Countering jamming attacks against an authentication and key agreement protocol for mobile satellite communications

Ioana Lasc, Reiner Dojen, Tom Coffey
Department of Electronic & Computer Engineering,
University of Limerick, Ireland
ioana.lasc@ul.ie, reiner.dojen@ul.ie, tom.coffey@ul.ie

ABSTRACT

The radio-based medium of satellite communication systems is vulnerable to interference on physical channels: Unintentional interferences occur frequently and jamming attacks can be achieved using low-grade technology. While application layer security protocols cannot defend against denial of service (DoS) attacks where the attacker jams continuously, effective security protocols ensure that communication can continue after such interference has stopped.

This paper analyses an authentication and key agreement protocol for satellite communications. The presented analysis reveals that the protocol is susceptible to a new DoS attack, where attackers jam a single message to achieve a permanent DoS condition. A new authentication and key agreement protocol is proposed that additionally addresses the scenario, where messages send over the mobile satellite channel may not reach their intended recipient due to accidental or malicious interference. Analysis of the new protocol demonstrates that it is effective in countering the disruptive effects of jamming.

Keywords
Denial of service attack, security protocol, satellite communications, mobile, authentication, jamming.

1. INTRODUCTION

Satellite communication systems are nowadays employed in the provision of advanced personal communication services [1], [2] [3], as they offer the benefits of global coverage and enhanced mobility for users. In such a satellite system, Low-Earth Orbit Satellites (LEO – at altitudes bellow 5000 km [4]) enable communication between mobile devices and the Network Control Centre via gateways (see Figure 1).

The main components are the LEO satellites, the gateways, the Network Control Centre (NCC) and the mobile devices.

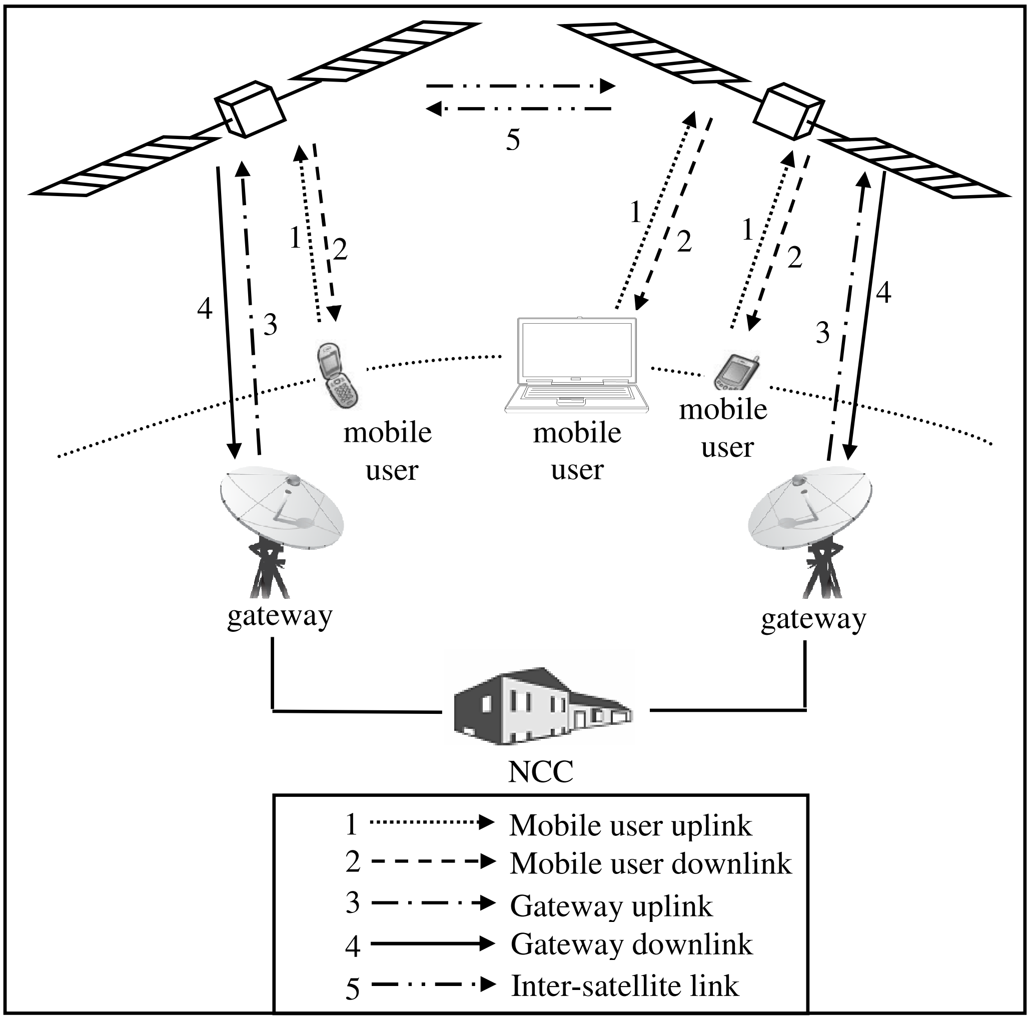


Figure 1. A LEO communications system.

