Tatra Mt. Math. Publ. **37** (2007), 49–57

TATRA MOUNTAINS
Mathematical Publications

INTERSECTION ATTACK AND USING DUMMY ADDRESSES

Jędrzej Kabarowski — Mirosław Kutyłowski

ABSTRACT. We consider anonymous communication protocols and the intersection attack exercised against them. We analyze defense strategy of sending extra messages to dummy destinations.

We show that the optimal number of dummy destinations should be determined based on the traffic intensity and the number of the real destinations m as well as on the number of communication rounds we want to participate in. We present an integral expression for computing the optimal value and show examples that it need not to be m, as often believed.

1. Introduction

We consider communication protocols in public networks which deliver encrypted messages to recipients in an anonymous way: the protocol hides the link between the source of the message and its destination. Messages are cryptographically encoded and re-coded on their route. No relationship can be derived from the codes. Privacy protection of this kind is necessary in many practical situations: electronic voting, access to databases with certain medical information, business negotiations and so on.

The case when a single message is sent by each recipient and there is exactly one communication round is well understood and analyzed in the literature. Severe problems occur when communication lasts for a longer time, the users establish and break connections. There are many techniques that help an adversary to break anonymity protocols that would offer provable security in the simplest scenario mentioned above. We analyse a solution, based on using dummy addresses, in order to ensure better anonymity.

2000 Mathematics Subject Classification: 94A60.
Keywords: anonymous communication, intersection attack.
Partially supported by KBN grant 0 T00A 003 23.

2. Intersection attack

One of the simplest, but effective method for breaking anonymity is the intersection attack [3, 5, 1]. It is assumed that a passive eavesdropper observes for each time step which users send anonymous messages and which destinations receive these messages. The adversary does not attempt to knack cryptographic encoding of the messages but only analyzes traffic data. His goal is to reveal the destinations that get messages from Alice.

The main point of a statistical intersection attack [3] is that if Alice is sending a message, then a *random* subset of other users is sending as well. Even if each of the users has its own set of possible destinations, the adversary may treat the remaining users as sending messages at random according to a single probability distribution describing popularity of destinations. On top of that there are messages from Alice; they always have destinations in the set corresponding to Alice. So, if the number of observations is large enough, with simple statistical methods [2] we can filter out the destinations of high frequencies—the destinations of Alice have a fair chance to occur there. In this paper we present more detailed statistical analysis of the attack.

3. Model assumption

We consider a network with N participants exchanging messages. The network supports anonymous communication in the sense that during each round the passive eavesdropper can only learn, for each user, the number of messages sent and received.

For the sake of simplicity we assume that in each turn $b = k \cdot N$ users send messages (k is a constant less than 1). Alice has m potential recipients of her messages, called *friends*. Each time she sends, the recipient is chosen uniformly at random. Communication is in rounds and within a round all messages are delivered.

Let us consider t communication rounds. Let N_P be a random variable denoting the number of messages received by a non-friend and let A_F be a random variable denoting the number of messages received by a friend. Let $B(M, p)$ stand for the number of successes in a Bernoulli process with M trials and success probability p for a single trial. The probability distributions for N_P and A_F are as follows:

$$N_P \sim B\left(t \cdot b, \frac{1}{N}\right), \qquad A_F \sim B\left(t \cdot b, \frac{1}{N}\right) + B\left(t, \frac{1}{m}\right),$$

$$E(N_P) = t \cdot \frac{b}{N} = t \cdot k \ , \ \ Var(N_P) = t \cdot k \cdot \left(\frac{N-1}{N}\right),$$
$$E(A_F) = t \cdot k + \frac{t}{m}, \ Var(A_F) = t \cdot k\left(\frac{N-1}{N}\right) + \frac{t(m-1)}{m^2}.$$

It is needless to point out that even if a single round offers a good level of anonymity, the adversary may collect statistical information from many rounds, when Alice is active. He may analyse differences between the rounds when Alice is active and when not. Let us remind the definition of a *quantile:*

Definition 3.1. *q_α is a α% quantile of a random variable X if* $\Pr(X \leq q_\alpha) = \alpha$.

