SCIS'99 The 1999 Symposium on
Cryptography and Information Security
Kobe, Japan, January 26-29, 1999
The Institute of Electronics,
Information and Communication Engineers

発信フィルタリング環境下の鍵共有プロトコルにおける閉塞率評価
Blocking Probability in Key-Agreement Protocol with Ingress Filtering

松浦幹太* 今井秀樹*
Kanta MATSUURA Hideki IMAI

Abstract— Participants of key-agreement protocol are recognized as a server-and-client pair; the initiator (client) first sends a request to the responder (server) which is a potential target of Denial-of-Service (DoS) attack. If a malicious initiator launches quite a large number of bogus requests to an honest responder, computational and/or memory resource of the responder may be exhausted. One strategy to limit the number of such bogus requests is *network ingress filtering*; local routers restricts outgoing traffic which originates from a downstream network to known legitimate prefixes. Another strategy is *falling-together mechanism* in which DoS attacks impose expensive computation on the attackers themselves. This paper evaluates these two strategies in a statistically equilibrated situation.

Keywords: denial-of-service attack; network ingress filter; key-agreement protocol; falling-together mechanism; authentication.

1 はじめに

オープンなネットワークで安全な通信を行うためには、いかにセッション鍵を共有するかが大変重要である。例えばインターネットでは、ISAKMP(Internet Security Association and Key Management Protocol)/Oakley 鍵共有プロトコル [1] が標準的な方式として開発されている。ISAKMP/Oakley は、周知の Diffie-Hellman(DH) 鍵共有プロトコル [2] に基づいており、プロトコル参加者の間に入って双方に対してなりすましを行う中間一致攻撃対策のため、認証メカニズムが組み込まれている。ところが、とりわけ公開鍵を利用した方式では、認証に要するコストがサービス妨害 (Denial-of-Service: DoS) 攻撃に悪用されかねない。すなわち、でたらめなリクエストを次々と送られた場合、それらすべてに対して真面目に検証作業をする応答者は計算機資源を使い果たしてしまってついにはサービス不能状態に陥る恐れがある。

サービス妨害攻撃を防止または抑制する手段として、例えばインターネットでは、Network Ingress Filtering が RFC(Informational) となっている [3]。これは、ローカルルータが外部へ向かうパケットの送信元アドレスをチェックし、自分の管轄外の不正な（または誤った）ものは破棄するというものである。また別の対策として、攻撃者にも応答者並の計算機資源消費を余儀なくさせる「共倒れ方式」が検討されている [4],[5]。ただし、これら 2 つの対策の定量的な効果は必ずしも自明ではない。そこで、本稿では、単純化した閉塞系モデルを仮定し、Network Ingress Filter のような発信フィルタが実装されたネットワークにおいて、共倒れ方式鍵共有プロトコルのサービス妨害攻撃耐性を評価する。

2 サービス妨害攻撃対策

2.1 Network Ingress Filtering

Network Ingress Filter は、偽の IP アドレスを送信元アドレスに用いた攻撃を抑制する。ローカルルータ管轄内の正当なアドレスを用いたサービス妨害攻撃を防ぐわけではないが、罪に問われたくない攻撃者に（その攻撃者と直結したわけではないとしても）管轄内のアドレスを使用させる効果が期待できる。ローカルルータが用いるルールは、RFC では次のように規定されている [3]。

- パケットの送信元アドレスが正当なプレフィックスの範囲内ならば、合格としてフォワードする。
- そうでなければ、パケットを棄却する。

ネットワーク管理者は、棄却したパケットに関する情報をログに残すべきであるとされている。これは、不審な挙動をモニターするためである。

---

* 東京大学生産技術研究所 〒106-8558 港区六本木 7-22-1. Institute of Industrial Science, the University of Tokyo Roppongi 7-22-1, Minato-ku, Tokyo 106-8558, JAPAN.

