Autenticação de Sensores usando Eventos Físicos

Wilson S. Melo Jr.[1], **Charles B. Prado**[1], **Luiz F. R. C. Carmo**[2]

[1]Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro)
Av. Nossa Senhora das Graças, 50 – Duque de Caxias – RJ

[2]Universidade Federal do Rio de Janeiro
Rio de Janeiro – RJ.

{wsjunior,cbprado}@inmetro.gov.br, lfrust@nce.ufrj.br

Abstract. *Sensors authentication is a challenge that need to be properly addressed. In this paper we propose the use of physical events for sensors authentication. Unpredictability and uniqueness physical systems properties are explored to generate event identifiers from sensing information. Being unique and hard to guess, event identifiers can be used for strengthening authentication. Moreover, event identifiers provide evidences of authentication co-location and simultaneity, preventing relay and replay attacks. The authentication feasibility is demonstrated using sensing systems real cases related to vehicle crash test instrumentation, with promising results.*

Resumo. *A autenticação de sensores é um desafio que necessita ser tratado de forma apropriada. Neste artigo é proposto o uso de eventos físicos para autenticação de sensores. A imprevisibilidade e unicidade dos sistemas físicos são exploradas para gerar identificadores de evento a partir de dados de sensoriamento. Sendo únicos e difíceis de se deduzir, identificadores de evento podem ser usados para reforçar a autenticação. Além disso, eles proveem evidências de co-alocação e simultaneidade da autenticação, evitando ataques do tipo relay e replay. A viabilidade dessa proposta é demonstrada em sistemas de instrumentação de testes de impacto veiculares, com resultados promissores.*

1. Introdução

O mundo testemunhou na última década um crescimento significativo no uso de tecnologias pervasivas. Os computadores estão hoje presentes nas mais diferentes áreas de aplicação. Novas tendências, como Internet das Coisas (IoT) [Al-Fuqaha et al. 2015] e Sistemas Físicos-Cibernéticos (CPS) [Mitra et al. 2013], surgem como campos promissores de pesquisa e desenvolvimento. Atividades de trabalho, negócios, ensino, saúde, mobilidade e lazer podem ser monitoradas, medidas e controladas por aplicações complexas classificadas como "inteligentes" (*smart*).

Neste complexo conjunto de conceitos e tecnologias, o sensoriamento é parte fundamental. Sensores podem ser descritos como blocos elementares na criação das funcionalidades esperadas de uma aplicação "inteligente". Complexos industriais, edificações, veículos, eletro utilitários e mesmo dispositivos biomédicos empregam atualmente uma diversidade de sensores capazes de medir praticamente qualquer tipo de evento físico. Todavia, a segurança da informação continua a ser um preocupação quando tais sistemas complexos são analisados [Al-Fuqaha et al. 2015]. Algumas questões resultam do fato

de que estes dispositivos interagem diretamente com o mundo físico, um desafio relativamente novo cujas consequências não são ainda totalmente conhecidas [Mitra et al. 2013]. Neste contexto, processos como autenticação e autorização são especialmente críticos para se garantir propriedades essenciais de segurança da informação.

Uma vez que sensores se conectam a outros sensores e também a componentes do sistema em níveis mais altos, eles necessitam prover mecanismos de autenticação para garantir acesso mútuo e proteção de informações. Diversas abordagens propondo autenticação de sensores são encontradas na literatura [Priya and Patil 2014]. Pode-se citar as implementações de ICP (Infraestrutura de Chave Pública), assinaturas HMAC que são comuns em sensores inteligentes, soluções baseadas em PUF (*Physical Unclonable Function*) [Suh and Devadas 2007] e funções *one-time* [Hsieh and Leu 2011]. Entretanto, estas soluções podem ser custosas quando dependem de infraestrutura específica. Em outros casos, restrições inerentes à construção dos sensores (bateria, memória e poder computacional por exemplo) podem restringir o uso de soluções de autenticação mais sofisticadas. Assim, mecanismos de autenticação que possam ser implementados sem a necessidade de qualquer recurso adicional são muito desejáveis.

Este trabalho se origina da seguinte questão. Considerando-se a existência de um grupo de sensores que necessitam ser autenticados e que estes sensores monitoram um mesmo evento físico, que possui propriedades físicas intrínsecas, seria possível propor um mecanismo de autenticação baseado em um identificador deste evento físico? Considerando esta questão, este trabalho propõe condições nas quais sistemas físicos são usados como geradores de eventos não determinísticos. Ao mesmo tempo, esses sistemas podem ser vistos como um canal exclusivo para distribuição de identificadores em condições onde um atacante não possua acesso ao ambiente físico, assim evitando ataques *eavesdrop*. Além disso, eventos físicos servem como evidência de simultaneidade e co-alocação, dois conceitos que reforçam a autenticação em situações relacionadas a ataques do tipo *relay* e *replay*. Esta estratégia é denominada *Autenticação baseada em Eventos Físicos* e pode ser implementada em sistemas que utilizam sensoriamento sem a necessidade de qualquer infraestrutura adicional. A proposta é validada usando casos reais de sensoriamento associados com a instrumentação de testes de impacto veiculares.

2. Trabalhos Relacionados

Ideias relacionadas à presente proposta são encontradas na biometria comportamental [Yampolskiy and Govindaraju 2008], que se baseia na análise das ações físicas de um usuário tais como piscar de olhos, técnica de digitação, modo de caminhar, ou qualquer ação que possa ser medida e classificada dentro de um padrão específico. Estabelecido o padrão, este serve para identificar o usuário. Capturar um padrão comportamental envolve o uso de diferentes sensores que descrevem, essencialmente, um evento físico.

