人間の動作に対するアノマリ型異常検知システムの実装

藤原 大輔 † 阿部 洋丈 † 岡部 正幸 †† 梅村 恭司 †
† 豊橋技術科学大学 情報工学系　†† 豊橋技術科学大学 情報メディア基盤センター

1 はじめに

近年，セキュリティシステムはさまざまな場所において需要があり，それぞれの環境に応じたシステムの設計が必要となる．本研究では，環境に依存しないセキュリティシステムの実現を目指し，センサを用いたアノマリ型異常検知システムの実装を示す．本システムの基本方針は先行研究 [1]，[2] を参考とする．別の領域では先行研究 [3] で同様のアプローチがある．今回実装するシステムは，正常動作のみを定義して学習データからその行動の確率モデルを生成し，そのモデルに合致しない行動を異常と判定する．

2 実験環境と定義イベント

実験環境は研究室とし，研究室内にシステムの入力となる 12 個の焦電型センサ $s_1, s_2, \ldots, s_{12}$ を配置する．研究室の上面図とセンサの配置を図 1 に示す．焦電型センサとは，センサの取得範囲で物が動いたときにオンとなるものである．今回はオンを 1，オフを 0 とする 2 値センサとして使用する．

正常動作（以下，定義イベント）を “入口から入室して各席に着席する動作” と設定し，時刻 n に各席 $desk_i$ に座るイベントを $e_i(n) = 1$ と表す．ここで $e_i(n) = 1$ となる n は着席した時刻のみであり，かつ，そのときに限るとする．

3 センサデータの時間圧縮

焦電型センサによるセンシングの時間間隔は 0.2 秒である．今回は通常の人間の動きを対象としているため，この時間間隔は妥当であると考える．

さらに，0.2 秒間隔の時系列データを圧縮することを考える．これは，時間軸に対する人間の動作のゆれやセンサのノイズに対応するため，および，動作の終了タイミングを表現するための処理である．以下の二つの場合に，圧縮後のデータとしてセンサ値を保存する．

(a) 以前にセンサ状態が変化した時刻から
　一定時間 T_1 経過後にセンサ状態が変化した場合
(b) 一定時間 T_2 センサ状態に変化がない場合

焦電型センサの性質から，何らかの動作が発生した場合はオフからオンになる，および，定常状態では多くの場合センサがオフになると想定する．(a) は動作部分の抽出に対応し，センサが連続でオンとなる状態を圧縮後時間軸の単位時間にうまく表現できる．また一定時間 T_1 を設けることでセンサのノイズを除去している．(b) は定常状態の記録に対応しており，後に述べる動作を判定するタイミングに等しい．この時間圧縮は，(a) で定める一定時間 T_1 を最小圧縮時間とし，(b) で定める一定時間 T_2 を最大圧縮時間とする可変圧縮であり，学習データの時間的なゆれを吸収できると考える．一定時間のパラメータは，対象が人間の行動であるため経験的に $T_1 = 1.0$ 秒，$T_2 = 6.0$ 秒と定める．

Implementation of Anomaly Detection System for Human Behavior
† Daisuke FUJIHARA
† Hirotake ABE
†† Masayuki OKABE
† Kyoji UMEMURA
Depertment of Information and Computer Sciences, Toyohashi University of Technology (†)
Information and Media Center, Toyohashi University of Technology (††)

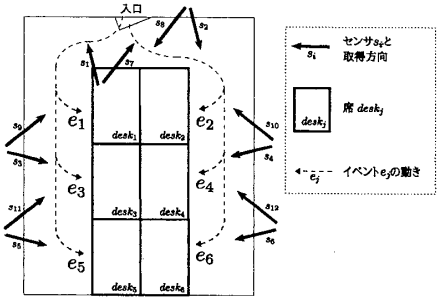

図 1　センサ配置と定義イベント

4 イベント発生確率の推定

いま，センサの集合 S_p と，ある時間定数 K_p というパラメータに対して，時刻 $n-K_p$ から $n-1$ までのセンサ集合 S_p の状態の観測値 $\dot{S}_p(n-K_p, n-1)$ が与えられたとする．このとき時刻 n における定義イベント $e_p(n)$ の発生確率を推定したい．観測値 $\dot{S}_p(n-K_p, n-1)$ を条件とするイベント $e(n)$ の発生確率の推定値を式 (1) と定義する．

$$\hat{\mathrm{P}}(e_p(n) = 1 | \dot{S}_p(n-K_p, n-1)) \qquad (1)$$

ここで，イベント $e_p(n)$ を推定する際に必要な二つのパラメータ S_p，および，K_p をどのように決定するかという問題がある．S_p は条件となる観測値をもつセンサ集合であり，K_p はどのくらい過去の状態まで対象にするかを表す時間軸探索数であるが，S_p をセンサの全集合とすることや $K_p = \infty$ とすることは，計算効率が悪く，ノイズの影響などによる判別性能の低下を招くため好ましくない．したがって，各イベントに適応するパラメータの導出が必要となる．