The wireless mobile environment in such a satellite system is intrinsically a radio-based transmission medium for which a denial of service attack (DoS) is a common threat. A DoS attack can be mounted by injecting or suppressing messages between communicating parties to disrupt the service for legitimate users [5], [6]. These denial of service attacks can take two forms: The first is directed at large number of users with the intent to interrupt the entire service. The second form, called a selective denial of service attack, is specifically directed at a particular mobile user. Due to the threat presented by these attacks, service availability is a basic requirement for any security system for mobile satellite communication systems. Due to the threat presented by these attacks, service availability is a basic requirement for any security system for mobile satellite communication systems.

Security protocols lie at the heart of a security system and ensure the security of both the infrastructure itself and the information that runs through it [7]. Basic security protocols allow agents to authenticate each other, to establish fresh session keys for confidential communication and to ensure the authenticity of data and services [8], [9]. Building on such basic security protocols, more advanced services like non-repudiation, fairness, electronic payment and electronic contract signing are achieved [10]. The design of such security protocols should be robust enough to resist attacks, such as replay attacks, parallel session attacks or type-flaw attacks [11]. Recent research in wireless communication security proposed new approaches for efficient execution security schemes in wireless protocols with high performance [12]. Further, the possibility of interfering with communication on physical channels needs to be considered as it can affect the security at the application layer. This is particularly important in the wireless environment: Unintentional interferences caused by other active devices in geographical proximity of a terrestrial terminals or weather impairments occur frequently [13] [14]. Moreover, messages may be lost due to constraints on frequencies bands and satellite handover issues in LEO systems [15]. In addition to such accidental interference, the security of the communication may be compromised by an attacker that is intentionally jamming messages. In particular, the jamming of a mobile user’s downlink is easily achievable using low-grade technology [16], [17], [18]. While jamming the uplink of the NCC is more difficult, it is nevertheless achievable [19], [20], [21]. Thus, to counter disruptive effects of both accidental interference and jamming, security protocols need to remain in a safe state after the interference has stopped.

In this paper the authentication and key agreement protocol by Chen, Lee and Chen for satellite communications (CLC protocol) is analysed. The presented analysis reveals that the protocol is susceptible to a new DoS attack, where the attacker jams a single message in the protocol to create the DoS condition. Subsequently, the NCC and the mobile user are desynchronised on their shared secrets. Thus, the mobile user is denied any future access to the services provided by the NCC. A new authentication and key agreement protocol for satellite communications is proposed to overcome the revealed weaknesses in the CLC protocol. The new protocol includes a resynchronisation challenge to address the possibility that the mobile user and the NCC are desynchronised on their shared secrets due to loss of messages, which may happen due to accidental or malicious interference. A security analysis of the new protocol is presented that demonstrates the effectiveness of the new protocol in countering the disruptive effects of jamming.

2. REVIEW OF CLC PROTOCOL

In 2009 TH. Chen, WB. Lee and HB. Chen proposed an authentication mechanism for mobile satellite communication systems [22] – hereafter referred to as the CLC protocol. This protocol is based on the Chang and Chang protocol [23] and aims to provide authentication between a mobile user and the Network Control Centre within a LEO satellite communication system, such as Globalstar [24] or Iridium [25]. The authors of the CLC protocol claim the following advantages [22]:

1. removes the complexity of PKI
2. avoids complex computations for mobile users
3. requires no sensitive verification table, which may cause the NCC to become an attractive target for numerous attacks

The CLC protocol comprises three phases: initialization, registration and authentication. In the initialization phase the NCC computes its own long term private and public key pair x and y. During the registration phase, the NCC assigns each mobile user a permanent identity U_{ID}, an initial temporary identity T_{ID} and a long term secret key k_U. For each mobile user, the NCC generates a random number k and computes $r = g^k \bmod p$, $s = h(U_{ID})x + kr^{-1} \bmod q$ and $k_U = h(U_{ID}, k)$. The registration phase completes with the NCC storing (U_{ID}, T_{ID}, r, s) in its verification table and (U_{ID}, T_{ID}, k_U) into the mobile user's smart card. The authentication phase is required whenever the mobile user wants to access a service. Each execution of the authentication phase establishes a session key between the mobile user and the NCC and updates the temporary identity T_{ID}.

2.1 CLC authentication phase

In the authentication phase the two communicating parties, U and NCC, use the shared secrets established during the initialisation and registration phase to prove their identity to each other. The notations used throughout this paper to describe the protocols are defined in Table 1 and the details of the authentication phase are shown in Figure 2.

Table 1. Notation for protocol descriptions.

U	The mobile user
LEO	Low Earth Orbit Satellite
NCC	Network Control Centre
U_{ID}, LEO_{ID}	User/LEO permanent identity
T_{ID}	User temporary identity
sk	Session key
MAC(k)(.)	Keyed one-way hash function using the key *k*
{m}k	Secret-key encryption function for a message using the key *k*
h(.)	One-way hash function
k_U	User's long term secret key
x	NCC's long term private key
y	NCC's long term public key

Before the mobile user can access a service, the NCC and the user mutually authenticate each other in the following way: The mobile user computes the message authentication code $MAC(k_U\ )$ for U's permanent identity U_{ID}, temporary identity T_{ID} and the current session key $sk = h(k_U, T_{ID})$. U then sends $T_{ID}, MAC(k_U\ )(U_{ID}, T_{ID}, sk)$ to the LEO. On receiving message 2 from LEO, the NCC looks up the verification table and retrieves the entry (U_{ID}, r, s) corresponding to the received T_{ID}.

