福井大学 大学院工学研究科 研究報告 第57巻 2009年3月
Mem. Grad. Eng. Univ. Fukui, Vol. 57 (March 2009)

ユーザの挙動に基づく個人認証におけるファジィ測度評価手法
– Schonlau データによる手法の評価 –

白井治彦* 黒岩丈介† 小高知宏‡ 小倉久和†

Evaluation of the Fuzzy Measure Authentication Method based on the User Behavior
– Schonlau's data case –

Haruhiko SHIRAI* Jousuke KUROIWA† Tomohiro ODAKA‡ and Hisakazu OGURA†

(Received February 9, 2009)

In this paper, we reported the effects of the user authentication method with fuzzy measure evaluation we had proposed. In the method a authentication system checks the current user's behavior by monitoring command chains user inputted in the interactive computer environment. We apply the method to the Schonlau's data set and analyze the detection capability comparing with other methods.

We evaluated performance of the its method with a ROC(Receiver Operating Characteristic) curve. According to the results of several experiments, the method revels ability to check intrusion at the same level as the other methods such as the HMM method.

Key words : User Authentication, Fuzzy Measure, Intrusion Detection, User Behavior, Schonlau's data, ROC Curve

1. はじめに

現在のインターネット社会において情報セキュリティ対策は常に重要課題である．外部ネットワークからのセキュリティ侵略行為はファイアウォール技術の向上で多くの場合防御することが可能となった．しかし，内部のネットワークに接続された個々のコンピュータにおけるセキュリティは，未だに従来からのパスワード方式等による個人認証法に委ねられているのが現状である．悪意ある侵入者がネットワークの盗聴やパスワードクラックを用いてコンピュータの個人認証システムを一度突破してしまうと，正当なユーザ自身の知らぬ間に「なりすまし」行為などで自分のシステムが悪用されてしまう．そのような行為を防ぐためには，個人認証を行った後でも絶えずシステムが利用ユーザの監視を続けている必要がある．その監視方法として，侵入や不正使用などを直接検出するのではなく，ユーザの挙動を常に監視し続け，通常と異なった振る舞いがあった場合に不正使用等として扱う異常検出技術法やその有効性がいくつか報告されている[8],[9],[12]–[14].

我々はこれまでにその手法として対話的な計算機環境下において入力コマンド列に見られるユーザの挙動を用いた個人認証法（不正ユーザの検出法）をいくつか提案し，その有効性を報告してきた[1]–[4]．その中で，あるコマンドからその直後に入力されるコマンドの条件付き確率に注目し，更にファジィ積分を用いてあるコマンド同士の出現頻度や異なる組み合わせ数をより大きく評価して個人の挙動の特徴を強調した方法が有効であることも報告した[1].

本稿では，ユーザの挙動を用いたコンピュータシス

*技術部
†知能システム専攻科
‡原子力・エネルギー安全工学専攻
*Technical Support Division
†Graduate course of Human And Artificial Intelligent Systems
‡Graduate course of Nuclear Power and Energy Safety Eng.

テムの異常検出方法の性能評価に広く用いられているSchonlauらによって提供された入力コマンド列データを対象に，我々が提案したファジィ積分を用いた認証法の性能評価についてその結果と手法の有効性を報告する．認証性能評価は，正当なユーザの入力コマンド列であるにも関わらず異常侵入と判断してしまった誤報（false alarm）と侵入者の入力コマンド列であるにも関わらず異常検出できない欠報（missing alarm）について双方の比率の関係をROC(Receiver Operating Characteristic)曲線を用いて行う．また，学習モデルのための入力コマンド列の長さや検査データ長と本手法との関係についても分析した結果について述べる．

2. コマンド連鎖を用いたユーザモデルの生成と異常検出法と性能評価のためのSchonlauデータ

2.1 ファジィ測度によるモデル生成と認証評価

対話的環境における計算機システムのユーザの挙動を用いた異常検出法は図1で示すように2つのフェイズで構成される．ひとつはシステムを利用している正当なユーザからあらかじめ採取した入力コマンド列を学習データとし，その学習データにみられる特徴を抽出してユーザの挙動モデルを構築する．2つ目のフェーズは挙動モデルを基に，現在監視を行っている振る舞いが正当なユーザのモデルと似ているかどうかを判別する認証評価部である．本稿では正当なユーザの学習データの特徴抽出および監視対象の判別にコマンド列の遷移状態に着目し，ファジィ積分による評価法を用いた[1]．

