Universidade do Minho
Escola de Engenharia

Nadine Dos Santos Domingos

Biometrias comportamentais em dispositivos móveis

Outubro de 2014

Biometrias comportamentais em dispositivos móveis
Nadine Dos Santos Domingos
UMinho | 2014

Universidade do Minho
Escola de Engenharia

Nadine Dos Santos Domingos

Biometrias comportamentais em dispositivos móveis

Dissertação de Mestrado
Ciclo de Estudos Integrados Conducentes ao Grau de
Mestre em Engenharia e Gestão de Sistemas de Informação

Trabalho efetuado sob a orientação do
Professor Doutor Henrique Manuel Dinis Santos

Outubro de 2014

DECLARAÇÃO

Nome: Nadine dos Santos Domingos

Endereço eletrónico: naddomingos@hotmail.com Telefone: 917726251

Número do Bilhete de Identidade: 13758834

Título dissertação: Biometrias Comportamentais em Dispositivos Móveis

Orientador:

Professor Doutor Henrique Manuel Dinis dos Santos

Ano de conclusão: 2014

Mestrado em Engenharia e Gestão de Sistemas de Informação

É AUTORIZADA A REPRODUÇÃO INTEGRAL DESTA DISSERTAÇÃO APENAS PARA EFEITOS DE INVESTIGAÇÃO, MEDIANTE DECLARAÇÃO ESCRITA DO INTERESSADO, QUE A TAL SE COMPROMETE.

Universidade do Minho, _____/_____/_____

Assinatura: Nadine dos Santos Domingos

Agradecimentos

Agradeço aos meus pais João e Júlia, pelo incentivo e apoio que me proporcionaram, para que pudesse realizar esta etapa, pois sem os seus sacrifícios esta não poderia ser concretizada.

Agradeço ao meu irmão Marco, pela preocupação constante que demonstrou, bem como ao seu incansável incentivo e disponibilidade para me ajudar.

Agradeço ao meu orientador Henrique Santos o encorajamento e entusiasmo que me transmitiu, uma vez este me permitiu olhar para este projeto de uma forma entusiástica. Agradeço ainda a sua disponibilidade para me auxiliar nas diversas etapas da dissertação.

Agradeço à Benedita e à Marta pela amizade e incentivo que me deram ao longo do meu percurso académico e desta dissertação.

Por fim, agradeço a todos os que me auxiliaram de alguma forma neste projeto.

Resumo

Ao longo dos tempos, tem-se verificado um aumento da utilização de dispositivos móveis tácteis, que proporcionam diversos benefícios e facilidades, como o acesso à internet e contas pessoais. Ou seja, estes já não se destinam unicamente a funcionalidade de comunicação. Uma vez que os dispositivos guardam credenciais e outras informações pessoais e são facilmente roubados ou perdidos, torna-se importante encontrar mecanismos de autenticação mais eficazes que protejam estes dados.

Uma técnica que é amplamente utilizada para a autenticação é a inserção de palavras-chave. Contudo esta técnica possui algumas limitações, pois as palavras-chave são fáceis de roubar e é necessário a sua memorização. Desta forma é desejável encontrar soluções que sejam mais fáceis de utilizar e que não provoquem desconforto aos utilizadores, proporcionando até algum tipo de autenticação continua.

Neste trabalho propõem-se demonstrar a possibilidade de utilização das biometrias comportamentais na autenticação contínua do utilizador, em dispositivos móveis de ecrã táctil e, de uma forma mais objetiva, que variáveis afetam a sua eficácia.

Palavras-chave: Biometrias comportamentais, Touch-Screen, Autenticação

Abstract

Through the times, there has been an increased use of touch-screen devices, which provide many benefits and facilities, such as internet access and personal accounts. That is, they are no longer solely intended for communication. Once the devices store credentials and other personal information and are easily stolen or lost, it's important to find new authentication mechanisms that are more efficient that protecting this data.

A technique that is widely used for authentication is the insertion of passwords. However this technique has some limitations, because keywords are easy to steal and it's necessary to memorize them. Thus it's desirable to find solutions that are easier to use and do not cause distress to the user, offering some sort of continuous authentication.

In this dissertation it is proposed to demonstrate the feasibility of using behavioral biometrics in continuous user authentication in touch-screen devices, and in a more objective way witch variables affect its effectiveness

Keywords: Behavioral biometrics, Touch-screen, Authentication

Índice

Índice de Figuras

Índice de Tabelas

Lista de Abreviaturas e Siglas

PIN – Personal Identification Number

PDA – Personal Digital Assistants

KDA – Keystroke Dynamic-based Authentication

AND – Ácido desoxirribonucleico

FAR – False Acceptance Rate

FRR – False Rejection Rate

EER – Equal Error Rate

FP – False Positive

TP – True Positive

FN – False Negative

TN – True Positive

ROC – Receiver Operating Characteristic

AUC – Area Under the Curve

SVM – Support Vector Machine

PCA – Principal Component Analysis

SMS – Short Message Service

URL – Uniform Resource Locator

GPS – Global Positioning System

SSID – Service Set Identifier

API – Global Positioning System

Capitulo I - Introdução

1.1 Motivação e problema de investigação

Os dispositivos móveis assumem uma grande importância na sociedade atual. Destes pode-se enunciar algumas tecnologias como os telemóveis, computadores portáteis, assistentes pessoais digitais (PDAs), *smartphones, notebooks*, agendas eletrónicas, entre outros.

Este tipo de dispositivos tem vindo a tornar-se cada vez mais essencial no quotidiano das pessoas, uma vez que estes proporcionam cada vez mais funcionalidades, não se baseando apenas na funcionalidade de comunicação, ou seja, já não se destina unicamente à realização de telefonemas ou envio de mensagens de texto (Dedhia, 2011). Atualmente um indivíduo pode jogar, editar documentos, aceder à internet e, consequentemente, aceder ao correio eletrónico, assim como outros serviços pessoais. Além destas novas funcionalidades os dispositivos móveis são desenvolvidos de forma a suportar sistemas de ecrãs tácteis. Deste modo a interação entre o utilizador e o dispositivo é melhorada uma vez que existe uma maior rapidez de acesso, promovendo a mobilidade ao dispensar o recurso de periféricos. Em suma, estes dispositivos são desenvolvidos para permitir suportar mecanismos de rápido acesso e de utilização amigável (Saevanee & Bhattarakosol, 2009).

O mecanismo de autenticação mais frequentemente utilizado nestes dispositivos é a palavra-chave, seguindo uma tendência herdada dos computadores. Apesar de vários estudos terem já refletido sobre as vulnerabilidades deste mecanismo de autenticação – e em particular nos dispositivos móveis –, ele continua a ser o preferido dos utilizadores e, como seria de esperar, os fabricantes dos dispositivos móveis não quererão alterar radicalmente essa função, sob pena de o tornarem menos utilizável (Angulo & Wästlund, 2012)

Na autenticação por palavra-chave, as credenciais de acesso são guardadas no dispositivo e esse facto acarreta diversos problemas de segurança, pois caso o dispositivo seja roubado ou perdido, este pode ser explorado e usado inapropriadamente pelo indivíduo que o rouba ou encontra (Dörflinger, Voth, Krämer , & Fromm, 2010).

Segundo (Jansen, 2003) uma das melhores formas de proteger os dispositivos da utilização inapropriada por outros indivíduos é a autenticação segura do utilizador.

Este autor afirma que a autenticação de um utilizador pode ser efetuada através de um dos três procedimentos que são descritos a seguir:

- Prova de conhecimento: A autenticação que recorre a este procedimento é efetuada com base numa informação secreta que apenas o utilizador sabe (e que está armazenada no dispositivo), ou seja, um PIN ou palavra-chave.
- Prova de posse: O utilizador efetua a sua autenticação com um objeto, como por exemplo *Smart Cards.*
- Prova de propriedade pessoal: Efetua-se a autenticação através de uma característica do utilizador, ou seja, biometria.

As propriedades de segurança que normalmente um sistema deve oferecer são a confidencialidade, a integridade e a disponibilidade. A autenticação afeta todas as propriedades e diz respeito à verificação da identidade do utilizador, ou seja, verificar se o indivíduo é quem clama ser. A confidencialidade pretende assegurar que a informação é acedida apenas por pessoas autorizadas. A propriedade que pretende prevenir a modificação de informação por indivíduos não autorizados é a integridade. A disponibilidade pretende assegurar a utilização de um recurso quando requisitado. Outra propriedade que pode ainda ser detalhada, é a autenticidade. Esta pretende assegurar a não alteração da origem da informação, ou seja, que o recetor receba realmente a informação do emissor. Para além destas propriedades um sistema pode também oferecer algum tipo de controlo, como o não repúdio. Ou seja, quando se pretende que um utilizador não possa posteriormente afirmar que não efetuou uma determinada ação (Ricci, et al., 2006).

Um problema relacionado com a função de autenticação dos utilizadores nos dispositivos móveis é que habitualmente só se efetua uma autenticação inicial, isto é, quando ligamos o dispositivo. Após esta autenticação o utilizador pode mexer livremente no dispositivo sem que lhe seja requerido mais nenhum tipo de identificação (Clarke, 2004). Como os dispositivos móveis são de dimensões reduzidas, estes são facilmente perdidos ou roubados por terceiros. Caso isto aconteça poderá haver invasão de privacidade, perdas financeiras (uma vez que os dispositivos são utilizados também para transações) através a impersonificarão do utilizador por parte do atacante (Angulo & Wästlund, 2012).

Dado o prejuízo que pode advir da perda ou roubo do dispositivo é essencial desenvolver técnicas que permitam proteger da melhor forma os dispositivos móveis, no que respeita ao controlo da autenticação (Saevanee & Bhattarakosol, 2009). Deste modo, a principal questão que se pretende abordar está relacionada com a utilização de biometrias comportamentais na autenticação em dispositivos móveis de ecrã táctil. Ou seja, a sua viabilidade para identificar um indivíduo através da interação entre este e o dispositivo, e a possibilidade de fornecer algum tipo de autenticação contínua e não intrusiva.

1.2 Objetivos

Uma vez que os métodos de autenticação utilizados nos dispositivos de ecrã táctil possuem algumas falhas de usabilidade e segurança, é necessário explorar novas técnicas, mais eficazes num ambiente de mobilidade e que tenha o menor impacto possível na interação com o utilizador. Em resposta a estes requisitos poder-se-á propor uma solução que permita a autenticação contínua e transparente do utilizador. Ou seja, que o proprietário do dispositivo seja constantemente autenticado sem que seja necessária a inserção de palavras-chave, PIN ou outra informação. Esta última característica é possível através da utilização das biometrias comportamentais

Tendo em conta as características atrás enunciadas é proposto neste trabalho:

- Contextualizar o tópico de segurança nos dispositivos móveis, bem como os métodos existentes de autenticação e as suas vantagens e desvantagens;
- Análise das técnicas biométricas para dispositivos Touch-Screen;
- Análise das variáveis associadas ao *Touch-Screen*, como a pressão que o utilizador aplica no ecrã do dispositivo, a posição, orientação, a velocidade e direção de deslocamento;
- Identificar fatores que possam influenciar as variáveis associadas ao *Touch-Screen*, como a faixa etária, experiência de utilização de tecnologias, mão e dedos utilizados na interação com o dispositivo;
- Verificar a viabilidade das biometrias comportamentais na autenticação do utilizador em dispositivos *Touch-Screen.*

Os dois primeiros objetivos foram alcançados através da análise bibliográfica presente neste documento.

Os restantes objetivos foram alcançados através de uma experiência, realizada com um grupo de utilizadores que, embora limitado, contém elementos que garantem a variabilidade investigada. Nesta experiência foram recolhidos dados sobre a pressão, posição, orientação, velocidade e direção de deslocamento que utilizadores exercem quando efetuam movimentos num dispositivo de ecrã táctil, bem como os fatores faixa etária, experiência de utilização de tecnologias, mão e dedos utilizados na interação com o dispositivo.

O último objetivo é alcançado através da análise do cruzamento das variáveis associadas ao uso de *Touch-Screen* e os fatores idade, experiência, mão e dedos usados.

1.3 Métodos

Para se atingir os objetivos recorreu-se ao método de investigação *Survey* Bibliográfico e *Design Science*. O primeiro método foi utilizado numa primeira fase, na revisão bibliográfica. A metodologia *Design Science* foi aplicada na segunda fase. Esta metodologia é constituída por 5 passos, que podem ser visualizados na Figura 1.

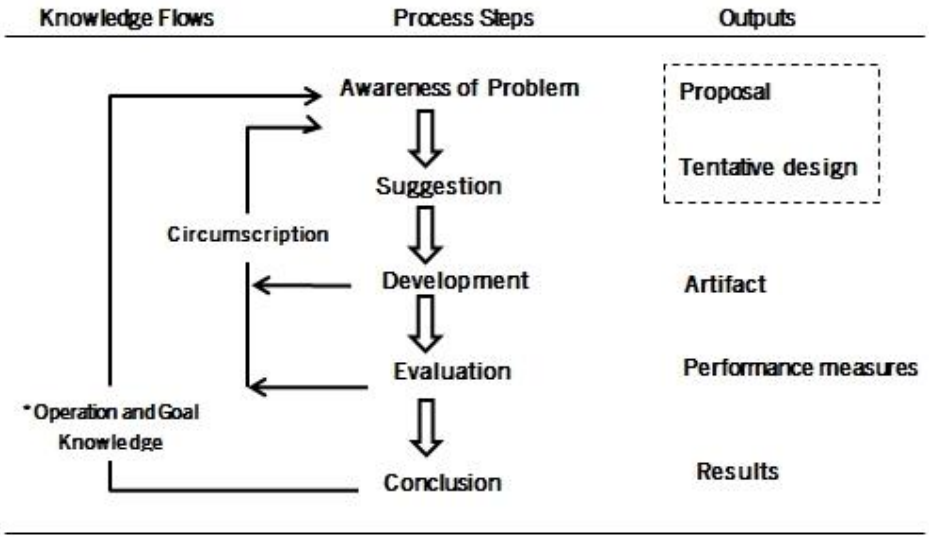

Figura 1 – Metodologia Design Science (Järvinen, 2007)

Na primeira etapa do processo "Awareness of *Problem*", existe uma sensibilização para o problema. Esta resulta da constatação da existência de uma falha de conhecimento. Desta etapa resulta a descrição do tópico a ser investigado. Na etapa "*Suggestion*", pretende-se encontrar uma solução para o problema através da análise de literatura existente. Esta etapa serve de

suporte teórico para investigação. Na etapa seguinte "*Development*", desenvolve-se o artefacto de acordo com as diretrizes apresentadas na etapa anterior. De seguida efetua-se a avaliação do artefacto produzido, ou seja, a sua validação. Por fim, "*Conclusion*", onde se determina a qualidade do artefacto produzido.

Deste modo a primeira fase da elaboração deste projeto consistiu numa análise detalhada dos conceitos relacionados com o tema. Procurou-se abranger bibliografia diversificada (artigos de conferências, teses de mestrado e doutoramento, revistas científicas, livros), de forma a compreender a necessidade de autenticação e como as técnicas utilizadas evoluíram ao longo dos tempos.

Depois da compreensão dos conceitos e técnicas relativas à autenticação em dispositivos moveis, foram de seguida analisadas as falhas e vantagens das técnicas existentes e as direções apontadas para colmatar as falhas e usufruir das vantagens apontadas nas técnicas existentes.

Nesta fase analisaram-se experiências similares desenvolvidas por diversos autores, no âmbito de dispositivos Touch-Screen. Isto com a finalidade de identificar os indicadores que podem apresentar-se como únicos e individuais. Ou seja, identificar os indicadores comportamentais que permitem autenticar um indivíduo.

A segunda fase consistiu na execução de uma experiência, que abrange a realização de movimentos de toque por parte de indivíduos num dispositivo móvel de ecrã táctil. Os indicadores selecionados para a experiência foram a pressão, posição, orientação, velocidade e direção de deslocamento. Foram ainda selecionadas as variáveis faixa etária, experiência dos indivíduos com tecnologias, que mão e dedos usam para interagir com os dispositivos móveis.

Após a recolha dos dados relativo aos indicadores e variáveis selecionados, elaborou-se uma análise de dados, de forma a obter o impacto das variáveis no sucesso de utilização dos indicadores para identificar um indivíduo. Os dados recolhidos foram organizados, tratados e analisados para a dedução da viabilidade dos indicadores comportamentais na identificação única de um indivíduo.

Para validar o artefacto produzido foram usadas medidas de performance para sistemas biométricos Feita a avaliação de performance procedeu-se à fase de conclusão. Nesta foram apontadas as conclusões relativas à qualidade do artefacto produzido.

1.4 Organização do documento

Nesta secção é descrita a estrutura do documento, assim como uma breve síntese do conteúdo de cada um dos capítulos.

Neste primeiro capítulo (Introdução), para além da descrição da organização do documento encontra-se uma secção com a motivação e o problema de investigação da dissertação. Encontra-se também uma secção com a descrição dos objetivos a serem alcançados e uma secção com os métodos de investigação usados para o desenvolvimento da dissertação.

No segundo capítulo apresenta-se uma revisão bibliográfica sobre os principais conceitos relacionados com a função de autenticação em dispositivos móveis. Numa primeira fase é apresentada a descrição das técnicas mais utilizadas para autenticar um indivíduo, focando depois as vantagens das biometrias em relação às restantes técnicas, no contexto em questão. É também descrito o fluxo dos sistemas biométricos, os métodos de análise de desempenho e o algoritmo SVM e PCA para a análise de dados. De seguida apresenta-se uma secção relativa às biometrias, sendo apresentado exemplos de biometrias físicas e comportamentais. Após esta descrição é apresentada a comparação entre biometrias, apontando as vantagens e desvantagens que possuem entre si, mais uma vez considerando o contexto do problema em investigação. É apresentada uma secção relativa ao *Touch-Screen*, em que são descritas as interações, os obstáculos da utilização de dispositivos com a funcionalidade de ecrã táctil. São ainda apresentados diversos estudos efetuados para a autenticação em dispositivos com esta funcionalidade.

No terceiro capítulo é descrita a experiência desenvolvida, os resultados alcançados bem como a análise dos dados obtidos na experiência.

No quarto capítulo são apresentadas as conclusões retiradas da elaboração da dissertação, assim como as contribuições que esta acrescenta na área de biometrias comportamentais para dispositivos móveis *Touch-Screen*. São ainda apresentadas as limitações deste trabalho, bem como sugestões para trabalhos futuros.

Capitulo II - Revisão bibliográfica

2.1 Técnicas de autenticação

Para a proteção de um sistema é necessária a existência de controlo de acessos. Este é o processo de mediar pedidos a recursos e dados, ou seja, existe uma identidade que determina o que outra identidade pode fazer com os recursos (Sandhu & Samarati, 1996). Com isto, pode-se ainda afirmar que o contro de acessos tem como tarefa permitir ou negar o acesso de um indivíduo (Lee & Oh, 2013).

O contro de acessos é uma solução incompleta para a segurança de sistemas. Assim sendo, é necessário englobar os serviços de autenticação, autorização e auditoria. Idealmente um sistema deveria ser implementado de acordo com a Figura 2.

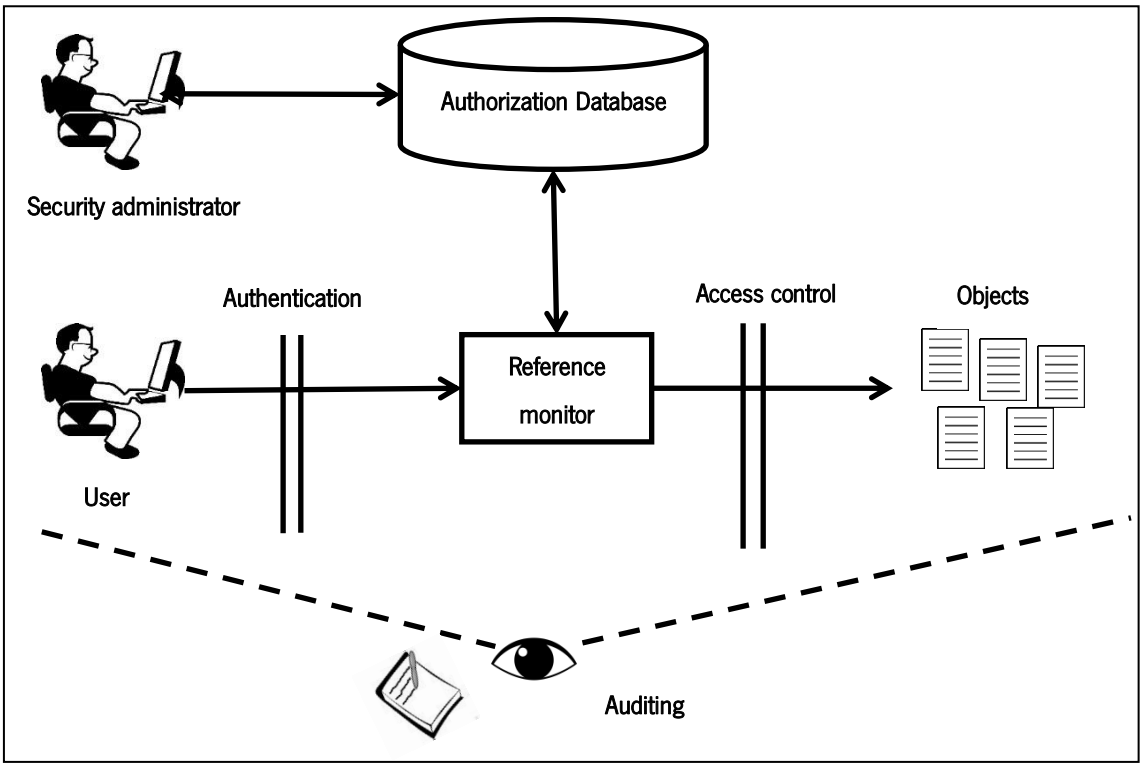

Figura 2 – Controlo de Acesso e outros serviços (Sandhu & Samarati, 1994)

Um sistema pode ou não englobar todos os serviços. Contudo o controlo de acesso normalmente requer a autenticação como pré-requisito (Sandhu & Samarati, 1996). Deste modo a autenticação do utilizador é a base para verificar se um indivíduo é autorizado a efetuar determinada ação (Lee & Oh, 2013). O controlo de acesso assume que a autenticação identifica corretamente o indivíduo, consequentemente a eficácia do controlo de acesso recai na correta identificação do indivíduo, ou seja, na autenticação (Sandhu & Samarati, 1994).

Uma das técnicas amplamente utilizada para a autenticação de dispositivos móveis, como os telemóveis, é o número de identificação pessoal (PIN). Este é normalmente constituído por uma sequência de quatro dígitos, sendo estes apenas uma variação dos dez algarismos (Jansen, 2003). Outra técnica que é muito usada para a segurança dos dispositivos é a autenticação por palavra-chave (Skaff, 2007). Esta oferece um maior número de combinações do que o PIN, pois podem ser constituídas por combinações de números, letras do alfabeto, e outros caracteres (Jansen, 2003).

Apesar destas serem as técnicas mais frequentes, elas evidenciam algumas desvantagens, entre elas o fato de o ser humano não possuir uma grande facilidade para memorizar grandes sequências constituídas por números e letras (Weiss & Luca, 2008). E dado que a segurança é melhorada proporcionalmente ao tamanho da palavra-chave torna-se mais complexo memorizar estas (Weiss & Luca, 2008). Por esse motivo as palavras-chave são normalmente sequências que os utilizadores memorizam com maior facilidade (data de nascimento, moradia, nomes de pessoas), o que as tornam suscetíveis a ataques baseados em dicionário (Chang, Tsai, & Lin, 2012). Outra falha de segurança relativa a estas duas técnicas é o fato de os utilizadores escreverem os códigos num papel ou revelarem-nos a amigos ou colegas (Clarke, 2004).

Além destas técnicas, baseadas na memorização de sequências alfanuméricas, outra vertente que tem sido explorada para a autenticação são as técnicas baseadas em biometrias. Estas não necessitam do fator de memorização, pois baseiam-se em caraterísticas do indivíduo. Segundo o autor de (Clarke, 2004), uma autenticação baseada em biometrias refere-se *"a algo que o utilizador é"*. Assim sendo as caraterísticas únicas e individuais de cada indivíduo podem ser consideradas como um elemento de identificação e autenticação (Costa, Obelheiro, & Fraga, 2006).

As biometrias têm vindo a assumir uma maior relevância em grande parte devido ao esforço de investigação nessa área. Contudo a utilização da autenticação por palavra-chave e PIN continua

a ser o método de autenticação mais utilizado. Isto deve-se ao fato de serem mais simples e fáceis de implementar do que as técnicas baseadas em biometrias (Jansen, 2003).

A autenticação através de biometrias tem sido alvo de grande interesse por parte de académicos e profissionais da área de segurança de sistemas de informação (Costa, Obelheiro, & Fraga, 2006), sendo que este tipo de autenticação surge pela necessidade de melhorar e fortalecer a autenticação de dispositivos móveis (Clarke, 2004). Esta última característica deve-se ao fato de serem difíceis de furtar ou copiar, compartilhar ou modificar (Costa, Obelheiro, & Fraga, 2006).

2.2 Sistemas Biométricos

Um sistema biométrico pode testar se uma amostra pertence a um utilizador conhecido ou a um indivíduo desconhecido ao sistema. Na primeira situação, os sistemas são denominados de sistemas de identificação positiva e rejeitam o indivíduo que forneça uma amostra que não corresponda a uma das amostras guardadas. Na segunda hipótese os sistemas são denominados de sistemas de identificação negativa e rejeitam o indivíduo que forneça uma amostra que corresponda a uma das amostras guardadas. Deste modo, um sistema pode verificar se o indivíduo é quem clama ser ou verificar que realmente é desconhecido (Wayman, Jain, Maltoni , & Maio, 2005).

A utilização das biometrias para a autenticação de utilizadores pode ter duas finalidades. Uma das finalidades da autenticação é a de verificação, ou seja, determinar se um utilizador é realmente quem ele alega ser (Delac & Grgic, 2004). A verificação é normalmente utilizada para a identificação positiva. Para se efetuar a verificação o utilizador apresenta o elemento de autenticação, o qual vai ser comparado com o registo existente numa base de dados, previamente criada com todos os elementos de autenticação de cada um dos utilizadores envolvidos. Deste modo, a verificação é efetuada através da comparação de um-para-um. Com o resultado da comparação é possível verificar se a característica apresentada pelo utilizador corresponde realmente ao indivíduo que afirma ser (Jain, Ross, & Prabhakar, 2004).

A outra finalidade da autenticação biométrica é a identificação. Este tipo de operação permite determinar quem é o indivíduo (Clarke, 2004). Ou seja, responde à questão *"quem é o utilizador?".* Para se fazer a identificação do utilizador este apresenta o elemento de autenticação, que vai ser analisado e comparado com os elementos armazenados na base de dados. Ou seja, o sistema efetua a comparação de um-para-muitos. Segundo o autor de (Costa,

Obelheiro, & Fraga, 2006) no final da análise o sistema vai indicar a quem pertence aquela característica. Os autores de (Jain, Ross, & Prabhakar, 2004) dizem que o módulo de correspondências, é onde se efetua a comparação entre as características extraídas e os *templates* guardados, de forma a gerar *scores*. O resultado da identificação é uma lista dos indivíduos mais prováveis, ordenados segundo o *score* obtido na comparação.

Um sistema biométrico é constituído por quatro componentes: módulo sensor, módulo de extração de característica, módulo de correspondência e o módulo de tomada de decisão. (Delac & Grgic, 2004). Assim sendo, os sistemas que utilizam as biometrias como forma de autenticação são constituídos por quatro importantes fases. Estas são a captura, a extração de características, a comparação e a decisão. Na fase de captura obtém-se o elemento de autenticação, tipicamente sua representação digital. Na segunda etapa faz-se a extração da informação e caraterísticas únicas para um modelo (ou padrão), que é posteriormente guardado. Após a criação e armazenamento do modelo é então possível fazer a comparação entre este e a amostra apresentada no momento de autenticação. Por fim o sistema vai negar ou aceitar a autenticação de acordo com a concordância entre o modelo guardado e a amostra apresentada (Dedhia, 2011). A Figura 3 condensa as etapas atrás definidas, assim como o seu fluxo.

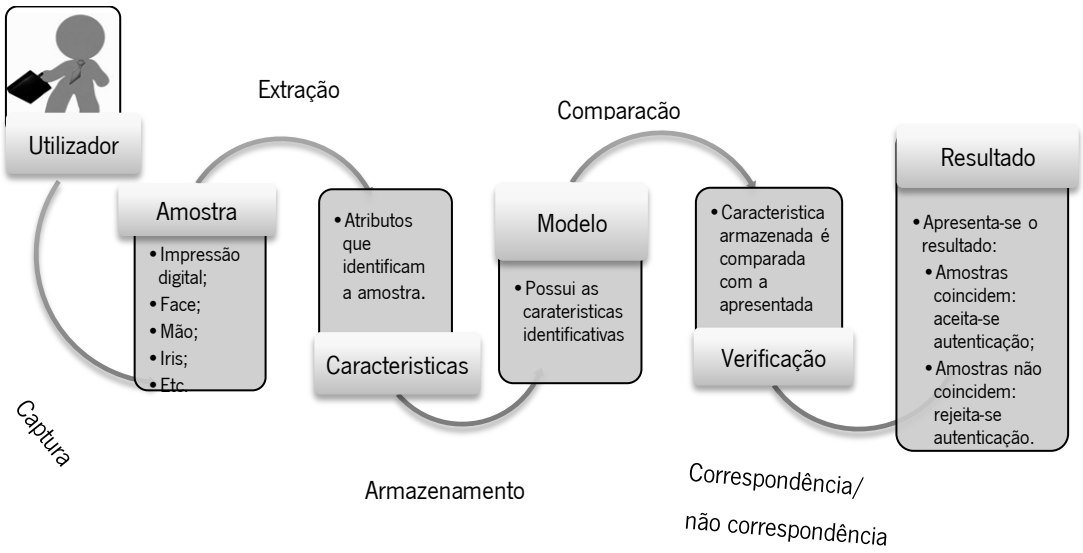

Figura 3 – Etapas de um sistema biométrico (adaptado de (Costa, Obelheiro, & Fraga, 2006))

Para se poder utilizar um elemento como biometria, é necessário que este obedeça a determinados critérios. Os critérios são a universalidade, unicidade, permanência, coleção e

aceitação. O primeiro significa que todos os indivíduos têm de possuir essa característica, ou seja, caso uma característica só esteja presente em certos indivíduos, não podemos utiliza-la como biometria. O critério de unicidade significa que essa característica deve ser única, ou seja, deve identificar unicamente um indivíduo. Por exemplo, não podemos usar a característica peso para diferenciar os indivíduos, uma vez que diversas pessoas podem pesar o mesmo. A permanência significa que a característica não se deve alterar ao logo do tempo, ou seja tem de ser imutável. Ainda para o exemplo anterior, o peso não pode mais uma vez ser considerado já que um indivíduo pode engordar ou emagrecer facilmente. É também necessário que a característica seja possível de medir, ou seja, que seja possível coletar os dados associados. Por fim temos a aceitação, ou seja o indivíduo deve ser capaz de tolerar a utilização da característica, para fins biométricos, naturalmente. Um outro aspeto que permite diferenciar as biometrias é o seu nível de intrusão. Por exemplo a identificação através da retina é mais desconfortável do que através da voz, pois diversos utilizadores sentem-se intimidados por ter de colocar o olho perto do dispositivo que irá captar a imagem da retina. Um exemplo que pode ser considerado ainda mais intrusivo é a utilização do ADN, pois caso seja necessário picar o indivíduo para obter sangue, tal é bastante desconfortável (Costa, Obelheiro, & Fraga, 2006).

Contudo, as biometrias não necessitam de obedecer a todos estes critérios. Na verdade, a maior parte das biometrias não cumpre na totalidade aquele conjunto de critérios. Por exemplo, a voz é um identificador único, mas que todavia não obedece plenamente ao critério de permanência, pois o estado de saúde pode influenciar a voz (Costa, Obelheiro, & Fraga, 2006).

2.3 Análise de desempenho

Por forma a avaliar a adequação de um sistema biométrico a uma dada aplicação é bastante útil dispor da sua avaliação em termos de desempenho. Um dos parâmetros do desempenho é a sua precisão, indicada através da verificação da taxa de Falsos Negativos (FRR), ou seja, a taxa dos indivíduos que possuem autorização e são rejeitados, e da taxa de Falsos Positivos (FAR), correspondendo à taxa dos que são autorizados erradamente (Dedhia, 2011). Estes indicadores variam de forma inversa, em função do ponto de decisão estabelecido como o limiar do resultado da comparação entre o padrão apresentado e o que se encontra armazenado, conforme se mostra na Figura 4. Devido a essa relação é vulgar identificar como indicador de

desempenho o ponto em que FRR = FAR, o qual é designado por EER (*Equal Error Rate*) – ver também a Figura 4

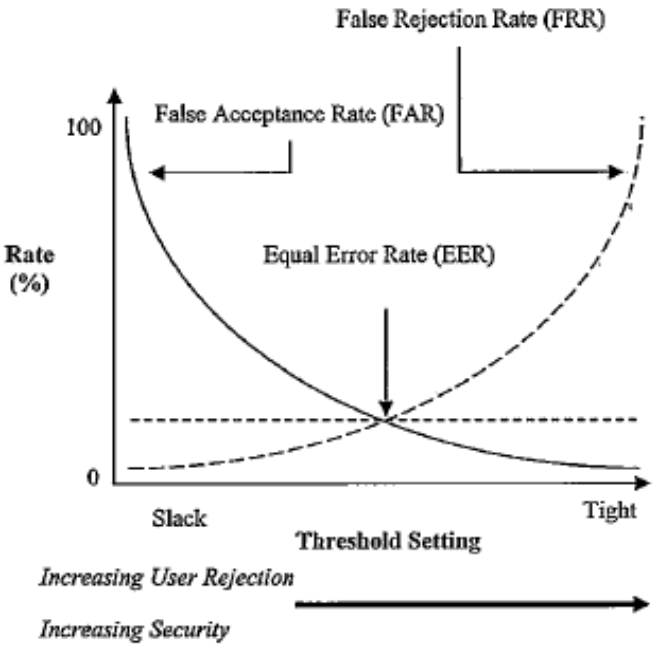

Figura 4 – Falsos Positivos e Falsos Negativos (Clarke, 2004)

Se o valor de limiar for escolhido para obter uma taxa baixa de Falsos Positivos, o sistema é mais seguro, pois é mais complicado para um impostor conseguir penetrar o sistema sem autorização, contudo tem a desvantagem de não permitir o acesso a utilizadores com autorização, uma vez que a taxa de Falsos Negativos é elevada. Pelo contrário caso tenha uma taxa de Falsos Positivos elevada, o sistema é mais vulnerável uma vez que permite o acesso a pessoas não autorizadas, mas será menos impeditivo para os utilizadores legítimos (Delac & Grgic, 2004).

Apesar dos sistemas em que a taxa de falsos positivos é grande não ser adequado a sistemas que requerem um elevado grau de segurança, estes podem ser utilizados em situações em que é necessário a identificação de um maior número de indivíduos. Um caso em que é adequado a utilização deste tipo de sistemas é a análise forense (Delac & Grgic, 2004).

Outra forma de avaliar o desempenho é o *Receiver Operating Characteristics* (ROC) – ver exemplo na Figura 5. Este é um gráfico que expressa a taxa de verdadeiros positivos contra a

taxa de falsos positivos. Deste gráfico é possível obter os valores de FRR, FAR e EER (Hempstalk, 2009).

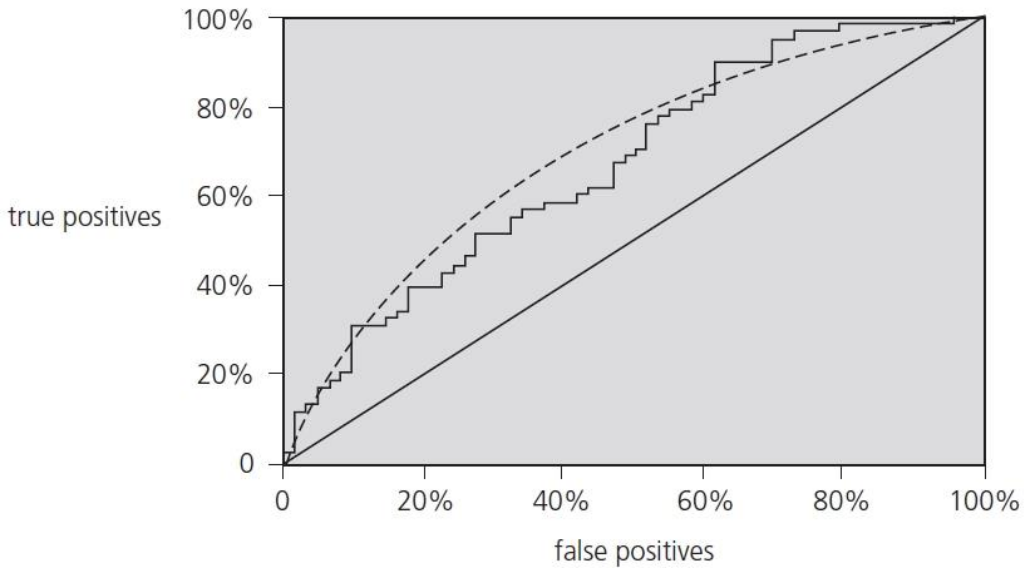

Figura 5 – Exemplo de uma curva ROC (Witten & Frank, 2005)

Segundo os autores de (Witten & Frank, 2005) a curva ROC quer-se o mais próximo possível do canto esquerdo. Ou seja quanto mais próxima se encontra do canto superior esquerdo melhor é a performance.

A taxa de TP e FP são consideradas como medidas de especificidade. Estas podem ser obtidas através das fórmulas:

$$Especificidade \rightarrow TP = \frac{TP}{TP + FN} \times 100\%$$

$$1 - Especificidade \rightarrow FP = \frac{FP}{FP + TN} \times 100\%$$

As curvas podem ser sintetizadas num valor, *area under de curve* (AUC). Este valor é independente de quaisquer limites que o algoritmo de classificação define. Quanto maior o valor de AUC melhor é o modelo (Hempstalk, 2009).