1. U -> LEO: $T_{ID}, MAC(k_U\ )(U_{ID}, T_{ID}, sk)$

2. LEO -> NCC: $T_{ID}, MAC(k_U\ )(U_{ID}, T_{ID}, sk), LEO_{ID}$

3. NCC -> LEO: $\{T_{ID}, T_{IDnew}\}sk, LEO_{ID}$

4. LEO -> U: $\{T_{ID}, T_{IDnew}\}sk$

Figure 2. Authentication Phase of the CLC Protocol.

The NCC then performs the following:

- Validates *k* using the equation $s = h(U_{ID})x + kr^{-1} \bmod q$

- Computes the possible user master key: *k_U' = h(U_{ID},k)* and the possible session key *sk' = h(k_U, T_{ID})*
- Computes *MAC(k_U)(U_{ID}, T_{ID}, sk')* to see if it matches the received value. If they match, the mobile user is authenticated otherwise the authentication request is rejected
- Generates a new temporary identity for the mobile user T_{IDnew} and updates its verification table with it. Then sends message 3.

On receiving message 4, U decrypts the message and verifies that T_{ID} matches the stored T_{ID}. If they are identical, the mobile user U has authenticated the NCC and updates its temporary identity to T_{IDnew} for the next authentication request.

After authentication, the two parties encrypt their data with the session key *sk* = h(*key*, T_{ID}). The value T_{IDnew} will be used in the next authentication request.

3. A NEW DENIAL OF SERVICE ATTACK ON THE CLC PROTOCOL

In this section, we present an analysis of the operation of the CLC protocol. This analysis reveals that the protocol is vulnerable to a denial of service attack. Mounting of this new denial of service attack on the protocol is also demonstrated.

3.1 Analysis of the CLC Protocol

The structure of the CLC protocol is presented in Figure 3.

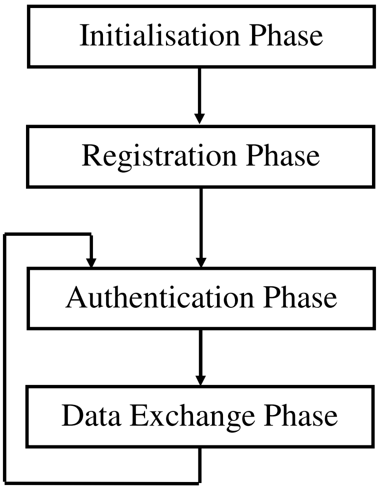
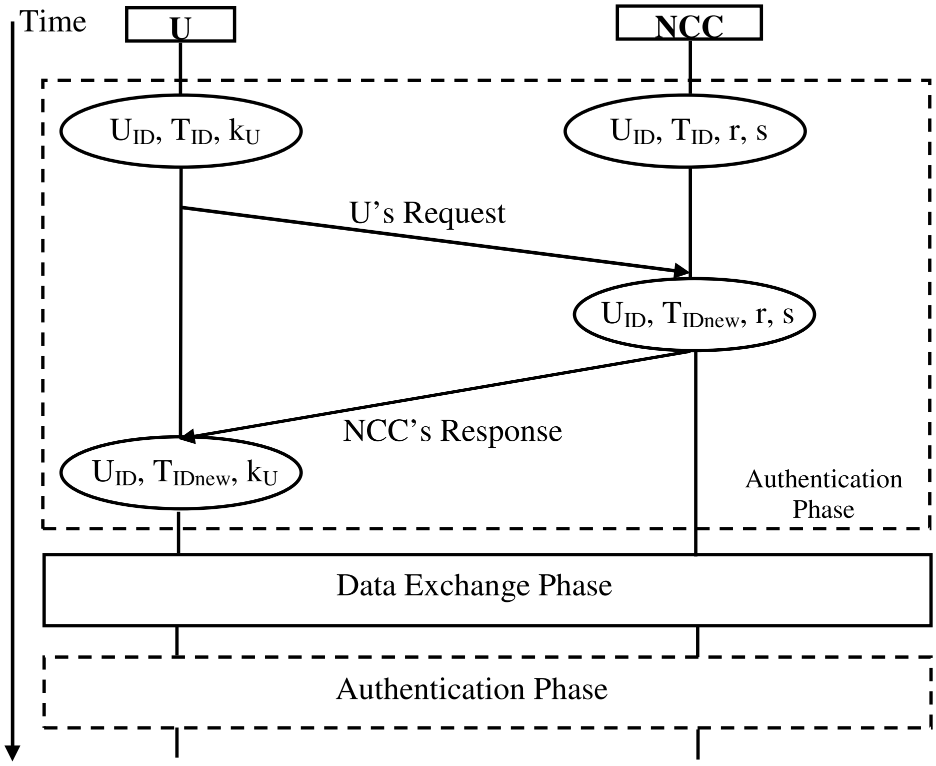


Figure 3. Flow diagram of the CLC protocol

The NCC initializes a discrete logarithm-based cryptosystem and creates its pair of private/public keys (*x*/*y*) in the initialisation phase. Subsequently, the registration phase ensures establishment of shared secrets between the NCC and mobile user U. These credentials are used in the initial authentication phase between NCC and U. Also, during each run of the authentication phase NCC and U update to a new temporary identity T_{IDnew}. The NCC generates this T_{IDnew} and updates its verification table before sending its response in message 3 via the LEO to the mobile user. On receiving message 4, the mobile user evaluates that the received value T_{ID} matches the corresponding stored value. If it matches, then U updates to T_{IDnew}. NCC and U have now mutually authenticated each other and U can access the requested service using the session key $sk = h(k_U, T_{ID})$. If a message with a matching $\mathrm{T_{ID}}$ value is not received within a time-out period, U assumes that NCC has rejected the authentication request.

