SYN flood DoS 攻撃耐性を強化する TCP コネクション確立手法

三宅 基治，中川智尋，稲村 浩
NTT ドコモ　マルチメディア研究所

An approach of TCP handshake for Denial of Service attacks

Motoharu Miyake, Tomohiro Nakagawa, and Hiroshi Inamura
Multimedia Labs., NTT DoCoMo Inc.

あらまし

本稿では，SYN cookie における TCP オプションの利用制限および，セグメントロスによるクライアント・サーバ間のコネクション確立の状態不一致問題を改善するための TCP コネクション確立手法について提案する．提案方式では，サーバの 3 way ハンドシェイクにおける TCP 状態遷移ダイアグラムを修正し，クライアント側の TCP に実装されている同時オープン機能を利用する．この結果，SYN flood に対する攻撃耐性を維持したまま，TCP オプションの利用を可能にするとともにコネクション状態に不一致が発生する問題を回避する．更に，提案方式はクライアントへの修正を必要としないことから，既存システムとの親和性が高く，導入が容易といった特徴を有することを明らかにする．
キーワード: TCP, DoS 攻撃, SYN flood, SYN cookie, 3 way ハンドシェイク

1　はじめに

インターネットの普及にあわせ TCP は WEB ブラウジング，メール送受信，ファイル転送など幅広く利用されている．利用範囲の拡大に伴い，TCP の脆弱性を狙った攻撃も近年増加している [1, 2].

代表的な DoS 攻撃の一つとして知られている SYN flood 攻撃は，TCP コネクション確立に用いられる 3 way ハンドシェイクの脆弱性を狙い，大量の SYN を攻撃対象とするホストに送信する．この結果，ホストではコネクション確立のためのリソース枯渇が引き起こされ，正規ユーザの接続を困難とすることに加え，ホスト自身のハングアップといった問題が発生する．特に，IP spoofing による DoS 攻撃に対して Firewall や IDS (Intrusion Detection System) によるフィルタリングでは，悪意のある第三者と正当なユーザを区別できずに正当なユーザの SYN も破棄してしまう可能性があり，SYN flood 攻撃への対処を困難としている [1]．そこで，プロバイダ，ルータによるサブネットマスクと SYN の送信元ホストアドレスをもとにしたフィルタリングも提案されているが，完全な実施には及んでいない．

SYN flood への攻撃耐性を高めるために TCP 状態遷移ダイアグラムの SYN_RECV 状態を削除した SYN cookie が多くの OS で採用されている．SYN cookie は，アクティブ・オープン側のホストから送信される SYN に含まれる IP アドレス，ポート番号，シーケンス番号にパッシブ・オープン側のホストの Secret を加えた cookie を SYN/ACK のシーケンス番号として送信する．そして，ACK 到着時にも SYN と同様に cookie を作成し，確認応答番号から 1 を引いた値と一致するか否かの判断を通してコネクション確立を行う．SYN cookie を利用した場合，SYN_RECV 状態の削除により SYN に含まれる情報を保持しないため，MSS (Maximum Segnent Size) を除く TCP オプションを利用することができない．唯一利用可能な MSS も事前に設定された値に限定され，通信効率の低下は避けられない．特に，SYN flood 攻撃による高トラヒック環境下では，ルータのキー溢れも想定されるため，ウインドウ中の複数セグメントロスに対する効率的なリカバリを提供する SACK (Selective Acknowledgment) [3] の利用が切望される．更に，アクティブ・オープン側のホストから送信される ACK がロスした場合，パッシブ・オープン側のホストでは SYN_RECV 状態をもたないために SYN/ACK 再送が行われず，ホスト間のコネクション状態に不一致が生じるといった問題が発生する [4].