A associação entre biometria comportamental e eventos físicos torna-se mais evidente em trabalhos que usam acelerômetros para compor padrões. Em [Gafurov et al. 2007] é descrito um método que usa acelerômetros para reconhecer o jeito de andar de uma pessoa. Aspectos como o posicionamento do sensor, a carga carregada pela pessoa e a taxa de amostragem do sinal afetam o processo de identificação. A mesma ideia é explorada em [Mayrhofer and Gellersen 2007] ao propor um método intuitivo de autenticação mútua de dois dispositivos inteligentes usando acelerômetros. Ambos os

dispositivos devem ser chacoalhados juntos de modo que seus acelerômetros exibirão um alto grau de correlação. O mesmo princípio é explorado em [Wu et al. 2011] que introduz o termo "aperto de mão físico-cibernético". Dois usuários usam dispositivos inteligentes similares a relógios e equipados com acelerômetros. Ao apertarem de mãos, o que constitui um evento físico, os usuários criam um padrão para autenticação mútua.

Também é possível encontrar ideias relacionadas em trabalhos que propõem autenticação a partir de eventos da camada física de redes de comunicação. O uso de *traces* de pacotes de rede para gerar identificadores que atestam que duas entidades estão fisicamente próximas uma da outra, conceito denominado pelos autores como *co-alocação*, é descrito em [Scannell et al. 2009]. Já o conceito de autenticação baseada em canal, com o argumento de que o canal de rádio entre duas entidades é único, é introduzido por [Mathur et al. 2010]. Esta propriedade física é usada para gerar chaves secretas e prover funcionalidades seguras, incluindo autenticação.

Quando comparada aos trabalhos prévios discutidos, a proposta apresentada neste artigo pode ser dita inovadora uma vez que integra diferentes ideias dentro de um método formal e conciso para se implementar autenticação baseada em eventos físicos. Nas próximas seções essa proposta de autenticação é discutida e descrita em detalhes, o que possibilita seu uso em diferentes casos práticos envolvendo sistemas dotados de sensoriamento. Além disso, os conceitos de co-alocação e simultaneidade são apresentados como condições importantes para se evitar ataques do tipo *replay* e *relay*. Por fim, é apresentado um caso de estudo relacionado à instrumentação de testes de impacto veiculares, onde nosso mecanismo de autenticação é aplicado usando dados reais de sensoriamento, sem a necessidade de qualquer componente físico adicional.

3. Autenticação baseada em Eventos Físicos

3.1. Propriedades de um Evento Físico

A existência de uma camada física é provavelmente o principal fator que diferencia sistemas que usam tecnologias pervasivas dos sistemas de computação tradicionais. Nestes sistemas, um conjunto de entradas de dados do mundo físico são capturadas por diferentes sensores. Seus sinais são tratados de modo a coletar dados ou implementar estratégias de controle. Pode-se dizer que estes sensores capturam eventos físicos que por sua vez influenciam o comportamento do sistema como um todo. Sensores descrevem estes eventos medindo grandezas físicas como comprimento, massa, velocidade e temperatura.

Eventos físicos são imprevisíveis e ocorrem apenas uma vez. Isso sugere que cada evento físico é único. Na maioria dos sistemas que interagem com o mundo físico, sensores capturam diversas informações que são filtradas e descartadas quando não são relevantes à aplicação do sistema. Todavia, tais informações podem ser úteis para se caracterizar um evento físico como único. Por sua vez, sua unicidade pode ser associada a uma assinatura ou identificador do evento, extraído das informações de sensoriamento.

Além desse aspecto, quando duas entidades descrevem um mesmo evento físico, pode-se afirmar que as seguintes condições são satisfeitas:

- *Co-alocação*: as entidades estão na mesma localização física ou relativamente próximas. Esta condição é discutida por [Scannell et al. 2009] como estratégia contra ataques do tipo *relay*.

- *Simultaneidade*: as entidades capturam o evento físico ao mesmo tempo. Entende-se que esta condição é importante para evitar ataques do tipo *replay*, algo que apenas a co-alocação não provê.

Nesse trabalho, nossa proposta de autenticação é baseada nas propriedades descritas dos eventos físicos. Assumindo que um evento físico é único e que as entidades a serem autenticadas mensuram este evento, elas serão capazes de descrever o evento físico em termos de grandezas físicas, determinando sua "assinatura" ou identificador.

3.2. Modelo de Ataque

A proposta de autenticação baseada em eventos físicos considera o seguinte modelo de ataque. Duas entidades A e B trocam informações ou proveem serviços uma à outra em um sistema que interage com o mundo físico. Ambas as entidades são sensores ou possuem sensores com os quais monitoram o ambiente físico, mensurando alguma grandeza física. Por questões de segurança, A deve autenticar B antes de qualquer comunicação. Isso é feito por meio de um protocolo de autenticação qualquer onde B apresenta sua identificação e A avalia se a mesma é autêntica. Considera-se que A e B interagem entre si somente quando estão fisicamente próximas. Assim, ambas podem utilizar algum evento físico como informação complementar para a identificação.

Também se considera a existência de uma entidade maliciosa M que realiza ataques contra A e B, com o objetivo de roubar informações ou comprometer serviços. Todavia, M não possui acesso ao ambiente físico onde A e B se encontram. Por definição, M é capaz de executar as seguintes ações:

- M pode expor qualquer informação secreta compartilhada por A e B, como uma senha ou chave criptográfica, usada para estabelecer a autenticação.
- M pode "bisbilhotar" (*eavesdrop*) a comunicação entre A e B, roubando qualquer identificação apresentada por B.
- M pode tentar ataques tipo *relay* contra A, personificando B.
- M pode tentar ataques tipo *replay* contra A, usando uma identificação legítima de B obtida em uma autenticação anterior.

