Uma Abordagem de Autenticação Sensível ao Contexto Baseada em Definições Comportamentais

Cristiano C. Rocha[1], João Carlos D. Lima[2], Iara Augustin[3] and M. A. R. Dantas[1,2]

[1]Departamento de Informática e Estatística, Universidade Federal de Santa Catarina (UFSC), Brasil
[2]Pós-Graduação em Engenharia e Gestão do Conhecimento, Universidade Federal de Santa Catarina (UFSC), Brasil
[3]Pós-Graduação em Informática, Universidade Federal de Santa Maria (UFSM), RS, Brasil

crocha@inf.ufsc.br, {caio,august}@inf.ufsm.br, mario@inf.ufsc.br

Resumo– Dispositivos móveis estão se tornando equipamentos obrigatórios na vida moderna devido ao crescente poder de processamento e oferta de recursos cada vez mais sofisticados. Entretanto, as conexões estabelecidas são, geralmente, baseadas em processos de autenticação tradicionais, que se mostram vulneráveis e inadequados. Novas abordagens devem considerar as características ambientais, restrições dos dispositivos e informações provenientes dos sensores presentes no espaço pervasivo. Neste trabalho, apresenta-se uma abordagem que adota a autenticação de usuários baseada em um contexto espaço-temporal, que permite a modelagem do seu comportamento através de perfis explícitos e implícitos. Este comportamento é definido pelos eventos e tarefas que compõem a atividade do usuário. Os resultados experimentais indicam: (i) um mecanismo mais dinâmico e autonômico para autenticação de usuários em um ambiente móvel e pervasivo, e (ii) uma eficiência significativa na detecção de anomalias de autenticação através da utilização de um modelo de permutação espaço-temporal.

I. Introdução

Computação ubíqua ou pervasiva representa um cenário aonde usuários e atividades humanas cotidianas compõem a parte central do ambiente [1]. Problemas de segurança são comumente observados em diversos projetos [2][3]. Em particular, desafios como acesso aberto, conexões instáveis, restrições de largura de banda e consumo energético são questões comumente abordadas [3], e são relevantes para aspectos de segurança como autenticação, integridade e confidencialidade.

O processo de autenticação tem como objetivo verificar a ligação entre um identificador e um indivíduo [4]. Além disso, um modelo eficiente de autenticação em um ambiente de computação móvel deve oferecer artefatos para preservar a energia dos dispositivos [5][6].

Existe uma tendência recente em considerar o comportamento dos usuários em sistemas computacionais, a fim de caracterizar os padrões de um usuário específico [3][7]. Por exemplo, em [3] define-se um comportamento como as ações e reações de um usuário específico enquanto este opera um sistema.

O desafio reside na complexidade de modelar o comportamento de indivíduos, visto que modelos devem ser desenvolvidos para lidar com os diversos comportamentos de usuários. Computação sensível ao contexto é um aspecto importante presente em ambientes ubíquos, cujo objetivo consiste em estabelecer e entender a relação entre usuários, dispositivos e ambientes [8]. Mais especificamente, a quantidade significante de informação em um ambiente ubíquo pode auxiliar na compreensão do comportamento do usuário em tal ambiente.

Um ambiente móvel, pervasivo e ubíquo é caracterizado pela riqueza de contextos aonde usuários, dispositivos e agentes se deslocam entre diversos lugares e diversas entidades, como serviços (GPS), aplicações (agendas em celulares) e recursos (rede de sensores) têm sua disponibilidade alternada sobre o tempo. Assim, a informação relacionada ao cenário tempo-espaço pode ser utilizada para definir um padrão de comportamento de uma entidade em diversos contextos.

Esse artigo apresenta uma abordagem diferenciada para autenticação dinâmica de usuários em ambientes de computação móvel e pervasiva, considerando o comportamento desses usuário em um contexto espaço-temporal. O restante do artigo está organizado em diversas seções. A Seção 2 apresenta a motivação para o desenvolvimento desta proposta. Os trabalhos relacionados à essa pesquisa são apresentados na Seção 3. A Seção 4 descreve a proposta para autenticação sensível ao contexto. Na Seção 5, são relatados os resultados experimentais. Finalmente, na Seção 6, as conclusões e trabalhos futuros são apresentados.

II. Motivação

Dispositivos móveis, como smartphones e PDAs, têm sido amplamente empregados como interfaces de acesso pervasivo ("*anytime*" e "*anywhere*") às entidades, como recursos e serviços, em ambientes de computação móvel. Os dispositivos móveis são adequados para aplicações sensíveis ao contexto, pois possuem diversos recursos, os quais permitem capturar características ambientais (como entidades que cercam o usuário), espaciais (como localização do usuário) e operacionais (como tarefas que o usuário desempenha) [8].

Em ambientes altamente dinâmicos, como os ambientes móveis, são necessários mecanismos de segurança sensíveis ao contexto, pois a mudança de contexto é utilizada por estes mecanismos para permitir o ajuste baseado na situação atual [2]. Sendo assim, tais mecanismos são capazes de contornar de forma efetiva as limitações de sistemas tradicionais de segurança, desenvolvidos para ambientes estáticos e, então,

são inapropriados para o paradigma de computação móvel e pervasiva. Além disso, em [2], é apresentada a definição de contexto relevante à segurança (*security-relevant context*) que consiste em qualquer informação que possa ser utilizada para caracterizar a situação de uma entidade que possa afetar uma tentativa do sistema de proteger informações, a fim de garantir a confidencialidade, integridade e disponibilidade destas.