以下では，文献[1]に示したユーザモデルの構成と，ユーザモデルを用いた認証方法について簡単にまとめる．

あらかじめ，ある期間（ユーザモデル生成期間）にわたって正当なユーザの入力コマンド列を採取しておき，採取した入力コマンド列より，コマンド連鎖を用いてユーザモデルを生成する．

ひとつのコマンド A の出現頻度を N_A とするとその出現確率は $1/N_A$ である．コマンド A からコマンド B へのコマンド連鎖 S_{AB} の出現頻度を N_{AB} とすると，A から B 遷移する確率は $1/N_A \times N_{AB}$ である．出現頻度 N_{AB} のコマンド連鎖 S_{AB} に対する連鎖グレード $G(S_{AB})$ を，λ ファジィ測度の定義[5]-[7]を参考に，次の式 (1) で定義する．

$$G(S_{AB}) = ((1+\mu/N_A)^{N_{AB}} - 1)/\mu \tag{1}$$

ユーザモデルは，学習データ中に現れるすべてのコマンド連鎖の連鎖グレードの組とする．式 (1) におけるファジィ測度パラメータ μ の設定値により，コマンド連鎖の出現頻度の大きい連鎖をより高く評価することができる．なおこの $G(S_{AB})$ は1に規格化されておらず，μ により飽和値が異なる．ユーザモデルは，正当なユーザごとに生成し，必要に応じて更新する．

次に，認証の対象となる入力コマンド列が本人のものであるかどうかを，あらかじめ作成された各ユーザのコマンド入力連鎖によるユーザモデルを用いて評価する方法について説明する．認証評価は λ ファジィ測度の式を参考に，文献[1]で示した評価方法で認証評価を行う．

いま，あるユーザ X' があるユーザ名 X でログインし，長さ $K+1$ のコマンド列 (検査コマンド列) $C_0, C_1, \ldots, C_K$ を入力したとする．これを利用して，X の名前で入力している X' の認証検査をする．X' が入力したコマンド連鎖 $S_i = S_{C_{i-1}C_i}, i = 1 \sim K$ のうち同じコマンド連鎖を集約し出現頻度の昇順にソートして，それを改めて $S_k, k = 1 \sim K_s$ とおく．K_s は異なるコマンド連鎖の数で，コマンド連鎖 S_k の出現頻度を n_k とする．$n_1 \le n_2 \le \ldots \le n_{K_s}$ で，$\sum_{k=1}^{K_s} n_k = K$ である．まず，k 番目のコマンド連鎖 S_k に対し，対応する連鎖グレード $G(S_k; X, X')$ をユーザ X のユーザモデルから求める．

$$G(S_k; X', X) = G(S)|_{S=S_k} \quad \text{of User } X \tag{2}$$

X のユーザモデルにないコマンド連鎖の連鎖グレードは $G(S) = 0$ とする．

λ ファジィ測度の式を参考に，組合せグレード G_r を定義する．$S_i, i = 1 \sim k$ の組合せグレードを $G_r(\{S_1, \ldots, S_k\}; X', X)$ として，式 (3) とする．

$$G_r(\{S_1, \ldots, S_k\}; X', X) = (\prod_{i=1}^{k}(1+\lambda G(S_i)) - 1)/\lambda \tag{3}$$

簡単のため $G(\{S_k\}; X', X)$ を $G(S_k)$ と表してある．$\lambda > -1$ は λ ファジィ測度のパラメータで，$\lambda > 0$ ならば優加法的，$-1 < \lambda < 0$ ならば劣加法的である．本手法では常に $\lambda > 0$ として，使用されたコマンド連鎖の種類が多いほど評価を高くする．

次に，G_r に対して $\{S_1, S_2, \ldots, S_{Ks}\}$ 上のショケ (Choquet) 積分を援用して，式 (4) に示す $I(X'; X)$ を求める．

$$I(X'; X) = \sum_{k=1}^{K_s}(n_k - n_{k-1}) \cdot G_r(\{S_k, S_{k+1}, \ldots, S_{K_s}\}; X', X) \tag{4}$$

