SERBIAN JOURNAL OF ELECTRICAL ENGINEERING
Vol. 13, No. 1, February 2016, 21-29

UDC: 004.056.55:004.722 **DOI: 10.2298/SJEE1601021T**

Implementation Theoretical Information Protocol for Public Distribution Cryptology Keys

Milomir Tatović[1], Saša Adamović[1], Milan Milosavljević[1]

Abstract: This paper presents the design and implementation of a key distribution protocol over public channels. This protocol has its own source of randomness, based on data from civil air traffic. An equivalent protocol scheme has been developed according to the theoretical protocol, “satellite scenario”. Both parties to generate symmetric keys without preshared secrets have been allowed. Keys generated in this way can be used with symmetric encryption (AES, DES). The performance of the proposed protocol has been conducted with rigorous theoretical information analysis.

Keywords: Key Exchange, Perfect Protocol, Satellite Scenario.

1 Introduction

In the modern world of communication, there is a need for cryptographic mechanisms that will ensure the confidentiality of service at all levels of communication. The safety of these services is based on the secrecy, power, and distribution of cryptographic keys used in symmetric cipher systems. In certain situations, the problem of key distribution can be solved with the help of a delivery service, but there are situations where this is not possible. In addition, there are no secret computer channels through which such a thing is feasible in real scenarios.

It is possible to perform key distribution over the well-known commercial protocols of today (Difi-Hellman, RSA, Forteza). All of these protocols for key distribution have been implemented in all versions of SSL (Secure Socket Layer).

The most famous protocol of this type is certainly the Diffie-Hellman protocol [1], which consists of public parameters and a one-way function called a discrete exponent. However, in such a protocol there is a problem of generating cryptographic keys. Also, for this type of protocol there is no strong mathematical proof that the protocol is unconditionally secure. This means it will not be immune to the attacks of someone with huge computing resources.

[1]Singidunum University, Danijelova 32, Belgrade;
E-mails: milomir@tatovic.com; sadamovic@singidunum.ac.rs; mmilosavljevic@singidunum.ac.rs

Today, when computers have a lot of processing power, relying on hard computable functions is not recommended. This is why new protocols for the distribution of keys are being researched in other scientific fields, for example, the BB84 protocol [2], which is based on the indeterminacy of the quantum world. The BB84 protocol was used by Ueli Maurer in order to define the theoretical protocol "satellite scenario," in which the optical quantum channel protocol is replaced by the radio link between the satellites and receivers on the ground. The three phases of this protocol are implemented on a correlated, purely random binary sequence of radio waves. The first phase is Advantage Distillation, the second is Information Reconciliation, and the third phase is Privacy Amplification [3].

The easiest way of presenting the satellite scenario idea is through the theory of sets and set intersections.

Participants Alice, Bob, and Eve, receive sequences and various series presented as sets. Sets each have mutual or individual elements. Alice and Bob are legitimate participants, while Eve is a malicious participant, who is eavesdropping on their communication. The purpose of this protocol is to determine the elements of the intersection "PK," because that very intersection represents the mutual information that Alice and Bob possess, and Eve does not (Fig. 1).

2 Proposal of Protocol

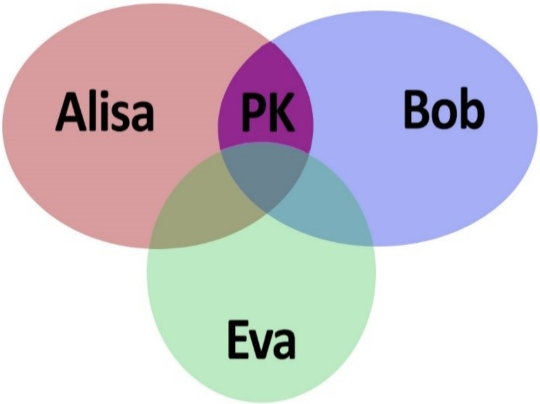

Fig. 1 – *Set intersection and mutual element.*

Modeled after the satellite protocol theoretical scenario, the protocol was implemented using the existing infrastructure available to everyone. Since the information about the current locations of aircraft in civil aviation is available to the public, and can be collected at different geographical remote locations, it was easy to use it for the implementation of this protocol. The fact that it is possible to collect data on different geographical locations from different numbers of planes is reminiscent of an equivalent scheme (satellite scenario), which is presented with the theory of sets in Fig. 1.