Entretanto, muitos dos esforços para o desenvolvimento de sistemas de autenticação sensíveis ao contexto utilizam limitados contextos ou apresentam uma noção vaga de contexto [9][10]. Usualmente, tais sistemas consideram apenas aspectos tradicionais, como a localização do usuário e, desta forma, obtêm uma visão abstrata e deficiente de uma determinada situação [2]. Deste modo, as decisões tomadas por esses mecanismos tornam-se fracas, pois são baseadas em um cenário incompleto.

Nota-se, então, a falta de sistemas alternativos de autenticação. Nossa abordagem considera a análise comportamental, ou seja, como os usuários interagem nas diversas situações (contextos) que se apresentam, considerando ainda, simultaneamente, aspectos temporais e espaciais como critérios relevantes para o diagnóstico preciso dos históricos de decisões.

III. Trabalhos Relacionados

O contexto está relacionado com o projeto, avaliação e implementação de sistemas computacionais interativos para uso humano e com o estudo de importantes fenômenos que cercam os usuários e suas atividades [11]. Assim, o conceito de contexto envolve todo o ambiente que provê artefatos para que o usuário possa atingir seus objetivos. Logo, o contexto desempenha um importante papel na compreensão e desenvolvimento de aplicações pervasivas, visto que as atividades do usuário não podem ser isoladas do ambiente do qual ocorrem, ou seja, atividades não podem ser interpretadas sem um contexto [8].

A área de *context-awareness* visa lidar com questões de modelagem, representação e, explora a inferência/raciocínio sobre o ambiente [12]. Entretanto, historicamente o conceito de contexto e propriedades espaço-temporais (localização e tempo), têm sido tratados como sinônimos, devido à mobilidade dos usuários (localização) e à variação de disponibilidade de recursos e serviços sobre o tempo.

A. O Papel do Tempo

Alguns trabalhos buscam definir o papel do tempo em sistemas sensíveis ao contexto [7][8][12]. Em particular, Cassens e Kogod-Petersen [12] apresentam um modelo de contexto no qual é definido um subcontexto, que faz parte do contexto do usuário, e é chamado de contexto espaço-temporal. Esse subcontexto possui como propriedades as informações relativas ao tempo e localização. Porém, ao modelar desta forma, o sistema apenas captura informações do atual contexto ou situação. Tal modelagem não provê uma descrição adequada das intenções ou objetivos atuais do usuário, visto que esses geralmente são resultados de contextos e experiências passadas.

Consequentemente, o histórico é uma parte importante do contexto como um todo, e não apenas de um subconjunto deste, pois o comportamento de uma entidade reflete sua cultura e desenvolvimento histórico em circunstâncias específicas [13]. Desta forma, a informação temporal é crucial para a interpretação do comportamento das entidades que integram o espaço pervasivo.

Com o objetivo de posicionar o trabalho no estado da arte são apresentadas três abordagens relevantes relacionadas à autenticação sensível a contexto.

B. TBAS

Babu e Venkataram apresentam em [3] um esquema de autenticação para transações móveis, chamado de TBAS (*Transaction-Based Authentication Scheme*), que visa o processo de autenticação no nível de transação, ao invés de depender, apenas, da força dos identificadores durante o processo de autenticação. O objetivo principal consiste em classificar as transações operadas pelo usuário ao nível de aplicação em ambientes de computação móvel. Através desta classificação, o sistema é capaz de inferir e analisar o comportamento do usuário através da abordagem de agentes cognitivos (agentes inteligentes). Além disso, através dessa categorização de transações, o sistema pode determinar o nível de segurança necessário, prevendo, então, o custo associado ao atraso do processo de autenticação devido à aplicação de algoritmos de criptografia. O TBAS utiliza dois tipos de agentes cognitivos: agente cognitivo móvel (*Mobile Cognitive Agent* - MCA) e agente cognitivo estático (*Static Cognitive Agent* - SCA). Assim, o SCA cria o MCA e, então, envia este agente cognitivo móvel para o dispositivo móvel. Este procedimento é realizado enquanto o cliente é autenticado.

C. Abordagem de Hung et al.

Hung et al [14] propõem um mecanismo de segurança baseado em atividades que visa auxiliar as atividades dos usuários em ambientes ubíquos. Tal mecanismo é composto por um sistema de autenticação baseado na identificação humana de imagens [15] e por um modelo de controle de acesso orientado a atividades.

O modelo proposto suporta diferentes tipos de dispositivos, incluindo dispositivos móveis (PDAs), laptops e desktops. Com essa finalidade, o gerenciador de reconhecimento de atividades (*Activity Recognition Manager* - ARM) provê informações sobre a atividade do usuário ao serviço de autorização através da coleta de dados contextuais de baixo nível relacionados a tal atividade e, então, produz informação contextual de alto nível. Desta forma, o ARM pode realizar o processo de raciocínio sobre as ações do usuário.

D. UbiCOSM

Corradi, Montanari e Tibaldi [16] propõem um *middleware* de segurança, chamado de UbiCOSM (*Ubiquitous Context-based Security Middleware*). Tal abordagem adota o contexto como conceito básico para especificação e execução de políticas de segurança. Portanto, as permissões são associadas

diretamente aos contextos, ao invés das identidades e papéis dos usuários. As informações sobre os contextos e recursos são providas pelo *middleware* CARMEN [17].

O gerenciador de controle de acesso do UbiCOSM trabalha com duas classificações de contexto: contexto físico e lógico. Contextos físicos identificam espaços físicos delimitados por coordenadas geográficas específicas. Desta forma, um usuário opera em um determinado contexto físico dependendo da sua localização atual; logo, o usuário só pode pertencer a somente um contexto físico. Além disso, os contextos físicos definem limites específicos para o gerenciador de controle de acesso, pois, cada contexto físico possui as referências para os recursos a serem protegidos.