上記のチェックに合格するアドレスしかサービス妨害攻撃に利用しないとすれば、短時間に発信する不正なリクエストの総数が抑えられる。その結果、アドレスを偽称した攻撃の問題がある程度は解決されるものと期待される。

2.2 鍵共有プロトコルの改良

ここでは、通信負荷の少ない鍵共有プロトコルとして、メッセージパスが 3 回のものを考える。そのような 3 パスの鍵共有プロトコルは、図 1のような構造として捉えればわかりやすい。そこでは、プロトコルの始動者 (Initiator) を I、応答者 (Responder) を R と表記している。始動者と応答者が同じ公開鍵インフラストラクチャーを利用可能であると仮定し、彼らの (公開鍵, 秘密鍵) 対をそれぞれ (PK_I, SK_I), (PK_R, SK_R) と表記している。

共倒れ方式 [4],[5] を採用したければ、以下の方針にしたがってプロトコルを設計する。

1. ステップ ((4)) では、べき乗剰余演算のように負荷の高い計算を避ける。
2. メッセージ ((5)) で、ステップ ((6)) において負荷の高い計算を実行しなければ復元できない形で implicit にランダムなパラメータを送る。このパラメータを、以降では、単にランダムパラメータと呼ぶことにする。
3. ランダムパラメータも認証に利用する。
4. メッセージ ((7)) には、正しく復元されたランダムパラメータを知らなければ生成できないパラメータを含ませる。このパラメータを、確認パラメータと呼ぶことにする。
5. ステップ ((8)) の始めに、確認パラメータを検証する。この検証作業は、ステップ ((6)) のランダムパラメータ復元作業と比べて、計算負荷が軽いものでなければならない。

以上の方針に従った鍵共有プロトコルでは、ステップ ((8)) で確認パラメータを検証した後に行う負荷の高い計算を応答者に強いるためには、サービス妨害攻撃者もステップ ((6)) でそれ相応の計算機資源を消費しなければならない。この仕組みが、サービス妨害攻撃抑止策として期待される。ただし、メモリが不十分ならばステップ ((4)) で用いる事前計算値が枯渇する恐れがあり、定量的な効果（どの程度の確率で応答者の窓口が閉塞するか）は自明ではない。

	始動者 **(I)**		応答者 **(R)**
((1))	事前計算		事前計算
((2))	PK_R, SK_I を使った計算		
((3))	リクエスト	$\Rightarrow$	
((4))			PK_I, SK_R を使った計算
((5))		$\Leftarrow$	応答
((6))	PK_R, SK_I を使った計算		
((7))	応答確認	$\Rightarrow$	
((8))			PK_I and/or SK_R を使った計算
((9))	セッション鍵確立		セッション鍵確立

図 1: 3 パス鍵共有プロトコルの典型的な構造.

3 評価モデル

応答者が十分なメモリ資源を有しており事前計算値の蓄えが枯渇しないならば、共倒れ方式のメカニズムでサービス妨害を抑止できる。ここでは、そうでない場合について、ネットワークが発信フィルタを実装していると仮定して評価を行う。

具体的には、以下のように単純化したモデルを用いる。

1. 攻撃者が 1 回の攻撃で送りつけるでたらめなリクエストの数は一定（M個とする）である。
2. 応答者が蓄えることのできる事前計算値は、C組までである。これを事前計算容量と呼ぶ。
3. 時域 $[t, t+dt]$ の間に 1 つのサービス妨害攻撃が到来する確率は dt に比例し、$D \cdot dt$ である。D を攻撃生起率と呼ぶ。
4. 時域 $[t, t+dt]$ の間に正当なリクエストが到来する確率は dt に比例し、$R \cdot dt$ である。R を要求生起率と呼ぶ。
5. 時域 $[t, t+dt]$ の間に新たな事前計算値を 1 組計算できる確率は dt に比例し、$U \cdot dt$ である。U を事前計算能率と呼ぶ。
6. システムは閉塞系である。すなわち、事前計算値の蓄えが尽きた状態で到来したリクエストは待ち行列に並べられるのではなく、棄却される。
7. システムは、統計的平衡状態にある。