Based on a statistical analysis, an eavesdropper may choose the following strategy: if some destination obtains more messages than 95 % quantile from N_P distribution (that is this destination obtains such a number of messages that if it is a normal destination, probability of that case will be smaller than 5 %) it will be Alice's friend with significant probability. Of course, this probability depends on model's parameters such as N, k, and t. Let us consider $m = 2, 5, k = .1, .3, .5, t = 10, 50$. The situation is presented within Figures 1, 2 and 3.

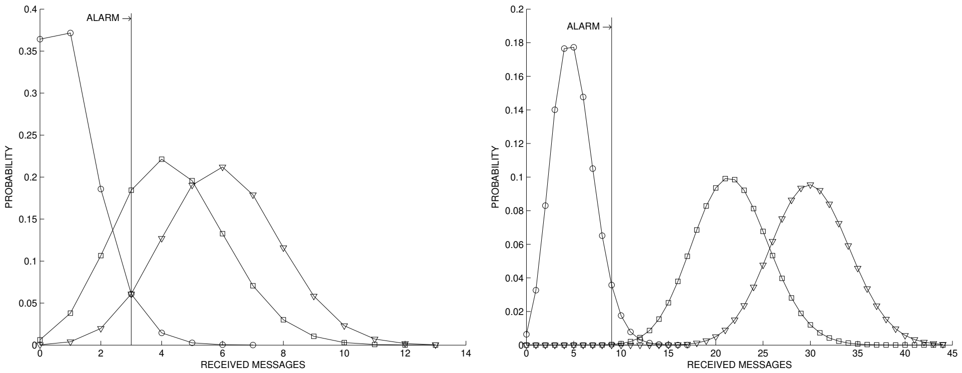

Figure 1. Probability density functions for N_P - $\circ$ and A_F (m=2 -'$\triangledown$', m=5 -'$\square$') for k=0.1 and t=10 (the left figure) and t=50 (the right figure).

The *Alarm* line denotes the case when someone becomes a suspect, i.e., he is supposed to be an Alice's friend. This is the case if some destination receives more messages than the number indicated by the *Alarm* line.
Figure 4 presents the probability of becoming a suspect in the above mentioned scenarios. We can clearly see that those probabilities are quite significant even for a small number of communication rounds. Let us observe that the relationship

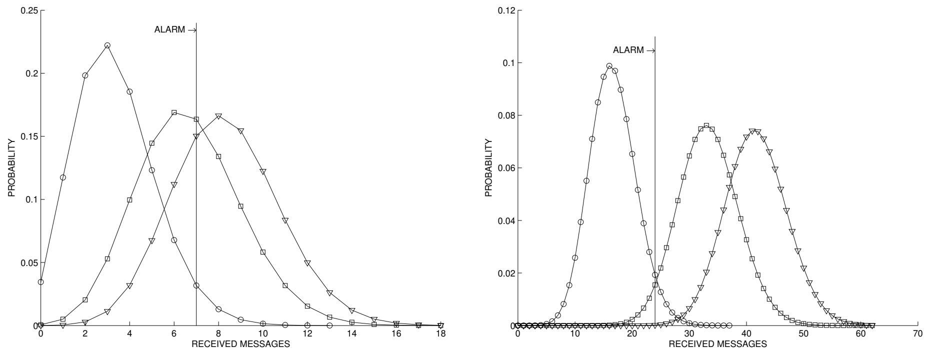

FIGURE 2. Probability density functions for N_P - ∘ and A_F (m=2 -'▽', m=5 -'□') for k=0.3 and t=10 (the left figure) and t=50 (the right figure).