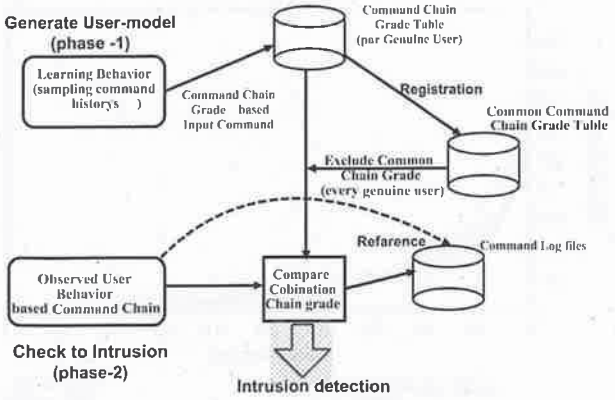

図 1: 本手法を用いた認証手法の流れ

ただし，$n_0 = 0$ である．これを連鎖の数 $K = \sum n_i$ で平均して，認証評価値 $I_m(X'; X)$ を求める．

$$I_m(X'; X) = I(X'; X)/K \tag{5}$$

この I_m が大きいほど本人に近いコマンド連鎖であると判断する．なお，I_m は，1 に規格化されていない．認証判定は，それぞれの正当なユーザ X の過去の認証評価値 $I_m(X; X)$ に基づいた学習を行った結果で認証閾値 $I_{sh}(X; X)$ を定めて，その閾値以上の X' を X であると認証し，閾値未満であれば侵入者として扱う．

$$I_m(X'; X) \geq I_{sh}(X; X) \tag{6}$$

本手法を用いた認証手法の流れを図 1 に示す．

2.2 性能評価に用いる Schonlau データの特徴

ここでいう Schonlau データは，Schonlau らが提供している[10] UNIX システムの acct で採取した入力コマンド列群で，web 上でデータセットとして公開されている[11]．このデータを用いたユーザ挙動に基づいたシステムの異常検出法の評価結果ががいくつか報告されている[10],[12],[13]．

入力コマンド列データはテストユーザ 50 人分で，各テストユーザひとりあたり 15,000 ステップの入力コマンドで総コマンド数 750,000 ステップで構成される．また，各ユーザの入力コマンドについて 100 ステップ単位で 1 セッションのデータとする．つまり，評価実験対象となるセッションは各ユーザあたり 150 セッションである．また全テストユーザ 50 人の検査データ（5,000 セッション）のうち，侵入者データとして 231 セッションがランダムに挿入されている．

図 2 は各テストユーザの検査データについて 1 セッションごとに見られる異なるコマンド連鎖の組み合わせ数の分布を示す．侵入者データを含めコマンド連鎖の組合せ数が比較的広範囲に分布している．

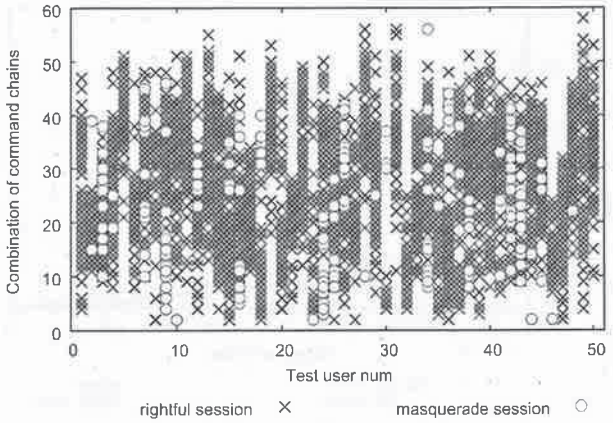

図 2: 侵入者データを含んだ各テストユーザの検査データのコマンド連鎖数の分布

3. Schonlau データに基づく本手法の評価実験

Schonlau データを用いた本手法の評価実験を参考文献に基づき行った[10],[12]．性能の評価は，正当なユーザのセッションにも関わらず侵入者と判断した誤報（false alarm）と侵入者のセッションにも関わらず正当なユーザと判断した欠報（missing alarm）の関係を ROC（Receiver Operating Characteristic）[15]曲線を用いる．ROC 曲線は，式 (6) で示す本人の認証閾値を変化させて閾値ごとに X 軸に誤報率（FAR）を Y 軸に欠報率（MAR）を表して双方の関係を示したものである．この ROC 曲線において認証手法の性能はグラフの軸と ROC 曲線で囲まれた面積が小さい程優れていると判断される[10],[12],[15]．