2.1 Source of randomness

There are many sources of randomness in nature. Some may be easily used to generate a binary sequence, whereas others may require some complex infrastructure. Choosing the ideal source depends on its further implementation. For this reason, the use of publicly available data, which contain a certain level of uncertainty, is a good potential source for further syntheses of the true random generator.

The system, which integrates the data collected by GPS satellites and the relevant flight data, is called ADS-B [4]. This is a radio communication system for the exchange of data from aircraft to the ground, and vice versa. Only the portion of data collected from the aircraft on the ground has been used in this study. The radio signal that is broadcast from a plane encapsulates information relevant to the flight at that moment.

The condition for the use of these data in this paper is that they are variable in time. This requirement at any moment during the time of the flight only meets the data of latitude and longitude, which is the reason why it has been used. Data represented by a series of random binary tests achieved remarkable results [5] and for this reason can be considered as random binary sequences. For testing purposes web service for data collection has been developed [6].

Table 1

Results of Statistical Test (NIST).

	Random.org	**FlyBit [6]**
Frequency test	0.75075	0.82538
Runs Test	0.98036	0.88365
Serial Test	0.31743	0.82238
Entropy Monobit	0.999999	0.999996
Entropy Bigram	0.999982	0.999995
Entropy Trigram	0.999878	0.999992
Entropy 4x4 matrix	0.999855	0.999992

The results shown in the **Table 1**, on test basis NIST standards, indicate the exceptional quality of randomness of binary sequences. This confirms that there is a great similarity in quality between the proposed source of randomness and so far confirmed sources such as atmospheric noise, time decay processes nuclear material.

2.2 Equivalent scheme

Fig. 2 shows the satellite scenario protocol scheme. The satellite sends signals to Earth, which are collected by legitimate participants (Alice, Bob), but also by Eve. It is expected that because of imperfections (α, β, ε) in the radio wave propagation transmission errors occur, and Alice, Bob, and Eve receive a signal from the satellite, which will be partially modified.

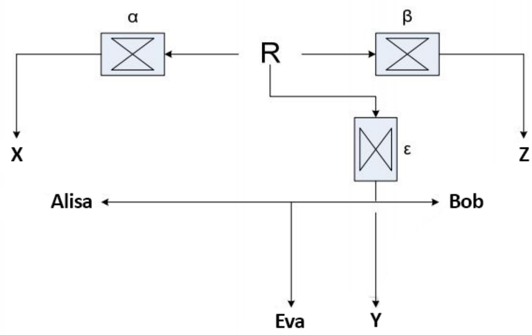

Fig. 2 – *Satellite Scenario.*

This imperfection in the transfer is a condition for safe protocol operation. In our implementation, a satellite replaces a large number of aircraft that broadcast the ADS-B signal continuously, while Alice, Bob, and Eve, in this embodiment, collect airplane data, and perform the decoding and binarization. The required error in transmission in the satellite scenario protocol becomes, in this case, a different number of observed aircrafts for Alice and Bob, but also a different number for Eve. Furthermore, Alice and Bob also introduce their local coincidence, which additionally secures the protocol in the case of Eve's error, and is 0. In this way, a condition for the safe use of the satellite scenario in the proposed equivalent scheme is fulfilled.

3 Experimental Results

The antennas needed to collect the radio signals (omnidirectional antenna) can have different strengths and range. For the implementation of the protocol antennas ranging from 400 km have been used. In addition to the antennas used for collecting the ADS-B systems, radio wave decoders were also needed. From the decoded radio signal, it is possible to extract information about the current latitude and longitude of the plane. Latitude and longitude phase data are encoded in binary code with a total length of 8 bits. Eight-bit representation of one aircraft position becomes the field value of a square matrix of size. The position of a given element in the matrix is also determined by the values of latitude and longitude. With the introduction of geographical data in binary code and storage in a square matrix, it is possible to find common aircraft, which represent the mutual information for the legitimate participants of the protocol.

3.1 Implementation

In order to confirm the initial hypothesis, and achieve the theoretical model, the possibility of application of this protocol in different fields has been explored (the realization in two different areas in which there is an obvious difference in the density of air traffic). Two real cases were chosen as an experiment. The first case is the antenna placement in an area where the flow of air traffic is less dense. In this case, the distance between participants should be smaller. In the second case, the antenna is installed in a place with the highest density of air traffic flow, which allows a greater distance between legitimate participants.

The third antenna is set in order to simulate a potential attacker (Man in the Middle). Alice and Bob as legitimate participants want to exchange secret keys securely via public channels, which would later be used to ensure the confidentiality of the service. Eve, as an attacker, observes their communication passively. For this reason, Eve’s position is placed geographically between the locations of Alice and Bob. All participants have the appropriate equipment and collect data in the same time interval.

