Quantum Key Distribution and Adaptive Protocols.

V. SOULIOTI[1,2], Y. BAKOPOULOS[2], S. KOUREMENOS[2], S. NIKOLOPOULOS[3], Y. VRETTAROS[2] and A.S.DRIGAS[2]
1. Mathematic Department, University Of Patras
2. Department of Applied Technologies NCSR "DEMOKRITOS"
3. National Technical University of Athens
Ag. Paraskevi
GREECE

Abstract: Some new ideas are presented for the improvement of the known QKD protocols and their application to an Internet environment. The full automatization of a technological setup is considered, as a result of the property of most basic QKD protocols to have the appearance of step by step algorithmic procedures and thus to offer themselves to materialization as computer code applications. This is the basis for the creation of a computer network connecting various users to be developed, working as an expert system and making decisions on the best strategy to recognize and counter especially dangerous eavesdropper attacks. The use of robotic technology, knowledge based simulation of the most dangerous and complicated attacks, game theory and neuronic networks to make these decisions, permits the system to adapt its behavior in the face of adverse situations.

Key-words: QKD, Adaptive protocols, security, eaves droppers, simulation, network

1. Introduction

Security on the Internet is a big issue of today [1 – 36], in the days of prospective wireless communications, business transactions, e-learning, e-government, e-health etc. The application of QKD methods and protocols is a new arrival to the networks of today [2], [36] (and references therein).

The authors have done work on Key Creation and Distribution both by classical methods (Chaotic Dynamic Systems Behavior for Random Number Generation) [1], [3], [4], [19], as well as in QKD applications [2], [3], [4].

A QKD protocol is essentially an algorithm, having a finite number of well defined logical steps. Most decisions, about the validity and security of each distributed key, about the quantity of information possibly obtained by potential eavesdroppers, about the interruption of the process and the repetition under better conditions, are taken based on straightforward numerical calculations. With the help of suitable hardware and software, all such processes may be made to work completely automatically, without the intervention of the human users, except to compose and send the messages as in ordinary e-mail. Such an advance in the state of the art of QKD would be by itself welcome, since most users of the Internet are not and should not be concerned with quantum mechanics and the technology involved. The automatization, with the added simplicity, ease of use and speed offered along with traditional QKD security should be motivation enough for the idea to be worth to offer to today's security thirsty market.

The biggest problem is that QKT protocols, being at this experimental stage rather complicated and cumbersome, relying on sophisticated and expensive photonics technology and with little practical experience of their everyday application, are not yet by themselves too attractive for the Internet users. The situation is further complicated by the fact that all protocols so far, having been designed by experimental physicists, are not very well adapted to the peculiarities of the Internet applications. From the point of view of the network engineers, a peer – to – peer protocol like the ones offered today is not the ideal way to exploit the natural advantages of a large scale digital network environment, with its infinitely many and usually unknown to third parties pathways for communicating information from one point to another, or the possibility of using 'proxies', 'decoys' or 'avatars' to break a message into parts and so propagate it through the labyrinth of the Internet with less probability of eavesdropping.

At this stage, where the versatility and chaotic complexity of the Internet and the power of modern digital technology and know - how have the most to offer, where the decision making must be based on concrete facts backed up by fully provable calculations, the automatization of the QKD protocol to be used becomes essential. It is the only way in order to ensure that the decisions and countermeasures necessary for recognizing and countering specific dangerous attacks, so that the users' communications will be as seamlessly and smoothly continued as possible, without compromising either the security or the utility of the services traditionally offered by the Internet. More so if the extension and expansion of these services is to be realized as envisioned by the designers of the Information Society of tomorrow.

2. The Idea of an Adaptive Protocol

The automatization process is easy to realize with state of the art technology. The idea is described in detail in [2] and utilized in a protocol proposed in [36]. The references in [2] describe a variety of protocols and the application of the idea is more or less the same in every case. It is the utilization and exploitation of the advantages such a setup offers for Internet use.