2.2 節で示したように Schonlau データはテストユーザ 50 人で，ひとりあたり 100 コマンドステップを 1 セッションとした 150 セッションで構成される．テストデータは 100 セッション/1 人で計 5,000 セッションのうちランダムに 231 セッション侵入者データが挿入されている．ここで，評価実験では全テストユーザの正当なセッションデータ 4,769 件と侵入者データの 231 件の認証検査値を用いて，各認証閾値に対応する FAR および MAR を算出することで ROC 曲線を描く．その他，学習モデルの長さやモデル更新の効果と認証性能との関係および式 (4) 等で示される学習モデルと一致する異なるコマンド連鎖の種類数 K_s との関係も実験を通して検討する．

3.1 本手法と他の手法との性能比較実験

性能の比較を行うため，2.2 節で示した条件のもとで，テストユーザひとりあたりの最初の 50 セッション（5,000 ステップ）を正当なユーザの挙動を獲得するため

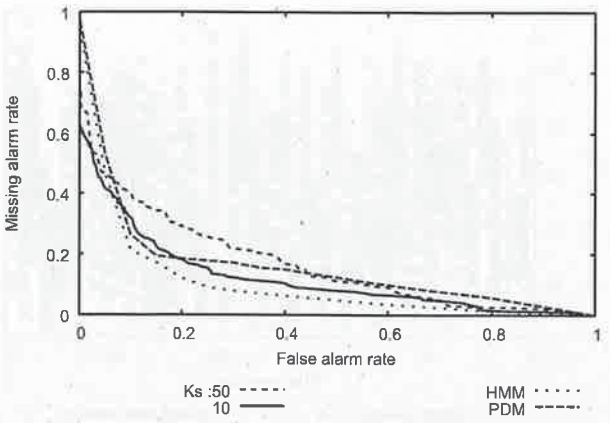

図 3: 本手法と他の確率モデル手法の比較

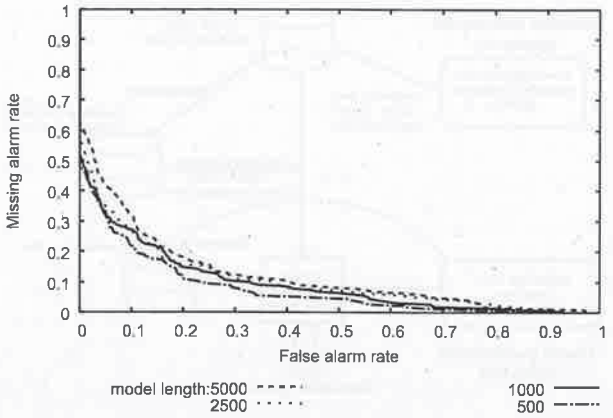

図 4: 学習モデル生成のためのコマンド列の長さと ROC 曲線との関係

の学習データに使用し，残りの 100 セッション（10,000 ステップ）を本人認証（または異常検出）のための検査データとして本手法の評価実験を行った．図 3 にその ROC 曲線を示す．認証評価実験では，一致するコマンド連鎖の種類の数 K_s の違いについても行った．図 3 は K_s を最大 50 とした場合，すなわち検査コマンド列中で学習モデルと一致したコマンド連鎖の大半を評価した場合と，最大 10（一致頻度が上位のコマンド連鎖）とした場合についての ROC を示す．但し，検査評価が 0 となる（一致するコマンド連鎖が全くない）セッションについては ROC 曲線の作成からは除外した．また比較のために，HMM(隠れマルコフモデル) を用いた手法や PDM(出現確率分布モデル) を用いた手法など確率を用いた手法[13],[14]についても併せて示す．

この結果，本手法による認証性能は $K_s = 50$ の場合は他の 2 つの手法と比較してあまり良くならないが，$K_s = 10$ では HMM 手法に近い性能を得ることができる．これは，侵入者の検査コマンド列中に学習モデルと一致するコマンド連鎖の種類が多く含まれ，評価結果も高くなる場合があったためである．それで，一致頻度の低いコマンド連鎖まで強調されてしまうためである．しかし，比較的出現頻度の高いコマンド連鎖に絞って評価することで余分な連鎖を評価対象から除くことができる．