In case of a successful authentication, the next authentication phase is performed with the updated value T_{IDnew}. Figure 4 presents a detailed view of the update mechanism for T_{ID}.



Time
U
NCC
$\mathrm{U_{ID}, T_{ID}, k_U}$
$\mathrm{U_{ID}, T_{ID}, r, s}$
U's Request
$\mathrm{U_{ID}, T_{IDnew}, r, s}$
NCC's Response
$\mathrm{U_{ID}, T_{IDnew}, k_U}$
Authentication Phase
Data Exchange Phase
Authentication Phase

Figure 4. Update mechanism for T_{ID} in the CLC protocol

As satellite communication systems use wireless transmission, messages can be easily interfered with at the physical layer [19], [20]. However, the design of the CLC protocol regards the update mechanism as an atomic operation - it does not consider the possibility of interference or loss of messages. On the other hand, the update mechanism is a sequential process that requires successful message reception to ensure synchronisation of the shared secrets at completion time. If any unwanted event occurs that interrupts the authentication process, then the CLC protocol reaches an undefined state (see Figure 5) and U and NCC are desynchronised on T_{ID}. Such an interruption of the authentication process may occur randomly through accidental interference or intentionally by an intruder through jamming.

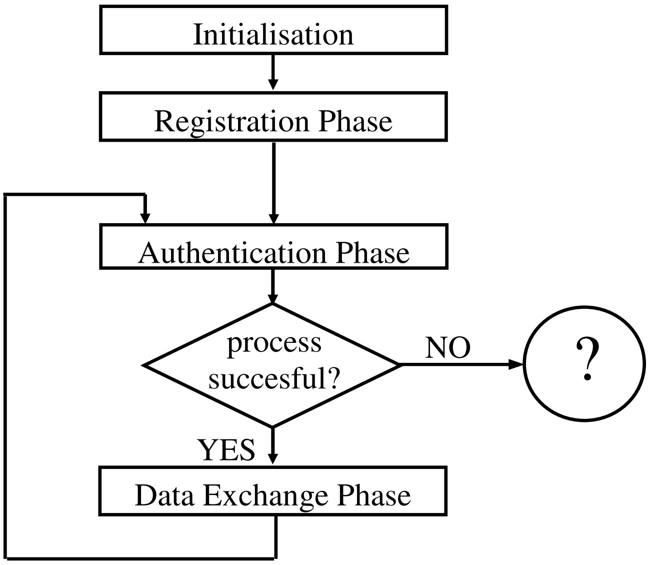


Figure 5. Reaching an undefined state in the CLC protocol.

3.2 Mounting the DoS attack

The dependence on successful message reception is a weakness in the authentication phase of the CLC protocol that can cause a DoS condition: If the last message of the authentication phase is not successfully delivered to U (see Figure 6), the NCC has already updated to T_{IDnew} , while U does not update. Consequently, NCC and U are desynchronised on their $\mathrm{T_{ID}}$ value: While U is using the old T_{ID}, the NCC expects U to use the updated value T_{IDnew} . Thus, the mobile user is now incapable of producing the correct evidence of its legitimate identity for the NCC and therefore will be denied access to the satellite services. Further, all of U’s subsequent authentication requests will equally be interpreted by the NCC as illegitimate requests.

If this DoS condition occurs, then the user times out while waiting on a response from the NCC (message 4). However, the mobile user cannot distinguish a time-out caused by a rejected authentication request from a time-out caused by interference (cf. Figure 5). As U's reaction to such a time-out is not defined by the CLC protocol, two options are available to U: to resend its authentication request or to go into the data exchange phase. If U resends its authentication request, this request will be rejected, as the NCC has already updated and expects U to use the value T_{IDnew} rather than T_{ID}. Alternatively, U can enter the data exchange phase with the NCC. As the data exchange phase is based upon the value T_{ID}, rather than T_{IDnew}, U has the correct secrets. Nevertheless, U will not be able to authenticate itself to the NCC in the next authentication phase, as it does not possess the required value T_{IDnew}.

