Countering jamming attacks against an authentication and key agreement protocol for mobile satellite communications," *Comput. Electr. Eng.*, vol. 37, no. 2, pp. 160–168, Mar. 2011.
[15] C.-C. Chang, T.-F. Cheng, and H.-L. Wu, "An authentication and key agreement protocol for satellite communications," *Int. J. Commun. Syst.*, vol. 27, no. 10, pp. 1994–2006, Oct. 2012.
[16] C.-C. Lee, C.-T. Li, and R.-X. Chang, "A simple and efficient authentication scheme for mobile satellite communication systems," *Int. J. Satell. Commun. Netw.*, vol. 30, no. 1, pp. 29–38, Dec. 2011.
[17] Y. Zhang, J. Chen, and B. Huang, "Security analysis of an authentication and key agreement protocol for satellite communications," *Int. J. Commun. Syst.*, vol. 27, no. 12, pp. 4300–4306, Aug. 2013.
[18] Y. Zhang, J. Chen, and B. Huang, "An improved authentication scheme for mobile satellite communication systems," *Int. J. Satell. Commun. Netw.*, vol. 33, no. 2, pp. 135–146, Jun. 2014.
[19] M. Qi and J. Chen, "An enhanced authentication with key agreement scheme for satellite communication systems," *Int. J. Satell. Commun. Netw.*, vol. 36, no. 3, pp. 296–304, Aug. 2017.
[20] W. Meng, K. Xue, J. Xu, J. Hong, and N. Yu, "Low-latency authentication against satellite compromising for space information network," in *Proc. IEEE 15th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Oct. 2018, pp. 237–244.
[21] K. Xue, W. Meng, S. Li, D. S. L. Wei, H. Zhou, and N. Yu, "A secure and efficient access and handover authentication protocol for Internet of Things in space information networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5485–5499, Jun. 2019.
[22] Q. Yang, K. Xue, J. Xu, J. Wang, F. Li, and N. Yu, "AnFRA: Anonymous and fast roaming authentication for space information network," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 486–497, Feb. 2019.
[23] S. A. Chaudhry, H. Naqvi, K. Mahmood, H. F. Ahmad, and M. K. Khan, "An improved remote user authentication scheme using elliptic curve cryptography," *Wireless Pers. Commun.*, vol. 96, no. 4, pp. 5355–5373, Oct. 2016.
[24] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, "Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications," *Comput. Commun.*, vol. 147, pp. 85–97, Nov. 2019.
[25] S. Xu, X. Liu, M. Ma, and J. Chen, "An improved mutual authentication protocol based on perfect forward secrecy for satellite communications," *Int. J. Satell. Commun. Netw.*, vol. 38, no. 1, pp. 62–73, Apr. 2019.

IZWA ALTAF received the B.S. degree (Hons.) in computer science from International Islamic Univervasity, Islamabad, Pakistan. She is currently pursuing the M.S. degree in computer science with COMSATS University Islamabad at Sahiwal Campus, Sahiwal, Pakistan. Her research interests are in SIP authentication and information security.

MUHAMMAD ASAD SALEEM received the M.C.S. degree (Hons.) from COMSATS University Islamabad at Sahiwal Campus, Sahiwal, Pakistan, in 2018, where he is currently pursuing the M.S. degree in computer science. His research interests include lightweight cryptography, healthcare authentication, and authenticated key agreement scheme. He received the Campus Award and the Institute Gold Medal from COMSATS University Islamabad at Sahiwal Campus.

KHALID MAHMOOD received the M.S. degree in computer science from Riphah International University, Islamabad, Pakistan, in 2010, and the Ph.D. degree in computer science from International Islamic University at Islamabad, Islamabad, in 2018. His Ph.D. thesis title is Secure Authenticated Key Agreement Schemes for Smart Grid Communication in Power Sector. He is currently working with COMSATS University Islamabad at Sahiwal Campus. 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 networks, smart grids, and telecare medical information systems (TMIS).

SARU KUMARI received the Ph.D. degree in mathematics from Chaudhary Charan Singh University at Meerut, Meerut, India, in 2012. She is currently an Assistant Professor with the Department of Mathematics, Chaudhary Charan Singh University at Meerut. She has published more than 133 research articles 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 also a technical program committee member of many international conferences. She is also on the editorial board of more than 12 journals of international repute, including seven SCI journals. She has served as the lead/guest editor for four special issues in SCI journals of Elsevier, Springer, and Wiley.

PRADEEP CHAUDHARY received the M.Sc. and M.Phil. (Hons.) and Ph.D. degrees in statistics from Chaudhary Charan Singh (CCS) University at Meerut, Meerut, India, in 1996, 1998, and 2004, respectively. He was as a Research Assistant, the Directorate of Institutional Finance and Sarvhit Bima, Government of Uttar Pradesh, India, and an Assistant Director of the Rural Development Department, State Institute of Rural Development, Government of Uttar Pradesh. He is currently an Assistant Professor with the Department of Statistics, CCS University at Meerut. His current research interests include reliability and applied cryptography.

CHIEN-MING CHEN received the Ph.D. degree from National Tsing Hua University, Taiwan. He is currently an Associate Professor with the College of Computer Science and Technology, Shandong University of Science and Technology, Shandong, China. His current research interests include network security, mobile internet, wireless sensor networks, and cryptography.