Proposta de um Sistema de Apoio à Tomada de Decisão para o Monitoramento Remoto de Centrais de Alarme Patrimoniais

Alex Luiz de Sousa [1]
André Bittencourt Leal [2]
Ricardo Ferreira Martins [3]
Claudio Cesar de Sá [3]

Resumo: Este artigo apresenta uma proposta de sistema de apoio à tomada de decisão para o monitoramento remoto de centrais de alarme patrimoniais. A base do sistema é modelada com autômatos finitos determinísticos e o apoio à tomada de decisão emprega indução de árvores de decisão e raciocínio baseado em casos. Um protótipo de sistema foi desenvolvido para fins de validação e testes.

Palavras-chave: Sistemas Eletrônicos de Segurança. Autômatos Finitos. Árvores de Decisão. Raciocínio Baseado em Casos.

Abstract: *This article proposes a system to support decision making for the remote monitoring of commercial and residencial central alarm systems. The basis of the system is modeled with deterministic finite automata and the support for decision-making uses of induction of decision trees and case-based reasoning. A prototype system was developed for validation and testing.*

Keywords: *Electronic Security Systems. Finite Automata. Decision Trees. Case-Based Reasoning.*

1 Introdução

A vigilância patrimonial é uma atividade da segurança privada que trata de medidas de proteção para a segurança patrimonial de estabelecimentos públicos ou privados, além da segurança física e da integridade de pessoas [1]. Essas medidas incluem, de forma geral, a instalação de dispositivos eletrônicos (sensores, detectores), equipamentos de segurança (centrais de alarme, câmeras, barreiras) e recursos humanos para a proteção dos interesses de seus segurados. O monitoramento remoto de Sistemas Eletrônicos de Segurança (SESs) representa a principal atividade (mais lucrativa) das empresas do ramo. Entretanto, apesar de ser uma atividade que está em constante fase de expansão, principalmente em soluções tecnológicas, apresenta uma problemática na determinação de ações estratégicas para a tomada de decisão. Essa problemática está relacionada a inconsistências (falta de informações precisas e pontuais) nos Sistemas de Monitoramento de Centrais de Alarme Patrimoniais (SMCAPs) e falhas devidas ao fator humano, que acabam prejudicando o processo de tomada de decisão.

Nesse contexto, uma tomada de decisão é uma ação a ser seguida (estratégia), definida pelo profissional que opera o SMCAP quando ocorrências de alarme são sinalizadas pelos SESs instalados nos bens patrimoniais. É baseada em dados históricos e experiências individuais vividas pelo profissional, que, normalmente, toma decisões sem nenhum apoio do sistema. Além disso, foi verificado que vários SMCAPs apenas exibem as mensagens de alarme recebidas [2], [3], [4], sendo necessária a experiência de um profissional para poder

[1,2,3]UNIVERSIDADE DO ESTADO DE SANTA CATARINA - UDESC [http://www.udesc.br]
[1]Departamento de Sistemas de Informação (DSI) - Centro de Educação do Planalto Norte (CEPLAN)
{alex.sousa@udesc.br}
[2]Departamento de Engenharia Elétrica (DEE) - Centro de Ciências Tecnológicas (CCT)
{leal@joinville.udesc.br}
[3]Departamento de Ciência da Computação (DCC) - Centro de Ciências Tecnológicas (CCT)
{claudio,rfm@joinville.udesc.br}

http://dx.doi.org/10.5335/rbca.2011.1311

interpretá-las e definir estratégias de ação. No entanto, nem sempre a estratégia seguida é a mais adequada, pois a quantidade de associações lógicas (p. ex.: o cenário monitorado, o projeto de segurança, histórico de ocorrências, sequência de mensagens, equipamentos instalados) pode ser muito complexa para o raciocínio humano refletir uma decisão rápida e coerente, em situações nas quais o tempo de resposta é fundamental. Além disso, em contrapartida com um sistema que apresente insuficiência de informações, informações errôneas, ou atrasos e falhas na recepção de mensagens, os erros que comprometem a tomada de decisão tornam-se muito mais propícios de acontecer.

Segundo [5], a falha humana é uma grande preocupação em qualquer área de trabalho. Nos SMCAPs, erros de percepção, erros de decisão e erros de ação podem ser resultados de falha humana. Esses erros são causados principalmente por tentativas de soluções ou decisões equivocadas, negligência ou incompetência, erros pelo desvio de uma norma existente, ou pelo excesso de estímulos interpretados por uma mesma pessoa (p. ex.: muitas mensagens de alarme num SMCAP). Contudo, erros de tomada de decisão, sejam causados por falha humana ou sejam influenciados por problemas ou deficiências nos sistemas de monitoramento, podem gerar prejuízos significativos às empresas de vigilância patrimonial. Por exemplo, o envio de supervisão motorizada para a verificação de falsos alarmes, gastos com ligações telefônicas para contatar clientes e compensações financeiras (p. ex.: processos judiciais). No entanto, inclusive situações envolvendo risco de vida são possíveis de acontecer. Para os clientes isso também causa desconforto, insegurança e denota uma visão de despreparo por parte da empresa prestadora de serviços.

Para o desenvolvimento de uma solução computacional, é necessário que o domínio de conhecimento no qual um problema está situado seja bem compreendido. Entretanto, geralmente algumas empresas desenvolvem soluções isoladas (paliativas), baseadas em seu próprio planejamento de segurança e que não refletem as reais necessidades do setor como um todo. Porém, como é facultada às empresas de segurança privada a criação do seu próprio planejamento de segurança [6], são encontradas poucas pesquisas voltadas ao dimensionamento detalhado do setor.