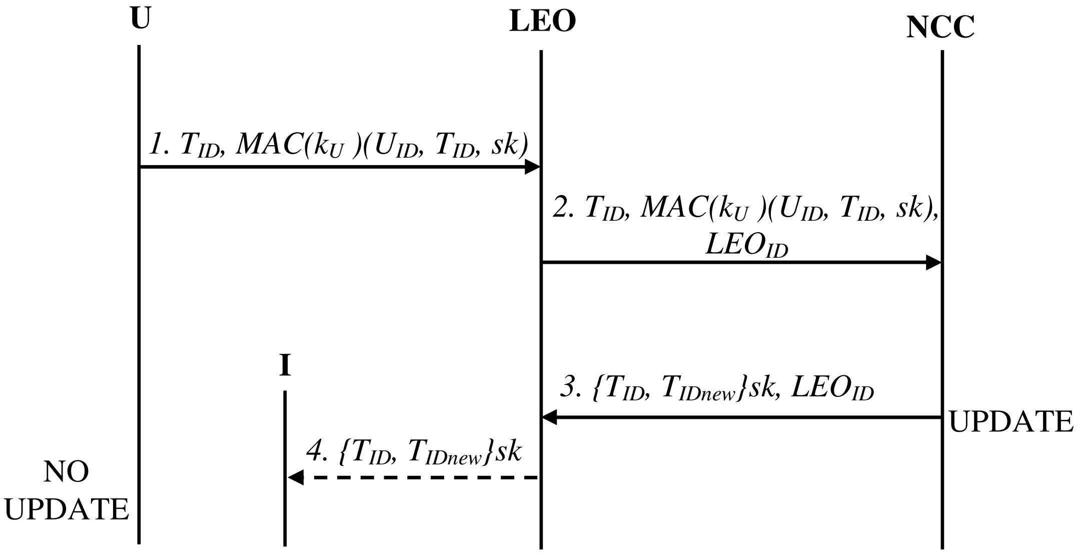

U
LEO
NCC
1. T_{ID}, $MAC(k_U)(U_{ID}, T_{ID}, sk)$
2. T_{ID}, $MAC(k_U)(U_{ID}, T_{ID}, sk)$, LEO_{ID}
I
3. $\{T_{ID}, T_{IDnew}\}sk$, LEO_{ID}
UPDATE
4. $\{T_{ID}, T_{IDnew}\}sk$
NO UPDATE

Figure 6. A jamming attack on the downlink in the CLC protocol.

3.3 Realising the presented attack

The jamming attack on the CLC protocol presented in section 3.2 is directed at a single mobile user, jamming its downlink. Thus, an attacker can achieve a selective denial of service attack against an individual mobile user by using a low-power jammer.

The presented attack can also be directed at the NCC's uplink to the LEO to achieve a denial of service attack against a large number of users. This attack affects all the mobile users executing an authentication phase with the NCC at the time the jamming occurs. In this attack all the affected mobile users are out of synchronisation with the NCC and any of their subsequent authentication requests will be denied by the NCC. While attacking an NCC's uplink is more difficult than jamming a mobile user's downlink, it is nevertheless achievable.

4. A NEW AUTHENTICATION AND KEY AGREEMENT PROTOCOL

The attack presented in the previous section highlights the possibility of affecting the security at application layer by interfering with the communication on physical channels. While an application layer protocol cannot defend against continuous jamming, an effective security protocol needs to ensure that communication can continue from a safe state after such interference has stopped. In this section we propose a new authentication and key agreement protocol for satellite communications to counter the disruptive effects of jamming attacks.

The CLC protocol design only considers the ideal situation where all messages are received by their intended recipients. If a message is not successfully delivered, U and NCC are desynchronised on their shared secrets and any subsequent authentication request of the legitimate user U is rejected. Furthermore, as desynchronisation is not considered, no process to renegotiate access is provided in the CLC protocol. To overcome this weakness, we propose a new protocol that includes a resynchronisation challenge as outlined in Figure 7. The desynchronisation problem of the CLC protocol is solved by extending NCC's storage time for T_{ID} until U enters the next authentication phase using the expected value T_{IDnew}, which proves that U has successfully updated its secrets.

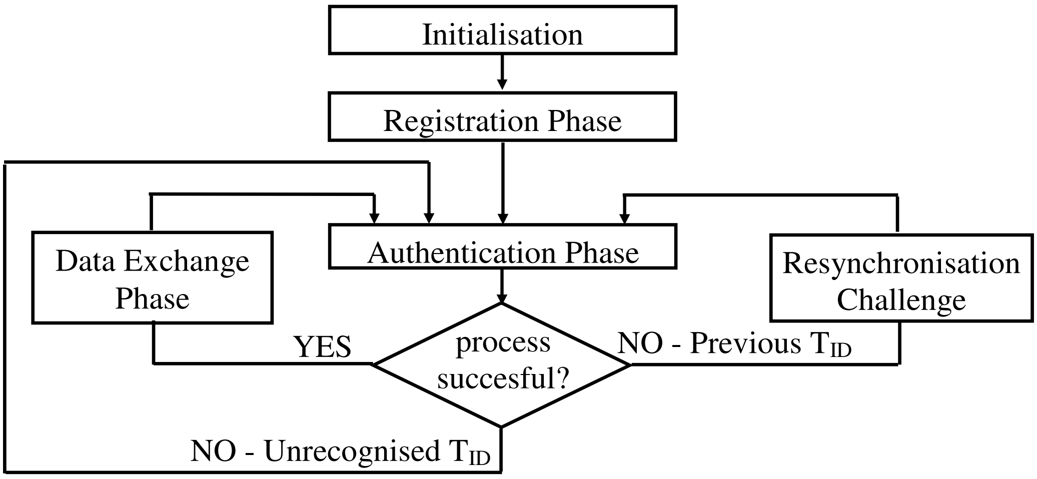


Figure 7. Flow diagram of the new protocol.

Storing the value T_{ID} used in the previous authentication session allows the NCC to differentiate its response depending on the content of U's authentication request as outlined in Figure 8. Messages 1 and 2 of the proposed authentication phase are identical to the CLC protocol.

On receiving a correct request from U, the NCC grants access to U and the protocol proceeds with messages 3.a and 4.a, which contain the GRANT flag, the current T_{ID} and the new T_{IDnew} all encrypted with the current session key sk_{crt}.

