A New Key Management Protocol for Remote Sensing Satellite With Multi Ground Stations

Hany Habbak
Electronics and communication Department
AAST
Cairo, Egypt
hanyelshall@gmail.com

Nabil Hamdy
Electronics and communication Department
MIU
Cairo, Egypt
nabil.hamdy@miuegypt.edu.eg

Khaled Shehata
Head of Electronics and communication Department
AAST
Cairo, Egypt
k_shehata@aast.edu

Abstract—**The key management in remote sensing satellites is the most critical and important part in the security scheme in general and especially in case of multi ground stations. These ground stations may be under official contract to receive the data from the satellite for particular period of time. The problem with the schemes is if any ground station leaks the key information to the other ground station whose official contract is expired the encryption schemes fails. Further if the satellite service provider leaks the key information to the intruder, the symmetric key schemes fails. This paper solves the key management problem of encryption scheme in remote sensing satellite. The solution is a new key management protocol uses both traditional security verification methods and new orbital parameter verification method.**

Keywords-key mangement; OPAM; remot sensing satellite; multi ground stations;

I. INTRODUCTION

A start to the study is carried by reviewing the available key managements used in space over the last few years. It was started by Tanya Vladimirova et al [1], 2004, where they mentioned that to secure the communication between SC and GS (uplink/downlink) all security services like authentication, integrity and encryption should be used for complete protection of the satellite communication links. Michael P. Howarth.et al and M. Gokcen Arslan.et al [2,3],2004,2006, they proposed two different solutions to enhance multicast key management for satellite communication on a predefined communication scenario; The proposed solutions are based on distributed logical key hierarchy (LKH) and logical key hierarchy Group Diffie-Hellman (LKH-GDH) mechanisms. A.Koltuksuz [4], 2007, he proposed the possibility to conceive a space based key management center. Chayan Dutta.et al [5], 2008, they provide a solution to the key management problem of private key encryption in remote sensing satellite; the solution is a new encryption scheme that uses combination of both private key and public key encryption schemes. YaHui Li. et al [6], 2011, proposed solution achieved the dynamic multi-level security group key management solution by using the public key technology based on the identity and the security group communication mechanism in security domain. Ahmad Kassem. et al [7,8], 2011, 2012, they firstly proposed an Enhanced Unidirectional Lightweight Encapsulation (EULE) derived from ULE method. Secondly, for solving the frequently rekeying problem, a new key management scheme of two independent LKH key distributions layered architecture: a satellite-layer and a terrestrial layer. In this paper the study deals with solving the key management problem of encryption scheme in remote sensing satellite; the reached approach is a new key management protocol that uses both traditional security verification methods and new orbital parameter verification method, which is named in this paper as Orbital Parameter Authentication Method (OPAM).

Symmetric key encryption scheme in remote sensing satellite are used to secure Payload data, telemetry data (downlink) and encrypt commands (uplink) [5]. The reason for using symmetric key encryption rather than asymmetric key scheme for encrypting uplink and downlink data that symmetric key encryption is faster than public key encryption schemes [9]. Especially that the payload data and the telemetry data are huge. The problem with symmetric key encryption for remote Sensing satellite is the key management. Asymmetric key cryptography solves the key management problem of the symmetric cryptosystems.

This protocol combines authentication with key exchange to solve a general remote sensing satellite problem. For key exchange, this paper will address a new protocol that combines an arbitrator protocol and a self-enforcing protocol. An arbitrator is a disinterested third

978-1-4673-4810-2/12/$31.00 ©2012 IEEE

party trusted to complete a protocol. A self-enforcing protocol is the best type of protocol, the protocol itself guarantees fairness. No arbitrator is required to complete the protocol. For the authentication in this protocol we use the traditional authentication and a new authentication method called (OPAM).

II. KEY MANAGEMENT PROBLEM

Figure 1.shows a remote sensing satellite and its receiving ground stations. Usually remote sensing satellite uses low earth orbit for orbiting. The receiving ground stations are equipped with systems to receive the satellite payload data, telemetry data (downlink) and transmit commands (uplink). G_A, G_B, G_C … G_n are the ground stations.