4.1 イベントに反応するセンサの学習

イベントの発生確率を推定するために用いるセンサの集合を，学習データから求める．求めるセンサの条件は，イベントの発生に反応していることである．焦電型センサの性質から定常状態ではセンサがオフになることが多くなるので，ここでの “反応” とはセンサがオンになることとする．

学習データとして，焦電型センサの時間圧縮後のデータを与える．時間圧縮後のイベント e_i の発生時刻を基準にして，K_{e_i} 時刻前までのセンサ状態を確率変数としてモデルに含める範囲とする．ここでセンサ間の依存関係はないものとする．そして反応するセンサの集合 S_{e_i} と K_{e_i} が与えられるとき，イベント e_i と S_{e_i} の同時確率は式 (2) となる．

$$\mathrm{P}(e_i(n), S_{e_i}(n-K_{e_i}, n-1)) = \mathrm{P}(e_i(n)) \prod_{s_p \in S_{e_i}} \prod_{k=1}^{K_{e_i}} \mathrm{P}(s_p(n-k) | e_i(n)) \quad . \qquad (2)$$

イベントに反応するセンサを求めるために，時刻 n でイベント e_i が発生した時に，時刻 $n-k$ でセンサ s_p がオンとなる条件付確率 $\mathrm{P}(s_p(n-k) = 1 | e_i(n) = 1)$ を利用する．この条件付確率は学習データから推定できる．これより，イベント e_i に反応するセンサ集合 S_{e_i} を式 (3) で定義する．ここで閾値 0.7 は，実際のデータをもとにして定めている．

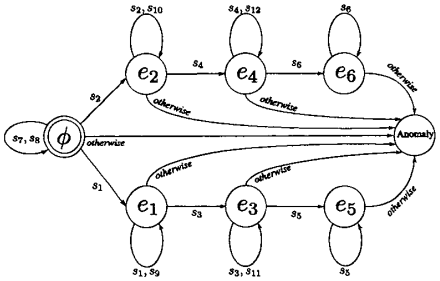

図 2　オートマトンの状態遷移図

$$S_{e_i} = \{s_p | \exists k \in \{1, \ldots, K_{e_i}\} \\ \mathrm{P}(s_p(n-k) = 1 | e_i(n) = 1) \geq 0.7\}. \quad (3)$$

4.2　時間軸探索数の決定法

各イベントに対してどこまでの時間範囲を確率分布の変数として含めるかはイベント依存であるので，環境非依存性の実現のためには学習データから求めるのが望ましいと考える．以下に時間軸探索数を学習データから求める方法を示す．

式 (4) に示すように，K_{e_i} は，$\mathrm{P}(s_p(n-k) = 1 | e_i(n) = 1)$ が高い範囲で最大の k とする．すなわち，イベントと関連性のあるセンサにおいて最も過去にオンとなった時刻からイベントごとの時間軸探索数を決定する．式 (4) で S_{ALL} はセンサの全集合である．

$$K_{e_i} = \max_{\substack{\forall s_p \in S_{\mathrm{ALL}}, \forall k \in \{1, \ldots, \infty\} \\ \mathrm{P}(s_p(n-k) = 1 | e_i(n) = 1) \geq 0.7}} k \quad . \quad (4)$$

5　隣センサの学習

4.1 節では，各イベントに対してオンになるセンサを反応のあるセンサとして学習した．ここで，オフのセンサが有用な情報をもつ場合もある．この場合，オンとなるかオフとなるかの境目にあるセンサが該当するといえる．そこで，イベントに対して反応のあるセンサの隣に位置するセンサを，イベントごとに定める入力用のセンサ集合に加えることとする．

隣位置のセンサは学習データから求めることとし，センサ s_p の隣にあるセンサ s_q の条件は式 (5) を満たすものとする．ただし隣のセンサは基準となるセンサ s_p に対して最大 2 個なので，式 (5) の左辺値が大きい順に二つ選ぶ．

$$\frac{\mathrm{fr}(s_q(n) = 1, s_p(n-1) = 1)}{\sum_{j \neq p} \mathrm{fr}(s_j(n) = 1, s_p(n-1) = 1)} > 0.2 \quad . \quad (5)$$

ここで $\mathrm{fr}(a(n) = 1, b(n-1) = 1)$ は，学習データ中にセンサ状態が $a(n) = 1, b(n-1) = 1$ となった回数である．n は任意時刻である．