この時、状態遷移図は図 2のようになる。各状態は、応答者が保持している事前計算値の組数で表す。

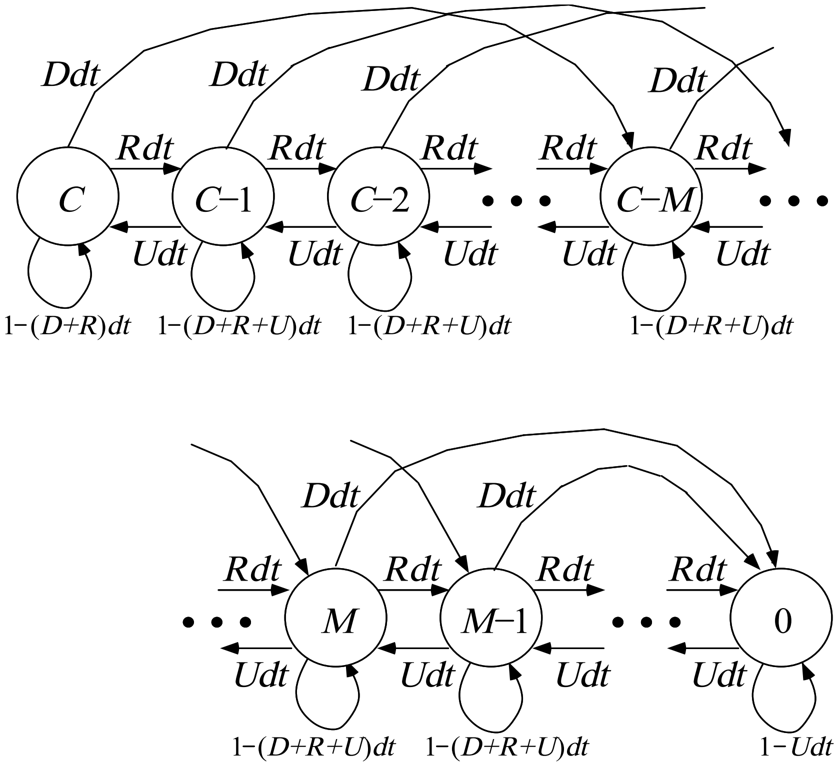


図 2: 発信フィルタが実装されたネットワークにおける鍵共有プロトコル応答者の状態遷移図. 各状態は, 応答者が保持している事前計算値の組数 (最大で C) で表す.

状態遷移図から状態方程式を書き下せば、

$$\frac{dP_C}{dt} = UP_{C-1} - (D+R)P_C \tag{1}$$

$$\frac{dP_i}{dt} = UP_{i-1} - (D+R+U)P_i + RP_{i+1} \tag{2}$$

$$(C-M < i < C)$$

$$\frac{dP_i}{dt} = UP_{i-1} - (D+R+U)P_i + RP_{i+1} + DP_{i+M} \tag{3}$$

$$(0 < i \leq C-M)$$

$$\frac{dP_0}{dt} = -UP_0 + RP_1 + D\sum_{j=1}^{M} P_j \tag{4}$$

となる。ただし、 P_i は応答者が状態 i にある確率である。統計的平衡状態では、時間微分を 0 とおいた

$$UP_{C-1} - (D+R)P_C = 0 \tag{5}$$

$$UP_{i-1} - (D+R+U)P_i + RP_{i+1} = 0 \tag{6}$$

$$(C-M < i < C)$$

$$UP_{i-1} - (D+R+U)P_i + RP_{i+1} + DP_{i+M} = 0 \tag{7}$$

$$(0 < i \leq C-M)$$

を

$$\sum_{j=0}^{C} P_j = 1 \tag{8}$$

と連立させて解けば、確率 $P_0, P_1, \cdots, P_C$ を求めることができる。そして、P_0 を閉塞率としてサービス妨害攻撃耐性を評価する。なお、連立一次方程式の係数行列は疎な行列なので、高速な計算ルーチンが利用可能である。