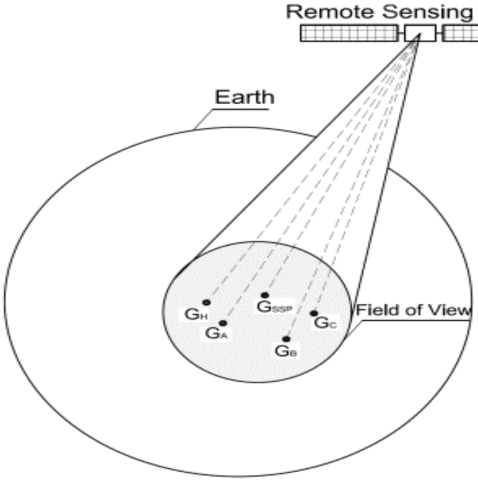

Figure 1. Remote sensing satellite and its receiving ground stations

Suppose that G_A is a new costumer and have official contract and want to start communication with the satellite. Both G_B and G_C are two ground stations having official contract and already communicate with the satellite. Satellite service provider G_{SSP} is the owner of the satellite. G_H is the hostile ground station. A satellite wants to give data to ground station G_A, G_B, G_C and not to G_H. Suppose ground station G_A, G_B, G_C and G_H belong to neighboring countries and they want their information to be kept secret from G_H.

A. A new Protocol

A protocol is a series of steps, involving two or more parties, designed to accomplish a task, a cryptographic protocol is a protocol that uses cryptography [10]. A cryptographic protocol involves some cryptographic algorithm, in most practical implementations asymmetric cryptography is used to secure and distribute session keys; those session keys are used with symmetric algorithms to secure data, this is called a hybrid cryptosystem [11]. The steps of the new protocol as follows:

1) G_A sends its public key to the satellite service provider.

$$G_A \xrightarrow{K_{pub(a)}} G_{SSP}$$

2) G_{SSP} will assign ID_a for G_A.

3) G_{SSP} signs the ID_a, ID_{sc},and the public key of *SC* by its own private key and then encrypts it by the public key of G_A and sends it back to G_A.

$$E_{Kpub(a)}\,[S_{ssp}(ID_a,ID_{sc},K_{pub(sc)})]$$

4) G_A decrypts the message using its own private key and then verifies it by the public key of G_{SSP}.

5) G_{SSP} will sign the public key and the ID_a of G_A and then send it to the *SC*.
$S_{ssp}(K_{pub(a)}\,,ID_a)$

6) *SC* will make the first verification by the public key of G_{SSP} to verify its sign to be sure that G_A public key and *ID* are certified by G_{SSP}.

7) SC will encrypt its own *ID*, random number and the time stamp by the public key of G_A and then send it to G_A.
$E_{kpub(a)}\,[ID_{sc}\,,R_{sc}\,,T]$

8) G_A will decrypt the received message by its own private key and verify the *ID* of *SC*.

9) G_A will send the spacecraft *ID* and timestamp plus one, all encrypted by spacecraft public key and also sends its own *ID* to *SC*.
$E_{kpub(sc)}\,[ID_{sc}\,,T+1\,]\&ID_a$

10) SC receives the message sent from G_A and decrypt it by its own private key and then makes the second verification by the following:
    - Check its *ID*.
    - Check the *ID* of the ground station by comparing the received *ID* from G_A with the one certified and stored in the onboard (received from G_{SSP}).
    - Check the value of the timestamp plus one which requires time synchronization.

11) *SC* will broadcast the initial key *(IK)* and its *ID* all signed by the private key of the spacecraft.
$S_{kpri(sc)}[IK\ \&\ ID_{sc}]$

12) The ground stations G_A, G_B and G_C will verify the message by the public key of *SC* and recover the initial key.

13) Every ground station (under official contract) send to the spacecraft its random number and the spacecraft random number minus one all signed by the private key of each ground station and also send its *ID*.

$S_{kpri(a)}[R_a \,\&\, R_{sc} \,-1] \,\&\, ID_a$

$S_{kpri(b)}[R_b \,\&\, R_{sc} \,-1] \,\&\, ID_b$

$S_{kpri(c)}[R_c \,\&\, R_{sc} \,-1] \,\&\, ID_c$

14) *SC* will verify the message by the public key of the each ground station and recover the random number and check the *ID* of each ground station and then start the last verification as the following:
    - Check the ID of each ground station by comparing the received ID from the ground station with the one certified and stored in the onboard (received from GSSP).
    - Check its random number (minus one).
    - Determine the longitude and latitude of the ground station (OPAM) to be sure that is the authenticated & wanted station in predefined time period specific for each ground station.
15) The spacecraft and the ground stations can start secure communication using symmetric encryption algorithm and the key which will be got from specific operation (combination) for every ground station random number (which is considered a unique for each ground station) and the common initial key coming from spacecraft so every communication session between spacecraft and specific ground station has its specific session key.