Propõe-se que A e B podem fortalecer a autenticação usando informações de um evento físico que M desconhece. Desta forma, as chances de sucesso de M seriam reduzidas.

3.3. Como a Autenticação baseada em Eventos Físicos funciona

Considerando o modelo de ataque descrito, a autenticação baseada em eventos físicos constitui um método que explora o uso de eventos físicos existentes em sistemas que dispõem de funcionalidades de sensoriamento. Dadas as propriedades de imprevisibilidade e unicidade de um evento físico, espera-se que seu identificador também será único ou pelo menos difícil de se deduzir. O identificador de evento pode ser mensurado pelas entidades legítimas A e B, enquanto um atacante M terá dificuldades de reproduzí-lo. Note-se que um identificador de evento não identifica uma entidade em si, mas está associado à função exercida por essa entidade no sistema. O identificador de evento pode então ser combinado com informações como um número sequencial de identificação da entidade, por exemplo, de modo a prover um mecanismo de autenticação mais forte.

Pode-se afirmar que a autenticação proposta oferece as seguintes vantagens:

1. Assume-se que um evento físico é imprevisível e único, dadas as propriedades do sistema físico a ele associado. Consequentemente, espera-se que um identificador deste evento seja difícil de se adivinhar ou deduzir.
2. Uma vez que M não possui acesso ao ambiente físico do sistema, pode-se dizer que o identificador de evento é obtido por um canal exclusivo, protegido contra ataques *eavesdropping*.
3. O identificador de evento evidencia que A e B satisfazem as condições de co-alocação e simultaneidade, protegendo a autenticação contra ataques tipo *relay*.
4. Como o identificador de evento está associado à função de A e B no sistema, o mesmo pode ser combinado com outro mecanismo para implementar uma autenticação de dois fatores. Pode-se dizer também que o identificador de evento é comparável a uma informação dinâmica que uma entidade legitima conhece.
5. Pode-se implementar esta autenticação em qualquer sistema que disponha de funcionalidades de sensoriamento, sem a necessidade de qualquer infraestrutura ou *hardware* adicional.

3.4. Descrição do Mecanismo de Autenticação

Seja E um evento físico observado e mensurado por um conjunto de N sensores $S = \{s_1, ..., s_i, ..., s_N\}$, onde cada sinal de s_i é dado por um vetor de grandezas físicas $Q = \{q_{i,1}, ..., q_{i,k}, ..., q_{i,K}\}$ correspondentes à medição realizada por s_i em cada amostra $k = 1, 2, .., K$, sendo K o total de amostras. Suponha também um conjunto de M funções $P = \{p_1, ..., p_M\}$ que implementam fusão de dados sobre o sinal de s_i. O identificador ID_i associado ao sensor s_i é dado pela seguinte equação:

$$ID_i = p_1(s_i) \oplus ... \oplus p_k(s_i) \oplus ... \oplus p_M(s_i) \tag{1}$$

onde $\oplus$ é um operador de combinação definido em função da natureza de E e/ou P.

O conjunto de funções P tem um papel importante uma vez que será o responsável por extrair características de um sinal que efetivamente determinarão o identificador de evento. É intuitivo supor que determinadas funções apresentarão melhores resultados em diferentes tipos de eventos e grandezas físicas.

Embora obtidos de um mesmo evento E, não se pode esperar que os identificadores sejam idênticos. É preciso definir uma função de comparação C e um valor de limiar Th, de modo que ID_A e ID_B correspondem a um mesmo evento físico quando:

$$C(ID_A, ID_B) \leq Th \tag{2}$$

4. Estudo de Caso: Autenticação de Sensores em um Testes de Impacto

4.1. Instrumentação de um Teste de Impacto Veicular

Um teste de impacto veicular (*vehicle crash test*) é um teste destrutivo que avalia a segurança passiva de um veículo. São baseados em um conjunto de protocolos de teste que estabelecem diferentes configurações, condições de controle e monitoramento [Insurance Institute for Highway Safety 2014].

Uma visão geral da arquitetura de instrumentação de um teste de impacto é apresentado na Figura 1. Diferentes sensores, usualmente acelerômetros e células de carga,

são posicionados em diferentes pontos do veículo, bem como na barreira de colisão e também no ATD *(Anthropomorphic Test Dummy)*, boneco humanoide usado para avaliar as consequências do impacto sobre pessoas dentro do veículo. Os dados de sensoriamento são coletados por um DAS *(Data Acquisition System)* que digitaliza e armazena os sinais. Em alguns casos o DAS possui sensores integrados, como acontece com o ATD que é também um DAS na prática. As informações de configuração e calibração dos sensores são obtidas de um banco de dados representado como *SensorDB*. O DAS envia os dados a um centro de análise, referenciado como *Control*, onde estes serão verificados e processados. Todo o resultado dos testes é armazenado em um banco de dados *TestDB*.

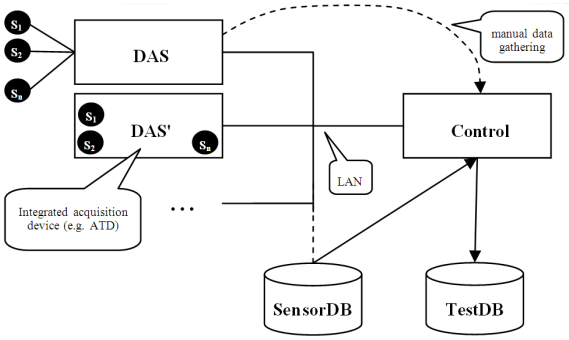

Figura 1. Visão geral da arquitetura de instrumentação de um teste de impacto.