E. Considerações sobre as abordagens propostas

Todas as abordagens apresentam uma modelagem contextual fraca, pois, consideram apenas aspectos sobre as características dos dispositivos utilizados pelo usuário e seu contexto espacial. Desta forma, tais sistemas possuem uma visão incompleta do cenário, prejudicando, assim, o processo de tomada de decisão.

Além disso, uma pequena parte das abordagens analisadas apresentam algum mecanismo de análise e modelagem comportamental do usuário de forma dinâmica.

IV. Modelo Proposto para Autenticação Sensível ao Contexto

O espaço pervasivo consiste em um ambiente rico em situações (contextos) que cercam o usuário. Tais contextos são relevantes para o processo adaptativo de serviços e informações oferecidas ao usuário através de aplicações sensíveis ao contexto [18]. Portanto, as diversas experiências, que podem ser experimentadas pelo usuário em um ambiente pervasivo, são pessoais, e, então, dificultam a modelagem e a representação do contexto do usuário e seus parâmetros.

A fim de identificar os contextos e propriedades relevantes aos usuários e seus comportamentos em ambientes pervasivos, analisaram-se os recursos oferecidos pelos dispositivos móveis e concluiu-se que os seguintes contextos são relevantes à autenticação:

- *Contexto operacional:* descreve o que o usuário está fazendo, assim como os objetivos, tarefas e atividades do usuário;
- *Contexto interpessoal:* descreve os aspectos sociais do usuário, ou seja, as relações e canais de comunicação que este possui com as pessoas da sua comunidade;
- *Contexto espacial:* considera os atributos relativos à localização do usuário;
- *Contexto ambiental:* captura as situações que cercam o usuário, como, serviços, pessoas e informações acessadas pelo usuário.

A propriedade temporal foi integrada ao modelo de contexto com a finalidade de melhorar o processo de tomada de decisão. Portanto, dados históricos, como a capacidade de aprendizagem do usuário, incluindo a aquisição de habilidades e conhecimento, e a evolução de suas atividades e comportamentos, foram considerados na modelagem, que é apresentada na Figura 1.

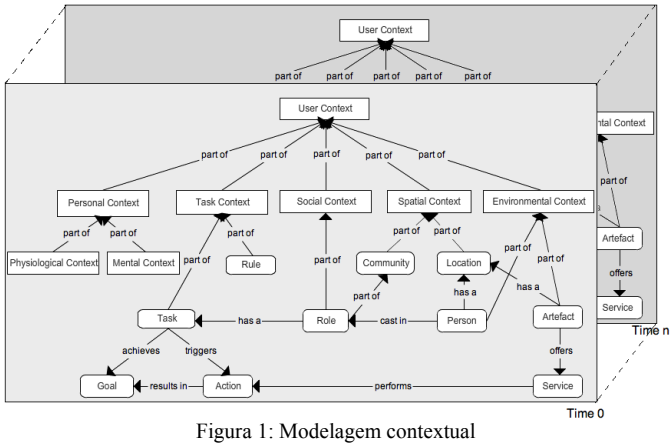

Figura 1: Modelagem contextual

A. Modelo Comportamental

Visto que os seres humanos são criaturas de hábitos, correlações temporais são importantes para a determinação de eventos sucessivos [7]. Deste modo, a inferência de eventos define as ações e comportamentos que o usuário irá adotar. A fim de, formalmente, definir os conceitos de evento e comportamento, este trabalho utiliza as seguintes definições:

- *Evento:* a situação de um entidade determinada por um ou mais contextos, em uma determinada localização e em um certo espaço de tempo. Assim, um evento por ser determinado como:

$$E_i = \langle situacao, tempo, localizacao \rangle$$

- *Comportamento:* o conjunto de eventos relacionados à execução de uma atividade; Pode ser definido como:

$$C_i = \langle atividade, \sum_{i=1}^{n} E_i \rangle$$

Assim, tempo e localização desempenham um importante papel na modelagem comportamental de indivíduos em um ambiente pervasivo, pois esses dois aspectos provêm artefatos para o diagnóstico de dados históricos, possibilitando a determinação dos hábitos de uma entidade.

B. Modelo Analítico

Os eventos observados na execução de atividades formam uma base de dados para o processo de detecção de conglomerados (*clusters*) de informações, estas informações traduzem os hábitos dos usuários. Esses conglomerados podem ser classificados em três categorias: i) puramente espaciais – quando a ocorrência de eventos é mais alta em determinadas regiões que em outras; ii) puramente temporais – quando a ocorrência de eventos é mais alta em um período que os demais; e iii) espaço-temporais – quando a ocorrências

dos eventos é temporariamente maior em determinadas regiões.

Dentre os modelos utilizados para inferência de eventos em um contexto espaço-temporal propõe-se a utilização da permutação espaço-temporal que permite a incorporação de informação de co-variáveis, oriundas dos demais contextos do espaço pervasivo. Os modelos de Poisson [19] (aplicados para contextos puramente temporais) e Bernoulli [20] (aplicados para contextos preferencialmente espaciais) foram estudados, mas foram descartados devido à necessidade de determinar previamente os hábitos comportamentais do usuário.

O modelo de permutação espaço-temporal segundo Kulldorff [21] é baseado em três características: i) a varredura para detecção de conglomerados de dados é realizada no espaço e no tempo simultaneamente; ii) flexibilidade de trabalhar somente com eventos ou casos; iii) o modelo probabilístico sob hipótese nula resulta que os casos seguem uma distribuição hipergeométrica.