B. *The New Verification Method OPAM*

Using two consecutive signals (including send and receive) between SC and GS, the SC can determine from trajectory measurements calculations, the current orbital characteristics including the inclination and right ascension of ascending node (RAAN), this current data is also known to the SC from its navigational system. Verification is carried out by comparing the current orbital parameters obtained from trajectory measurement calculations with SC navigational system data. It is carried out by indicating the GS position in Cartesian coordinate system; SC trajectory measurements (TM) provides the Azimuth, elevation and range of SC, obtained data from TM are transferred using transformation matrices from topocentric coordinate system to Earth Centered Inertial (ECI) coordinate system. Using two consecutive TM's, two position vectors of SC are obtained in the ECI system and from the vector perpendicular to these two vectors ($\overline{K}$), inclination and Right ascension of ascending node (Ω) are obtained, as shown in Eq. 1 – Eq. 5 [12].

$$\overline{K} = \begin{bmatrix} K_x \\ K_y \\ K_z \end{bmatrix} \qquad (1)$$

$$K = \sqrt{K_x^{\,2} + K_y^{\,2} + K_z^{\,2}} \qquad (2)$$

$$\overline{q} = \begin{bmatrix} q_x \\ q_y \\ q_z \end{bmatrix} = \frac{\overline{K}}{K} \qquad (3)$$

$$i = \operatorname{acos} q_z \qquad (4)$$

$$\Omega = \operatorname{atan}\left(-\frac{q_x}{q_y}\right) \qquad (5)$$

Above equations (Eq. 1- Eq. 5) shows that Trajectory measurement calculations contain the approved ground station position data (longitude and latitude) as an input. If another unknown ground station tries to communicate with the SC, trajectory measurements on SC will produce orbital parameters that differ from its navigational system data, as a result SC will reject to communicate with this unknown ground station.

C. *Orbit determination mathematical proof*

Numerical verification of the OPAM was carried out using a Satellite tool Kit application (STK). A scenario was created with a Ground station placed at Alexandria with geodetic latitude φ_g = 31.0746° and longitude λ = 29.9778°, a satellite model with inclination 60^{o} and RAAN 0o was also created. Two trajectory readings from the ground station and the satellite were obtained, Table I, to be used as an input to the OPAM set of equations.

TABLE I. Satellite Trajectory Measurements

	Date/Time,	**Azimuth, deg**	**Elevation , deg**	**Range, km**
First Trajectory Measurements	1st of Oct 2011/ 20:42:26	107.826	8.706	2677.2
Second Trajectory Measurements	1st of Oct 2011/ 20:42:26	98.658	8.256	2716

OPAM set of equations were implemented in a Matlab based application-Simulink and the obtained orbital parameters were found for inclination is 62.92^{o} and for RAAN is 0.56^{o}.

Trajectory measurement data used in Table.1 was used to investigate inclination and RAAN change when ground station location is changed (for different longitude and latitude), first, geodetic latitude was fixed at 30o and longitude varies over its whole range (-180 ÷ 180^{o}), Figure.2, analysis shows that for an unauthorized ground station placed at the same latitude of the authorized ground station, satellite will obtain from OPAM verification the same inclination but different RAAN.

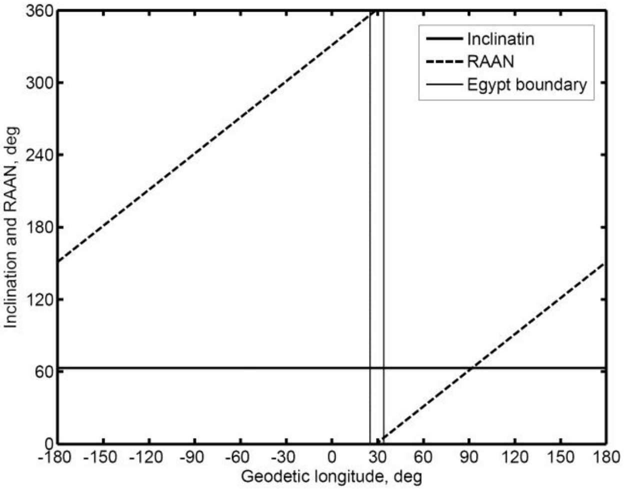

Figure.2 Variation of inclination and RAAN for different geodetic longitude.