4.2. Instanciando o Modelo de Ataque

Uma vez que os resultados de um teste afetam significativamente as decisões de consumo a respeito de um modelo de veículo, um fabricante malicioso pode ter interesse em modificar os resultados de seu próprio teste de modo a obter uma melhor avaliação de mercado. Ao mesmo tempo, este fabricante pode tentar prejudicar um concorrente, modificando os resultados de seu teste de modo a refletir uma pior avaliação. Ambos os casos estão relacionados à adulteração de dados de sensoriamento ou mesmo à substituição de sensores confiáveis por sensores corrompidos. Ambos os casos também implicam a possibilidade de existência de ataques internos, uma vez que os testes são usualmente conduzidos por laboratórios independentes, em ambientes onde os fabricantes não deveriam ter acesso.

Um exemplo está relacionado com a avaliação de risco de ferimento na cabeça do ATD. Dois indicadores são usualmente aceitos: o HIC (*Head Injury Criteria*) e o vetor resultante de aceleração máxima, ambos obtidos a partir de acelerômetros posicionados dentro da cabeça do ATD [Insurance Institute for Highway Safety 2014]. Um atacante pode modificar dados dos acelerômetros, comprometendo o cálculo destes indicadores e consequentemente modificando o resultado dos testes. Tal ataque poderia ser feito pela substituição do sensor, ou apenas do sinal processado pelo DAS por um sensor/sinal gerado em um teste diferente.

Desse modo, considera-se uma instância do modelo de ataque onde o atacante pode realizar as seguintes ações:

- Interceptar e modificar o sinal de um sensor legítimo antes que este seja recebido por *Control* (ataque tipo *relay*).
- Substituir o sinal de um sensor legítimo por outro sensor também legítimo, todavia obtido em um teste prévio (ataque tipo *replay*).

Em um ataque onde um sensor legítimo pode ser usado em um ambiente de teste manipulado para gerar resultados maliciosos, abordagens tradicionais de autenticação não são suficientes. Se um sensor legítimo é usado, nenhuma suspeita será levantada quanto à sua identificação. Neste caso, um método de autenticação que satisfaça as condições de co-alocação e simultaneidade pode oferecer maior confiabilidade.

4.3. Propondo uma Autenticação Baseada em Eventos Físicos

Como resposta para o modelo de ataque descrito, este trabalho propõe implementar uma autenticação baseada em eventos físicos para alguns sensores posicionados dentro do ATD durante um teste de impacto. O evento físico é a colisão em si. Mesmo quando um único protocolo de testes é considerado, cada colisão produz um resultado único devido à resposta cinética dos materiais utilizados na construção do veículo. Quando sensores descrevem um mesmo evento físico, proveem evidências de que foram utilizados no mesmo teste de impacto, satisfazendo as condições de co-alocação e simultaneidade.

O processo de autenticação ocorre da seguinte forma. Primeiramente define-se *Control* como a entidade responsável por autenticar um sensor antes de aceitar seus dados. Supõe-se também que cada sensor já dispõe de algum mecanismo para prover uma identificação (por exemplo, um código de fabricação), embora esse mecanismo não possa atestar qualquer informação sobre tempo e local onde os dados foram obtidos. Assim, a identificação do sensor deve ser complementada com um identificador de evento físico. Este identificador é calculado usando dados brutos de sensoriamento, sendo determinado simultaneamente ao evento. Uma vez obtido o identificador de evento, este é verificado por meio da função de comparação definida para tal. Para cada sinal, se a função de comparação satisfaz o critério de limiar estabelecido, o sensor é autenticado por *Control*.

4.4. Cenários de Autenticação

O protocolo de testes escolhido determina que a instrumentação do ATD inclua acelerômetros e/ou células de carga em seu corpo e membros. Durante a colisão, as partes do ATD sofrem a ação de diferentes forças co-relacionadas. As forças que agem na cabeça do ATD são também observadas em seu pescoço e peito. O termo *sensores vizinhos* será usado para se referir a grupos de sensores que compartilham esta propriedade.

Também é comum que protocolos de teste especifiquem o uso de sensores redundantes, prevenindo a perda de sinais em função de falhas na instrumentação durante a colisão. Este aspecto pode ser útil para a autenticação uma vez que sensores posicionados no mesmo local capturam praticamente as mesmas informações sobre o evento físico.

Neste estudo, são autenticados sensores posicionadas na cabeça e no pescoço do ATD. A razão desta escolha é que estes sensores são os mais significativos na avaliação dos resultados do teste de impacto. Diversos programas de avaliação de segurança passiva em veículos propõe o valor do HIC como decisivo na pontuação a ser atribuída ao veículo. Além disso, os sensores de cabeça e pescoço são sensores vizinhos, o que facilita determinar a similaridade entre seus sinais. Também foi escolhido um protocolo de testes que determina o uso de sensores redundantes na cabeça do ATD. Deste modo, é possível determinar dois cenários de teste distintos, a saber:

- *Cenário NS (Sensores Vizinhos)*: um identificador de evento resulta de sensores posicionados em uma mesma "vizinhança" dentro do veículo.

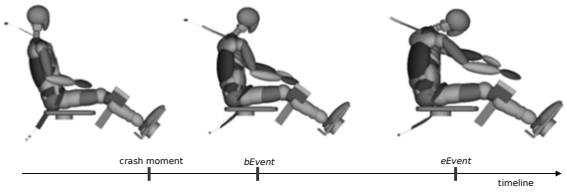

Figura 2. Movimento do ATD na linha de tempo da colisão

- *Cenário RS (Sensores Redundantes)*: um identificador de evento resulta de sensores redundantes.