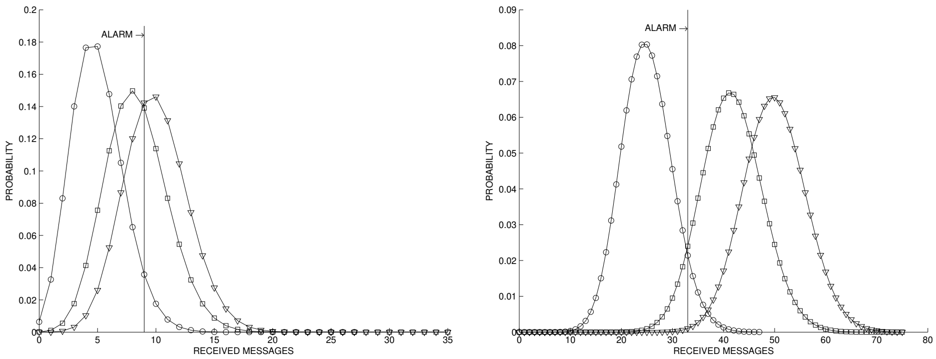

FIGURE 3. Probability density functions for N_P - ∘ and A_F (m=2 -'▽', m=5 -'□') for k=0.5 and t=10 (the left figure) and t=50 (the right figure).

between the number of rounds and the probability of detection according to 95% quantile is not monotonous. There is no monotonousness due to changing in quantiles according to increases of rounds (quantile increases as number of communication rounds increase and the alarm line moves right with the reference to the Alice's friends density for a while). It is needless to point out that the eavesdropper can very quickly reveal the Alice's friends with high probability. In order to provide better anonymity one can use dummy messages. We discuss how many of them should be actually used.

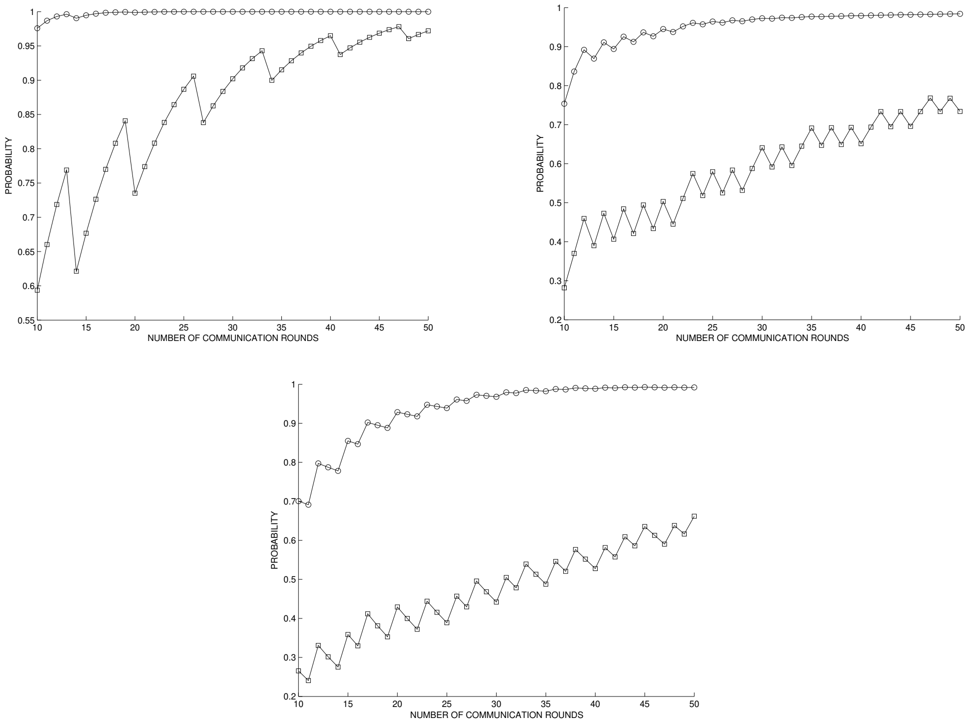

FIGURE 4. $\Pr(A_F > q_{95}(N_P))$ for m=2 - '○' and m=5 - '□' and k=0.1 (upper-left), k=0.3 (upper-right) and k=0.5 (lower).