Outra medida de desempenho é a sensibilidade. Esta pode ser dividida em *recall* e precisão. A precisão é igual a divisão do número de documentos relevantes obtidos e o número total de

documentos obtidos. O *recall* é igual ao número de documentos relevantes obtidos a dividir pelo número total de documentos relevantes. Assim sendo podem ser calculados através das fórmulas (Witten & Frank, 2005):

$$Recall = \frac{TP}{TP + FN} \times 100\%$$

$$Precisão = \frac{TP}{TP + FP} \times 100\%$$

Uma forma de comparar os valores de *recall* e precisão é através da *F-measure.* O modelo é tanto melhor quanto maior o valor de *F-measure.* Este valor é calculado:

$$F - measure \ = 2(\frac{Precisão * Recall}{Precisão + Recall})$$

É ainda possível medir a performance do modelo através da sua assertividade. Ou seja, a percentagem de classificações corretas e incorretas. Estas taxas são determinadas através das fórmulas seguintes (Dean, 2014):

$$Corretas = \frac{TN + TP}{TP + FP + FN + TN} \times 100\%$$

$$Incorretas = (1 - \frac{TN + TP}{TP + FP + FN + TN}) \times 100\%$$

2.4 Análise de dados

- SVM

O *support vector machines* (SVM) é uma mistura de modelação linear (todas as equações são lineares) e aprendizagem baseada em instâncias. Nesta última, quando surge uma nova instância, esta é comparada ao conjunto de instâncias de treino memorizado, para encontrar a instância de treino que se assemelha mais à nova instância. Ao contrário dos modelos lineares simples, o SVM não representa limites lineares entre as classes, mas sim limites não lineares (Witten & Frank, 2005).

Segundo o autor de (Dean, 2014) o conceito básico SVMs é a habilidade de dividir os objetos em dois grupos diferentes, ou seja, encontrar limites entre duas classes. O SVM seleciona a linha de separação das classes tendo em conta a distância entre esta e as linhas paralelas a ela – linhas

de margem – ver Figura 6. Quanto maior a distância entre as linha de margem e a linha de separação melhor é o desempenho. Ou seja, quando uma nova instância é classificada, esta é feita tendo em conta o lado do hiperplano em que calha, logo se a distância da margem for maior há uma menor probabilidade de ser classificada erradamente.

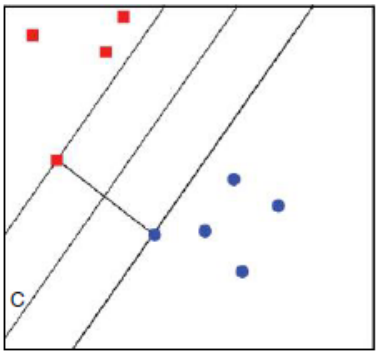

Figura 6 – Melhor linha de separação e linhas de margem (Dean, 2014)

Assim sendo o SVM seleciona vetores de suporte de cada classe e cria uma função que os separa de forma a atingir uma maior amplitude. Os vetores de suporte encontram-se dispostos ao longo das linhas de margem (Witten & Frank, 2005).

Apesar da ideia inicial de separação do SVM usar linhas, planos ou hiperplanos, estudos mais recentes usam *kernels* para o mapeamento dos dados num espaço dimensional maior. Os *kernels* mais utilizados são o polinomial, o gaussiano e o Sigmoide (Witten & Frank, 2005).

- PCA

O *principal componente analysis* ajuda na redução de dimensão, ou seja é um procedimento de redução de variáveis. Normalmente o PCA é utilizado em conjuntos de dados que possuem um valor elevado de variáveis. Com a utilização deste algoritmo os dados são tratados de forma a serem mais fáceis de analisar e compreender (Conway & White, 2012).

Os dados a serem analisadas podem ser visualizados como um conjunto de pontos num espaço de k dimensões. Este conjunto de pontos pode ser transformado noutro sistema de coordenadas, com isto o PCA tenta projetar os dados num plano que minimize o erro de projeção. Ou seja tenta encontrar uma direção – vetor – em qual a projeção dos dados produza um valor mínimo de erro de projeção (Witten & Frank, 2005).

2.5 Biometrias

As biometrias podem ser classificadas em duas categorias. Biometrias fisiológicas que dizem respeito às caraterísticas físicas do indivíduo, estas variam pouco longo do tempo (Costa, Obelheiro, & Fraga, 2006). Alguns exemplos deste tipo de biometria são as impressões digitais, reconhecimento facial, termograma facial, geometria da mão ou orelha, reconhecimento da iris ou da retina, o ADN, entre outras (Clarke, 2004). A outra categoria de biometrias são as comportamentais, estas são relativas ao comportamento do indivíduo. Estas são adquiridas ao longo do tempo, uma vez que vão sendo aprendidas ou desenvolvidas devido à sua constante utilização. Estas são consideradas dinâmicas uma vez que vão alterando ao longo do tempo tanto por vontade própria como pelo estado emocional do indivíduo (Costa, Obelheiro, & Fraga, 2006). Alguns exemplos de biometrias comportamentais são a forma como se escreve a assinatura, a voz, perfil de utilização de serviço, *Keystroke* ou *Gait* (Clarke, 2004).

2.5.1 Biometrias Físicas

- Impressão digital

Para se obter uma impressão digital é necessário capturar uma "imagem" desta através de um *scanner* próprio. Este possui um sensor, de onde vai ser extraído um padrão da impressão digital. Esse padrão vai ser armazenado para posterior reconhecimento. Para se autenticar um indivíduo efetua-se a comparação entre o padrão armazenado e o padrão obtido da impressão digital apresentada no momento de autenticação (Dedhia, 2011).

Esta é uma técnica que já é utilizada há muito tempo e, uma das primeiras situações em que se fez uso desta foi a identificação civil. Desde então esta tem sido aplicada a uma grande variedade de opções, como autenticação em telemóveis, computadores e PDAs (Clarke, 2004).

Apesar de a impressão ser singular e identificar unicamente o seu proprietário, as tecnologias biométricas associadas possuem diversas falhas, sendo considerada uma das técnicas biométricas menos fiáveis (Magalhães, 2005). A baixa fiabilidade desta técnica deve-se ao fato das impressões digitais poderem ser falsificadas e utilizadas sem o consentimento do proprietário. Com efeito é possível copiar uma impressão digital que se encontre gravada num objeto. Para além de se poder fazer uma falsificação é possível ainda utilizar o dedo do indivíduo contra a sua vontade, até mesmo de forma violenta. Para contrariar este efeito, os verificadores de impressões digitais têm sido melhorados através da adição de novas funcionalidades que

permitem verificar a temperatura, a tensão arterial, condutividade e ainda efetuar a leitura de padrões característicos a camadas inferiores da epiderme (Magalhães & Santos, 2003).

- Reconhecimento facial

Esta é uma técnica que permite reconhecer um indivíduo pela sua face. A aquisição da imagem da face pode ser feita de acordo com três tipos de abordagens, que são (ver também Figura 7): Imagem 2D, ou seja imagem digitalizada na forma de fotografia; Imagem 3D, em que imagens são tridimensionais e sequência de imagens, ou seja, imagens guardadas em vídeo (Costa, Obelheiro, & Fraga, 2006).

Figura 7 – Obtenção da imagem da face: 2D; 3D; Infravermelhos. Costa, et al., 2006

Após a obtenção da imagem da face são analisadas caraterísticas como a distância entre os olhos, largura do nariz, posição das bochechas, linha da mandibula, queixo, cor da pele, etc. Por fim efetua-se a ligação entre estas caraterísticas, tendo em atenção a posição e tamanho, de forma a delinear a face do indivíduo (Dedhia, 2011).

Esta tecnologia é largamente aceite pelo público, uma vez que a identificação através de fotografias é comum em documentos, não sendo necessário qualquer contacto para fazer a autenticação e os dispositivos que captam imagens não são dispendiosos (Costa, Obelheiro, & Fraga, 2006). Porém esta tecnologia apresenta diversos obstáculos, uma vez que é necessário ter em atenção aspetos como a iluminação, pose da face, a escala da imagem, idade das imagem ou a sua qualidade, o envelhecimento, existência de variantes como óculos, barba ou bigode (Dedhia, 2011).

- Termograma facial

Um termograma facial consiste na identificação dos padrões de calor da face, que são causados pelo fluxo de sangue inferior à pele. Para a obtenção do termograma são utilizadas radiações infravermelhas (Clarke, 2004).

Esta técnica pode ser considerada de caracter único, uma vez que cada indivíduo possui uma estrutura única de veias e tecidos. Contudo, está sujeita a diversos fatores que podem adulterar os resultados, como a temperatura do meio ambiente. Apesar disso tem vantagens em relação a outras técnicas, uma vez que não é influenciado por caraterísticas como a luz do dia, ou seja, tanto de noite como de dia (Clarke, 2004).

- Geometria da mão

Esta técnica é datada dos anos 60, e é considerada de simples utilização e não possui gastos elevados (Delac & Grgic, 2004).

Esta técnica captura as caraterísticas da mão, assim sendo é necessário ter em conta aspetos como o tamanho, largura, espessura e curvatura dos dedos, e a superfície da mão. Estas caraterísticas não são muito descritivas o que leva a uma taxa elevada de erros (Costa, Obelheiro, & Fraga, 2006). A geometria da mão não é considerada como uma característica única de um indivíduo, e assim sendo é aconselhável combinar esta técnica com outras para melhores resultados. Uma técnica que pode ser usada para melhorar o desempenho da geometria da mão é a impressão digital (Magalhães, 2009). Apesar de não ser considerada como muito distintiva esta técnica não é afetada por caraterísticas da pele, como por exemplo, se a pele é seca ou caraterísticas temporais (Delac & Grgic, 2004).

- Geometria da orelha

Para a obtenção da geometria da orelha são considerados os relevos e tamanho da orelha (Clarke, 2004), estas caraterísticas são selecionadas uma vez que são consideradas únicas de cada se humano (Dedhia, 2011).

Apesar de não ser uma técnica amplamente utilizada e implementada esta pode ser considerada como tecnologia com potencial, uma vez que as suas caraterísticas são robustas (Clarke, 2004).

- Reconhecimento da iris

A iris do olho é composta por caraterísticas únicas, dando origem a um padrão um padrão intrínseco de saliências, fissuras, veias, sardas, rugas, fendas e cores e que se revelam caraterísticas únicas e invariáveis, permitindo uma taxa de sucesso bastante elevada (Clarke, 2004). Para efetuar o reconhecimento da iris é necessário fazer uma análise à parte colorida do olho sendo esta tecnologia uma das mais apropriadas para a identificação dum indivíduo (Magalhães, 2009).

Para a obtenção da imagem da iris o indivíduo coloca o olho no foco duma câmara. Através da imagem obtida do olho, vai ser calculado a posição da iris (esta é calculada pela estimativa do centro da pupila), e isolada da pupila. Após este processo são extraídas as caraterísticas e armazenadas para posterior verificação ou identificação do sujeito (Costa, Obelheiro, & Fraga, 2006).

Apesar do elevado grau de precisão desta técnica, a iris não é uma superfície facilmente capturada, uma vez que é um alvo pequeno. Para além deste fato a iris encontra-se parcialmente obstruída, dado que se encontra por de trás das pálpebras, que por sua vez estão em constante movimento. Outros fatores para a sua obstrução são as lentes, óculos, dilatação da pupila e reflexos (Costa, Obelheiro, & Fraga, 2006).

Dado o grau de desconforto de captação desta biometria, diversos autores têm vindo explorar formas de melhorar o reconhecimento da iris em termos de robustez, assertividade e rapidez. Alguns dos estudos revelam uma melhoria significativa a nível de sensores. Este avanço permite um menor desconforto para os utilizadores, pois reconhecem a iris mais facilmente (George & Durai, 2013).

Esta tecnologia possui algumas funcionalidades e obstáculos ainda não resolvidos. Os dispositivos que efetuam o reconhecimento da iris ainda não possuem sensores que permitam identificar se é realmente um olho, existindo ainda alguns dispositivos que são ludibriados pela utilização de fotografias de alta qualidade. Assim esta técnica deve ser utilizada com a supervisão de outro indivíduo, pois assim é possível evitar aquela fraude. Outro método para a verificação da veracidade do olho é a utilização da alternação de luzes para verificar se a pupila dilata ou contrai (Dedhia, 2011).

- Reconhecimento da retina

A retina é constituída por veias na parte de trás do olho. Estas veias constituem um padrão único que permite identificar o indivíduo. Esta técnica é muito similar ao reconhecimento de iris, uma vez que a imagem é obtida através de uma fonte de luz de baixa intensidade (Magalhães, 2009)

Esta técnica proporciona algum desconforto aos utilizadores, uma vez que para se captar a imagem da retina é necessário colocar o olho muito próximo da câmara (Clarke, 2004), e existe a necessidade de olhar para dentro de um recetáculo e focar um ponto específico (Magalhães, 2009).

Devido às suas inconveniências para os utilizadores e o seu elevado grau de precisão esta técnica tem sido apenas usada em edifícios e instalações onde são necessários elevados níveis de segurança (Clarke, 2004). Outro motivo para a pouca disseminação desta técnica é o fato de que até relativamente pouco tempo esta tecnologia era de difícil implementação, pois os equipamentos necessários para obter o padrão da retina são de custo elevado (Magalhães, 2009).

2.5.2 Biometrias Comportamentais

- Keystroke

A forma como um indivíduo digita num teclado tem propriedades únicas permitindo assim identificar um utilizador (Clarke, 2004).

Para fazer a identificação do utilizador é efetuada uma monotorização das suas ações enquanto escreve uma frase ou palavras num determinado tempo (Magalhães, 2009). Esta verificação pode ser efetuada de duas formas, de forma estática, ou seja, é dependente do texto ou pode ser efetuada de forma dinâmica, em que o texto é independente (Clarke, 2004).

A identificação do padrão de escrita dum indivíduo tem em conta medidas como o tempo de espera, ou seja, o tempo durante o qual a tecla é pressionada, e o tempo de "voo" ou latência entre teclas, ou seja, o tempo que o utilizador demora a passar de uma teca para outra. O tempo que um utilizador demora a encontrar uma determinada letra pode ser superior ou inferior ao tempo que outro indivíduo demora a encontrar a mesma letra havendo ainda diferença entre o tempo que um utilizador demora a transitar entre letras deferente. Assim sendo e num caso muito simples, pode-se verificar se um utilizador é o autorizado ou se é um impostor

através do tempo que escreve uma frase – se o utilizador demorar sessenta segundos a escrever uma frase com dez palavras e o impostor demorar quarenta segundos a escrever a mesma frase (Dedhia, 2011).

Inicialmente o utilizador escreve uma frase repetitivamente, até que o sistema possua suficiente informação para encontrar o padrão de escrita do utilizador (Magalhães, 2009). A forma mais comum de autenticação através desta técnica é a medição da entrada da palavra-chave e nome de utilizador. Após inserção destas palavras, os tempos associados são sujeitos a um algoritmo que vai efetuar a comparação entre as caraterísticas dos dados inseridos no momento atual e as caraterísticas guardadas previamente na base de dados (Dedhia, 2011). Estes algoritmos recorrem normalmente a métodos como as redes neuronais, estatísticas e probabilidades (Magalhães, 2009).

Este tipo de biometria possui algumas vantagens relativamente a outras, pois normalmente faz a combinação da utilização de palavra-chave e PIN, não necessita de nenhum dispositivo especial para a obtenção da biometria (apenas necessita dum teclado, que normalmente já vem incluído no dispositivo) e permite ainda a autenticação de uma forma continua (Ferreira & Santos, 2012).

Contudo um utilizador pode não escrever sempre da mesma forma, o que pode levar a rejeição deste por parte do sistema (Dedhia, 2011).

- Reconhecimento da assinatura

A assinatura pode ser considerada *off-line,* ou seja estática ou *on-line,* ou seja dinâmica. O primeiro tipo de assinatura é aquela que é apresentada num documento e posteriormente captada, quer por câmara ou *scanner.* A assinatura dinâmica e obtida através de um dispositivo próprio para esta finalidade (Costa, Obelheiro, & Fraga, 2006). Para o reconhecimento da assinatura são tidos em conta aspetos como a velocidade, força e pressão aplicada nos traços da assinatura, o formato da letra e as condições a que o indivíduo se encontrava sujeito no momento de assinatura. Características como a velocidade, pressão e tempo dificultam a falsificação da assinatura (Dedhia, 2011).

Apesar de este tipo de autenticação ser bastante apoiada pelo público - é aceite como método de verificação em transações governamentais, legais e comerciais-, esta não é uma técnica muito eficiente, pois sofre alterações ao longo do tempo e é influenciada por condições físicas e emocionais (Jain, Ross, & Prabhakar, 2004).

- Verificação da voz

Esta biometria permite fazer a verificação ou identificação dum indivíduo através da sua voz, que contém um conjunto único de características. A voz pode ser considerada dessa forma uma vez que esta depende das atividades, comportamento e caraterísticas físicas do indivíduo (Magalhães, 2009).

Para se obter um padrão biométrico da voz é necessário um microfone com um *software* apropriado (Dedhia, 2011). A voz pode ser representada por um espectro de frequências e amplitude (Magalhães, 2009).

A autenticação dos utilizadores por voz pode ser classificada consoante o tipo de protocolo que segue. Deste modo a autenticação pode ser feita através de texto fixo, ou seja, é inicialmente guardado o padrão biométrico baseado numa determinada frase e para se proceder a autenticação o utilizador vai ter de pronunciar essa mesma frase. Podemos ainda considerar o protocolo dependente do texto, em que são inicialmente gravados os padrões biométricos de uma serie de frases, podendo o sistema selecionar qualquer uma delas em determinada altura. No protocolo independe de texto, o utilizador não tem que dizer nenhuma frase previamente especificada, podendo pronunciar uma frase a seu desejo, da qual serão extraídas características únicas e que serão comparadas de uma forma semelhante. Por fim existe o protocolo conversacional, em que o utilizador vai responder ao sistema, que lhe coloca um conjunto de questões previamente estabelecidas (Costa, Obelheiro, & Fraga, 2006).

A autenticação através da voz pode ser considerada como acessível uma vez que faz uso de dispositivos baratos e pode ser facilmente implementada uma vez que pode ser desenvolvida utilizando a rede telefónica (Costa, Obelheiro, & Fraga, 2006). Outra vantagem desta tecnologia é que a maior parte dos dispositivos atuais já vêm equipados com microfone, tornando-se mais fácil aplicar esta tecnologia (Magalhães, 2009).

Apesar da facilidade de aplicação desta tecnologia e do seu reduzido grau de investimento esta tecnologia tem algumas desvantagens como seja a facilidade de imitações, utilização de gravações, utilização de sistemas treinados para imitar a voz, interferência devido aos sons do ambiente envolvente, e ainda alterações da voz devido ao estado de saúde, emoções, pressa, sono, preguiça e outros fatores do utilizador (Costa, Obelheiro, & Fraga, 2006).

- Perfil de utilização de serviço

Esta biometria permite fazer a autenticação dos utilizadores através das suas interações com as aplicações ou serviços. As aplicações que um utilizador usa, como as usa e por quanto tempo as usa, são fatores que permitem identificar o utilizador. Contudo, estas caraterísticas de utilização não são suficientemente distintivas para sistemas de identificação. Apesar de esta técnica não interferir com o utilizador e permitir a autenticação contínua, pode trazer alguns problemas de segurança, como por exemplo a captura de palavras-chave (Clarke, 2004)

Devido às suas fracas capacidades para a autenticação e ao perfil de utilização de aplicações em dispositivos móveis, esta é uma técnica que não se encontra em utilização para sistemas deste género. Contudo, esta técnica é de interessante utilização em contexto organizacional, pois permite ajudar na proteção contra fraude (Clarke, 2004).

- Gait

A autenticação que usa a forma de andar de um indivíduo como biometria é denominada por *Gait.* O estilo de andar de um indivíduo é uma característica individual, sendo este difícil de copiar por outros indivíduos (Mäntyjärvi, Lindholm, Vildjiounaite, Mäkelä, & Ailisto, 2005). Entre as características que é possível medir encontra-se a amplitude do passo, a velocidade de deslocação, a variação na altura e ainda a oscilação dos braços (Magalhães, 2009).

Para se obter o padrão biométrico de um indivíduo é necessário verificar as diferentes atividades em que um indivíduo se encontra, sendo necessário distinguir quando caminha, corre, sobe ou desce uma inclinação ou escadas (Mäntyjärvi, Lindholm, Vildjiounaite, Mäkelä, & Ailisto, 2005).

Desde o ano de 2005 que os desenvolvimentos desta técnica têm sido relacionados com sensores de aceleração, frequentemente disponíveis em dispositivos moveis. Esta é uma técnica não intrusiva, que permite ultrapassar diversos problemas característicos de outras formas de autenticação biométricos. Contudo esta técnica possui desvantagens, sendo uma delas a alteração das características do padrão de andar ao longo da vida de um indivíduo (Hu, Tao, Xiaopeng, & Yu, 2012).

- *Mouse dynamics*

A técnica *Mouse dynamics* tem como base o estudo dos movimentos efetuados com o rato, ou seja, arrastar e largar um objeto e que no seu conjunto permitem obter caraterísticas comportamentais do utilizador (Traore, Woungang, S. , Nakkabi, & Lai, 2013) e (Agrawal, 2012).

Algumas das caraterísticas extraídas e analisadas são a distância, ângulo, velocidade e direção entre diferentes pontos (Meng, Wong, Schlegel, & Kwok, 2012).

Apesar de esta técnica analisar o comportamento do utilizador, esta não é a mais adequada para a autenticação em dispositivos móveis, uma vez que estes normalmente não possuem rato como *input.* Deste modo é uma técnica mais apropriada para a autenticação em dispositivos que possuam rato (Meng, Wong, Schlegel, & Kwok, 2012).

- *Touch dynamics*

Touch dynamics é uma técnica que permite identificar os utilizadores através da análise dos *inputs* que o utilizador efetua num dispositivo *Touch-screen* (Meng, Wong, Schlegel, & Kwok, 2012). Ou seja, selecionando e analisando a interação com o dispositivo, é possível determinar os comportamentos específicos de um utilizador, como por exemplo se este só usa uma mão para lidar com o dispositivo ou as duas, se é esquerdino ou direito, entre outros (Sandnes & Zhang, 2012).

Segundo (Zheng, Bai, Huang, & Wang, 2012) cada utilizador possui um padrão de utilização. Uma vez que este depende da forma da mão e da agilidade, cada indivíduo efetua movimentos no dispositivo com velocidades ou ritmos diferentes, com mais ou menos força ou seja mais ou menos pressão contra o ecrã e diferentes ângulos.

A informação obtida da interação com o ecrã do dispositivo depende também dos comportamentos de utilização e do contexto das aplicações. Assim sendo a forma como o utilizador segura no dispositivo (com a mão direita ou esquerda), os padrões de mobilidade (se se encontra parado ou a andar), o tempo e localização (no trabalho ou em casa) e a aplicação a ser utilizada (email, SMS, GPS) são variáveis que influenciam a velocidade, pressão, tamanho e direção do toque (Feng, Yang, & Yan, 2014).

As interações efetuadas pelos utilizadores podem ser divididas em quatro categorias, que são: toque único, toque de movimento, toque múltiplo e sem interação. Na primeira categoria o toque começa com a pressão dedo no ecrã e finaliza com o levantar do dedo, não tendo nenhum movimento entre estes dois eventos. Na segunda categoria, existe a pressão do dedo no ecrã seguido de um movimento e finaliza com o levantar do dedo. Na terceira categoria ao iniciar o contato com o ecrã deteta-se mais do que uma coordenada, ou seja, mais do que um dedo, e o toque pode ser com ou sem movimento consequente (Meng, Wong, Schlegel, & Kwok, 2012).

Deste modo um sistema de autenticação que utiliza a técnica de *Touch dynamics*, efetua a extração das caraterísticas das interações e verifica se o utilizador é o dono do dispositivo ou um impostor (Bo, Zhang, & Li, 2013).

- Outras técnicas

A investigação nesta área encontra-se constantemente em busca de novas formas de autenticação e de melhorar a segurança e a autenticação, em particular. Existem mais técnicas biométricas em estudo, podendo-se citar técnicas como a verificação dos padrões das veias, ADN, análise dos poros num dedo, reconhecimento de imagens (o ser humano tem mais facilidade de memorizar imagens que sequências alfanuméricas), o odor emitido e ainda a análise das unhas (Dedhia, 2011).

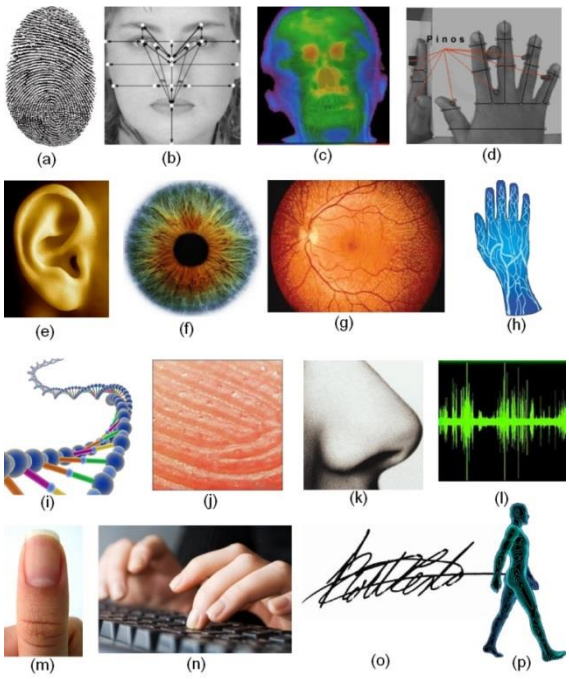

Figura 8 – Biometrias Físicas: (a) impressão digital; (b) reconhecimento facial; (c) termograma; (d) geometria da mão; (e) geometria da orelha; (f) reconhecimento da iris; (g) reconhecimento da retina; (h) padrão das veias; (i) ADN; (j) poros da pele; (k) odor; (l) reconhecimento da voz; (m) unha; (n) keystroke; (o) reconhecimento da assinatura; (p) gait (adaptado de (Nandakumar, 2005))

2.5.3 Comparação entre Biometrias

As biometrias podem ou não existir em todos os indivíduos a autenticar (exemplo: impressão digital não encontra presente em determinados indivíduos), ou possuir mais ou menos caraterísticas que permitem identificar um indivíduo unicamente. Algumas são imutáveis outras

sofrem alterações, algumas são mais fáceis de medir, outras são mais precisas e rápidas na obtenção de resultados. Existem ainda biometrias que não são tão bem aceites pelos indivíduos e podem ser ludibriadas. Deste modo as biometrias apresentadas podem ser comparadas em termos de universalidade, distinção, permanência, medição, desempenho, aceitação e evasão.

Na Tabela 1 pode ser verificado que as técnicas que são mais facilmente contornadas, ou seja, são mais facilmente falsificadas por impostores são as tecnologias que fazem o reconhecimento da face, da assinatura e da voz. Podemos ainda constatar que apesar das técnicas relativas ao ADN, iris e retina serem as técnicas mais difíceis de contornar, que permitem fazer uma melhor distinção e ter um melhor desempenho, estas são também as técnicas mais difíceis de aceitar pelos indivíduos. Isto deve-se ao fato destas serem mais desconfortáveis e intrusivas.

Tabela 1 – Comparação Biometrias. E-Elevado; M-Médio; B-Baixo (Delac & Grgic, 2004)

Identificador Biométrico	Universalidade	Distinção	Permanência	Medição	Desempenho	Aceitação	Evasão
ADN	E	E	E	B	E	B	B
Orelha	M	M	E	M	M	E	M
Face	E	B	M	E	B	E	E
Termograma Facial	E	E	B	E	M	E	B
Impressão digital	M	E	E	M	E	M	M
Gait	M	B	B	E	B	E	M
Geometria da Mão	M	M	M	E	M	M	M
Veias da mão	M	M	M	M	M	M	B
Iris	E	E	E	M	E	B	B
Keystroke	B	B	B	M	B	M	M
Odor	E	E	E	B	B	M	B
Palma da Mão	M	E	E	M	E	M	M
Retina	E	E	M	B	E	B	B
Assinatura	B	B	B	E	B	E	E
Voz	M	B	B	M	B	E	E

Assim pode ser constatado que as técnicas devem ser selecionadas consoante as caraterísticas que são mais adequadas à situação e aos resultados esperados. Ou seja, uma técnica com um elevado desempenho deve ser usada em situações critica e de elevada importância. Por exemplo as técnicas de ADN, iris e retina devem ser usadas em situações de elevada segurança (prisões, bancos, etc), pois são muito precisas. Contudo estas não são as mais adequadas para a identificação de um utilizador num dispositivo móvel, pois são intrusivas e não permite a autenticação contínua.

2.5.4 Comparação entre *keystroke, mouse* e *touch dynamics*

Apesar das técnicas *keystroke, mouse* e *touch dynamics* efetuarem a identificação do utilizador através dos padrões comportamentais, estas possuem diversas semelhanças e diferenças.

Uma das diferenças entre estas três técnicas é o tipo de *input* a que recorrem. Enquanto no *touch dynamics* é possível ter em conta o toque múltiplo e movimento, no *mouse dynamics* só é utilizado o movimento; já o *keystroke dynamics* não permite nenhum destes *inputs,* permitindo apenas *inputs* através de teclas. *Touch dynamics* pode ser descontínuo, ou seja, o movimento não tem de necessariamente que começar no ponto onde finalizou. Isto significa que um utilizador pode iniciar um novo movimento a partir de uma posição aleatória, e desconectado do movimento anterior. O que não acontece no *mouse dynamics*, uma vez que o movimento inicia-se na última posição do rato, ou seja, um movimento é continuado (Meng, Wong, Schlegel, & Kwok, 2012). Outra diferença entre mouse e *touch dynamics,* é que neste último caso não existe um ponteiro visível, ou seja, o movimento de uma posição para outra é invisível ao ecrã, o que não acontece no *mouse dynamics*, uma vez que este possui um movimento continuo. Um movimento contínuo pode ser considerado aleatório, pois nem sempre possuí uma finalidade – um exemplo é o deslocamento do ponteiro para outra posição, sem que se efetue um pedido (clicar) (Frank, Biedert, Ma, Martinovic, & Song, 2013).

Contudo, estas três técnicas evidenciam algumas semelhanças. No *touch dynamic*s pode-se comparar o pressionar e o levantar do dedo do ecrã com o pressionar e levantar o dedo das teclas no *Keystroke dynamics* e com o clique do botão do rato no *mouse dynamics* (Meng, Wong, Schlegel, & Kwok, 2012). As variáveis distância, velocidade e direção podem ser estudadas no *touch e mouse dynamics*, uma vez que ambas as técnicas possuem movimento como *input* (Sandnes & Zhang, 2012).

Desta breve comparação pode-se afirmar que a técnica *touch dynamics* possui um maior número de variáveis relativamente às outras duas técnicas, e engloba algumas das suas interações principais. Deste modo, permite a análise de um maior número de caraterísticas que as outras técnicas, ou seja, permite a análise de mais caraterísticas comportamentais.

2.5.5 Aplicações das técnicas biométricas

A segurança é uma área que tem vindo a ter cada vez mais importância, tanto para organizações como para indivíduos. Portanto torna-se essencial desenvolver tecnologias que permitam satisfazer as necessidades de segurança do público.

Anteriormente foi feita uma descrição de algumas das técnicas que permitem fazer a autenticação de um indivíduo por forma a barrar ou permitir o acesso.

Algumas das utilizações de segurança que as biometrias têm tido ao longo dos tempos são na prevenção por parte de indivíduos não autorizados às caixas automáticas, telemóveis, computadores, transações de negócio através da internet ou telecomunicações. Assim sendo as áreas de utilização deste tipo de tecnologia são os bancos, o acesso a edifícios, serviços eletrónicos, controlo de bordo, segurança dos aeroportos e ciberespaço, acesso ao banco através do telefone, sistemas de monitorização dos visitantes à prisão e sistemas de votação (Dedhia, 2011).

2.6 Touch-Screen

2.6.1 Interações Touch-Screen

Ao longo dos tempos os dispositivos móveis têm evoluído de forma a serem mais fáceis e mais rápidos de utilizar. Com isto em mente desenvolveu-se a funcionalidade de *Touch-Screen.* Apesar de esta ter surgido na época de 1070s, só nos últimos anos é que esta tomou um maior relevo e importância no mercado (Kolly, Wattenhofer, & Welten, 2012).

Touch-Screen passou a ser usado em telemóveis, computadores, PDAs e outros dispositivos móveis. Como foi referido anteriormente, estes dispositivos permitem o acesso a informação de grande sensibilidade. Deste modo existe a necessidade de criar métodos de autenticação que ofereçam um nível de segurança superior à proporcionada pelos métodos convencionais -

palavras-chave, PINs e *tokens.* É neste contexto que surgem os métodos baseados em biometrias comportamentais (Clarke, 2004).

Os dispositivos móveis com *Touch-Screen* são adequados à utilização de técnicas que recorrem às biometrias comportamentais. Isto deve-se ao facto dos dispositivos possuírem o *Hardware* adequado para o reconhecimento dos identificadores biométricos. Ou seja, os dispositivos já vêm incorporados de sensores que permitem captar indicadores biométricos (Bo, Zhang, & Li, 2013).

Deste modo vão ser descritas algumas das interações entre o indivíduo e o dispositivo, que podem ser usadas nas biometrias comportamentais. Estas são a posição, a pressão, a velocidade e direção de deslocamento.

Como poderá ser constatado estas interações com o ecrã dos dispositivos móveis são específicas de cada indivíduo. Ou seja, são variáveis que permitem criar um padrão biométrico dos movimentos do indivíduo, e assim permitir a autenticação através do padrão biométrico.

- Posição

Segundo o Kolly et al (2012) a deslocação da posição inicial do objeto em contato com o ecrã para uma posição seguinte poderá ser considerada como singular de um indivíduo. Assim a posição dos toques que o utilizador efetua no ecrã são determinantes para a sua identificação. O utilizador do dispositivo possui pontos do ecrã que toca mais, por exemplo um utilizador que use muito o telemóvel para enviar mensagens clica muitas vezes no botão para as mensagens. Assim sendo a posição permite determinar as ações decorridas durante o dia (Kolly, Wattenhofer, & Welten, 2012).

- Pressão

A pressão que um utilizador aplica não é conscientemente medida, o que permite considerar a pressão como uma característica exclusiva a cada indivíduo (Kolly, Wattenhofer, & Welten, 2012). A pressão é uma característica que pode ser medida nos dispositivos móveis, pois sempre que utilizador toca no ecrã do dispositivo, este aplica uma determinada pressão (Kolly, Wattenhofer, & Welten, 2012).

A pressão é uma característica importante para a segurança. Por exemplo na técnica de *Look Pattern* (técnica em que o utilizador efetua um padrão para bloquear o ecrã do dispositivo), é facilmente roubado o padrão desenhado, quer por marcas de gordura no ecrã como através de câmaras. Assim se se acrescentar a medição da pressão a esta técnica é mais complicado para

um impostor conseguir aceder ao dispositivo, pois apesar de saber o padrão que deve efetuar este não sabe que pressão a aplicar (Angulo & Wästlund, 2012).

- Velocidade e direção de deslocamento

A velocidade que um utilizador aplica para efetuar um movimento é uma forma de identificação, pois indivíduos diferentes demoram tempos distintos para percorrer a mesma distância. Assim sendo a velocidade pode ser usada em métodos de autenticação. Ao combinar a velocidade e a técnica de *Look Pattern*, existe uma melhoria de segurança pois, apesar de um impostor conseguir o padrão do *Look Pattern*, este muito dificilmente conseguirá copiar a velocidade de deslocamento que o indivíduo aplica para desenhar o padrão (Angulo & Wästlund, 2012).

Segundo Kolly et al (2012) os indivíduos possuem um padrão mental individual bastante fixo da direção tanto horizontal como vertical. Assim sendo um indivíduo pode ser caracterizado por movimentos mais horizontais ou verticais.

2.6.2 Obstáculos Touch-Screen

Apesar da funcionalidade de *Touch-Screen* trazer o benefício de uma interação direta do utilizador com o dispositivo, e consequentemente uma maior facilidade de interação, esta tecnologia necessita ultrapassar diversas limitações. Uma delas é a oclusão. Outra é o problema do dedo "gordo", ou seja, *"Fat Finger*" (Wigdor, Forlines, Baudisch, Barnwell, & Shen, 2007). E ainda o problema do *smudge.* Estas limitações são descritas a seguir:

- Oclusão

Um dos problemas que é característico da interação táctil com o ecrã dos dispositivos é a oclusão. Quando um indivíduo tenta tocar num ponto específico do ecrã, este pode ser ocultado pelo dedo do indivíduo. Este fenómeno ocorre mais frequentemente em dispositivos pequenos, pois em muito dos casos a mão é maior do que o dispositivo, fazendo assim a obstrução da posição que se deseja guardar (Wigdor, Forlines, Baudisch, Barnwell, & Shen, 2007).

- *Fat Finger*

O problema do dedo "gordo", é que na maioria das vezes a área que se pretende tocar é demasiado pequena. Sendo que o dedo do indivíduo é muitas vezes superior que um pixel do ecrã (Wigdor, Forlines, Baudisch, Barnwell, & Shen, 2007). Ou seja, por vezes o utilizador pretende tocar num ponto específico, mas seleciona uma área diferente daquela que deseja

realmente (Bi, Li, & Zhai, 2013). Dada a imprecisão do toque no ecrã torna-se necessário desenvolver técnicas que permitam a máxima precisão.

- *Smudge*

Outro dos problemas que afeta a autenticação em dispositivos *Touch-Screen* é fato de se deixarem resíduos no visor do dispositivo. Os *smudges*, ou resíduos gordurosos, são marcados no visor com a repetição de técnicas como o *lock pattern.* Os resíduos marcados no visor do dispositivo podem ser analisados e assim fornecer os padrões de autenticação (Aviv, Gibson, Mossop, Blaze, & Smith, 2010). Deste modo técnicas que recorram à repetição de padrões no ecrã ficam sujeitas a ataques, pois estas deixam marcas gordurosas no visor que são fáceis de copiar por impostores.

2.6.3 Técnicas Baseadas em Biometrias Comportamentais para *Touch-Screen*

As biometrias comportamentais têm sido alvo de estudo e exploração por parte de diversos autores, isto com o intuito de desenvolver técnicas seguras de autenticação para os dispositivos móveis.

As biometrias podem ser utilizadas de forma implícita e contínua para autenticar os utilizadores, ou seja, é efetuada a autenticação periódica do utilizador de forma não intrusiva (sem que este se aperceba) (De Luca, Hang, Brudy, & Hussmann, 2012). Três técnicas que permitem efetuar a autenticação do utilizador de forma implícita e contínua são *Mouse Dynamics*, *Keystroke Dynamics* e Touch Dynamics. Contudo a técnica *Mouse Dynamics* apenas foi explorada no contexto de Computadores (Meng, Wong, Schlegel, & Kwok, 2012).