4.5. A Colisão como Evento Físico

Os sensores da cabeça do ATD são acelerômetros triaxiais cuja grandeza física é dada em G's (sendo $G \approx 9,8m/s^2$). O sensor de pescoço é uma célula de carga triaxial que reporta medidas de força em Newtons (N). Ambas as grandezas são inter-comparáveis por meio da equação $F = ma$. Mesmo sem conhecer a massa m do veículo, é possível normalizar ambos os sinais. Além disso, ao invés de avaliar cada eixo do sinal de forma separada, opta-se pela resultante do vetor de aceleração/força, dada pela equação:

$$R_s = norm\left(\sqrt{X_s^2 + Y_s^2 + Z_s^2}\right) \tag{3}$$

onde $norm()$ é a função de normalização, R_s é a resultante do sinal de um sensor s e X_s, Y_s e Z_s são as componentes em cada eixo.

São definidas também as variáveis $bEvent$ e $eEvent$ como pontos na linha do tempo onde o evento físico tem início e fim, respectivamente (Figura 2). No exato instante da colisão, o ATD manterá sua inércia e continuará sua trajetória dentro do veículo por aproximadamente 50 ms. Considera-se como $bEvent$ o instante de tempo aproximado quando o peito do ATD desacelera gradualmente pela tensão do cinto de segurança. Por sua vez $eEvent$ deve coincidir com o pico de desaceleração do ATD, determinante no cálculo do HIC e do vetor resultante de aceleração máxima. Após $eEvent$, a trajetória do ATD torna-se imprevisível em função do impacto contra o *air-bag* do veículo, o que dificulta identificar e analisar a relação entre as forças resultantes do impacto.

4.6. O Identificador ID_i e a Função de Comparação C

Um identificador de evento ID_i pode ser obtido extraindo-se características relevantes do sinal de cada sensor. Isso é feito combinando-se dois métodos de fusão de dados. O primeiro é algoritmo de quantização proposto por [Liu et al. 2009] que combina Filtro de Médias Móveis (MAF) com passo variável como fator de compressão e discretização do sinal para eliminar operações de ponto flutuante. Este método resulta na redução do número de amostras e requer menor esforço computacional. O segundo é uma função de extração de informações projetada a partir de observações empíricas dos sinais de diferentes sensores posicionados na cabeça e pescoço do ATD. Foi verificado que os sinais de sensores usados em um mesmo teste apresentam um padrão similar em termos de frequências médias. Isto pode ser evidenciado nos valores de máximos e mínimos locais do sinal, quando quantizações com MAF usando diferentes tamanhos de janela são comparadas (Figura 3).

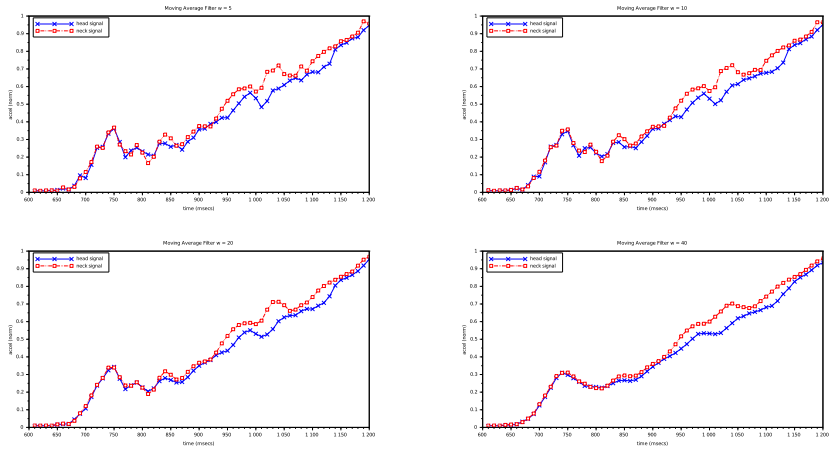

Figura 3. Aplicando MAF com diferentes tamanhos de janela w

Uma descrição formal do método usado para obtenção do identificador de evento é obtida instanciando-se a equação 1. Sejam $M = 3$ e $P = \{p_1, p_2, p_3\}$, tem-se:

$$ID_i = p_1 \oplus p_2 \oplus p_3 \tag{4}$$

onde $\oplus$ é definido como um operador de função composta.

Primeiramente define-se p_3 como o algoritmo de quantização de [Liu et al. 2009]:

$$p_3 = quant(R_s, w_i, step) \tag{5}$$

onde $quant(...)$ é uma função que aplica o algoritmo MAF em R_s com um tamanho de janela w_i e fator de compressão $step$.

Para extrair informação de frequências médias de um sinal R_s, são obtidos dois sinais quantizados diferenciados pelo tamanho da janela w_i usada pelo algoritmo MAF. Sejam w_a e w_b tamanhos diferentes de janela onde $w_a < w_b$, informação associada a frequências médias de R_s podem ser obtidas calculando-se p_2 como:

$$p_2 = p_3(R_s, w_b, step) - p_3(R_s, w_a, step) \tag{6}$$

Como último passo, a informação resultante de p_2 é normalizada e discretizada dentro de uma faixa de valores $range$, sendo que p_1 é definida como:

$$p_1 = int(norm(p_2) * range) \tag{7}$$

onde $int(...)$ é o truncamento de cada valor em p_2 e $range$ é a faixa de discretização.