Assim, houve uma dificuldade em consolidar um estudo sistemático sobre a forma como as empresas prestadoras de serviços de vigilância patrimonial atuam, inclusive porque o acesso a algumas informações expõe vulnerabilidades sobre os serviços prestados. Entretanto, manuais e documentos técnicos sobre centrais de alarme, dispositivos e SMCAPs podem ser encontrados como referência. Essas informações, juntamente com a figura de um especialista da área, constituem o conhecimento aplicado ao desenvolvimento do sistema, que está dividido em duas etapas: a modelagem da base de um SMCAP consistente e o projeto de uma ferramenta de apoio à tomada de decisão.

Na primeira etapa, um formalismo baseado em Autômatos Finitos Determinísticos (AFDs) é definido, visando à construção de modelos genéricos para representar o comportamento de SESs. A modelagem é fundamentada em conceitos de AFDs porque os SESs também assumem um número finito e predefinido de estados, o que os caracteriza como um sistema de estados finitos [7]. Outra característica nos SESs é que não existe paralelismo ou concorrência, pois as mensagens de alarme são enviadas na ordem em que ocorrem, ou seja, seguindo uma sequência. Portanto, um SES não pode estar em mais de um estado ao mesmo tempo (não existe o não-determinismo), o que favorece o uso de AFDs para o desenvolvimento de um SMCAP com uma base bem consolidada. Os modelos de SESs projetados são de fácil compreensão e utilização, e uma significativa base teórica e resultados práticos empregando autômatos também podem ser encontrados na literatura [8], [9], [10].

Na segunda etapa, para o projeto de uma ferramenta de apoio à tomada de decisão é utilizado um algorítimo de indução de árvores de decisão (C4.5) e o Raciocínio Baseado em Casos (RBC). As árvores de decisão têm a vantagem de poderem ser aplicadas a qualquer tipo de dados e revelam-se normalmente robustas e insensíveis a erros de classificação [11]. Segundo [12], elas também representam uma boa opção para solução de problemas de classificação em termos de desempenho. Seu uso foi adotado não apenas pela eficiência das técnicas de classificação, mas pela facilidade de compreensão dos resultados produzidos. Porém, a definição de regras para compor o padrão de treinamento não é uma tarefa trivial, exigindo um certo nível de conhecimento específico sobre como resolver o problema. O RBC permite solucionar problemas em domínios de conhecimento que não são completamente resolvidos [13], mas é necessário que se tenha uma base de casos mínima já formada. A técnica também auxilia na solução rápida de problemas, evitando tempo desnecessário em derivar respostas de um ponto de partida inicial, além de fornecer ao utilizador uma justificativa de como a solução foi tomada.

Muitos trabalhos envolvendo monitoramento remoto podem ser encontrados na literatura, inclusive com propostas de soluções para problemas análogos ao problema proposto [14], [15], [16], [17]. Segundo [18], também existem várias técnicas que podem ser empregadas na classificação de padrões, como Redes Neurais, Algoritmos Genéticos, Lógica Fuzzy, Rough Sets, entre outras. Entretanto, a eficiência de uma técnica é dependente do tipo de problema que está sendo resolvido, pois não existe a melhor técnica de todas, mas, sim, aquela mais adequada para um dado problema.

Outro fato é que a solução computacional para o problema descrito não deve-se basear unicamente em conhecimentos gerais sobre o domínio do problema, pois também existe a necessidade de se levar em consideração a opinião de um especialista. Nesse sentido, as técnicas de indução de árvores de decisão e de raciocínio baseado em casos são complementares e podem perfeitamente ser aplicadas na solução do problema. As seções seguintes apresentam uma visão geral dos SESs, juntamente com a modelagem da base do SMCAP, a modelagem da ferramenta de apoio à tomada de decisão e os experimentos realizados neste trabalho.

2 Visão Geral dos SESs

Os Sistemas Eletrônicos de Segurança (SESs) são constituídos normalmente por uma central de alarmes e um conjunto de dispositivos de detecção. São instalados nos clientes, geralmente estabelecimentos comerciais ou residenciais, e monitorados por empresas que prestam serviços de vigilância eletrônica. Segundo [19], todos os SESs têm três funções em comum: detecção, controle e sinalização, conforme ilustrado na Figura 1.

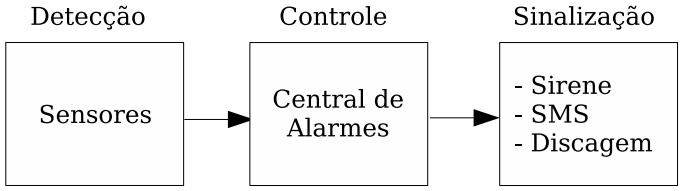

Figura 1. Funções básicas de um SES.

A entrada de sinais (*Detecção*), normalmente feita por dispositivos conhecidos como *sensores*, pode acionar contatos que são sentidos pela *central de alarmes* (*Controle*). Esse impulso (ou sinal) representa nos SESs uma saída que se alterna entre dois estados: contato *aberto* ou contato $fechado$ [4]. As centrais de alarme possuem um número limitado de zonas de proteção, que consistem de entradas dedicadas (bornes) para a conexão de sensores. Elas não identificam fisicamente que tipo de sensor está conectado a cada borne; apenas detectam quais zonas estão com o circuito *aberto* ou $fechado$. A central (ou controle) produz saídas (*Sinalização*) que podem disparar uma sirene ou campainha e enviar mensagens de alarme para comunicar a empresa de vigilância. A comunicação ocorre, normalmente, via linha telefônica convencional ou GPRS. Mas também pode ser feita por redes TCP/IP [20] [21], reduzindo custos com serviços de telefonia e proporcionando um monitoramento mais efetivo.