4 評価結果

まず、事前計算容量を $C = 10000$ として、閉塞率と攻撃生起率の関係を調べた。RSA 合成数や ElGamal 暗号で乗法群を規定する素数のサイズが 1024bit 程度の安全性を仮定すると、事前計算容量 $C = 10000$ は概ね数 MB 程度のメモリ資源に相当する。その他のパラメータを表 1のように設定した時の評価結果を、図 3に示す。

表 1: 評価で用いたパラメータ設定.

パラメータ	値	備考
M	256	クラス C の IP アドレス
U	1.0	単位
R	0.001	毎分数個の正常な要求

次に、事前計算容量を $C = 1000$ として、閉塞率と攻撃生起率の関係を調べた場合の結果を図4に示す。その他のパラメータ設定は、同じである。

これらの結果は、以下のようにまとめることができる。

- たとえ攻撃生起率が0.1（要求生起率の100倍、つまり、毎分数個来る正常な要求の $100M = 25600$ 倍のでたらめな要求に襲われる場合）であっても、閉塞率 P_0 は10% に満たない。
- 攻撃生起率が0.007を越えれば、閉塞率の特性は事前計算容量 C が10000（数MB程度のメモリ資源に相当）であっても1000であっても同じで、攻撃生起率に対して一次関数的に増大する。
- 事前計算容量 C が10000の場合、閉塞率が0.001% を越える境界を与える攻撃生起率は、C が1000の場合のほぼ2倍である。

5 むすび

本稿では、発信フィルタリング環境下の統計的平衡状態で、鍵共有プロトコルの応答者の閉塞率を評価した。その結果、クラスCのIPアドレスを管轄するローカルルータがフィルタリングしているという程度の前提で、数百KBのメモリを事前計算値用に準備すれば閉塞率が10% に抑えられた。メモリをその10倍に増やした場合の効果は、主として、閉塞率が0.5% を下回る場合に現れた。これらは単純化したモデルに基づいてはいるが、鍵共有プロトコルに組み込んだ共倒れ方式の効果を十分にはとり入れていないという意味で、控え目な評価となっていると考えられる。実際には、でたらめな要求に対しては事前計算以外の計算負荷をほとんど負わないことから、正常な要求の場合よりも事前計算能率が上がることが期待できる。今後は、そのような面でより踏み込んだ解析も行う予定である。

謝辞: 本研究の一部は、日本学術振興会の未来開拓学術推進事業 JSPS-RFTF 96P00604 の支援を受けた。

参考文献

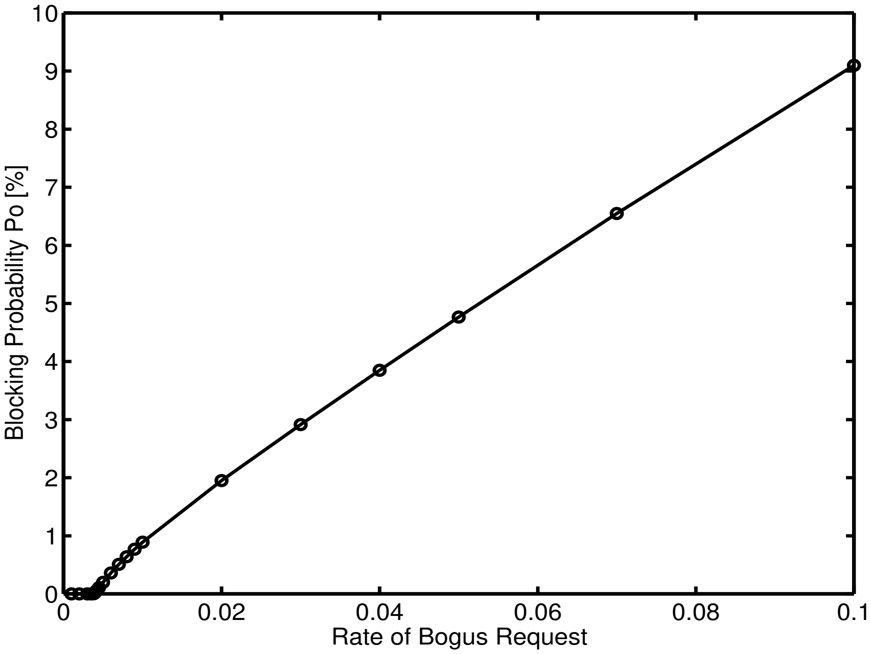
[1] D. Harkins and D. Carrel. “The resolution of ISAKMP with Oakley”. *Internet Draft (Work in progress)*