Das técnicas expostas a que toma um maior relevo para a autenticação de dispositivos *Touch-Screen* é a técnica *Touch Dynamics,* uma vez que esta permite obter informação sobre os toques efetuados no dispositivo.

Diversos autores exploraram as interações com os dispositivos *Touch-Screen*, tais como a pressão, posição, velocidade e direção de deslocamento, com objetivo de verificar a sua eficácia na identificação dos utilizadores. Ou seja, se estas interações e comportamentos permitem autenticar os utilizadores de forma única e exata.

Em 2004 foi apresentado por Varenhorst um sistema de autenticação com base no reconhecimento de *doodles* (traços efetuados com os dedos). Para testar o sistema foi

requisitado a 10 indivíduos que desenhassem um traço com o dedo no dispositivo e efetuassem a sua réplica diversas vezes, o mais semelhante possível. Isto para a sua posterior conversão para uma grelha de distribuição e armazenamento.

Para testar a fiabilidade do sistema foram selecionados três componentes diferentes, a grelha de distribuição, a velocidade instantânea e o ponto de variância na grelha de distribuição. Estes componentes permitiram a comparação do traço inserido para autenticação e o traço guardado anteriormente. Destes componentes, a velocidade instantânea foi aquela que atingiu um menor número de comparações corretas, atingindo apenas 57.1% de resultados corretos. Este baixo desempenho deve-se ao fato de alguns utilizadores terem uma grande variância de velocidade no desenho do traço. Os outros dois componentes de avaliação atingiram níveis de comparação mais satisfatórios, 97.1% e 95.7%. Apesar destes componentes serem independentes matematicamente, o autor acredita na possibilidade de não o serem verdadeiramente, o que torna a sua utilização desnecessária. A utilização dos três componentes em simultâneo proporciona uma assertividade de 98.5%.

Com este trabalho o autor demonstrou a viabilidade de utilização de *doodles* para a autenticação, oferecendo novas perspetivas para a autenticação em dispositivos *Touch,* como o reconhecimento da escrita, ou a elaboração de um desenho, ou seja, palavras-chave gráficas. Segundo (Sun, Li, Jiang, & Kot, 2008) as palavras-chave são mais fáceis de memorizar, contudo no estudo (PassShapes - Utilizing Stroke Based Authentication to Increase Password Memorability, 2008) os autores demonstram que é necessário efetuar a repetição da palavra-chave gráfica para aumentar a memorização.

Este tipo de autenticação pode ser dividido em 3 classes, *locimetric, cognometric e drawmetric*. *Locimetric* refere-se a sistemas de autenticação em que o utilizador deve selecionar uma sequência de regiões de uma imagem de forma a construir uma palavra-chave. Os sistemas baseados em palavras-chave *cognometric* efetuam a autenticação através da seleção de imagens. Inicialmente o utilizador seleciona um grupo de imagens que vão constituir o seu portefólio, aquando da autenticação são expostas imagens do portefólio e imagens escolhidas aleatoriamente, o utilizador deve escolher todas as imagens que fazem parte do seu portfólio para efetuar a autenticação. A autenticação efetuada através de palavras-chave *drawmetric* consiste na execução de uma forma previamente selecionada, ou seja, o utilizador deve desenhar uma figura para se autenticar (Weiss & Luca, 2008).

Os autores Saevanee & Bhattarakosol (2009) efetuaram uma experiência em que os utilizadores deveriam digitar um número com 10 algarismos cerca de 30 vezes seguidas. Para analisar o comportamento do utilizador, foi utilizada técnica *Keystroke Dynamics* e Pressão do dedo. Assim foram memorizadas três variáveis, a pressão que o utilizador aplica quando pressiona um algarismo, o tempo que demora num algarismo e entre dois algarismos. Com base nesta experiência os autores defendem que a pressão que o utilizador aplica e o tempo que pressiona identificam o utilizador com uma precisão de 99%. A pressão, usada individualmente, identifica o utilizador com 99% de precisão. Com combinação dos três indicadores obtém-se 90% de precisão. O indicador que possui uma percentagem mais baixa de assertividade é o tempo entre algarismos.

Em Berlim, 2009, foi iniciada uma experiência pelos autores (Dörflinger, Voth, Krämer , & Fromm) com o intuito de analisar os níveis de segurança, tecnologias de autenticação e verificar o seu impacto nos utilizadores. Para isto os autores conduziram quatro grupos de foco, ou seja, moderaram debates em grupo. Na experiência participaram 19 indivíduos. Na primeira parte da experiência foi questionada a importâncias dos dispositivos moveis no dia-a-dia e a necessidade de métodos de segurança para as aplicações usadas. Na segunda etapa os utilizadores debateram sobre os métodos de autenticação que ouviram falar ou usaram, para além do método convencional PIN. Na terceira parte, os participantes lidaram com oito métodos de autenticação diferentes. As tecnologias que exploraram foram a autenticação por impressão digital, reconhecimento da retina ou iris, reconhecimento da voz, reconhecimento facial, reconhecimento de gestos 3D (em que os gestos são reconhecidos através de sensores de movimento), verificação baseada na atividade (autenticação baseada em palavra-chave e ritmo, velocidade e pressão do toque), reconhecimento de gestos 2D (técnica *drawmetric* com as propriedades de velocidade e pressão para desenhar), e autenticação baseada no reconhecimento (ou seja *Locimetric*). Dos métodos apresentados, a autenticação por impressão digital foi a que obteve uma melhor resposta para utilização diária por parte dos utilizadores, já as técnicas de reconhecimento de voz, retina e face tiveram uma resposta mais negativa. Com a experiência, os autores confirmaram que apesar dos participantes verificarem que algumas técnicas oferecem um maior grau de segurança, estas não são a sua primeira escolha. Isto deve-se ao facto dos métodos serem muito intrusivos ou provocarem algum embaraço.

Para além da experiência em laboratório, elaboraram também um inquérito na web a 308 indivíduos, sendo que 77 eram alemães e 231 eram israelitas. Da análise efetuada, verificou-se que a identificação da impressão digital foi a técnica selecionada como método mais seguro.

A técnica de autenticação de palavra-chave gráfica foi também explorada pelos autores de (Chang, Tsai, & Lin, 2012), contudo estes adicionaram os indicadores de pressão e tempo do toque. Com o indicador de pressão foi possível verificar um decréscimo da percentagem de impostores autenticados e a rejeição de utilizadores autorizados. Na experiência participaram cem indivíduos fluentes na utilização de dispositivos *Touch-Screen*. Estes foram requisitados para selecionar a imagem preferida dentro de um grupo de imagens. A imagem selecionada é posteriormente dividida em 30 partes de igual dimensão. Após este processo o participante constrói a sua palavra-chave através da seleção de 3 a 6 desses fragmentos da imagem.

Com esta experiência foi possível verificar a viabilidade de utilização da técnica no dia-a-dia, uma vez que esta técnica permite um elevado grau de assertividade, e a sua utilização não é intrusiva.

Em 2012, os autores (Kolly, Wattenhofer, & Welten) efetuaram uma experiência para reconhecer os utilizadores com base no seu comportamento. Para efetuar esta análise os autores desenvolveram um jogo em que os utilizadores deveriam responder a um questionário sobre Harry Potter e series televisivas. O jogo era constituído por três tipos de questões: estimativas, Puzzles e escolha múltipla. Os autores utilizaram esta divisão de forma a dispor diferentes elementos de interface (*button, radio button, lists*) e analisar os indicadores tempo, posição e pressão que um utilizador aplica no ecrã do dispositivo.

Foram analisadas as interações de 14890 utilizadores. Da análise os autores concluíram que o reconhecimento dos utilizadores é maior quando possuem um conjunto menor de utilizadores, ou seja, o reconhecimento de dois utilizadores é superior que o reconhecimento de um grupo de dez utilizadores. Concluíram também que será necessário adicionar mais indicadores te toque para diminuir a percentagem de falsas rejeições e falsos aceites. Atingiram um EER de 30%.

Os métodos de autenticação, como palavras-chave, provocam algum desconforto aos utilizadores de *Touch-Screen*, uma vez que a área de toque pode ser pequena. Para contornar este desconforto foi apresentada a técnica de *Lock Pattern*. Contudo esta técnica apresenta algumas falhas contra os ataques, pois está sujeita a ataques *Smudge*. Os autores (Angulo & Wästlund, 2012) exploraram esta técnica com a adição de caraterísticas biométricas. Na experiência que

realizaram, foi pedido a 32 utilizadores para desenharem três *Lock Pattern* diferentes de forma a ser analisado o tempo que os utilizadores demoravam em cada ponto, e a velocidade para mudar de ponto. Os autores concluíram que a adição das biometrias à técnica *Lock Pattern* aumenta a sua segurança. Concluíram também que é possível identificar os utilizadores com qualquer um dos tipos de bloqueios, atingindo um EER de 10.39%.

Também os autores (De Luca, Hang, Brudy, & Hussmann, 2012) exploraram a técnica *de Lock Pattern* associada às biometrias. Os autores desenvolveram uma experiência constituída por duas fases, na primeira fase os utilizadores deveriam desbloquear 160 vezes o dispositivo nos 4 tipos de bloqueios apresentados (horizontal, vertical, vertical com dois dedos e diagonal). Os indicadores que foram utilizados para analisar o desbloquear do dispositivo foram as coordenadas, a pressão, o tamanho e o tempo. Na segunda fase da experiência os utilizadores foram requisitados para efetuar o desbloqueio do dispositivo com uma palavra-chave específica, utilizando a técnica *Lock Pattern.* Participaram 48 pessoas na primeira parte da experiência e 31 na segunda parte.

Da análise efetuada aos dados da primeira parte da experiência, foi possível verificar que o tipo de desbloqueio mais ineficaz é o vertical com dois dedos, pois permite mais impostores de se autenticarem. E o mais eficaz é o diagonal, uma vez que atinge o maior número de autenticações corretas. Este tipo de autenticação necessita de mais exploração, uma vez que a maior percentagem de assertividade é de 57%.

Da análise dos dados da segunda parte da experiência os autores concluíram que a utilização dos indicadores pressão, área e velocidade permitem uma maior assertividade, cerca de 77%

Com a experiência os autores demonstraram a viabilidade da técnica *Lock Pattern* associada às biometrias para a autenticação dos utilizadores e quantos mais indicadores forem usados na autenticação melhores serão os resultados.

Em 2011, (Shi, Niu, Jakobsson, & Chow) efetuaram uma experiência com base na autenticação implícita, ou seja, para se autenticar não necessitam de inserir nenhum PIN ou outra informação. Na experiência participaram 276 indivíduos, oriundos de todo o mundo, e estes deveriam interagir normalmente com o dispositivo. Da interação, os autores memorizaram quatro tipos de atividades: SMS, chamadas telefónicas, histórico da Web e a localização. Das SMS foram memorizados o tempo, número de telefone, e direção da mensagem, ou seja, se era uma mensagem enviada ou recebida. Das chamadas telefónicas foi memorizado o número de

telefone, se a chamada foi feita do dispositivo ou se foi recebida, quando começou a chamada e a sua duração. Do histórico foi guardado o domínio dos URLs, e quantas vezes foi acedido anteriormente. Na localização, foram guardadas as coordenadas do GPS (se este estivesse ativo), e a localização calculada pelo sistema operativo do dispositivo Android, guardaram também o SSID da rede WiFi.

Cada vez que o utilizador efetua uma das quatro atividades, o sistema vai determinar se é um bom ou mau evento, ou seja, se é um evento que o utilizador efetua várias vezes ou se é um evento desconhecido.

Dos participantes iniciais foram analisados os dados de 50 utilizadores. Dos dados analisados, os autores verificaram que a utilização de todos os indicadores é a forma que permite distinguir o verdadeiro dono do dispositivo com maior eficácia.

Os autores (Sandnes & Zhang, 2012) analisaram várias caraterísticas do comportamento, como a dominância da mão, operação *bimanual*, o tamanho do movimento, a simetria, o tempo, a velocidade e regularidade. A dominância da mão refere-se, à preferência do utilizador para usar a mão direita ou esquerda, operação *bimanual* refere-se ao fato de o utilizador apenas utilizar uma ou as duas mãos, o tamanho do movimento refere-se ao fato de alguns utilizadores efetuarem movimentos mais longos enquanto outros efetuam movimentos mais curtos. Alguns utilizadores possuem padrões mais simétricos do que outros. Um toque é também caracterizado pelo tempo e velocidade aplicada. A regularidade é o ritmo que o utilizador aplica. Para analisarem as caraterísticas os autores solicitaram a 20 participantes para lerem uma banda desenhada dos Simpsons. Os autores concluíram que o tamanho e tempo do movimento possibilitam a classificação do utilizador.

Também os autores (Zheng, Bai, Huang, & Wang, 2012) analisaram o comportamento dos utilizadores em dispositivos *Touch-Screen*, selecionando as caraterísticas de pressão, tempo de toque, tempo entre toques, tamanho do toque e aceleração. Para analisarem estes, os autores requisitaram a 80 utilizadores para inserirem códigos PIN de quatro e oito dígitos. Após analisarem a viabilidade destas caraterísticas para identificar o utilizador, foi possível verificar que a combinação de todas as caraterísticas é solução mais adequada para a autenticação. Foi ainda possível verificar que a característica individual que apresenta uma maior taxa de erro é o tamanho. Com a utilização de todos os indicadores os autores obtiveram um EER de 3.37%.

Os autores (Bo, Zhang, & Li, 2013) efetuaram um estudo com duas vertentes para a identificação dos utilizadores. Uma das vertentes baseia-se na forma que o utilizador usa o dispositivo, a outra vertente baseia-se na forma como o dispositivo reage às ações do utilizador. Para analisarem esta vertentes os autores utilizaram os indicadores de pressão, área, duração, posição, aceleração e rotação. Na experiência participaram 100 indivíduos e apresentaram dois senários (estático e em movimento). No primeiro senário os autores atingiram um EER de 20% e no segundo senário 18%, ou seja, quando um utilizador se move a autenticação é menos assertiva.

Em 2012, (Frank, Biedert, Ma, Martinovic, & Song) efetuaram uma experiência em que os participantes deveriam numa primeira fase ler três textos seguidos por um questionário de escolha múltipla e na segunda fase encontrar as diferenças em dois pares de imagens. Após este experimento os participantes foram requisitados para fazer outro estudo. Neste deveriam ler um texto e comparar apenas um par de imagens. Das interações que os participantes efetuaram, foram guardados o código do movimento, o tempo, a orientação do dispositivo, as coordenadas, a pressão, a área, a orientação do dedo em relação ao ecrã e a orientação do ecrã. Na experiência foram usados quatro dispositivos e participaram 41 indivíduos.

Os autores verificaram que quantos mais traços se usarem para classificar um utilizador, menor será a percentagem de EER, contudo não é necessário analisar mais do que 12 traços, uma vez que a percentagem se mantém nos 3%. O valor de EER difere quando analisado em intra ou intercessões, obtendo um EER de 0% e 2%-3% respetivamente. Os autores consideram esta técnica como insuficiente para autenticação. Estes sugerem que este sistema deve ser usado em complemento a outros métodos de autenticação.

Em 2012 os autores (Meng, Wong, Schlegel, & Kwok) efetuaram uma experiência com 20 participantes. Estes deveriam utilizar o dispositivo móvel de forma usual, e efetuarem a coleção de dados de 6 sessões (com 10 minutos de duração). Os dados guardados consistiam no tipo de *input*, as coordenadas (x e y) e o tempo do sistema. Com estes dados foi-lhes possível analisar as seguintes caraterísticas: velocidade média do toque por direção, fração de movimentos por direção, tempo médio de um único toque e de um *multi-touch*, número de movimentos de toques numa sessão, número de toques únicos numa sessão e *multi-touch.* Dos dados analisados verificou-se EER de 2.29%

Capitulo III - Experiência

Para se responder à questão proposta neste trabalho foi elaborada uma experiência. Deste modo é apresentada nesta secção uma descrição da experiência desenvolvida – descreve-se a aplicação desenvolvida para captação das variáveis em estudo –, os resultados atingidos.

3.1 Explicação da experiência

Como já foi referido anteriormente, o objetivo deste trabalho é verificar a viabilidade de utilização das variáveis de toque para a autenticação de um utilizador. É também estudada a sua viabilidade em ambientes de autenticação contínua do indivíduo.

Para o desenvolvimento desta experiência foi selecionada a plataforma Android. Esta escolha foi feita tendo em conta as funcionalidades oferecidas pela API e a pela crescente utilização de dispositivos móveis Android.

Deste modo foi desenvolvida uma aplicação que permite obter os valores da pressão, área de contato, duração, coordenadas, orientação do contato do dedo, a duração do movimento e o tamanho.

Estes dados são obtidos recorrendo à API. A classe utilizada para obter os dados é a classe MotionEvent. Esta possui o método onTouchEvent (MotionEvent event) que permite lidar como os movimentos de toque. Um evento pode ter três tipos de ação: ACTION_DOWN (início do evento), ACTION_MOVE (quando existe movimento entre o início e fim do evento), ACTION_UP (fim do evento). Estes são determinados através do getAction(). Para obter a pressão exercida é usado o método getPressure(); para obter a área pressionada é usado getSize(); para obter a orientação da área de toque é usado getOrientation(); para obter as coordenadas usa-se o getX() e getY(); para se obter a duração do evento usa-se o getDowTime() e o getEventTime(), que fornecem o tempo em ms de quando o utilizador inicialmente pressiona o ecrã e o do fim do evento, respetivamente.

Para obter a duração do movimento foi usada a fórmula:

$$t = tempo\ final - tempo\ inicial$$

Para além da pressão, área, posição, duração e orientação é guardado o tipo de ação (*action: touch down* = 1, *touch move* = 2, *touch up* =3) e tipo de movimento (*gesture: drag=1, scroll=2, press=3, zoom=4*).

A aplicação não requer a inserção de dados pessoais, sendo assim criados utilizadores anónimos.

Na aplicação é solicitado aos utilizadores para responderem a três questões. Estas são relativas à faixa etária e experiência dos utilizadores com tecnologias, bem como que mão utiliza para mexer no dispositivo, ou seja, se são destros ou esquerdinos, e que dedos costumam utilizar para tocar no ecrã.

Estas questões são efetuadas de modo a verificar o seu impacto nas variáveis de toque. Por exemplo, se um indivíduo que tem mais experiência com tecnologias efetua movimentos mais rápidos ou mais lentos que indivíduos com menos experiência, se a área de contato com o ecrã está relacionada com os dedos que utiliza para efetuar os movimentos.

A aplicação consiste num conjunto de atividades que pretendem representar os movimentos comuns efetuados num dispositivo *touch-screen*. Os movimentos explorados são o *swipe* vertical e horizontal (scroll), o *zoom,* o *drag* e o *press (Tap).*

Para analisar as variáveis relativas ao swipe horizontal, é pedido ao utilizador para ver uma sequência de imagens, que só podem ser movidas da esquerda para a direita e vice-versa, e estas possuem uma marca que obrigam o utilizador a iniciar o movimento no mesmo local, removendo assim o fator aleatório.

O swipe vertical é explorado com uma atividade em que o utilizador tem de ler diversos provérbios. Simulando assim os movimentos verticais, para cima e para baixo, representando as situações de leitura de um *e-mail*, ver uma conversa de mensagens e outras situações normais de utilização do dispositivo móvel.

Para verificar o movimento de zoom de uma área, é pedido aos utilizadores para aumentarem e diminuírem objetos específicos de uma imagem, impondo assim movimentos semelhantes para os diversos utilizadores.

Para representar o movimento de arrastar um ícone, ou outro objeto do ecrã, é pedido aos participantes para arrastarem oito frutas para uma cesta. A cesta encontra-se no centro das frutas, de modo a obrigar o utilizador a arrastar um objeto para cima, para baixo, para a esquerda, para a direita e de forma oblíqua – ver Figura 90 – Orientações do Movimento Drag dos anexos.

Por fim é solicitado aos utilizadores para pressionarem os botões dispostos em diversas posições do ecrã. Nesta atividade pretende-se simular um utilizador a pressionar um ícone de uma aplicação, ou outras atividades em que o indivíduo necessita pressionar uma determinada área do ecrã para determinada finalidade. São dispostos vários botões em diversas posições para verificar as diferenças das variáveis de toque nestas posições.

Para a obtenção da distância do movimento, foi utilizada a fórmula:

$$d = \sqrt{(xf - xi)^2 + (yf - yi)^2}$$

A velocidade é definida através da distância definida em pixéis percorrida em determinado tempo (segundos). Assim sendo foi obtida através da equação:

$$v = \frac{Tamanho\ movimento}{duração\ movimento}$$

A experiência foi realizada apenas num dispositivo, Samsung Galaxy SIII mini, de forma a reduzir as discrepâncias dos valores obtidos em dispositivos com caraterísticas diferentes.

Na experiência são analisados os dados relativos a 17 utilizadores e este foram recolhidos no período de 2 semanas.

3.2 Resultados obtidos

Dos dados obtidos, foram descartados os dados relativos à atividade do *zoom*, uma vez que alguns dos utilizadores não efetuaram a divisão do movimento de aumentar do movimento de diminuir, ou seja, efetuaram o aumentar e diminuir de forma continua, deste modo os dados ficaram inviabilizados para análise. Relativamente a atividade dos botões, foi apenas selecionado um dos botões, uma vez que, não foi detetado nenhum padrão diferenciativo entre estes.

Uma vez que os dados obtidos através do getOrientation() não foram conclusivos (o dispositivo forneceu o valor 0.0 para todos os movimentos), a orientação foi determinada através da posição final e inicial.

Para a análise dos dados foi selecionada a ferramenta de *Data Mining* WEKA. Os atributos selecionados para análise foram a pressão, área, orientação (direita, esquerda, cima, baixo, e obliqua (ver orientações anexo I), x e y da posição inicial, x e y de uma posição intermédia, x e y da posição final, o tipo de movimento, a duração, tamanho e velocidade do movimento. Deste modo a análise foi efetuada tendo em conta 13 atributos diferentes.

Os dados foram divididos por utilizador, e foram selecionados 5 registos de cada movimento. Assim sendo, selecionaram-se 130 registos classificados para treino, dos quais 65 pertenciam ao utilizador. Para efetuar o teste foram selecionados 65 registos do utilizador a identificar e 1040 registos dos restantes utilizadores. Deste modo pretende-se identificar o utilizador através de 13 movimentos diferentes.

Como o conjunto de dados usados para análise não é muita extensa, e a redução da dimensão não é muito significativa neste caso, foi descartada a utilização do PCA. O classificador usado para obter o modelo de cada utilizador foi o SVM. O *kernel* selecionado foi o *polynomial* com expoente 2.0.

3.3 Padrão Comportamental

Cada indivíduo possui um padrão único de interação com o dispositivo. Assim, apresenta-se a análise efetuada ao padrão comportamental dos 17indivíduos.

A análise é dividida por tipo de movimento descrito – Drag, Scroll e Tap – e a orientação que este pode tomar – horizontal (para a esquerda e para direita), vertical (para cima e para baixo), oblíqua (ver Figura 90 – anexo I), sem orientação.

Com a análise do padrão comportamental pretende-se demonstrar as diferenças comportamentais entre os diferentes indivíduos e se as interações selecionadas possuem características diferentes, ou seja, verificar se as diferenças entre a pressão, área, coordenadas, duração, distância e velocidade aplicadas nos diferentes movimentos são distintivas.

De seguida é apresentada a análise do movimento *drag* tendo em conta as 8 direções diferentes.

- Movimento Drag

Orientação – Vertical para cima

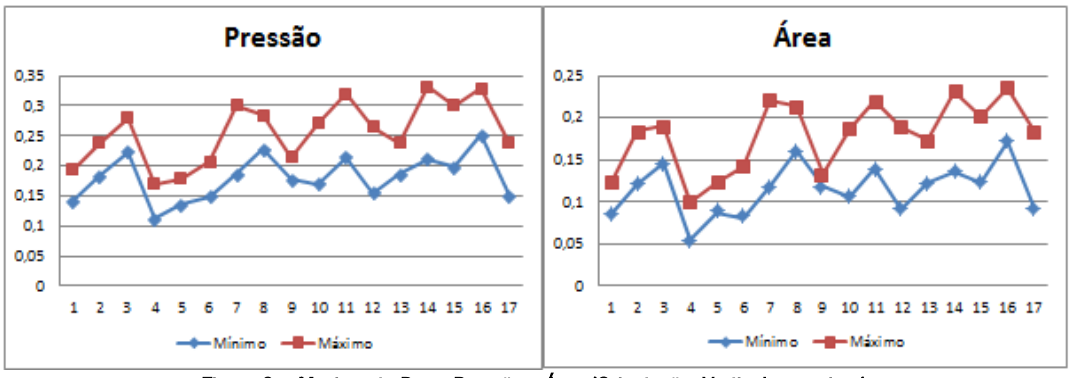

Figura 9 – Movimento Drag: Pressão e Área (Orientação: Vertical para cima)

Da Figura 9 é possível observar a pressão mínima e máxima que os 17 indivíduos aplicam ao arrastar um objeto verticalmente para cima. Pode-se verificar que os indivíduos aplicam pressões diferentes, havendo indivíduos que aplicam uma pressão elevada (acima dos 0,25) – 3, 7, 8, 10, 11,12,14, 15 e 16 -, e uns aplicam uma pressão baixa (abaixo dos 0,25) – 1, 2, 4, 5, 6, 9, 13, 17 -. O indivíduo que aplica uma maior pressão é o número 16 e o que aplica uma pressão mais baixa é o 4. Do gráfico é ainda possível observar que alguns dos indivíduos possuem um nível de pressão mais constante do que outros. Os indivíduos 7, 10, 11, 12, 14, 15 e 17 possuem uma maior amplitude entre o valor máximo e mínimo de pressão, ou seja, são mais inconstantes.

É possível verificar que a área que os indivíduos aplicam é mais inconstante do que a pressão, contudo o indivíduo 9 aplica uma área mais constante. Apesar de a amplitude ser elevada, é possível observar diferenças entre os indivíduos. Os números 8 e 16 são os que ocupam uma área maior do ecrã e o número 4 é o que ocupa uma área mais pequena.

Os indivíduos que demoram mais tempo a efetuar o movimento de arrastar um objeto para cima são o 3 e o 15, pelo contrário os indivíduos 5, 11, e 13 são os que demoram menos tempo. Pode-se verificar que, excetuando os indivíduos 3 e 15, todos os outros indivíduos demoram menos de um segundo a arrastar um objeto para cima.

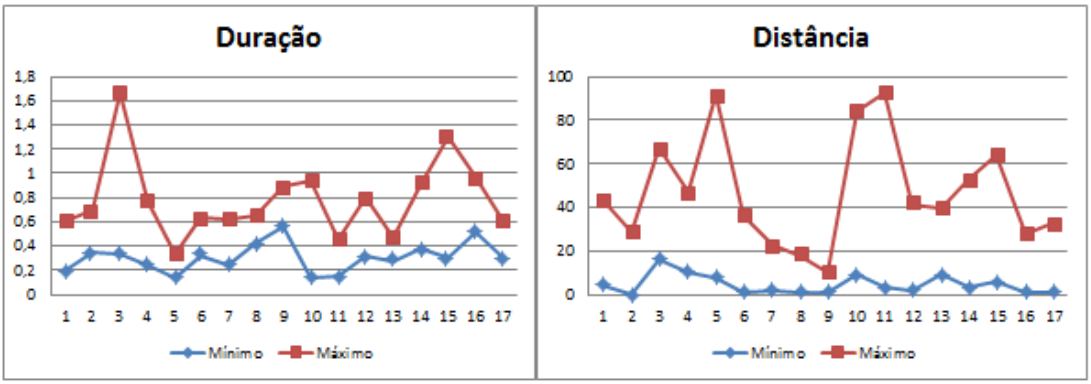

Figura 10 – Movimento Drag: Duração e Distância (Orientação: Vertical para cima)

Da Figura 10 conclui-se que o 3, 5, 10, 11 e o 15 são os que efetuam movimento mais compridos, pois percorrem mais pixéis. Os indivíduos 7, 8 e 9 são os que percorrem uma distância mais constante. Com isto pode-se afirmar que os indivíduos traçam movimentos de dimensões diferentes, havendo elementos que traçam movimentos curtos e outros mais compridos.

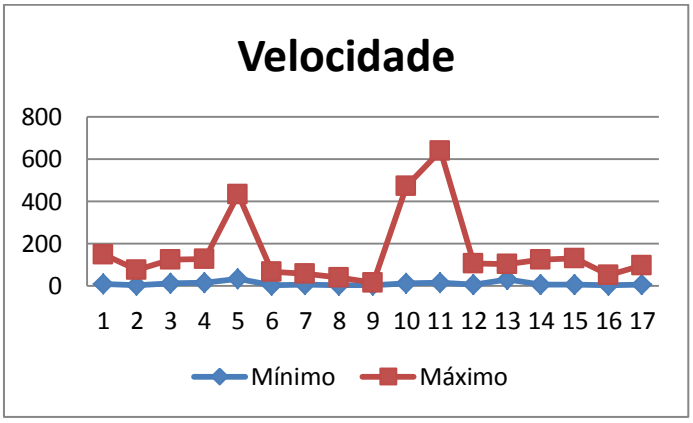

Figura 11 – Movimento Drag: Velocidade (Orientação: Vertical para cima)

Consegue-se verificar que o indivíduo que percorre mais pixéis por segundo é o número 11, ou seja, é o elemento que é mais rápido a efetuar o movimento. Os indivíduos 10 e 5 também têm movimentos bastante rápidos em comparação aos outros elementos. O que percorre uma distância menor é o indivíduo 9. Porém os elementos 2, 6, 7, 8 e 16 também percorrem pouca distância por segundo.

Como se pode ver na figura abaixo, para traçar um movimento, os indivíduos tocam o ecrã em posições diferentes. Ou seja, iniciam o movimento em posições diferentes e finalizam em

posições diferentes. Os valores dos pontos intermédios também são diferentes nos indivíduos, pois alguns elementos efetuam movimentos mais direitos do que outros, ou seja, direcionam o movimento mais para a direita ou esquerda.

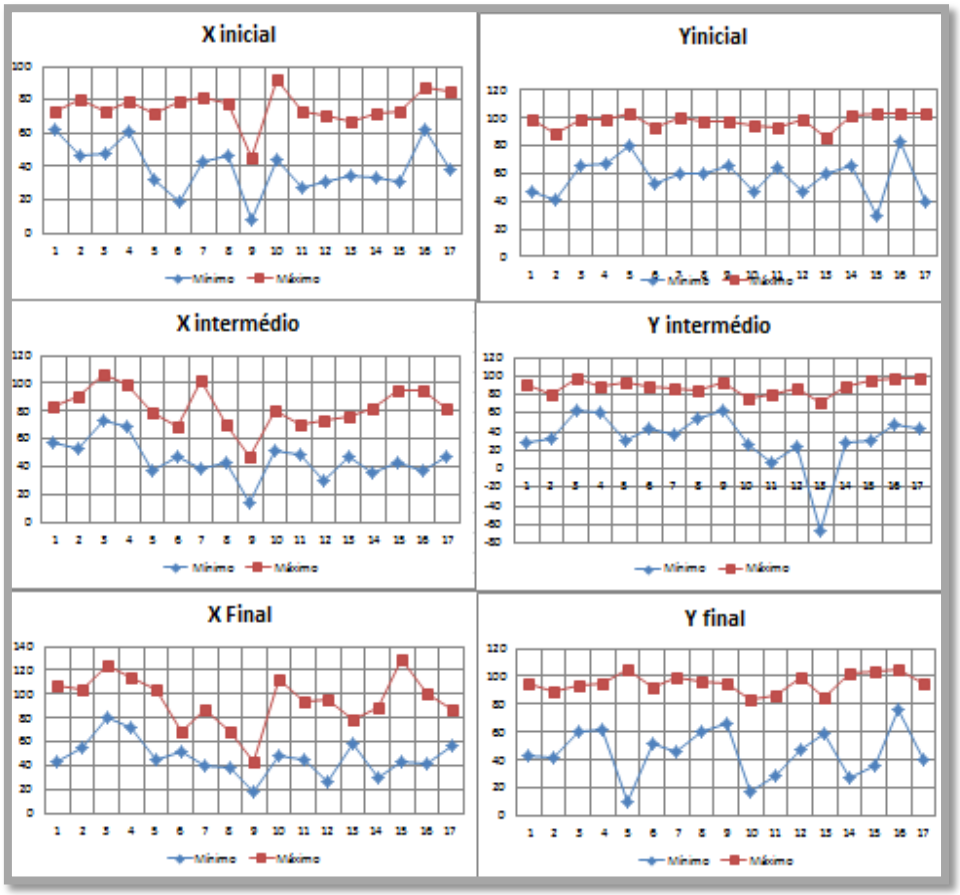

Figura 12 – Movimento Drag: X e Y (Orientação: Vertical para cima)

Relativamente à coordena do X pode-se observar que se mantém mais ou menos uniforme ao longo do movimento. É ainda possível observar que os indivíduos 10, 16 e 17 iniciam o movimento mais à direita, e excetuando o indivíduo 9 que inicia o movimento mais a esquerda, os outros indivíduos iniciam o movimento numa posição mais centralizada. Relativamente ao eixo do Y, os indivíduos 1, 2, 10, 12, 15 e 17 são os que iniciam o movimento numa posição mais baixa. É ainda possível observar que os valores de Y iniciais e intermédios não são tão discriminativos como os de X. Os indivíduos 5, 10, 11, 14 e 15 são os que terminam o movimento numa posição mais baixa, contudo o número 16 termina o movimento mais acima.

Orientação – Vertical para baixo

Como se pode visualizar na Figura abaixo, os indivíduos possuem padrões distintos de pressão. Alguns dos indivíduos são mais inconstantes na pressão que aplicam – o 7, 10, 12 e 14 -, porem os indivíduos 1, 5, 13 e 17 mantem a pressão aplicada num intervalo mais pequeno, ou seja, aplicam uma pressão mais constante. É ainda possível observar os que aplicam uma pressão mais alta – 7, 11, 14, e 16 -, e os que aplicam uma pressão menor contra o visor – 1, 4, 5 e 17 –. Do gráfico pode-se concluir que o movimento de arrastar um objeto para baixo é discriminativo, ou seja, os indivíduos aplicam pressões diferentes.

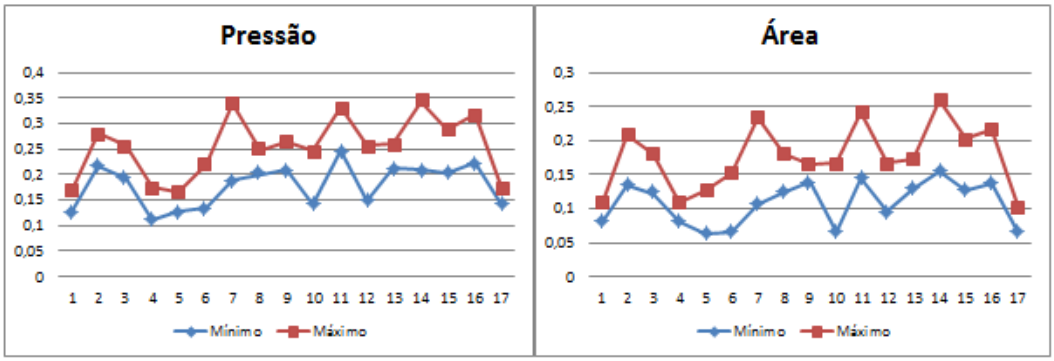

Figura 13 – Movimento Drag: Pressão e Área (Orientação: Vertical para baixo)

Pode-se verificar que os indivíduos que aplicam uma pressão mais elevada ocupam uma superfície maior de contato do visor, já os indivíduos que aplicam uma pressão baixa tocam uma superfície inferior. Com isto, pode-se concluir que a área que ocupam está relacionada com a pressão que aplicam, ou seja, estas variáveis estão correlacionadas.

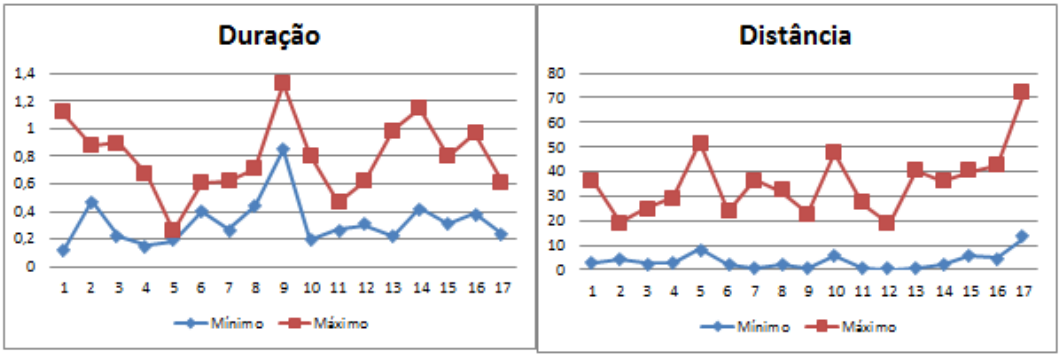

Figura 14 – Movimento Drag: Duração e Distância (Orientação: Vertical para baixo)

Em relação à duração, o elemento que demora menos tempo a efetuar este tipo de movimento é o número 5, pode-se ainda verificar que este é o indivíduo que possui uma menor amplitude entre a duração máxima e mínima. É ainda observável que o elemento que demora mais tempo é o 9. O indivíduo que possui uma maior amplitude entre a duração mínima e a duração máxima é o 1. Da Figura 14 pode-se concluir que os indivíduos demoram tempos diferentes a efetuar o movimento.

Consegue-se observar que os valores mínimos percorridos são muito semelhantes entre os elementos, porém os indivíduo 5 e 17 são os que percorrem uma maior distância. Contudo a distância máxima que percorrem varia bastante de indivíduo para indivíduo, ou seja, os indivíduos efetuam traços com dimensões diferentes.