As mensagens de alarme devem seguir um *protocolo* (formato) comum para que haja comunicação entre o SES e o SMCAP. Um protocolo padrão de mercado, adotado por inúmeros fabricantes para prover a compatibilidade de seus equipamentos com equipamentos de terceiros, é o Contact ID [22]. O formato de uma mensagem é dado por: $ACCT\ QZXY\ GG\ CCC$, onde $ACCT$ identifica o *cliente* que originou a mensagem; Q identifica o *tipo de evento* (1: novo evento, 3: restauração, 6: reportagem); ZXY identifica o *código do evento*; GG identifica o *grupo* ou *partição* monitorada pela central de alarmes, e CCC identifica a *zona de proteção* ou *usuário* que originou o evento. Os campos Q e CCC da mensagem estão diretamente relacionados com esta modelagem. Uma lista completa de todos os códigos de eventos é encontrada na documentação do Contact ID [5].

[4] Sensores configurados tipo N.C. (*Normally-Close*) são mais utilizados em SESs.
[5] SIA DC-05-1999.09

3 Modelagem da Base do SMCAP

A modelagem da base do SMCAP é definida segundo conceitos de AFDs, considerando informações sobre a visão geral dos SESs (seção 2) e o perfeito funcionamento dos equipamentos e dispositivos.

3.1 Representação de uma Central de Alarme

As centrais de alarme podem ser classificadas de acordo com o número de zonas de proteção. A representação formal de uma central de alarme é dada por uma n-tupla de valores:

$$C_n = (z_1, z_2, z_3, ..., z_n) \tag{1}$$

Logo, n corresponde ao número de zonas de proteção de determinada central C_n, e z_i pertence ao conjunto $\{0, 1\}$ (contato $fechado$ (0) ou contato *aberto* (1)), de acordo com a situação de cada zona. Por exemplo, uma central de alarmes com cinco zonas de proteção $C_5 = (z_1, z_2, z_3, z_4, z_5)$ representando as zonas z_1 e z_3 com contatos abertos: $C_5 = (1, 0, 1, 0, 0)$. No exemplo os *1's* representam as zonas *abertas* em sinal de alarme e os *0's*, as zonas $fechadas$ ou restabelecidas.

3.2 Modelagem de uma Planta Genérica

Uma planta genérica é um modelo que define o comportamento global de cada SES em um SMCAP. Os SMCAPs podem monitorar o comportamento de vários SESs ao mesmo tempo. A planta é dita genérica porque um mesmo modelo de planta pode ser utilizado por SESs distintos, desde que tenham o mesmo número de zonas de proteção. Nesse formalismo, uma planta genérica é modelada por um autômato finito determinístico $G = (\Sigma, Q, \delta, q_0, F)$, onde: Σ representa o *alfabeto de entrada* aceito pela planta; Q, o *conjunto de estados* que compõe a planta; δ, a *função de transição* de estados; q_0, o *estado inicial* da planta, e F, o *conjunto de estados finais*.

Cada central de alarme C_n (equação 1) é representada por uma planta genérica G_n independente. O exemplo da Figura 2 ilustra o modelo de uma planta G_3 para uma central de alarmes C_3. Este modelo é o mesmo empregado para qualquer SES com uma central de alarmes com três zonas de proteção. A modelagem será detalhada seguindo a explicação deste exemplo.

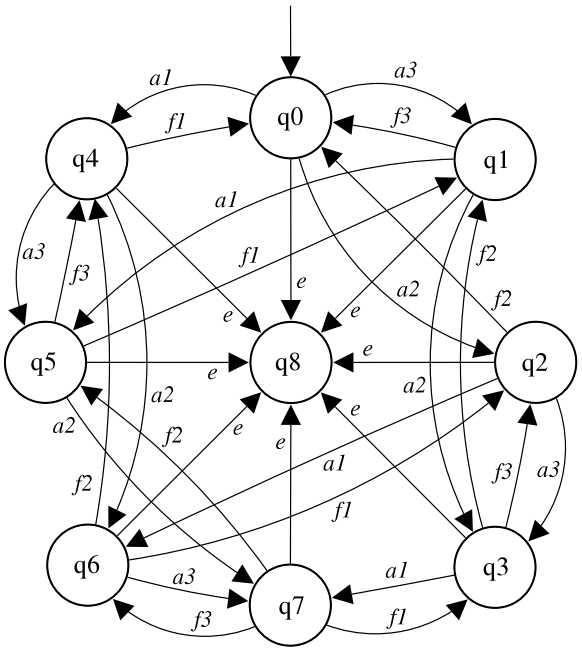

Figura 2. Modelo de uma planta genérica G_3.

Cada planta genérica G_n possui um *alfabeto de entrada* Σ comum. O alfabeto para uma planta G_3 é dado por $\Sigma = \{a_1, a_2, a_3, f_1, f_2, f_3, e\}$. Um alfabeto de entrada para uma planta G_n é dado por:

$$\Sigma = \{a_1, ..., a_n, f_1, ..., f_n, e\} \tag{2}$$

onde a_j e f_j representam, respectivamente, a *abertura* e o *fechamento* de uma zona j (com $j = 1$ a n) e n representa o número de zonas de proteção. O símbolo e representa o evento de todas as transições que levam ao estado de erro. No exemplo da Figura 2, o estado de erro de uma planta G_3 é identificado por q_8. Durante o monitoramento, os a's e f's devem ser mapeados do campo Q de uma mensagem em Contact ID, e j mapeado do campo CCC da mesma mensagem (seção 2). O símbolo e também é mapeamento dos campos Q e CCC sempre que alguma anomalia é detectada no sistema. O número de símbolos de um alfabeto de entrada Σ é dado por:

$$|\Sigma| = 2n + 1 \tag{3}$$

onde $|\Sigma|$ representa o total de símbolos do alfabeto Σ e n, o número de zonas de proteção. Nem todas as mensagens do Contact ID influenciam mudanças de estado na planta. Algumas mensagens são apenas reportagens sobre alterações no sistema (p. ex.: mudanças na programação da central), que devem ser exibidas e armazenadas pelo SMCAP. Apenas as mensagens de interesse, que influenciam mudanças de estado na planta, devem ser mapeadas para o alfabeto de entrada.