Second, Longitude was fixed at 30^o and latitude varies over its whole range (-90 ÷ 90^o), Figure.3, the analysis shows for unauthorized ground stations placed at the same longitude of authorized station that inclination and RAAN calculation will give different values than that calculated for the authorized ground station.

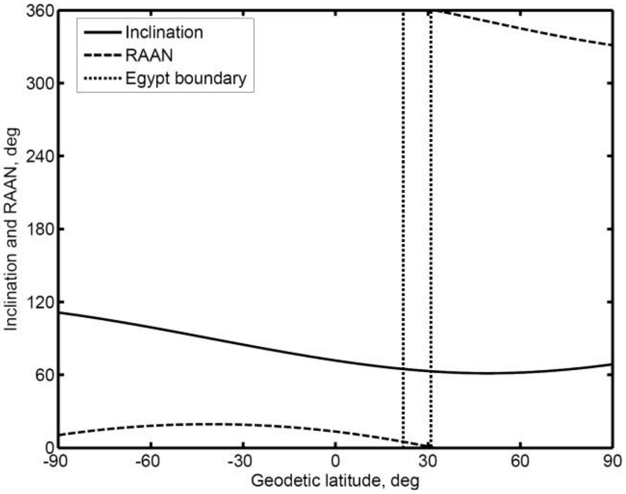

Figure.3 Variation of inclination and RAAN for different geodetic latitude.

The initial satellite orbital parameters used were inclination 60^o and RAAN 0^o, obtained orbital parameters were found for inclination 62.92^o and RAAN 0.56^o, the error refers to the assumption that earth is not rotating. To indicate the range of accepted results, Egypt's boundary was assumed to be rectangular with the following ranges of latitude and longitude, Table II.

TABLE II. Egypt's Boundary

Latitude, deg	Longitude, deg
22 - 31	25 - 34

Egypt's boundary was plotted on both figures (2 and 3) to get the limit of accepted error, that if the satellites indicated orbital parameters out of the range stated by Egypt's boundary, means that ground station is outside Egypt and hence, unauthorized ground station. The limit of error in inclination is in the range 64.8 ÷ 62.9^o and for RAAN in the range 5 ÷ 0.5^o.

D. Security of the New Protocol

This protocol combine authentication with key exchange to solve a key management problem. The spacecraft and the authorized ground stations can exchange a secret key and at the same time each will be sure that it is talking to each other and not to the hostile ground station.

The main advantage of this protocol is that the secrete key which transferred between SC and GS's is just a part of the key used in symmetric encryption scheme, it is the seed which is combined with the random number generated by each GS to generate the secret key which belongs to each GS and it is different from GS to another GS according to the GS random number.

Each authorized ground station has its own secret key and a predefined specific time to communicate with SC, so any other GS trying to communicate with SC with a different key or in different communication session will be rejected; this gives kind of authentication and protects the secret key. If GS under official contract leaks its own key to the hostile ground station, it will not be able to receive data from SC because it needs the same period of communication session and in the same coverage area and if the hostile ground station got all keys from official ground however, it seems impossible, the hostile GS will not be able to receive data because the spacecraft will determine its position by OPAM and compare it with the stored position for the official ground stations. Also in case of the satellite service provider leaks any data it will not affect the security schemes because of the same reasons and also because the SSP hasn't any information except the ground station ID and public key.

This hybrid system is how public-key cryptography is most often used in a communications system. Symmetric cryptography provides some authentication. When *SC* receives a message from G_A encrypted in their shared key, it knows it is from G_A. No one else knows their key. Also the mission plan will include predefined timetable for each communication session of each ground station which will be used as time authentication of each ground station. Using R_A, R_B, R_C, R_{SC} and R_{SC} - *1* is to prevent replay attacks. In this attack, G_H can record old messages and then use them later in an attempt to subvert the protocol. When G_A, G_B and G_C successfully decrypts R_{sc} and sends R_{sc} - *1* to the *SC* with their own random numbers in step (13), SC is ensured that G_A, G_B and G_C*'s* messages are not replays from an earlier execution of the protocol. Also using timestamps can defeat this attack [10]. A time-stamp is added to the protocol messages in steps (7) and (9) encrypted with public key of *GS* and *SC*. Timestamps require a secure and accurate system clock.