そこで本稿では，SYN cookie におけるこれらの問題を改善するために TCP 同時オープンを用いたコネクション確立手法について提案する．提案方式では，アクティブ・オープンを行う際に実装されている同時オープン機能を利用するために，パッシブ・オープンのための TCP 状態遷移ダイアグラムを修正する．具体的には，

SYN 受信時にパッシブ・オープン側のホストは，SYN cookie 同様の方法で作成したシーケンス番号，IP アドレス，ポート番号および，URG ビットを SYN に加えて送信する．このとき，アクティブ・オープン側のホストでは同時オープンとなり，内部の TCP 状態遷移ダイアグラムを SYN_SENT から SYN_RECV に移行する．そして，最初に送信した SYN の情報を維持したまま，確認応答番号のみを修正した SYN/ACK を送信する．この結果，パッシブ・オープン側ホストでは SYN/ACK 到着時に SYN cookie における ACK 確認と同様の処理を行うことが可能となる．ここで，提案方式が SYN cookie と異なる点は，コネクション確立の判定を SYN/ACK により実施しており，TCP オプションを利用可能としていることである．また，ネゴシエーションの途中のメッセージがロスしたとしても，アクティブ・オープン側のホストからの再送が行われ，ホスト間の状態不一致が発生しない．この結果，提案方式を用いることにより，SYN flood 攻撃への耐性を維持したまま，TCP オプションの利用を可能にするとともに，ホスト間のコネクション状態の不一致問題を回避でき，効率的な通信が可能となる．また，クライアントへの修正を必要としないことから，既存システムとの親和性が高く，導入が容易といった特徴を有する．

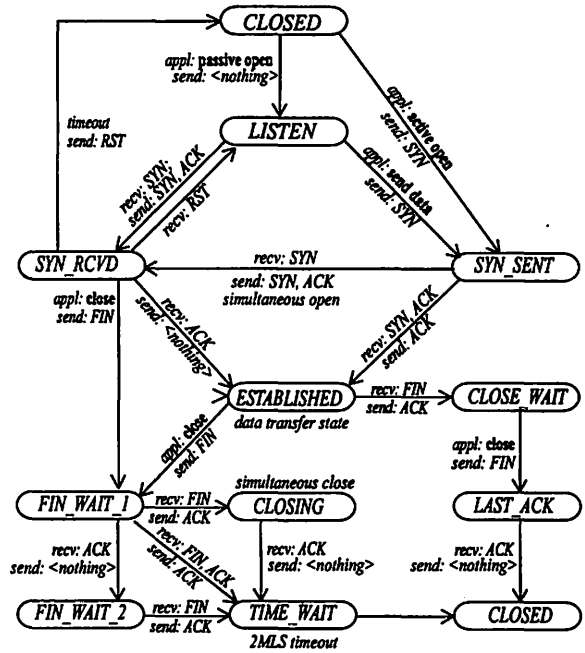

図 1: TCP 状態遷移ダイアグラム

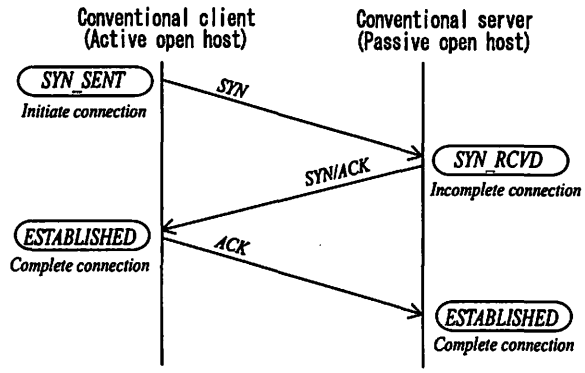

図 2: 3 way ハンドシェイクのシーケンス

2 関連研究

2.1 TCP コネクション確立

TCP コネクションは，図 1 に示す状態遷移ダイアグラムに従い，アクティブ・オープンまたは，パッシブオープンのいずれかを経て確立される．このとき，アクティブ・オープン，パッシブ・オープンを行うそれぞれのホストは，図 2 に示した 3 way ハンドシェイク (SYN, SYN/ACK, ACK) により，IP アドレス，ポート番号，シーケンス番号および，TCP オプションのネゴシエーションが行われる [5]．なお，本稿では誤解の恐れのない限りアクティブ・オープンを行うホストをクライアント，パッシブ・オープンを行うホストをサーバとそれぞれ呼ぶものとする．