O *conjunto de estados* Q é um conjunto finito e predefinido de estados, ou seja, todos os estados de Q são conhecidos. Cada estado da planta deve representar a visão geral do sistema num dado momento, informando quais zonas de proteção estão *abertas* ou *fechadas*. Essa definição está relacionada com a representação formal das centrais de alarme (equação 1). O conjunto Q também inclui um estado de erro, que indica a ocorrência de anomalias detectadas pelo sistema. Essas anomalias podem ser resultado de falhas na comunicação, intervenção humana e defeitos nos sensores ou na própria central. São comportamentos raros, mas não improváveis de acontecer, que podem ser previstos mas não podem ser tratados pelo sistema sem intervenção externa (p. ex.: resetar um SES ou reparar um link de comunicação). A Tabela 1 mostra a definição do conjunto de estados para o exemplo da Figura 2.

Tabela 1. Conjunto de estado de uma planta G_3.

Q	z_1	z_2	z_3
q_0	0	0	0
q_1	0	0	1
q_2	0	1	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$
q_7	1	1	1
q_8	*Erro*		

Cada linha da tabela define um estado (de q_0 a q_8) e cada estado representa a visão geral das zonas de proteção (de z_1 a z_3) a cada evolução da planta. O número de estados para uma planta genérica G_n é dado por:

$$\omega = 2^n + 1 \tag{4}$$

onde ω representa o total de estados da planta e n, o número de zonas de proteção. A exemplo da Figura 2, uma planta genérica G_3 possui nove estados.

Os SMCAPs analisados apenas exibem mensagens de alarme sem apresentar uma visão geral do sistema. A abordagem proposta valoriza essa informação, pois acredita-se ser essencial ao processo de tomada de decisão para classificar perfis de ocorrência distintos. No entanto, o estado de erro representa um estado de poço (desconhecido), onde não é mais possível afirmar a situação atual das zonas de um SES.

Atingido este estado, um SMCAP volta a operar da forma tradicional, ou seja, apenas exibindo as mensagens de alarme para o operador do sistema. A tomada de decisão não pode mais ser analisada com base na planta, já que algumas anomalias podem significar o não recebimento de mensagens de alarme. Esse é um problema comum para todos os tipos de SMCAPs, que estão dependentes do perfeito funcionamento dos meios de comunicação e dos SESs.

A *função de transição* δ permite a transição de estados no autômato em função da ocorrência de eventos. A saída da função δ é um elemento de Q e usa como argumentos o estado atual e um símbolo para definir o próximo estado da planta ($\delta : Q \times \Sigma \rightarrow Q$). Um AFD é dito determinístico porque para cada estado existe, no máximo, apenas uma transição saindo do estado com ela como rótulo. De fato, a modelagem baseada em AFDs se identifica com os SESs, pois não é característica desses sistemas o envio simultâneo de mensagens de alarme.

De acordo com o funcionamento das centrais de alarme e do protocolo Contact ID (seção 2), qualquer zona de proteção aberta só pode ser reaberta se antes for fechada, e qualquer zona fechada só pode ser novamente fechada se antes for aberta. Qualquer comportamento fora desse padrão leva ao estado de erro. Assim, define-se que para cada estado normal (conhecido) existe uma transição que leva ao estado de erro (desconhecido). E a cada nova transição entre estados normais uma única zona de proteção deve ser alternada. Logo, a função de transição δ é parcial, pois não existe a necessidade de defini-la para todos os elementos de Σ a cada estado de Q. O número de transições de uma planta genérica G_n é dado por:

$$\pi = n2^n + 2^n \tag{5}$$

onde π representa o total de transições e n, o número de zonas de proteção. A exemplo da Figura 2, uma planta genérica G_3 possui 32 transições.

Quando uma central de alarme precisa ser ativada (armada), todas as zonas de proteção devem estar $fechadas$ (seção 2); caso contrário, ela permanecerá desativada. Define-se que o *estado inicial* q_0 de uma planta genérica G_n deve representar o estado de ativação de um SES. Logo, o estado q_0 representa a condição normal de funcionamento do sistema, e qualquer outro estado da planta representa uma condição de alarme ou de erro. A ativação e desativação de um SES não é modelada na planta, pois depende de intervenção externa e dos meios de comunicação utilizados no monitoramento. Portanto, é tarefa do software sincronizar o carregamento das plantas de acordo com a ativação do SES.

Nesta modelagem, define-se que o *conjunto de estados finais* F é um conjunto vazio ($F = \{\}$). A marcação de estados foi desconsiderada porque o principal objetivo é observar a sequência de eventos na ordem em que ocorrem, não a conclusão de tarefas. Por fim, para que a base do SMCAP possa disponibilizar informações precisas e pontuais para a ferramenta de apoio à tomada de decisão, a definição de AFDs foi estendida. Assim, a exemplo da máquina de Mealy [7], uma palavra de saída associada à transição foi incluída e é gerada sempre a cada nova evolução da planta genérica de um dado SES.

4 Modelagem da Ferramenta de Apoio à Tomada de Decisão

A modelagem da ferramenta de apoio à tomada de decisão, que emprega o uso de indução de árvores de decisão e raciocínio baseado em casos, é uma particularidade deste trabalho e constitui informações úteis para definir perfis de ocorrência distintos.

4.1 Projeto de Segurança Complementar

O projeto de segurança complementar compreende um conjunto de dados específicos sobre a topologia física (patrimônio), além de definições e associações relacionadas com a modelagem da base do SMCAP (seção 3). Esses dados tangem sobre a análise conceitual dos seguintes itens de interesse:

- **Patrimônio Monitorado**: um patrimônio monitorado pode possuir um conjunto de várias áreas distintas $PM = \{A_1, A_2, A_3, ..., A_j, ..., A_m\}$ que, geralmente, se encontram separadas por paredes ou

divisórias (p. ex., cômodos de uma residência ou salas de um escritório). Logo, cada área normalmente está associada a uma ou mais zonas de proteção, de forma que $A_j \subseteq C_n$ para $j = 1, 2, ..., m$.