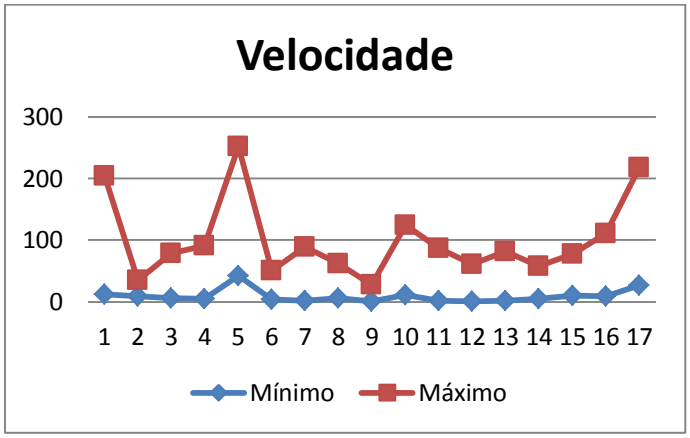

Figura 15 – Movimento Drag: Velocidade (Orientação: Vertical para baixo)

Neste tipo do movimento, os indivíduos que percorrem mais pixéis por segundo são o 1, 5 e 17. Ou seja, efetuam o movimento mais rapidamente. Os elementos que são mais lentos a arrastar um objeto para baixo, são o 2 e o 9. Como se pode ver no gráfico os indivíduos demoram tempos diferentes a efetuar o movimento.

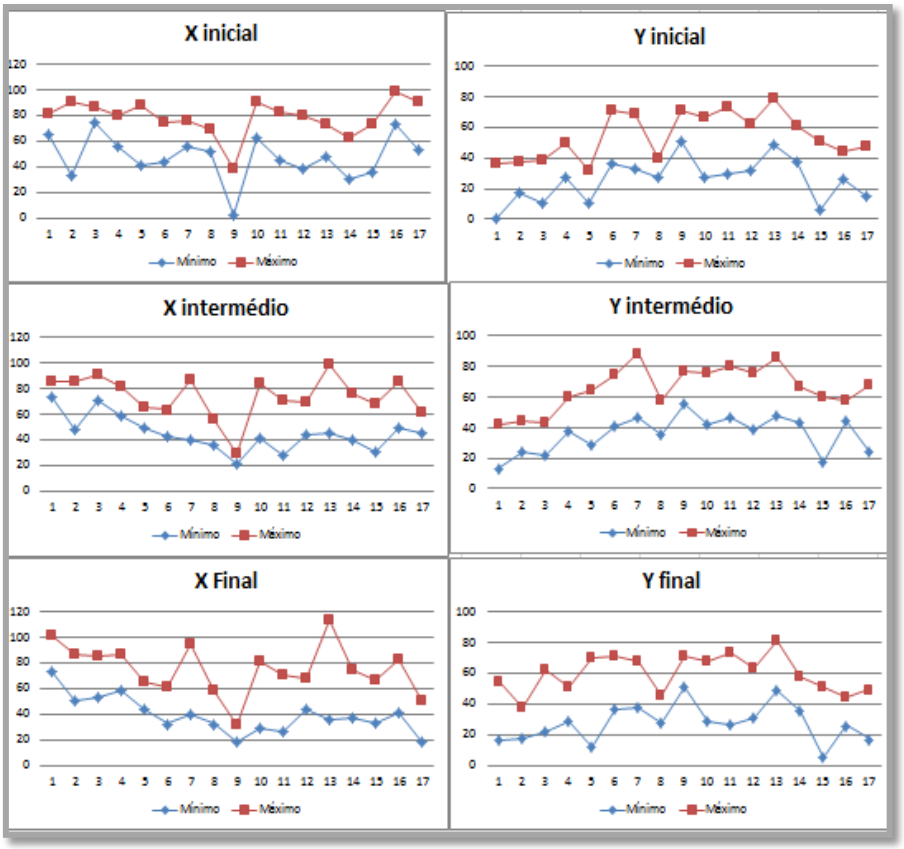

Figura 16 – Movimento Drag: X e Y (Orientação: Vertical para baixo)

Na Figura 16, pode-se visualizar os pontos mínimos e máximos em que os indivíduos iniciam o movimento, os pontos intermédios e a finalização do movimento. Pode-se observar que alguns dos indivíduo começam o movimento mais à esquerda e outros mais à direita. O indivíduo 9 é o indivíduo que inicia o movimento mais à esquerda e os que iniciam o movimento mais a direita são o 3 e o 16. Os indivíduos que iniciam o movimento num y mais alto são o 6, 7, 9, 10, 11, 12 e 13, os outros iniciam num valor mais alto. Assim sendo, os indivíduo passam por coordenadas diferentes para descrever o movimento de arrastar para baixo.

Orientação – Horizontal para a esquerda

Como se pode observar na Figura 17 os indivíduos aplicam pressões diferentes na execução do movimento de arrastar para a esquerda. Os indivíduos que aplicam uma maior pressão são o 7, 11, 14, 15 e 16, por outro lado os que aplicam uma pressão menor são o 1, 4, 5, 6, os que aplicam uma pressão intermédia são o 2, 8, 9, 12, 13 e 17. Do gráfico da pressão é possível observar que os indivíduos 7, 11, 12, 14, 15 e 16 possuem uma maior amplitude entre o valor

máximo e mínimo de pressão, deste modo, pode-se dizer que são mais inconstantes na pressão que aplicam.

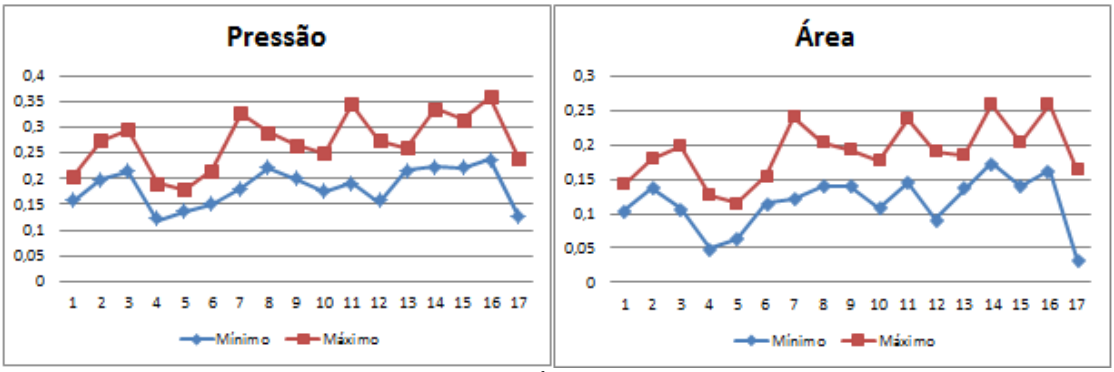

Figura 17 – Movimento Drag: Pressão e Área (Orientação: Horizontal para a esquerda)

Como se pode verificar na Figura 17 os elementos ocupam áreas diferentes do ecrã. Os indivíduos que ocupam uma menor área do ecrã são o 1, 4, 5, 6 e o 17. Dos indivíduos que ocupam uma área maior, o 14 e 16 são os que se destacam mais.

É possível observar que a área está correlacionada com pressão, ou seja, quanto mais pressão um indivíduo aplica, maior é a área de contato que ocupa, e vice-versa. Por exemplo o indivíduo 4 aplica uma pressão mais baixa e ocupa uma área mais pequena, já o elemento 16 aplica uma pressão mais elevada e ocupa uma área maior do ecrã.

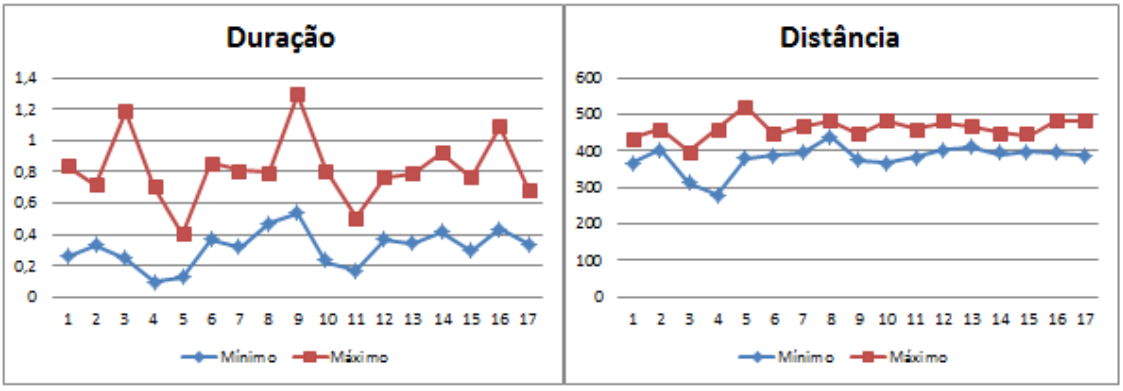

Figura 18 – Movimento Drag: Duração e Distância (Orientação: Horizontal para a esquerda)

Da Figura 18 é possível observar que os indivíduos 3 e 9 são os que demoram mais tempo a finalizar um movimento de arrastar um objeto para a esquerda, e os que demoram menos tempo são o 5 e o 11.

Como se pode ver na Figura acima, a distância não é muito discriminativa para este movimento. Ou seja, os indivíduos percorrem distâncias mais ou menos iguais. Contudo os indivíduos 4 e 5 são os que se diferenciam mais dos outros elementos. Estes são também os que possuem uma amplitude maior entre a distância máxima e mínima percorrida.

Da figura abaixo é possível observar que os indivíduos 4, 5, 10 e 11 são os que efetuam o movimento mais rapidamente, pois percorrem mais pixéis por segundo. Os indivíduos 8 e 9 são os que demoram mais tempo a efetuar o movimento, e possuem uma amplitude mais pequena entre a velocidade máxima e mínima.

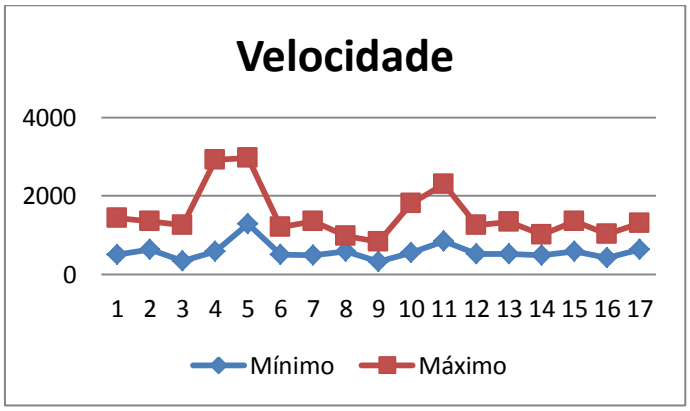

Figura 19 – Movimento Drag: Velocidade (Orientação: Horizontal para a esquerda)

Na Figura 20 é possível observar que os elementos 9 e 14 iniciam os movimentos mais à esquerda e o elemento 1 é o que inicia o movimento mais a direita. Pode-se observar que o x intermédio é bastante discriminativo entre os indivíduos.

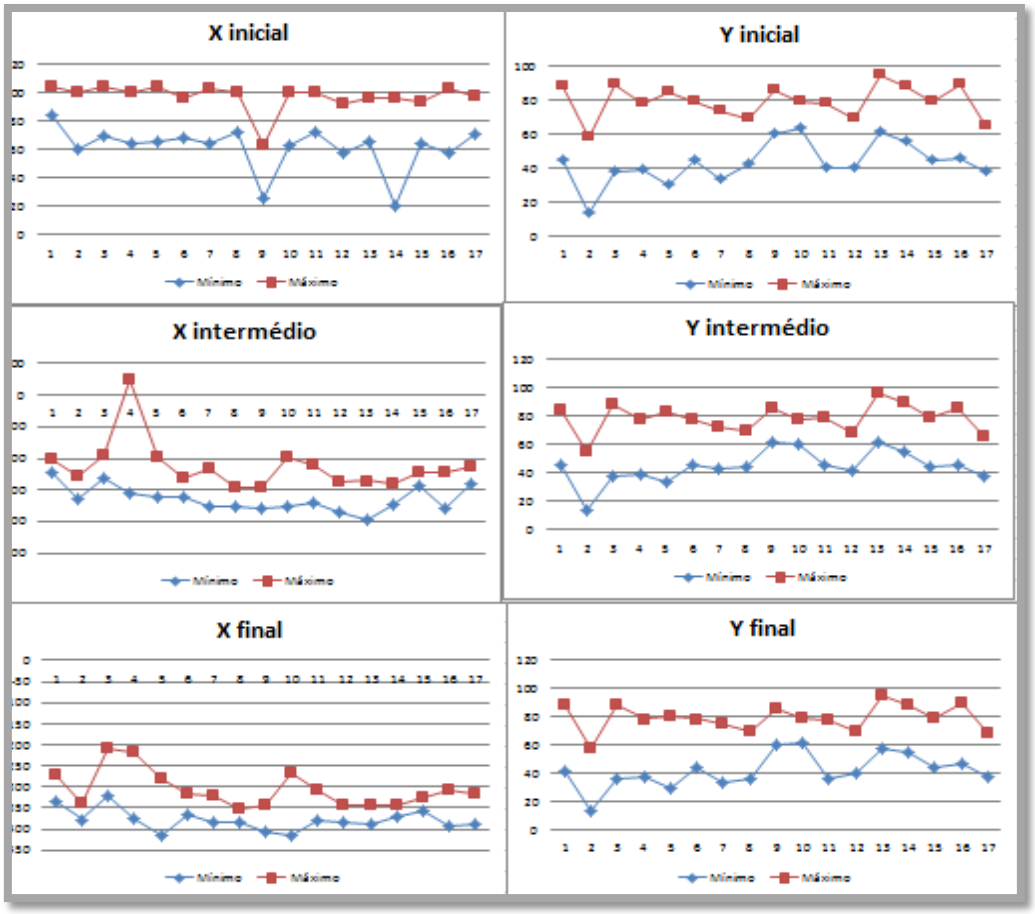

Figura 20 – Movimento Drag: X e Y (Orientação: Horizontal para a esquerda)

É ainda percetível que os elementos 3 e 4 são os que terminam o movimento mais a esquerda. Em relação ao eixo do Y pode-se observar que os elementos 2 e 17 são os que iniciam o movimento num valor mais baixo. O elemento 13 é o que inicia o movimento no valor mais elevado. Consegue-se visualizar que a amplitude entre os valores mínimos e máximos de x é mais pequena que a amplitude dos valores máximos e mínimos do Y. Ou seja, as posições de x são mais constantes do que as posições de Y.

Orientação – Horizontal para a direita

Como é possível visualizar na figura abaixo, os indivíduos aplicam uma pressão bastante constante, ou seja, não existe uma grande distância entre os valores máximos e mínimos de pressão. Pode-se observar que os elementos 1, 4, 5 e 17 são os que aplicam uma menor pressão e os elementos 7, 11, 14 e 16 aplicam uma pressão mais elevada.

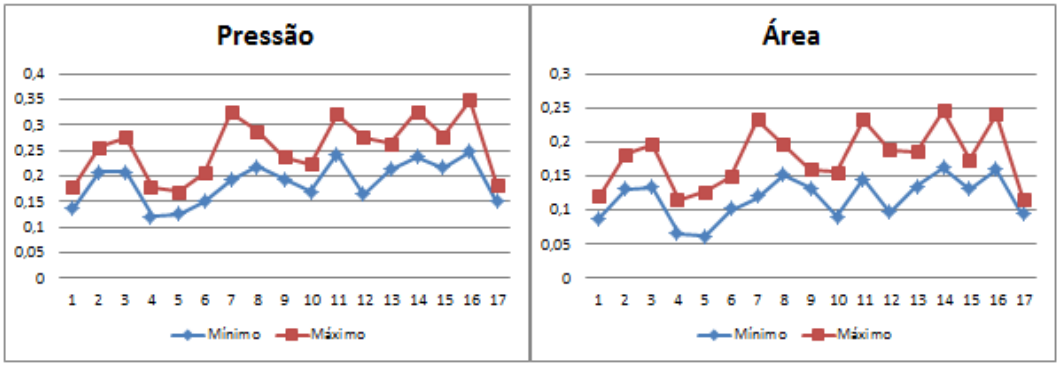

Figura 21 – Movimento Drag: Pressão e Área (Orientação: Horizontal para a direita)

Na Figura 21 observa-se que os indivíduos que aplicam uma maior pressão são também aqueles que ocupam uma maior área do ecrã, e os que aplicam uma menor pressão são os que ocupam uma menor área do ecrã.

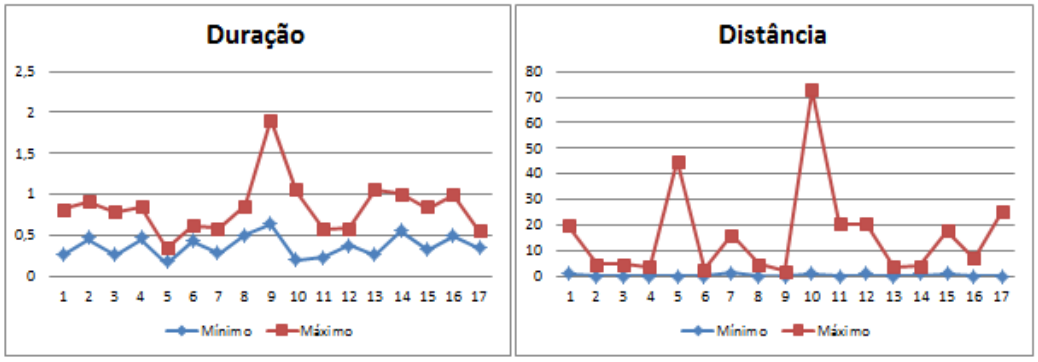

Figura 22 – Movimento Drag: Duração e Distância (Orientação: Horizontal para a direita)

Como se pode visualizar na Figura 22, os indivíduos demoram tempos distintos para efetuar o movimento. O elemento que demora mais tempo a arrastar um objeto para a direita é o 9, por outro lado os que demoram menos tempo são o 5, 6, 7 e 17.

Os indivíduos que percorrem uma maior distância são os números 5 e 10. Os que descrevem um movimento mais curto são o 2, 3, 4, 6, 8, 9, 13, 14 e 16. Os elementos 1, 7, 11, 12, 15 e 17 percorrem distâncias intermédias. Com isto pode-se dividir os elementos por três grupos, com distância percorrida diferenciada. Pode-se verificar que as distâncias mínimas não são discriminativas, ou seja, são semelhantes para todos os indivíduos.

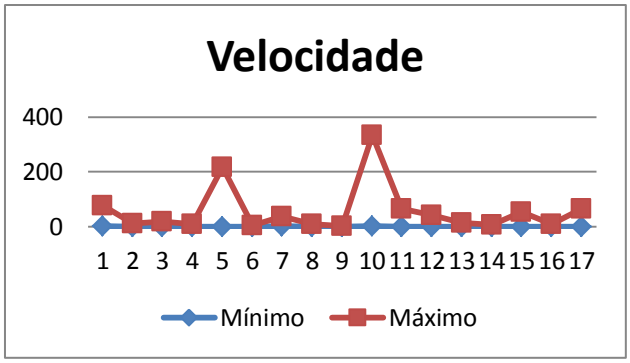

Figura 23 – Movimento Drag: Velocidade (Orientação: Horizontal para a direita)

No gráfico da velocidade é possível verificar que os indivíduos que percorrem uma maior distância são também os que efetuam o movimento de forma mais rápida e os que percorrem menos distância são os que são mais lentos a descrever o movimento de arrastar para a direita.

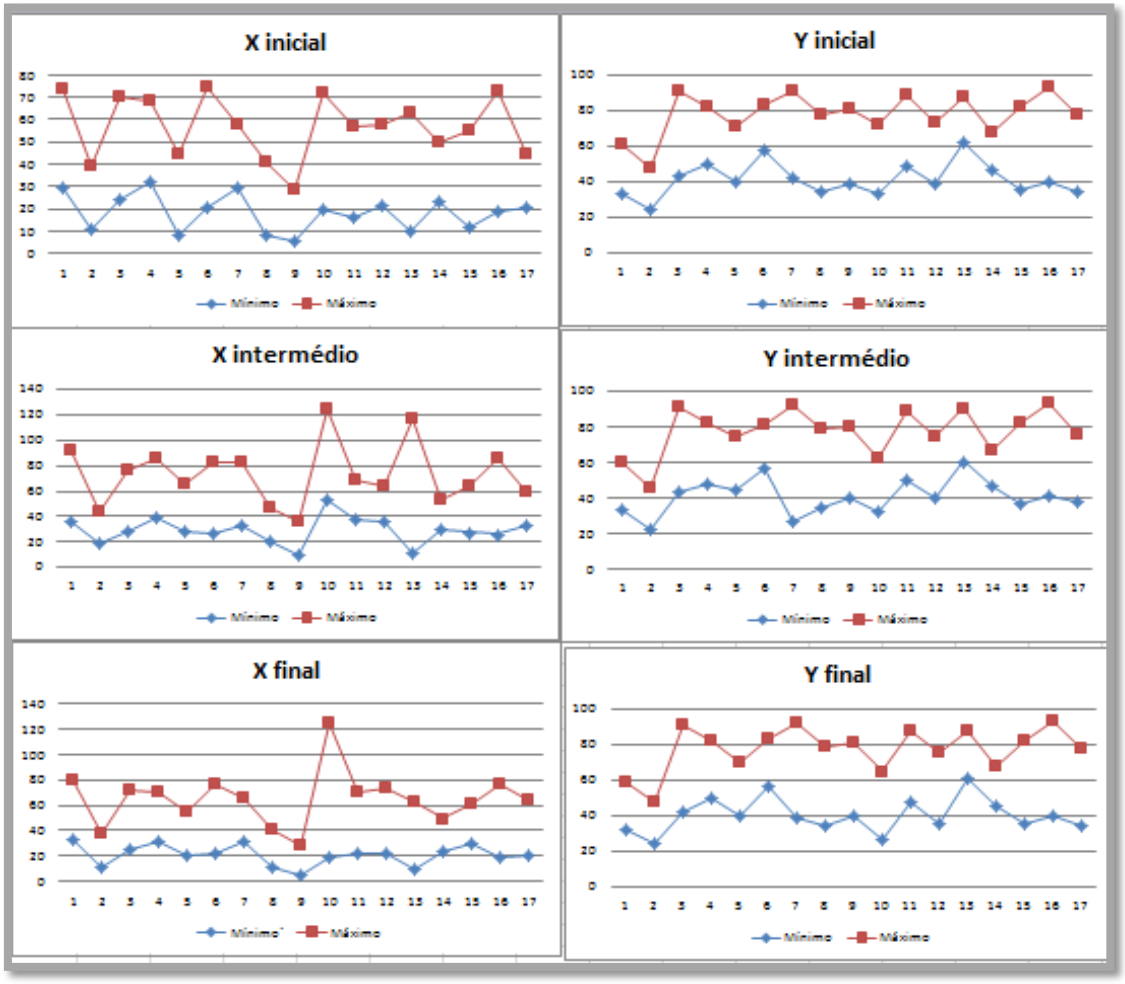

Figura 24 – Movimento Drag: X e Y (Orientação: Horizontal para a direita)

Da Figura 24 é possível observar que uns indivíduos iniciam o movimento mais à esquerda (2, 5, 8 e 9), enquanto outros iniciam o movimento mais à direita (1, 4 e 7). É ainda possível observar que uns indivíduos iniciam o movimento mais acima do que outros. Com isto pode-se apurar que os indivíduos traçam movimentos em posições diferentes.

Orientação – Oblíqua (para baixo e esquerda)

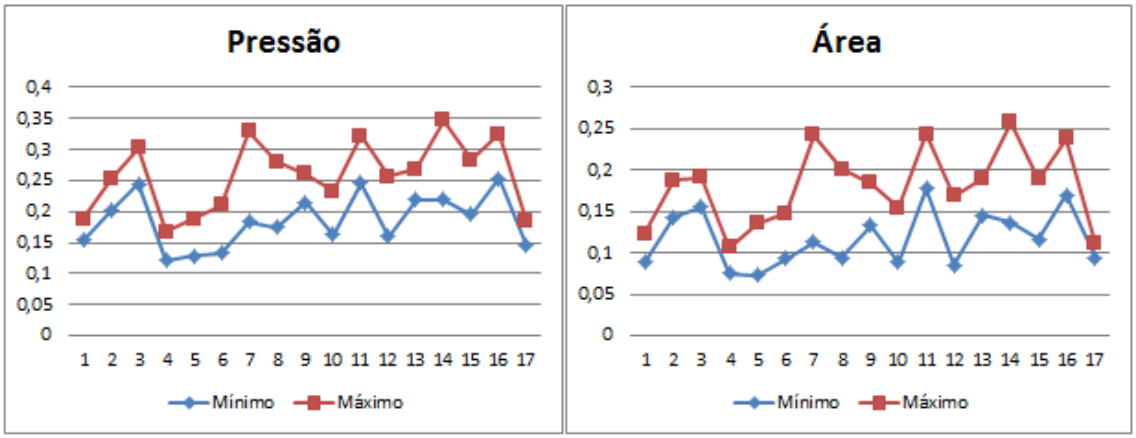

Figura 25 – Movimento Drag: Pressão e Área (Orientação: Oblíqua para baixo e esquerda)

Da Figura 25 observa-se que a pressão e a área estão correlacionadas. Deste modo os indivíduos 3, 7, 11, 15 e 16 são os que aplicam uma pressão mais alta e ocupam uma área maior do ecrã. Por outro lado os indivíduos 1, 4, 5, 6 e 17 são os que aplicam uma pressão menor no ecrã e a área que cobrem é inferior.

Da figura abaixo pode-se observar que os indivíduos demoram tempos diferentes a arrastar um objeto com orientação obliqua para baixo e esquerda. Os indivíduos 1, 3, 9, 15 e 16 são os que demoram mais tempo, contudo o elemento 1 possui uma duração mínima muito distante da duração máxima. O indivíduo 5 é o que demora menos tempo.

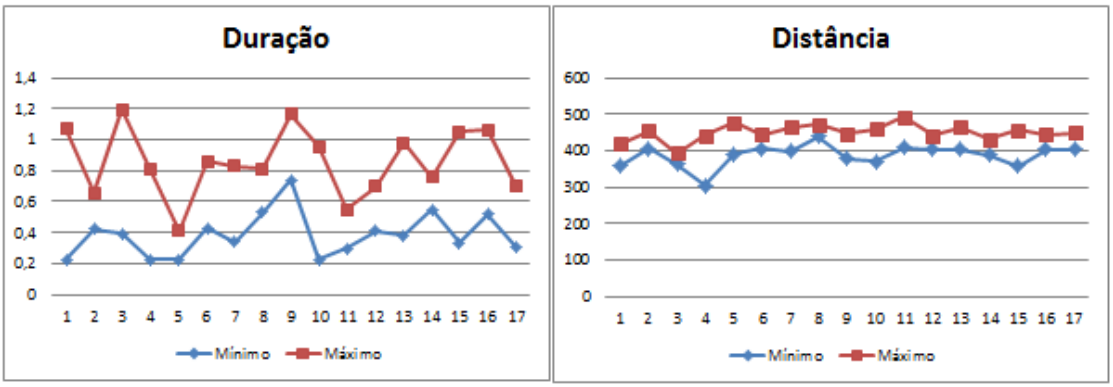

Figura 26 – Movimento Drag: Duração e Distância (Orientação: Oblíqua para baixo e esquerda)

Da Figura acima, pode-se visualizar que este movimento não é muito discriminativo em relação à distância. Como se pode ver, os indivíduos percorrem distâncias muito próximas.

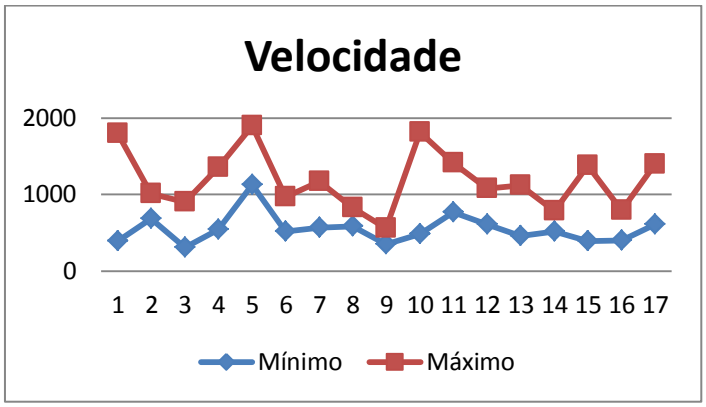

Figura 27 – Movimento Drag: Velocidade (Orientação: Oblíqua para baixo e esquerda)

Em relação a velocidade, os elementos que percorrem mais pixéis por segundo são o 1, 5 e o 10, o que demora mais tempo é o elemento 9. Como se pode verificar os indivíduos possuem velocidades diferentes.

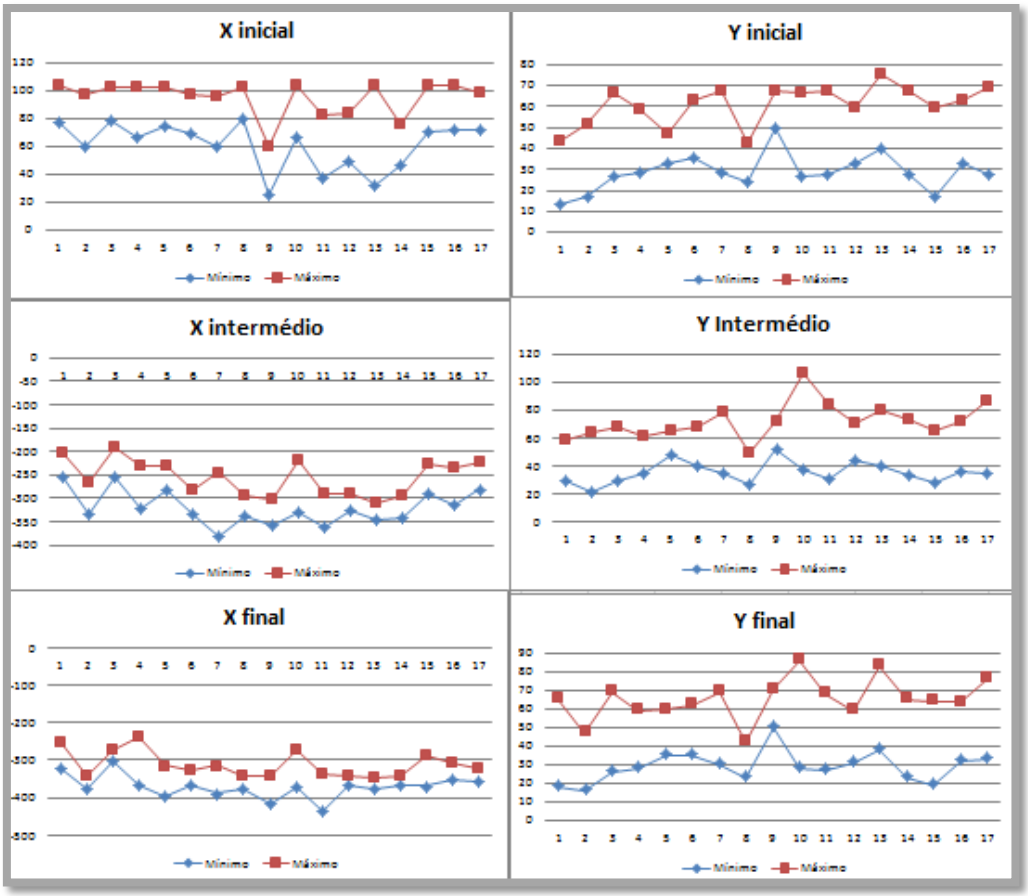

Figura 28 – Movimento Drag: X e Y (Orientação: Oblíqua para baixo e esquerda)

No gráfico das coordenadas – ver Figura 28 – pode-se observar que os indivíduos 9, 11, 12 e 14 são os que iniciam o movimento mais a esquerda, os outros iniciam o movimento mais à direita. Pode-se observar que os pontos intermédios e finais do x são diferentes nos indivíduos, é ainda observável que os indivíduos 1, 5, 8 iniciam o movimento no y mais baixo, e o indivíduo 13 é o que inicia numa posição mais alta. Ou seja, uns elementos iniciam o movimento mais acima do que outros. Com isto pode-se dizer que as posições que os indivíduos percorrem para realizar o movimento são diferentes.

Orientação – Oblíqua (para baixo e direita)

Como se pode observar na Figura 29 os indivíduos aplicam pressões diferentes na realização do movimento. Pode-se verificar que os indivíduos 1, 4, 5 e 17 não aplicam pressões superiores a 0.2, ou seja, são os elementos que aplicam uma pressão menor. Os outros indivíduos aplicam uma pressão um pouco mais elevada.

Pode-se verificar que a área está relacionada com a pressão. Como se pode confirmar os indivíduos que aplicam uma pressão mais elevada também ocupam uma área maior do ecrã e os que aplicam uma pressão menor, ocupam uma área menor de contato.

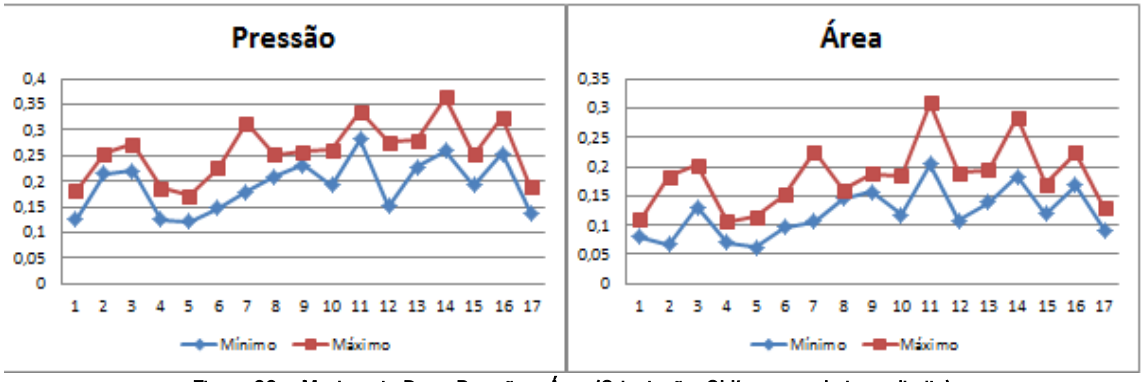

Figura 29 – Movimento Drag: Pressão e Área (Orientação: Oblíqua para baixo e direita)

Os indivíduos que possuem uma menor amplitude entre as durações máximas e mínimas são o 4, 9 e 16, ou seja, variam menos no tempo a efetuar o movimento do que os outros elementos. Os elementos 2, 3 e 8 são os que possuem uma maior amplitude entre os valores máximos e mínimos, bem como são os que demoram mais tempo a efetuar o movimento – demoram mais de um segundo e meio -.

Como se pode observar na figura abaixo, os indivíduos percorrem distâncias diferentes, alguns percorrem distâncias maiores - 1, 5, 7, 10, 13, 15 e 17 -, e outros percorrem distâncias mais curtas. Deste modo é possível distinguir um elemento tendo em conta a distância percorrida neste tipo de movimento.

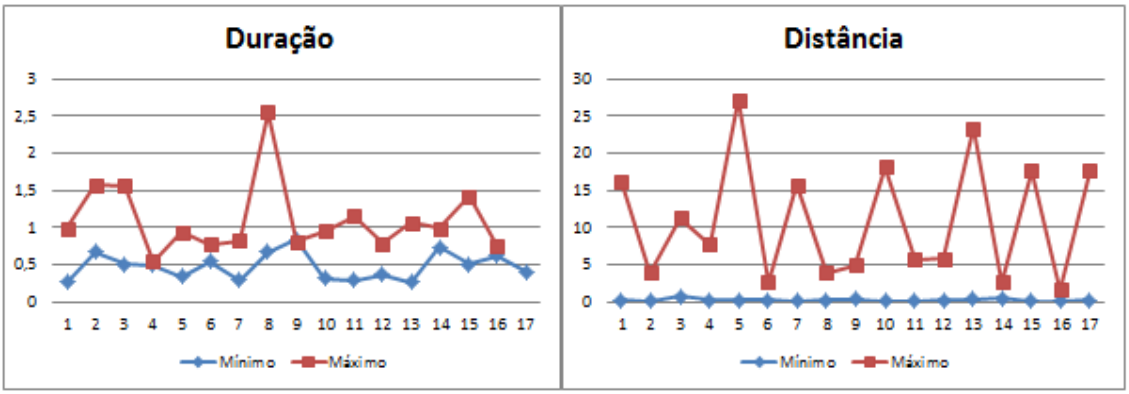

Figura 30 – Movimento Drag: Duração e Distância (Orientação: Oblíqua para baixo e direita)

Como se pode visualizar na Figura 31 alguns dos elementos são muito mais rápidos a descrever este tipo de movimento do que outros. Os elementos 5 e 13 são os que conseguem percorrer mais pixéis por segundo, porém os elementos 2, 6, 8, 9, 14 e 16 são bastante lentos em comparação aos outros. Com isto pode-se observar uma grande disparidade na rapidez com que os elementos efetuam este tipo de movimento.

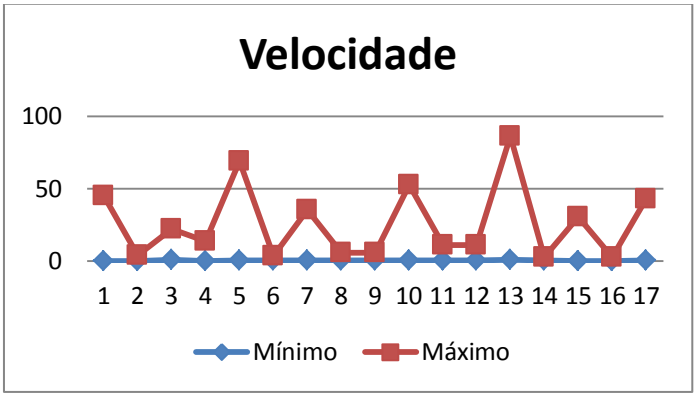

Figura 31 – Movimento Drag: Velocidade (Orientação: Oblíqua para baixo e direita)

Como se pode ver na Figura 32 os indivíduos começam e terminam o movimento em posições diferentes. Alguns elementos iniciam o movimento mais à direita e mais acima – indivíduos 4 10, 11, 12, 13, 14 e 16 -, enquanto outros iniciam o movimento mais à esquerda – 5, 9 e 15 - ,os elementos 1, 2, 3 são os que iniciam o movimento numa posição mais baixa do eixo do Y.

Consegue-se averiguar que alguns terminam o movimento mais acima ou abaixo do eixo do Y, ou seja, terminam em posições mais altas ou baixas do ecrã. Pode-se ainda observar que as posições intermédias são distinguíveis entre os indivíduos, ou seja, os pontos intermédios do movimento são diferentes de indivíduo para indivíduo.

Com isto pode-se verificar que os indivíduos podem ser distinguidos pelas posições que passam, ou seja, as coordenas são diferentes.