TCP 状態遷移ダイアグラムにより，サーバではクライアントからの SYN 受信によって，シーケンス番号に +1 した確認応答番号を含む ACK および，自身の初期送信シーケンス番号を加えた SYN から構成される SYN/ACK を送信する（図 3）．このとき，サーバでは SYN に含まれる TCP オプションに関する情報をコネクション確立後に有効とするために保持すると同時に，SYN/ACK によってレスポンスを通知する．そして，図 1 に示すように LISTEN から SYN_RECV 状態に遷移した後，ACK 到着によりコネクションが確立し，ESTABLISHED 状態となる [6]．

2.2 SYN flood 攻撃

悪意のある第三者からの IP spoofing による SYN flood 攻撃に対して，IP アドレス以外に SYN の正当性を確認する手段を TCP ではもたないため，送信元 IP アドレスに対して無条件に SYN/ACK を送信する．詐称された IP アドレスを用いたホストが実在する場合，SYN/ACK を受信したとしてもアクティブ・オープン

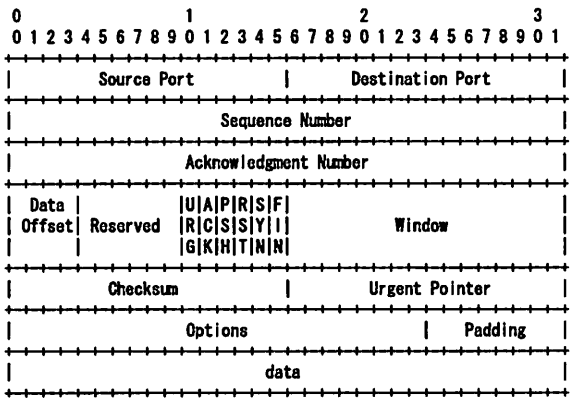

図 3: TCP ヘッダ

が行われていないため，コネクションが確立することはなく，即座に RST が送信される．このとき，SYN flood 攻撃を受けているホストでは，RST 受信によって SYN_RECV 状態を保持するためのキューを解放できるので，攻撃の影響を限定的に抑えることができる．しかし，IP アドレスを詐称されたホストが実在しない，または実在するがサブネットを構成する Firewall によって SYN/ACK が破棄されてしまうとクライアントの情報が得られず，キューを解放する契機を失う．更に，SYN_RECV 状態では，再送タイマにより SYN/ACK 再送が繰り返され，ネットワークへの過剰なトラヒックを送り出すことになる．この結果，SYN_RECV 状態の解放よりも SYN flood 攻撃が容易に勝る状況となり，キューの枯渇が引き起こされる [4].

2.3 SYN cookie

SYN cookie [4] は，TCP 状態遷移ダイアグラムにおける SYN_RECV 状態を用いず，ACK 受信により LISTEN から ESTABLISH に直接遷移し，コネクションを確立する．この際，3 way ハンドシェイク を用いた正規のアクセスを判別するため，SYN/ACK のシーケンス番号と，それに対応する ACK の確認応答番号が正しく対応するか否かを確認する．

図 4 に，SYN cookie により作成される SYN/ACK のシーケンス番号を示す．peer iss は SYN のシーケンス番号，laddr, faddr, lport fport, secret はサーバ IP アドレス，クライアント IP アドレス，サーバのポート番号，クライアントのポート番号および，サーバ内の秘密情報をそれぞれ表す．また，(A) は SYN の TCP オプションで通知された MSS を予め定義された 4 つの値の一つとして表現し，idx はウィンドウの index を表す．はじめに，MD5 (Message Digest 5) [7] による 25 ビットの情報に対し，2 ビットで表現した MSS (A) との排他論理輪 (XOR: eXclusive OR) を求め，7 ビットの index を加えて 32 ビットとする．次に，クライアントの SYN のシーケンス番号との排他論理輪を計算し，SYN/ACK のシーケンス番号を作成する．そして，ACK の確認応答番号が SYN/ACK のシーケンス番号に 1 を加えたものと一致する場合のみコネクションを確立する．上記過程の導入により，SYN/ACK のシーケンス番号として SYN に含まれる情報 (IP アドレス，ポート番号，サーバ内の秘密情報) を一方向関数のハッシュによって生成し，悪意のあるクライアントからのシーケンス番号の推測を困難とし，攻撃対象となるホストに ACK のみが送られてコネクションが確立することを防止している．