4. Defense strategy

Assume that Alice wants to avoid dangers of statistical intersection attack, or at least to make it harder. A straightforward approach is to add some dummy traffic. However, Alice cannot include too much dummy traffic, since it reduces her communication bandwidth.

We assume that Alice chooses at random a group of d dummy destinations and devotes 50% of her communication bandwidth for dummy traffic. That is, in each turn which would be used for sending a message she tosses a coin, and in the case of tails she sends a dummy message instead of a workload message waiting in her buffer. (Of course the choice of 50% is arbitrary and can be replaced by another parameter). The underlying idea of this strategy is to hide Alice's true recipients in the dummies midst.

The problem we are concerned with is what is the best value for d, given k and m?

The answer to this question depends on the number of communication rounds, but generally too high value of d is inconvenient, since dummy destinations could disappear from the list of suspects generated by the adversary. Keeping $d = m$ could be also inconvenient for a moderate number of rounds: we would like to force the adversary to discover the dummies instead of the true destinations. So it seems to be better to reduce d below m. However, we should not exaggerate: the adversary which is aware of this strategy can filter out the suspects that appear too frequently.

Let A_D be a random variable denoting the number of messages received by Alice's dummy destination. The variables N_P, A_F and A_D have now the following probability distributions

$$\begin{aligned} N_P &\sim B\left(t \cdot b, \frac{1}{N}\right), \qquad A_F \sim B\left(t \cdot b, \frac{1}{N}\right) + B\left(t, \frac{1}{2m}\right), \\ A_D &\sim B\left(t \cdot b, \frac{1}{N}\right) + B\left(t, \frac{1}{2d}\right). \end{aligned} \tag{1}$$

We discuss the scenarios like the following one: A dummy destination should get a sufficient number of messages in order to become a suspect. Setting the probability of false suspect to 5%, the minimum amount of messages that a dummy destination should receive is equal to 95% quantile from distribution N_P. On the other hand, a dummy destination should not receive much more messages than a real Alice's destination. Therefore, we should ensure that a dummy destination should not receive more than 95% quantile from distribution A_F. Let $q_{95}(N_P)$ denote 95% quantile from distribution N_P and $q_{95}(A_F)$ - 95% quantile from distribution A_F. We can propose the following formula for the best choice for d:

$$d_{best} = \max_d \int_{q_{95}(N_P)}^{q_{95}(A_F)} g_{A_F} dA_D, \tag{2}$$

where g_{A_F} is the distribution density function of A_F.

5. Results

5.1. Numerical results

Using equation (2) and expressions (1) we can derive the optimal values of d as a function of the number of rounds t. The numerical results are depicted on Figure 5, 6 and 7 and they give somewhat unexpected thumb rules for Alice. In our case the integral from the equation (2) can be simplified into a discrete sum (since Bernoulli distribution is discrete). We calculate the optimal d value for $N = 50$, $k = 0.1, 0.3, 0.5$ and $t = 20, 50, 200$. It is worth pointing out that the results concerning optimal d do not significantly depend on N. If we increase the number of participants from n to $c \cdot N$ $(c > 1)$, then the number of users sending messages in each turn increase as well from $k \cdot N$ to $k \cdot c \cdot N$. Therefore, the distribution changes from $B(t \cdot b, \frac{1}{N})$ to $B(t \cdot b \cdot c, \frac{1}{c \cdot N})$. Since the Bernoulli distribution $B(n, p)$, in the case when $n \cdot p$ is moderate, can be approximated by the Poisson distribution $P(n \times p)$ (see [4]), we can see that distributions $B(t \cdot b, \frac{1}{N})$ and $B(t \cdot b \cdot c, \frac{1}{c \cdot N})$ are the same as $c \to \infty$.

