Threshold scheme to share a secret by means of sound ranging[1]

Sergij V. Goncharov[2]

Abstract

In this short note we consider the scheme to share a bitstring secret among n parties such that any m of them, cooperating, can reconstruct it, but any $m-1$ of them cannot (a so-called (m,n)-threshold scheme). The scheme is based on the sound ranging problem, which is to determine the unknown position of the source and the unknown instant when it emitted the sound from known instants when the sound wave reached known sensors. The features are 1) shadows are computed not so much by the secret dealer, but rather by environment where the sound propagates, so the amount of computations performed by the dealer is $O(1)$ instead of $O(n)$ as $n \to \infty$, and 2) the dealer does not need to establish separate secure channel with each party. There are severe inherent drawbacks though.

MSC2020: Pri 94A62, Sec 65J22

Keywords: secret sharing, threshold scheme, sound ranging, TDOA

Introduction

Secret sharing is an important topic in cryptology ([6], [24, Sec. 3.7, 23.2], [28]). In particular, for any $m, n \in \mathbb{N}$ such that $m \leqslant n$, the (m,n)-*threshold scheme* (TS) for bitstring data is as follows: there is a bitstring *secret* $S \in \{0,1\}^l$ and n *parties*, or *shareholders*. Let them be enumerated from 1 to n. To i-th party, the *shadow*, or *share*, $s_i \in \{0,1\}^{l_i}$ is given. Each party knows only its shadow. The main requirement is that any m parties can fully reconstruct S from their m shadows, — that is, S is uniquely determined by $\{s_{i_1}, s_{i_2}, \dots, s_{i_m}\}$, where all i_j are distinct, — but any $m-1$ parties cannot do it, even if they have "infinite" computing power. Stronger requirement is that $m-1$ parties cannot obtain *any* (non-zero) information about S.

Various schemes of this kind were proposed in due course, the first being Blakley's [7] and Shamir's [27], then e.g. Asmuth-Bloom's [3] and Mignotte's [22]; the survey [6] references many more. See also [29] for a quantum flavour. Usually the *dealer* (who knows S initially) computes shadows and distributes them among parties. The distribution can be random, but shadows must be computed by the dealer. Then each shadow must be given to corresponding party, perhaps transmitted through encrypted channel that is accessible to this party and not to other parties.

For example, in Blakley's vector scheme [7] $S \in \mathbb{R}^m$ is a secret[3] and s_i are $(m-1)$-dimensional hyperplanes in $\mathbb{R}^m$, or rather the parameters that define them (i.e. $s_i = (a_{i1}, \dots, a_{im}, b_i)$, which defines the hyperplane $\{x \in \mathbb{R}^m \mid \sum_{j=1}^{m} a_{ij}x_j + b_i = 0\}$) such that any m of s_i have the single common point S. The intersection of any $m-1$ hyperplanes s_i is an infinite 1-dimensional straight line in $\mathbb{R}^m$, thus the main requirement holds. So, $\{a_{ij}\}$ and $\{b_i\}$ must be computed by the dealer for all $i = \overline{1,n}$ and provided to parties. The amount of computations is $O(n)$ as $n \to \infty$.

Sound ranging (SR), or *source localization*, or *time-difference-of-arrival* (TDOA) problem arises when there is an unknown point $\mathbf{s}$ of space, called *source*, which at unknown instant t_0 of time emits the sound wave. The wave propagates through space and reaches *sensors*, which are known points $\{\mathbf{r}_i\}$, at known instants t_i. The problem is to determine $\mathbf{s}$ and t_0 from $\{\mathbf{r}_i, t_i\}_{i \in I}$. There are numerous applications of this problem in acoustics [30], sensor networks [20], warfare [4] etc., and many methods to solve it have been proposed, see e.g. [10, Sec. 1], [16, Sec. 9.1] for references.

[1] Part of "Decaennead: ruminations about sound ranging in abstract space(time)s and related themes" project

[2] Faculty of Mechanics and Mathematics, Oles Honchar Dnipro National University, 72 Gagarin Avenue, 49010 Dnipro, Ukraine. *E-mail: goncharov@mmf.dnu.edu.ua*

[3] To be more precise, a secret is encoded in one of S coordinates, not in all of them, otherwise the scheme loses the so-called information theoretic security.