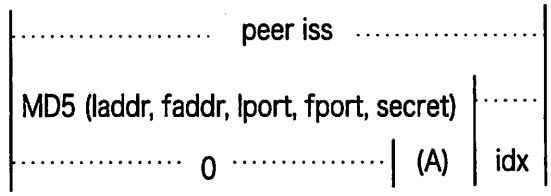

図 4: SYNcookie によるシーケンス番号作成

SYN cookie の導入により SYN flood 攻撃によるキューの枯渇の問題を回避できる反面，以下の問題が指摘されている [4].

- クライアント・サーバ間の状態不一致
- TCP オプションの限定的な運用

一つ目の問題は，コネクション確立途中に ACK がロスした場合でも，クライアントは ESTABLISHED 状態となり，ハーフオープンとなる．しかし，SYN_RECV 状態をもたないサーバは SYN/ACK を再送することができずに LISTEN 状態を維持するため，クライアント・サーバ間でコネクション状態の不一致が発生する．WEB ブラウジングを行う場合，ACK 送信と合わせて HTTP プロトコルの GET リクエストが送信されるため，セグメントロスが発生したとしても 後続の GET リクエストが再送され，コネクション状態の不一致は発生しない．一方，telnet を利用した場合，コネクション確立によりサーバ側からのみリクエストが送信される．このため，ACK ロスによってコネクション状態の不一致が発生した場合，クライアントではサーバからのリクエストを得ることができず，サービスを利用することはできない．

二つ目の問題は，リソース枯渇を防ぐために SYN に含まれる TCP/IP に関する情報を SYN cookie では保持しない．このため，クライアントからの SYN によって通知される TCP オプション（MSS を除く）が利用できなくなる．代表的な TCP オプションとしては，ウインドウ中の複数セグメントロスに対する効率的なリカバリを提供する SACK [3]，帯域幅遅延積の大きなギガビット・ネットワークで必要となる受信ウインドウサイズ拡大のための Window scale option [8] および，T/TCP [9] を実現するための TCP オプション (CC:connection count, CCECHO) などがあげられる．また，MSS に関しても．既定の 4 つのセグメント・サイズの一つが割り当てられるため，IPSec 利用の有無などに応じた柔軟な MSS 設定は困難であり，通信効率を低下させる要因となる [10].

3 提案する 4 way ハンドシェイク

本稿では，SYN cookie 利用時に問題となる TCP オプションの提供を可能とするとともに，セグメントロスにより発生していたホスト間のコネクション状態の不一致を回避する 4 way ハンドシェイクを提案する．

3.1 4 way ハンドシェイク

提案方式を用いたサーバは，通常のアクティブ・オープン，パッシブ・オープンによるコネクション確立には従来の TCP 状態遷移ダイアグラム（図 1）を用いる．そして，SYN flood 攻撃によりコネクション確立のキューが枯渇し始めた場合のみ，図 5 に示す TCP 状態遷移ダイアグラムに従ったパッシブ・オープンを行う．図 6 に，提案する 4 way ハンドシェイクを実行する際のクライアント・サーバ間の TCP 状態遷移ダイアグラムとシーケンスを示す．

初めに，クライアントからの SYN に対し，SYN_ARRIVAL 状態を用いて SYN/URG を送信する．サーバから送信される SYN/URG には，SYN cookie 同様の方法で作成したシーケンス番号，IP アドレス，ポート番号および，URG ビットを加えて送信する．URG ビット付加に関しては，3.2 節で説明する．この結果，クライアントでは SYN 受信によって同時オープンとなり，内部の TCP 状態遷移ダイアグラムを SYN_SENT から SYN_RECV に移行し，最初に送信していた SYN の情報を維持したまま，確認応答番号を加えた SYN/ACK を送信する．次

