Meteor Time Transfer and Meteor Cryptography

V. Sidorov, A. Karpov, V.Korneev
Kazan State University
Kazan, Russia Federation
vladimir.sidorov@ksu.ru

A.Nasyrov
Tattransgaz
Kazan, Russia Federation
almaz.nasyrov@rambler.ru

Abstract— We show that peculiar properties of meteor wave propagation allow construction of radio channel that may deliver transfer of data with theoretically perfect protection from eavesdropping. Method uses natural stochastic process that is generated only for two communicating participants so that it is not available for possible cryptanalysis. Possible eavesdropper can not reproduce measurements that have been performed by participants at their particular locations, due to mirror-like channel properties and random positions of each meteor trail. The suggested method of data protection can be used, for example, for theoretically absolutely secure way of key exchange.

I. INTRODUCTION

Till now was considered, that protection of the information transmitted on the big distances, can be provided only with deep enciphering, and the information is inaccessible so far as while the key of enciphering is unknown. The connection channels were considered easily accessible to the analysis.

However the global control of all radio emissions and development powerful cryptanalytic systems plus no predictable successes of millions intruders allow to suppose, that only mathematical methods cannot guarantee human rights or communities on non-distribution of the private information.

Channel level of the information protection. The recognized successes of the American scientists [1] in development of quantum cryptography have shown that now there is also other way: a way of the perfect protection of a connection channel. But quantum cryptography is not a unique way of creation of completely protected connection channel. Other way is opened with the meteor phenomena and meteor precision time transfer.

II. METEOR PRECISION TIME TRANSFER.

An opportunity to use a meteoric radio channel for precision time transfer has specified V. Lattore and G. Jonson in 1964 year [2]. However the narrow pass band of the radio channel which was adapted for transfer of the information has not allowed to achieve errors smaller, than 0,3-0,5 micro seconds. Due to efforts of the Kazan and Kharkov [3] researchers by 1980 years, accuracy of time transfer through meteoric traces has improved up to 50 ns due to application of more broadband devices and automatic selection of meteoric reflections with required properties. In the 1981 have been published the work [4] in which for the first time it has been shown, that the reciprocity of conditions of meteoric radiowave propagation for a significant part of meteoric reflections is kept to within a phase of carrier frequency. This property, which is not carried out for the decameter waves, has allowed setting the task of increase in accuracy of meteor time transfer with errors less 1ns. At such high accuracy of time measurement there was a problem of its using as the determining factor but here was the problem of short-term instability of quantum standard frequency. The real time scales action were supported on a nanosecond level by using automatic control of a secondary time scale on base of results of meteoric measurements .

For a filtration non-uniformly distributed and non-equal measurements which was delivered by the meteoric channel, it was used Kalman filter for the experimental researches executed by the Kazan university with using of a measuring complex - Kama 5 on line Kazan - Mendeleevo in 1992 [5].

On fig 1 the distribution of mistakes of an automatic control have shown, that the most part of the time control mistake of a time scale are less 0,3 ns. It was supposed, that at the moment of meteor measurement a control was carried out by using interval weighing of some last measurements, and within intervals between meteors it was carried out by the Kalman forecast.

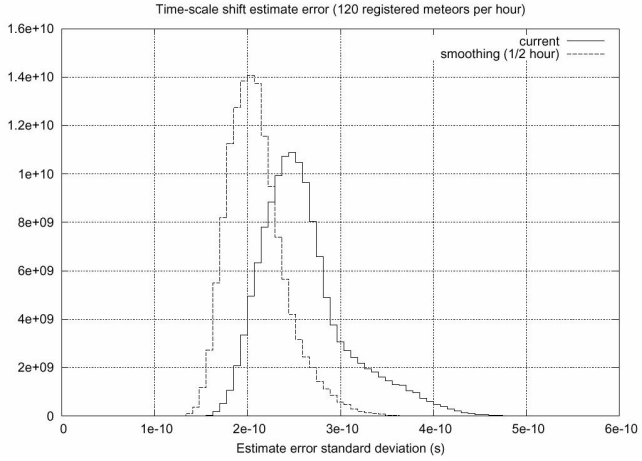

Figure 1. Errors of automatic control time transfer for 120 meteors reflection per hour

III. METEORIC CRYPTOGRAPHY

Meteoric nanotechnology of exact time transfers has allowed to solve another problem of the perfect protection of the information at a channel level by using well-known Shannon theorem of the perfect secrecy [6]. Shannon perfect secrecy requires identical and unitary used keys which are necessary for its realization on two ends of a radio line. Besides, the size of a key should be big or equal to the size of the message. The problem of keys delivery is the weak spot of this way.

The idea of meteoric cryptography [7]is to refuse transfer of a key to the other end of a radio line. Instead of it is to organize generation of identical natural-stochastic process on two ends of a meteoric radio line so that to use as a key for accomplish enciphering of the transmitted information by Shannon. It is process of changes of time of radiowaves propagation from one meteoric reflection to another. The reciprocity of conditions of meteoric wave propagation provides similarity of time propagation on both ends of a radio line.