The fundamental facts are the following: Strangely enough, the Internet is considered to be a very unsafe environment for secure services. Especially so, if the services are offered in a wireless environment, where, by common wisdom, "everybody can and will listen in" on what others say or do and act on what he listens to, to his benefit and to the detriment of legitimate users. It seems that the simple fact that one has to know "where" to listen and "what" to listen for, if one is to make any sense out of the chaos of Internet communications that escapes the average mind. If the potential eavesdropper is to eavesdrop at all, he must know beforehand the exact line of communication and use the appropriate attack to intrude upon it. It is here that an adaptive protocol may use the whole potential offered to elude and frustrate the opposition and maintain communication integrity, by making the necessary decisions and minimizing the information available to the eavesdropper to the point where it is essentially useless. The weapons of the defender's arsenal are to change the route or routes of information transfer, making it almost impossible for the eavesdropper to trace it. To break it down to many parts communicated by different routes and modes, so that it will be impossible for the eavesdroppers to get it all. To use proxies, decoy messages of indifferent content, using various obsolete and useless keys, effectively 'spamming' the opposition by the huge volume of nonessential traffic the illegitimate intruders will have to process in order to find the usable content of the real messages. To make use of 'security islands' like the well known Intranet groups within the Internet so that in their collaboration with other distant groups they will extend their security where desired. By depriving the eavesdroppers of any indication of what exactly goes to whom exactly, a user in any form or capacity will be able to supplement his defense arsenal with the formidable weapons of deception and elusion.

All this decision making goes beyond the simple 'continue or abort?' question of a typical QKD protocol. It is essential that the decisions are based on solid facts and are being made in split – second real time, in order for them to be effective. The theory and technology in this decision making must be based on realistic and complete information on the methods and protocols of attack, something that may only be ensured by proper preparation. So it will be essential for the computer systems realizing the adaptive protocol, the 'controllers' of [2], to have the expert ability to recognize the form and danger of the attack and have solid criteria on how to counter it. This may be achieved by the extensive use of detailed simulations, so that the expert systems included in the controller network will be able to be taught beforehand of the various forms of attacks and to be able to learn from experience during everyday routine use and even training in new attack methods as they appear.

This seems the only way to secure communications and business transactions through the Internet. It also seems obvious that a long way is to be traversed if the adaptive protocols are to have a practical application in the foreseeable future. The authors are very hopeful in this direction, considering it an essential part of the Internet of the future.

3. Examples of Adaptive Methods

One of the most dangerous forms of attack against any kind of protocol is the; split universe' attack. In this situation, Eve, an adversary user, wishes to eavesdrop on the conversations carried out by two other users, Alice and Bob. She intercepts their lines of communication and receives all messages they are trying to send. Each of them believes that he or she is talking to the other, and that all messages is sending are reaching the other without intervention. What happens if reality is that they are both exchanging messages from Eve, who is masquerading either as Alice or as Bob, depending on the situation. If Alice and Bob attempt to apply a QKD protocol for secure communication, they will supposedly send each other a number of light signals. In fact, Eve receives the signals from Alice and, posing as Bob, establishes an "Alice – Eve" communication line, by the application of the QKD protocol. Simultaneously, Eve establishes a different line of communication with Bob, sending him the quantum signals required by the protocol and, posing as Alice, proceeding to carry out all various tasks required for an "Eve – Bob" communication line.

This kind of attack has a weak point. If Alice and Bob happen to exchange an encrypted message through a line not intercepted by Eve, the result will be that the receiver will be unable to decrypt it, since the appropriate encryption – decryption code will not be available to the recipient but only to the sender and Eve. As a result, Alice and Bob will understand that their 'secure' communication has been compromised and take appropriate action.

In a large area network environment, the potential lines of communication are so many and the network architecture so complex that it is unconceivable that some eavesdropper will be able to carry out a 'split universe' attack against a pair of users. All that will be needed to neutralize such a possibility is to use a simple scheme of varying their communication routes when they are applying their protocol. They might use some kind of random process in alternating their communication lines and they should 'diffuse' their communication by splitting it in parts and sending them over various routes. It would be especially useful to make use of intermediate helpers, who would receive their part of the message accompanied with a note of the kind: 'Please send this to Bob by tomorrow noon'. This note might be encrypted by one of the usual public keys, as for example within an intranet, quite sufficient to keep it secret for the short time until it was sent. All this should be quite confusing to any eavesdropping system Eve would be applying, essentially 'spamming' it by making it try to monitor too many lines. The situation would by even worse for the eavesdroppers in the case of wireless communications. In that case, it would be inconceivable that Eve should manage to monitor both ground and wireless lines among two users with absolute success.

A similar situation should occur when the legitimate users would face a 'joint' or 'coherent' attack against their QKD protocol. These would very dangerous attacks, as conceived at this time, and their application should require a technology which does not exist yet today but may be available in the near future. The eavesdroppers should be able to copy the qubits sent from Alice to Bob by imperfect cloning, preserve them in some kind of storage space and perform the appropriate measurements when they have enough information from the public communications between Alice and Bob for the realization of the protocol procedures. This way, Eve and her coworkers should be able to take advantage of the entanglement between the clones they sent to the legitimate users and the signals they kept for measurement.