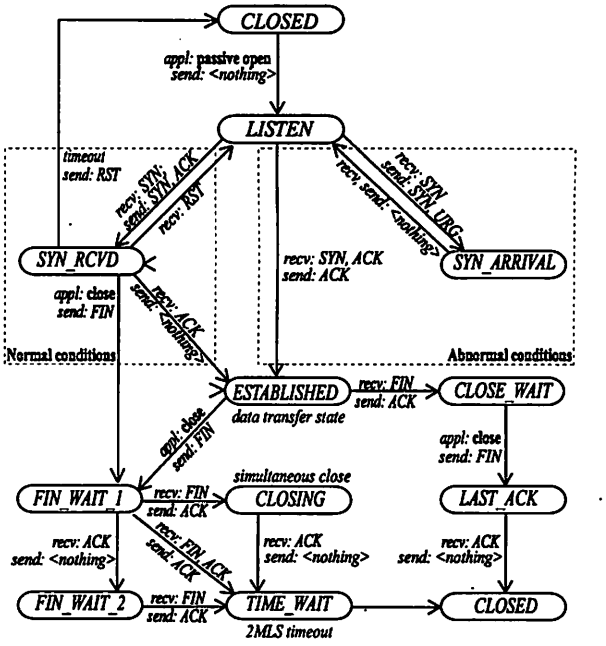

図 5: 提案する 4 way-handshake 状態遷移ダイアグラム（パッシブ・オープン）

に，サーバでは LISTEN 状態において SYN/ACK の正当性を SYN cookie の場合と同様に確認応答番号から確認し，コネクション確立を行う．この際，クライアントから送信される SYN/ACK には，SYN と同様の TCP オプションが含まれるため，SYN_ARRIVAL 状態においてこれらの情報を保持する必要がない．従って，リソース開放により SYN Flood 攻撃耐性を高めると同時に，SYN/ACK に含まれる TCP オプションを利用したコネクション確立が可能となる．

表 1 に，4 way ハンドシェイクを構成するセグメントがロスした際に再送タイムアウトによって送信され

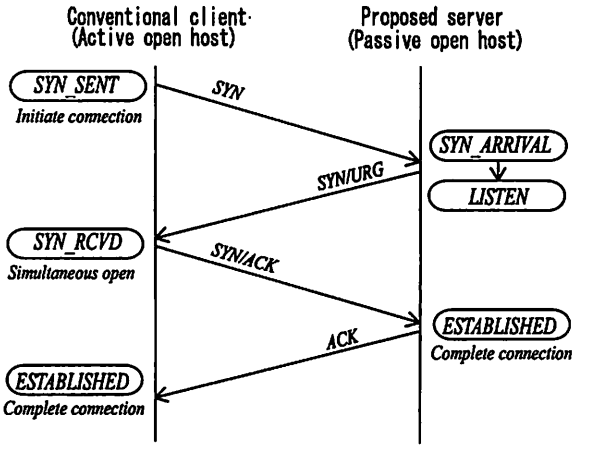

図 6: 4 way ハンドシェイクのシーケンス

るセグメントと送信元をそれぞれ示す．この結果，提案方式では ネゴシエーション中にセグメントが消失したとしてもクライアントからの再送が期待されるため，SYN cookie において問題であったコネクション状態の不一致を起こさないという特徴も備える．

表 1: セグメントロス発生時のセグメント再送動作

送信元	セグメントロス	再送元	再送セグメント
client	SYN	client	SYN
server	SYN	client	SYN
client	SYN/ACK	client	SYN/ACK
server	ACK	client	SYN/ACK

表 2 に 提案方式と従来方式（未実施，SYN cookeis）の特徴をまとめる．なお，Conventinal TCP では SYN flood 攻撃によりサーバのリソース枯渇が発生するが，比較のため記載している．SYN cookie では既存の 3 way ハンドシェイク実施時に SYN/ACK のシーケンス番号と ACK の確認応答番号を利用して攻撃耐性を高めているが，一方でセグメントロスによる状態不一致，TCP オプションの制限といった問題が発生する．提案方式では，サーバからの SYN 送信によるクライアントの同時オープンを利用しており，他に比べ 1 セグメント分のオーバヘッドとなる．同様に T/TCP の接続時間も 1 RTT が追加で必要となるため，T/TCP が目的とするコネクション確立時のオーバヘッド削減に関しては効果を期待することはできない．しかし，SYN cookie と同様の SYN flood に対する攻撃耐性を実現しつつ，上記問題を改善によって既存システムとの親和性を高く保ち，導入が容易といった特徴を有することが分かる．