Por sua vez, a função de comparação C é dada como uma medida de similaridade entre dois identificadores de um mesmo evento físico. Neste experimento foram obtidos bons resultados combinando-se Correlação de Pearson e a função Coerência usada por [Mayrhofer and Gellersen 2007]. Da mesma forma como desenvolvido para ID_i, a especificação formal de C foi obtida instanciando-se a equação 2 da seguinte forma:

$$C(ID_A, ID_B) = (1 - max(correl(ID_A, ID_B), 0) * (1 - coher(ID_A, ID_B)) \tag{8}$$

onde $correl(...)$ é a Correlação de Pearson e $coherence(...)$ é a função Coerência. Sobre a correlação é importante observar que valores negativos são considerados como zero.

5. Experimento Prático e Resultados

5.1. Descrição do Experimento

A autenticação é avaliada por meio de um experimento prático usando dados de testes de impacto da NHTSA [National Highway Traffic Safety Administration 2015]. Foram coletados 100 casos de teste mais recentes realizados com o protocolo de colisão frontal (*vehicle into barrier*) [National Highway Traffic Safety Administration 2012]. Os arquivos de dados disponibilizados pela NHTSA constituem séries temporais amostradas a uma frequência de 1 Khz durante um intervalo de 500 milissegundos (ms). Os dados de teste foram divididos em dois grupos: grupo de análise, onde diferentes métodos e ajustes foram testados de modo a se determinar os melhores resultados; e o grupo de validação, usado para se obter as métricas de desempenho das funções selecionadas.

5.2. Valores Atribuídos às Variáveis de Sintonia

O experimento utiliza as equações definidas na seção 4.6 para gerar os identificadores de evento, bem como a função de comparação. O método é sensitivo aos valores atribuídos para o intervalo de dados de análise determinado por $bEvent$ e $eEvent$, aos tamanhos de janela w_a e w_b usados no MAF, ao fator de compressão $step$ e ao fator de discretização $range$. Os respectivos valores e as justificativas para sua atribuição são discutidos a seguir.

Os valores de $bEvent$ e $eEvent$ foram escolhidos de modo a descartar dados amostrados antes dos primeiros 50 ms após a colisão e após a desaceleração máxima do ATD. $bEvent$ e $eEvent$ foram definidos testando-se valores nas faixas de 40 até 60 ms e 100 a 150 ms, respectivamente. Bons resultados foram obtidos com $bEvent$ em 60 ms e $eEvent$ em 120 ms. Tem-se assim um sinal R_s de 600 pontos de dados, para cada sensor.

As janelas w_a e w_b são variáveis críticas para a identificação do evento. Primeiramente w_a deve ser definido de modo a eliminar apenas frequências altas indesejáveis. Por sua vez, w_b é definido com o objetivo de preservar frequências baixas. Quando a equação 6 é aplicada, o resultado será essencialmente a informação de frequências médias do sinal. Os valores de w_a e w_b foram determinados empiricamente, testando-se valores na faixa entre 5 e 100 pontos de dados. Janelas de tamanho menor mostraram-se pouco efetivas enquanto janelas de tamanho maior eliminam praticamente toda a informação de frequência média. Os melhores resultados foram obtidos com $w_a \approx 10$ e $w_b \approx 40$.

O fator de compressão $step$ determina quanto do sinal de dados será comprimido. Um fator alto resulta em menos informação e consequente redução na acurácia do processo de autenticação. Bons resultados foram obtidos usando-se $step = 10$, que implica em 90% de compressão e redução dos 600 pontos de R_s a 60 pontos de dados.

Por fim, $range$ é definido de modo a se obter uma representação binária de ID_i. Atribuindo-se $range = 8$, os valores normalizados são distribuídos em valores discretos entre -7 e 8. Isto permite representar cada ponto de dados em ID_i como um valor hexadecimal entre `0x0` e `fx0`, ocupando 2 bytes. Uma vez que p_3 retorna um vetor de 60 pontos, tem-se um identificador de evento de 30 *bytes*, ou 240 *bits*.

5.3. Resultados do Cenário NS

Uma vez que a autenticação trabalha com sensores da cabeça e pescoço do ATD, considera-se que o atacante pode tentar corromper um desses sensores para comprometer os resultados do teste. Para o cenário NS duas situações são inicialmente descritas:

- **Ataque HxH**: O atacante compromete o sensor da cabeça do ATD usando um sinal legítimo obtido de um sensor de cabeça usado em um teste diferente.
- **Ataque NxN**: O atacante compromete o sensor do pescoço do ATD usando um sinal legítimo obtido de um sensor de pescoço usado em um teste diferente.

Com o objetivo de verificar a robustez do método de autenticação proposto, foram investigadas duas outras situações. Supõe-se que o atacante conhece o mecanismo de autenticação e portanto sabe que o identificador de evento obtido de um sensor de cabeça será comparado ao obtido pelo pescoço, ou vice-versa. Com a intenção de confundir o processo de autenticação, o atacante pode tentar substituir um sinal da cabeça do ATD por um sinal do pescoço. A ideia por trás desta estratégia é a possibilidade de que a comparação entre dois sinais do pescoço de um ATD, ainda que de eventos diferentes, apresente tanta similaridade quanto os sinais da cabeça e pescoço de um mesmo evento. Para testar um eventual ataque como este são acrescidas as seguintes situações:

- **Ataque HxN**: O atacante compromete o sensor da cabeça do ATD usando um sinal legítimo obtido de um sensor de pescoço usado em um teste diferente.
- **Ataque NxH**: O atacante compromete o sensor do pescoço do ATD usando um sinal legítimo obtido de um sensor de cabeça usado em um teste diferente.

A probabilidade de sucesso de tais ataques é verificada por meio do seguinte experimento. Para cada caso de teste $k = 1, 2, ..., K$, sendo K o total de casos analisados, determina-se o i-ésimo identificador de evento para os sensores da cabeça e pescoço do ATD, obtendo-se assim $ID_{i,H}$ e $ID_{i,N}$, respectivamente. Em seguida calcula-se $C_{leg,i} = C(ID_{i,H}, ID_{i,N})$ usando-se a equação 8. Simula-se então a tentativa de fraude do i-ésimo identificador de evento, substituindo-se os dados brutos do sensor sob ataque em cada situação descrita com os dados do j-ésimo evento, sendo $j = 1, 2, ..., K$ e $j \neq i$.