Successful realization of this idea appeared possible, due to the following unique properties of meteoric distribution of radiowaves:

- Random facts of occurrence of a meteoric trails, both in time, and in space.
- Mirror reflection of radiowaves: for concrete points of reception and transfer: each meteoric trail will have mirror point [8] which position will be random in space. As result there will be random time of wave propagation on a way *A* (transmitter) *M* (a mirror point on a trail) *B* (receiver) (Fig 2).
- Wide scattering of propagation time of a signal $\delta\tau$ from a meteor to a meteor, caused in random coordinates of meteor trails.
- Wide scattering of angular directions of the radiowaves arrival, also determined in random coordinates of points of reflection.
- Reciprocity is identical with experimentally proved accuracy ($\approx$ 0.5ns) time of a signal propagation τ in both directions within the limits of one meteoric reflection: ($\tau_{AB} \approx \tau_{BA}$).
- Identical personal set of the radio reflections providing a radio communication of persons in two concrete items, not repeating for other pairs the persons who are settling down in other items.

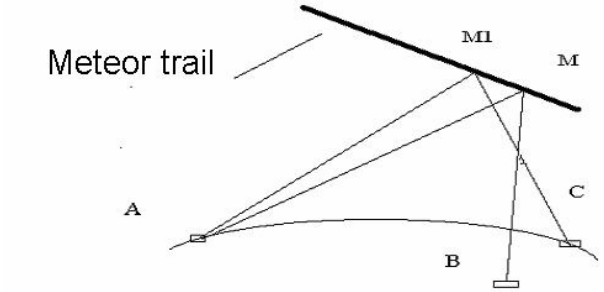

Figure 2. Mirror reflection of radiowaves from a meteor trail

IV. THE CIRCUIT OF THE ORGANIZATION OF A RANDOM KEY GENERATION WITH USE OF METEORIC REFLECTIONS

Key information Z = (… tP_{i-1}, tP_i) is created by sequence of measurements of counter time of distribution of radiowaves propagation tP_i for different meteoric trails and moves to coder at item A and to decoder at item B. For maintenance of the perfect protection of message X the ciphered message Y=Ez (X) is construction on the basis of application of code Vernam [9].

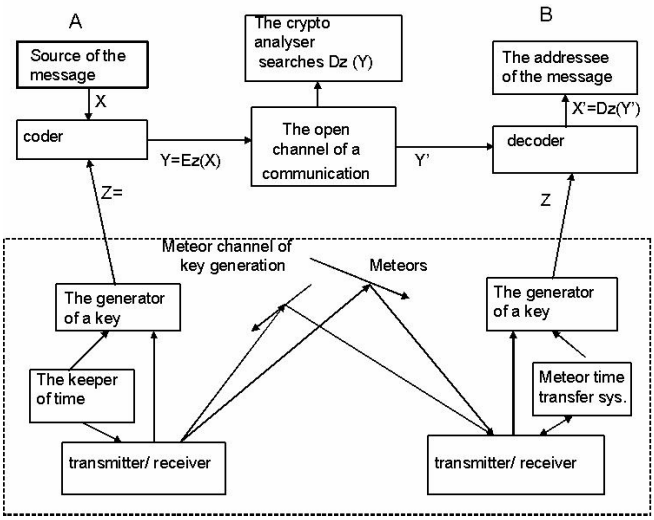

Figure 3. Function chart of meteor cryptography

It is not possible to decipher by eavesdroppers the information transmitted in such a way since for any other pair of correspondents sequence Z = (… tP_{j-1}, tP_j) will be different. Besides, to get such a sequence by registration of radiations from any remote item on a surface of the Earth, from the plane or from Space is impossible, as any key information does not radiated.

Moreover, attempt of cryptanalytic "to guess" the information accepted by the correspondent about time of propagation by using reception by independent receivers near correspondent zone is failed because of disorder of arrival corners of meteor echo signals and impossibility to resolve of ambiguity of phase measurements even at small distance of measuring aerials system of crypto analytic from the aerial of the interesting his correspondent.

On Fig 4 shown the card of uncertainty of the angular resolution which is resulted at removal of measuring aerials of crypto analytic on 11 λ from the aerial of the correspondent.

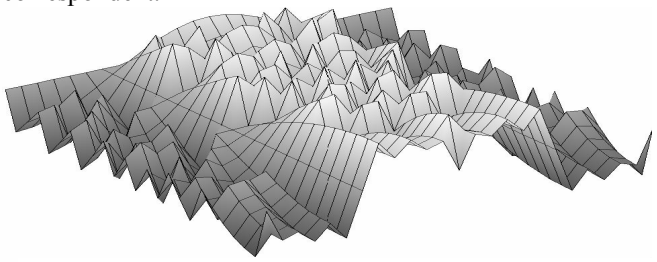

Figure 4. Angular uncertainty of a phase for the aerial of cryptoanalitic on distance of 11 lengths of waves from the aerial of the correspondent

V. Experimental check of a meteoric cryptography method

For check of a method of meteoric cryptography, experiment on phase synchronization of time scales on a meteoric radio line Mendeleevo-Kazan [5] has been used.