Combining these notions, the dealer packs a secret into bits of numerical values of the emission instant and/or the source coordinates and emits the sound at this instant at these coordinates. How many such bits are available depends also on the accuracy of the measurements attainable by parties. Each party has a single sensor that it places somewhere in space; as we should see below, the constraints on the entire set of sensors are very light. To determine a secret, m parties share positions of their sensors and instants when sound reached them, solve SR problem, and extract bits of a secret. For $m-1$ or less parties, possible solutions make an unbounded continuum and a secret cannot be determined exactly.

Of course, there are accompanying shortcomings, some common to threshold schemes and some specific to this approach. See "Drawbacks" below.

1 SR-based TS

For the sake of simplicity we apply the "classic" SR in homogeneous and isotropic $\mathbb{R}^{m-1}$, although the SR problem and the methods to solve it exist for other spaces, non-Euclidean as well (see e.g. [15]). Also, the space(time) can be, in a sense, virtual, where dealer and parties place their "avatars" and the wave propagation is computed by the hardware+software environment that hosts the space(time).

Let $\mathbf{s} = (s_1; \ldots; s_{m-1}) \in \mathbb{R}^{m-1}$ be the emitting source and $t_0 \in \mathbb{R}$ be the instant of sound emission. We assume that the dealer, who *is* the emitter or *affects* the emitter, has complete control over certain part of binary representation of at least some s_j and t_0, from k_s-th to k_e-th bit. For example, the dealer can make it so that t_0 is anything she/he needs from □□.□00000□□ to □□.□11111□□, where □ bits are not significant. The total number of bits controlled by the dealer must be enough to pack the secret S, in a way (layout) known both to dealer and to parties.

Having packed S into these bits, the dealer emits the sound accordingly.

The sound propagates through space and eventually reaches all n sensors. Without loss of generality, we assume that the speed of sound is 1.

i-th party, or, to be more precise, its sensor, whose position is $\mathbf{r}_i = (r_{i,1}, \ldots, r_{i,m-1}) \in \mathbb{R}^{m-1}$, records the time when the sound reaches it, which is

$$t_i = t_0 + \sqrt{\sum_{j=1}^{m-1} (r_{i,j} - s_j)^2} \quad \Rightarrow \quad (t_i - t_0)^2 = \sum_{j=1}^{m-1} (r_{i,j} - s_j)^2, \quad i = \overline{1,n}$$

Similarly to s_j and t_0, i-th party is able to determine $r_{i,j}$ and t_i only up to some binary digit due to measurement errors. We assume that the accuracy is sufficient for the next steps.

Consider any m parties and, without loss of generality, re-enumerate them as $1, \ldots, m$. When they share their SR data, they obtain the equation set with m equations related to $t_1, \ldots, t_m$ and m unknowns $s_1, \ldots, s_{m-1}, t_0$. Following the well-known procedure (see e.g. [13, Sec. II]), they subtract the m-th eq. from the rest and obtain

$$\begin{cases} t_i^2 - t_m^2 - 2t_0(t_i - t_m) = \sum\limits_{j=1}^{m-1} \left[r_{i,j}^2 - r_{m,j}^2 - 2s_j(r_{i,j} - r_{m,j}) \right], \quad i = \overline{1, m-1} \\ (t_m - t_0)^2 = \sum\limits_{j=1}^{m-1} (r_{m,j} - s_j)^2, \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} \sum\limits_{j=1}^{m-1} \underbrace{(r_{i,j} - r_{m,j})}_{a_{ij}} s_j = \underbrace{\frac{1}{2}\Big[\sum\limits_{j=1}^{m-1} (r_{i,j}^2 - r_{m,j}^2) - t_i^2 + t_m^2 \Big]}_{b_i} + \underbrace{(t_i - t_m)}_{c_i} t_0, \quad i = \overline{1, m-1} \\ t_0^2 - 2t_0 t_m + t_m^2 = \sum\limits_{j=1}^{m-1} \left[s_j^2 - 2s_j r_{m,j} \right] + \sum\limits_{j=1}^{m-1} r_{m,j}^2, \end{cases}$$