Espera-se que o algoritmo de autenticação proposto determine $C_{leg,i} \leq Th$, satisfazendo a equação 8. Em contrapartida, espera-se que cada situação de ataque simulado j resulte em $C_{X,j} > Th$, onde $X = \{HH, NN, HN, NH\}$. Casos de ataque duplicados não desconsiderados pois C é comutativa e portanto $C(ID_i, ID_j) = C(ID_j, ID_i)$.

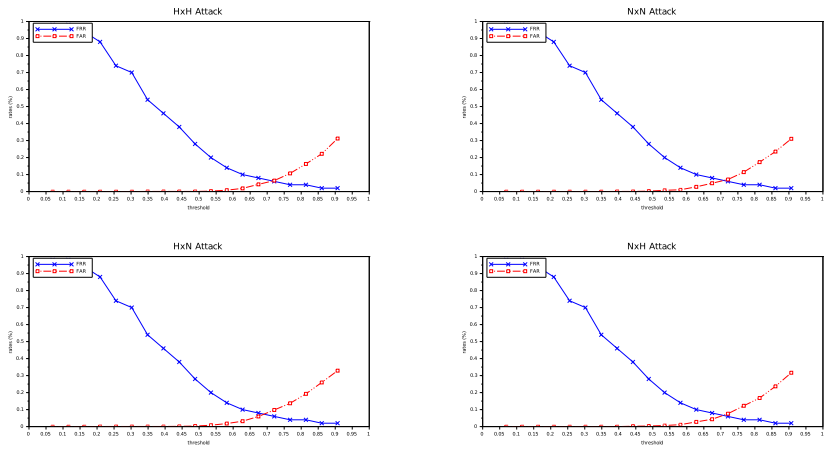

Figura 4. FRR e FAR para o Cenário NS, com diferentes valores de Th

A eficiência do método de autenticação proposto foi avaliada usando métricas comuns em sistemas biométricos, que são a FRR (*False Rejection Rate*) e FAR (*False*

Tabela 1. Taxas de desempenho da autenticação - Cenário NS com $Th = 0.5$

	HxH		**NxN**		**HxN**		**NxH**	
	OK	**NOK**	**OK**	**NOK**	**OK**	**NOK**	**OK**	**NOK**
Sensores legítimos	41	9	41	9	41	9	41	9
Sensores sob ataque	10	1215	9	1216	14	1211	7	1218
FRR	18%		18%		18%		18%	
FAR	0.8%		0.7%		1.1%		0.6%	
F-Measure	0.81		0.82		0.78		0.83	

Acceptance Rate). Primeiramente, usando o grupo de dados de análise, verificou-se como FRR e FAR se comportam em função do valor de limiar Th, conforme apresentado na Figura 4. Pode-se observar que o valor de erro CER (*Crossover Error Rate*) ocorre quando $0.65 < Th < 0.75$ em todas as situações de ataque. Uma vez que o problema tratado é a autenticação, pode-se afirmar que um menor valor de FAR é melhor do que um baixo valor de FRR. Se uma autenticação legítima é negada, a autenticidade do sensor pode ser verificada por um segundo método. Por outro lado, se uma tentativa de ataque é aceita pelo processo de autenticação, nenhuma suspeita será levantada e tem-se uma falha de segurança. Com base nestas considerações, definiu-se $Th = 0.5$ na expectativa de se obter um FRR superior a 10% mas ao mesmo tempo manter FAR abaixo de 1%.

Por fim o desempenho da autenticação é determinado usando-se o grupo de dados de validação. A Tabela 1 resume os resultados. Como esperado, FAR se mantém abaixo de 1% para todas as situações de ataque, exceto *HxN*. Como efeito colateral, tem-se FRR em 18%, o que pode ser considerado um resultado razoável pois compromete a usabilidade do método em razão de um excessivo número de sensores legítimos que serão considerados suspeitos de ataque. Conclui-se que as funções de geração do identificador de evento e de comparação necessitam ser melhorada, visando a redução do valor de FRR.

5.4. Resultados do Cenário RS

No cenário RS são usados sensores redundantes da cabeça do ATD. Dois sensores posicionados no mesmo local apresentam entre si uma alta correlação, facilitando a obtenção de um identificador. Em compensação, a autenticação de um cenário RS pode não ser factível se for considerado que um atacante pode substituir os sensores do ATD fisicamente, pois nesse caso ele pode substituir também o sensor redundante. Independente disso a autenticação com sensores redundantes pode ser útil em situações quando não se tem acesso físico aos sensores e o ataque consiste em se substituir os dados de sensoriamento obtidos pelo DAS, desde que a coleta de dados dos sensores principais e redundantes se dê por canais diferentes de acesso.

Repetindo o mesmo experimento descrito na seção anterior, o grupo de dados de análise foi usado para avaliar a variação de FRR e FAR em função do limiar Th. A diferença é que neste caso apenas a situação HxH se aplica por não haver sensores redundantes no pescoço. Os valores de FRR e FAR são exibidos na Figura 5. Pode-se observar que o CER ocorre durante um intervalo maior quando $0.3 < Th < 0.5$, onde tanto FAR quanto FRR apresente valores muito próximos de zero. Isto acontece devido a elevada similaridade entre os sinais dos sensores redundantes. Consequentemente definiu-se $Th = 0.4$ com a expectativa de valores praticamente ótimos para FRR e FAR.