3.2 IP spoofing 対策

IP spoofing による DoS 攻撃の防止方法としてプロバイダ，ルータによるサブネットマスクと SYN の送信元アドレスを基にしたフィルタリング手法が提案されている [1]．しかし，インターネットへの接続元すべてが同一のポリシーで運営されることは困難であり，最終的には各ホストでの対応が必要となる．そこで，本節ではクライアント・サーバに提案方式を用いた場合のネゴシエーションを中心に述べる．

提案方式を用いたサーバがパッシブ・オープンを行う場合，3.1 節に示したように URG ビットを SYN に付加し，従来の TCP 状態遷移ダイアグラムをもつホストとの接続を維持しつつ，提案方式を用いたホストに対して SYN Flood 攻撃に伴う SYN 送信であることを明示的に通知する．一例として，IP spoofing による SYN flood 攻撃がなされた環境下での，提案方式を用いたホスト間でのネゴシエーションを図 7 に示す．ここで，ホスト A, B は IP アドレス A, B をもち，ポート番号 a, b によりそれぞれサービスが提供されているものとする．このとき，悪意のある第三者により ホスト B を装った SYN がホスト A に対して送信された場合，正しいリクエストか，偽のリクエストかをホスト A では判断できず，SYN/URG を送信する．一方，IP アドレスを詐称されたホスト B は，LISTEN 状態など，アクティブ・オープンを行っていない状況下で SYN/URG を受信するため，SYN/URG を即座に破棄する．この結果，提案方式を用いていた場合，SYN/URG 破棄のみでよくネットワークリソースの過剰な消費を防止する．また，SYN/ACK やポート番号の異なる SYN 受信時のみ従来の TCP 状態遷移ダイアグラム同様に RST を送信するもとのする．

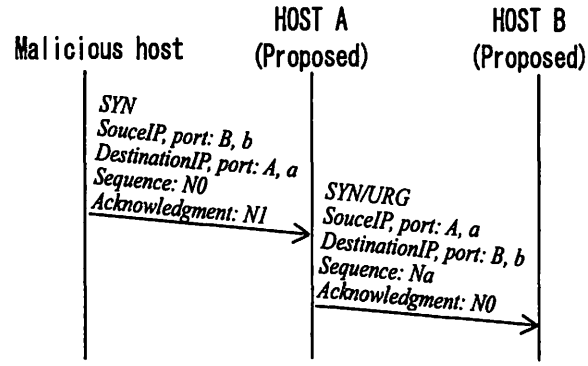

図 7: IP spoofing 環境下における提案方式を利用したホスト間でのネゴシエーション

次に，従来の TCP 状態遷移ダイアグラムをもつホストの IP アドレスおよびポート番号が詐称された場合のネゴシエーションを図 8 に示す．ホスト A からの SYN/URG によって 3way ハンドシェイクが開始され，SYN/ACK が送信される．次に，ホスト A では SYN/ACK の IP アドレス，ポート番号，シーケンス番号などをもとにしてシーケンス番号 Na に対する確認応答番号であるか否かを判断する．この際，確認応答番号は Na+1 となるものの，SYN/ACK のシーケンス番号がホスト B の初期送信シーケンス番号が設定されるため，ホスト A では不正なメッセージと判断し，RST を送信する．従って，詐称されたホスト B が従来方式を用いていた場合，1 セグメント分のオーバヘッドとなるものの RST によりネゴシエーションは中止される．

表 2: SYN flood 攻撃に対する提案方式と従来方式の耐性比較

	DoS 攻撃耐性	セグメントロス耐性	TCP オプション	T/TCP	ネゴシエーション期間
Conventional TCP	× なし	○ 再送あり	○ 全て利用可能	○ 1 RTT	○ 1.5 RTT
SYN cookie	○ あり	× 状態不一致発生	△ MSS のみ	× 未サポート	○ 1.5 RTT
4 way ハンドシェイク	○ あり	○ 再送あり	○ 全て利用可能	△ 2 RTT	△ 2 RTT