1. U -> LEO: T_{ID}, MAC(k_U) (U_{ID}, T_{ID}, sk)
2. LEO -> NCC: T_{ID}, MAC(k_U)(U_{ID}, T_{ID}, sk), LEO_{ID}

3.a. NCC -> LEO: {GRANT, T_{ID}, T_{IDnew}}sk_{crt}, LEO_{ID}
4.a. LEO -> U: {GRANT,T_{ID}, T_{IDnew}}sk_{crt}

3.b. NCC -> LEO: {DENY, T_{ID}, T_{IDnew} }sk_{prev}, LEO_{ID}
4.b. LEO -> U: {DENY, T_{ID}, T_{IDnew} }sk_{prev}

Figure 8. Proposed authentication phase.

If NCC receives an authentication request based on the previous value T_{ID}, the NCC assumes desynchronisation has occurred: NCC denies U's request and issues a resynchronisation challenge (messages 3.b. and 4.b). In this resynchronisation challenge, NCC sends the DENY flag, the previous value T_{ID} and the expected value T_{IDnew}. The user U is requested to repeat authentication with the provided T_{IDnew}.

The NCC will ignore any other authentication requests, which are deemed replay attacks.

On receiving message 4.a, the user establishes that it contains the expected value T_{ID}, in which case authentication is successful and the protocol now enters a data exchange phase using the session key sk_{crt}, which is based upon the current T_{ID}. If the expected value is not contained, authentication fails and U resends message 1.

If the user receives message 4.b, the user also establishes that it contains the expected value T_{ID}, which ensures NCC is the source of the message. In this case U recognises the resynchronisation challenge as valid, extracts T_{IDnew} from the messages and uses it to compute and resend the authentication request. If the expected T_{ID} is not included, the resynchronisation challenge is deemed bogus and U resends the original message 1.

In the case that U receives neither 4.a nor 4.b, U times out and resends message 1.

In Figure 9 the first two authentication phases of the new protocol are presented. Initially, both U and NCC are storing the shared secrets established in the registration phase. As these are securely stored in the user's smart card, desynchronisation is not possible at this stage. After the first valid authentication request, NCC stores two temporary IDs for U: T_{ID} and T_{IDnew1}. The value T_{IDnew1} is expected to be used in the next authentication request by U, while T_{ID} is used to detect a potential desynchronisation condition.

4.1 Motivation for extended Storage

The correct execution of the CLC protocol depends on the successful update of T_{ID} by both U and NCC. This update of T_{ID} is a sequential process performed without NCC's awareness of U's update status. However, such awareness is required to enable NCC to detect a potential desynchronisation condition. There are several options how this can be achieved, such as:

- adding extra confirmation messages,
- adding an independent session key update phase
- adding time-stamps to the structure of the protocol
- extending storage time of suitable information.

We propose to extend the storage time of the value T_{ID} by the NCC, which has the following properties:

- Simple protocol structure, as it eliminates the need for an extra key update phase to resynchronise on T_{ID}.
- Minimises the amount of messages required, thus avoiding further potential jamming options introduced by extra messages used for update confirmation.
- Avoids the need for synchronised clocks.
- Provides data synchronisation assurance.