Following the collection and processing of data, Alice and Bob can begin the first phase of the protocol, Advantage Distillation.

During this phase of the protocol Eve collected all the messages sent by Alice and Bob. In this way, Eva simulates key exchange with two legitimate sides. After this phase of the protocol, Alice and Bob received bits that represent their shared information, while Eve got two sequences, where one is a joint information between her and Alice, and the other is joint information shared between her and Bob. For the first experimental implementation of the protocol, the territory of Belgrade was chosen. The locations are presented in Fig. 3.

After application of the protocol in Fig. 3 Alice and Bob have a smaller number of mutual bits because of the slightly lower air traffic density. **Table 2** below shows the results obtained. As it can be seen, total between Alice and Bob is 348 bits, while between Alice and Eve it is 319. It should be noted that mutual bits between Alice and Bob and mutual bits between Alice and Eve are completely different, which is confirmed by the Hamming distance (HD = 0.5).

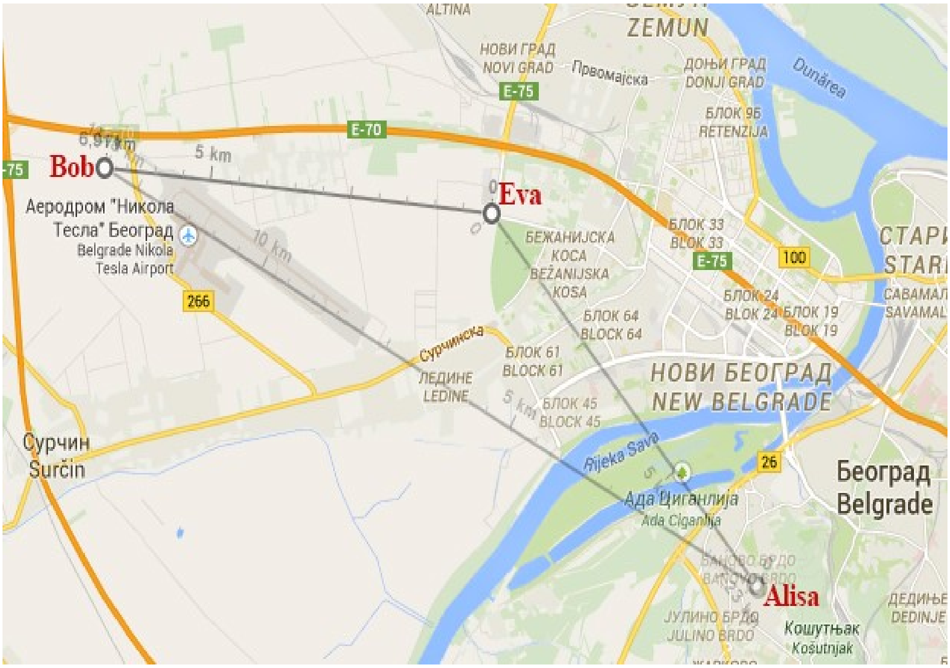

Fig. 3 – *Area 1.*

Table 2
Mutual bits in Area 1.

	Alice (bits)	Bob (bits)
Alice	348	319
Bob	/	129

Another research area is the central area of the German province of Bavaria. The distances between the receivers are several times greater, but the density of air traffic is also much greater. Fig. 4 shows the arrangement of the receivers.

The results obtained by applying the protocol are presented in **Table 3**.

Based on these results, it has been found that the mutual information between the legitimate participants increases as the density of traffic increases. Based on this dependency, it can be said that the crypto key velocity also depends on the traffic density and the position of legitimate protocol participants.