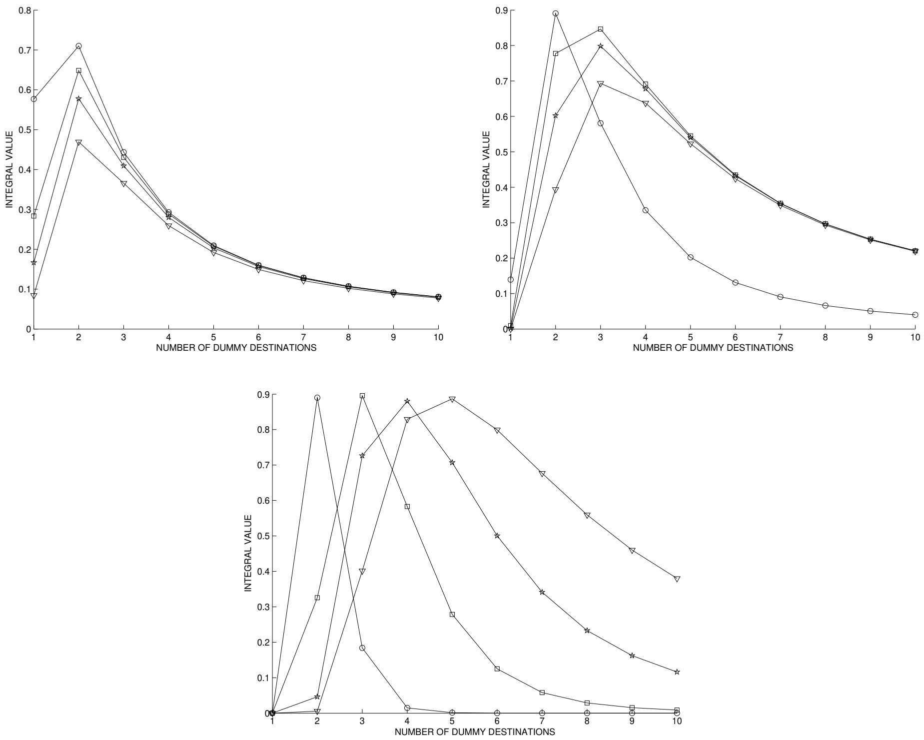

FIGURE 5. Optimal value of d, given $k = 0.1$, $m = 2$ ('$\circ$'), $m = 3$ ('$\square$'), $m = 4$ ('$\star$'), $m = t$ ('$\bigtriangledown$') and $t = 20$ (upper-left), $t = 50$ (upper-right) and $t = 200$ (lower).

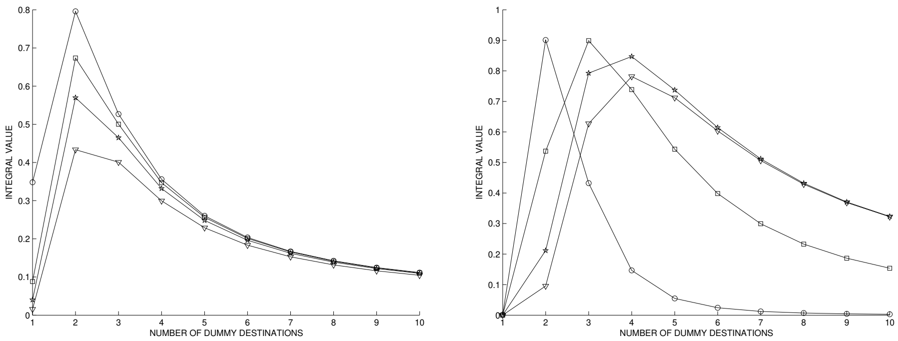

FIGURE 6. Optimal value of d, given $k = 0.3$, $m = 2$ ('$\circ$'), $m = 3$ ('$\square$'), $m = 4$ ('$\star$'), $m = t$ ('$\bigtriangledown$') and $t = 50$ (the left figure) and $t = 200$ (the right figure).