Denoting $A = \|a_{ij}\|_{1 \leqslant i,j \leqslant m-1}$, $B = (b_1 \dots b_{m-1})'$, $C = (c_1 \dots c_{m-1})'$, the set of first $m-1$ equations is $AX = B + Ct_0$, where $X = (s_1 \dots s_{m-1})'$ and $'$ means transposition. By Kramer method, this equation has a unique solution if and only if $\det A \neq 0$, which, in turn, is equivalent to $\{\mathbf{r}_i - \mathbf{r}_m\}_{i=1}^{m-1}$ being linearly independent (i.e. a basis of $\mathbb{R}^{m-1}$), and the coordinates of that solution are $s_j = \det A(j \leftarrow B + Ct_0)/\det A$, $j = \overline{1, m-1}$, where $A(j \leftarrow B + Ct_0)$ is A with j-th column replaced by $B + Ct_0$. Linearity implies $s_j = u_j + v_j t_0$, where $u_j = \det A(j \leftarrow B)/\det A$ and $v_j = \det A(j \leftarrow C)/\det A$.

Our m parties then substitute these s_j represented through t_0 into m-th equation and, after trivial transformations, obtain a quadratic equation in t_0, $d_2 t_0^2 + d_1 t_0 + d_0 = 0$. Here we additionally assume that from the pair of its real roots, $t_0 = \frac{1}{2d_2}(-d_1 \pm \sqrt{d_1^2 - 4d_0 d_2})$, they can determine the true one, using e.g. physical reasonings like $t_0 \leqslant t_i$, although in general case both roots can satisfy such constraints.

Thus they have determined $s_1, \dots, s_{m-1}$ and t_0, with an accuracy (we suppose) sufficient to extract the original bits of S and reconstruct it.

Linear independency of $\{\mathbf{r}_{i_j} - \mathbf{r}_{i_m}\}_{j=1}^{m-1}$, required by Kramer method, for any m-element subset of $\{\mathbf{r}_i\}$ is equivalent to $\dim\{\mathbf{r}_{i_1}, \dots, \mathbf{r}_{i_m}\} = m-1$. Put differently, there must be no m sensors that belong to some $(m-2)$-dimensional hyperplane of $\mathbb{R}^{m-1}$.

If the number of parties if less than m, then the equation set is underdetermined. In general case, there is a continuum of $(s_1, \dots, s_{m-1}, t_0)$ satisfying it, and the bits of S cannot be determined in their entirety. However, similarly to Blakley's TS, from information theoretic security point of view it is better to encode S in only one of $s_1, \dots, s_{m-1}, t_0$ values.

Partitioning. In case of very large secret S, it can be split into several parts, and each part is shared through the corresponding emission.

Drawbacks. We elaborate on those specific to this TS, although there are more common ones, such as: 1) Unfair party lies to others. If others are fair, this party can reconstruct S for itself, while others cannot. *Counteraction:* "lie detector"; 2) The scheme does not work without the dealer who knows an entire secret beforehand; 3) Unfair party spies on the dealer and thus obtains $\{s_j\}$, t_0 directly; 4) Members of different parties communicate and some information leaks.

Now, back to specific drawbacks:

♦ Unfair party can use more than 1 sensor. m non-coplanar ones suffice to ignore other parties. Also, several unfair parties can cooperate. *Counteraction:* more intense control over parties.

♦ A group of less than m parties, analyzing the continuum of $(s_1, \dots, s_{m-1}, t_0)$ that satisfies their share of SR data, can guess more probable values of certain bits of a secret, even if not all of them. How much they can guess depends on the shape of that continuum, which, in turn, depends on relative positions of their sensors and the source. For example, in the part of that continuum that is cut by "the source is not farther than 10^4 m" constraint, 2nd bit after the point is 1 in 70% cases and 0 in 30% cases. *Counteraction:* use higher bits of s_j and t_0.