[2] W. Diffie and M. Hellman. “New directions in cryptography”. *IEEE Trans. Information Theory*, Vol. IT-22, No. 6, pp. 644–654, 1976.

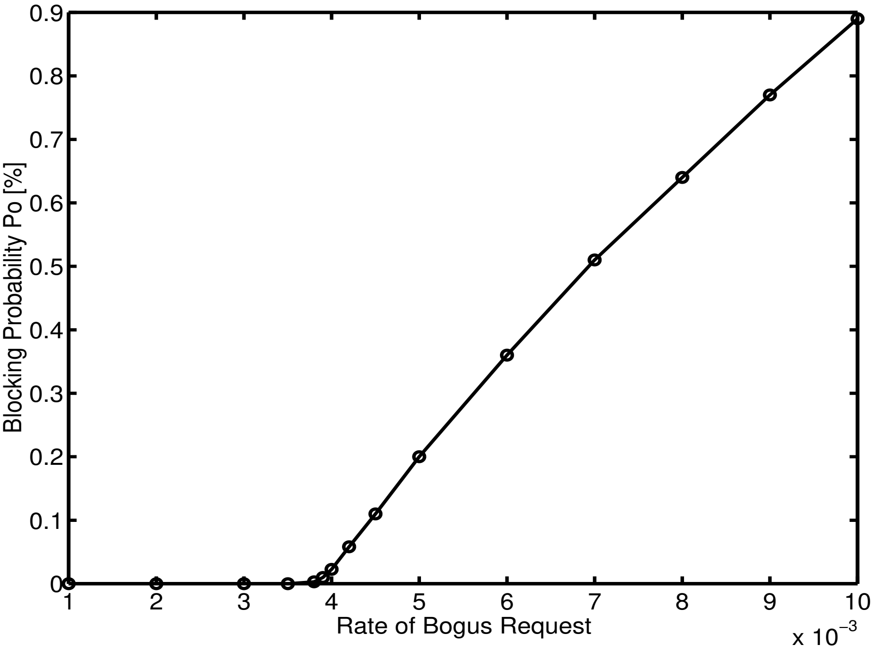
[3] P. Ferguson and D. Senie. “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”. RFC2267, January 1998.

[4] 廣瀬勝一, 松浦幹太. “サービス拒否攻撃に対して耐性のある鍵共有プロトコル”. 電子情報通信学会1998年基礎・境界ソサイエティ大会, A–7–7, 1998.

[5] K. Matsuura and H. Imai. “Protection of authenticated key-agreement protocol against a Denial-of-Service attack”. *Proceedings of 1998 International Symposium on Information Theory and Its Applications (ISITA’98)*, pp. 466–470, October 1998.