3.2 学習モデル生成のための入力コマンド列の長さとの関係についての検討

3.1 節では他手法の条件と同一にするため，学習モデル生成のためのコマンド列長を 5000 ステップ（50 セッション）固定とした実験結果を示したが，ここでは本手法における学習モデル生成のためのコマンド列の長さに関わる ROC 曲線の変化について検討する．図 4 は $K_s = 10$，ひとつの認証検査コマンド列を 1 セッション=100 ステップとして，学習モデル生成のためのコマンド列の長さを 5,000～500 ステップの 4 種類の長さの違う学習モデルを構成した場合の ROC 曲線をそれぞれ示す．

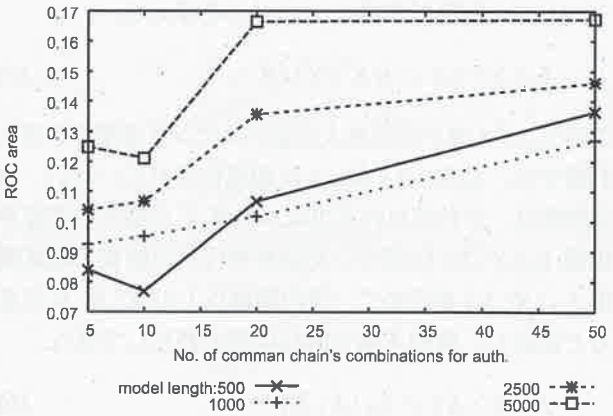

図 5: K_S と ROC 曲線の面積との関係

この ROC 曲線より比較的学習期間の長いモデルでは，認証性能が悪くなっている傾向が見られる．これは学習データが大きくなれば学習されたコマンド連鎖の種類も当然多くなるためで，侵入者データの認証時にも一致するコマンド連鎖数が増加してしまうためである．反対に学習データが小さくなればコマンド連鎖数が少なくなるが，認証検査値が 0 となるセッションも多くなり評価対象セッション数も多くなるための影響も大きい．

図 5 は本手法における K_s および学習モデルのための入力コマンド列長と ROC 曲線と X,Y 軸からなる面積との関係を示す．

比較のため，HMM 手法では ROC 曲線の面積は 0.100，PDM 手法では 0.151 である[12]．

結果より，今回用いた Schonlau データでは K_s は 10

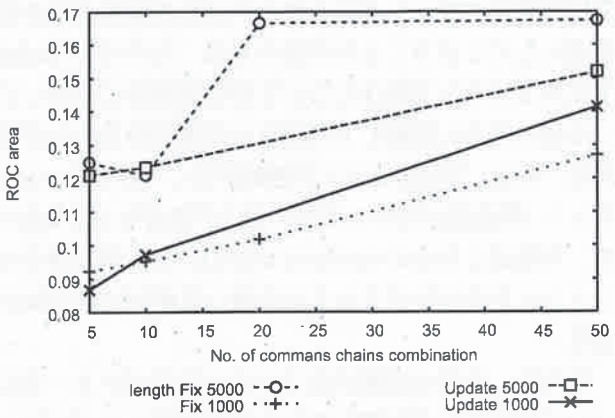

図 6: 学習モデルの更新と認証性能の変化

程度で最小となり，それ以下では反対に増える傾向にある．

学習モデルのための入力コマンド列長は 500〜1,000 程度での評価が良くなった．但し，この実験では学習データ長が小さくなるとモデルに含まれるコマンド連鎖が減少するため検査値 0 のセッションが増える．そのため，評価から除外されるセッションが増えるため，見掛け上認証性能が良くなる傾向がある．

3.3 学習モデルの更新についての検討実験

我々は文献[1],[2]で，ユーザの挙動を利用した侵入検出法では学習モデルを定期的に最新のものに更新することがより効果的であると報告した．この実験では学習モデルの更新による効果を検討するため，各ユーザの初期の学習データは他の手法の条件通り最初の 50 セッションで構成する．各テストユーザの各セッションについて認証実験を行い本人のセッションであると認証されれば，50 セッションのうち最初の 1 セッションを除き，代わって認証された 1 セッションを加えて学習モデルを再構成し更新する．侵入者データと判断したらモデルは更新しない．すなわち，入力コマンド列長はモデルの更新如何に関わらず常に 50 セッションである．このような手順で各ユーザの最後のテストセッションの認証実験までモデルを更新して行く．図 6 は 3.1 節で示したようにモデルを更新なしの場合（Fix) と更新させた場合（Update）について，評価対象となるコマンド連鎖の種類 K_s を X 軸に，ROC 曲線の面積を Y 軸に表す．