♦ Outside/unauthorized parties beside the initial n ones can use their sensors and then reconstruct S or cooperate with authorized ones. *Counteraction:* the dealer and authorized parties preconcert the sound, and the dealer emits many sounds, only one of them encoding the true S. At that, all sounds must encode verisimilar secrets, not "garbage", because the number of sounds the dealer is able to emit during limited time is not just finite but relatively small.

♦ False sounds. Even if dealer and parties preconcert the sound, an adversary can make it "jump" by appropriately placing the microphone-transmitter (MT) and the receiver-loudspeaker (RL). When true sound reaches MT, it is transmitted with the speed of light (orders of magnitude faster than sound) to RL, which replays it as a false sound that reaches some nearby sensor earlier than the true one. Now the corresponding party has to distinguish false and true sounds, otherwise the equations will be inconsistent or the solution will be distorted. Surely, an adversary can install many MT-RL pairs. *Counteraction:* ability to distinguish original and replayed sound. Or use light instead of sound.

♦ An adversary suppresses sounds or alters atmosphere so that sound speed becomes variable.
Counteraction: control over the part of environment surrounding the dealer and the parties.

Add combinations of the above.

Conclusion

The TS that we have considered here shifts the "burden" of shadows computation from the dealer to the environment where the dealer and the parties reside. On the one hand, it simplifies the dealer's task; on the other hand, it complicates control over distribution of shadows. In traditional TSes, when the dealer transmits a shadow over secure channel to a party, and does it for all parties over their individual separate channels, the result is quite definite, particularly because an unfair party cannot obtain more that its own shadow without cooperating with other parties (assuming that individual channel's security is not broken). In SR-based TS, such party can do it, and several unfair parties bring additional forms of "unforeseen" interactions. To mitigate them, the underlying environment must be highly controllable, and who controls the controllers?

Meanwhile, from practical point of view, the principal obstacle to the usage of this TS is perhaps the fixed dimensionality $m-1$ of the "real" space that the dealer and the parties inhabit. Unless there is a virtual environment, whose reliability introduces its own complications.

References

[1] X. Alameda-Pineda, R. Horaud: *A geometric approach to sound source localization from time-delay estimates.* IEEE TASLP **22**:1082–1095, 2014. doi:10.1109/TASLP.2014.2317989

[2] R. Alvarado, M. Mitrea: Hardy Spaces on Ahlfors-Regular Quasi Metric Spaces. Springer, 2015. doi:10.1007/978-3-319-18132-5

[3] C. Asmuth, J. Bloom: *A modular approach to key safeguarding.* IEEE Trans. Inf. Theory **29(2)**:208–210, 1983. doi:10.1109/TIT.1983.1056651

[4] D. Aubin, C. Goldstein (eds.): The war of guns and mathematics: mathematical practices and communities in France and its western allies around World War I. AMS, 2014.

[5] B.B. Baker, E.T. Copson: The mathematical theory of Huygens' principle. Oxford Univ. Press, 1939.

[6] A. Beimel: *Secret-Sharing Schemes: A Survey.* IWCC 2011: Coding and Cryptology, 11–46. doi:10.1007/978-3-642-20901-7_2

[7] G.R. Blakley: *Safeguarding Cryptographic Keys.* Proc. Nat. Comp. Conf. **48**:313–317, 1979. doi:10.1109/AFIPS.1979.98

[8] H.P. Bucker: *Use of calculated sound fields and matched-field detection to locate sound sources in shallow water.* J. Acoust. Soc. Amer. **59(2)**:368–373, 1976. doi:10.1121/1.380872

[9] W. Chiu, B. Chen: *Mobile Positioning Problem in Manhattan-Like Urban Areas: Uniqueness of Solution, Optimal Deployment of BSs, and Fuzzy Implementation.* IEEE Trans. Sig. Proc. **57(12)**:4918–4929, 2009. doi:10.1109/TSP.2009.2026601

[10] M. Compagnoni, A. Canclini, P. Bestagini, F. Antonacci, A. Sarti, S. Tubaro: *Source localization and denoising: a perspective from the TDOA space.* Multidim. Syst. Sign. Process **28(4)**:1283–1308, 2017. doi:10.1007/s11045-016-0400-9

[11] M.M. Deza, E. Deza: Encyclopedia of Distances. Springer, 2009.