This time, Alice and Bob should 'diffuse', among various routes, not the message but the light signals they intended to use for the distribution of the key. This would need an all optical connection between all Internet users who might participate in the process in one way or another. By today's technology, this may be accomplished using the available hardware of the Internet. {Patent Number: US5953421, Date: 14 Sept. 1999, Inventor: TOWNSEND, PAUL DAVID. (GB). Applicant: BRITISH TELECOM (GB)} [37]. Even better, Alice or Bob might even send, along with the normal signals, a number of dummy 'signals' to uninformed third parties who would not have either the equipment or the knowledge to use them and probably wouldn't even be aware of their arrival. By the use of some open key encryption protocol Alice and the true recipients of her signals would be able to authenticate and refine their keys before Eve had even time to find out her real 'targets' among the throng of signals and messages. In order to minimize the use of the QKD protocol, Alice might initiate communications by the use of a "virtual encryption machine" protocol described in [3] (see also [1], [2], [4], [36]). Then Eve might be unable to discover what signals or messages went to whom, until it would be too late to act.

All this would be a static environment with the decisions taken beforehand and the appropriate actions preprogrammed. But if Alice, Bob and their collaborators had some idea of the technological capabilities and the method of operation of Eve, then the necessary actions should have to be decided upon and executed in real time. Such information might vary from guessing the kind of Eve's attack at a given occasion to what lines is Eve eavesdropping upon etc. This information may be obtained in the following ways: First, the expert system controlling Alice's and Bob's communications [2], [36], would have to be trained trough suitable simulations of the most dangerous attacks. Second, by using specially designed tests and calculation to be performed in real time by the system of controllers [2], [36]. Finally through the experience and information accumulated during everyday application of the system. The system of controllers should have the ability to 'learn' from the attacks it encountered in routine communications. This would mean measuring the amount of losses in the communication lines in ways suitable to the task at hand, or even testing Eve's responses by fake or 'dummy' messages of indifferent content or by applying specialized procedures in order to catch more noise than expected normally.

This information should dictate the appropriate decisions and direct the actions of the adaptable system to face and successfully counter Eve's attacks, or at least to recognize them and alert the human users.

4. Aknowledgements

The authors are grateful to Dr. Nikolaos Papadakos for his help and valuable ideas. To Profs. N. Kalouptsidis, A. Boudis and M. Vrahatis for help and encouragement. To Dr. S. Kotsios for his advice and discussions. To V. Soulioti for invaluable cooperation. To S. Domoxoudis, L. Koukianakis and Y. Loukidis for discussions and suggestions on the functions of the Internet and valuable help.

5. References

[1]. Yannis Bakopoulos, 'Application of Dynamic Systems for Cryptographic Key Distribution' 15th Congress on Nonlinear Dynamics, Chaos and Complexity Patras Aug. 19 – 30, 2002 (A. Bountis)

[2]. Yannis Bakopoulos, Yannis Vrettaros, Athanasios Drigas, 'An automatic process for the reliable and secure creation and distribution of quantum keys' National Patent No 1003891, OBI, 2002.

[3]. Yannis Bakopoulos, Vassiliki Soulioti, 'A protocol for secure communication in digital networks' National Patent No 1004308 OBI, 2003;

[4]. Yannis Bakopoulos, Vassiliki Soulioti, 'A protocol for secure communication in digital networks' PCT/GR 03/ 00035 2003

[5]. L. O Chua. and T.Lin, (!988) IEEE Trans. CAS 35, pp. 648 – 658.

[6]. Robert L Devaney., Physica 10D (1984) pp. 387 – 393.

[7]. O. Feely and L. O. Chua 'Nonlinear Dynamics of a class of analog - to - digital converters', Int. J. Bifurcation and Chaos, Vol. 2, 1992, pp. 325 – 340.

[8]. Orla Feely "Nonlinear Dynamics and Chaos in Sigma – Delta Modulation"., Journal of the Franklin Institute Vol. 331B, No. 6, 1995 pp. 903 – 936.

[9]. Orla Feely 'Nonlinear Dynamics of Chaotic Double-Loop Sigma Delta Modulation' , ISCAS 1994: pp.101-104

[10]. T Habutsu. et al. 'A secret key cryptosystem by iterating a chaotic map' International Conference on the Theory and Application of Cryptographic Techniques, Springer Verlag, DE pp 127 – 140, XP000607774

[11]. Leo P. Kadanov, and Chao Tang, Proc. Natl. Acad. Sci. USA Vol. 81, pp. 1276 – 1279, February 1984, Physics.

[12]. K. Karamanos "Entropy analysis of substitutive sequences revisited" J. Phys. A, Math. Gen. 34, (2001) 9231 – 9241.