Supondo a contagem de eventos **e** (em espaço temporal definido em **t**), localizados em uma região **z** de características circulares (definido por coordenadas de GPS), definido como $\mathbf{e_{zt}}$; o número total de eventos observados **E** e o número total de eventos condicionados $\mathbf{M_{zt}}$ são expressos pelas fórmulas:

$$E = \sum_{z} \sum_{t} e_{zt} \qquad M_{zt} = \frac{1}{E} \left(\sum_{z} E_{zt} \right) \left(\sum_{t} E_{zt} \right)$$

Para realizar a predição de um evento, tem-se a pressuposição: a probabilidade condicional de um evento $\mathbf{P(E_a)}$ na região **z** foi observado no tempo $\mathbf{t_1}$ e no tempo $\mathbf{t_2}$, logo $\mathbf{E_a}$ tem uma média $\mathbf{M_a}$ e segue distribuição hipergeométrica dada pela função

$$M_a = \sum_{(z,t) \in A} M_{zt}$$

$$P(E_a) = \frac{\begin{pmatrix} \sum_{t \in (t_1 \cup t_2)} \sum_{z \in A} E_{zt} \\ E_a \end{pmatrix} \begin{pmatrix} E - \sum_{t \in (t_1 \cup t_2)} \sum_{z \in A} E_{zt} \\ \sum_{t \in (t_1 \cup t_2)} \sum_{z \in A} E_{zt} - E_a \end{pmatrix}}{\begin{pmatrix} E \\ \sum_{t \in (t_1 \cup t_2)} \sum_{z \in A} E_{zt} \end{pmatrix}}$$

A fim de determinar as regiões dos conglomerados utiliza-se a ferramenta SaTScan desenvolvida por Kulldorff [21] e a significância estatística é validada utilizando-se o teste de hipótese de Monte Carlo.

A probabilidade condicional $\mathbf{P(E_a)}$ do usuário possibilita estimar que tipo de atividade o usuários estava executando e qual esta executando atualmente. Assim, existem quatro casos possíveis: i) mesma atividade no mesmo contexto espaço-temporal - define-se como execução normal; ii) mesma atividade em contexto espaço-temporal diferente - define-se com execução suspeita mas será o contexto de segurança da atividade que definirá as políticas de autenticação; iii) atividades diferentes no mesmo contexto espaço-temporal - define-se como execução suspeita; iv) atividades diferentes em contexto espaço-temporal diferente - define-se como execução anormal.

C. Arquitetura de Autenticação Sensível ao Contexto

A fim de monitorar o comportamento do usuário em diferentes situações e eventos aonde o usuário está imerso no espaço pervasivo, a arquitetura proposta para autenticação sensível ao contexto busca utilizar recursos que são comumente encontrados em dispositivos móveis, como telefones celulares. Esses dispositivos são considerados artefatos especiais, utilizados frequentemente pelos usuários com a finalidade de alcançar seus objetivos em ambientes móveis [8]. Tais dispositivos oferecem recursos como:

- *Chamadas do usuário:* provêm informações considerando o contexto interpessoal, que envolve a comunidade aonde o usuário está inserido e o contexto ambiental, que diz respeito às pessoas que cercam o usuário;
- *Agenda do usuário:* um dos recursos mais ricos em contexto, pois provê informações sobre as relações entre o usuário e os membros de sua comunidade. Pode determinar a localização do usuário, as pessoas que o cercam e as atividades que o usuário deseja executar em um determinado intervalo de tempo;
- *GPS:* provê informações relativas à situação espacial do usuário;
- *Nível de bateria do dispositivo:* pode indicar a forma de interação entre o usuário e o ambiente, assim como a intensidade dessa interação;
- *Aplicações do usuário:* provê informações relacionadas ao contexto operacional e ambiental; em particular, tais aplicações indicam que artefatos o usuário utiliza para alcançar seus objetivos através das atividades desempenhadas;
- *Sensores:* podem prover informações sobre o ambiente, autenticação visual e outras informações que definem o ambiente aonde o usuário está interagindo com o sistema de autenticação;
- *Perfil de grupo:* um perfil predefinido que considera as características padrões dos agentes (usuários, aplicações, sessão de uso e ambiente) que interagem com o sistema;
- *Perfil explícito:* criado durante a primeira interação do sistema com o usuário através de uma interface interativa e contém os eventos explicitados pelo usuário e extraídos de seus contatos e da agenda pessoal armazenadas no dispositivo móvel. Este perfil pode ser customizado e/ou sincronizado a qualquer momento;
- *Perfil implícito:* criado através do processamento dos eventos do usuário e do seu perfil explícito, contém as informações relevantes sobre os eventos que ocorrem com maior frequência, as ações tomadas pelo usuário e as suas características espaço-temporal. Este perfil é determinado por uma estratégia de recomendação baseada no modelo de espaço vetorial (VSM – Vector Space Model)[22];

- *Filtro VSM:* filtro que utiliza o modelo de espaço vetorial para calcular a relevância da informação, utiliza um tratamento formal através de vetores para o cálculo de similaridade entre os perfis em análise.

A arquitetura de autenticação sensível a contexto é ilustrada na Figura 2. O subsistema de contexto, ou, contexto do usuário, é responsável por capturar todas as situações que determinam a ocorrência de um novo evento através dos recursos descritos anteriormente. Assim, este subsistema envia a descrição do evento (e_i) para o subsistema de análise de crenças (Analisador de Crenças).