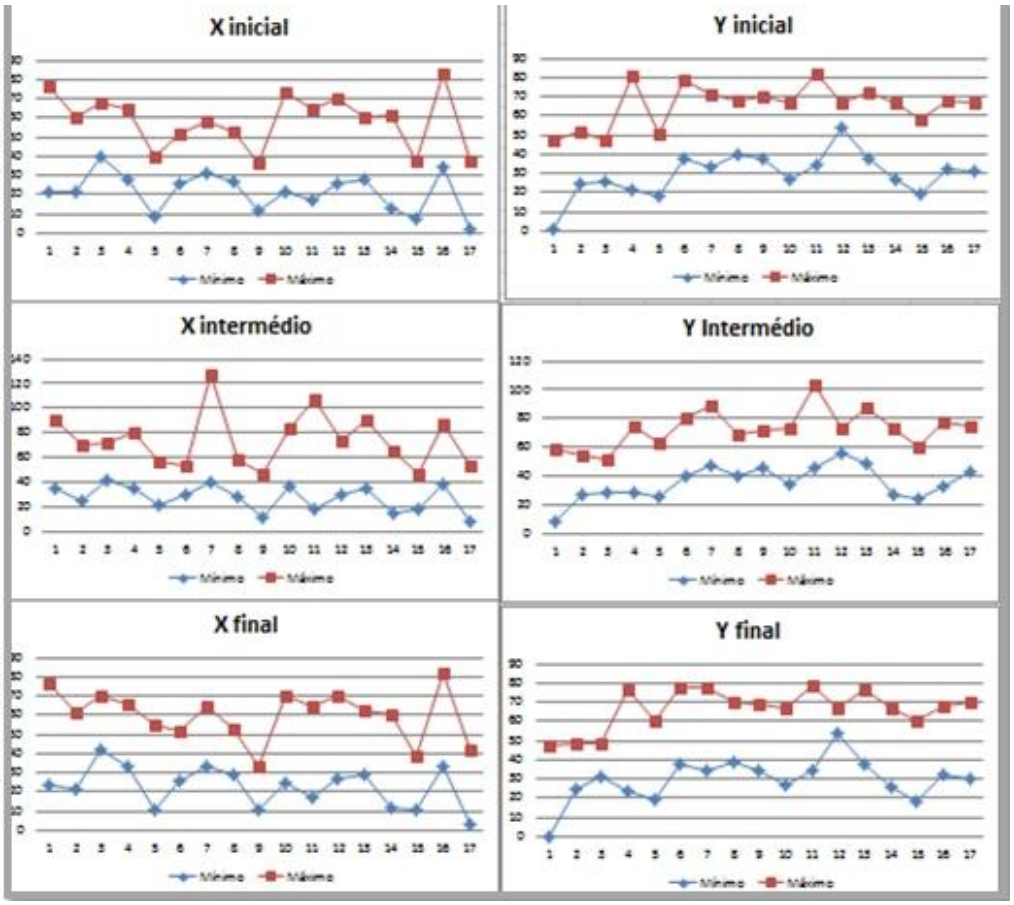

Figura 32 – Movimento Drag: Pressão (Orientação: Oblíqua para baixo e direita)

Orientação – Oblíqua (para cima e esquerda)

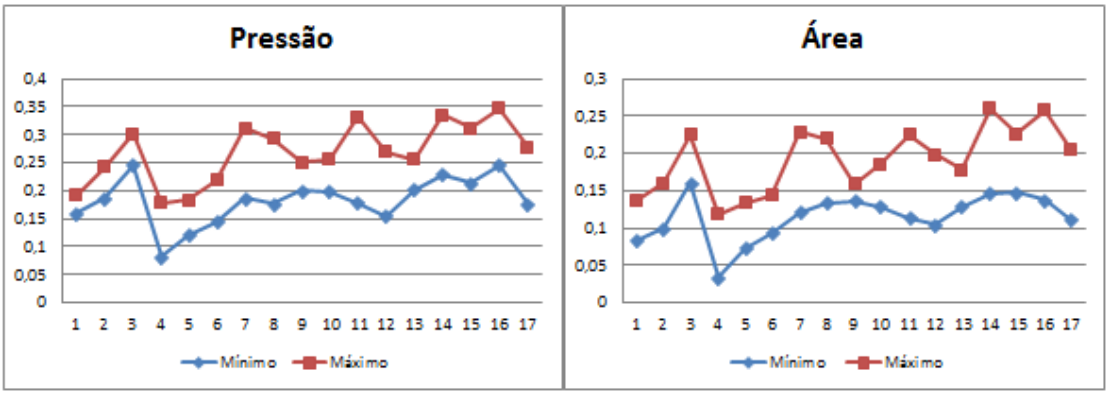

Figura 33 – Movimento Drag: Pressão e Área (Orientação: Oblíqua para cima e esquerda)

Como se pode observar na Figura 33 a pressão e a área estão correlacionadas e são distintas nos diferentes indivíduos. Como é visível nos gráficos os indivíduos 3, 7, 8, 11, 14 e 16 são os

que aplicam uma maior pressão e ocupam uma área de contato maior. Os indivíduos 1, 4, 5 e 6 aplicam uma pressão mais baixa e ocupam uma área menor.

Os indivíduos demoram tempos diferentes a arrastar um objeto de forma oblíqua para cima e para a esquerda. Como pode ser visto na Figura 34 o elemento 3 é o que demora mais tempo a descrever este tipo de movimento, por outro lado o elemento 5 é o que demora menos tempo a concluí-lo.

Em relação à distância percorrida, os elementos que possuem uma maior amplitude entre a distância máxima e mínima são o 1, 3, 4, 5 e 11. Como se pode ver na Figura abaixo, a distância percorrida é muito semelhante entre os indivíduos, ou seja, percorrem distâncias muito próximas.

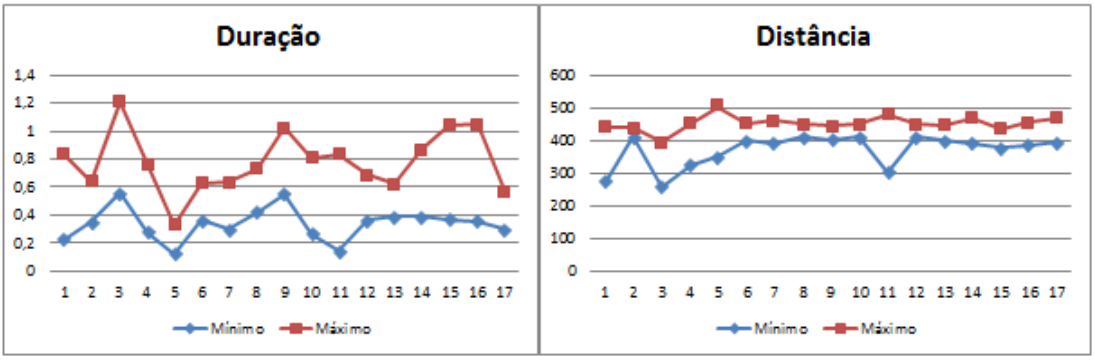

Figura 34 – Movimento Drag: Duração e Distância (Orientação: Oblíqua para cima e esquerda)

Dos indivíduos, o que percorre mais pixéis por segundo é o indivíduo 5, ou seja, é o elemento que efetua este movimento mais rapidamente. Por outro lado o indivíduo 3 e o 9 são os mais lentos. Como é visível na Figura 35 os indivíduos descrevem este tipo de movimento com velocidades diferentes, contudo a velocidade mínima não é muito discriminativa.

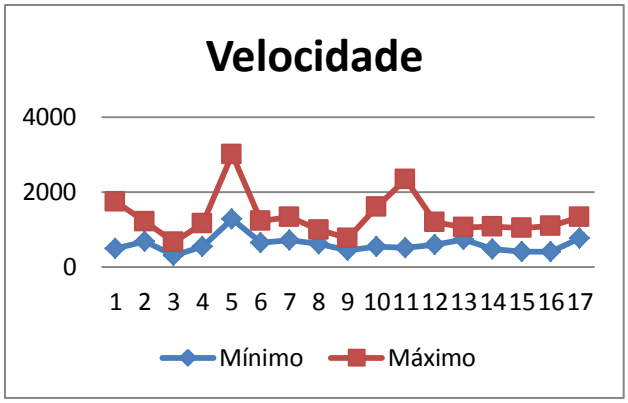

Figura 35 – Movimento Drag: Velocidade (Orientação: Oblíqua para cima e esquerda)

Como se pode ver na figura abaixo, os indivíduos passam por pontos diferentes, ou seja, iniciam e finalizam o movimento em posições distintas. Pode-se ver que uns indivíduo descrevem movimentos mais à esquerda e outros mais à direita, e uns iniciam e termina o movimento mais a cima ou mais abaixo do ecrã.

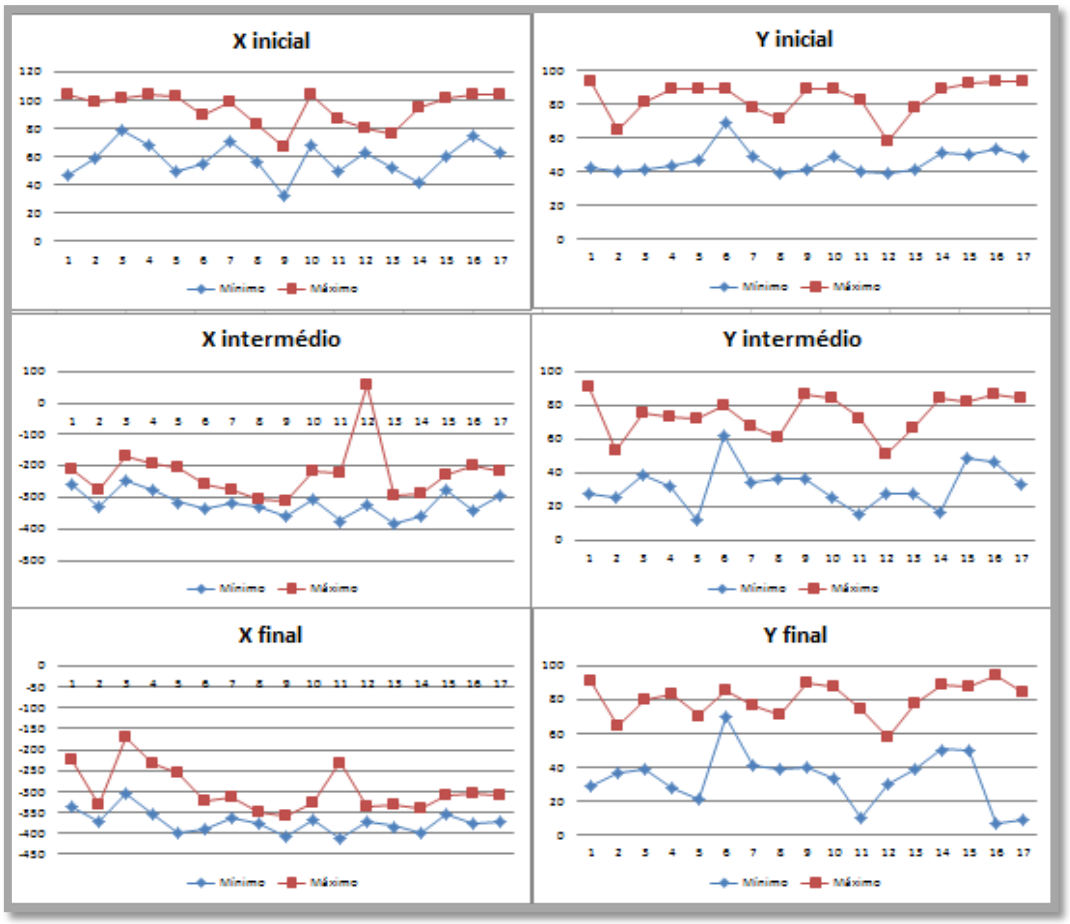

Figura 36 – Movimento Drag: X e Y (Orientação: Oblíqua para cima e esquerda)

Orientação – Oblíqua (para cima e direita)

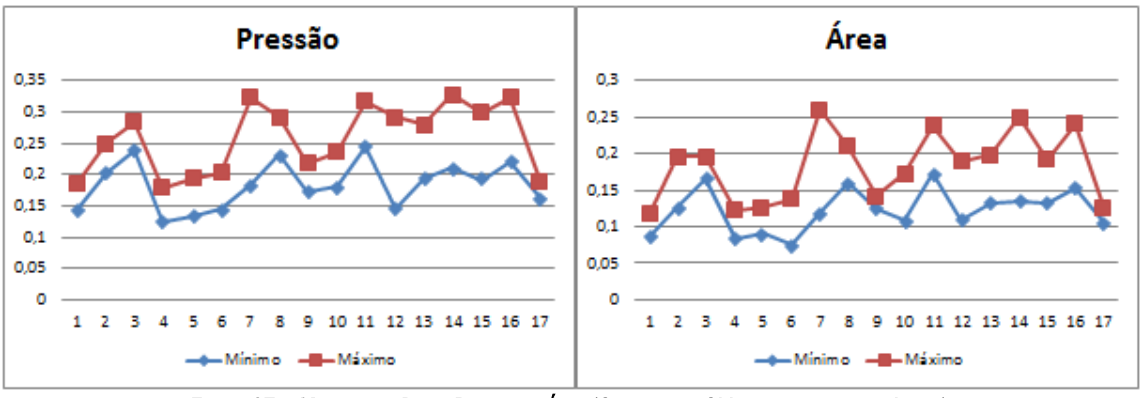

Figura 37 – Movimento Drag: Pressão e Área (Orientação: Oblíqua para cima e direita)

Como se pode ver na Figura 37 a pressão e a área são bastante distintivas entre os indivíduos. Como nos outros movimentos, pode-se confirmar a existência de interdependência entre estas variáveis. Ou seja, a área que os indivíduos ocupam está relacionada com a pressão que aplicam. Pode-se ver que quanto mais pressão aplicam maior é a área ocupada. Como se pode observar os indivíduos 1, 3, 4, 5 e 17 são os que efetuam movimentos com menos pressão e ocupam uma área menor de contato

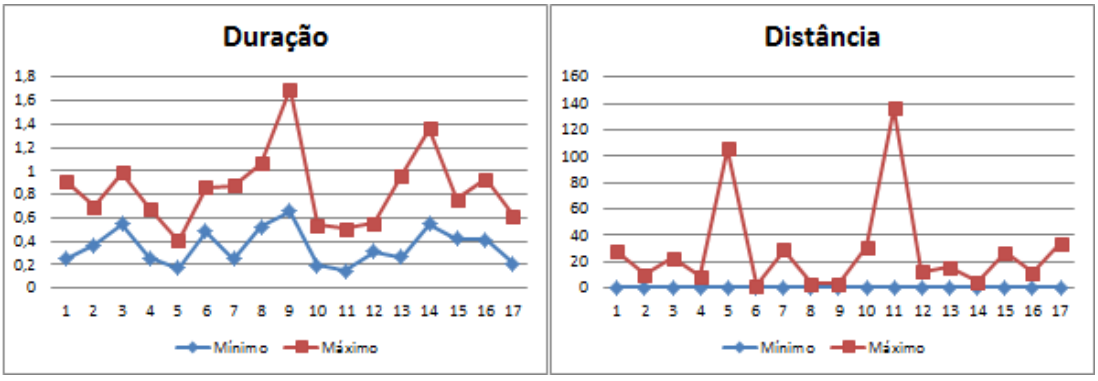

Figura 38 – Movimento Drag: Duração e Distância (Orientação: Oblíqua para cima e direita)

Em relação a duração deste movimento, pode-se visualizar alguma disparidade entre os diferentes indivíduos. Alguns elementos demoram muito tempo a efetuar o movimento, como é o caso do indivíduo 9 e o 14, por outro lado os indivíduos 5, 10, 11, 12 e 17 demoram menos tempo a finalizar o movimento.

Na Figura 38 é visível a distância máxima e mínima que os indivíduos percorrem, pode-se ver que a distância mínima é muito semelhante, porém a distância máxima é um pouco mais discriminativa, principalmente nos indivíduo 5 e 11.

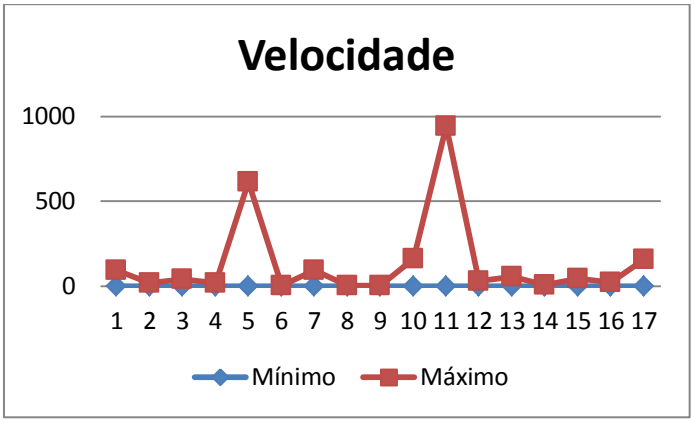

Figura 39 – Movimento Drag: Velocidade (Orientação: Oblíqua para cima e direita)

Este movimento não é muito discriminativo no que diz respeito à velocidade que os indivíduos efetuam o movimento, como se pode ver na Figura 39 os indivíduos percorrem uma distância por segundo muito próxima, apenas os indivíduos 5 e 11 se destacam com uma velocidade superior.

Da Figura 40, pode-se visualizar os valores máximos e mínimos das coordenadas inicias, intermédias e finais. Como se pode visualizar os indivíduos tocam o ecrã em posições diferentes para realizar o movimento. Por exemplo os elementos 8, 9, 14, 15 e 17 iniciam o movimento mais a esquerda, já os elementos 10 e 16 começam numa posição mais à direita. Os indivíduos 5 e 11 finalizam o movimento num valor mais baixo do eixo do Y.

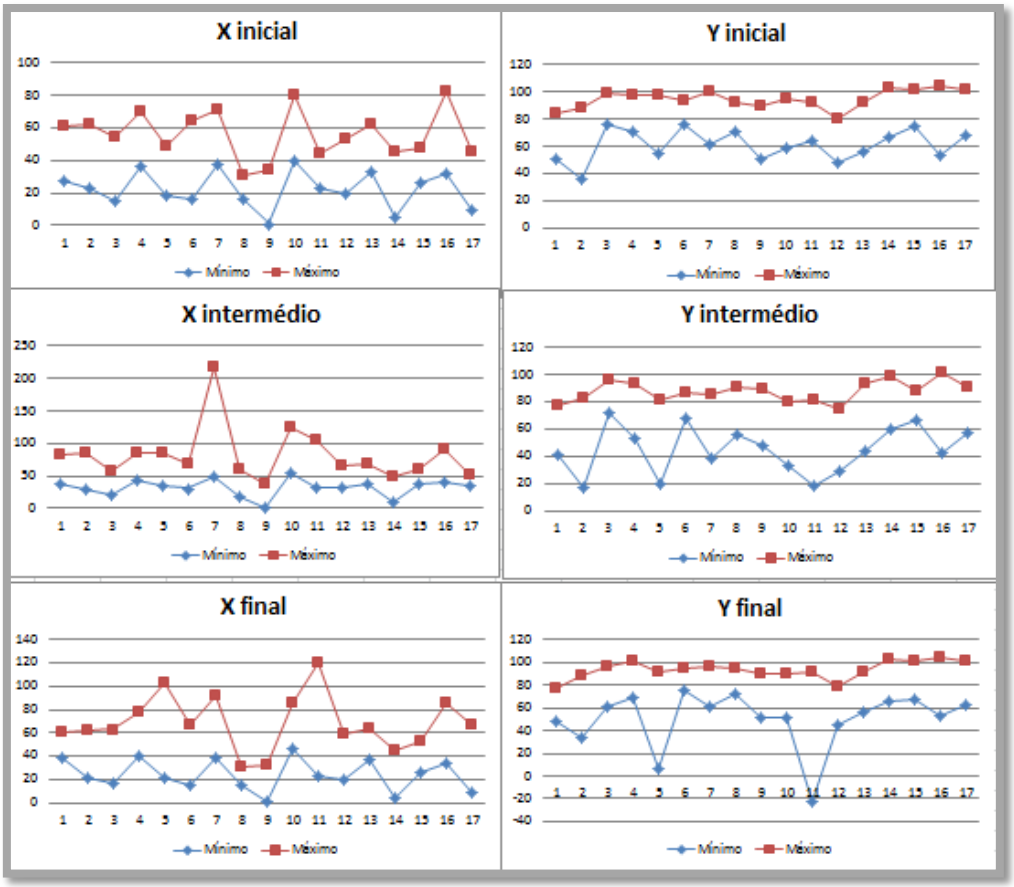

Figura 40 – Movimento Drag: X e Y (Orientação: Oblíqua para cima e direita)

De seguida é analisado o movimento *scroll* nas diferentes orientações. Ou seja analisa-se o movimento *scroll* com as orientações verticais (para cima e para baixo) e horizontais (para a direita e para a esquerda).

- Movimento Scroll

Orientação – Vertical para cima

Das Figura 41 é possível observar a relação entre a pressão e a área. Como se consegue ver os indivíduos que aplicam mais pressão ocupam uma área maior, e os que aplicam uma pressão menor ocupam uma área menor. Como se pode visualizar neste tipo de movimento, a amplitude entre os valores máximos e mínimos é menor do que no movimento *drag* (das diferentes orientações). Deste modo, os indivíduos são mais constantes valores da pressão e da área.

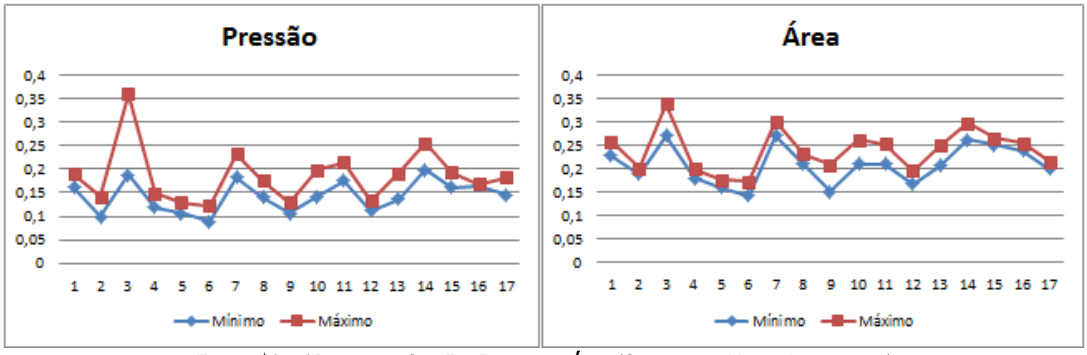

Figura 41 – Movimento Scroll: Pressão e Área (Orientação: Vertical para cima)

Os indivíduos demoram tempos distintos para realizar este tipo de movimento, como se pode ver na Figura 42 os indivíduos que demoram mais tempo a fazer o *scroll* para cima são o 3 e o 15; os elementos 1, 4, 9 e 10 demoram um pouco menos do que os indivíduos anteriores; os indivíduos que demoram menos tempo a efetuar este tipo de movimentos são o 2, 5, 6, 7, 8, 11, 12, 13, 14, 16 e 17. Como se pode ver na Figura 42, os indivíduos realizam movimentos com comprimentos diferentes. Alguns efetuam movimentos curtos – 2, 7 e 12 -, enquanto outros traçam movimentos compridos – 1, 3, 15, 16 e 17.

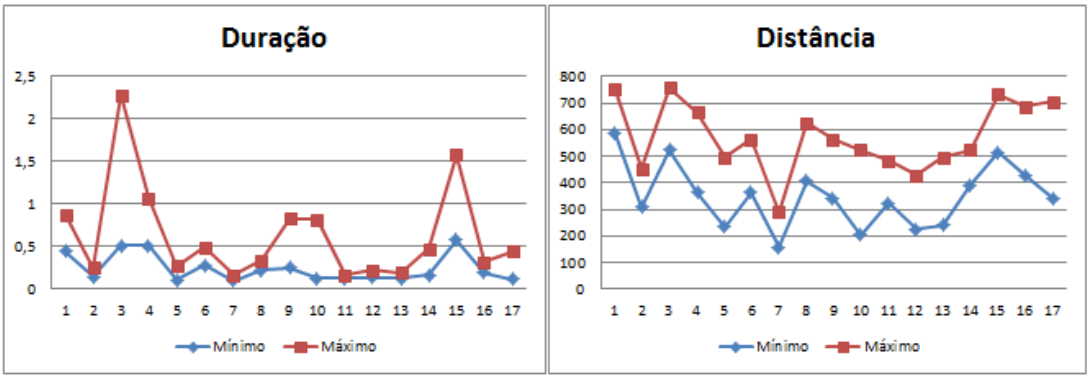

Figura 42 – Movimento Scroll: Duração e Distância (Orientação: Vertical para cima)

Como se pode ver na Figura 43, alguns indivíduos são mais rápidos do que outros a descrever este tipo de movimento. Deste modo é possível distinguir velocidades distintas para indivíduos diferentes. No gráfico é possível identificar os indivíduos que aplicam uma velocidade inferior – indivíduos 3, 4 e 15 – e os que aplicam uma velocidade superior – 5 e 6.

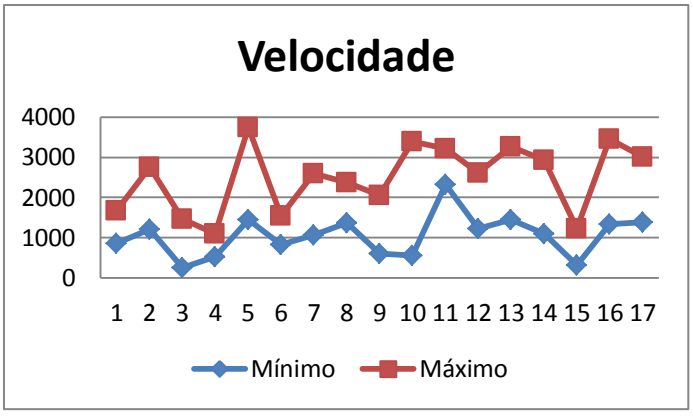

Figura 43 – Movimento Scroll: Velocidade (Orientação: Vertical para cima)

Na Figura 44, é possível verificar que os indivíduos traçam os movimentos por pontos diferentes, ou seja, iniciam e terminam o movimento em posições diferentes.

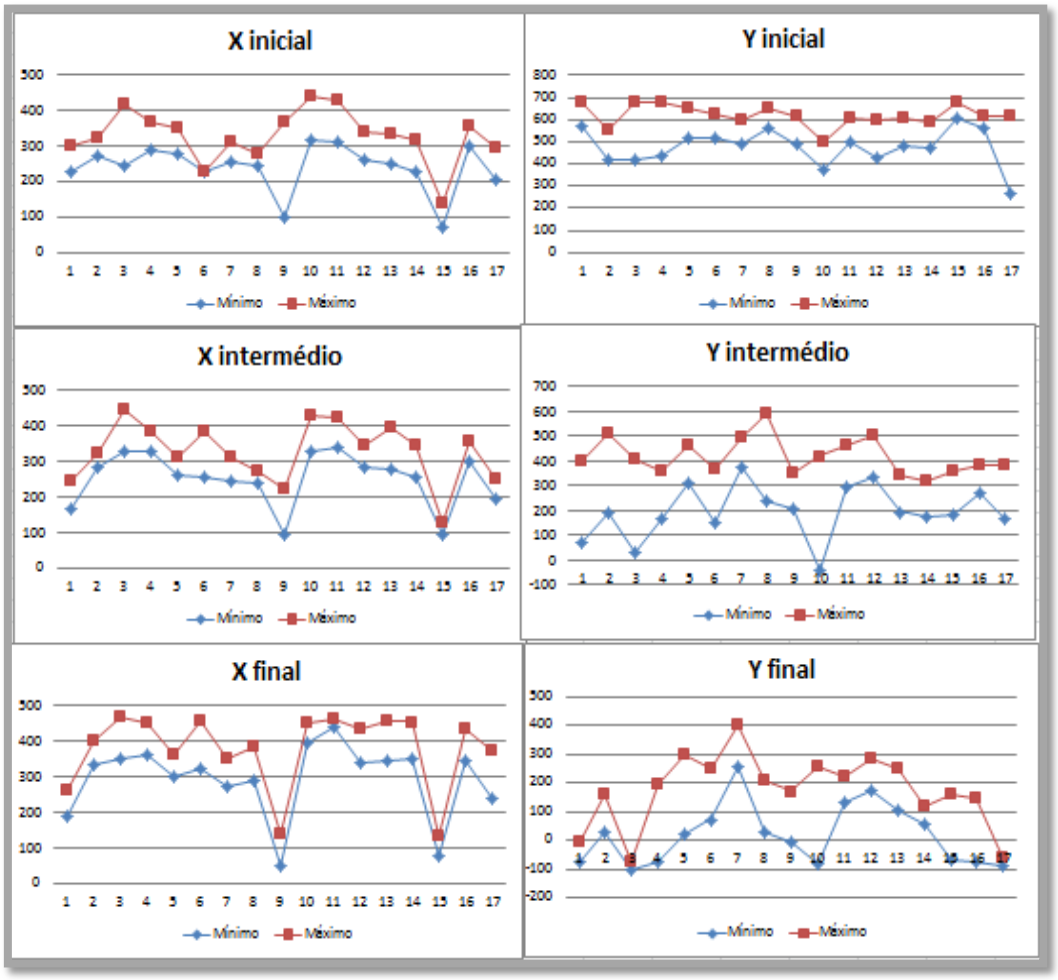

Figura 44 – Movimento Scroll: X e Y (Orientação: Vertical para cima)

Como se pode observar o indivíduo 15 é o que inicia o movimento mais a esquerda, por outro lado o indivíduo 10 é o que inicia o movimento mais à direita. É possível ainda observar os indivíduos que iniciam o movimento mais acima ou abaixo, ou seja, alguns indivíduos iniciam mais acima do eixo do Y e outros mais a baixo.

Orientação – Vertical para baixo

Como se pode ver na Figura 45 os indivíduos possuem padrões bastante definidos em relação à área que ocupam e pressão que aplicam. É visível uma pequena discrepância entre os valores máximos e mínimos, ou seja, os indivíduos não variam grandemente nos valores de pressão e área. Pode-se ainda observar que os indivíduos 3 e 15 são os que aplicam uma pressão mais elevada e ocupam uma área maior do ecrã. Por outro lado os que aplicam uma pressão mais baixa são o 4, 5 e 6, este são também os que ocupam uma área menor.

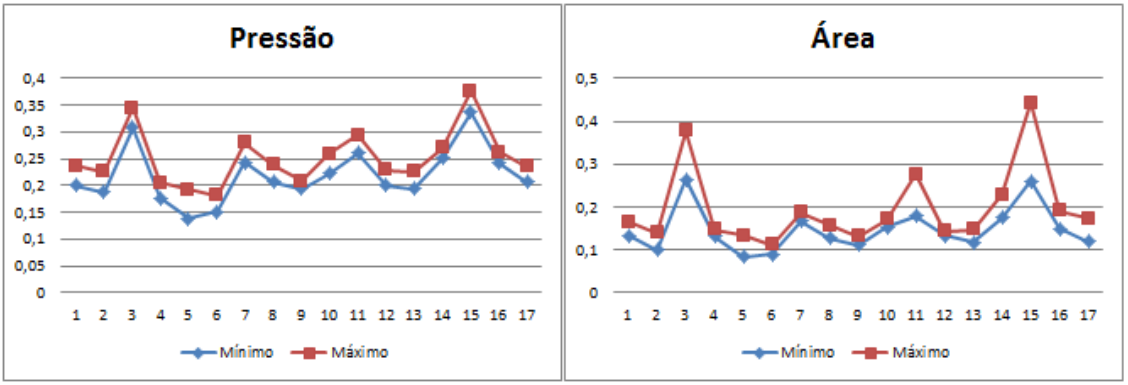

Figura 45 – Movimento Scroll: Pressão e Área (Orientação: Vertical para baixo)

No gráfico da área é possível observar que os indivíduos 3, 11 e 15 são os que variam mais na área que cobrem do ecrã. Apesar da pressão e da área serem valores bastante discriminativos, o tempo que os indivíduos demoram a fazer o *scroll* para baixo não é tao distintivo. Como se pode ver na Figura 46 o elemento que demora mais tempo a fazer este tipo de movimento é o 3.

Em relação a distância percorrida, consegue-se observar que os indivíduos efetuam movimentos com comprimentos diferentes. Deste modo, o indivíduo que efetua movimentos mais curtos é o 7. Pelo contrário o que descreve movimentos mais compridos é o 8. Pode-se observar que a amplitude entre a distância máxima e mínima é bastante elevada neste tipo de interação, como

se pode ver na Figura abaixo os elementos 1 e 15 são os que possuem uma maior amplitude, e por outro lado o indivíduo 7 é o que possui uma menor amplitude.

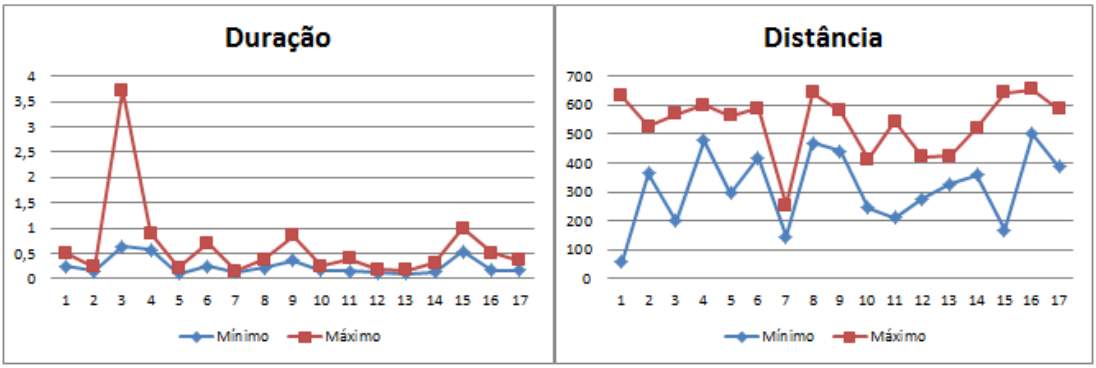

Figura 46 – Movimento Scroll: Duração e Distância (Orientação: Vertical para baixo)

Como se pode observar na Figura 47 os indivíduos possuem velocidades diferentes, ou seja, é possível verificar que uns indivíduos fazem este movimento de forma mais rápida do que outros. Pode-se ver que os indivíduos 3, 4, 9 e 15 são os mais lentos a efetuar este tipo de movimento.

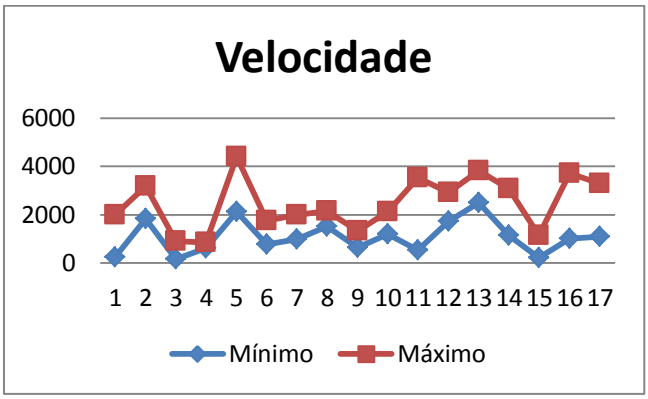

Figura 47 – Movimento Scroll: Velocidade (Orientação: Vertical para baixo)

É possível visualizar, na Figura 48, os valores máximo e mínimos das posições iniciais, intermédias e finais que os indivíduos descrevem.

Pode-se observar que os indivíduos passam por posições diferentes, estes iniciam e terminam o movimento em posições bastante distintas. Consegue-se visualizar que alguns indivíduos iniciam o movimento mais a esquerda – 9 e 15 -, enquanto outros iniciam mais à direita – 4, 6 e 12 -.

Pode-se ainda visualizar que os uns indivíduos iniciam o movimento no Y mais elevado – 3 e 11 - , e outro numa posição mais baixa - 1, 6 e 15 -.

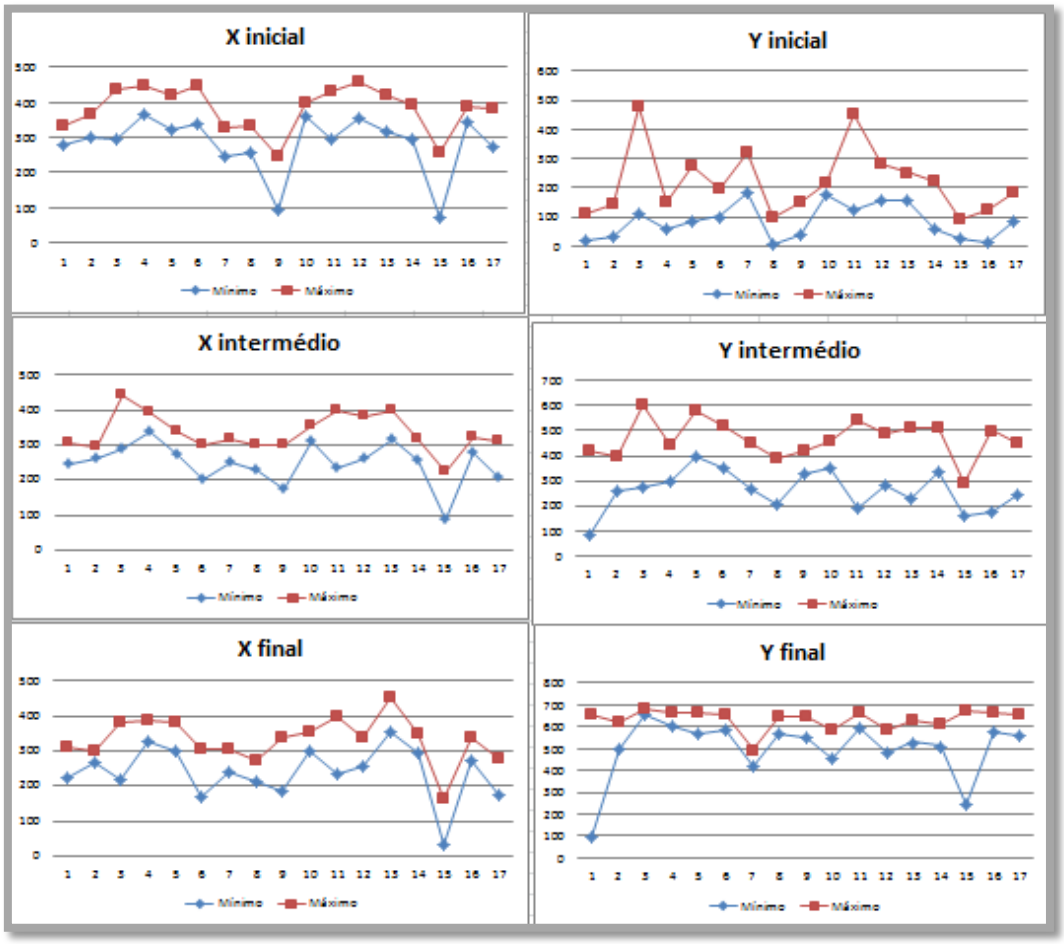

Figura 48 – Movimento Scroll: X e Y (Orientação: Vertical para baixo)

Orientação – Horizontal para a esquerda

No movimento, *scroll* para a esquerda, é possível observar que as pressões e áreas são distintas para os diferentes indivíduos. Na Figura 49 pode-se visualizar que os indivíduos que aplicam uma maior pressão ocupam mais área de contato, por outro lado os indivíduos que aplicam uma pressão menor ocupam uma área menor.