なおこの方法は結果におけるセンサ配置の論理性を保証していないが，有用な情報を持つセンサの選択という目的においては厳密に隣である必要はないと考える．

6　判定方法

ベイズの定理を用いれば，式 (2) の同時確率から，時刻 $n - K_p$ から $n-1$ までのセンサ集合 S_{e_i} の状態の観測値 $\dot{S_{e_i}}(n - K_{e_i}, n-1)$ が与えられたときのイベント e_i の発生確率が推定できる．

$$\hat{\mathrm{P}}(e_i(n) = 1 | \dot{S_{e_i}}(n - K_{e_i}), n-1) \\ = \frac{\mathrm{P}(e_i(n) = 1, \dot{S_{e_i}}(n - K_{e_i}, n-1))}{\mathrm{P}(\dot{S_{e_i}}(n - K_{e_i}, n-1))} \\ = \frac{\mathrm{P}(e_i(n) = 1, \dot{S_{e_i}}(n - K_{e_i}, n-1))}{\sum_{v \in \{0,1\}} \mathrm{P}(e_i(n) = v, \dot{S_{e_i}}(n - K_{e_i}, n-1))} \quad . \quad (6)$$

表 1　定義イベント判別

方法	正解	不一致	アノマリ
$K_{e_i} = 2$	0.99	0.01	0.00
$K_{e_i} = 4$	0.89	0.07	0.04
$K_{e_i} = 6$	0.82	0.08	0.10
$K_{e_i} = 8$	0.69	0.18	0.13
学習による K_{e_i}	0.72	0.16	0.12
オートマトン	0.39	0.03	0.57

表 2　アノマリ動作検知

方法	アノマリ	検知漏れ
$K_{e_i} = 2$	0.00	1.00
$K_{e_i} = 4$	0.21	0.79
$K_{e_i} = 6$	0.63	0.37
$K_{e_i} = 8$	0.90	0.10
学習による K_{e_i}	0.73	0.27
オートマトン	0.97	0.03

この事後確率を推定するタイミングは，タイムアウトの発生とする．タイムアウトとはすべてのセンサの状態が一定時間変化がないことを表し，イベント発生後は定常状態になるという仮定のもとにこの時点で判定する．タイムアウトの閾値は 6.0 秒とする．

式 (6) に学習データを入力すると，各イベント e_i ごとに最小値 $P_{min}(e_i)$ が求まる．アノマリか定義イベントかの判定には式 (7) で表される，テストデータから得られる事後確率と $P_{min}(e_i)$ との比をを用いる．

$$\frac{\mathrm{P}(e_i(n) = 1 | \dot{S_{e_i}}(n - K_{e_i}, n-1))}{P_{min}(e_i)} \quad (7)$$

すべての定義イベント e_i に対して式 (7) を計算し，1.0 以上のイベントのなかで最も大きいものをシステムが判別したイベントとする．また，すべてのイベントにおいて式 (7) が 1.0 未満であればシステムはアノマリと判定する．

7　実験

ベースラインとしてオートマトンを設計し比較した．システムには学習データとして各定義イベント 24 件のセンサデータを与え，各定義イベント 6 件のテストデータで定義イベント判別を，アノマリ動作 6 種類（席のまわりをうろつく）それぞれ 6 件のテストデータでアノマリ検知を実験した．結果を表 1，表 2 にそれぞれ示す．性能改善の余地は残るが，オートマトンのようにセンサ配置や定義イベントを考慮せずにシステムが動作していることを確認した．

8　おわりに

環境に依存しないセキュリティシステムを目指した，アノマリ型異常検知システムを実装した．

謝辞　この研究は，戦略的情報通信研究開発推進制度（SCOPE）の課題「インターユビキタスネットワーク情報基盤の研究」の成果である．また，平成 20 年度科学研究補助金課題番号（19500120）の研究成果を使用した．

参考文献

[1] 青木茂樹, 大西正輝, 小島篤博, 菅原康博, 福永邦雄. 人感センサによる独居高齢者の行動パターンの認識. 電子情報通信学会技術研究報告. WIT, 福祉情報工学, Vol. 101, No. 703, pp. 43–48, 2002.

[2] 関弘和, 多田隈進. 全方位センサのベイジアンネットワーク表現に基づく高齢者非日常行動検出モニタリングシステム. 電気学会論文誌 D（産業応用部門誌）, Vol. 128, No. 8, pp. 1052–1059, 2008.

[3] C. Kruegel, D. Mutz, W. Robertson, and F. Valeur. Bayesian event classification for intrusion detection. In *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*, pp. 14–23, 2003.