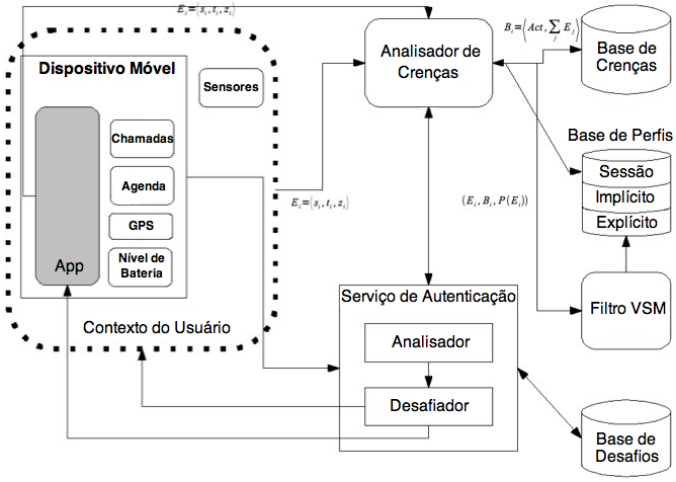

Figura 2: Arquitetura de autenticação sensível ao contexto proposta

O Analisador de Crenças é responsável pela definição de comportamentos, ou crenças, assim como pela classificação de eventos e inferência de comportamentos através das atividades, dos perfis armazenados e eventos que são percebidos e registrados. Os comportamentos são analisados probabilisticamente a fim de definir novas ocorrências e determinar a atitude a ser adotada pelo sistema, assim como as ações que serão tomadas em uma nova ocorrência. A base de dados de crenças trabalha como um repositório de conhecimento (base de dados de crenças e base de dados de perfis). O Algoritmo 1 resume o funcionamento do Analisador de Crenças.

Algoritmo 1: Analisador de Crenças

Início
Buscar na *Base de Perfis* os eventos passados associados ao usuário que gerou o evento *E*
Extrair as coordenadas geográficas dos eventos
ExecutaPermutacaoEspacoTemporal ()
Pvalue <= min(AnalisaResultadoPermutacao())
$VetorE_{local}$ <= $VetorE_{timestamp}$ <= *PValue*
Definir *VetorE* baseando-se no vetor de pesos (*VetorP*)
GrauSimilaridade<=CalculaSimilaridade(*VetorE*, *VetorP*)
Fim

O Filtro VSM tem como objetivo determinar os novos perfis implícitos, ou seja, a cada combinação de evento com o perfil explicito é determinado um novo vetor ortogonal, determinado pela fórmula abaixo. Este vetor é utilizado para o cálculo da similaridade, comparando se o grau de similaridade for superior a um determinado valor, o perfil é considerado relevante e, então, será armazenado no sistema como um novo perfil implícito com peso igual ao grau de similaridade.

$$Similar(E, P_j) = \frac{E \times P_j}{\|E\| \times \|P_j\|} = \frac{\sum_{i=1}^{n} e_i \cdot p_{(j,i)}}{\sqrt{\sum_{i=1}^{n} e_i^2 \cdot \sum_{i=1}^{n} p_{(j,i)}^2}}$$

O subsistema que analisa probabilidades (Analisador de Probabilidades), é responsável pela categorização do usuário, baseando-se nas probabilidades condicionais do seu comportamento. Essa classificação é dividida em três categorias: normal, suspeito e anormal. O funcionamento do Analisador de Probabilidades é resumido no Algoritmo 2.

Algoritmo 2: Analisador de Probabilidades

Início
IF NaturezaUsuario is *USUARIO_NORMAL* **THEN**
Realizar a operação requerida pelo usuário
Definir o evento *E* como *Perfil_de_Sessao* do usuário
Inserir o evento *E* ao *Perfil_Implicito* do usuário
ELSE
Desafiador(NaturezaUsuario, NívelRestriçãoAplicação)
END IF
Fim

Por fim, o subsistema de desafios (Desafiador), determina como o usuário será questionado a fim de provar sua identidade no sistema, baseando-se na categorização feita pelo Analisador de Probabilidades e o no nível de autenticação necessário para a operação desejada. A reposta ao desafio proposto ao usuário é, então, armazenada para consultas futuras.

V. Resultados Experimentais

No desenvolvimento deste projeto, fez-se necessária a criação de módulos auxiliares, descritos em [23]. Assim, partiu-se para a análise do núcleo da arquitetura (Analisador de Crenças) e a sua interação com os demais módulos. Tal análise foi realizada através de ciclos completos de autenticação, ou seja: (i) o evento é capturado no dispositivo móvel, (ii) este evento é analisado sob a perspectiva espaço-temporal, (iii) a probabilidade condicional determinada pelo modelo de permutação espaço-temporal é utilizada para verificar o grau de similaridade deste evento com o perfil comportamental do usuário e (iv) analisa-se a necessidade de desafiar o usuário, baseando-se no nível de autenticação exigido pela aplicação.

A partir dessa análise, é possível determinar a capacidade do sistema de autenticação sensível ao contexto em agregar

novos conhecimentos e habilidades do usuário, possibilitando uma maior autonomicidade do sistema. Com este propósito, primeiramente, definiu-se quais seriam os atributos comportamentais a serem considerados. Optou-se pelos seguintes parâmetros: dispositivo móvel utilizado, localização em que o evento ocorre, marca de tempo (*timestamp*) do momento em que o evento ocorre, aplicação executada e restrição da aplicação executada. Posteriormente, definiu-se os pesos associados a cada atributo comportamental, a fim de atribuir diferentes níveis de prioridade para a análise dos diferentes atributos comparativos. Assim, utilizaram-se os seguintes pesos:

$$P = (P_{device}, P_{local}, P_{timestamp}, P_{appid}, P_{apprestriction})$$
$$P = (0.75, 1.00, 1.00, 0.5, 0.5)$$

Quando o usuário faz seu primeiro acesso ao sistema, cadastrando suas informações pessoais, o usuário está, automaticamente, autenticado no sistema. A partir dessa entrada de informações, o sistema é capaz de extrair o perfil explícito e o perfil de sessão do usuário (apresentados na Figura 3), que na primeira interação são iguais.

```
<explicit-profile>
    <timestamp>1265039001</timestamp>
    <device>
        <id>1</id>
        <battery-level>high</battery-level>
    </device>
    <location>
        <latitude>-27.594176<longitude>
        <longitude>-48.522159</longitude>
    </location>
    <app>
        <id>1</id>
        <restriction>2</restriction>
    </app>
</explicit-profile>
```
(a)

```
<session-profile>
    <timestamp>1265039001</timestamp>
    <device>
        <id>1</id>
        <battery-level>high</battery-level>
    </device>
    <location>
        <latitude>-27.594176<longitude>
        <longitude>-48.522159</longitude>
    </location>
    <app>
        <id>1</id>
        <restriction>2</restriction>
    </app>
</session-profile>
```
(b)