[13]. Stelios Kotsios and Orla Feely, NDES Congress Spain '96.

[14]. Stelios Kotsios and Orla Feely 'The model – matching problemfor a special class of discrete systems with discontinuity'IMA Journal of Mathematical Control & Information (1998) Vol. 15, pp 93 – 104

[15]. Stelios Kotsios 2000 Nonlinear Dynamics 22 pp.175 – 191 (and refs therein)

[16]. George Marsaglia "A Current View of Random Generators" Keynote Address, Computer Scienѕe and Statistics: 16th Symposium on the Interface, Atlanta, 1984 (It appeared in "The Proceedings" of the Conference, published by Elsevier Press).

[17]. S. Papadimitriou, A. Bezerianos, T. Bountis, G. Pavlides, "Secure Communication protocols with

discrete nonlinear chaotic maps", Journal of Systems Architecture, Vol. 47, No 1, 2001, pp. 61 – 72.

[18]. James Rössler et al., PHYSICAL REVIEW A, VOLUME 39, NUMBER 11, JUNE 1 1989, pp.5954 – 5960.

[19]. V. Soulioti 'A study on Discrete Dynamic Systems with a linear part and discontnuity', 15th Congress on Nonlinear Dynamics, Chaos and Complexity Patras Aug. 19 – 30, 2002 (A. Bountis)

[20]. Richard J. Hughes et al 'Method and apparatus for free space quantum key distribution in daylight' US 2001/055389, December 27, 2001.

[21]. Yuan et al 'Method and system for establishing a cryptographic key agreement using linear protocols', US 5 966 444, Oct. 12 1999

[22]. Tohru Kohda et al 'Enciphering/Deciphering apparatus and method incorporating random variable and keystream generation' USPatent 6 014 445 Jan 11, 2002.

[23]. L. O. Chua and T. Lin, 'Chaos in digital filters', IEEE Trans. Circuits and Systems, Vol 35, pp. 648-658 (1988).

[24]. L.O. Chua and T. Lin, 'Fractal patern of second order non-linear digital filters: Anew symbolic analysis', International Journal of Circuit theory and Applications, Vol. 18, pp. 541-550, (1990).

[25]. L.O. Chua and T. Lin, 'Chaos and fractals from 3rd order digital filters', International Journal of Circuit theory and Applications, Vol. 18, pp. 241-255, (1990).

[26]. Zbigniew Galias and Maciej J. Orgozalec, 'On symbolic dynamics of a chaotic second-order digital filter', International Journal of Circuit theory and Applications, Vol. 31, pp. 401-409, (1992).

[27]. Zbigniew Galias and Maciej J. Orgozalec, 'Bifurcation phenomena in second-order digital filter with saturation-type adder overflow characteristics' IEEE Transactions on Circuits and Systems, Vol. 37, No 8, pp.1068-1070, (1990)

[28]. Chai Wah Wu and Leon o. Chua, 'Symbolic dynamics of piecewise-linear maps', IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing, Vol. 41, No 6, (1994).

[29]. Chai Wah Wu and Leon o. Chua, 'Properties of admissible symbolic sequences in a second order digital filter with overflow non-linearity', International Journal of Circuit theory and Applications, Vol. 21, pp. 299-307, (1993).

[30]. A. Ammar, A. S. S. El – Kabbany, M. I. Youssef and A. Emam, 'A Novel Secure Image Ciphering Technique

[31]. Stamatios V. Kartalopoulos, Secure Optical Links in the Next Generation DWDM Optical Networks, WSEAS TRANSACTIONS. on COMMUNICATIONS. Issue 2, Volume 3, April 2004. ISSN 1109-2742

[32]. Chandra B. Panday and Nikos Mastorakis, "Secure Protocols for Variety Cash Transactions", WSEAS Transactions on Computers, Issue 1, Volume 3, October 2002, pp.195-200, WSEAS Trans. on Communications, April 2004

[33]. Nikolaos Bardis, Echoplex Error Control System Using Avalanche Transformations, WSEAS Trans. on Communications, April 2004,

[34]. N.G. Bardis, A.P. Markovskyy, M. Mitrouli, A. Polymenopoulos, Methods for Design of Balanced Boolean Functions Satisfying Strict Avalanche Criterion (SAC), WSEAS Trans. on Communications, April 2004

[35]. Chih-Ta Lin, Hira Sathu and Donald Joyce, Network Security of Wireless LANs in Auckland's Central Business District, WSEAS Trans. on Communications, April 2004

[36]. Nikolaos Papadakos, Quantum Information Theory and Applications to Quantum Cryptography, arXive: quant – ph/ 0201057 v1 (2002)