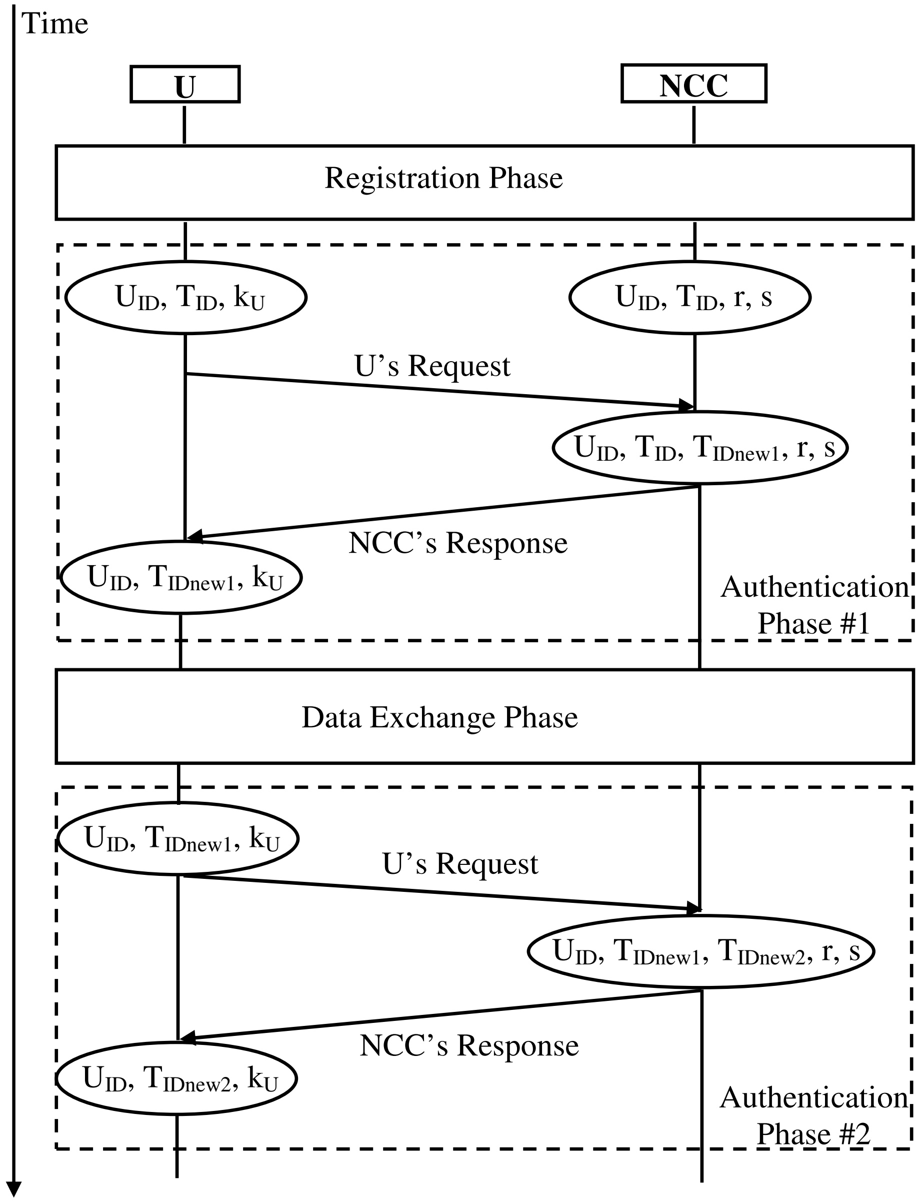


Figure 9. Authentication phases in the new protocol

5. ANALYSIS OF THE NEW PROTOCOL

In the ideal situation that all messages are received by their intended recipients, the security of the new protocol is equivalent to the CLC protocol [22]. The following discusses security aspects of the new protocol that arise from the included resynchronisation challenge.

5.1 Security Implications of Extended Storage Time of T_{ID}

In the new protocol the NCC is extending its storage time for the temporary user's identity until the next successful authentication request is received. Even though NCC recognises an authentication request based on the previous T_{ID}, it will not grant access on such a request. Instead, the NCC will only issue a resynchronisation challenge, expecting the user to reauthenticate using the updated T_{IDnew}. As the life-time of the previous session key is not prolonged, gaining either the previous T_{ID} or the previous *sk* will not enable an attacker to compromise the security the protocol. Consequently, NCC's extended storage time for T_{ID} does not introduce any security risks.

5.2 Replaying authentication requests of U

If an attacker replays an authentication request of U that it is older than the most recent one, the NCC ignores the received request. If U's most recent authentication request is replayed, the NCC responds with the resynchronisation challenge. The following cases need to be considered:

Case 1: U did not send out any authentication request. Therefore, it does not expect any message from NCC and will ignore the received message.

Case 2: U requested authentication and is desynchronised with NCC. U accepts the resynchronisation challenge, uses the included data to resynchronise and sends a new authentication request using the updated T_{IDnew}.

Case 3: U requested authentication and is synchronised with NCC. As the resynchronisation request is based upon old $\mathrm{T_{ID}}$ values, U will ignore the message. Eventually, U will time-out and subsequently will resend its authentication request to NCC.

In either case, the attacker only delays the authentication process, but does not compromise the security of the protocol. Once the replay is discontinued, NCC and U will be able to authenticate each other.

5.3 Replaying of NCC's responses

The NCC is responsible for generating new values for T_{ID}. U can only update as a response to message from the NCC and, therefore, U never needs to roll back to old T_{ID} values. Hence, U will ignore any received messages that are based on previous T_{ID} values. Consequently, an attacker cannot compromise the security of the protocol by replaying NCC responses.

5.4 Jamming messages

The new protocol addresses the realistic scenario, where message might not reach their intended recipient due to accidental or malicious interference. The following scenarios need to be considered:

- If U's authentication request does not reach the NCC, U eventually times out and resends the request. Once the request reaches the NCC, authentication will be successful.
- If NCC's grant message to the mobile user is jammed, U will eventually resend its authentication request. However, in this situation U and NCC are desynchronised and NCC will respond with a resynchronisation challenge. After successful resynchronisation U and NCC will be able to authenticate each other.
- If the resynchronisation challenge issued by the NCC is jammed, U times out and keeps resending its authentication request. Eventually, when the jamming stops, U and NCC will resynchronise and will be able to authenticate each other.

In summary, as long as the jamming attack is not continuous U and NCC will eventually be able to authenticate. All the attacker can gain by jamming messages is to delay the authentication process.

6. CONCLUSIONS

Satellite communications are nowadays employed in the provision of advanced personal communication services. However, interference with the radio transmission medium of satellite communications is a common threat: Unintentional interferences occur frequently and jamming attacks can be achieved using low-grade technology. While application layer security protocols cannot defend against DoS attacks where the attacker jams communications continuously, effective security protocols ensure that communication remains in a safe state after such interference has stopped.

In this paper the authentication and key agreement protocol for satellite communications by Chen, Lee and Chen was reviewed. Analysis of the CLC protocol revealed that it is susceptible to a new DoS attack, where an attacker interrupts the authentication phase by jamming a single message. Subsequently, the NCC and the user will continuously fail to mutually authenticate each other. Thus, the mobile user is denied any future access to the provided services.

A new authentication and key agreement protocol for satellite communications was proposed to overcome the revealed weaknesses in the CLC protocol. In the new protocol the authentication phase extends the storage time of some shared secrets. If the NCC assumes desynchronisation has occurred, it denies U's request and issues a resynchronisation challenge. U uses the provided information in the resynchronisation challenge to update to the correct shared secrets and attempts to reauthenticate. A security analysis of the new protocol demonstrated its effectiveness in countering the disruptive effects of jamming. Regardless of link availability guaranteed by the satellite service provider, the synchronization problem is successfully managed at the application layer by the new protocol.