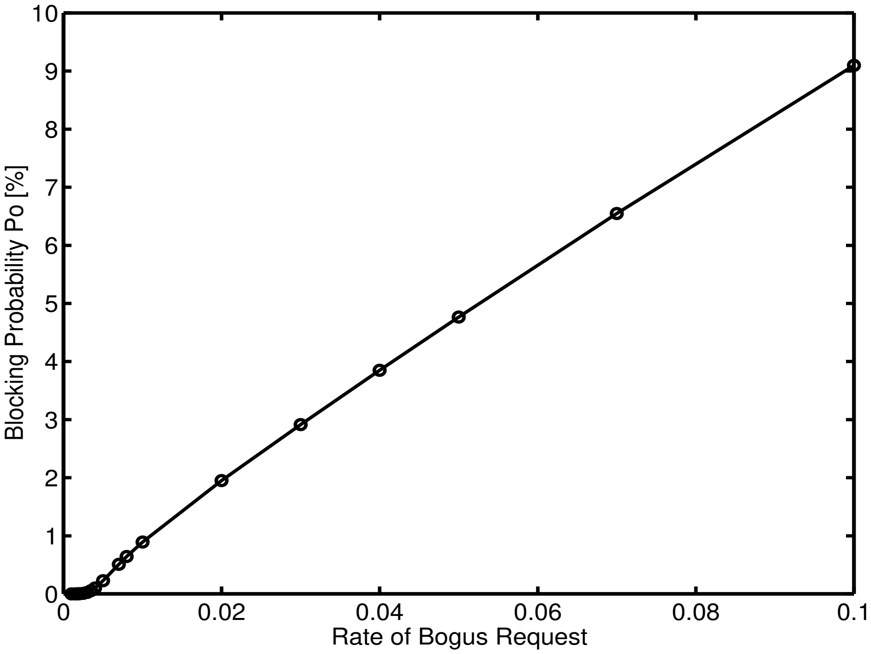


(a) $D \leq 0.1$

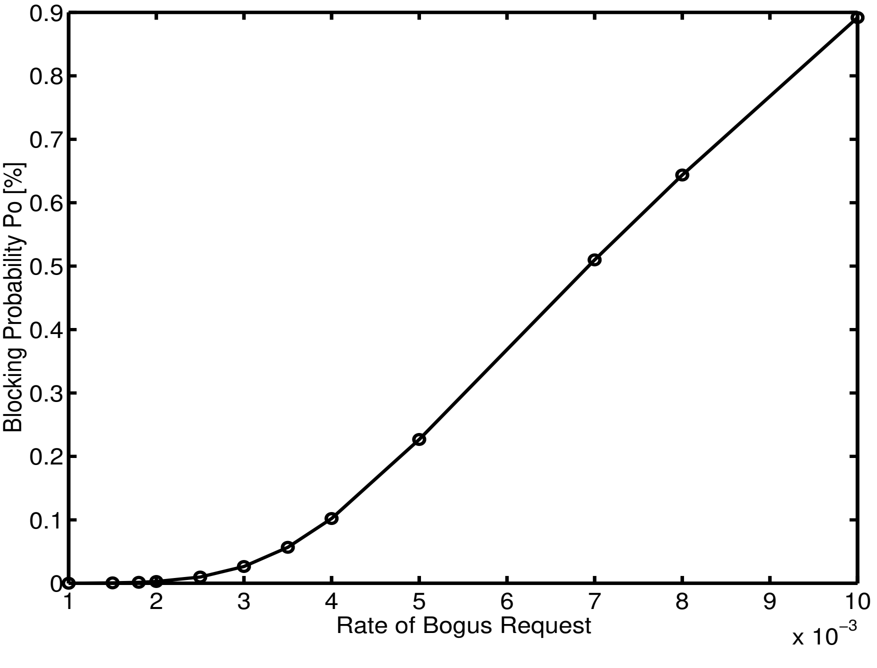


(b) $D \leq 0.01$

図 3: 事前計算容量が 10000 である場合の閉塞率特性.



(a) $D \leq 0.1$



(b) $D \leq 0.01$

図 4: 事前計算容量が 1000 である場合の閉塞率特性.