- **Tipos de Áreas**: as áreas podem ser identificadas segundo três tipos de classificação: *áreas de perímetro* (P), são áreas que têm seus limites (perímetro) protegidos por sensores de barreira (p. ex., pátio); *áreas externas* (E), são áreas edificadas que permitem acesso externo, normalmente através de portas ou janelas (p. ex., garagem); *áreas internas* (I), não podem ser acessadas diretamente por estarem localizadas dentro de áreas externas (p. ex., corredor).

- **Tipos de Ação**: dependendo do tipo de mensagem que é enviada por um SES, o atendimento a uma ocorrência pode ser classificado segundo três tipos de ação: *imediata* (I), para ocorrências que exigem ação imediata, como, por exemplo, emergências médicas ou incêndio; *combinada* (C), para ocorrências cuja tomada de decisão é deduzida com base na sequência de eventos e na combinação de informações; e *reportagem* (R), quando não dependem de decisão, como, por exemplo, informações de controle e relatórios.

- **Áreas Contíguas**: dependendo da sequência de eventos e da relação de proximidade entre as áreas, perfis de ocorrência distintos podem ser definidos com base na relação de proximidade (p. ex., para detectar dois ou mais indivíduos num local). Exemplo:

Tabela 2. Relação de proximidade entre áreas

	A1	**A2**	**A3**	**A4**	**A5**
A1	0	1	1	1	1
A2		0	1	0	0
A3			0	1	1
A4				0	1
A5					0

na tabela 2, os 1's representam as áreas contíguas e os 0's as não contíguas.

- **Funcionalidade dos Sensores**: quanto à funcionalidade (comportamento), os sensores podem ser classificados segundo dois tipos distintos: sensores que *detectam presença* (S), como, por exemplo, sensores infravermelho; e sensores que *não detectam presença*, (N) como, por exemplo, sensores magnéticos.

- **Tempo de Atendimento**: representa o tempo médio de atendimento de uma ocorrência de alarme, determinado entre a prestadora de serviços (empresa de vigilância eletrônica) e o contratante (cliente). O sistema classifica o perfil de uma ocorrência com base na sequência em que os eventos ocorrem, analisando se está dentro (D) ou fora (F) do período de tempo previsto.

As informações sobre o projeto complementar constituem atributos da base de dados empregados na classificação. A classificação é o processo de encontrar um conjunto de modelos (ou funções) que descrevem e distinguem classes de dados para o propósito de poder usar o modelo para prever a classe de objetos (conjuntos de dados) ainda não rotulados [18]. Quando a classificação é baseada em algoritmos de aprendizagem indutiva, necessita de um padrão de treinamento e seu método de aprendizagem é dito do tipo supervisionado [23].

4.2 Construção do padrão de treinamento

Na construção do modelo utilizado como padrão de treinamento, os conceitos empregados na formulação do conjunto de regras deve ser baseado na figura de um especialista de segurança. A Tabela 3 apresenta como exemplo parte do modelo utilizado como padrão de treinamento para gerar o classificador.

Inicialmente, foi criado um arquivo, formado pelo nome e pelos possíveis valores de cada um dos atributos (de a_1 à a_8), onde: a_1 representa o código ZXY de uma mensagem em Contact ID; a_2 indica, com base no campo Q da mensagem, se é um evento de abertura (A) ou fechamento (F), ou um possível erro (E)

Tabela 3. Exemplo de padrão de treinamento

R	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	C
1	133	A	I	?	?	?	?	?	1
2	133	E	I	?	?	?	?	?	2
3	?	A	C	E	0	0	N	F	3
4	?	A	C	E	0	0	N	D	3
5	?	E	C	E	0	0	N	?	4
6	?	A	C	I	0	0	N	F	5
7	?	A	C	I	0	0	N	D	5
8	?	E	C	I	0	0	N	?	6
9	?	A	C	I	0	0	S	F	7
10	?	A	C	I	0	0	S	D	7
11	?	E	C	I	0	0	S	?	8
12	100	A	I	?	?	?	?	?	9
13	100	E	I	?	?	?	?	?	10
14	101	A	I	?	?	?	?	?	11
15	101	A	I	?	?	?	?	?	12
16	?	A	C	E	2	1	S	F	13
17	?	A	C	E	2	1	S	D	13
18	?	E	C	E	2	1	S	?	14
19	?	F	C	E	2	0	N	F	15
20	?	F	C	E	2	0	N	D	15
21	400	?	R	?	2	?	?	F	16
22	400	?	R	?	2	?	?	D	16
23	401	?	R	?	2	?	?	F	16
24	400	?	R	?	2	?	?	D	16
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

detectado pelo sistema (p. ex., quando ocorre uma falha de comunicação); a_3 indica, com base em ZXY, se a ação deve ser imediata (I), combinada (C), ou apenas um relatório (R) gerado pelo SES; a_4 indica se a área que originou o evento é interna (I), externa (E) ou de perímetro (P); a_5 identifica o código do caso classificado pela sequência de eventos anteriores (C), ou então, é atribuído o valor zero (0) se ainda não houve nenhuma ocorrência registrada; a_6 indica (se $a_5 \neq 0$) área contígua (1) ou não contígua (0); a_7 informa se o sensor detecta (S) ou não detecta (N) presença; e a_8 identifica se o tempo de atendimento está dentro (D) ou fora (F) do limite previsto. Os atributos com valores desconhecidos ou vazios foram representados com um ponto de interrogação (?), de acordo com as definições aceitas pelo C4.5 [24].