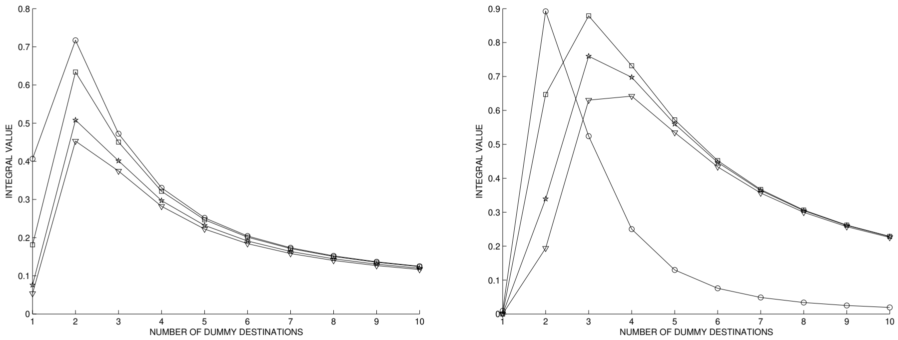

FIGURE 7. Optimal value of d, given $k = 0.5$, $m = 2$ ('$\circ$'), $m = 3$ ('$\square$'), $m = 4$ ('$\star$'), $m = t$ ('$\bigtriangledown$') and $t = 50$ (the left figure) and $t = 200$ (the right figure).

5.2. Conclusions

Our analysis reveals some important facts. First of all, greater number of communication rounds makes Intersection Attack easier. Parameter k increase (higher communication rate) slows down the attack, what is reasonable. Important result concerns choice of parameter d. A common belief was that d should be equal m. However, we have seen that for small number of rounds, d should be smaller than m. When t grows, then the optimal choice of d converges to m. If we consider a bigger quantile (if we, for example, set *Alarm* line equal to 97.5% quantile) the convergence rate will be even slower.

With sufficiently many rounds the adversary may filter out both the dummy and the real destinations. Essentially, nothing can help against an adversary that can monitor all source and destination points, when dummy traffic is limited.

Parameter k does not to be less than 1 - different users may send different number of messages per round. Moreover, one can consider the case when real recipients are not selected uniformly at random, but according to an arbitrary distribution. However, it seems that then it would be even harder to hide the destinations.

REFERENCES

[1] BERTHOLD, O.—PFITZMANN, A.—STANDTKE, R.: *The disadvantages of free MIX routes and how to overcome them*. In: Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability (H. Federrath, ed.), Lect. Notes Comput. Sci., Vol. 2009, Springer-Verlag, Berlin, 2000 pp. 30–45.

[2] DANEZIS, G.: *Statistical disclosure attack: Traffic confirmation in open environments*. In: Proceedings of Security and Privacy in the Age of Uncertainty, (SEC2003) (D. Gritzalis et al., eds.), Athens, May 2003, Kluwer Acad. Publ., Boston, MA 2003, pp. 421–426.

[3] DANEZIS, G.—SERJANTOV, A.: *Statistical disclosure or intersection attacks on anonymity systems*. In: Information Hiding '04, Lect. Notes Comput. Sci., Vol. 3200, Springer-Verlag, Berlin, 2004 pp. 293–308.

[4] FELLER, W.: *An Introduction to Probability Theory and Its Applications I*, John Wiley&Sons, New York, 1968.

[5] KESDOGAN, D.—AGRAWAL, D.—PENZ, S.: *Limits of anonymity in open environments*. In: Information Hiding '02 (F. A. P. Petitcolas, ed.), Lect. Notes Comput. Sci., Vol. 2578, Springer-Verlag, Berlin, 2003, pp. 53–69.

Received October 28, 2005

Institute of Mathematics and Computer Science
Wroclaw University of Technology
ul. Wybrzeże Wyspiańskiego 27
50-370 Wrocław
POLAND

E-mail: Jedrzej.Kabarowski@pwr.wroc.pl
Miroslaw.Kutylowski@pwr.wroc.pl