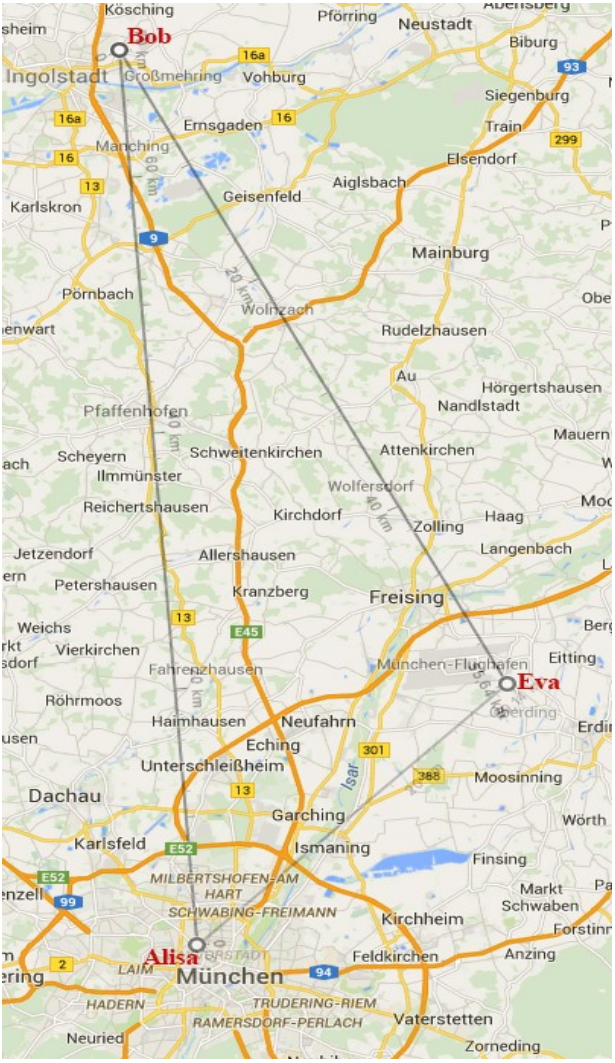

Fig. 4. – *Area 2.*

Table 3
Mutual bits in Area 2.

	Alice (bits)	Bob (bits)
Alice	1452	1256
Bob	/	985

4 Discussion

The channel model presented in this paper implies that the attacker receives noisy versions of legitimate received signals (unknown gatherings of selected aircraft). In addition, before the term "capacity of secrecy" first appeared, theoretical security information found itself in the shadow of the Diffie-Hellman protocol, which dominated the field of security research. This protocol was developed on the basis of public-key cryptography. This type of cryptography relies on mathematical functions which are believed to be hardly calculable.

Authentication of the sender is a tactical assumption in most theoretical contributions of information security, except in exceptional and rare cases, and an established key between Alice and Bob requires authentication at both sides.

However, in a theoretical information protocol an attacker may decide to interfere with some methods of communication-jamming signals. It should be noted that the interference of the signal is not only limited to active attackers. United obstruction, in which one or more of the legitimate users send encoded messages, increases attacker confusion, which effectively influences the increase in the capacity of secrecy.

So far has been assumed that Eve was the passive attacker, who wanted to extract as much information as possible from the channel. However, in addition to a passive attack, Eve has a wide range of active attacks at her disposal. Eve can imitate Alice or cause Bob further confusion, by intercepting traffic and editing messages sent across the channel with noise, or simply hinder Alice and Bob's ability to communicate.

An authentication service in this protocol realization is not available. By combining high level services, it is possible to develop a sufficiently reliable and safe protocol based on theoretical and practical information security.

5 Conclusion

In this study an equivalent scheme of the "satellite scenario" protocol using the ADS-B system, which allows the correlation of binary sequences between the two sides that are exchanging keys via public channels, has been presented.

Ultimately, a protocol for the exchange of encryption keys via public channels has been successfully implemented and tested. The keys can be used for symmetric encryption algorithms (AES, 3DES). There is also the possibility of using a perfect encryption system as One-time pad. However, then it is necessary to make a compromise between the length of the encrypted messages and velocity of keys, which can be achieved with this protocol.

6 Acknowledgment

This work was supported by the Ministry of Science and Technological Development of Serbia through the projects TR32054.

7 References

[1] W. Diffie, M. Hellman: New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. 22, No. 6, Nov. 1976, pp. 644 – 654.

[2] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin: Experimental Quantum Cryptography, Journal of Cryptology, Vol. 5, No. 1, Jan. 1992, pp. 3 – 28.

[3] U.M. Maurer: Secret Key Agreement by Public Discussion from Common Information, IEEE Transactions on Information Theory, Vol. 39, No. 3, March 1993, pp. 733 – 742.

[4] F. Kunzi; R.J. Hansman: ADS-B Benefits to General Aviation and Barriers to Implementation, Report No. ICAT-2011-6, MIT International Center for Air Transportation, Cambridge, MA, USA, 2011.

[5] A. Rukhin, et al.: A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, NIST Special Publication 800-22, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2010.

[6] M.Tatovic; S. Adamovic; M. Milosavljevic: FlyBit: Online Random Number Generator, International Scientific Conference of IT and Business-Related Research – Synthesis 2015, Belgrade, Serbia, 16-17 April 2015, pp. 107 – 111. (In Serbian).