[12] J.R. Giles: Introduction to the Analysis of Metric Spaces, Cambridge Univ. Press, 1987.

[13] M.D. Gillette, H.F. Silverman: *A Linear Closed-Form Algorithm for Source Localization From Time-Differences of Arrival*. IEEE Sign. Process Lett. **15**:1–4, 2008. doi:10.1109/LSP.2007.910324

[14] S.V. Goncharov: *On sound ranging in some non-proper metric spaces*, 2019. arXiv:1910.09248

[15] S.V. Goncharov: *On sound ranging in proper metric spaces*. Acta Comment. Univ. Tartu. Math. **24(2)**:205–223, 2020. doi:10.12697/ACUTM.2020.24.14

[16] Y. Huang, J. Benesty (eds.): Audio signal processing for next-generation multimedia communication systems. Kluwer Acad. Pub., 2004.

[17] A.N. Kolmogorov, S.V. Fomin: Introductory Real Analysis (tran.). Dover Pub., 1975.

[18] K. Liu, Y. Xu, J. Zou: *A Multilevel Sampling Method for Detecting Sources in a Stratified Ocean Waveguide*. J. Comput. Appl. Math. , 2016. doi:10.1016/j.cam.2016.06.039

[19] A. Louni, K.P. Subbalakshmi: *Who Spread That Rumor: Finding the Source of Information in Large Online Social Networks With Probabilistically Varying Internode Relationship Strengths*. IEEE Trans. on Comp. Soc. Sys. **5(2)**:335–343, 2018. doi:10.1109/TCSS.2018.2801310

[20] G. Mao, B. Fidan: Localization Algorithms and Strategies for Wireless Sensor Networks. Inf. Sc. Ref., Hershey, 2009.

[21] M. Maroti, G. Simon, A. Ledeczi, J. Sztipanovits: *Shooter localization in urban terrain*. Computer **37(8)**:60–61, 2004. doi:10.1109/MC.2004.104

[22] M. Mignotte: *How to Share a Secret*. EUROCRYPT 1982, LNCS **149**, 1983. doi:10.1007/3-540-39466-4_27

[23] M. Robinson, R. Ghrist: *Topological Localization Via Signals of Opportunity*. IEEE Trans. Signal Process. **60(5)**:2362–2373, 2012. doi:10.1109/TSP.2012.2187518

[24] B. Schneier: Applied Cryptography. 2nd ed. Wiley, 1996.

[25] W. Schriever: *Sound ranging in a medium having an unknown constant phase velocity*. Geophysics **17(4)**:915–923, 1952. doi:10.1190/1.1437827

[26] V. Schroeder: *Quasi-metric and metric spaces*. Conform. Geom. Dyn. **10**:355–360, 2006. doi:10.1090/S1088-4173-06-00155-X

[27] A. Shamir: *How to share a secret*. Comm. ACM **22(11)**:612–613, 1979. doi:10.1145/359168.359176

[28] G.J. Simmons: *An Introduction to Shared Secret and/or Shared Control Schemes and Their Application*. In: Contemporary Cryptology: The Science of Information Integrity, 1992. doi:10.1109/9780470544327.ch9

[29] W. Tittel, H. Zbinden, N. Gisin: *Experimental demonstration of quantum secret sharing*. Phys. Rev. A **63(4)**:042301, 2001. doi:10.1103/PhysRevA.63.042301

[30] W.A. Watkins, W.E. Schevill: Four-hydrophone array for acoustic three-dimensional location: Tech. Report. Woods Hole Ocean. Inst., 1971.

[31] W.A. Wilson: *On Quasi-Metric Spaces*. Amer. J. Math. **53(3)**:675–684, 1931. doi:10.2307/2371174