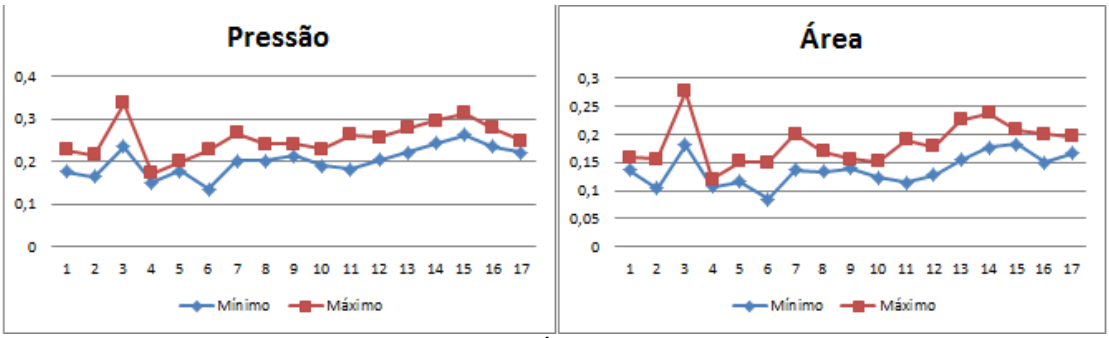

Figura 49 – Movimento Scroll: Pressão e Área (Orientação: Horizontal para a esquerda)

Em relação à duração do movimento, pode-se observar uma grande disparidade entre os valores máximos. Alguns indivíduos demoram menos de meio segundo a efetuar o movimento, enquanto outros chegam a demorar mais de segundo e meio.

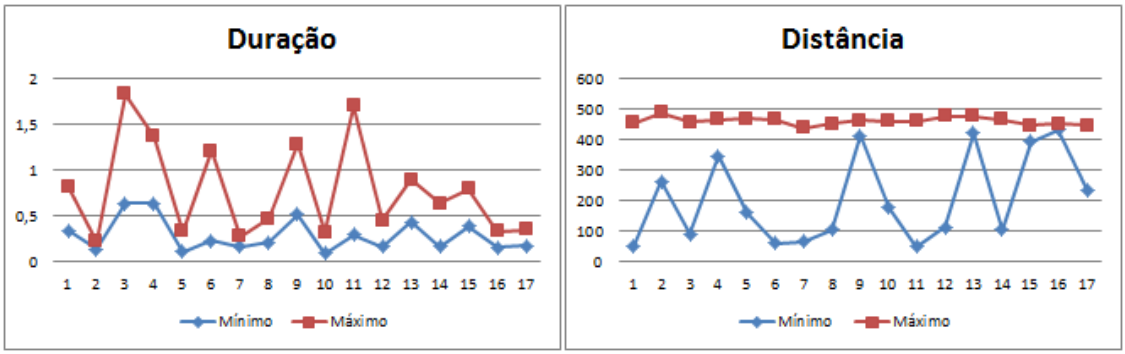

Figura 50 – Movimento Scroll: Duração (Orientação: Horizontal para a esquerda)

Na Figura 50, é possível observar que a distância máxima que os indivíduos percorrem é muito semelhante, contudo as distâncias mínimas são bastante díspares. Pode-se observar que os elementos 9, 13, 15 e 16 não variam muito na distância que percorrem. Ou seja, efetuam movimentos com comprimento bastante constante.

Da Figura 51, consegue-se observar que os indivíduos 2, 5 e 16 são os que conseguem efetuar este movimento com maior rapidez. Por outro lado os indivíduos 1, 3, 4, 6 e 9 são os que demoram mais tempo.

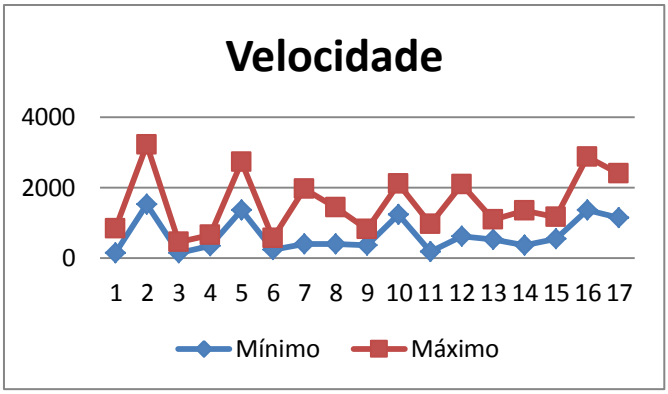

Figura 51 – Movimento Scroll: Velocidade (Orientação: Horizontal para a esquerda)

Da Figura abaixo, pode-se verificar que os valores do eixo do Y não são tão distintivos como os do eixo do X. Contudo a posição inicial máxima do X não é muito diferenciativa. Pode-se observar que a posição intermédia do x distingue bastante os indivíduos. É ainda observável que as posições finais são muito semelhantes entre os indivíduos.

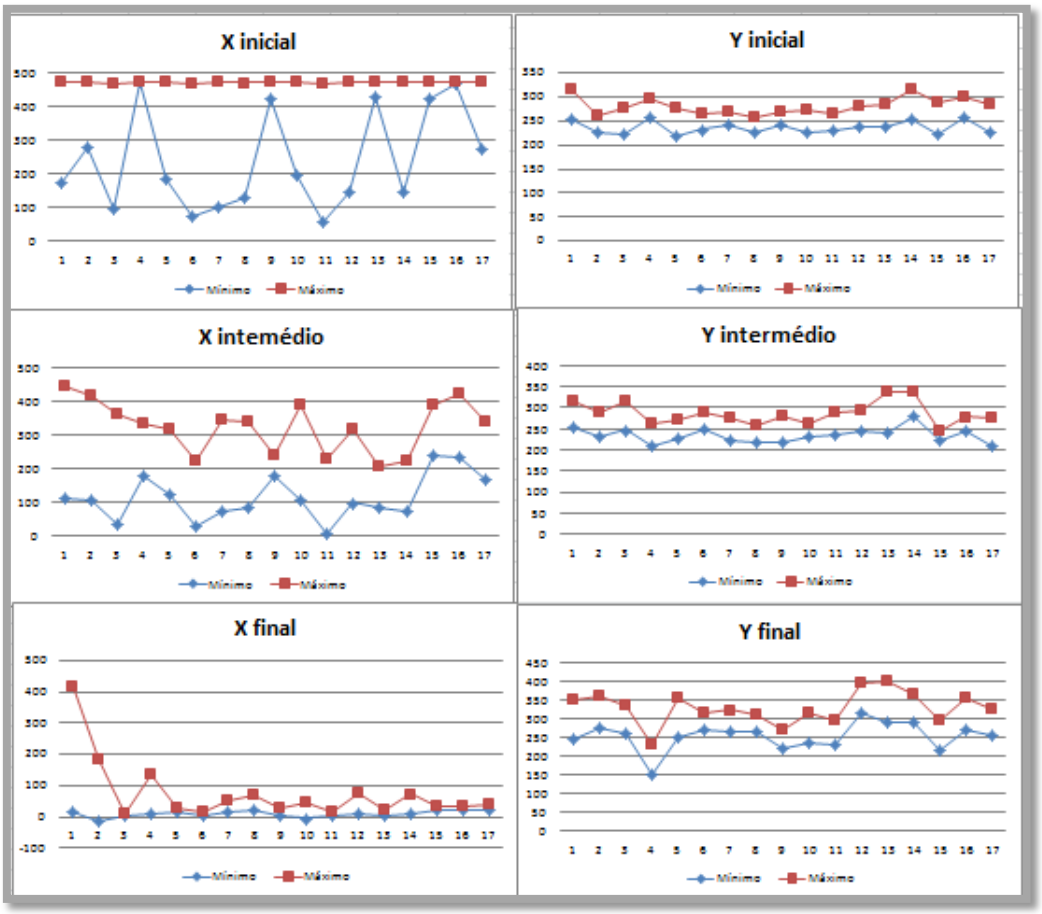

Figura 52 – Movimento Scroll: X e Y (Orientação: Horizontal para a esquerda)

Orientação – Horizontal para a direita

Como é visível na Figura 53 os indivíduos aplicam uma pressão muito semelhante entre eles, assim como a área que ocupam. Pode-se observar que o indivíduo que aplica uma pressão maior e ocupa uma maior área do ecrã é aquele que se distingue mais dos outros indivíduos.

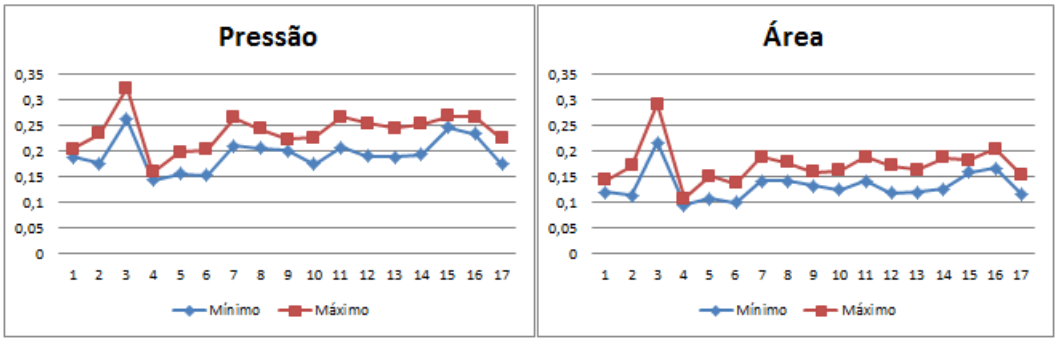

Figura 53 – Movimento Scroll: Pressão e Área (Orientação: Horizontal para a direita)

Relativamente à duração do movimento pode-se observar tempos diferentes para os elementos. Como se pode observar na Figura 54 os indivíduos 3 e 6 demoram mais tempo a concluir o movimento, e possuem uma grande amplitude entre duração máxima e mínima.

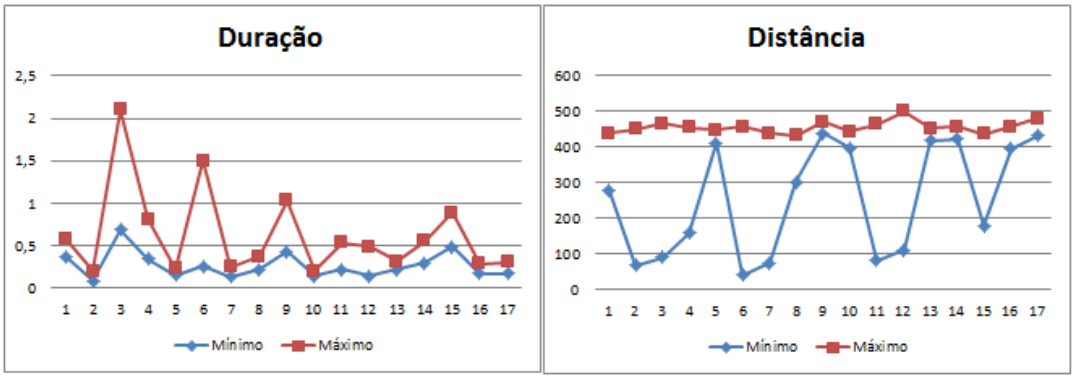

Figura 54 – Movimento Scroll: Duração e Distância (Orientação: Horizontal para a direita)

Na Figura acima, pode-se observar que a distância máxima que os indivíduos percorrem encontra-se bastante próxima, contudo os valores mínimos estão bastante distanciados. Pode-se

observar que os elementos que efetuam movimentos mais curtos são o 2, 3, 6, 7, 11 e 12, por outro lado, os indivíduos 5,9,10, 13, 14, 16 e 17 são os que percorrem distâncias maiores.

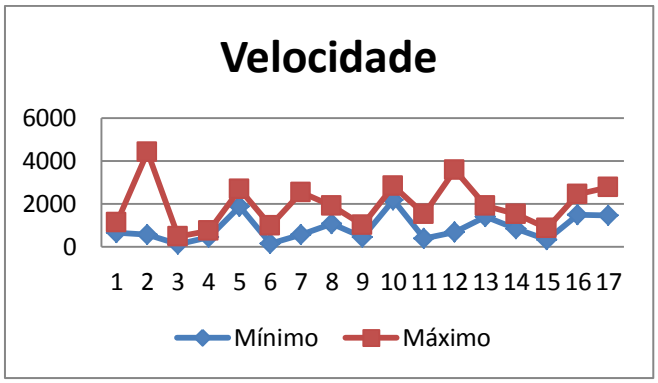

Figura 55 – Movimento Scroll: Velocidade (Orientação: Horizontal para a direita)

No que diz respeito à velocidade, pode-se visualizar que os indivíduos 2, 5, 7, 8, 10, 12, 16 e 17 são os que conseguem atingir uma maior velocidade neste tipo de movimento. Por outo lados os elementos 1, 3, 4, 6, 9 e 15 são os que atingem uma menor velocidade.

Da Figura 56, pode-se visualizar que o X inicial mínimo é muito próximo nos indivíduos, contudo o valor máximo é bastante diferenciativo. Consegue.se ver que o valor do X intermédio é bastante díspar entre os indivíduos, porém o X final e muito semelhante. É ainda possível observar que o valor do Y é mais diferenciativo do que o valor de X.

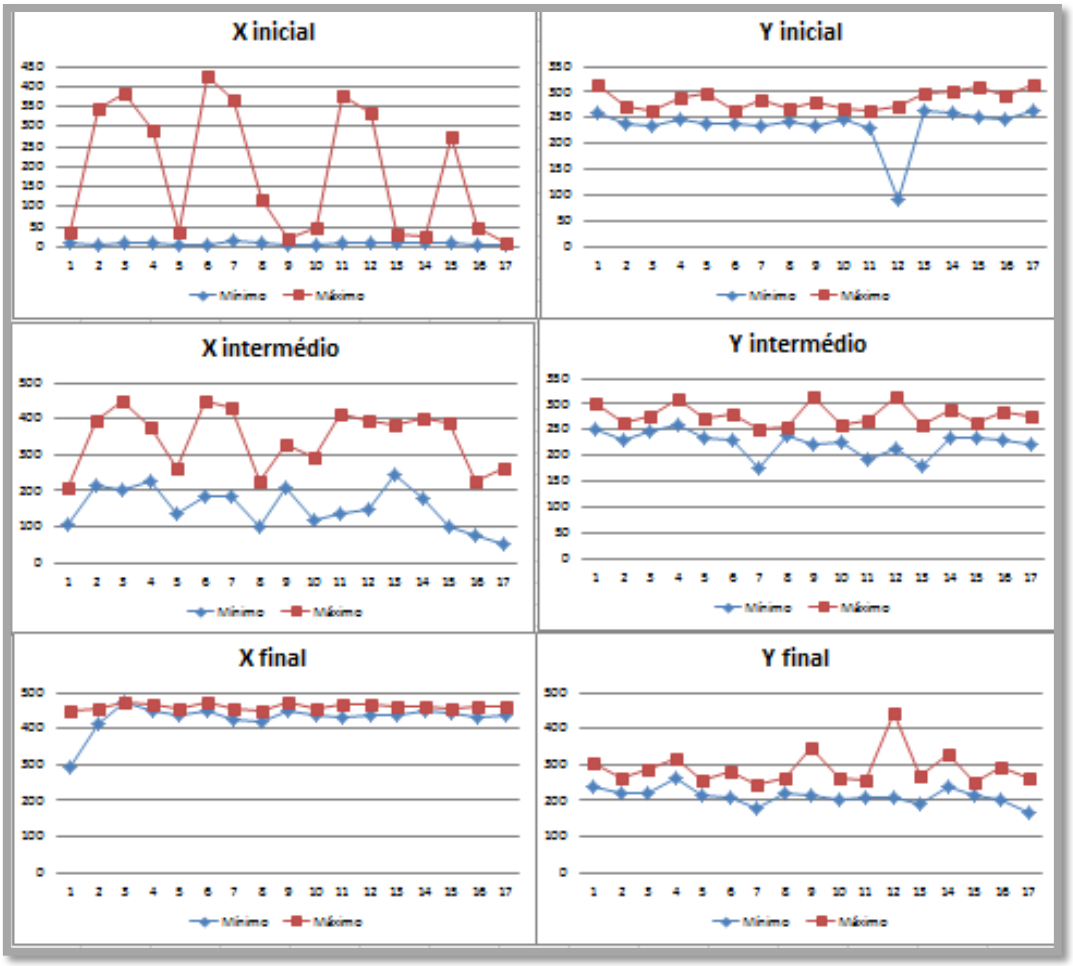

Figura 56 – Movimento Scroll: X e Y (Orientação: Horizontal para a direita)

De seguida é apresentada a análise da interação Tap. Esta não possui orientação.

- Movimento Tap

Como se pode ver na Figura 57, os indivíduos aplicam pressões diferentes ao efetuar uma interação deste género. Pode-se observar que o indivíduo 16 é o que aplica uma pressão maior. Por outro lado o indivíduo 4 é o que aplica uma pressão menor.

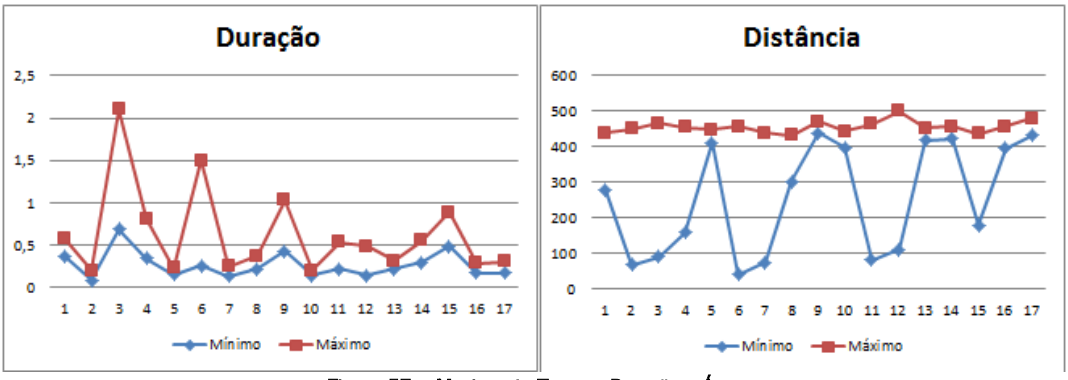

Figura 57 – Movimento Tap: Pressão e Área

Pode-se observar que as áreas de contato são distintas para os diferentes indivíduos. Pode-se ainda visualizar que os indivíduos que aplicam uma pressão mais elevada no ecrã.

Relativamente à duração do movimento, pode-se observar que os indivíduos 1, 3, 4, 15 e 16 são os que demoram mais tempo a realizar o movimento e que possuem uma maior discrepância com os outros elementos. Pode-se também observar que os outros indivíduos demoram tempos bastante próximos uns dos outros. Ou seja, não são valores muito discriminativos - ver Figura 58.

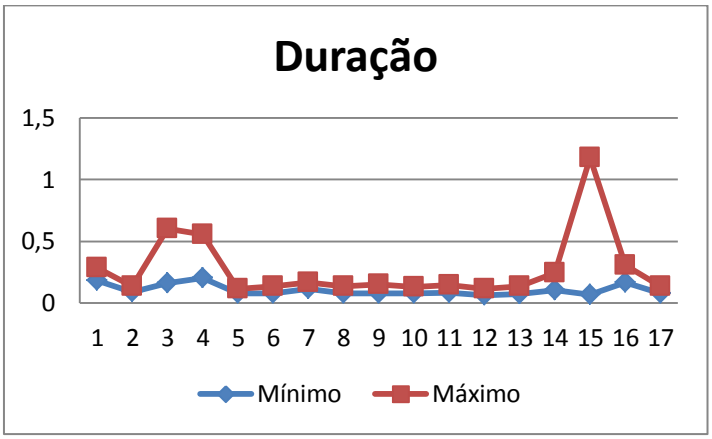

Figura 58 – Movimento Tap: Duração

Neste tipo de interação, os indivíduos não efetuam movimento, ou seja, iniciam e terminam a interação na mesma posição.

Da Figura 59, pode-se observar que os indivíduos iniciam e finalizam o movimento em posições diferentes. Como se pode observar uns indivíduos iniciam interação mais à direita, enquanto outros iniciam mais à esquerda. Pode-se ainda visualizar que uns indivíduos iniciam o movimento mais abaixo do que outros.

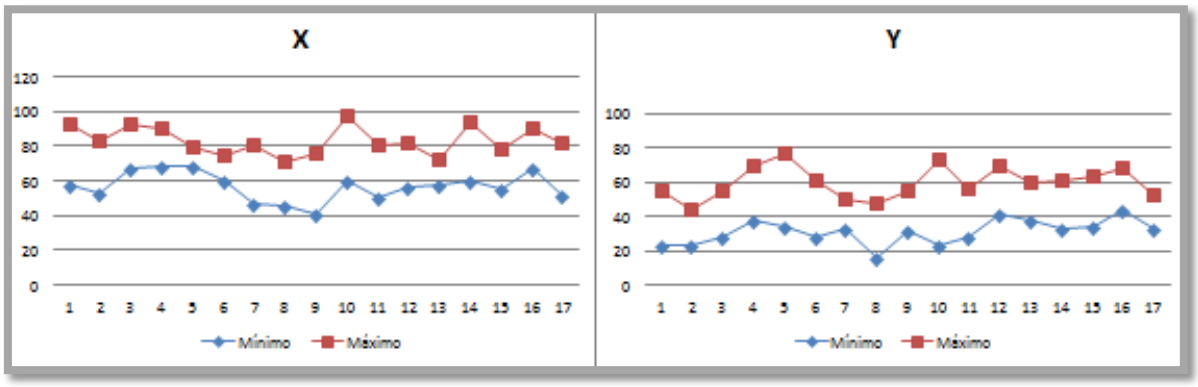

Figura 59 – Movimento Tap: X e Y

Da análise aos diferentes movimentos, foi possível identificar padrões diferentes para os indivíduos. Como se pôde observar os indivíduos possuem características diferentes nas diferentes interações.

3.3.1 Variáveis versus características dos indivíduos

Nesta secção é analisada a correlação entre as variáveis – pressão, área, duração, distância e velocidade – e as características dos indivíduos – idade, a experiência que possuem a lidar com tecnologias e os dedos que usam para interagir com o dispositivo -.

Para as variáveis foi calculada a média que cada indivíduo aplica nos três tipos de interações. As caraterísticas dos indivíduos podem ser visualizadas em anexo - Anexo II.

- Movimento Drag

Da Figura 60, pode-se observar que a experiência com tecnologias não é muito relevante para a pressão, pois tanto os indivíduos com mais de 10 e menos de 10 anos de experiência aplicam pressões elevadas. Contudo pode-se observar que os elementos com mais de 10 anos de experiência aplicam uma pressão superior a 0,2 (exceto o elemento 9). Os elementos com menos de 10 anos de experiências possuem pressões muito distintas. Pode-se ver que os indivíduos que possuem uma menor pressão têm pouca experiência e mais de 50 anos (exceto o 3 e 15). Assim, possuir mais experiência não implica aplicar uma menor pressão e vice-versa.

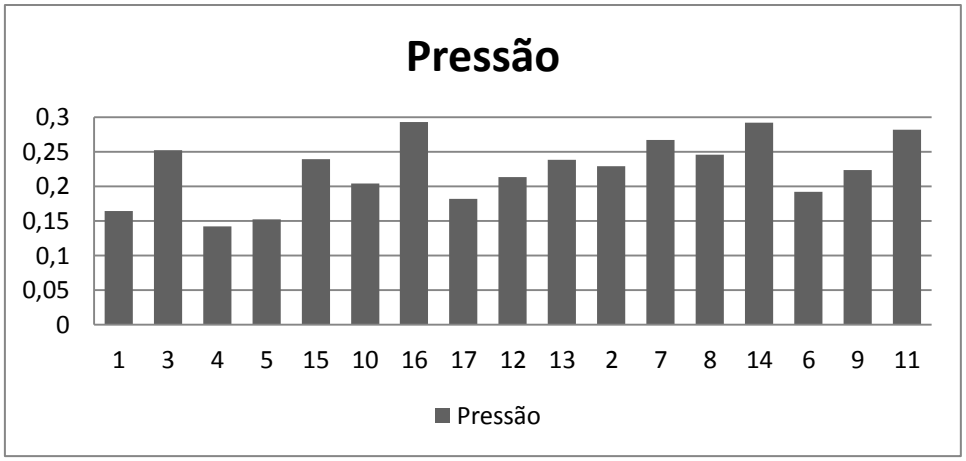

Figura 60 – Movimento Drag: Pressão

Em relação aos dedos utilizados na interação pode-se visualizar que os indivíduos que utilizam o dedo indicador atingem valores muito próximos dos que usam o polegar, ou seja, os dedos que usam não é imperativo na pressão aplicada. Como se pode ver os indivíduos 16, 7, 14 e 11 usam dedos diferentes e aplicam pressões muito próximas. Ou seja, usar o polegar não implica maior pressão do que usar o indicador ou dedo médio.

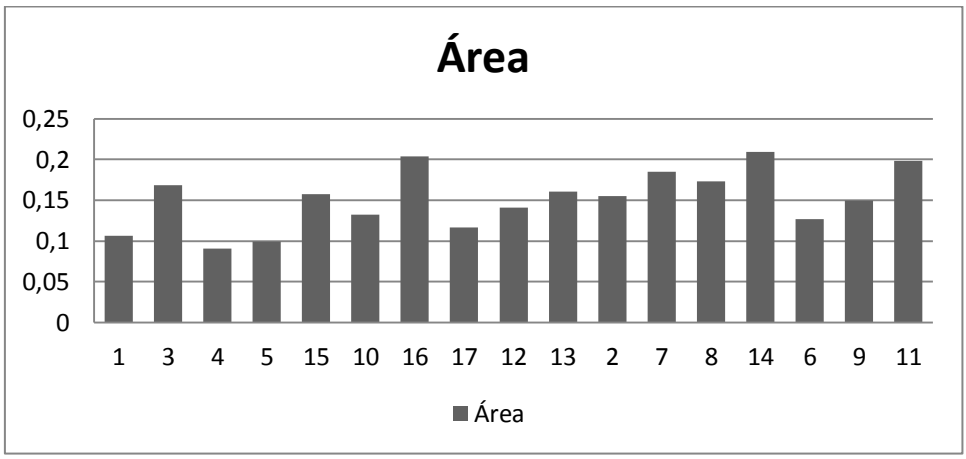

Figura 61 – Movimento Drag: Área

O dedo que o utilizador usa não tem influência na área que ocupa do ecrã. Como se pode ver na Figura 61 os indivíduos que usam o dedo indicador conseguem ocupar áreas semelhantes aos que usam o polegar. Pode-se ainda ver que o indivíduo 9 (usa polegar) ocupa uma área relativamente pequena e inferior ao indivíduo 11 (usa indicador).

O que influencia a área que o indivíduo ocupa é a pressão. Como se pode ver na Figura 60 e na Figura 61 os indivíduos que aplicam uma área maior são também os que ocupam uma maior área.

Da Figura 62, pode-se observar que os indivíduos com mais experiência demoram mais tempo a finalizar este tipo de movimento. Deste modo, ter mais experiência não implica efetuar este tipo de interação de forma mais rápida, como se pode ver o indivíduo 9 têm mais de 10 anos de experiência e têm menos de 25 anos, contudo é o elemento mais lento.

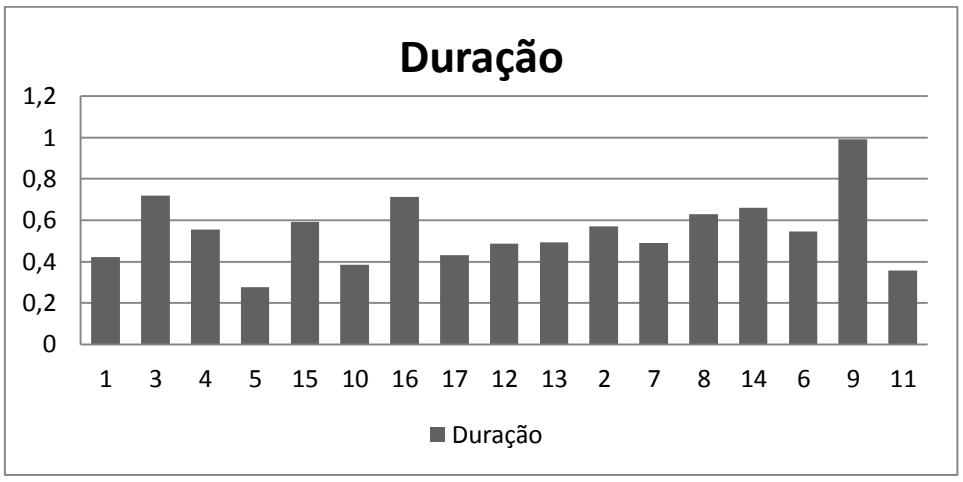

Figura 62 – Movimento Drag: Duração

Como se pode ver na Figura 63, os indivíduos percorrem uma distância média muito semelhante entre eles. Assim sendo, a distância não é afetada pela idade, experiência e dedos usados.

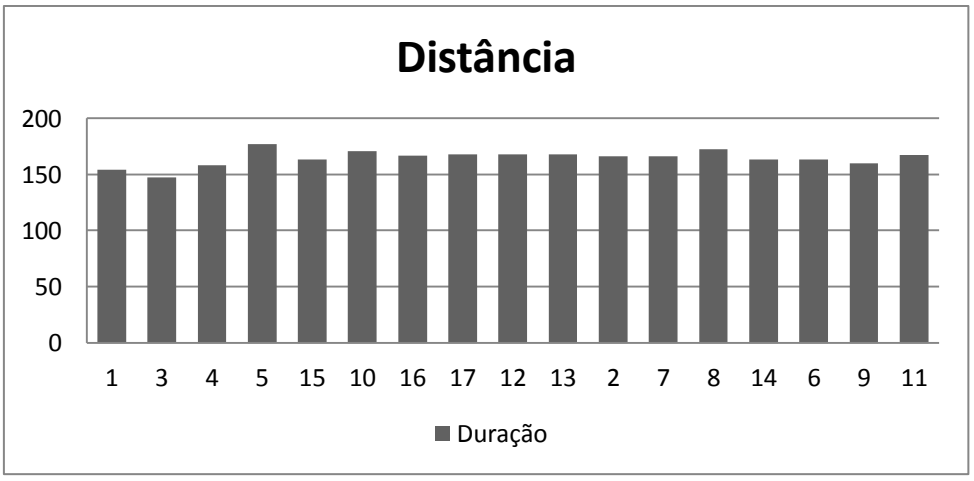

Figura 63 – Movimento Drag: Distância

Do gráfico da velocidade é possível observar que os indivíduos que descrevem este tipo de movimento mais lentamente têm uma experiência inferior a 10 anos. Deste grupo, os indivíduos que são mais lentos têm idade superior a 25 anos. Excetuando o indivíduo 9, todos os indivíduos que possuem uma experiência superior a 10 anos, conseguem percorrer pelo menos 300 pixéis por segundo.

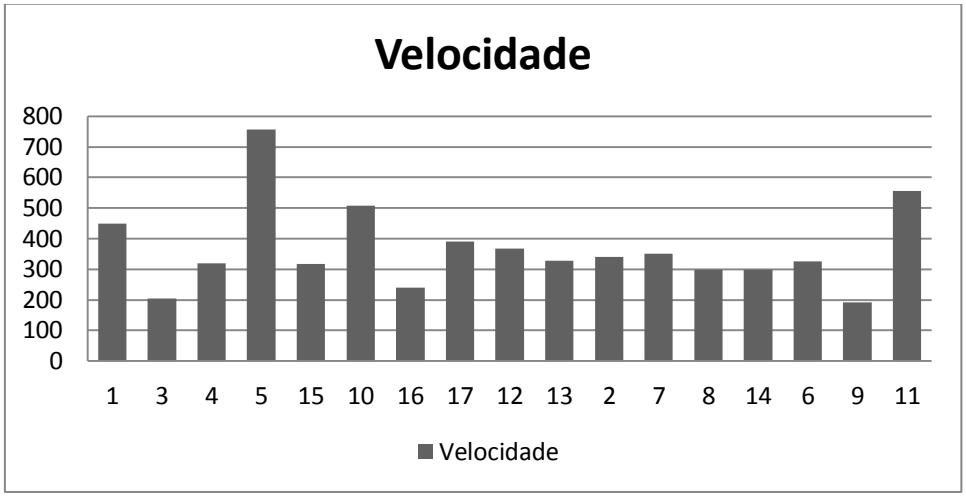

Figura 64 – Movimento Drag: Velocidade

Pode-se verificar que ter mais experiência com tecnologias não implica ser mais rápido, pois como se pode ver o indivíduo 5 é o mais rápido e não possui muita experiência, por outro lado o indivíduo 9 possui mais experiência e é o elemento mais lento.

- Movimento Scroll

Tal como no movimento *Drag*, a experiência que os indivíduos possuem não é relevante para a pressão aplicada. Como se pode ver na Figura 65 os indivíduos com mais experiência aplicam pressões tao elevadas como os que não tem tanta experiência. A idade também não é um fator importante, pois como se pode ver, os indivíduos 3, 4, 5 e 15 são os que aplicam maior e menor pressão do grupo e possuem todos a mesma faixa etária.

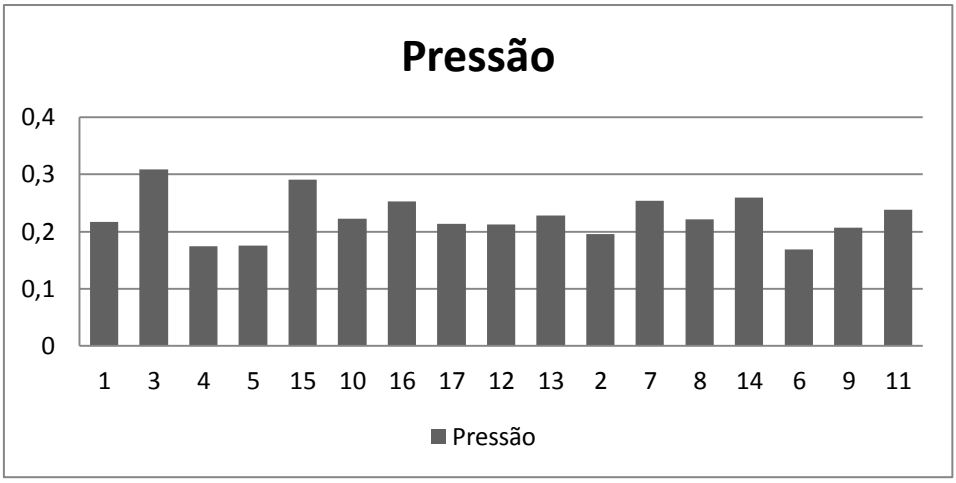

Figura 65 – Movimento Scroll: Pressão

A área de contato deste movimento não está relacionada com o dedo que o indivíduo usa. Como se pode ver os indivíduos 3, 15, 14 e 11 usam o dedo indicador e ocupam uma maior área do que os indivíduos 16, 7 e 9, que usam o polegar.

Tal como o movimento Drag, esta variável está correlacionada com a pressão. Como se pode ver, os indivíduos aumentam a área de contato consoante a pressão que aplicam, ou seja, quanto mais pressiona o ecrã maior é a área de contato.

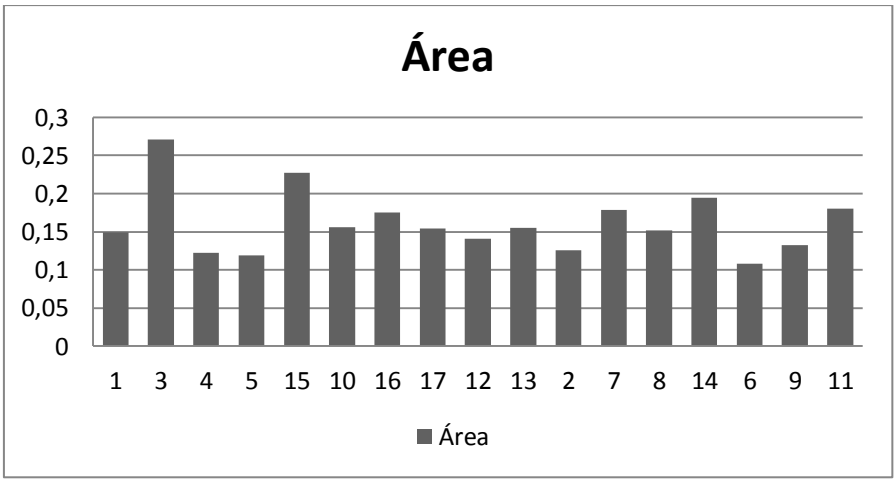

Figura 66 – Movimento Scroll: Área

Pode-se observar na Figura 67, que os indivíduos que demoram mais tempo a efetuar este tipo de movimento têm idade superior a 50 anos e experiência inferior a 10 anos. Porém os

indivíduos com idade inferior a 25 anos e experiência superior a 10 anos também efetuam movimentos lentos.