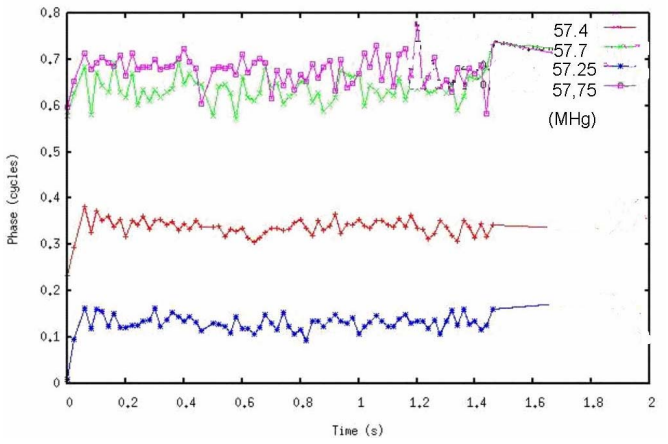

Figure 5. Example of reciprocity of conditions of direct and return propagation on phases of carrier frequencies. One large reflection, some frequencies.

Times of radiowaves propagation were measured, and results of measurement were subtracted one of another.

On Fig 5 the example of registration of the long meteoric received reflection is shown. It is visible, that in the beginning of reflection of a condition of reciprocity are not carried out because of effect of formation of a meteoric trail, however then the difference of times of propagation remains to a constant to within noise of the receiver. So there is an opportunity not only to measure time of propagation, but also to check up result of repeated measurements. Besides it is possible to show, that if for enciphering and decoding can be used not process of measurements, but to apply irreversible transformation of historical lines of measurements, so-called hash transformation, there is an opportunity to carry out accomplished mutual correspondents identification, to provide check of correctness of generation of a key and to protect system meteoric cryptography from rare cases of interception of a part of the key information.

VI. Conclusion

The meteoric cryptography is the probable candidate for realization of the perfect channel protection of the information by its transfer on distances up to 1800-2000 kms on open lines.

The size of the key information is unlimited, and productivity of its generation is defined by accuracy of synchronization and number of registered meteoric reflections.

The key at meteoric cryptography is natural-random. Before the end of procedure of mutual identification the key is not known, it is used unitary, automatically destroyed after using. It cannot be stolen or sold.

The suggested method of data protection can be used, for example, for theoretically absolutely secure way of key exchanges.

References

[1] C.Bennett, F.Bessette, G.Brassard, L.Salvail, J.Smolin "Experimental quantum cryptography" Journal of cryptology, 1992, V.5, N1, p.3-28

[2] Lattore V., Jonson G., "Time synchronization techniques" IEE INT.Conv.Rec 1964. Part 6.P.422-428

[3] I. Antipov, J. Koval, V .Obelchenko, Development of the theory and perfection of radiometeoric systems of communication and synchronization // Kharkov, publishing house-Collegium, 2006 (Russian)

[4] Kurganov,A.R., Ovchinnikov, V.V., Pleukhov A.N., Sidorov V.V., Khusiashev R.G., "Experimental researches of phase instability and relative phase nonreciprocity at meteoric and Es propagation of radiowaves," Meteornoe rasprostranenie radiovoln.-Kazan, 1981 - №. 17, pp 30-39 (Russian)

[5] Epictetov L.A., Merzakreev R.R., Sidorov V.V. "Application of Meteor Burst Equipment for High Precision Comparisons of Time and Frequency Standards," Proc. of 7th European Frequency and Time Forum (EFTF'93), Neuchatel, 16-18 March 1993, pp. 413-416.

[6] Shannon C.E. Communication theory of secrecy systems. Bell Syst. Tech. J., V.28, 1949, P. 656-715.

[7] Karpov A.V., Sidorov V.V., "Way of protection of the information in a meteoric radio channel by enciphering by stochastic natural process," the patent of the Russian Federation № 2265957.-МПК6 H 04 B 7/22, H 04 L. The bulletin. №34 , 10.12.2005.

[8] Villard O.G., Peterson A.M., Manning L.A., Eshleman V.R. "Some properties of oblique radio reflections from meteor ionization trails," J.Geophys.Res.- 1956.- V.61.- P.233-249.

[9] G.S.Vernam "Cipher printing telegraph systems for secret wire and radio telegraphic communications," J. Amer. Inst. Elec. Eng. Vol.55, p.p.109-115, 1926.