図で示すように学習モデルを 50 セッションで構成した場合は明らかにモデルの更新効果が見られた．しかし，10 セッションで構成した場合は期待した効果は見られなかった．この結果より Schonlau データでは比較的長いコマンド列から構成されるモデル，すなわち多くの特徴を含むモデルでは更新は有効であるが，小さい場合はモデルの更新は必ずしも有効とは言えない．

4. 考察

Schonlau データについて ROC 曲線を用いた本手法の性能評価を行ったが，得られた結果を基に本手法の特徴について考察する．

4.1 異なるコマンド連鎖の種類数 K_s と認証評価の関係

まず，認証検査時における学習モデルと認証評価の対象となる一致した異なるコマンド連鎖の種類数 K_S との関係について述べる．本手法を提案した文献[1]では一致した異なるコマンド連鎖の種類数が多い方がより個人の特徴を表すのに有効であると報告した．しかし，3.1 節で示した実験では評価時に必ずしも K_s が大きくても有効とはならないことが解った．この原因として考えられるのは，今回の学習モデルは入力コマンド数を比較的長い 5,000 ステップから構成されるので各テストユーザのモデルには多くのコマンド連鎖が含まれる．そのため，たとえ侵入者セッションの認証検査であっても一致するコマンド連鎖の種類が増える可能性があるので多くの K_s を評価対象とすれば，認証結果も高くしてしまうからであろう．また提供された入力コマンド列は UNIX システムの acct により採取されているので，コマンドの別名付機能（alias）は元の UNIX コマンドに展開された形で採取される．そのため，ユーザ挙動の特徴に大きく影響する別名付機能が利用できないことも原因として挙げられる．しかし実験のように，K_s を評価時に調整することで改善できる可能性があることを示した．

4.2 学習モデル構成のための入力コマンド列長と認証評価との関係

3.2 節で示した実験では学習モデルを構成するための入力コマンド列の長さの違いが与える影響について検討した．この実験では 1,000 ステップ程度のコマンド数で本手法の認証効果が得られることを示した．これは学習モデルに含まれるコマンド連鎖のバリエーションがモデルが大きい程多くなるため，認証時には逆に特徴を強調しにくくし，その結果，侵入者コマンド列との識別が出来にくくなるためであると予想される．

本手法ではユーザの特徴にコマンドの連鎖を用いるため，ユーザ独自のコマンド連鎖が学習モデルに多く含まれれば，モデル構成のためのコマンド数が大きくなるほどファジィ測度によりより個人の特徴が強調されるが，連鎖バリエーションが多い場合は反対に個人

の特徴を弱めてしまう．そのため，あまり長いコマンド数はモデルの構成には適さない．学習モデルのためのコマンド数は検査コマンドとの比が概ね10倍程度で効果的である．実際に本手法によりシステムで運用する場合，ユーザがログオンからログオフまでの1セッションでは数十ステップ～数百ステップ程度であるから10セッション程度で学習モデルを構成すればより効果があると予想できる．

4.3 学習モデルの更新効果

ユーザの挙動を利用した認証法は，ユーザが時間経過とともにシステムの利用目的などが変わる可能性があるので，学習モデルを定期的に更新するのは効果的であると考える．そのため，この実験に使用したコマンド列を時系列データであることを前提に，学習モデルの更新による改善効果を検討した．その結果，K_s を最大50としたようにコマンド連鎖の評価対象を大きくした場合明らかに認証性能の改善が見られた．しかし，K_s を最大10とした場合には期待したような改善が見られずむしろ僅かに悪くなった．これは学習モデルの更新により正当なユーザの出現頻度の高いコマンド連鎖と侵入者のものが上位に来てしまったことで起きたと予想される．そのため，正当なユーザのテストデータの認証検査値も高くなったが侵入者データについても検査値を上げてしまい，結果的に性能を落とすことになったためであろう．