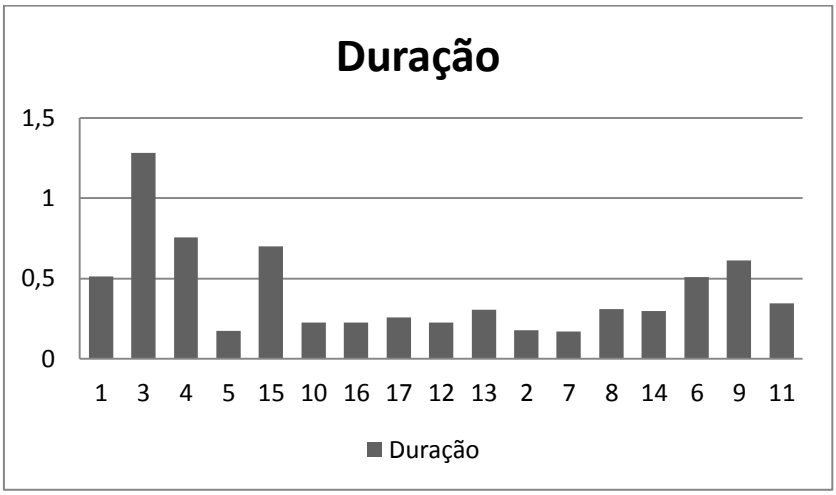

Figura 67 – Movimento Scroll: Duração

Os indivíduos que efetuam movimentos mais compridos têm experiência inferior a 10 anos, por outro lado os indivíduos com mais experiência efetuam movimentos mais curtos. Deste modo a experiência influência o comprimento dos movimentos.

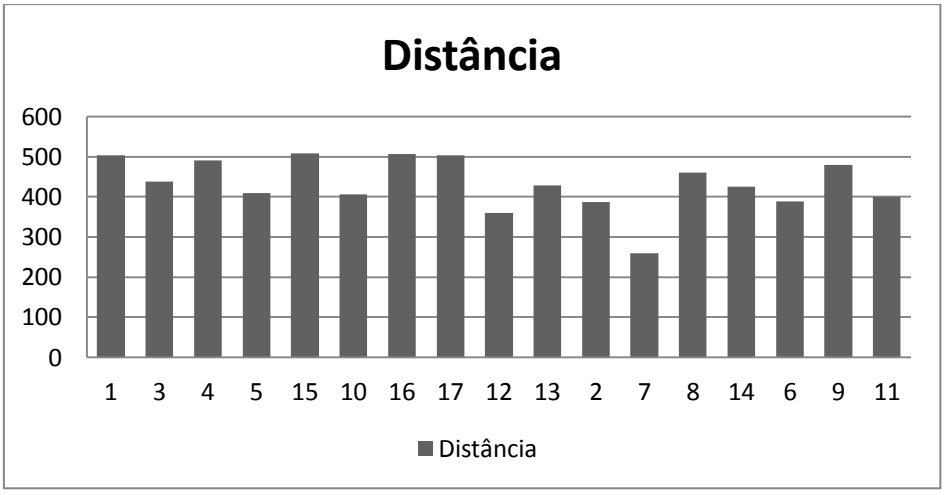

Figura 68 – Movimento Scroll: Distância

Como se pode visualizar na Figura 69, os indivíduos que possuem uma experiência inferior a 10 anos e idade inferior ou igual a 50 são mais rápidos a efetuar este género de movimento.

Excetuando o indivíduo 5, todos os indivíduos com idade superior a 50 anos e experiência inferior a 10 anos possuem uma velocidade muito pequena.

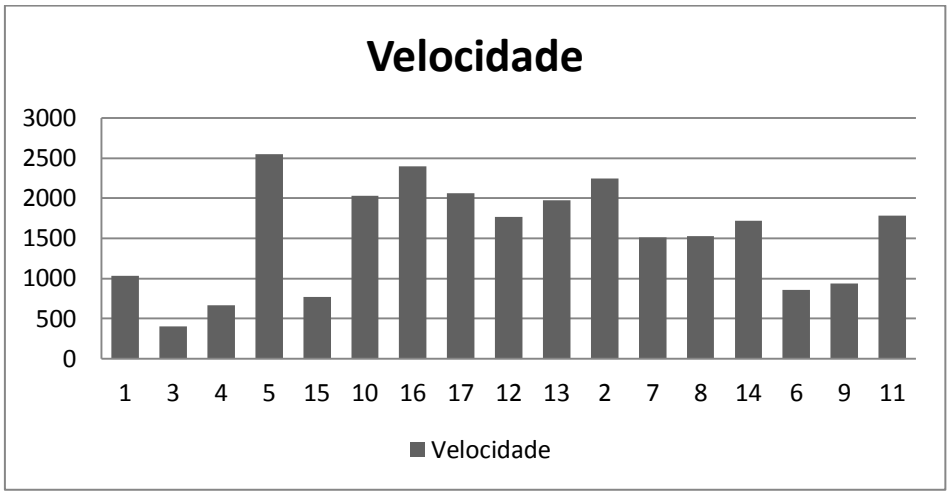

Figura 69 – Movimento Scroll: Velocidade

- Movimento Tap

Neste tipo de movimento, excetuando os indivíduos 10 e 14 que usam o dedo indicador, os indivíduos que usam o polegar possuem pressões mais elevadas. Como nos movimentos anteriores, a experiência não influencia a pressão aplicada. Pode-se observar que os indivíduos que possuem mais experiência aplicam pressões tão elevadas como os que não tem tanta experiência.

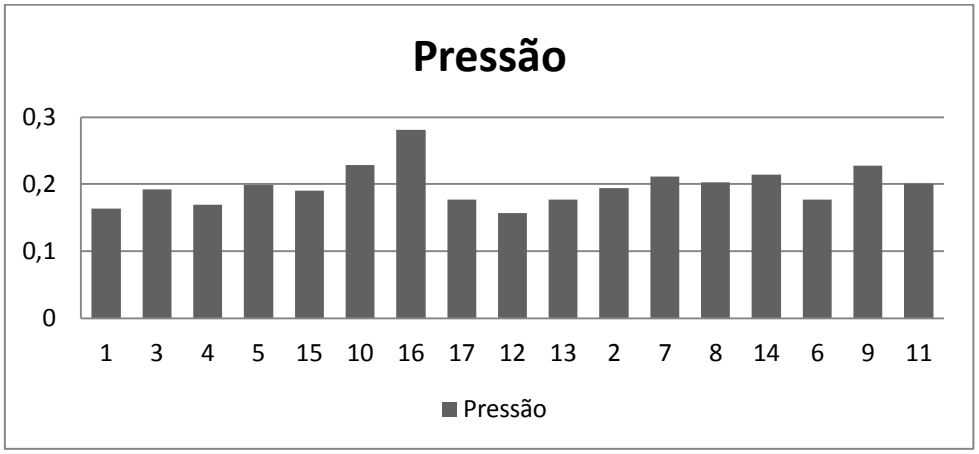

Figura 70 – Movimento Tap: Pressão

Excetuando os indivíduos 10 e 11 que usam o dedo indicador, os indivíduos que ocupam uma maior área são os que usam o polegar. Tal como nos movimentos anteriores, a área está relacionada com a pressão, pois quanto maior é a pressão que o indivíduo aplica maior é a área ocupada.

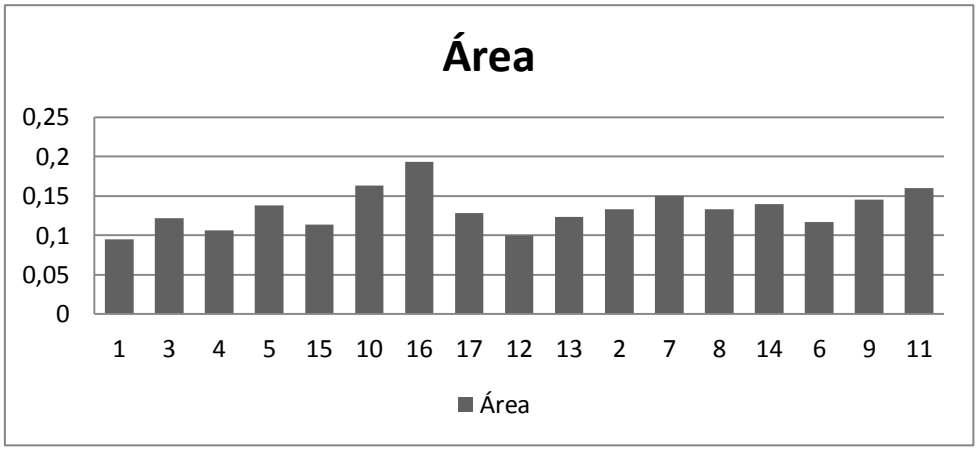

Figura 71 – Movimento Tap: Área

Do gráfico da duração é possível observar que os indivíduos que demoram mais tempo a efetuar o *Tap*, são os que possuem uma experiência inferior a 10 anos e que tem idade superior a 25 anos. Deste modo, a experiência que um indivíduo possui influência o tempo que demora a efetuar este tipo de interação, bem como a sua idade.

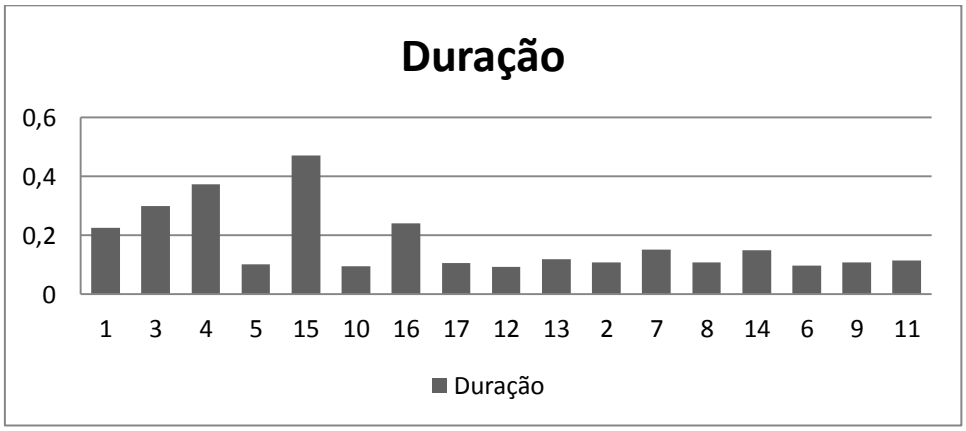

Figura 72 – Movimento Tap: Duração

3.3.2 Resultados dos testes

Nesta secção são descritos os resultados dos testes, e a análise de desempenho dos modelos criados. Assim sendo é efetuada a análise de desempenho dos modelos criados através das medidas FAR, FRR, precisão*, recall*, assertividade, área abaixo da curva.

- Indivíduo 1

Do teste efetuado ao indivíduo 1 obteve-se a seguinte matriz:

Tabela 2 – Matriz do Indivíduo 1

TP	FP
55	10
FN	**TN**
227	813

Na Tabela 2 é possível verificar que o modelo classificou 868 instâncias corretamente e 237 incorretamente, ou seja, obteve-se uma assertividade de 78,552%.

Relativamente às instâncias mal classificas, 10 correspondem às vezes que o modelo aceitou intrusos e 227 correspondem às vezes que o utilizador foi rejeitado pelo modelo. Assim sendo, atingiu-se uma taxa FAR de 1,22 %, ou seja, não é um valor elevado. Deste modo o modelo não permite muitas intrusões, ou seja, possui um elevado nível de segurança. Por outro lado atingiu-se uma taxa FRR de 80,5%, este valor é muito elevado, o que implica a rejeição do indivíduo elevada. Este facto é um pouco incómodo para o indivíduo, pois será rejeitado pelo sistema várias vezes.

Relativamente a precisão do modelo obteve-se o valor 84,62%, ou seja, o modelo possui um valor razoável de precisão. E obteve-se um *recall* de 19,5%, ou seja, é um valor baixo.

Na Figura abaixo é possível observar a área por baixo da curva ROC, ou seja, AUC. A curva encontra-se relativamente perto do canto superior esquerdo e o valor da área é de 0.8734, que pode ser considerado um valor alto. Assim sendo o modelo pode ser considerado bom.

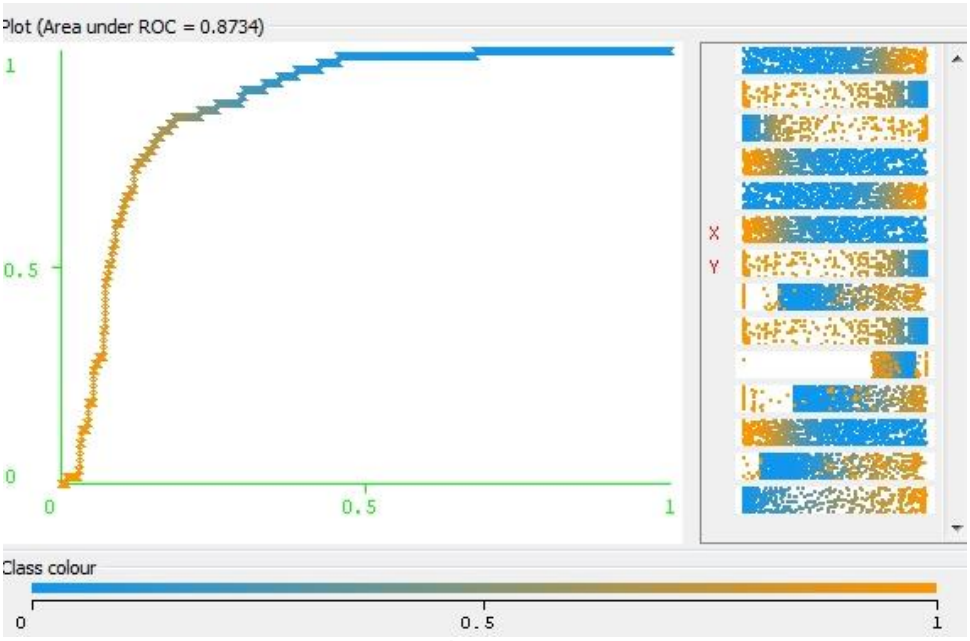

Figura 73 – Área ROC, Indivíduo 1

- Indivíduo 2

Do teste efetuado ao indivíduo 2 obteve-se a seguinte matriz:

Tabela 3 – Matriz do Indivíduo 2

TP	FP
54	11
FN	TN
382	658

Da matriz acima apresentada pode-se constatar que foram corretamente classificadas 712 instâncias, ou seja, obteve-se uma assertividade de 64,4344%. Pode-se ainda observar que foram mal classificadas 393 instâncias. Das instâncias incorretamente classificadas 11 correspondem ao número de ocorrência de intrusão por parte do atacante e 382 corresponde ao número de vezes que o utilizador é rejeitado. Assim sendo o modelo atingiu uma taxa de rejeição de 87,6% e uma taxa de intrusão de 1,22%. Com isto, pode-se verificar que o modelo atingiu um

grau elevado de segurança, pois não permite a aceitação de muitos intrusos. Este modelo rejeita mais vezes o indivíduo do que o modelo anterior. Ou seja, é mais incómodo para o indivíduo.

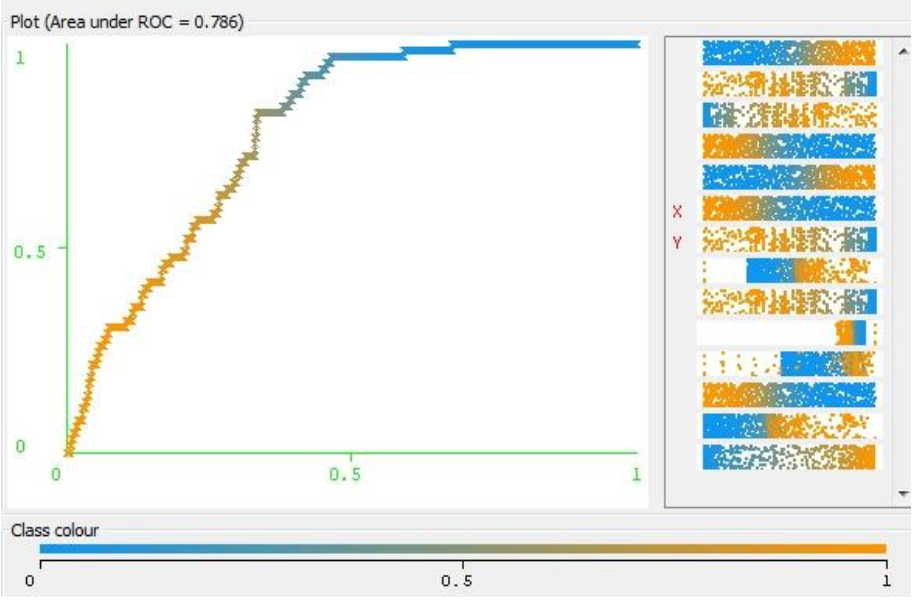

Figura 74 - Área ROC, Indivíduo 2

Dos dados obtidos conclui-se que o modelo possui uma precisão de 83.0769% e um *recall* de 12.3853%. Apesar de a precisão ser um valor elevado o número de rejeições é um pouco elevado.

Na Figura 74 encontra-se delineada a curva ROC e a sua área inferior, que corresponde ao valor 0.786. O valor não é muito elevado, contudo a curva não se encontra muito distante do canto superior esquerdo.

- Indivíduo 3

Do teste efetuado ao indivíduo 3 obteve-se a seguinte matriz:

Tabela 4 – Matriz do Indivíduo 3

TP	FP
59	6
FN	**TN**
231	809

Da Tabela 4 – Matriz do Indivíduo 3 é possível verificar que foram bem classificadas 868 instâncias, ou seja, obteve-se um acerto de 78,552%. É possível ainda verificar que foram mal classificadas 237 instâncias, ou seja, o modelo possui uma taxa de erro de 21,448%.

Das instâncias incorretamente classificadas apenas 6 correspondem a intrusões e 231 correspondem às vezes que o utilizador é rejeitado incorretamente pelo modelo. Deste modo o modelo possui uma FAR de 0,74% que é um valor bastante reduzido, ou seja, existem poucas intrusões. Por outro lado atingiu-se uma FRR de 79,65%, que é elevado. O modelo atingiu uma precisão de 90.7692% e um *recall* de 20.3448%. destes dados obteve-se um F-score de 33,24

Na Figura 75 é possível verificar que o modelo é bom, uma vez que a AUC é elevada, 0.8929 e a curva encontra-se muito próxima do canto esquerdo.

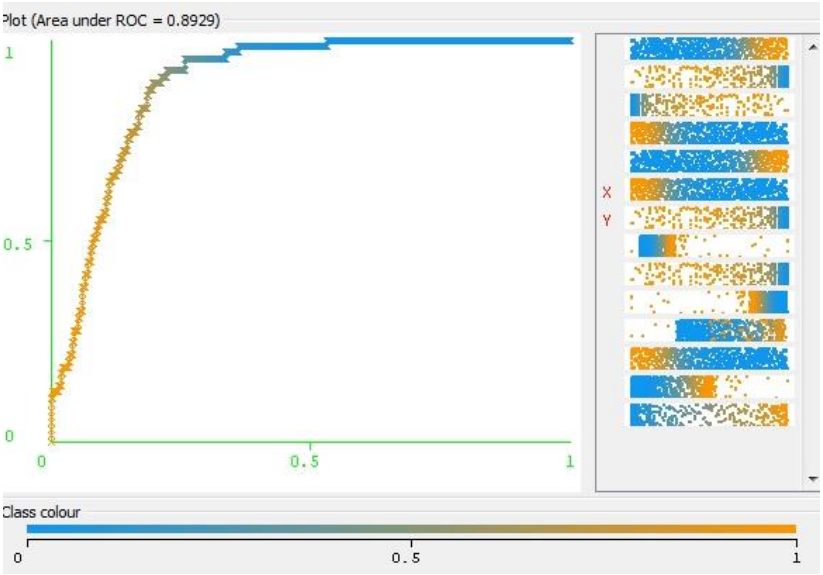

Figura 75 – Área ROC, Indivíduo 3

- Indivíduo 4

Do teste efetuado ao indivíduo 4 obteve-se a seguinte matriz:

Tabela 5 – Matriz do Indivíduo 4

TP	FP
59	6
FN	**TN**
116	924

Tendo em conta a matriz acima apresentada é possível verificar que foram bem classificadas 983 instâncias, ou seja, obteve-se uma assertividade de 88,9593%, e foram mal classificadas 122 instâncias.

Das instâncias incorretamente classificadas, 6 correspondem às intrusões e 116 correspondem às rejeições do utilizador. Deste modo o modelo atingiu uma taxa FAR 0,65%, este valor é bastante baixo, o que implica um maior grau de segurança. Por outro lado atingiu-se uma taxa FRR de 66,3%. Ou seja, existe um elevado grau de rejeições, deste modo o indivíduo é rejeitado pelo modelo diversas vezes. Obteve-se uma precisão de 90.7692% e um *recall* de 33.7143%. Assim sendo o modelo atingiu um valor alto de precisão e não possui um valor muito baixo de *recall*.

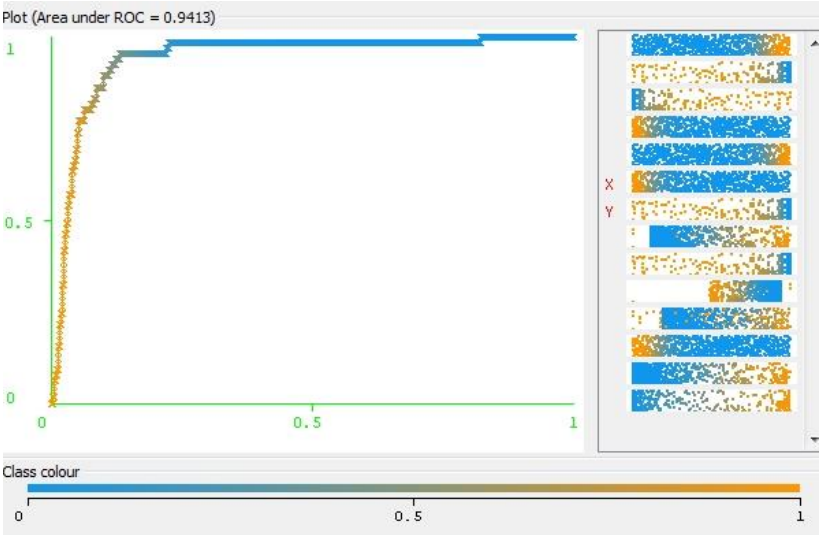

Figura 76 – Área ROC, Indivíduo 4

Na Figura 76 é possível verificar que existe um bom equilíbrio entre a taxa de falsos positivos e de verdadeiros positivos, uma vez que a curva ROC se encontra muito próxima do canto esquerdo e atinge o valor 0.9413 de AUC.

- Indivíduo 5

Do teste efetuado ao utilizador 5 obteve-se a seguinte matriz:

Tabela 6 – Matriz do Indivíduo 5

TP	**FP**
63	2
FN	**TN**
266	774

Do teste efetuado ao indivíduo 5 obteve-se uma taxa de acertividade de 75.7466%, uma vez que foram classificadas corretamente 837 instâncias e 268 erradas.

Das instâncias incorretamente classificadas apenas 2 correspondem às intrusões e 266 às rejeições, assim sendo o modelo atingiu uma FAR de 0,26%, ou seja, possui uma taxa intrusões bastante baixa e uma FRR de 80,9%, que é um valor elevado. Da matriz acima apresentada é possível deduzir uma precisão de 96,9231% e um *recall* de 19,1489%.

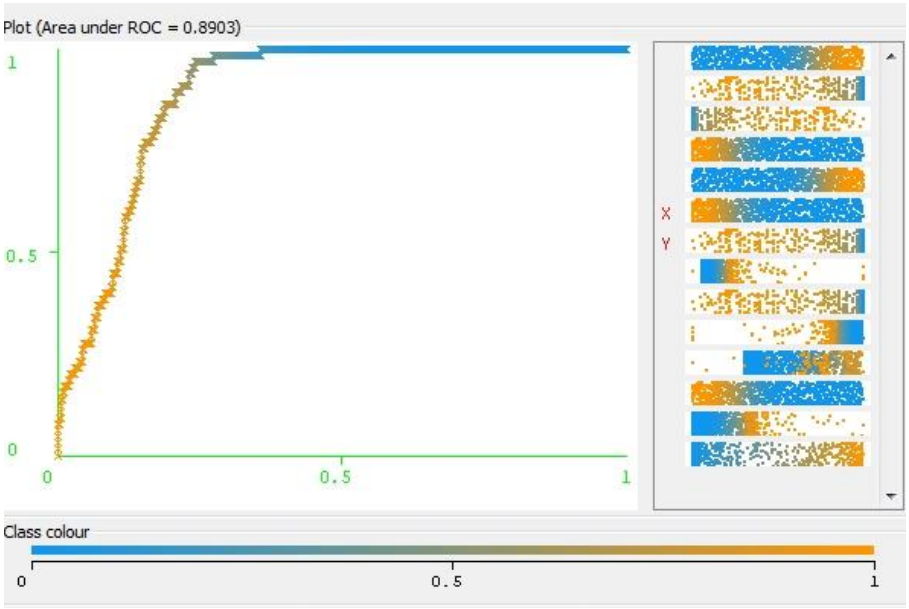

Figura 77 – Área ROC, Indivíduo 5

Na Figura 77 é possível verificar que a curva ROC se encontra próxima do canto esquerdo direito, e que a área abaixo da curva possui um valor alto, 0.8903. Deste modo o modelo possui um bom equilíbrio entre a taxa de falsos positivos e verdadeiros positivos.

- Indivíduo 6

Do teste efetuado ao utilizador 6 obteve-se a seguinte matriz:

Tabela 7 – Matriz do Indivíduo 6

TP	FP
59	6
FN	TN
339	701

Da matriz acima apresentada conclui-se que foram classificadas acertadamente 760 instâncias e 345 erradamente. Assim atingiu-se uma taxa de acerto de 68.7783%.

Das instâncias mal classificadas 6 correspondem às intrusões e 339 às rejeições. Ou seja, apesar do número de intrusões não ser alto o número de rejeições é um pouco elevado, assim o modelo atingiu uma FAR de 0,85% e uma FRR 85,2%.

O modelo atingiu uma precisão de 90.7692% e um *recall* de 14.8241%. Assim sendo atingiu-se uma precisão elevada, contudo o *recall* é um pouco baixo.

Como se pode ver no gráfico atingiu-se uma AUC de 0.7974, que é um valor relativamente alto, ou seja, o modelo possui algum equilíbrio entre a taxa de verdadeiros positivos e de falsos positivos.

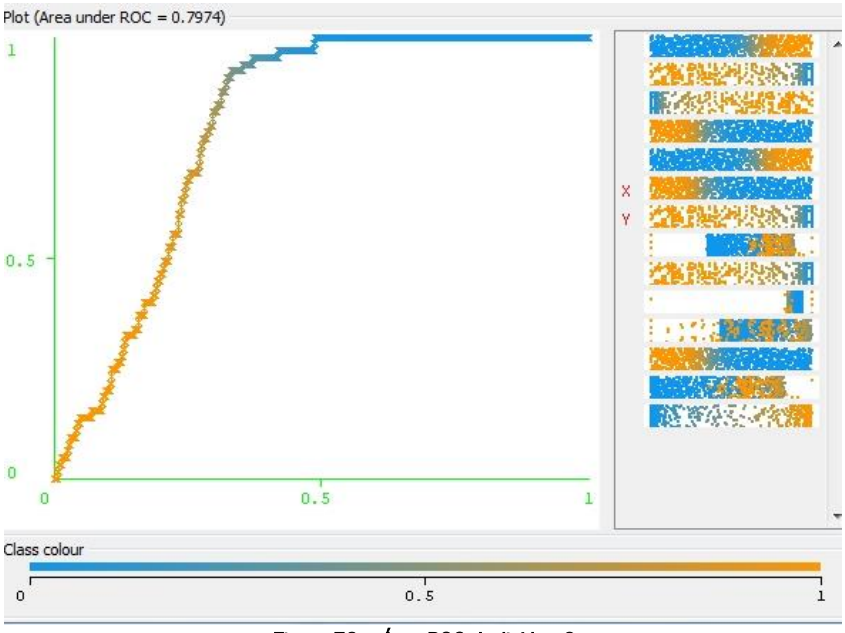

Figura 78 – Área ROC, Indivíduo 6

- Indivíduo 7

Do teste efetuado ao utilizador 7 obteve-se a seguinte matriz:

Tabela 8 – Matriz do Indivíduo 7

TP	FP
48	17
FN	TN
291	749

Do teste efetuado ao utilizador 7 alcançou-se uma taxa de assertividade de 72,1267%, ou seja, foram classificadas corretamente 797 instâncias e 308 incorretamente.

Na matriz é possível verificar que o modelo permite 17 vezes a intrusão do atacante e rejeita o utilizador 291 vezes. Assim sendo o modelo atingiu uma FAR de 2,22%, ou seja, o valor de intrusões é um pouco mais elevado do que os indivíduos anteriores. Por outro lado atingiu-se uma FRR de 85,8%, ou seja, o modelo rejeita muitas vezes o indivíduo.

Dos dados dispostos na Tabela 8 – Matriz do Indivíduo 7 conclui-se que se atingiu uma precisão de 73,8462%, ou seja, é um pouco baixa e atingiu um *recall* de 14,1593%.

Na Figura disposta abaixo, é possível verificar que existe algum equilíbrio entre a taxa de falsos positivos e a taxa de verdadeiros positivos, atingindo uma AUC de 0.7958.

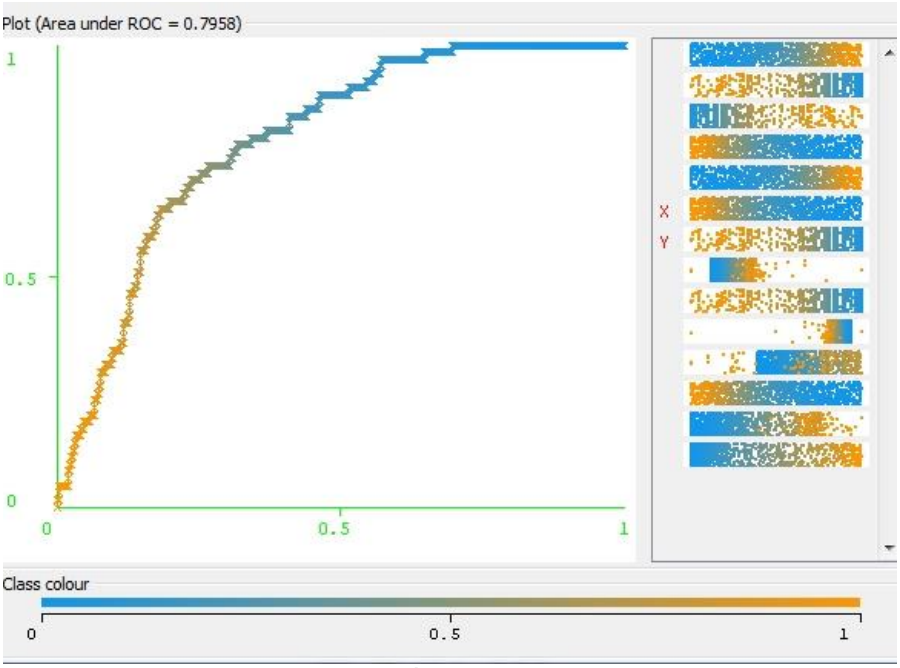

Figura 79 – Área ROC, Indivíduo 7

- Indivíduo 8

Do teste efetuado ao utilizador 8 obteve-se a seguinte matriz:

Tabela 9 – Matriz do Indivíduo 8

TP	FP
54	11
FN	**TN**
389	651

Da Tabela 9 – Matriz do Indivíduo 8 conclui-se que foram incorretamente classificadas 400 instâncias e foram bem classificadas 705 instâncias, ou seja, foi obtida uma taxa de assertividade de 63,8009%.

Das instâncias incorretamente classificadas 11 correspondem às intrusões e 389 às rejeições. Apesar do modelo não possuir uma FAR muito alta 1,7%, a taxa de FRR é bastante elevada 87,8%. Deste modo este modelo não permite muitas intrusões, mas rejeita muitas vezes o indivíduo. Do modelo foi obtido uma precisão de 83,0769% e um *recall* de 12,1896%. Ou seja, atingiu-se um valor elevado de precisão, e um *recall* baixo.

Na Figura 80 é possível verificar que a área por baixo da curva é de 0.7236, ou seja, e um pouco baixo.

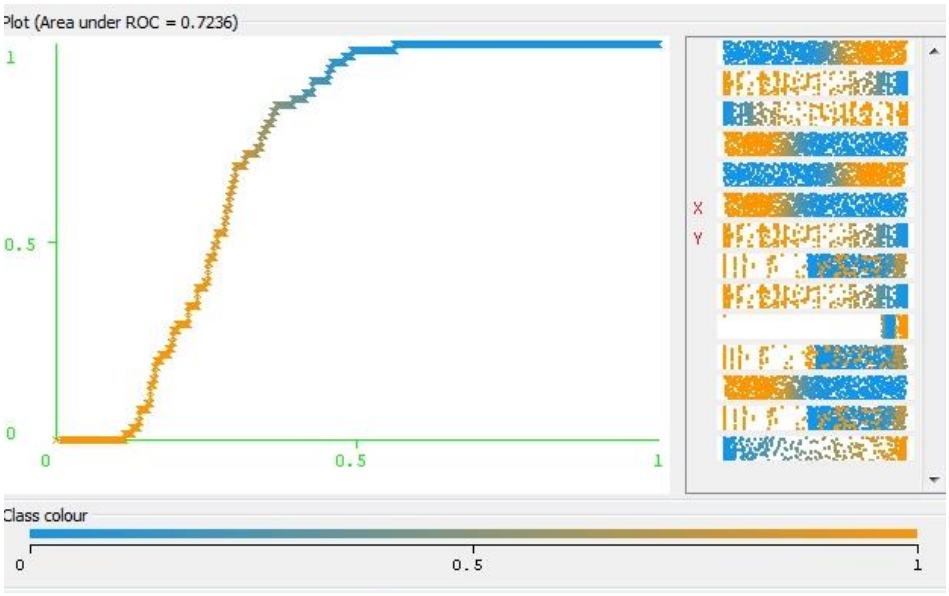

Figura 80 – Área ROC, Indivíduo 8

- Indivíduo 9

Do teste efetuado ao utilizador 9 obteve-se a seguinte matriz:

Tabela 10 – Matriz do Indivíduo 9

TP	FP
65	0
FN	**TN**
242	798

Do teste efetuado ao utilizador 9 foi obtida uma assertividade de 78,0995 %, ou seja, foram mal classificadas 242 instâncias e bem classificadas 863 instâncias.

Da matriz é possível verificar que as instâncias incorretamente classificadas correspondem apenas a rejeições. Assim sendo atingiu-se uma FAR de 0%, ou seja o modelo não permite nenhuma intrusão. Por outro lado atingiu um FRR de 78,87%, ou seja, existe um elevado número de rejeições. A precisão obtida foi de 100% e o recall de 21,1726%. Ou seja o modelo classificou corretamente todas as instâncias do indivíduo.

Da Figura abaixo é possível verificar um bom equilíbrio entre a taxa de falsos positivos e a taxa de verdadeiros positivos. Pode-se observar que a curva ROC se encontra bastante próxima do canto esquerdo, o que indica um bom modelo. Outro fator que indica a boa performance do modelo é o valor alto de AUC, 0.8192.

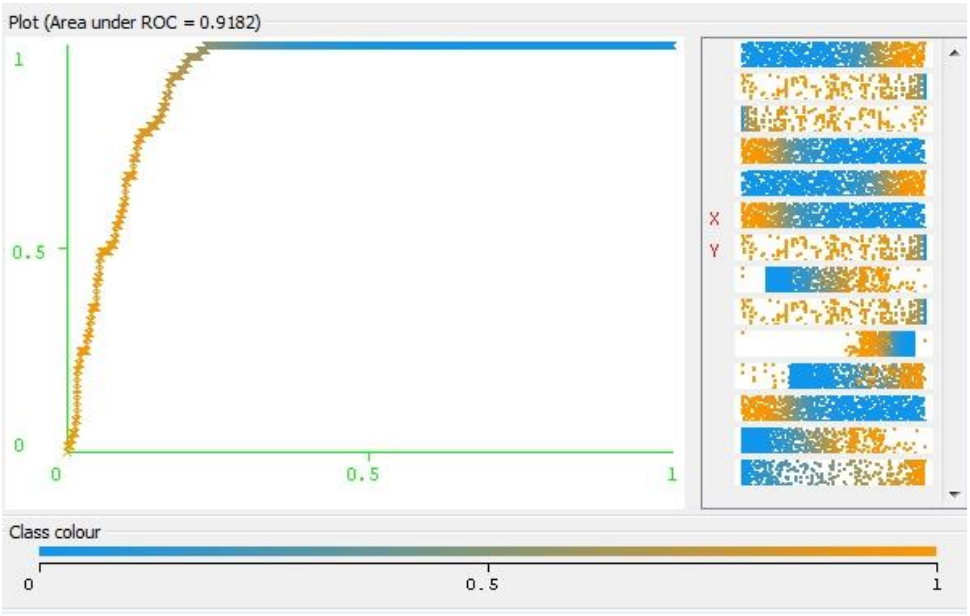

Figura 81 – Área ROC, Indivíduo 9

- Indivíduo 10

Do teste efetuado ao utilizador 10 obteve-se a seguinte matriz:

Tabela 11 – Matriz do Indivíduo 10

TP	FP
55	10
FN	**TN**
399	641

Da Tabela 11 – Matriz do Indivíduo 10 é possível verificar que foram corretamente classificas 696 instâncias e 409 incorretamente, ou seja, obteve-se uma taxa de 62,9864% de assertividade. Ou seja, o modelo classificou uma grande percentagem de instâncias incorretamente.

Das instâncias incorretamente classificas, 10 correspondem às intrusões e 399 às rejeições, ou seja, obteve-se uma FAR de 1,5% e uma FRR de 87,9%. Apesar de a FAR não ser muito elevada, a taxa de rejeições é muito elevada. Do teste efetuado ao indivíduo 10 foi obtida uma precisão de 84,6154% e um *recall* de 12,1145%.

Na Figura 82 é possível observar a curva ROC com uma AUC de 0.7512, pode-se verificar que existe algum equilíbrio entre a taxa de falsos positivos e de verdadeiros positivos.