Assim, cada regra R é formada por oito atributos, que correspondem às características avaliadas para um determinado caso (rótulo da classe), ou seja, a combinação dos atributos representa determinada regra de classificação:

$$R = a_1 \wedge a_2 \wedge a_3 \wedge a_4 \wedge a_5 \wedge a_6 \wedge a_7 \wedge a_8 \tag{6}$$

Logo, cada regra ou conjunto de regras conduz a determinado caso C. Por exemplo, de acordo com o padrão de treinamento da Tabela 3, a regra $R = 1$ identifica um caso do tipo $C = 1$. Já um caso do tipo $C = 13$ é identificado pelas regras $R = 2 \wedge R = 16$ ou $R = 2 \wedge R = 17$, preservando histórico dos casos anteriores, que é memorizado no atributo a_5 de cada regra, ou seja, uma tomada de decisão final (TDF) é baseada não apenas na regra explícita, mas também no histórico de casos precedentes: $C_1 \prec C_2 \prec \cdots \prec C_n \equiv TDF$.

4.3 Transformação dos Dados em Casos

O RBC pode fazer uso dos mesmos atributos utilizados no padrão de treinamento para representar o conhecimento na forma de casos (Tabela 3). Para cada caso um valor de similaridade (*sim*) é calculado, indicando o grau de semelhança entre o problema presente e um caso específico na base [13]. Observando

o padrão de treinamento, existem casos que podem ser definidos com apenas alguns descritores mais significativos. Assim, nesta modelagem o valor de similaridade é calculado com base na similaridade local, utilizando-se pesos para indicar níveis de importância diferentes (Tabela 4).

Tabela 4. Pesos dos descritores para o cálculo de similaridade global.

	ZXY (a_1)	**Evento** (a_2)	**Ação** (a_3)	**Zona** (a_7)	**Tempo** (a_8)
Pesos	1,5	1,3	1,5	1,2	1,2

Para o cálculo da similaridade local a comparação é realizada com uma proposição: *verdadeira* (1) ou *falsa* (0), e o método de busca é do tipo serial, ou seja, a análise é feita descritor a descritor. Assim, o caso recuperado que possuir o maior número de atributos de proposição verdadeira (o maior valor *sim*) será eleito para compor a solução do novo problema. O valor de similaridade *sim* é dado por:

$$sim(X,Y) = \frac{\sum_{i=1}^{n} \omega_i (1 - \frac{|x_i - y_i|}{R_i})}{\sum_{i=1}^{n} \omega_i} \tag{7}$$

onde:

$sim(X,Y)$ denota a semelhança entre o caso X e Y;
x_i e y_i denotam o valor dos descritores em X e Y, respectivamente;
ω_i denota o peso relativo ou importância da i-ésima característica com que $\omega_i \in [0,1]$;
n número total de características nos casos $i = 1, 2, ..., n$;
R_i denota a extensão da escala do i-ésimo descritivo.

O caso eleito para a solução do problema é adaptado, se existir a necessidade de adaptação, e armazenado na base de casos. A adaptação do caso consiste em reescrever o problema (situação) conjuntamente com a solução (decisão e ações). Não devem ser aceitos casos já existentes na base de casos a fim de evitar processamento desnecessário (custo computacional). Exemplo de recuperação dos casos X e Y:

descritores →	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
Caso X	133	A	I	I	0	0	S	F
	↓	↓	↓	↓	↓	↓	↓	↓
Caso Y	133	A	I	E	0	0	N	D
proposições →	1	1	1	0	1	1	0	0

onde:

$$sim(X,Y) = \frac{1\times1,5}{9,7} + \frac{1\times1,3}{9,7} + \frac{1\times1,5}{9,7} + \frac{0}{9,7} + \frac{1}{9.7} + \frac{1}{9,7} + \frac{0\times1,2}{9,7} + \frac{0\times1,2}{9,7}$$

$$= 0,649484538.$$

Logo, o cálculo do valor de similaridade *sim* entre o novo caso X e o caso passado Y é 0,65 de aproximação (65 %), numa escala onde 0 seria um caso totalmente *diferente* e 1 seria um caso *idêntico* ou o mais similar.

5 Protótipo do Sistema

O protótipo de SMCAP foi implementado de acordo com o formalismo definido neste trabalho. Para cada SES monitorado, uma planta genérica independente é carregada pelo sistema e as mensagens de alarme são mapeadas para o alfabeto de entrada das respectivas plantas. Como cada empresa de vigilância patrimonial possui seu próprio planejamento de segurança, optou-se por implantar o algoritmo C4.5 dentro do

próprio SMCAP. Desta forma, o sistema pode ser adaptado para funcionar de acordo com as necessidades de cada empresa, ao invés de utilizar um classificador estático como o gerado pelo Weka [6]. Quando novos casos não podem ser classificados, devido à falta de algumas regras no padrão de treinamento, passam a ser analisados pelo RBC, que recupera os casos de maior valor de similaridade para compor uma solução. A solução recuperada é adaptada para o novo caso, repetindo o método do caso recuperado (descrição e estratégia) e fazendo a substituição dos atributos distintos. Essa adaptação é possível devido à forma com que os casos são armazenados na base, seguindo uma padronização de sintaxe. Assim, novos casos podem ser incluídos na base de casos e aproveitados como padrão de treinamento para gerar um novo classificador, otimizando o processo de classificação à medida que a base de casos vai se desenvolvendo.

O sistema foi testado numa arquitetura *cliente-servidor*, onde o papel de *cliente* foi representado por uma central de alarmes real com quatro zonas de proteção (C_4), e o papel de *servidor* foi representado por um computador onde o SMCAP foi instalado. Um módulo de comunicação [21] foi conectado à central para prover conectividade em redes TCP/IP. As mensagens de alarme são transmitidas em rede local, no formato do protocolo Contact ID, e processadas no servidor como ilustra a Figura 3.