これらの実験結果より本手法を実際のシステムで運用するためには，評価対象とするコマンド連鎖の種類 K_s，学習モデルの大きさ，モデルの更新についてバランス良く調整することで認証性能を上げることができる．

5. まとめ

本稿では対話的計算機環境下におけるユーザの挙動を利用した侵入者検出法（なりすまし）のひとつとして，我々がこれまでに提案したファジィ測度に基づく検出手法について，Schonlauデータを用いた認証評価を報告した．SchonlauデータはUNIXシステムのacctコマンドを元に採取された入力コマンド列である．採取コマンド列にはユーザがシェル上で入力したコマンドの他，プログラム内部で実行されたコマンド，例えばシェルスクリプト内部で実行されるコマンドやXウィンドウマネージャ上で実行されたコマンド，または電子メールの定期的な確認に利用されるバックグラウンドコマンドなどが含まれる．そのため，ユーザが直接入力したコマンド列の間にそれらのコマンドが時系列的にいくつか挿入される場合があるのでコマンド連鎖の間に他のコマンドが挿入されればある程度認証性能を悪くしてしまうことが予想される．その中でHMM手法などコマンド単体についての出現確率に着目している他の手法と比較して同程度の性能を得ることが出来た．但し，今回はコマンド連鎖が全く一致しないセッション（検査値がゼロ）については評価対象としなかった．今後はこれらのセッションについても侵入者セッションとするのかどうかという扱いを検討する必要がある．

その他，今回の実験ではファジィ測度パラメータについてはほとんど影響しなかったので取り上げなかった．しかし，今後，ファジィ測度パラメータの影響をより深く検討する必要がある．

参考文献

[1] 白井治彦，小高知宏，小倉久和，“コマンド入力連鎖による認証におけるファジィ測度的手法の検討”，日本知能情報ファジィ学会論文誌，in press.

[2] 白井治彦，西野順二，小高知宏，小倉久和，“対話的計算機環境におけるコマンド入力連鎖を用いた認証手法の提案”，信学論(A)，Vol.J82-A，No.10，pp.1602-1611，Oct.1999.

[3] 小高知宏，白井治彦，西野順二，小倉久和，“コマンド利用の周期性に基づく個人認証手法の提案”，情報処理学会論文誌，Vol.42，No.10，pp.2533-2536，Oct.2001.

[4] 小高知宏，白井治彦，小倉久和，“コマンド入力系列における特徴のGAによる抽出と認証への応用”，信学論(D)，Vol.J85-D-I，No.5，pp.476-478，May.2002.

[5] 日本ファジィ学会編，“講座ファジィ3 ファジィ測度”，日刊工業新聞社，1993.

[6] 日本ファジィ学会編，“講座ファジィ14 ファジィ理論と人文・社会科学”，日刊工業新聞社，1994.

[7] 高秋栄一郎，“重要度とλによるファジィ測度の同定について”，日本ファジィ学会誌，Vol.12，No.5，pp.665-676，Oct.，2000.

[8] S.Upadhyaya and K.Kwiat，“A distributeed concurrent intrusion detection scheme based on assertions，”，SCS Int.Sysmp. on Pref.Eval. of Comput.and Telecom.Systems，pp.369-376，July 1999.

[9] Teresa F. Lunt, " A survey of intrusion detection techniques " ,Computer & Security,12,pp.405-418,1993.

[10] M.Schonlau etc.,Computer Intrusion:Detecting Masquerades,Statistucal Science,Vol. 16 No.1,pp.58-74,2001.

[11] Matthias Schonlau's HomePage,

http://www.schonlau.net/.

[12] 岡本剛 他," 「なりすまし」ユーザ検知システムの性能評価 ー隠れマルコフモデルと他の確率モデルの比較 ", システム制御情報学会論文誌,Vol.16,No.2,pp.61-69,2003

[13] T.Lane,Hidden Markov Models for human / computer interface modeling, Proc. the IJCAI-99 Workshop on Learning About Users,pp.35-44,1999.

[14] J.Choi and S. Cho,Hidden Markov model for sequence recognition in intrusion detection system,Proc. the 4th International Conference on Advances in Pattern Recognition and Digital Techniques,1999.

[15] J.P.Egan,Signal Detection Theory and ROC Anaysis,Academic Press,1975.