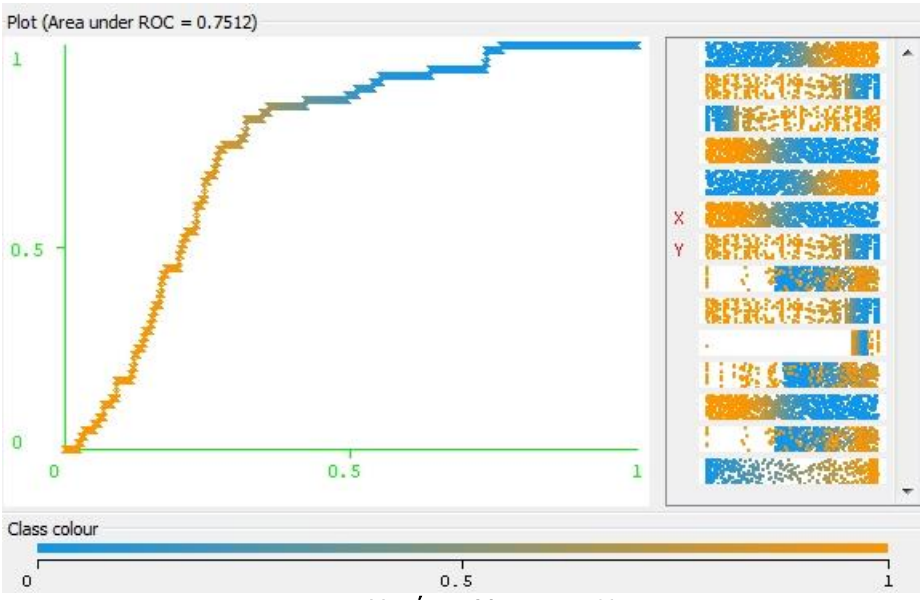

Figura 82 – Área ROC, Indivíduo 10

- Indivíduo 11

Do teste efetuado ao utilizador 11 obteve-se a seguinte matriz:

Tabela 12 – Matriz do Indivíduo 11

TP	FP
55	10
FN	**TN**
184	856

Da matriz acima apresentada é possível concluir que foram corretamente classificadas 911 instâncias e 194 incorretamente. Deste modo obteve-se uma taxa de assertividade de 82,4434%.

Das instâncias incorretamente classificadas apenas 10 correspondem às intrusões e 184 às rejeições. Assim sendo o modelo atingiu uma FAR 1,2%, o que indica uma taxa baixa de

intrusões. Por outro lado atingiu-se uma FRR de 76,9%, que é um valor elevado. É ainda possível concluir que o modelo atingiu uma precisão de 84.6154% e um *recall* de 23,0126%.

Na Figura 83 é possível observar que a AUC equivale a 0.8991 e que a curva se encontra próxima do canto esquerdo, o que indica um bom modelo.

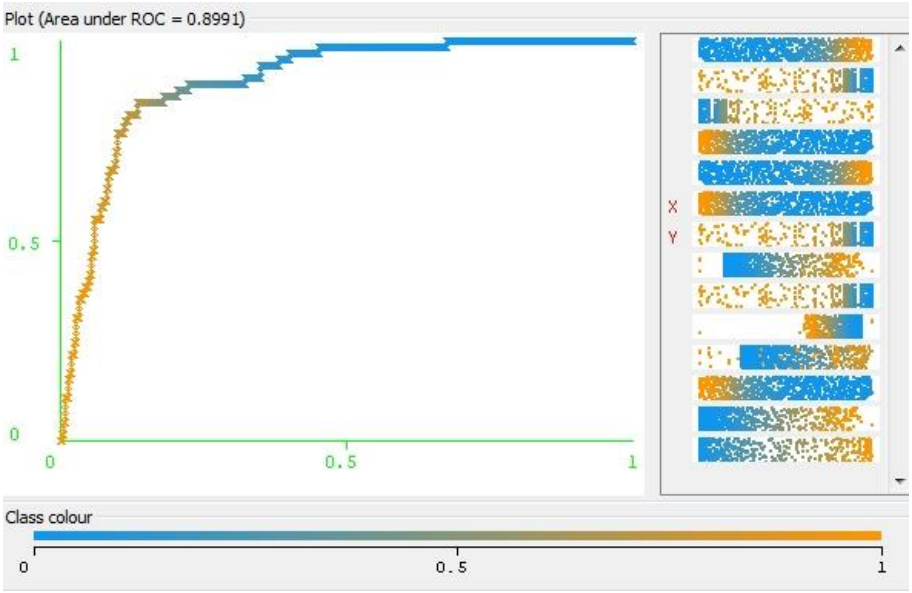

Figura 83 – Área ROC, Indivíduo 11

- Indivíduo 12

Do teste efetuado ao utilizador 12 obteve-se a seguinte matriz:

Tabela 13 – Matriz do Indivíduo 12

TP	FP
49	16
FN	**TN**
428	612

Da Tabela 13 – Matriz do Indivíduo 12 é possível verificar que foram corretamente classificadas 661 instâncias e 444 incorretamente. Assim sendo o teste atingiu uma taxa de acerto de 59,819%.

A FAR é um pouco elevada, 2,5%, ou seja, são aceites bastantes intrusões. A FRR é bastante elevada, de 89,72%, ou seja, são rejeitadas muitas interações do indivíduo. Este é dos modelos com uma taxa de rejeições mais elevada. Da matriz é possível concluir que o modelo produziu uma precisão de 75,3846% e um *recall* de 10,2725%.

O valor da área por baixo da curva é um pouco baixa, 0.7046.

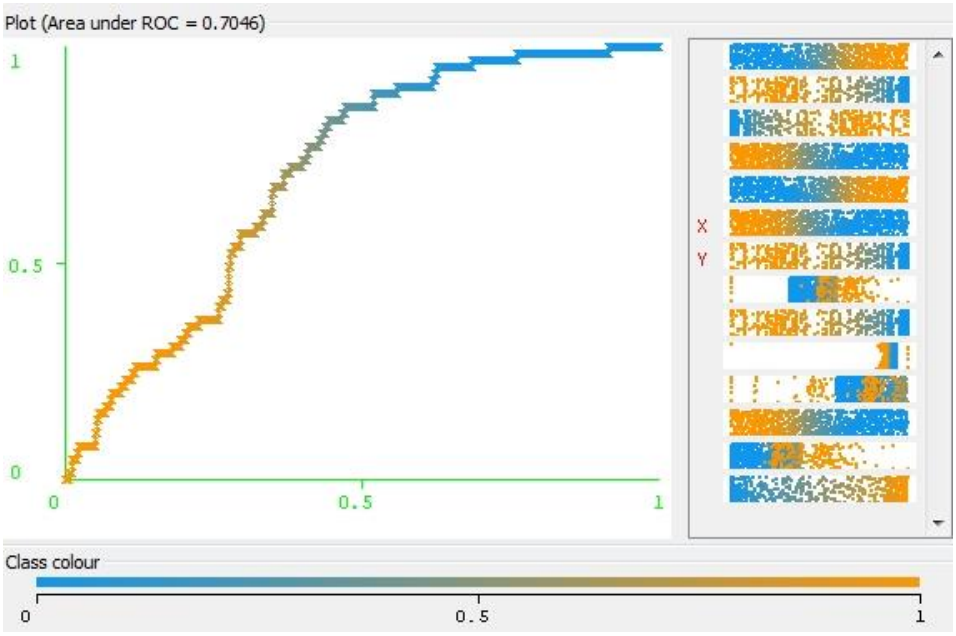

Figura 84 – Área ROC, Indivíduo 12

- Indivíduo 13

Do teste efetuado ao utilizador 13 obteve-se a seguinte matriz:

Tabela 14 – Matriz do Indivíduo 13

TP	FP
57	8
FN	**TN**
351	689

Da matriz acima disposta é possível concluir que o teste produziu uma taxa de 67.5% de assertividade. Ou seja, foram classificadas corretamente 746 instâncias e 359 incorretamente.

É possível verificar que a FAR é de 1,15 %, ou seja, não é alta e a FRR é um pouco elevada, de 86%. Deste modo o número de intrusões não é muito elevada, mas o número de rejeições é elevado. Dos dados é possível concluir que foi atingida uma precisão de 87,6923% e um *recall* de 13,9706%.

Na Figura 85 é possível verificar que a curva não se encontra muito distante do canto esquerdo e o valor da AUC é de 0.8001, ou seja, existe um equilíbrio entre a taxa de falsos positivos e a taxa de verdadeiros positivos.

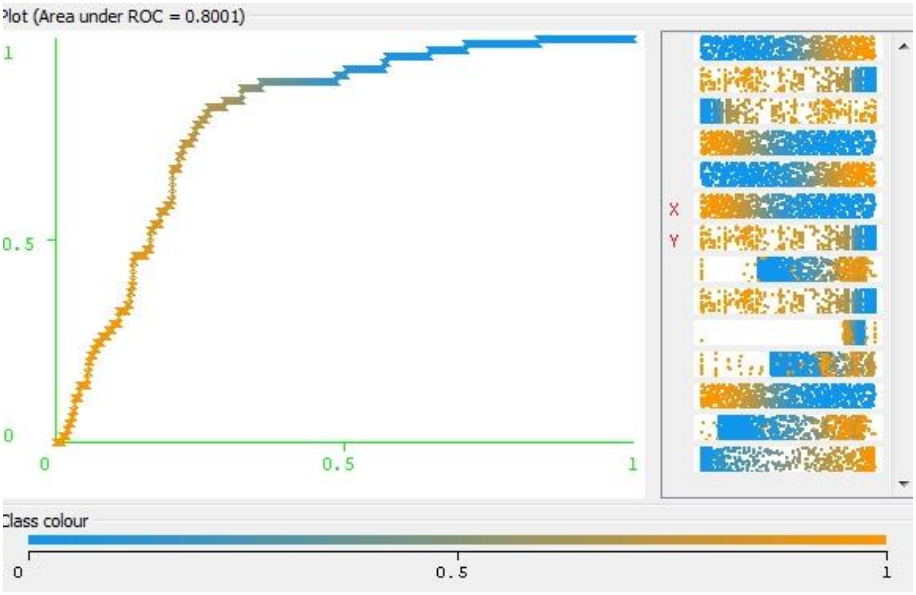

Figura 85 – Área ROC, Indivíduo 13

- Indivíduo 14

Do teste efetuado ao utilizador 14 obteve-se a seguinte matriz:

Tabela 15 – Matriz do Indivíduo 14

TP	FP
56	9
FN	**TN**
255	785

No teste efetuado ao utilizador 14 atingiu-se uma taxa de assertividade de 75,6561%, ou seja foram classificadas corretamente 841 instâncias e 264 incorretamente.

Das instâncias incorretamente classificadas, 9 correspondem às intrusões e 255 às rejeições. Assim sendo atingiu-se uma FAR de 1,13% e uma FRR de 82%. Com isto, o nível de intrusões é baixo, por outro lado, o nível de rejeições é um pouco elevado. No teste atingiu-se uma precisão de 86,1538% e um *recall* de 18,0064%.

Como é possível verificar na Figura 86 o modelo pode ser considerado bom, uma vez que a AUC é elevada, 0.859, e a curva encontra-se perto do canto esquerdo.

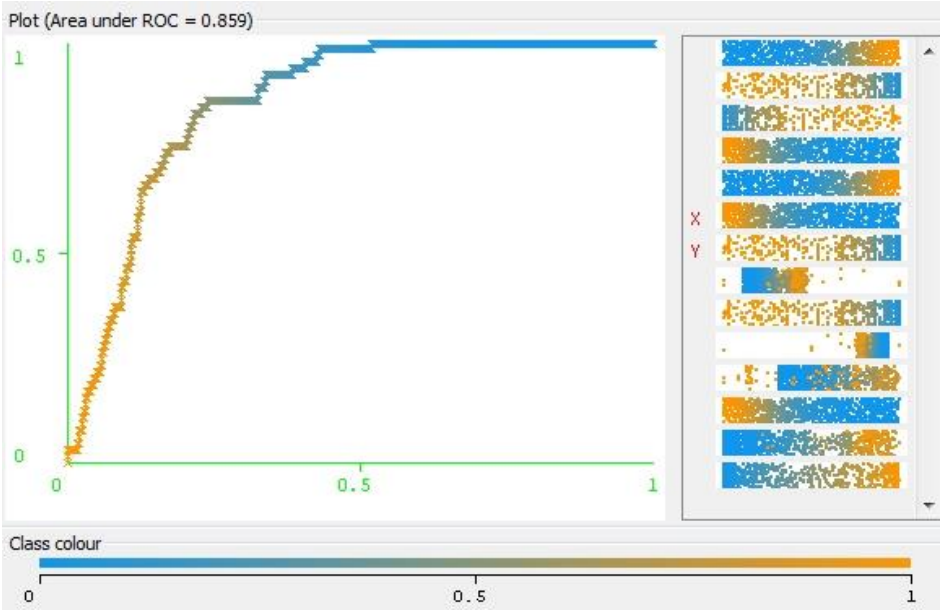

Figura 86 – Área ROC, Indivíduo 14

- Indivíduo 15

Do teste efetuado ao utilizador 15 obteve-se a seguinte matriz:

Tabela 16 – Matriz do Indivíduo 15

TP	FP
61	4
FN	**TN**
463	577

Da matriz acima apresentada é possível verificar que foram corretamente classificadas 638 instâncias e 467 erradamente. Assim sendo atingiu-se 57,7376% de assertividade.

O modelo atingiu uma FAR de 0,7% e uma FRR de 88,4%. Como é possível observar, o número de intrusões não é elevado contudo o número de rejeições é bastante elevado. Relativamente à precisão e *recall*, obteve-se 93,8462% e 11,6412%, respetivamente.

Na Figura 87 é pode-se observar que a AUC do modelo é de 0.7444, que pode ser considerado um valor relativamente alto.

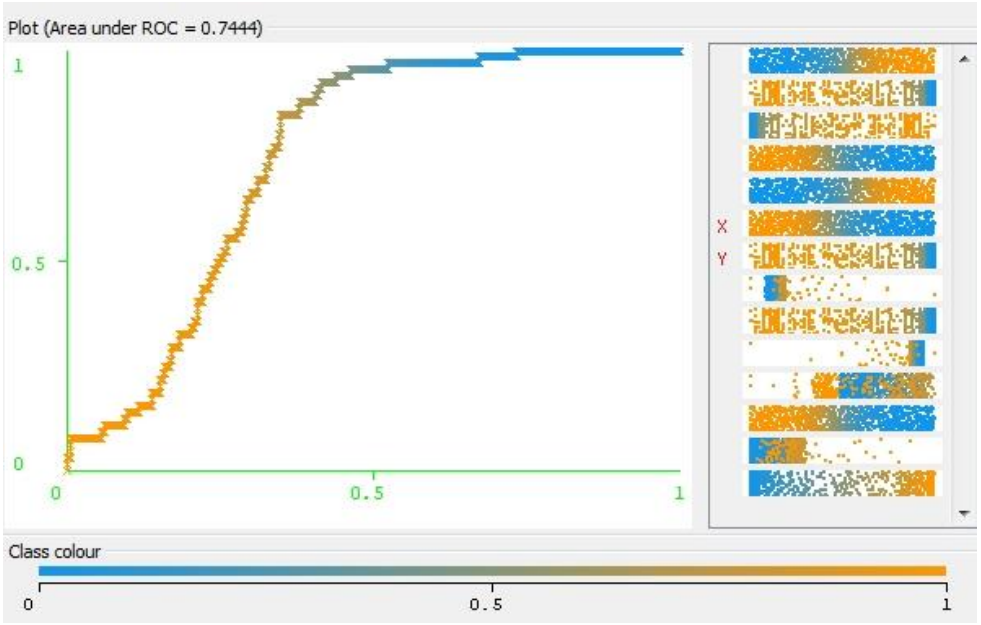

Figura 87 – Área ROC, Indivíduo 15

- Indivíduo 16

Do teste efetuado ao utilizador 16 obteve-se a seguinte matriz:

Tabela 17 – Matriz do Indivíduo 16

TP	FP
51	14
FN	**TN**
166	874

Da matriz acima apresentada é possível verificar que foram bem classificas 925 instâncias e mal classificadas 180 instâncias. Assim sendo o modelo atingiu uma taxa de assertividade de 83,7104%.

Apesar do número de rejeições não ser muito elevado o número de intrusões é um pouco elevado. Assim sendo atingiu-se uma FAR de 1,6% e uma FRR de 76,5%. O modelo atingiu um valor baixo de precisão, 78,4615% e um *recall* de 23.5023%.

Na Figura 88 é possível verificar que a AUC é de 0.8888, que é uma valor elevado, assim sendo o modelo pode-se considerado bom.

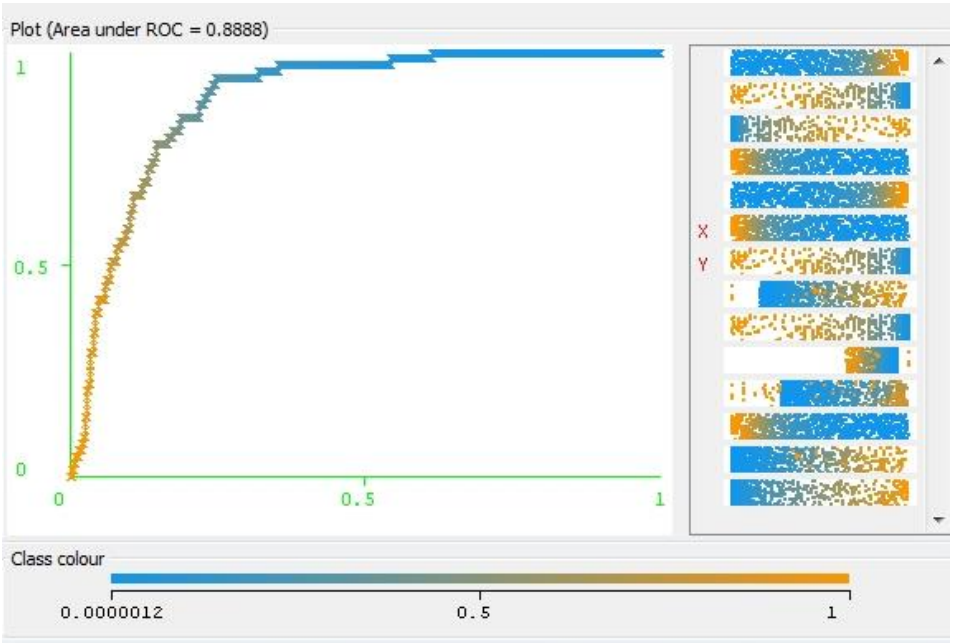

Figura 88 – Área ROC, Indivíduo 16

- Indivíduo 17

Do teste efetuado ao utilizador 17 obteve-se a seguinte matriz:

Tabela 18 – Matriz do Indivíduo 17

TP	FP
53	12
FN	**TN**
344	696

O teste efetuado ao utilizador 17 atingiu uma taxa de assertividade de 67,7828%, ou seja, foram corretamente classificadas 749 instâncias e 356 incorretamente.

O modelo atingiu uma FAR de 1,7% e uma FRR de 86,6%. Assim sendo o número de intrusões não é muito elevado, porém o número de rejeições é elevado.

Relativamente à precisão atingiu-se o valor de 81,5385% e o *recall* atingiu o valor de 13,3501%.

O modelo do utilizador 17 atingiu uma área por baixo da curva de 0.7649, ou seja, existe algum equilíbrio entre as taxas de falsos positivos e verdadeiros positivos.

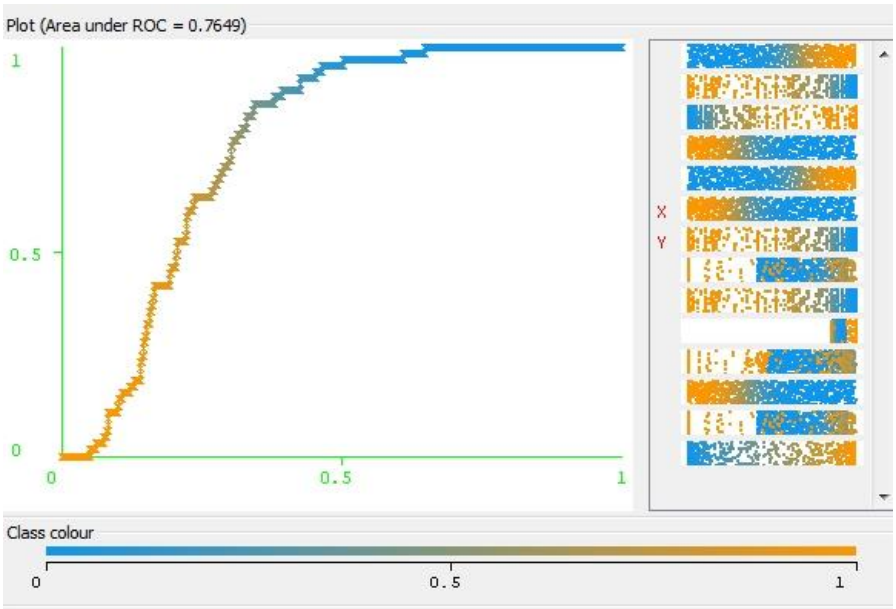

Figura 89 – Área ROC, Indivíduo 17

- Comparação dos Modelos

Nesta secção são apresentados os valores obtidos na análise de desempenho, bem como a comparação dos modelos dos diferentes indivíduos.

Tabela 19 – Valores de Desempenho

Indivíduo	Assertividade	FAR	FRR	Precisão	Recall	F-Score	AUC
1	78,6	1,26	80,5	84,62	19,5	31,7	0.8734
2	64,4	1,6	87,7	83,1	12,4	21,6	0.786
3	78,6	0,74	79,65	90,8	20,34	33,24	0.8929
4	89	0,65	66,3	90,8	33,7	49,2	0.9413
5	75,75	0,26	80,9	97	19,15	31,99	0.8903
6	68,8	0,85	85,2	90,77	14,8	25,5	0.7974
7	72,13	2,22	85,8	73,85	14,2	23,8	0.7958
8	63,8	1,7	87,8	83,1	12,2	21,6	0.7236
9	78,1	0	78,8	100	21,2	34,95	0.8192
10	63	1,5	87,9	84,62	12,11	21,2	0.7512
11	82,4	1,2	76,9	84,62	23	36,2	0.8991
12	59,8	2,5	89,7	75,4	10,3	18,1	0.7046
13	67,5	1,15	86	87,7	14	24,1	0.8001
14	76,1	1,134	82	86,2	18	29,8	0.859
15	57,7	0,69	88,4	93,85	11,6	20,7	0.7444
16	83,7	1,58	76,5	78,5	23,5	36,2	0.8888
17	67,8	1,695	86,6	81,54	13,4	22,9	0.7649
Média	72,2	1,22	82,7	86,2	17,3		0.82

Da Tabela 19 pode-se observar que o modelo do indivíduo 4 foi o que atingiu um valor mais alto de assertividade, ou seja, foi o que classificou mais instâncias corretamente. Por outro lado o que atingiu uma menor assertividade foi o indivíduo 15.

Em média os modelos obtiveram uma taxa de assertividade de 72,2%. Ou seja, ainda classificaram erradamente 27,8% das instâncias. Como se pode ver o valor de assertividade não é muito alto, contudo os modelos atingem uma taxa de precisão elevada, ou seja, possuem uma FAR baixa. Deste modo os modelos não permitem um valor de intrusão alto.

Pode-se observar que o modelo do indivíduo 9 atingiu a melhor precisão - 100 % - ou seja, este modelo não aceitou um único intruso. Por outro lado o modelo do indivíduo 12 foi o que permitiu uma taxa de intrusões maior.

Pode-se observar que o modelo que atingiu uma F-score mais elevado foi o do indivíduo 4, ou seja, é o modelo que possui uma melhor relação entre a precisão e o *recall*. Por outro lado o que possui um F-score mais baixo é o do indivíduo 12. Como se pode ver é o modelo com uma precisão e um *recall* mais baixo.

Apesar da taxa de intrusões ser baixa, a taxa de rejeições é bastante elevada. Como se pode visualizar o elemento que possui uma taxa de rejeições mais elevada é o elemento 12, por outro lado o modelo do elemento 4 atingiu uma taxa de rejeições menor.

Em suma, os modelos atingiram uma FAR baixa, ou seja, os modelos não permitem um valor de intrusões alto. Por outro lado a FRR é um pouco alta, ou seja, os modelos rejeitam os indivíduos muitas vezes.

Com isto pode-se verificar que é possível identificar os indivíduos através das suas interações com o dispositivo. Pois os modelos identificam corretamente os indivíduos, com uma elevada taxa de precisão. Deste modo, atinge-se um elevado grau de segurança, pois não existe um número elevado de intrusões.

Apesar do número de intrusões não ser elevado, o número de rejeições é bastante elevado. Como se pode ver na tabela 19 a taxa FRR é bastante elevada, o que implica um valor elevado de rejeições. Este fato é desfavorável para autenticação contínua, pois o utilizador será rejeitado muitas vezes pelo sistema.

Capitulo IV - Conclusões

Neste capítulo é apresentada uma reflexão sobre o trabalho realizado ao longo desta dissertação, bem como as suas limitações. Por fim é apresentado o trabalho futuro a realizar de forma a acrescentar valor ao trabalho apresentado.

Dada a revisão de literatura apresentada, no âmbito de tecnologias de autenticação para touch-screen, é possível constatar que a utilização de biometrias comportamentais acrescenta valor à área de segurança. Como se pode observar, a utilização de biometrias comportamentais em adição a técnicas de autenticação, reduz a probabilidade de roubo dos dispositivos e de informação. Pois estas são mais difíceis de obter e copiar. Apesar dos benefícios das biometrias comportamentais, estas têm sido utilizadas maioritariamente como suporte de técnicas que se baseiam no conhecimento (palavras-chave, *lock pattern*). Contudo nos últimos anos, a comunidade científica têm-se direcionado para utilização das biometrias comportamentais na autenticação contínua e não intrusiva.

O trabalho desta dissertação é contributo importante para esta área, pois apresenta-se uma análise mais controlada das interações comportamentais e a relação destas às características do indivíduo. O fato das interações serem controladas permite uma melhor comparação dos indivíduos, pois efetua-se a análise de interações semelhantes e não aleatórias.

Este trabalho acrescenta valor para o estudo da autenticação contínua do utilizador, pois como se pôde constatar é possível identificar um utilizador através das interações cotidianas. Deste modo é possível autenticar um utilizador através dos movimentos que este efetua ao logo do dia, sem a necessidade de introduzir palavras-chave ou outra informação de forma explícita. Ou seja, de forma não intrusiva e contínua.

O trabalho proposto possui algumas limitações. A amostra usada para análise das interações comportamentais é um pouco reduzida, o que pode influenciar os resultados obtidos. Pois numa situação real há uma maior probabilidade de ataques.

Outro fator que poderá ter influenciado os resultados, é a dimensão reduzida de instâncias usadas para o treino e teste dos modelos.

Outra limitação do estudo é o facto de só se ter efetuado a experiência num dispositivo móvel. Pois a utilização de outros dispositivos com características diferentes podem implicar mudanças nas interações e comportamento dos indivíduos.

Deste modo uma forma de acrescentar valor ao trabalho apresentado seria a análise do comportamento através de uma amostra maior e mais diversificada, ou seja, mais estratificada por idade, experiência e características físicas. Outro aspeto seria a aplicação da experiência em dispositivos diferentes de forma a verificar as diferenças entre eles. Por fim a adição de movimentos multi-touch (uma vez que estes foram invalidados neste trabalho).

Bibliografia

Agrawal, A. (2012). *User Authentication Mechanisms on Android.*

Angulo, J., & Wästlund, E. (2012). Exploring Touch-screen Biometrics for User Identidentification on Smart Phones. *IFIP Advances in Information and Communication Technology*, 130-143.

Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., & Smith, J. M. (2010). Smudge Attacks on Smartphone Touch Screens. *Proceedings of the 4th USENIX conference on Offensive technologies*, (p. 10). Washinton, DC.

Bi, X., Li, Y., & Zhai, S. (2013). FFitts Law: Modeling Finger Touch with Fitts' Law. *ACM Conference on Human Factors in Computing Systems.* França: 1-10.

Bo, C., Zhang, L., & Li, X.-Y. (2013). SilentSense: Silent User Identification via Dynamics of Touch and Movement Behavioral Biometrics. *Proceedings of the 19th annual international conference on Mobile computing & networking* (pp. 187-190). New York, NY, USA : ACM.

Chang, T.-Y., Tsai, C.-J., & Lin, J.-H. (2012). A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. *The Journal of Systems and Software*, 1157-1165.

Clarke, N. L. (2004). *Advanced User Authentication For Mobile Devices.* Orange Personal Communication Services Ltd.

Conway, D., & White, J. M. (2012). *Machine learner for hackers.* O'Reilly Media, Inc.

Costa, L., Obelheiro, R., & Fraga, J. (2006). Introdução à Biometria. In L. Costa, R. Obelheiro, & J. Fraga, *ivro-texto dos Minicursos, VI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais* (pp. 103-151). Santos, SP.

De Luca, A., Hang, A., Brudy, F., & Hussmann, H. (2012). Touch me once and I know it's you! Implicit Authentication based on Touch Screen Patterns. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 987-996). New York, USA: ACM.

Dean, J. (2014). *Big Data, Data Mining, and Machine Learning: Value Creation for Business Leaders and Practitioners.* John Wiley & Sons.

Dedhia, R. K. (2011). Keystroke Dynamics For Mobile Devices – Data Collection.

Delac, K., & Grgic, M. (2004). A Survey of Biometric Recognition Methods. *46th International Symposium Electronics in Marine* (p. 10). Zadar, Croatia: ELMAR.

Dörflinger, T., Voth, A., Krämer , J., & Fromm, R. (2010). "MY SMARTPHONE IS A SAFE!" The User's Point of View Regarding Novel Authentication Methods and Gradual Security Levels on Smartphones. *Proceedings of the 2010 International Conference on Security and Cryptography* (pp. 1-10). Athens: Security and Cryptography.

Feng, T., Yang, J., & Yan, Z. (2014). TIPS: Context-Aware Implicit User Identification using Touch Screen in Uncontrolled Environments. *The 15th International Workshop on Mobile Computing Systems and Applications*, (p. 6). Santa Barbara, USA.

Ferreira, J., & Santos, H. (2012). Keystroke Dynamics for Continuous Access Control Enforcement. *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)* (pp. 216 - 223). Sanya: IEEE.

Frank, M., Biedert, R., Ma, E., Martinovic, I., & Song, D. (2013). Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication. *The IEEE Transactions on Information Forensics and Security*, 136 - 148.

George, A. M., & Durai, A. D. (2013). A survey on prominent iris recognition systems. *International Conference on Information Communication and Embedded Systems (ICICES)* (pp. 191 - 195). Chennai: IEEE.

Hempstalk, K. (2009). *Continuous Typist Verification using Machine Learning.* The University of Waikato, Department of Computer Science, Hamilton, New Zealand.

Hu, S., Tao, Y., Xiaopeng, L., & Yu, H. (2012). Accelerometer-based Gait Authentication via Neural Network. *Chinese Journal of Electronics*, 481-484.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *Circuits and Systems for Video Technology*, 14.1: 4-20.

Jansen, W. (2003). Authenticating Users on Handheld Devices. *In Proceedings of Canadian Information Technology Security Symposium*.

Järvinen, P. (2007). Action research as an approach in design science. *Quality & Quantity*, 37-54.

Kolly, S. M., Wattenhofer, R., & Welten, S. (2012). A Personal Touch - Recognizing Users Based on Touch Screen Behavior. *Proceedings of the Third International Workshop on Sensing Applications on Mobile Phones* (pp. 1-5). New York: ACM.

Lee, K., & Oh, H. (2013). Research on Access control Method by User Authority using Two-Factor Authentication. *Proceedings of the 1st International Conference on Convergence and It's Applicatio*, (pp. 24: 172-175).

Magalhães, P. S. (2005). *Estudo dos padrões de digitação e a sua aplicação na autenticação biométrica.*

Magalhães, P. S. (2009). *Estudo de viabilidade da utilização de tecnologias biométricas comportamentais na autenticação do cidadão perante os serviços electrónicos do Estado.*

Magalhães, P. S., & Santos, H. D. (2003). Biometria e autenticação. *Actas da 4ª Conferência da Associação Portuguesa de Sistemas de Informação.* Porto: Associação Portuguesa de Sistemas de Informação.

Mäntyjärvi, J., Lindholm, M., Vildjiounaite, E., Mäkelä, S.-M., & Ailisto, H. (2005). Identifying users of portable devices from gait pattern with accelerometers. *Acoustics, Speech, and Signal Processing. Proceedings. (ICASSP '05)*, (pp. ii/973 - ii/976).

Meng, Y., Wong, D., Schlegel, R., & Kwok, L.-f. (2012). Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones. *8th International Conference, Inscrypt* (pp. 331-350). Beijing, China: LNCS.

Nandakumar, K. (2005). *Integration of Multiple Cues In Biometric Systems.*

Ricci, R., Chollet, G., Crispino, G., Jassim, S., Koreman, J., Soria-Rodriguez, P., . . . Olivar-Dimas, M. (2006). SecurePhone: a mobile phone with biometric authentication and e-signature support for dealing secure transactions on the fly. *Proc. SPIE Symp. Mobile Multimedia/Image Processing for Military and Security Applications*, (p. 11).

Saevanee, H., & Bhattarakosol, P. (2009). Authenticating user using keystroke dynamics and finger pressure. *Consumer Communications and Networking Conference* (pp. 1-2). Las Vegas: IEEE.

Sandhu, R., & Samarati, P. (1994). Access Control: Principles and Practice. *IEEE Communications Magazine*, 40-48.

Sandhu, R., & Samarati, P. (1996). Authentication, Access Control, and Audit. *ACM Computing Surveys*, 28: 241-243.

Sandnes, F. E., & Zhang, X. (2012). User Identification based on Touch Dynamics. *9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic*, (pp. 256 - 263). Fukuoka.

Shi, E., Niu, Y., Jakobsson, M., & Chow, R. (2011). Implicit Authentication through Learning User Behavior. *Proceedings of the 13th international conference on Information security* (pp. 99-113). Heidelberg: Springer-Verlag Berlin.

Sieger, H., Kirschnick, N., & Möller, S. (2011). Poster: User preferences for biometric authentication methods and graded security on mobile phones. *roceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services* (pp. 1-2). New York: ACM.

Skaff, G. (2007). An alternative to passwords? *Biometric Technology Today, 15*(5), 10-11.

Sun, Q., Li, Z., Jiang, X., & Kot, A. (2008). An Interactive and Secure User Authentication Scheme for Mobile Devices. *Circuits and Systems* (pp. 2973-2976). Seattle, WA: IEEE.

Traore, I., Woungang, I., S. , M. O., Nakkabi, Y., & Lai, I. (2013). Online risk-based authentication using behavioral biometrics. *Multimedia Tools and Applications*, 31.

Varenhorst, C. (2004). *Passdoodles; a Lightweight Authentication Method.* MIT Research Science Institute.

Wayman, J., Jain, A., Maltoni , D., & Maio, D. (2005). An introduction to biometric authentication systems. *Biometric Systems*, 1-20.

Weiss, R., & Luca, A. (2008). PassShapes - Utilizing Stroke Based Authentication to Increase Password Memorability. *Proceedings of the 5th Nordic Conference on Human-Computer Interaction*, (pp. 383-392). Lund, Sweden.

Wigdor, D., Forlines, C., Baudisch, P., Barnwell, J., & Shen, C. (2007). LucidTouch: A See-Through Mobile Device. *Proceedings of the 20th annual ACM symposium on User interface software and technology* (pp. 269-278). New York, NY, USA ©2007.

Witten, I. H., & Frank, E. (2005). *Data Mining: Practical Machine Learning Tools and Techniques.* Morgan Kaufmann.

Zheng, N., Bai, K., Huang, H., & Wang, H. (2012). *You Are How You Touch: User Verification on Smartphones via Tapping Behaviors.*

Anexos

6.1 Anexo I

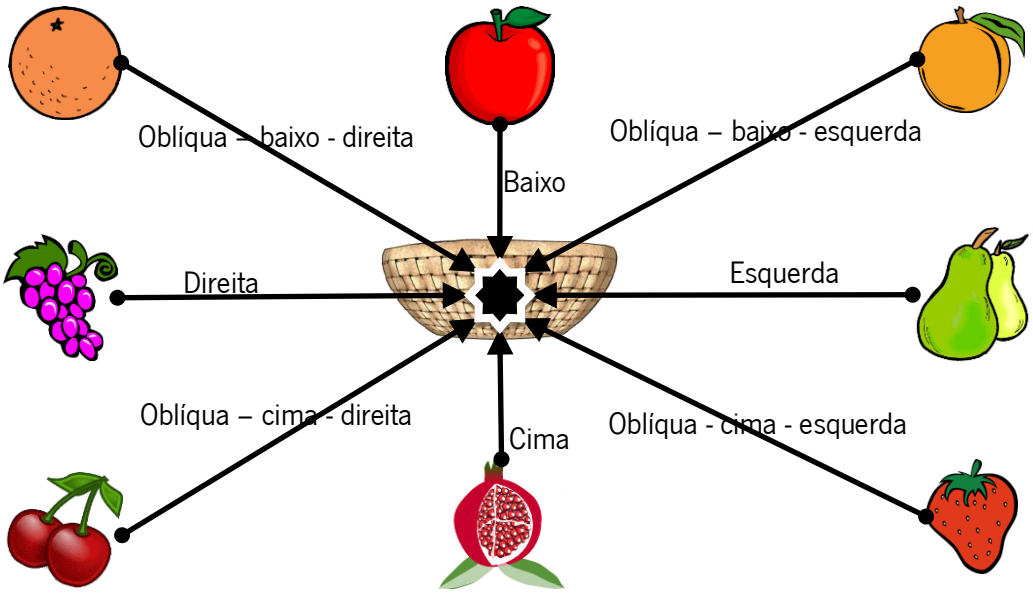

Figura 90 – Orientações do Movimento Drag

6.1 Anexo II

Tabela 20 - Caraterísticas dos indivíduos

Utilizador	Idade	Experiência	Dedo
1	Mais de 50 anos	Menos de 10 anos	Indicador
2	Entre 25 e 50 anos	Mais de 10 anos	Indicador
3	Mais de 50 anos	Menos de 10 anos	Indicador
4	Mais de 50 anos	Menos de 10 anos	Indicador
5	Mais de 50 anos	Menos de 10 anos	Indicador
6	Menos de 25 anos	Mais de 10 anos	Indicador
7	Entre 25 e 50 anos	Mais de 10 anos	Polgar

8	Entre 25 e 50 anos	Mais de 10 anos	Médio
9	Menos de 25 anos	Mais de 10 anos	Polgar
10	Entre 25 e 50 anos	Menos de 10 anos	Indicador
11	Menos de 25 anos	Mais de 10 anos	Indicador
12	Menos de 25 anos	Menos de 10 anos	Indicador
13	Menos de 25 anos	Menos de 10 anos	Indicador
14	Entre 25 e 50 anos	Mais de 10 anos	Indicador
15	Mais de 50 anos	Menos de 10 anos	Indicador
16	Entre 25 e 50 anos	Menos de 10 anos	Polgar
17	Entre 25 e 50 anos	Menos de 10 anos	Indicador