7. ACKNOWLEDGMENTS

This work was funded by the Irish Research Council for Science, Engineering and Technology (IRCSET Embark Initiative) and Science Foundation Ireland - Research Frontiers Programme (SFI RFP07CMSF 631).

8. REFERENCES

[1] G. Comparetto, Ramirez R, Trends in mobile satellite technology. IEEE Computer, Vol. 30, Issue 2 (1997) 44-52.

[2] E. Lutz, Issues in satellite personal communication systems. Wireless Networks, Vol. 4, Issue 2 (1998) 109-124.

[3] J.V. Evans, Satellite systems for personal communications. Proc. IEEE, Vol. 86, Issue 7 (1998) 1325-1341

[4] Z. Sun. Satellite networking principles and protocols. John Wiley and Sons Ltd. 2005

[5] W. Xu, W. Trapper, Y. Zhang, T. Wood, The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. Proc. of the 6th ACM International symposium on Mobile ad hoc networking and computing, Urbana-Champaign, IL, USA (2005) 46-57

[6] T. Peng, C. Leckie, K. Ramamohanarao, Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems, ACM Computing Surveys, Vol. 39, No. 1, Article No. 3 (2007) 1-42.

[7] R. Dojen, T. Coffey, Layered Proving Trees: A Novel Approach to the Automation of Logic-Based Security Protocol Verification, ACM Transactions

on Information and System Security (TISSEC), Volume 8, Issue 3, (2005) 287-311.

[8] R. Dojen, I. Lasc, T. Coffey, Establishing and Fixing a Freshness Flaw in a Key-Distribution and Authentication Protocol. IEEE 4th International Conference on Intelligent Computer Communication and Processing, (2008) 185-192

[9] T. Coffey, R. Dojen, T. Flanagan, Formal verification: An imperative step in the design of security protocols, Computer Networks Journal, Elsevier Science, Vol. 42, No. 5 (2003) 601-618.

[10] T. Coffey, R.Dojen, A Formal Verification Centred Design Process for Security Protocols, Handbook of Research on Information Security and Assurance, Eds: Gupta, J.N.D. and Sharma, S.K., IGI Global, 2008, pp. 165-178

[11] M. Ventuneac, R. Dojen, and T. Coffey, Automated Verification of Wireless Security Protocols using Layered Proving Trees. WSEAS Transactions on Communications, Vol. 5, No. 2 (2006) 252-258

[12] N. Sklavos, X. Zhang, Wireless Security & Cryptography: Specifications and Implementations, CRC-Press, A Taylor and Francis Group, ISBN: 084938771X, 2007.

[13] J. Louis, Jr. Ippolito, Satellite communications systems engineering: atmospheric effects, satellite link design and system performance. Wiley Series on Wireless Communications and Mobile Computing, 2008.

[14] A.D. Panagopoulos, M.P. Anastasopoulos, P.G. Cottis, Error Performance of Satellite Links Interfered by Two Adjacent Satellites, IEEE Antennas and Wireless Propagation Letters, Vol. 6 (2007) 364-367

[15] A. Gurov, S. Floyd, Modeling Wireless Links for Transport Protocols, ACM SIGCOMM Computer Communications Review, Vol. 34, No. 2, (2004) 85-96

[16] T. Mahoney, P. Kerr, B. Felstead, P. Wells., M. Cunningham, G. Baumgartner, L. Jeronim, An investigation of the military applications of commercial personal satellite-communications systems. Military Communications Conference Proceedings 1999, MILCOMM 1999 IEEE. Volume 1, (1999) 112 – 116.

[17] E.B. Felstead, R.J. Keightley, Robustness capabilities of transponded commercial satellite communications. Conference Record, Military Communications Conference, IEEE MILCOM 95, San Diego, CA, USA, Vol. 2, (1995) 783-787

[18] J.W. Lee, V.A. Marshall, Maximum capacity prediction and anti-jamm performance analysis for commercial satellite communication systems. Conference Record, Military Communications Conference, IEEE MILCOM 94, Forth Monmouth, NJ, USA (1994) 506-510

[19] J.S. Gansler, H. Binnendijk, Information assurance: Trends in vulnerabilities, threats and technologies. National Defense University, Center for technology and national security policy, Washington, D.C. 2005.

[20] United States General Accounting Office 2002. Critical Infrastructure Protection: Commercial Satellites Should Be ore Fully Addressed. GAO Report to the Ranking Minority Member, Permanent Subcommittee on Investigations, Committee on Government Affairs, U.S. Senate August 2002.

[21] H. Rausch, Jamming commercial satellite communications during wartime: an empirical study. Proceedings of the Fourth IEEE International Workshop on

Information Assurance, IEEE Computer Society, Washington, DC, USA (2006) 109-118.

[22] TZ. Chen, WB. Lee and HB. Chen, A self-verification authentication mechanism for mobile satellite communication systems. Computers and Electrical Engineering, Vol. 35, Issue 1 (2009) 41-48.

[23] YF. Chang, CC. Chang, An efficient authentication protocol for mobile satellite communication systems. ACM SIGOPS Operating Systems Review, Vol. 39, Issue 1 (2005) 70-84.

[24] R.A. Wiedeman, A.J. Viterbi, The Globalstar mobile satellite system for worldwide personal communications. Proceedings of the Third International Mobile Satellite Conference, Pasadena (1993) 291-296.

[25] J.E. Hartleid, L. Casey, The Iridium system personal communications anytime, anyplace. Proceedings of the Third International Mobile Satellite Conference, Pasadena (1993), 285-290.