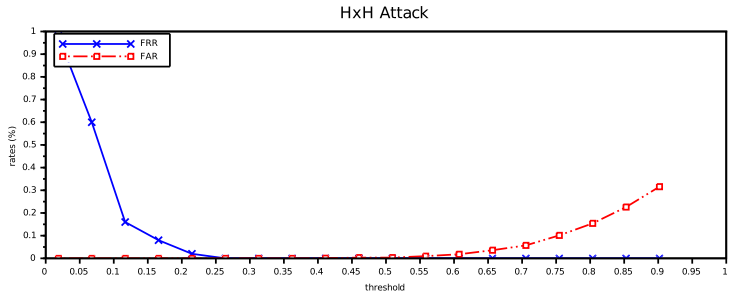

Figura 5. FRR e FAR para o Cenário RS, com diferentes valores de Th

Usando o grupo de dados de validação, foram calculadas as taxas de desempenho da autenticação para ao cenário RS, conforme a Tabela 2. Como esperado, ambos os valores de FRR e FAR ficam próximos de zero, mostrando que sensores redundantes permitem a autenticação baseada em eventos físicos com elevada eficiência.

Tabela 2. Taxas de desempenho da autenticação - Cenário RS com $Th = 0.4$

	HxH	
	OK	**NOK**
Sensores legítimos	50	0
Sensores sob ataque	1	1224
FRR	0%	
FAR	0.08%	
F-Measure	0.99	

6. Conclusão

Este artigo apresentou uma proposta de implementação de autenticação de sensores baseada em eventos físicos. Pode-se afirmar que esta pesquisa é importante dada a necessidade de mecanismos de autenticação em sistemas com sensoriamento. Além disso, o método proposto produz evidências de co-alocação e simultaneidade das entidades envolvidas, podendo ser implementado em qualquer sistema de sensoriamento sem a necessidade de infraestrutura adicional. Os argumentos são fortalecidos pelos resultados práticos obtidos no estudo de caso. Foi demonstrado que o evento da colisão é capturado por diferentes sensores que preservam informações comuns entre si. Dada a similaridade dos sinais, é possível implementar a autenticação atestando que os sensores operam no mesmo tempo e local, evitando assim ataques tipo *replay* e *relay*. Ambos os cenários NS e RS foram avaliados com resultados promissores.

Este estudo também abre diversas possibilidades em termos de pesquisas futuras. Primeiramente, a investigação quanto à possibilidade de se aplicar esta autenticação em soluções de IoT e CPS. Outra linha de futuros estudos será a natureza aleatória dos eventos físicos, visando descrever quais classes de eventos são mais apropriados para prover este tipo de autenticação. Por fim, a investigação de métodos e estratégias de fusão de dados e reconhecimento de padrões pode auxiliar na criação de um arcabouço de algoritmos para implementação deste tipo de autenticação em diferentes classes de sistemas físicos.

Referências

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347 –2376.

Gafurov, D., Snekkenes, E., and Bours, P. (2007). Gait authentication and identification using wearable accelerometer sensor. *2007 IEEE Workshop on Automatic Identification Advanced Technologies - Proceedings*, pages 220–225.

Hsieh, W.-B. and Leu, J.-S. (2011). Design of a time and location based One-Time Password authentication scheme. In *Wireless Communications and Mobile Computing Conference IWCMC 2011 7th International*, pages 201–206.

Insurance Institute for Highway Safety (2014). Moderate Overlap Frontal Cashworthiness Evaluation. Technical Report September.

Liu, J., Zhong, L., Wickramasuriya, J., and Vasudevan, V. (2009). uWave: Accelerometer-based personalized gesture recognition and its applications. *Pervasive and Mobile Computing*, 5(6):657–675.

Mathur, S., Reznik, A., Ye, C., Mukherjee, R., Rahman, A., Shah, Y., Trappe, W., and Mandayam, N. (2010). Exploiting the physical layer for enhanced security. *IEEE Wireless Communications*, 17(5):63–70.

Mayrhofer, R. and Gellersen, H. (2007). Shake Well Before Use: Authentication Based on Accelerometer Data. In *5th International Conference, PERVASIVE 2007*, pages 144–161.

Mitra, S., Wongpiromsarn, T., and Murray, R. M. (2013). Verifying Cyber-Physical Interactions in Safety-Critical Systems. *IEEE Security & Privacy*, 11(4):28–37.

National Highway Traffic Safety Administration (2012). Laboratory Test Procedure For New Car Assessment Program Frontal Impact Testing. Technical Report September.

National Highway Traffic Safety Administration (2015). NHTSA Vehicle Crash Test Database. http://www-nrd.nhtsa.dot.gov/database/veh/veh.htm. Accessed: 2015-05-05.

Priya, L. C. and Patil, S. D. (2014). A Survey on Sensor Authentication in Dynamic Wireless Sensor Networks. *International Journal of Computer Science and Information Technology Research*, 2(2):454–461.

Scannell, A., Varshavsky, A., Lamarca, A., and de Lara, E. (2009). Proximity-based authentication of mobile devices. *International Journal of Security and Networks*, 4(1/2):4–16.

Suh, G. E. and Devadas, S. (2007). Physical unclonable functions for device authentication and secret key generation. *Proceedings - Design Automation Conference*, pages 9–14.

Wu, F.-J., Chu, F.-I., and Tseng, Y.-C. (2011). Cyber-physical handshake. *ACM SIGCOMM Computer Communication Review*, 41(4):472.

Yampolskiy, R. V. and Govindaraju, V. (2008). Behavioural biometrics: a survey and classification. *International Journal of Biometrics*, 1(1):81–113.