Figura 3: (a) Perfil explícito e (b) Perfil de sessão das informações do usuário

Assim, o processo de autenticação proposto é realizado a partir da segunda interação do usuário. Na segunda interação, realizou-se a requisição da mesma aplicação, a partir da mesma localização da primeira interação. Entretanto, tal requisição foi realizada a partir de outro dispositivo móvel disponível. A descrição do segundo evento e a descrição do perfil de sessão são apresentadas na Figura 4.

```
<event>
    <timestamp>1265040061</timestamp>
    <device>
        <id>2</id>
        <battery-level>high</battery-level>
    </device>
    <location>
        <latitude>-27.594176<longitude>
        <longitude>-48.522159</longitude>
    </location>
    <app>
        <id>1</id>
        <restriction>2</restriction>
    </app>
</event>
```
(a)

```
<session-profile>
    <timestamp>1265039001</timestamp>
    <device>
        <id>1</id>
        <battery-level>high</battery-level>
    </device>
    <location>
        <latitude>-27.594176<longitude>
        <longitude>-48.522159</longitude>
    </location>
    <app>
        <id>1</id>
        <restriction>2</restriction>
    </app>
</session-profile>
```
(b)

Figura 4: (a) Descrição do evento da segunda interação e (b) Perfil de sessão

Para determinar os vetores para o cálculo do grau de similaridade, faz-se necessária a utilização dos pesos definidos anteriormente para o ***VetorP***. Por outro lado, para determinar o ***VetorE***, faz-se necessária a comparação dos valores dos atributos, realizando-se um comparativo entre o evento capturado e o perfil de sessão. Aqueles atributos que permaneceram iguais receberam um valor 1 (um), os diferentes 0 (zero). No caso dos atributos espaço-tempo (local e *timestamp*) o valor a ser atribuído é o menor valor do modelo de permutação espaço-temporal considerando o *cluster* espaço-temporal de referencia, determinado através da ferramenta SaTScan [21].

A base para análise, na ferramenta SaTScan, é composta de 28 eventos que foram coletados anteriormente. Assim, ao comparar o *p-value* entre as duas execuções do modelo de permutação espaço-temporal (com co-variáveis e sem co-variáveis), o sistema escolhe o valor mínimo entre tais valores, a fim de realizar a análise sobre o pior caso (caso que representa um maior risco ao processo de autenticação). Portanto, o sistema utiliza o *p-value* de 0,826 determinado pela análise espaço-temporal sem co-variáveis, que esta representado na Figura 5. Então, tal valor é utilizado para o cálculo do grau de similaridade entre o evento capturado e o perfil de sessão, que representa o contexto de execução do usuário e, portanto, existe apenas durante a interação do usuário com a aplicação em questão. Os demais Modelos da Figura 5 são apresentados para demonstrar a eficiência da permutação espaço-temporal na detecção de anomalias em ambientes pervasivos.

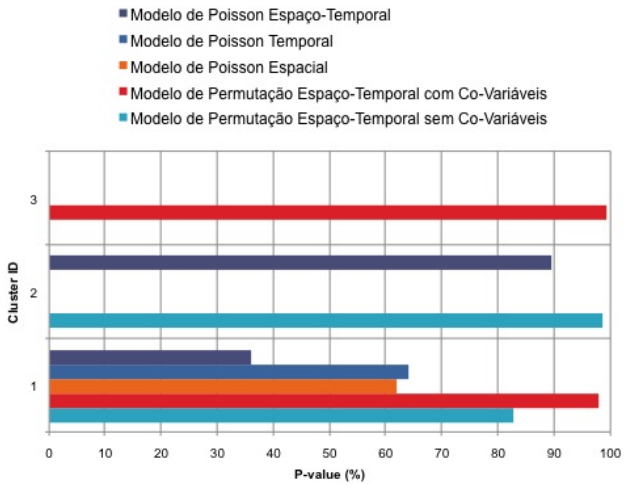

Figura 5: Resultados do modelos analíticos do SatScan

Após a definição desses dois vetores, é possível a determinação do grau de similaridade entre o vetor capturado e o perfil de sessão, conforme é apresentado abaixo:

$$P = (0.75, 1.0, 1.0, 0.5, 0.5)$$
$$E = (0.0, 0.826, 0.826, 1.0, 1.0)$$
$$Grau\ Similaridade(E, P) = \frac{E \times P}{\|E\| \times \|P\|} = 0.862119$$

Entretanto, fez-se necessário determinar quais são os intervalos de valores do grau de similaridade que determinam cada categoria do usuário (normal, suspeito e anormal). Então, assumiu-se a seguinte definição:

- **Usuário normal**: grau de similaridade superior a 90%;
- **Usuário suspeito**: grau de similaridade entre 70% e 90%; e
- **Usuário anormal**: grau de similaridade inferior a 70%.

Conforme a definição dos intervalos de valores acima, faz-se necessário que o usuário seja testado com o desafio referente a um usuário suspeito e referente ao nível de autenticação exigido pela aplicação (nível médio), conforme a Tabela 1. Quando o usuário responde de forma correta ao desafio, ele é autenticado no sistema, executa a operação desejada e o evento requisitado é inserido no perfil de usuário, que contém o histórico de suas interações com o sistema.