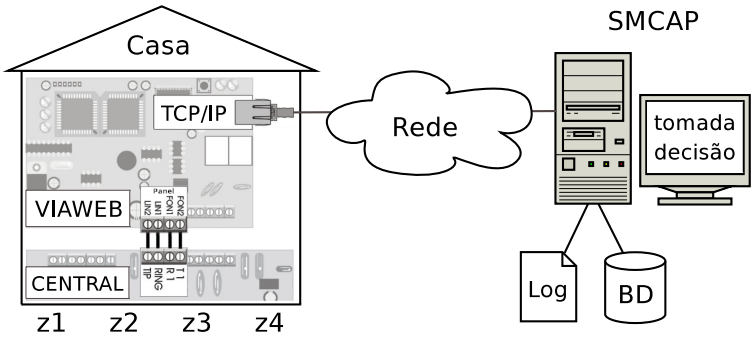

Figura 3. Típico cenário *cliente-servidor*.

Cada zona da central de alarme foi programada da seguinte forma: $z1$, zona interna; $z2$, zona segura 24 horas; $z3$, sensor de fumaça; e $z4$, zona de perímetro (barreira). Essa programação define que códigos de alarme devem ser enviados para um SMCAP (seção 2). A central de alarme também foi conectada a um painel de chaves (interruptores) adaptado para simular a função dos sensores. Os testes foram realizados abrindo e fechando as chaves de forma aleatória, com a evolução da planta sendo observada de acordo com a sequência em que as chaves foram acionadas. Para testar o estado de bloqueio, o canal de comunicação foi interrompido. A zona z_3 foi aberta e o *buffer* da central foi resetado, evitando o envio de uma mensagem de *abertura* da zona. Com a comunicação restabelecida, a zona de proteção foi restaurada e uma nova mensagem informando seu fechamento foi enviada. Como nenhuma mensagem sobre a abertura de z_3 havia sido recebida pelo protótipo, a planta genérica do SES foi conduzida ao estado de bloqueio. Entretanto, para tratamento do erro, o sistema continua com o monitoramento tradicional (exibição de eventos), informando para o operador do sistema que a tomada de decisão não deve mais ser baseada na planta. Uma nova planta volta a ser carregada quando a central de alarmes é novamente rearmada (código ZXY 400 ou 401).

6 Conclusão

A problemática dos SMCAPs está associada com a interpretação dada ao domínio do problema, que depende de informações claras e precisas geradas pelos sistema para auxiliar no processo de tomada de decisão. Esta reflexão é resultado de uma conscientização sobre a importância de abordagens mais coordenadas, que podem ser aplicadas no desenvolvimento não apenas de SMCAPs, mas também de sistemas em geral. Assim, como uma iniciativa deste trabalho, uma proposta de formalismo foi fundamentada e aplicada no desenvolvimento de um protótipo de SMCAP com uma base consistente. Os modelos projetados foram baseados no funcionamento e nas características comuns dos SESs e puderam ser utilizados para sistemas distintos sem a necessidade de desenvolver modelos específicos para cada tipo de SES monitorado.

[6] Waikato Environment for Knowledge Analysis

Dentre as vantagens mais significativas desta abordagem está o determinismo, dando a condição de projetar modelos que caracterizam sistemas onde todo comportamento pode ser predefinido.

A fase de desenvolvimento consistiu, basicamente, na tradução do formalismo em linguagem de programação, com a construção das plantas a partir da obtenção dos elementos da 5-tupla (que definem um AFD) e equações (seção 3.2). A visão geral de todas as zonas de proteção a cada estado da planta pode ser caracterizada como uma nova funcionalidade para os SMCAPs, representando uma informação útil para auxiliar no processo de tomada de decisão. O desempenho do protótipo, comparado com os SMCAPs tradicionais, também se apresentou satisfatório, já que a carga com processamento desnecessário pode ser reduzida, pois nem todos os símbolos do alfabeto foram utilizados como argumento para definir o próximo estado válido da planta, que é um ponto positivo da modelagem por ter uma função de transição parcial. O conjunto de estados finitos também favorece o poder de reconhecimento de uma linguagem, possibilitando que as sequências de símbolos possam ser reconhecidas mais rapidamente que em outras abordagens.

As árvores de decisão oferecem a vantagem de serem de fácil compreensão e interpretação, uma vez que é gerado conhecimento simbólico com a capacidade de fornecer uma explicação para um determinado problema, ou seja, oferecem a vantagem de acompanhar o procedimento de classificação através dos nodos da árvore, de forma que os modelos podem ser facilmente entendidos depois de uma simples explicação. As árvores de decisão também são ferramentas que podem ser utilizadas para dar ao usuário do sistema a capacidade de aprender e de tomar decisões. Com a implantação do C4.5 no SMCAP, o conhecimento presente no sistema pode ser atualizado sempre que necessário (de forma manual ou automática), à medida que novas ocorrências dão origem a novos casos armazenados na base de dados. Com a implementação do RBC, o sistema também pode absorver conhecimento sobre novos fatos adquiridos, de forma que a saída de um profissional experiente não cause um grande impacto na empresa de vigilância.

O algoritmo utilizado neste trabalho trouxe os resultados finais esperados, que, do ponto de vista funcional, foram fiéis às regras definidas pelo especialista. A estrutura do classificador é simples e eficiente, e o C4.5 também pode se encarregar de gerar um novo classificador sem a necessidade de um padrão de treinamento. Entretanto, como para o desenvolvimento deste trabalho ainda não existia uma base de dados formada, foi utilizado um padrão de treinamento baseado na figura de um especialista da área. Por ter sua teoria documentada e ser disponibilizado com o código-fonte, o C4.5 disseminou-se rapidamente e hoje é incorporado em várias ferramentas educacionais e comerciais. Isso também facilitou o desenvolvimento do SMCAP, pois com o auxílio do software Weka foi possível a realização de vários testes sem a necessidade de ter o sistema básico já desenvolvido. Entretanto, na prática é muito comum que os domínios para os quais os sistemas são desenvolvidos não tenham sido ainda completamente compreendidos. No caso do SMCAP isso não foi diferente, a figura do especialista e o RBC exerceram um papel importante no projeto do sistema. Mas como cada empresa tem seu próprio planejamento de segurança, existe a necessidade de readaptação.