III. CONCLUSION

Satellite with high resolution optical payload and SAR payload that can take images day or night and all weather condition can be used as SPY satellite, consequently the data received and transmitted to the remote sensing satellite is considered critical to national security, it must be secured; the key management is the most critical part in the security scheme, our protocol concerned with this part. This protocol is concerned with remote sensing satellite security system; it can be useful for many applications.

If unauthorized ground station located with the same longitude of authorized ground station but with different latitude, OPAM will give same inclination but different RAAN. And if unauthorized ground station located with the same latitude of authorized ground station but with different longitude, OPAM will give same RAAN but different inclination. So double check of orbital parameter using inclination and RAAN assures the longitude and latitude of the authorized ground station.

Nomenclature

φ_g	Geodetic latitude of ground station, rad
$\overline{K}$	Perpendicular vector from r_1 and r_2 plane
q_z	Unit vector of $\overline{K}$
λ_g	Geodetic longitude of ground station
ECI	Earth center initial coordinate system
G_A	ground station A
G_B	ground station B
G_C	ground station C
G_H	Hostile ground station
GS	Ground station
G_{SSP}	Satellite service provider ground station
ID	identification
IK	Initial key
OPAM	Orbital Parameter Authentication Method
R_A	Random number of ground station A
R_B	Random number of ground station B
R_C	Random number of ground station C
R_{SC}	Random number of spacecraft
T	timestamp
UTC	Universal time coordinate
Ω	High ascension of ascending node
i	Orbital inclination, degree

REFERENCES

[1] Tanya Vladimirova, Roohi Banu and Martin N. Sweeting "On-Board Security Services in Small Satellites" Surrey Space Centre, School of Electronics and Physical, Sciences.University of Surrey, Guildford, UK, GU2 7XH

[2] M. P. Howard, S. Iyengar, Z. Sun, H. Cruischank "Dynamics of Key Mangement in Secure Satellite Multicast", IEEE Journal on Selected Areas in Communications, Vol. 22, No.3, Feb 2004.

[3] Arslan, M.G. Alagoz, F. "Security issues and performance study of key management techniques over satellite links".Computer-Aided Modeling, Analysis and Design of Communication Links and Networks, 2006 11th International Workshop on, 05 July 2006.P 122.

[4] Koltuksuz, A. "Satellite Networks for Key Management" Recent Advances in Space Technologies, 2007. RAST '07. 3rd International Conference on 08 August 2007 P103

[5] Dutta, C. Lalitkrushna, T. Nelson, A. Nagaraj, S.R. Lakshminarasimhan, P. "A New Encryption-Decryption Scheme that Solves Key Management Problem in Remote Sensing Satellite," ICETET '08. First International Conference on Emerging Trends in Engineering and Technology, pp. 1261 - 1266, 2008.

[6] YaHui Li ; WenSheng Niu ; YaDi Zhang ; JianFeng Ma ; YuLong Shen "Key Management Protocol Based on Finely Granular Multi-level Security Method in Wireless Networks". Computational Intelligence and Security (CIS), 2011 Seventh International Conference on. P: 731 - 735

[7] Ahmad, K. ; Bakhache, B. ; El Assad, S. ; Caragata, D. ; Chetto, M. "Multicast security protocol over satellite DVB based on chaotic sequences". Internet Technology and Secured Transactions (ICITST), 2011 International Conference for. P: 97 - 102

[8] Ahmad, Kassem , Bakhache, Bassem ; Assad, Safwan El ; Sindian, Samar "A scalable key management scheme for secure IP multicast over DVB-S using chaos", Electrotechnical Conference (MELECON), 2012 16th IEEE Mediterranean. P: 736 - 740

[9] William Stallings, "Cryptography and Network Security Principles and Practices", Fourth Edition

[10] Bruce Schneir , "Applied Cryptography" Second Edition, john wiley & Sons ,Inc

[11] Vijayakumar, P. ; Bose, S. ; Kannan, A. ; Subramanian, S.S. "An effective key distribution protocol for secure multicast communication". Advanced Computing (ICoAC), 2010 Second International Conference on. P: 102 - 107

[12] Howard Curtis, "Orbital Mechanics for Engineering Students" London, 2005.