Tabela 1: Relação entre os níveis e desafios de autenticação

Nível	Natureza do Usuário	Desafio
Alto	Suspeito	"Por favor, digite o seu CPF"
	Anormal	"Por favor, digite seu login e senha"
Médio	Suspeito	"Por favor, digite a sua data de nascimento"
	Anormal	"Por favor, digite o seu RG"
Baixo	Suspeito	"Por favor, digite/escolha o seu CEP"
	Anormal	"Por favor, digite/escolha a sua cor favorita"

Então, para analisar a capacidade do sistema em agregar as novas características do contexto de execução do usuário, executou-se uma nova requisição para a mesma aplicação, a partir da mesma localização e, desta vez, utilizando o mesmo dispositivo móvel. Assim, a definição dos vetores utilizados para o cálculo do grau de similaridade são as seguintes para este caso:

$$P = (0.75, 1.0, 1.0, 0.5, 0.5)$$
$$E = (0.0, 0.98, 0.98, 1.0, 1.0)$$
$$Grau\ Similaridade(E, P) = \frac{E \times P}{\|E\| \times \|P\|} = 0.9972$$

Conforme ilustrado na Figura 6, é perceptível que a arquitetura proposta para autenticação sensível ao contexto possibilita a evolução de seus parâmetros comportamentais, através da incorporação dos eventos (atividades) do usuário aos perfis explícitos, implícitos e de sessão do usuário.

Consequentemente, o sistema é capaz de ampliar sua base de conhecimento e, então, agregar as ações do usuário, que refletem o seu conhecimento e habilidades, refinando o processo de autenticação conforme o número de interações com o usuário. Através desse dinamismo, oferecido pela arquitetura proposta, é possível prover uma maior autonomicidade ao usuário, ou seja, o sistema de autenticação cada vez mais reduz a necessidade de entrada de informação de forma explícita ao sistema (resposta a desafios).

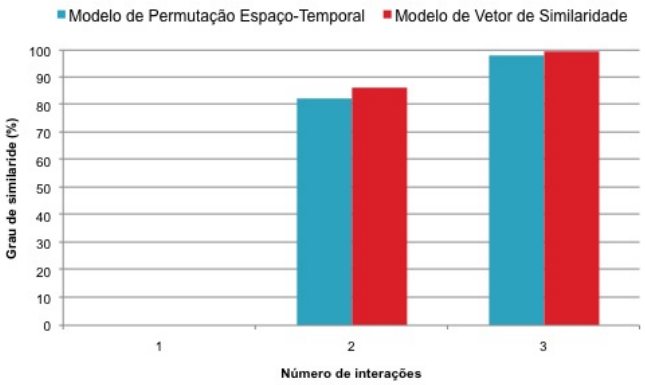

Figura 6: Evolução do sistema conforme o número de interações

A. *Resumo sobre as abordagens estudadas e a proposta*

Com objetivo de evidenciar as contribuições proposta pela abordagem é apresentado, na Tabela 2, um resumo das características analisadas nos modelos existentes.

Tabela 2: Resumo das Características das Abordagens

Características	Rocha [23]	Babu [3]	Hung [14]	Corradi [16]
Modelo Contextual	**Espaço-temporal**	Espacial	Espacial	Espacial
Modelo Comportamental	**Perfil Dinâmico com VSM**	Agentes Cognitivos	Explícito	Perfil Estático
Atomicidade e dinamicidade	**Sim**	Sim	Não	Não
Flexibilidade	**Sim**	Sim	Não	Sim

VI. Conclusão

Neste artigo foi abordado um problema encontrado em ambientes de computação móvel e pervasiva que empregam dispositivos móveis (*smartphones* e celulares) como interfaces de acesso a serviços e recursos: autenticação de usuários de forma dinâmica e ciente das restrições de tais dispositivos. Desta forma, a abordagem adotada para solucionar essa dificuldade foi a utilização dos recursos oferecidos por grande parte dos dispositivos móveis presentes no mercado, tais como, sistemas de geoposicionamento, calendário, ligações realizadas e recebidas, mensagens enviadas e recebidas, e aplicações executadas, por exemplo.

Através da pesquisa realizada, com relação à determinação do comportamento de usuários em ambientes de computação móvel, constatou-se a importância de considerar, simultaneamente, dois atributos fundamentais no contexto do usuário: espaço e tempo. Tais propriedades são importantes, visto que os seres humanos possuem hábitos, correlações de tempo são relevantes para determinar eventos sucessivos que definem um perfil comportamental. Desta forma, neste trabalho, um evento é definido como a situação de uma entidade definida por um ou mais contextos que compõem o

contexto total do usuário, em uma determinada localização e em um determinado espaço de tempo.

Portanto, fez-se necessária a pesquisa de modelos que considerassem a análise desses dois atributos simultaneamente, a fim de obter uma avaliação mais precisa do comportamento do usuário, ou seja, identificando uma conformidade no padrão de comportamento e possíveis anomalias de comportamento que caracterizam uma falha no processo de autenticação. Então, foi proposta a utilização de um modelo de permutação espaço-temporal para analisar probabilisticamente a ocorrência de tais anomalias, considerando os eventos capturados através dos recursos disponíveis nos dispositivos móveis. Os resultados experimentais envolvendo o modelo analítico proposto apresentam uma eficiência significativa na detecção e análise de anomalias no processo de autenticação devido à utilização do modelo de permutação espaço-temporal.