Referências

[1] BRASIL. **Lei n^o 7.102, de 20 de junho de 1983**. Dispõe sobre segurança para estabelecimentos financeiros, estabelece normas para constituição e funcionamento das empresas particulares que exploram serviços de vigilância [...]. Brasília - DF, 1983. Disponível em: <http://www.planalto.gov.br/ccivil/LEIS/L7102.htm>. Acesso em: 09 de nov. 2010.

[2] WINSAMM. **Reference Guide (Version 1.0)**. MCDI Inc., 7055, Jean-Bourdon Avenue, Montreal, QC, Canada H4K 1G7. Disponível em: <http://mcdi.com.br/download/wsgu_v14.pdf>. Acesso em: 10 nov. 2010.

[3] W.SECURITY. **Iris Monitor 4 - Professional**. W.Security, av. D. Pedro II, 1016 - Ponta Grossa - PR/Brasil. Disponível em: <http://interno.sistemairis.com.br/produtos/iris_monitor.aspx>. Acesso em: 10 nov. 2010.

[4] MONI SOFTWARE. **Manual de Instalação e Utilização**. Central de Monitoramento Bauru Ltda. ME., rua Vivaldo Guimarães, 75 - 17040-510 - Bauru - SP/Brasil. Disponível em: <http://www.sistemamoni.com.br/download/Manual%20Sistema%20Moni.pdf>. Acesso em: 08 nov. 2010.

[5] COUTO, H. A. **Ergonomia Aplicada ao Trabalho: o Manual Técnico da Máquina Humana**. São Carlos: ENEGEP - UFSCAR, 1996.

[6] BRASIL. **Lei n^o 8.683, de 28 de março de 1994**. Estabelece normas para a constituição e funcionamento das empresas de serviços de vigilância. Brasília - DF, 1994. Disponível em: <http://www.soleis.com.br/L8863.htm>. Acesso em: 08 nov. 2010.

[7] CASSANDRAS, C. G.; LAFORTUNE, S. **Introduction to Discrete Event Systems**. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2006.

[8] SCHITTENKOPF, C.; DECO, G.; BRAUER, W. **Finite Automata-models for the Investigation of Dynamical Systems.** Inf. Process. Lett., p. 137–141, n. 3. Amsterdam, The Netherlands: Elsevier North-Holland, Inc., 1997.

[9] ATTIE, P. C.; LYNCH, N. A. **Dynamic Input/Output Automata, a Formal Model for Dynamic Systems**. PODC '01: Proceedings of the Twentieth Annual ACM symposium on Principles of Distributed Computing, p. 314–316. New York, NY, USA: ACM, 2001.

[10] PARK, S.; PARK, J.; AGGAEWAL, J. K. **Video Retrieval of Human Interactions Using Model-Based Motion Tracking and Multi-layer Finite State Automata**. CIVR, p. 394-403, 2003.

[11] EDELSTEIN, H. **Introduction to Data Mining and Knowledge Discovery**. 10500 Falls Road, Potomac, MD 20854 - USA: Two Crows Corporation, 2005.

[12] LIM, T.; LOH, W.; SHIH, Y. **A Comparison of Prediction Accuracy, Complexity, and Training Time of Thirty-Three Old and New Classification Algorithms**. Mach. Learn. Hingham, MA, USA: Kluwer Academic Publishers, 2000.

[13] WANGENHEIM, C. G. **Raciocínio Baseado em Casos**. Santos, SP - Brasil: Editora Manole, 2003.

[14] NEILD, I. et al. **Sensor Networks for Continuous Health Monitoring**. BT Technology Journal, vol. 22, n. 3, p. 130–139. Hingham, MA, USA: Kluwer Academic Publishers, 2004.

[15] NELSON, C.; FITZGERALD, D. **Sensor fusion for intelligent alarm analysis**. IEEE Aero. and Elec. Sys. Mag., p. 18–24. IEEE AES Systems Magazine, 1997.

[16] TOOSI, A. N.; KAHANI, M.; MONSEFI, R. **Network Intrusion Detection Based on Neuro-Fuzzy Classification**. 1-4244-0220-4 2006 IEEE, 2006.

[17] CRUZ, D. et al. **Monitoração Remota e Análise de Desempenho de um Sistema Híbrido Solar-Eólico-Diesel**. São Paulo, SP, Brazil: IEEE-PES T&D Latin America, 2004.

[18] HAN, J.; KAMBER, M. **Data Mining: Concepts and Techniques**. Hardcover: Morgan Kaufmann, 2000.

[19] TRAISTER, J. E.; KENNEDY, T. **Low Voltage Wiring: Security/Fire Alarm Systems**. The McGraw-Hill Companies, Inc., 2002.

[20] MONIP UNIVERSAL. **Interface Ethernet de Transmissão para Centrais de Alarme**. PPA Conforto e Segurança. Disponível em: <http://www.ppa.com.br/produtos/seguranca_eletronica/lancamentos/monip_universal.html>. Acesso em: 10 nov. 2010.

[21] VIAWEB ETHERNET. **Manual de Programação e Instalação**. SI - Sistemas Inteligentes Eletrônicos Ltda. Rua Amadeu Piotto, 161 - CIC. Curitiba - Paraná - Brasil. Disponível em: <http://www.viawebsystem.com.br>. Acesso em: 10 nov. 2010.

[22] CONTACT ID. **Ademco Contact ID Protocol for Alarm System Communications**. SIA - Security Industry Association, Publication Order Number: 14085, sept., 1999.

[23] KANTARDZIC, M. **Data Mining: Concepts, Models, Methods and Algorithms**. New York, NY, USA: John Wiley & Sons, Inc., p. 343, 2003.

[24] QUINLAN, J. R. **C4.5: Programs for Machine Learning**. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1993.