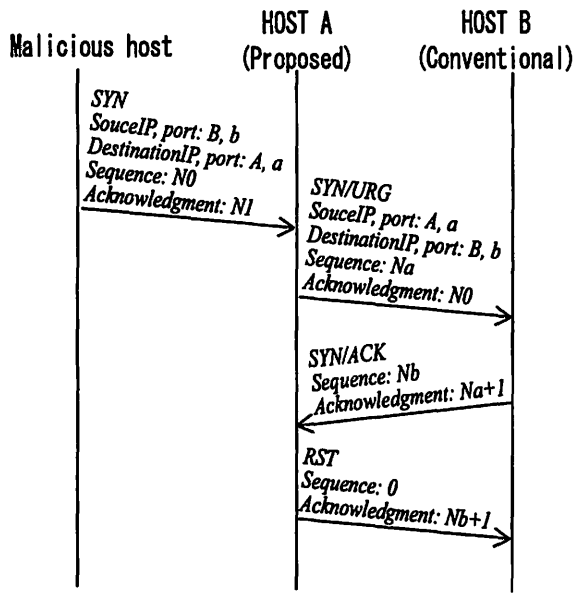

図 8: IP spoofing 環境下における提案方式を利用したホストから従来ホストへのネゴシエーション

4 まとめ

本稿では，サーバの TCP 状態遷移ダイアグラムを修正し，クライアント側の TCP に実装されている同時オープン機能を利用する 4 way ハンドシェイクによる TCP コネクション確立手法を提案し，以下の結果を得た．

1. TCP option を利用可能とする SYN cookie 実現
2. パケットロス時のクライアント・サーバ間の状態不一致問題の改善
3. クライアントの TCP プロトコル修正を必要とせず，既存システムとの高い親和性実現

現在，オープンソースの OS への実装を行っており，攻撃耐性評価をするめるとともに， SYN cookie と比べたオーバヘッドについても調査を予定している．

今後の課題としては， NAT (Network Address Translation) や Gateway を利用した環境下のクライアントからの接続を行う場合，外部からの接続要求を許容しない設定または， SYN 対する SYN/ACK 以外はフィルタの設定によって破棄される．このため，提案した 4 way ハンドシェイクを用いたコネクション確立を行うためには，SYN/URG 受信を許容する設定が必要不可欠となるため， NAT, Gateway に関する調査も合わせて行う予定である．

謝辞

本研究を進めるにあたりご協力頂いた大菅大吉氏に感謝いたします。

参考文献

[1] US-CERT. Vulnerabilities in TCP. Technical Cyber Security Alert TA04-111A, April 2004.

[2] M. Dalal. Transmission Control Protocol security considerations. draft-ietf-tcpm-tcpsecure-01.txt, June 2004.

[3] E. Blanton and M. Allman. Using TCP Duplicate Selective Acknowledgement (DSACKs) and Stream Control Transmission Protocol (SCTP) Duplicate Transmission Sequence Numbers (TSNs) to Detect Spurious Retransmissions. RFC3708, February 2004.

[4] J. Lemon. Resisting SYN flood DoS attacks with a SYN cache. In *Proceedings of the BSDCon 2002 Conference, USENIX*, February 2002.

[5] J. Postel. Transmission Control Protocol. RFC793, September 1981.

[6] W.G. Right and W.R. Stevens . *TCP/IP Illustrated, Volume 2 The Implementation.* ADDISON-WESLEY, 1995.

[7] B. Schneier. *APPLIED CRYPTOGRAPHY.* John Wiley & Sons, Inc., 1996.

[8] V. Jacobson, R. Braden, and D. Borman. TCP Extensions for High Performance. RFC1323, May 1992.

[9] R. Braden. T/TCP - TCP Extensions for Transactions Functional Specification. RFC1644, July 1994.

[10] 石川太郎，稲村 浩，高橋 修. W-CDMA 向け TCP プロファイル. 情処学 MBL 研報, Vol. MBL15-3, , November 2000.