Além disso, a arquitetura proposta mostrou que atende ao requisito de autonomicidade e dinamicidade, pois, através dos perfis comportamentais definidos pelo modelo de espaço vetorial, o sistema é capaz de agregar as habilidades e conhecimentos adquiridos pelo usuário durante a sua interação com o sistema. Em adição, a proposta provê flexibilidade por permitir diferentes formas de autenticação, conforme os níveis de segurança exigidos pelas aplicações executadas. Portanto, é perceptível que a abordagem proposta neste trabalho de pesquisa foi capaz de contornar com sucesso a falta de alternativas existentes na literatura para atender os requisitos de sensibilidade ao contexto, eficiência computacional, flexibilidade, autonomicidade e dinamicidade simultaneamente.

Como trabalhos futuros, espera-se realizar a análise sobre o impacto do número de usuários sobre o mecanismo de autenticação sensível ao contexto, ou seja, a capacidade do sistema em manter uma taxa aceitável de acerto no processo de autenticação, conforme o número de usuários cadastrados no sistema aumenta.

Agradecimento

Agradecemos ao CNPq que financiou parcialmente o desenvolvimento deste trabalho.

Referencias

[1] Saha, D., and Mukherjee, A. (2003) “Pervasive Computing: a Paradigm for the 21st Century”, IEEE Computer, vol. 36, no. 3, pp. 25-31, IEEE Computer Society Press, Los Alamitos, CA, USA.

[2] Johnson, G. (2009) “Towards Shrink-Wrapped Security: A Taxonomy of Security-Relevant Context”, Proceedings of the 7th IEEE International Conference on Pervasive Computing and Communications, pp. 1-2. IEEE Computer Society.

[3] Babu, S., and Venkataram, P. (2009) “A Dynamic Authentication Scheme for Mobile Transactions” International Journal of Network Security, vol. 8, pp. 59-74.

[4] Nielsen, E., and Jacobs, S. (2002) “A Security Model Supporting the Legacy UserID: Passphrase the Authentication Model that Won’t Go Away!”.

[5] Mahopatra, S. et al., (2005) “A Cross-Layer Approach for Power-Performance Optimization in Distributed Mobile Systems”, Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, vol. 11, pp. 8. IEEE Computer Society, Washington, DC, USA.

[6] Rong, P., and Pedram, M. (2003) “Extending the Lifetime of a Network of Battery-Powered Mobile Devices by Remote Processing: a Markovian Decision-Based Approach”, Proceedings of the 40th Conference on Design Automation, pp. 906-911. ACM New York, NY, USA.

[7] Peddemors, A., and Eertink, H., and Niemegeers, I. (2009) “Predicting Mobility Events on Personal Devices”, Pervasive and Mobile Computing Journal - Special Issue on Human Behaviour in Ubiquitous Environments, In Press, Accepted Manuscript. Elsevier.

[8] Uden, L. (2007) “Activity Theory for Designing Mobile Lerning”, International Journal of Mobile Learning and Organisation, vol. 1, pp. 81-102.

[9] Chen, G., and Kotz, D. (2000) “A Survey of Context-Aware Mobile Computing Research”, Technical Report TR2000-381, Dept. of Computer Science, Darthmouth College, November.

[10] Barkhuus, L. (2003) “Context Information vs. Sensor Information: A Model for Categorizing Context in Context-Aware Mobile Computing”, Symposium on Collaborative Technologies and Systems, pp. 127-133.

[11] Preece, J., and Rogers, Y., and Sharp, H., and Beyon, D., and Holland, S., and Carey, T. (1994) “Human-Computer Interaction”. Addison-Wesley. Harlow, UK.

[12] Cassens, J., and Kofod-Petersen, A. (2006) “Using Activity Theory to Model Context Awareness: a Qualitative Case Study”, Proceedings of the 19th International Florida Conference Artificial Intelligence Research Society, pp. 616-624.

[13] McMichael, H., and Melbourne, A. (1999) “An Activity Based Perspective for Information Systems”, Proceedings of the 10th Amsterdam Conference on Information Systems.

[14] Hung, L., Hassan, J., Riaz, A., Raazi, S., Weiwei, Y., Canh, N., Truc, P., Lee, S., Lee, H., Son, Y., et al. (2008). Activity- based security scheme for ubiquitous environments. In Proceedings of the 27th IEEE International Performance, Computing and Communications Conference, IPCCC 2008, pages 475–481. IEEE Computer Society.

[15] Jameel, H., Shaikh, R., Lee, H., and Lee, S. (2007). Human identification through image evaluation using secret predicates. topics in cryptology-ct-rsa 07. Lecture Notes in Computer Science, Springer-Verlag, 4377:67–84.

[16] Corradi, A., Montanari, R., and Tibaldi, D. (2004). Context-based access control management in ubiquitous environments. In Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications, NCA 2004, pages 253–260. IEEE Computer Society.

[17] Bellavista, P., Corradi, A., Montanari, R., and Stefanelli, C. (2003). Context-aware middleware for resource management in the wireless internet. IEEE Transactions on Software Engineering, 29(12):1086–1099.

[18] Dey, A. K. (2001) “Understanding and Using Context”, Journal of Personal and Ubiquitous Computing, vol. 5, pp. 4-7. Springer.

[19] Poisson, S. D. (1837) "Récherches sur la probabilité des jugements en matière criminelle et en matière civile", Paris.

[20] Bernoulli, J. (1975) "Ars conjectandi", Werke, 3, pp. 107–286. Birkhäuser, 1975 (Original: Basle, 1713)

[21] Kulldorff, M. (2009) “SaTScan v8.1.1: Software for The Spatial and Space-Time Scan Statistics”. Disponível em: <http://satscan.org/>. Acesso em: 27 dez. 2009

[22] Salton, G. (1989) “Automatic Text Processing: The transformation, analysis, and retrieval of information by computer”, Addison-Wesley, Massachusetts, USA.

[23] Rocha, C. (2010) “Uma Arquitetura para Autenticação Sensível ao Contexto Baseada em Definições Comportamentais”, Dissertação (Mestrado), Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis.