A Survey of User Interaction for Spontaneous Device Association

MING KI CHONG, Lancaster University
RENE MAYRHOFER, Johannes Kepler University Linz
HANS GELLERSEN, Lancaster University

In a wireless world, users can establish ad hoc virtual connections between devices that are unhampered by cables. This process is known as *spontaneous device association*. A wide range of interactive protocols and techniques have been demonstrated in both research and practice, predominantly with a focus on security aspects. In this article, we survey spontaneous device association with respect to the user interaction it involves. We use a novel taxonomy to structure the survey with respect to the different conceptual models and types of user action employed for device association. Within this framework, we provide an in-depth survey of existing techniques discussing their individual characteristics, benefits and issues.

Categories and Subject Descriptors: H.5.2 [**Information Interfaces and Presentation**]: User Interfaces–Interaction styles

General Terms: Human Factors

Additional Key Words and Phrases: Device Association, Pairing, Spontaneous Interaction, Wireless, User Interaction, Survey, Taxonomy

1. INTRODUCTION

We witness a proliferation of wireless devices, such as laptops, mobile phones, tablets, accessory devices, and more. Their wireless capability enables flexible formation of ad hoc networks. However, before devices can transfer any data wirelessly, they are required to establish a virtual connection, a process known as *device association*. Of particular interest is *spontaneous device association* where users establish a connection in an ad hoc manner, as this enables serendipitous interaction, for instance between a user's personal device and devices they encounter in their environment. In this article, we survey how users achieve spontaneous device association: the interactive techniques that have been proposed for device association and the conceptual models on which they are based.

Traditionally, a familiar way for users to associate devices was to connect them via a tangible medium, such as a cable. The user interaction involved, i.e. to plug in a cable, was based on a simple concept that applied universally. However, as devices have become wireless, the communication medium no longer dictates which devices will connect. Instead, connections are established based on user actions that can take many different forms. A widely deployed mechanism is Bluetooth pairing, which involves selection of a target device from a list of available devices (with an additional PIN authentication procedure, if security is required). However, researchers have demonstrated a great many alternative approaches; some focused on simplicity of the required user action [Hinckley 2003; Holmquist et al. 2001; Rekimoto et al. 2003b], and others on interactive authentication (addressing the problem that connections cannot

DOI:http://dx.doi.org/10.1145/0000000.0000000

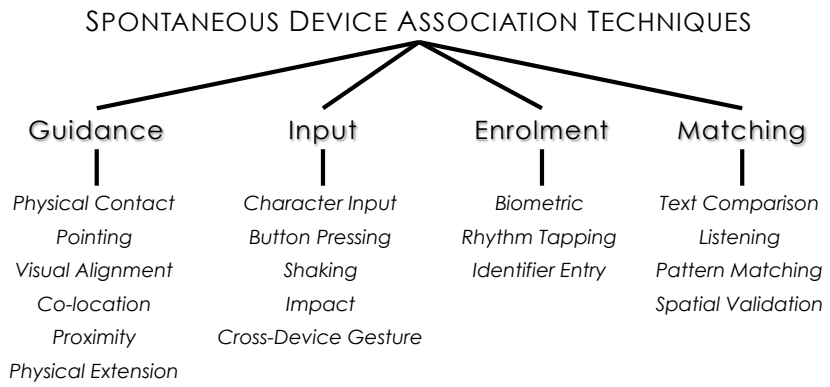

Fig. 1. A taxonomy of interaction techniques for spontaneous device association. The first layer classifies techniques based on overarching categories that capture key conceptual differences of perspective, and the second layer further sub-classifies techniques by specific concepts and types of user action.

be easily verified in the absence of wires [Balfanz et al. 2002; Kindberg and Zhang 2003b; Stajano and Anderson 1999]).

The existing body of work shows that a association task can be implemented in many different ways. The requisite user actions are hugely diverse, including for example synchronous device input [Hinckley 2003; Rekimoto 2004], device alignment and pointing [Kindberg and Zhang 2003b; Mayrhofer and Welch 2007; Swindells et al. 2002], gestural manipulation of devices [Holmquist et al. 2001; Patel et al. 2004; Chong et al. 2010] and context capture (e.g. select a target by taking a photo [McCune et al. 2005]). In this active research field, we are yet missing a generalisation of all the work done so far; thus, a literature survey and classification is needed.

Much work on device association has focused on enabling users to establish connections in a secure manner, commonly referred to as *secure pairing*. Prior surveys have examined this work and compared association techniques with respect to security concepts, such as use of out-of-band-channels for secure exchange of keys [Kumar et al. 2009a; 2009b; Malkani and Dhomeja 2009; Suomalainen et al. 2009]. We present a survey with a wider remit, inclusive of association techniques that are not a priori concerned with security, and with a different focus, on the user interaction involved in the association process. Ease of use has been a general concern in work on device association and Chong and Gellersen [2012] presented a framework for discussion of factors influencing usability, however there has not been any comprehensive review.

This article contributes a first comprehensive survey of interactive techniques for spontaneous device association. To structure the exposure, we use a novel taxonomy that we derived from our survey, shown in Fig. 1. The rationale for introducing a new taxonomy is to classify approaches by the user actions they involve, contrasting previous surveys that were structured by technology aspects such as the hardware required by different approaches, and the different types of channel used for communication. We argue that a classification based on concepts of human-computer interaction is an important complement to previous survey work, as methods for spontaneous device association critically depend on successful interaction.

The taxonomy we have developed aims to capture the concepts that underpin the process of device association, from a user's perspective. For every surveyed technique we considered the user action involved and the conceptual model underpinning that action. For example, a variety of techniques require a user to point one device at an-

other to establish a connection: this builds on a conceptual model that is common for identification of targets in a physical environment. Through our survey we have identified four general categories of interactive device association techniques:

— *Guidance* encompasses techniques where users act in the real world in order to connect devices, based on concepts that are external to the involved devices, such as contact, alignment and proximity.
— *Input* focuses user action on the involved devices, building on conventional user interface concepts such as triggering commands, entering data, or direct manipulation.
— *Enrolment* is based on one-time registration of devices with an identity, and the concept of users presenting an identity to a target device in order to associate.
— *Matching* describes approaches where users compare output of the involved devices to confirm or reject a connection.

Our taxonomy is of twofold utility. First, it brings to the foreground of the concepts that users deal with when they associate devices. In most of the device association literature, a user's involvement is developed pragmatically, with little or no consideration of the user's conceptual model of the process. However, a user's conceptual model is of central importance to the design of any interactive system [Liddle 1996; Johnson and Henderson 2002].

Secondly, we identify overarching categories that capture key conceptual differences of perspective—for example contrasting guidance where the user interaction is relative to the real world, and input where the interaction abstracts from the real world. Any of the user actions we review falls under one of the categories in terms of the "mindset" that underpins it. User actions might be syntactically similar (e.g., text input) but conceptually different (e.g., ID entry versus transfer of a passkey from one device to another). The taxonomy thus provides a useful framework for the review we present in this survey, and more generally for the interaction design of device association techniques.

We start our survey with a review of common terminology used in the literature in order to provide an understanding of the basic concepts. This is followed by a section each for the four general categories of association techniques we have identified. In each of these sections, we examine the implications of the overall conceptual model, and provide an in-depth review of individual techniques and their characteristics, benefits and issues. We further provide tabular overviews across the presented techniques to aid comparison, and review user studies on device association that have been reported in the literature. We conclude with a discussion of challenges for future research.

2. BACKGROUND

Wireless ad hoc networks enable spontaneous interoperation of devices. The concept of *spontaneity* implies serendipity, sporadicity and unpredictability [Gostner 2009]. The devices involved are not pre-configured to work with each other, and have no a priori knowledge of each other. Support for spontaneous interoperation between devices has been described as one of the defining concepts of ubiquitous computing, where user interact with many devices in configurations that change dynamically [Kindberg and Fox 2002; Kindberg and Zhang 2003a]. A wide range of discovery mechanism exist for devices to bootstrap spontaneous interoperation [Edwards 2006]. These mechanisms enable devices to be aware of the availability of other devices on the network.

A *device association* is an act of establishing a communication channel between two or more devices over a common medium (e.g., WiFi or Bluetooth) to form an ad hoc network [Mayrhofer 2008]. Various literature have adopted alternative terms for device association, such as *pairing*, *binding*, *coupling*, or *bonding*, but, essentially, the

terms denote the same concept. For consistency, throughout this article, we use the term "association" to denote the process of establishing a device connection and the term "pairing", as the name suggests, for association of only two devices.

It is possible for devices to associate autonomously, based on information exchanged via a discovery mechanism. This can be appropriate, for instance, when an application requires a service but is indifferent as to which devices provide the service. Mechanisms to support this have been widely explored, including in surveys [Meshkova et al. 2008; Ververidis and Polyzos 2008]. However, our focus is on user-controlled device association, where users are in the loop of the association process to ensure that devices connect in accordance with the users' goals. Specifically, when users encounter concrete devices they wish to associate spontaneously, they must have a way to unambiguously identify these as target devices in the association process. This requirement has been referred to as *demonstrative identification* [Balfanz et al. 2002]. It is a significant problem, as there is a gulf between how humans identify devices of which they have no prior knowledge (by their appearance and situation in the real world), and how the involved devices identify each other (by a network identifier).

Services that deal with sensitive data require secure communication. To establish security in an association, devices must first authenticate each other and share a secure session key prior to any exchange of data. When the association is made in a spontaneous manner, over an ad hoc network, devices cannot resort to any trusted third party for authentication. Instead, an *out-of-band* (OOB) channel (also called an *auxiliary* channel [Mayrhofer et al. 2013]) is used for bootstrapping security. An OOB channel is a secondary channel that is private and trusted, and independent of the primary communication channel over which the devices intend to communicate. The purpose of an OOB channel is to enable authentic exchange of data to establish security. The users themselves can act as an OOB channel (e.g., entering identical text into the intended devices). Other examples include communication channels that are limited by some physical property, such as *location-limited channels* [Balfanz et al. 2002], *movement-limited channels* [Mayrhofer and Gellersen 2009], and *time-limited channels* [Chong and Gellersen 2010; 2012]. These all employ physical constraints that limit access to the channel, and involve user interaction to ensure or to verify that only the intended devices can communicate over the limited channel.

Previous surveys of device association have focused on security. Malkani and Dhomeja [2009] surveyed features of secure pairing and compared different out-of-band channels. Kumar et al. [2009b] presented a review of secure pairing techniques that discussed the required hardware and OOB channels, as well as the user actions in the pairing process. They considered user actions with respect to phases involved in establishing security, and classifying them as concerned with setup (bootstrapping the technique), exchange (user actions as part of the protocol) and outcome (user actions finalising the method). This is a useful classification from a protocol design perspective and aids comparison of pairing protocols. However, contrasting that perspective we focus our survey on the concepts that users deal with in establishing device associations, and how they are implemented in specific interaction techniques. Suomalainen et al. [2009] presented a taxonomy of protocols for human-mediated establishment of session keys in personal networks. They focused on the protocols mechanisms involved for device authentication, and their taxonomy is useful in informing system design with respect to security. In contrast, Chong and Gellersen [2012] presented a framework of factors that could influence usability of device association but they did not include a survey of the existing techniques.[1].

[1]The classification framework was first introduced in [Chong and Gellersen 2010], and it was later extended with a thorough discussion and analysis in [Chong and Gellersen 2012].

3. GUIDANCE-BASED ASSOCIATION

Spontaneous device association emerged as a challenge with the advent of ubiquitous computing [Stajano and Anderson 1999]. Ubiquitous computing, in contrast to conventional human-computer interaction, draws attention to the situation of devices in the real world, and spontaneous association is specifically motivated by the meeting of devices in the world (i.e. in encounters that result from user and device mobility). It is therefore not surprising that many device association techniques have the real world context of devices as a conceptual basis. Here, association is directly linked to a physical relationship of the devices in the world, and users establish connections by bringing devices into this relationship. Once brought together, the devices establish a connection automatically and require no further user attention. We refer to this category of techniques as guidance-based, as users guide rather than instruct devices toward association.

The user actions involved in guidance are external to the devices and affect their relationship. This contrasts conventional interaction with devices through their user interfaces. In our survey we have found six categories of guidance-based association, distinguished by the physical relationship that users manipulate. These are *Physical Contact*, *Pointing*, *Visual Alignment*, *Co-location*, *Proximity*, and *Physical Extension*.

3.1. Physical Contact

Amongst the earliest papers that examined device association, Stajano and Anderson [1999] discussed the concept of *imprinting* devices. Their work was motivated by security. A digital device recognises its associates by the entity that sends it a secret key. To securely send a secret key, a simple, cheap and effective method is via a physical contact. When devices are in the pre-associated state, simply touching them with an *electrical contact* that transfers a shared secret constitutes the imprinting, hence an association. In other words, users associate devices by guiding the devices' electrical counterparts into making a contact of each other to form a closed-circuit. From a user's point of view, associating devices by making a physical contact is unambiguous, as only touching devices are connected. Since information is sent via a closed-circuit, any unconnected device is thus not part of the association. The closed-circuit connection permits the transfer of association data (or secret) exclusively between the corresponding devices, and hence minimises the risk of interference. For any intervention, an assailant would need to be present physically to tamper with the electrical contact, but it would be immediately obvious. Many of today's electronic devices already adopt this strategy for communication, like via cables or USB connectors; for example, plugging an MP3 player (as an USB dongle) into a computer. Although the devices require no prior knowledge of each other, the connectors must adopt the same standard and interfaces. Otherwise, mismatched interfaces cannot connect (e.g. a serial port cannot connect to a parallel port). Likewise, for a system to adopt electrical contact as an enabler for association, the involved devices need to be supporting the same standard and hardware.

Other than using electrical signals to transmit association data, physical human *tactile-based contact* is also possible. This scheme is derived from the concept of using human body as a conductor to transfer electrical signals between devices, known as *intrabody communication* [Zimmerman 1996]. Intrabody communication allows users to act as a physical communication medium, where they establish a channel by simply performing a tactile touch on the corresponding devices. The act of touching enables association data to flow between the devices and trigger a device association. Park et al. [2006b] introduced "Touch-And-Play" (TAP), a system that adopts intrabody communication for connecting devices. They illustrated examples of presenting

Fig. 2. A conceptual example of "Touch-And-Play" [Park et al. 2006a; Park et al. 2006b]: A user sends the desired photo stored in the digital camera by touching the printer while holding the camera.

pictures by sending the pictures' data from a camera to a display monitor and printing photos by simultaneously touching a printer and a camera (see Fig. 2). Although the touch interaction is simple, the approach has limitations. Since information is transferred over the body, the user's bare skin must touch the devices directly, which may cause sanitation concerns. Also, sending electrical signals across a human body may interfere with other systems that also use intrabody communication, such as wearable devices [Hachisuka et al. 2005] and biomedical sensors [Wegmüller 2007]. Other than interference, due to noise and signalling constraints, the bandwidth is limited. Users may need to hold onto the connecting devices for a period of time to establish an association.

The two examples above (electrical and tactile approaches) use contact as a guidance interaction to trigger device association. It provides users the immediate affordance of which devices are linked. When a contact point is formed, it helps the users to conceptualise a mental model where a physical contact denotes a virtual association. Meanwhile, since the act of contact requires interfaces to touch, this limits the distance of interaction between the corresponding devices; they must be within a close proximity.

3.2. Pointing

In daily life, the symbolic act of a pointing gesture often denotes the intent of identifying an object. The same notion is adopted for connecting devices. The act of *pointing* creates a relationship between devices, by aiming one device (the initiating device) in the direction of another device (the target device), and the devices will only associate if they are aligned correctly. Pointing-based interaction requires a clear line of sight and can be executed over a distance, and no physical contact between the devices is required. In literature, researchers have explored many pointing-based techniques with different communication media (such as light, audio) to transmit association data.

The use of light as a transmission medium has been a prominent approach for pointing-based association. Several research works have explored the use of visible beam (i.e., laser) to transmit association information between devices [Beigl 1999; Kindberg and Zhang 2003a; Mayrhofer and Welch 2007]. Their systems require a user to aim a laser pointer at a target (e.g. a light receiver). Once targeted, the laser transmits data as digital light pulses. At the receiver's end, the captured light signals are interpreted and used for associating the devices. Although the use of laser beam provides an accurate visual reference, the physical size of the target can influence the difficulty of performing the action. If the size of the target is small, statically pointing a laser dot onto it from a far distance (e.g. a few yards/meters) could be challenging. Also, due to the nature of single-point laser, the interaction only supports association

of two devices at a time; hence, the cardinality of devices is limited. For association of multiple devices, the pointing interaction needs to be repeated with each of the corresponding devices until they are all associated.

Human-imperceptible light (e.g., infrared) has also been suggested as a communication medium. Similar to laser, users must point the initiating device into the direction of the target. However, the techniques differ by the precision required from users. With imperceptible light, as users have no visible point of reference, the aiming is done by estimation; thus, the techniques cannot demand high accuracy. For instance, pointing an infrared remote at a television only requires the user to aim the remote approximately at the direction of a target. Balfanz et al. [2004] presented "Network-in-a-box", a system that uses laptops' infrared port as an auxiliary channel to join an ad hoc network. For the system to transmit infrared signals, the infrared ports must be facing each other, and it only works in indoor environment where there is little ambient infrared noise. Swindells et al. [2002] introduced a process of associating devices through a pointing gesture, by using a infrared stylus, called "gesturePen" (attached to an initiating device) and custom infrared tags (attached to target devices). The stylus emits infrared signals to communicate with the tags, and thus the devices find each other. Since users are not able to see the transmission of data, infrared-based pointing techniques require the devices to present adequate output information for users to be aware of the execution of the association.

In addition to light, Peng et al. [2009] suggested "Point&Connect", a device pairing solution that uses audible signals to discover a target device. When a user plans to pair a mobile device with another nearby device, the user makes a simple gesture of pointing the mobile device towards the intended target. In doing so, beep signals are emitted and used for calculating the distance between the devices. This allows the system to determine the selection of the target, as well as the intent to establish a pairing connection; hence, interpreting the user's intent to establish a device association.

3.3. Visual Alignment

Researchers explored the use of image sensors (i.e., cameras) for reading context information, by translating association data displayed on a target using computer vision techniques. McCune et al. [2005] introduced "Seeing-Is-Believing" (SiB), a system that uses computer vision for associating wireless devices with camera phones. The SiB system requires wireless devices to have their cryptographic material encoded in a visual tag format (e.g. a 2D barcode). Visual barcodes can be pre-configured and printed on labels (i.e. static barcodes), or they can be generated on demand and shown on a device's display (i.e. dynamic barcodes). To form an association, a user aligns a mobile phone's camera towards a visual tag of the target device. The camera captures a snapshot of the visual tag (see Fig. 3). The mobile phone decodes the tag to acquire the cryptographic information and then uses it to establish an association with the target device [McCune et al. 2005; 2009]. In other words, the user's guidance helps to form a visual identification channel between the corresponding devices. Chen et al. [2008] presented "GAnGS" and Lin et al. [2009] presented "SPATE"; both systems extended the SiB interaction approach for secure association of a group of devices. The former requires a situated device to act as a display proxy, while the latter was designed for scenarios where all devices are mobile. Brown et al. [2013] extended the SiB concept for associating mobile devices with a domestic wireless network.

Saxena et al. [2006] later simplified the SiB approach by using blinking patterns of light-emitting diodes (LEDs) instead of visual tags, a system they called "Visual authentication based on Integrity Checking" (VIC). A user aligns a device's camera towards an LED that emits association data as binary patterns. The notion of VIC was later extended and used a mixture of blinking light patterns and audio patterns

Fig. 3. Examples of "Seeing-Is-Believing" (SiB) [McCune et al. 2005; 2009]. A phone running SiB scans the barcode of a target device to capture its cryptographic information. (Left) Static visual barcode. (Right) Dynamic visual barcode. (Source: Jonathan McCune)

(called "Audio-Blink" and "Blink-Blink") [Saxena et al. 2008], as well as for associating a group of devices by emitting an identical visual blinking pattern (called "Blink 'em All") [Saxena and Uddin 2009a]. Likewise, Wilson and Sarin [2007] suggested "BlueTable", a system which adopts computer vision for associating a mobile phone with a camera-based interactive surface. A user places a mobile phone on an interactive surface, with the display of the phone facing the surface's camera. The phone computes association data as a series of binary signals, and then flashes its display according to the binary information (e.g. the display shows a full screen of bright light to represent a binary '1' and no light represents a '0'). The surface's camera then decodes the signals and analyses the information to establish a (secure) association with the phone [Wilson and Sarin 2007; Ramos et al. 2009]. Hesselmann et al. [2010] presented a similar system that uses the built-in flash-light of mobile phones for emitting signals.

Various requirements of computer vision-based association may limit its usability. The resolution of the camera must be adequate enough to capture the visual information over a distance. Visual obstruction between the camera and the target can limit the camera's vision. The lighting condition of the environment needs to be appropriate to prevent disrupting the camera's vision. For example, a powerful background light source (e.g. the sun or a flash light) can compromise computer vision.

3.4. Co-location

Devices become exposed to the same environmental context and signals when they are brought together. By comparing aspects of their environment, devices can confirm that they are in the same location. This can be used for association when the goal is to connect all devices in a given environment. From the user's perspective, device association can appear automatic although their manipulation of devices indirectly determines their co-location.

Wireless devices co-located in the same environment share similar radio signals. Varshavsky et al. [2007] exploited this idea and presented "Amigo". By examining similarity of radio signals between devices, Amigo can determine whether the devices are within the same vicinity of each other and establishes a device association. The user interaction is simple; it only requires a user to bring the devices into an environment where they can share the same radio context, and no further user interaction is required for the association process [Varshavsky et al. 2007; Scannell et al. 2009].

Kindberg et al. [2002] suggested the use of infrared as a constrained channel – a channel with physical properties that impose constrains upon the location of the communicating parties – to determine the co-location of devices. Since infrared cannot travel through physical obstacles (e.g. walls), infrared signals are limited within a physical boundary, and hence, forming a constrained channel. Similar to Active Badge [Want et al. 1992], Kindberg et al. [2002]'s system requires emission of infrared

signals. They placed infrared beacons in a room, which emit an identify of the environment. Thus, mobile devices that are inside this environment can use the infrared identity for examining co-location of each other. Only the devices within this channel can sense the emitted signals, so co-location is proved.

From a user's point of view, their involvement is minimal and can be entirely transparent. The only user requirement is to place the associating devices sufficiently close enough within a shared environment, so that the devices can sense the same context. Since their involvement is minimal, it is conceptually difficult for the user to follow the progress of the association. Without user intervention and no perceptible indication of the progress, the users have no perception (or reference) if the association executed or if the intended devices are indeed the ones that associated. This can raise concerns of users' trust, as the technique does not provide users with more explicit control over the association.

Besides infrared and radio environments, other broadcasting technologies that are physically constrained in a location can also be used, for example ultrasound [Mayrhofer and Gellersen 2007a]. Ultrasound shares similar properties as infrared. They are physically constrained in rooms, as signals attenuate over distance, and imperceptible by human users, hence, nonintrusive.

3.5. Proximity

Some identification and communication technologies are based on signal transmission over a deliberately limited range. Signals are set to attenuate and their power becomes too diminutive for detection beyond the range. As a result, only devices within a predefined proximity can communicate with one another. With the controlled range adjusted to a short distance (e.g., a few centimetres), the channel enforces users to present devices next to one another for communication, and, hence, supports physical device identification. Adopting this scheme for association, devices only connect if they are placed in proximity. Radio-frequency identification (RFID) and near field communication (NFC) are ideal for this type of interaction. RFID and NFC differ in technical detail and in communication range. NFC has a minimal range (1cm) and is therefore experienced by users as a touch technology although no contact is required. RFID typically operates over larger ranges and is experienced as contactless.

Rekimoto et al. [2003b] presented "Proximal Interactions", a technique that adopts RFID as an auxiliary channel for establishing wireless connections when devices are placed within a close proximity. The close proximity channel is designed for two purposes: identification of target devices, and passing of information for a secure connection. Although their interaction model was designed for quick access of wireless devices, the network protocol can be adjusted to accommodate security, such as session key exchange via the RFID channel.

Similarly, Seewoonauth et al. [2009] suggested storing Bluetooth addresses in NFC tags for pairing a mobile phone and a laptop. An NFC tag is attached to a laptop and embedded with the laptop's Bluetooth address. By bring an NFC-enabled phone near the tag, the phone directly collects the corresponding address over NFC (see Fig. 4). Chong et al. [2011] later extended these ideas and presented "GroupTap", which uses NFC as a proximity channel for associating a group of devices around a situated device.

Proximity-based interaction is simple and intuitive, and already widespread in conjunction with smart cards[2]. Mobile devices such as mobile phones increasingly support NFC, but use of devices for proximate interaction is still unfamiliar [Hang et al. 2010]. Another drawback of proximity is that the interaction is constrained within

[2]London's Oyster Card (https://oyster.tfl.gov.uk/) and Hong Kong's Octopus Card (http://www.octopus.com.hk/) are examples of existing smart card payment systems.

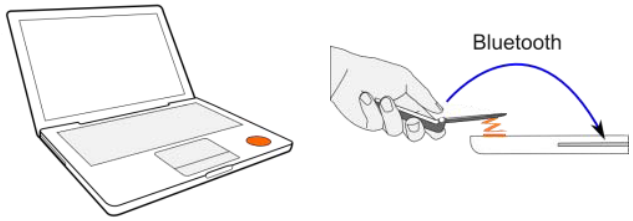

Fig. 4. An illustration of "Touch & Connect" [Seewoonauth et al. 2009]. (Left) A laptop is attached with an NFC tag that is embedded with the laptop's Bluetooth address. (Right) A user places a mobile device close to the tag to start a Bluetooth connection. (Source: Enrico Rukzio)

arm's length. Any physical barriers between entities (e.g., two users sitting across a large table) inherently inhibit the use of proximity.

Employing near-distance proximity for device interaction was one of the key characteristics of *proxemic interactions* by Greenberg et al. [2011]. Their notion explored proxemic relationships to mediate interactions between entities. Besides distance (as presented here), other physical characteristics (e.g., orientation, movement, identity, and location) can be used for cross-device interactions. Marquardt et al. [2011] further developed the notion as the *proxemic toolkit* for rapid prototyping.

Using proximity-based interaction for associating devices has an advantage because users must perform an explicit action (i.e. bringing devices close together). It explicitly involves the user, and hence increases their perception of the association while it executes [Chong and Gellersen 2011]. However, as humans cannot sense radio signals, they cannot perceive directly which devices are communicating. People therefore need to trust their devices as well as the procedure for establishing the intended association.

Other than using a communication technology with limited range, proximity can also be inferred from *wireless signal strength*. Rekimoto et al. [2004] suggested "ProxNet", which detects the proximity of two devices by measuring each other's signal strength. The advantage of the approach is that proximity is inferred from the primary communication channel without need for an additional channel, but signal strength has accuracy limitations for estimating distance. Like radio signals, audio signals also attenuate over distance. Claycomb and Shin [2009] presented "UbiSound", a technique that exploits this for exchange of authentication data over audio, where devices have to be within close proximity to "hear" the data reliably.

3.6. Physical Extension

Traditionally, a cable establishes a device connection directly by a user plugging each end of the physical wire into devices. This metaphor can be applied to wireless device association, where the same user action is preserved, but instead the cable is replaced by a virtual wireless connection. Ayatsuka and Rekimoto [2005] presented "tranStick", a technique that illustrates this concept. In their system, tangible tokens are used for establishing connections. A pair of tokens is first registered to represent a connection, and users can then associate devices by inserting a token each into the intended devices (see Fig. 5).

From a user's perspective, inserting a token into a device is like inserting a cable connector, only the cable is virtual (a "wireless wire"). On the basis of this metaphor, it is also natural for users to disconnect a device by removing the token. Thus, the interactions are symmetrical, where the mirrored action achieves the opposite (i.e. plug to connect, unplug to disconnect). This contrasts other association methods where it is not obvious that reversal of user action should lead to disconnection (e.g., in proximity-

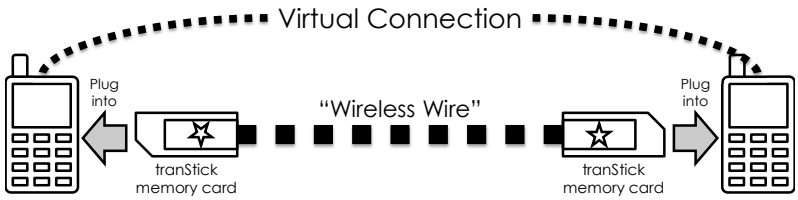

Fig. 5. An illustration of "tranSticks" [Ayatsuka and Rekimoto 2005]. Two memory cards are first registered to exclusively share a unique identity plus key. A user then inserts the cards (i.e. plugging in the "wireless wire") into devices to establish a virtual connection.

based association, it may not be desirable that devices immediately disconnect when users move them apart after the initial pairing act).

Multiple tokens can represent the same connections. Device extension with tokens can therefore also be used for group association, beyond pairing of just two devices. Beyond the use of tokens that get plugged into devices, it is conceivable that users might be provided with other means to physically extend devices for the purpose of association but this has not been addressed in existing literature.

4. INPUT-BASED ASSOCIATION

In conventional computing, as familiar from our desktops, devices are unaware of their situation in the real world, and can only receive data through direct input by a user. To this end, devices provide a well-defined user interface in terms of hardware and software for user input, usually coupled with output devices for feedback on input. Although device pairing is primarily associated with mobility, users are familiar from their desktops with concepts such as entry of data for authentication purposes. Many device association techniques build on this familiarity, and base the association process on user input through the devices' user interface. Hence, we call this category of techniques input-based.

The user actions involved in input-based association are focused on the involved devices and abstract from how the devices are situated in the physical world. They are based on familiar conceptual models of interaction with computers, such as issuing commands, entering data, and direct manipulation of interface elements. In our survey we identified five different types of input-based association: *Character Input* and *Button Pressing* as common input methods, and *Shaking*, *Synchronous Collision*, and *Cross-Device Gestures* as input methods that have emerged specifically for input to a pair of devices.

4.1. Character Input

A passkey is a string of elements that is repeatedly producible by human users. It is made up of any type of knowledge. Even though usually represented in textual form, other types of representation (e.g. graphical images [Biddle et al. 2012] or gestures [Chong 2009; Chong and Marsden 2009]) have also been suggested. To associate devices, users select a passkey and enter it into the associating devices. Numerous passkey-based association methods have been shown in research; some are even adopted as standards. Currently, the use of *textual* passkey is a prevalent technique for authenticating mobile devices, like Bluetooth pairing [Bluetooth Special Interest Group 2006].

Gehrmann et al. [2004] presented a family of "Manual Authentication" (MANA) protocols. Within that family of protocols, MANA I & III adopts the interaction of entering textual characters for associating devices. In MANA I, a passkey is generated by the

system, whereas in MANA III, the passkey is generated by the user. MANA I & III require users to manually transfer textual data between devices for association. A user first reads a passkey displayed on a device and then enters the same passkey into other associating devices. Thus, the techniques exploit users' ability to read and enter text on the devices. This interaction model is adopted by both Bluetooth Simple Pairing [Bluetooth Special Interest Group 2006] and WiFi Protected Setup [Wi-Fi Alliance 2007] as part of their standards.

As technology evolves, many small ubiquitous devices do not have space to accommodate an interface for text entry. To overcome this, an alternative passkey entry method is needed. Characters are replaced by gestures. Patel et al. [2004] presented a *gesture-based authentication* that uses a challenge-response protocol for pairing a mobile device with an untrusted public terminal. To associate devices, the system first generates a random series of shakes and pauses (the challenge). The user then authenticates by mimicking the gestures sequence (the response) on the mobile device. Any device with a display can act as the gestures generator; thus, the technique can be extended for mobile-only devices. Chong et al. [2010] suggested "GesturePIN", which uses built-in motion sensors of mobile devices for capturing *discrete gestures* as passkeys. They replaced the ten PIN digits with ten identifiable gestures, called *discrete gesture password* [Chong and Marsden 2009; Chong 2009]; hence, a one-to-one mapping between digits and discrete gestures.

From a usability perspective, passkey-based techniques require moderate mental effort, as people need to think of a passkey, and remember it, to establish an association. Nonetheless, since alphanumerical passwords are widely adopted, people are already very familiar with the use of textual passkey. Gestures, on the other hand, require extra effort, as users first need to learn the system.

4.2. Button Pressing

Although user interfaces vary widely, almost all devices have an on-off sensor that returns binary states, for example a button or a switch [Soriente et al. 2009]. Based on this, researchers have devised association techniques that are suitable for button-only interfaces, and, as a result, pushing buttons forms the primary user action.

Rekimoto et al. [2003a] presented "SyncTap", where a user establishes device connections through simultaneous button operations. When a user wants to associate two devices, the user presses and releases the SyncTap buttons on both devices at the same time [Rekimoto et al. 2003a; Rekimoto 2004]. SyncTap is based on the time domain of button events; only devices with simultaneous events can associate. Conflicts can occur when another pair of devices concurrently establishes a connection. To overcome this, the user repeats SyncTap.

Extending the idea of simultaneously pushing buttons, Ramos et al. [2009] presented "BlueRendezvous", a system designed for mobile phones. The system requires users to press the same number key on their phones' keypad while running the BlueRendezvous application. So, instead of having a single dedicated button, BlueRendezvous allows users to select any button from their phones' keypad. In addition, BlueRendezvous is designed for multi-operators. Two cooperating users can press keys on their own phones simultaneously. To compensate for multi-user operation, BlueRendezvous requires a longer time threshold (the period of allowing users to press and release buttons); as a result, the system induces higher collision rate.

Soriente et al. [2007] suggested "Button-Enabled Device Association" (BEDA), a technique that adopts synchronous bitwise button pushing operations to enter association data. The interaction consists of a series of button pushes, where each button press represents a binary bit. Similar to MANA I and III, BEDA's association data can either be entered by a user or first generated by a device and then transferred by a

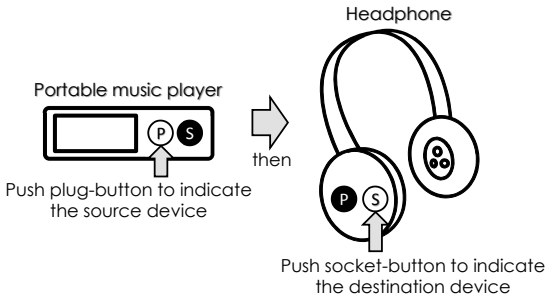

Fig. 6. An illustration of "Touch-and-Connect" [Iwasaki et al. 2003].

user. The latter requires an output mechanism to convey bitwise information, for example a visual display or tactile vibration [Soriente et al. 2009]. However, bitwise data entry is cumbersome and an evaluation showed that users needed over 50 seconds on average for entry of 21-bit information.

The above examples require users to push buttons in a synchronous manner. Alternatively, Iwasaki et al. [2003] presented an *asynchronous* technique, called "Touch-and-Connect". Using the metaphor of inserting a plug into a socket, Touch-and-Connect uses two buttons: a plug-button (P) and a socket-button (S). To associate two devices (in their example a portable music player and a headphone, see Fig. 6), the user first pushes the plug-button (P) on the source device (to indicate it is accepting connection), and then pushes the socket-button (S) on the destination device (to complete the connection). Only the correct sequence of button pushes enables a connection. To avoid conflicts, Iwasaki et al. [2003] included a lock mechanism in the Touch-and-Connect protocol. When one device triggers the plug mode, the plug function of the surrounding devices is disabled and only resets if one of the following occurs: (1) a destination device triggers the socket function, (2) the same plug button is pushed again for a manual cancel, or (3) the system has timeout, i.e. an automatic cancel. The recent WiFi Protected Setup (WPS) standard adopted a model similar to Touch-and-Connect, called "push button" (PBC) method, and defines it as mandatory for access points [Wi-Fi Alliance 2007].

The above button pressing schemes differ in their activation domain. While SyncTap, BlueRendezvous and BEDA are based on the *time* domain (i.e. button events must happen within a threshold period), Touch-and-Connect adopts the *sequence* domain, where events must happen in an order. Nonetheless, each domain has its own pros and cons. Using the time domain requires the users to push and release buttons precisely within a short interval; finding the correct threshold is crucial. On the other hand, using the sequence domain requires the user to be consciously aware of which button to push next. Overall, the interactions are straightforward, as the users only require to push a button on each device; however, the interaction can get complicated if the system has more modes, or requires repetition.

4.3. Shaking

Motion sensors (e.g., accelerometers) can capture device movements as user input. Researchers have explored ways of using movements as a means for device association. Besides discrete gestures (e.g., GesturePIN [Chong et al. 2010]), shaking has also been investigated. For example, a user inputs a rapid shaking pattern, which is captured by a set of connecting devices, and they then establish a (secure) connection. Shaking gives users explicit control over the association by a simple gesture. Users are not

Fig. 7. "Shake Well Before Use" [Mayrhofer and Gellersen 2007b; 2009]: A user holds two mobile devices in one hand and shakes them rapidly for several seconds to establish an association.

required to learn or perform any specific gesture, instead shaking a random pattern is adequate, which requires very little cognition.

Holmquist et al. [2001] proposed "Smart-Its Friends", the first system to suggest the use of rapid shaking for associating devices. Their notion was to use context matching, where shaking defines an explicit user-generated context. Users can simply take two mobile devices, hold them together, and rapidly move them by either waving or shaking. By imposing the same movement on the devices, they capture relatively symmetric data, and the system uses this symmetric input to identify pairing devices. This idea was later extended for secure pairing. Assuming three-dimensional shaking patterns are pseudo-random, unique and difficult to reproduce, several researchers suggested protocols (e.g. "Shake well before use" and "Martini Synch") that derive a secure key from shaking motions [Bichler et al. 2007; Kirovski et al. 2007b; 2007a; Mayrhofer and Gellersen 2007b; 2009]. Although the protocols differ, the underlying user interaction remains unchanged. A user must hold the pairing devices tightly together in one hand and shake them for several seconds (see Fig. 7). The longer the user shakes the devices, the stronger the security of the connection becomes – the entropy of the generated key becomes higher.

Castelluccia and Mutaf [2005] presented a pairing scheme based on asymmetric motions, called "Shake Them Up". Their scheme is different from the above ones, as the generated movement is not used to match up devices. Rather, users must rotate and move devices around each other. The action generates randomness, which prohibits a potential attacker from distinguishing the source of messages exchanged between the devices. Thus, the user input is used as quasi-randomness for added security.

Shaking-based schemes can be considered as *movement-limited* channel [Mayrhofer and Gellersen 2009; Chong and Gellersen 2010; 2012], as devices can only exchange data successfully if their movement matches. Users control the movement of the intended devices, and shaking has the advantage that it is an intuitive movement with natural variance. Users easily understand the technique and it does not require learning of any particular rhythm or pattern [Holmquist et al. 2001; Mayrhofer and Gellersen 2009]. Nevertheless, the usability of any movement-based technique is limited by the shape, size and weight of the involved devices [Chong and Gellersen 2010; 2012].

4.4. Impact

Other than detecting movements, motion sensors can also detect physical impact on devices, by examining sudden sharp changes in amplitude. Exploiting this sensing capability, researchers suggested the use of synchronous collisions for pairing devices. Hinckley [2003] proposed "Synchronous Gestures" (collisions) between the devices, where users initiate an association by bumping two devices together. The collision is detected by each of the devices, and analysis of the acceleration patterns disam-

Fig. 8. An illustration of “Synchronous Gestures” [Hinckley 2003]: (Left) A user connects two devices by bumping one device into another one. (Right) “Dynamic Display Tiling”, an application based on Synchronous Gestures. A user annexes the displays of two tablets, allowing a panoramic image to span both displays.

Fig. 9. “PhoneTouch” [Schmidt et al. 2010]: (Left) An illustration showing how the system detects phone tapping events. (Centre) A user drops a collection of photos on a surface. (Right) A user picks up a photo by tapping on it. (Source: Dominik Schmidt)

biguates which devices were involved. Hinckley [2003] illustrated a sample application, called “Dynamic Display Tiling”, for a scenario of tiling tablet displays by bumping them together (see Fig. 8). The Bump app[3] for mobile phones, a widely adopted commercial solution, embraces the same interaction concept for exchanging information (such as contact information, media files, etc.) between mobile phones.

Schmidt et al. [2010] proposed “PhoneTouch”, a technique specifically designed for connecting a mobile phone to a camera-based interactive surface by physically tapping the phone’s corner on the surface (see Fig. 9). The tapping action creates a synchronous event that is detected independently by phone and surface. As the devices use different sensing modalities, the association is based on correlation in time. As a result, conflicts are possible if multiple phones tap a surface precisely within the same video frame. In addition to association, PhoneTouch also provides precise coordinates of the contact points (i.e. where the phone touches the surface). This enables the phone to act as a stylus for pointing and selecting an object on the surface. For example, a user can drop photos on or collect a photo from a precise location on the surface [Schmidt et al. 2012].

Moving devices together to create an impact on both simultaneously is fast and intuitive. The interaction requires little learning, since it is a common habit for people to bump objects together. The interaction can be seen as metaphors of (1) joining objects into one by pushing them together, as well as (2) building a trusting relationship by knocking objects together, (e.g. the etiquette of people “clinking” drinking glasses during a toast).

[3]Bump Technologies, Inc. http://bu.mp/.

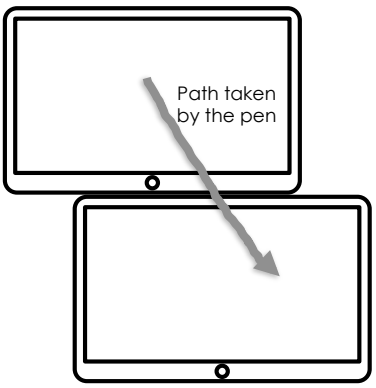

Fig. 10. An illustration of "Stitching" [Hinckley et al. 2004]: A user connects two tablets by drawing a stitching stroke from the top tablet to the bottom tablet.

4.5. Cross-Device Gestures

Many mobile devices nowadays have a large surface area for display as well as touch input (e.g. mobile phones and tablets). When users move the device surfaces together, they can perform gestures across the device surfaces in order to associate the devices.

Hinckley et al. [2004] demonstrated this approach to connecting devices with the "Stitching" technique for pen-based devices. Here, user perform a stroke-based gesture that *"spans multiple displays, consisting of a continuous pen motion that starts on one device, skips over the bezel of the screen, and ends on the screen of another device"*. A connection is established when a user draws (i.e. stitches) a continuous line across multiple touch displays (see Fig. 10). The drawing gesture is intuitive and trivial to execute, and the drawn stroke makes it transparent which devices are paired. In addition, it provides information on the relative spatial arrangement of the device surfaces, which can be exploited for treating the surfaces as one coherent display.

5. ENROLMENT-BASED ASSOCIATION

Devices are often attached with identities, for personalisation (e.g., a custom name) or unique identification (e.g., a system-assigned code). Enrolment-based association adopts this concept, where users attach an identity to a device, in order to be able to pair the device with other devices. Users can enrol a device with any type of information that is storable on the device and reproducible by the user. This enrolment takes the form of a one-time registration that enables the device for pairing. Users can then spontaneously associate the device with other devices they encounter, by presenting the enrolled identity to the target devices – an act of introducing one device to another.

For enrolment with an identity, users act through the devices' user interfaces, in common with input-based techniques. However, the conceptual model is not one of entering commands or data, but one of enrolling devices for trusted interaction. In our survey we identified three types of enrolment-based association that differ in the form of identity used, namely *Biometric*, *Rhythm Tapping*, and *Identifier Entry*.

5.1. Biometric

In authentication, a system can identify users by examining their *physiological* (related to the shape and features of the body) and/or *behavioural* (related to the manner or habits of a person) attributes [Jain et al. 2000]. These attributes are known as *biometrics*. Robust biometrics are distinctive across individuals, and ideally, no

two persons can present identical biometrics. Given this assumption, only the person him/herself can present matching biometrics to prove his/her identity.

Buhan et al. [2007] suggested "SAfE", which utilises physiological biometrics for secure pairing. They examined the use of facial features and of hand grip patterns. Device owners are first required to enrol their biometric information. In this one-time enrolment, the device takes multiple samples and stores them as a template. Once enrolled, the device is ready to pair with other SAfE-enabled devices. When two users meet, they can use their own device to take a snapshot of each other. The devices then exchange the snapshots, and each device extracts facial features and compares these with the stored features of it's user, in order to either accept or reject the connection. Hence, only a snapshot of the registered users can associate the devices [Buhan et al. 2007; Buhan et al. 2009]. As alternative to facial features, hand grip patterns were considered. During an encounter, this requires users to hand over their devices, so that these can take a sample of the other user's hand grip.

SAfE adopts physiological biometrics, which links a device to its owner. However, physiological biometrics are irreversible; once it is forged, it remains stolen for life, and there is no getting back to a secure state [Schneier 1999]. For security, the users must keep their biometrics private.

The usability and the interaction of SAfE depend on the type of biometrics employed. Different biometrics require different sensors and hardware. For facial recognition, the system only requires a simple interaction of taking a snapshot of the device owner's face. This is an intuitive way of registering a user as trusted, where the trust relationship is then extended to their device. However, Buhan et al. [2009] noted that the approach may not always be appropriate, e.g. taking pictures in restricted locations may draw unwanted attentions, or the system may fail because of ambient light conditions.

As facial recognition is a natural way of humans identify each other, people have a perception of how facial recognition works. Similarly, people perceive fingerprint biometrics as robust, because they are used as evidence in law enforcement [Coventry et al. 2003]. However, Iris verification – using the complex visual texture of the iris for distinctive identification – is in fact one of the most reliable type of biometrics [Coventry 2005].

We found no research that explores behavioural biometrics (e.g., gait, voice) for device association. However, behavioural biometrics have been widely used for user identification as well as authentication, and there is clearly potential for adopting it to device pairing. For example, Lester et al. [2004] presented a method of analysing people's gait to identify whether two devices are carried by the same person. Alternatively, voice print [Jain et al. 2000] is also possible.

5.2. Rhythm Tapping

People are rhythmic by nature; they often tap on objects to recreate rhythmic sound beats from a song. Wobbrock [2009] introduced "TapSong", a novel password entry method, where the key idea is to allow jingles to serve as text-less passwords. A TapSong password is made up of the rhythm of tap down/up events to a jingle timing model created by users. This work demonstrated that users can create and recall rhythms as identifiers.

Inspired by TapSong, Lin et al. [2011] presented "RhythmLink", where users tap an enrolled rhythm for pairing devices. Device owners enrol a rhythm into their device in a one-time registration. During spontaneous encounters with other (RhythmLink-enabled) devices, the user can enrol the same rhythm into a target device. The target device uses the rhythm to authenticate its connection with the user's device.

Input of rhythms into devices places minimal demands on required device hardware. Tapping on the device surface can be detected with microphones, accelerometers, or pressure sensors. Rhythm can also be entered via key or button presses.

5.3. Identifier Entry

Besides using user-generated identifiers as above, identifiers can be assigned by a system. Cellular network, for example, uses telephone numbers for users to identify devices.

Nicholson et al. [2006] presented "LoKey", a scheme that uses *Short Message Service* (SMS or text messaging) as a trusted auxiliary channel to send association data between GSM-enabled devices. Every LoKey-enabled device first needs a telephone number, supplied by a mobile network operator. The telephone number is then used as an identifier for the device. Upon device association, the user enters the telephone number into the target device (or vice versa, where the user enters the target device's phone number onto his/her device). Thereafter, the devices generate and exchange cryptographic data via the SMS channel and establish a secure connection.

LoKey was not designed for spontaneous encounters but rather for association of a priori known devices over a distance. However, LoKey can be applied in a spontaneous context, if user's can acquire a target device's phone number in situ.

6. MATCHING-BASED ASSOCIATION

Guidance-, input- and enrolment-based association involve user actions that devices sense and process to establish a connection. Matching-based association, in contrast, is centrally based on device output to users, for users to confirm or reject a connection. The conceptual model of matching-based schemes is to first establish a connection, in a sense speculatively, and to then involve the user in verifying that the connection matches their intent. Matching can have the purpose of providing users with control over connections that devices first establish automatically, but often it is combined with a guidance-, input- or enrolment technique. In the latter case, matching appears as a separate phase to the user, where they are prompted to confirm a connection that they first initiated via guidance, input or enrolment. The rationale for the additional phase is to ensure that the connection has been established as intended, and not been compromised by a third party (a "man in the middle") intercepting information exchanged during the initial setup.

We distinguish four types of matching-based device association: *Text Comparison*, *Listening*, *Pattern Matching*, and *Spatial Validation*.

6.1. Text Comparison

Much of today's information is represented in textual format. Manual comparison of text output for verification thus becomes an obvious solution. Devices display a text (e.g., a code), and users examine if the information matches exactly. In the family of MANA protocols [Gehrmann and Nyberg 2001; 2004], the second variant, MANA II, adopted this scheme. MANA II was designed for pairing two devices with limited input interface (it can be implemented with a single button on each device). Before pairing two devices, a user verifies that both devices are in their ready state. Once ready, the user signals the devices to begin association. The devices follow the MANA II protocol and exchange cryptographic keys. At the end of the process, the devices output a key and a *Message Authentication Code* (MAC). The user compares the key and the MAC values in both devices. If they agree, the user enters a signal of acceptance in both devices, or otherwise they signal rejection and the system cancels the pairing procedure.

The approach of having a user compare text output has been extended to many variations of security protocols for device association. This includes: "Short Authentication Strings (SAS)" [Vaudenay 2005], SAS for groups of devices [Laur and Pasini 2008], MANA IV (which can be seen as a generalisation of the previous string-comparison based protocols) [Laur and Nyberg 2006], an extension of MANA IV for groups [Valkonen et al. 2006], as well as the *numerical comparison* model of Bluetooth Simple Pairing [Bluetooth Special Interest Group 2006].

6.2. Listening

In the absence of a display component for outputting text, devices can present information via an audio channel for users to verify. Soriente et al. [2008] presented "Human-Assisted Pure Audio Device Pairing" (HAPADEP), which also uses audio tunes for human-assisted verification. In HAPADEP, the system uses a single audio channel for both protocol communication and human verification [Soriente et al. 2008; Goodrich et al. 2009]. It uses two types of encoder-decoder. System protocol data (for handshaking) is first encoded and sent via the audio channel as analogue signals that may sound like random noise (like the sound produced by a dial-up modem). Verification data is later encoded using a codec which produces rhythmic melodies. The second tune is for users to detect whether the devices produce matching audio sequences.

Researchers have also explored other audio encoding schemes. Goodrich et al. [2006] presented "Loud and Clear", which encodes verification data into *syntactically correct English-like sentences*. The system vocalises the sentences, and users verify by comparing the words of the sentences [Goodrich et al. 2006; Goodrich et al. 2009]. Encoding data into words creates several shortfalls. The number of commonly used English words is limited. Words with too many syllables should be omitted. English vocabulary contains homonyms (words that sound or spell the same, but have different meanings). Homonyms or words with similar enunciation should also be discarded. As a result, further restricting the pool of available words.

Using audio provides the advantage of not requiring the user to read. It is suitable for users with visual or reading disabilities. However, in a noisy environment, audio-based methods are prone to fail; noises can prevent or distract users from verifying audio messages. The approach can also be inappropriate depending on the social situation, for example in a quiet zone.

6.3. Pattern Matching

A minimal form of computer output is in binary signals. Assuming all computing devices have at least a simple binary output component (e.g. an LED or a monophonic speaker) to produce on-off signals, Prasad and Saxena [2008] proposed the technique of matching synchronised audiovisual patterns for pairing devices. Their system outputs verification data using devices' binary outputs – by emit blinking or beeping signals – for manual comparison. Saxena et al. [2008] later automated this verification using computer vision; thus, making it a guidance-based technique (see section 3.3). They compared the manual scheme with the automated scheme in a user study, and their results indicate that the automated scheme is generally faster and easier to execute. The finding is unsurprising, as the automation eliminates human errors and users no longer need to perform mentally exhausting tasks of matching binary outputs.

6.4. Spatial Validation

The above matching-based techniques require users to verify some form of device-generated information. In contrast, Kindberg and Zhang [2003b] proposed matching spatial positions of devices for device association. They used the combination of radio-frequency and ultrasound to locate the distance (by using the speed of sound) and the

Fig. 11. The two user interfaces for spatial references adopted by Mayrhofer et al. [2007] : (Left) an extension of Guinard et al. [2007]'s Gateways, and (Right) Kortuem et al. [2005]'s map view.

relative orientation of the target device. Once located, the system also displays information of the available surrounding devices for users to physically verify the target. To avoid ambiguity (e.g. multiple devices situated on the same line-of-sight), the user must turn as well as walk back-and-forth, so the system updates new positions and thus disambiguates the source of the signals. Consequently, the user validates a target device by identifying it using its spatial information. Mayrhofer et al. [2007] later generalised this concept and coined the term "Spatial References" with the following definition: "*Spatial references serve to establish shared context between a user and their device: a device can report a discovered network entity in a manner that the user can match with encountered devices, and a user can identify a target device in a way that their device can match with network entities*."

Mayrhofer et al. [2007] provided a complete implementation. Their system automatically discovers surrounding devices, computes their relative positions, and displays a spatially mapped visualisation of the discovered devices (see Fig. 11). The user matches the virtual representation with the actual device in the real world and then selects the target device from the visual display. Mayrhofer and Gostner [2007] conducted a user study to test the concept of using spatial user interface for selecting devices. Their results show that the participants were able to correctly select the target device and made very little errors.

7. SUMMARY OF SPONTANEOUS DEVICE ASSOCIATION SYSTEMS

To provide a quick reference for comparisons between techniques, tables I–IV summarise the association techniques discussed in the previous sections. Cells containing "n/a" indicate insufficient detail (or category not discussed) in the literature.

For each of the association techniques, in the first column of the tables, we identify the required action that a user must perform to trigger an association. In the second column, we then identify whether the technique implicitly provides device discovery. Some of the methods require their users to indicate which devices should associate; hence, the association is a one-step procedure as its device discovery is implicit (e.g. RhythmLink [Lin et al. 2011]). On the other hand, a two-step association (e.g. Bluetooth Simple Pairing [Bluetooth Special Interest Group 2006]) first requires users to explicitly find the connecting peer device, and then establish the association. The third column identifies the required minimum hardware that enables the interaction.

To summarise usability features provided by each technique, we adopt the usability categories identified by Chong and Gellersen [2012]. *Mobility* categorises whether an association is mobile or situated. A situated association denotes that the technique is only suitable for devices that are fixed in a location. A situated device cannot adopt a technique that was designed for mobility. For example, an association with an immobile device cannot adopt the shaking technique, as it requires a user moving the device rapidly.

Table I. Summary of Guidance-based Association Systems

Systems	Required User Action	Device Discovery	Enabling Hardware	Mobility	Max. Cardinality	User Controllability	Perceptibility	Max. Distance	Security	OOB Channel(s)
(Physical Contact)										
The Resurrecting Ducking [Stajano and Anderson 1999]	Create an electric contact between devices	Implicit	Metal Contact	Mobile	Pair	Single	Tangible	Reachable	✓	Elec. Connection
TAP [Park et al. 2006b; Park et al. 2006a]	Skin contact with devices	Implicit	Intrabody Communication	Mobile	Pair	Single	Tangible	Reachable	✗	Tactile
(Pointing)										
Point & Click [Beigl 1999]	Point an AIDE device towards another one	Implicit	Laser + receiver	Mobile	Pair	Individual	Visible	Noticeable	✗	Visible Laser
[Kindberg and Zhang 2003a]	Point a laser towards a light sensor	Implicit	Laser + receiver	Mobile	Pair	Individual	Visible	Noticeable	✓	Visible Laser
[Mayrhofer and Welch 2007]	Point a laser towards a light sensor	Implicit	Laser + receiver	Mobile	Pair	Individual	Visible	Noticeable	✓	Visible Laser
Network-in-a-box [Balfanz et al. 2004]	Point an infrared source towards an infrared sensor	Implicit	Infrared + receiver	Mobile	Pair	Individual	Imperceptible	Noticeable	✓	Infrared
gesturePen [Swindells et al. 2002]	Point an infrared-enabled gesturePen towards tags	Implicit	Infrared + receiver	Mobile	Pair	Individual	Imperceptible	Noticeable	✗	Infrared
Point&Connect [Peng et al. 2009]	Point a mobile phone towards another phone	Implicit	Speaker + Mic.	Mobile	Pair	Individual	Hearable	Noticeable	✗	Audio
(Visual Alignment)										
Seeing-Is-Believing [McCune et al. 2005; 2009]	Align a device's camera towards a 2D barcode	Implicit	Camera + Display	Mobile	Pair	Individual	Visible	Noticeable	✓	Comp. Visual
VIC (or Blinking- Lights) [Saxena et al. 2006]	Align a device's camera towards an LED light	Explicit	Camera + LED	Mobile	Pair	Individual	Visible	Noticeable	✓	Visible Light
Audio-Blink and Blink-Blink [Saxena et al. 2008]	Align a device's camera towards an LED light	Explicit	Cam. + LED + Speak. + Mic.	Mobile	Pair	Individual	Visible / Hearable	Noticeable	✓	Visual + Audio
Blink 'em All [Saxena and Uddin 2009a]	Align a device's camera towards a group of LED lights	Explicit	Camera + LEDs	Mobile	Restricted	Individual	Visible	Noticeable	✓	Visible Light
BlueTable [Wilson and Sarin 2007; Ramos et al. 2009]	Align a device's screen towards a surface's camera	Implicit	Surface + Display	Situated	Restricted	Individual	Visible	Noticeable	✗	Visible Light

(continued)

Table I. Summary of Guidance-based Association Systems (Continued)

Systems	Required User Action	Device Discovery	Enabling Hardware	Mobility	Max. Cardinality	User Controllability	Perceptibility	Max. Distance	Security	OOB Channel(s)
...	...	...	...	...	...	...	...	...	...	...
(Co-location)										
Amigo [Varshavsky et al. 2007; Scannell et al. 2009]	Place devices within a WiFi-enabled room	Explicit	Radio transceiver	Mobile	*n/a*	Individual	Imperceptible	Noticeable	✓	Radio Data
[Kindberg et al. 2002]	Place devices in an infrared-enabled room	Explicit	Infrared + receiver	Situated	*n/a*	Individual	Imperceptible	Noticeable	✓	Infrared
(Proximity)										
Proximal Interactions [Rekimoto et al. 2003b]	Bring a handheld device near a computer	Implicit	RFID/Infrared	Mobile	Pair	Individual	Tangible	Reachable	✓	RFID/ Infrared
Touch & Connect [Seewoonauth et al. 2009]	Place a mobile phone near an NFC tag	Implicit	NFC	Mobile	Pair	Individual	Tangible	Reachable	✗	NFC Prox.
GroupTap [Chong et al. 2011]	Bring devices near smart objects in a sequence	Implicit	NFC	Mobile	Unlimited	Individual	Tangible	Reachable	✓	NFC Prox.
ProxNet [Rekimoto et al. 2004]	Bring a ProxNet device near a computer	Implicit	Radio transceiver	Mobile	Pair	Individual	Tangible	Reachable	✓	Signal Strength
UbiSound [Claycomb and Shin 2009]	Bring one mobile phone near another one	*n/a*	Speaker + Mic.	Mobile	Pair	Individual	Hearable	Noticeable	✗	Audio
(Physical Extension)										
tranStick [Ayatsuka and Rekimoto 2005]	Insert memory cards	Implicit	Memory card + reader	Mobile	Pair (but extendable)	Individual	Tangible	Reachable	✗	Human Action

Table II. Summary of Input-based Association Systems

Systems	Required User Action	Device Discovery	Enabling Hardware	Mobility	Max. Cardinality	User Controllability	Perceptibility	Max. Distance	Security	OOB Channel(s)
(Character Input)										
MANA I [Gehrmann and Nyberg 2001; 2004; Gehrmann et al. 2004]	Copy a text from a device and enter it into anther	Explicit	Buttons + Display	Mobile	Pair	Individual	Tangible	Reachable	✓	Human Action
MANA III [Gehrmann et al. 2004; Gehrmann and Nyberg 2004]	Select a textual passkey and enter it into pairing devices	Explicit	Buttons	Mobile	Pair	Individual	Tangible	Reachable	✓	Human Action
Gesture-based authentication [Patel et al. 2004]	Mimic a machine-selected gesture sequence	Explicit	Accelerometer + Display	Situated	Pair	Single	Tangible	Reachable	✓	Movement
GesturePIN [Chong et al. 2010]	Enter predefined gestures as a passkey	Explicit	Accelerometer + Display	Mobile	Unlimited	Individual	Tangible	Reachable	✗	Movement
(Button Pressing)										
SyncTap [Rekimoto et al. 2003a; Rekimoto 2004]	Push sync buttons simultaneously	Implicit	Button	Mobile	Pair	Single	Tangible	Reachable	✓	Human Action
BlueRendezvous [Ramos et al. 2009]	Push sync buttons from a number pad	Implicit	Button	Mobile	Unlimited	Individual	Tangible	Reachable	✗	Human Action
BEDA [Soriente et al. 2007; 2009]	Enter binary sequences by pushing a button	Explicit	Button	Mobile	Pair.	Single	Tangible	Reachable	✓	Human Action
Touch-and-Connect [Iwasaki et al. 2003]	First push "Socket", then push "Plug"	Implicit	Button	Mobile	Pair	Individual	Tangible	Reachable	✗	Human Action
(Shaking)										
Smart-Its Friends [Holmquist et al. 2001]	Hold devices and shake them simultaneously	Implicit	Accelerometer	Mobile	Restricted	Single	Tangible	Reachable	✗	Movement
Shake well before use [Mayrhofer and Gellersen 2007b; 2009]	Hold devices and shake them simultaneously	Implicit	Accelerometer	Mobile	Restricted	Single	Tangible	Reachable	✓	Movement
Martini Synch [Kirovski et al. 2007b; 2007a]	Hold devices and shake them simultaneously	Explicit	Accelerometer	Mobile	Restricted	Single	Tangible	Reachable	✓	Movement
Shake Them Up [Castelluccia and Mutaf 2005]	Shake devices separately	*n/a*	Radio transceiver	Mobile	Pair	Individual	Tangible	Reachable	✓	Movement + Radio

(continued)

Table II. Summary of Input-based Association Systems (Continued)

Systems	Required User Action	Device Discovery	Enabling Hardware	Mobility	Max. Cardinality	User Controllability	Perceptibility	Max. Distance	Security	OOB Channel(s)
...	...	...	...	...	...	...	...	...	...	...
(Impact)										
Synchronous Gestures [Hinckley 2003]	Bump devices towards each other	Implicit	Accelerometer	Mobile	Pair	Single	Tangible	Reachable	✗	Movement
PhoneTouch [Schmidt et al. 2010]	Tap a phone on an interactive surface	Implicit	Accelerometer + Surface	Situated	Pair	Individual	Tangible	Reachable	✗	Movement
(Cross-Device Gesture)										
Stitching [Hinckley et al. 2004]	Draw a stroke across devices	Implicit	Touch Screen	Mobile	Pair	Single	Tangible	Reachable	✗	Human Action

Table III. Summary of Enrolment-based Association Systems

Systems	Required User Action	Device Discovery	Enabling Hardware	Mobility	Max. Cardinality	User Controllability	Perceptibility	Max. Distance	Security	OOB Channel(s)
(Biometric)										
SAfE [Buhan et al. 2007; Buhan et al. 2009]	Take a snap shot of enrolled users' biometrics	*n/a*	Biometric Sensor	Mobile	Pair	Single	*Depends on the biometric type*	Reachable	✓	Comp. Visual
(Rhythm Tapping)										
RhythmLink [Lin et al. 2011]	Tap devices' enrolled rhythms	Implicit	Binary Sensor	Mobile	Pair	Single	Tangible	Reachable	✓	Human Action + Audio
(Identifier Entry)										
LoKey [Nicholson et al. 2006]	Enter a telephone number	*n/a*	GSM Phone	Mobile	Pair	Individual	Tangible	*n/a*	✓	SMS (GSM)

Table IV. Summary of Matching-based Association Systems

Systems	Required User Action	Device Discovery	Enabling Hardware	Mobility	Max. Cardinality	User Controllability	Perceptibility	Max. Distance	Security	OOB Channel(s)
(Text Comparison)										
MANA II [Gehrmann and Nyberg 2001; 2004]	Compare text	Explicit	Button	Mobile	Pair	Individual	Tangible	Reachable	✓	Human Validation
SAS [Vaudenay 2005]	Compare text	Explicit	Button	Mobile	Pair	Individual	Tangible	Reachable	✓	Human Validation
MANA IV [Laur and Nyberg 2006]	Compare text	Explicit	Button	Mobile	Pair	Individual	Tangible	Reachable	✓	Human Validation
MANA IV for groups [Valkonen et al. 2006]	Compare text	Explicit	Button	Mobile	Unlimited	Individual	Tangible	Reachable	✓	Human Validation
Bluetooth Simple Pairing: Numerical Comparison [Bluetooth Special Interest Group 2006]	Compare numerical text	Explicit	Button	Mobile	Pair	Individual	Tangible	Reachable	✓	Human Validation
(Listening)										
HAPADEP [Soriente et al. 2008; Goodrich et al. 2009]	Check if devices' audio sources are in harmony	Explicit	Speaker + Button	Mobile	Pair	Individual	Hearable	Noticeable	✓	Audio
Loud and Clear [Goodrich et al. 2006; Goodrich et al. 2009]	Listen for and compare machine-generated words	Explicit	Speaker + Button	Mobile	Pair	Individual	Hearable	Noticeable	✓	Audiovisual
(Pattern Matching)										
Beep-Beep, Blink-Blink and Beep-Blink [Prasad and Saxena 2008]	Compare audiovisual binary patterns	Explicit	LED + Speaker	Mobile	Pair	Individual	Visible / Hearable	Noticeable	✓	Audiovisual
(Spatial Validation)										
[Kindberg and Zhang 2003b]	Selecta device baesd on relative distance and orientation	Explicit	Ultrasound transceiver	Mobile	Pair	Individual	Imperceptible	Noticeable	✓	Ultrasound + Radio
Spatial References [Mayrhofer et al. 2007]	Select a device from a spatial map	Explicit	Ultrasound transceiver	Mobile	Pair	Individual	Imperceptible	Noticeable	✓	Ultrasound + Radio

Maximum cardinality denotes the maximum number of devices that a technique can accommodate. In reality, we find situations where a group of devices associate. An association technique can fall into one of the following three categories: pairing (two devices only), restricted (can accommodate several devices, but constrained by some physical limitations), and unlimited (the number of devices is not limited). Selecting the wrong cardinality may not necessarily disable devices to associate, but it deprives usability, as users need to do more work and the process consumes more time. Adopting a pairing technique for a group association requires its user to perform multiple pairings; if N devices are involved, the user must conduct $N - 1$ pairings.

Controllability indicates social context; an association could be controlled by either a single user, where the rest of the users must surrender their possession of their devices, or individual user, where each user holds on to their own devices. Personal devices contain private information. People are reluctant to share their personal devices with others, especially strangers, as it raises privacy concerns [Uzun et al. 2011]. Techniques for individual-user association provide the advantage of establishing device connections while devices always remain with their owners. However, association with public devices needs single-user techniques, as the corresponding devices are not controlled by another human operator.

Perceptibility categorises the affordance of how users perceive the execution of an association (i.e. the clues given by the hardware that indicates an association is happening). The affordance could be either: tangible, visible, hearable, or imperceptible. Hardware that provides perceptible information helps users to judge the progress of an association. An imperceptible association fundamentally requires extra output hardware (e.g. a display) for providing users with system feedback.

Maximum distance indicates how far devices could be apart during the association. Devices can be within either a reachable (an arm's length) or noticeable (beyond an arm's length) distance. If a system adopts a technique that requires devices to be within a reachable distance, the devices are forced to be together during association. However, if the surrounding context enforces the devices to be separated (e.g. by a glass window), then the user cannot bring the device with a reachable action for association.

The last two columns in the tables indicate whether the literature includes a discussion of how to incorporate security within the suggested association technique, as well as the out-of-band channel(s) used for establishing an association.

The summary tables are convenient and useful for choosing an association technique with specific requirements. For example, if a system uses mobile hardware with limited user-interface, the designer can consider motion based techniques, such as using accelerometers. A quick glance at the tables shows that only the *shaking* and the *passkey* categories (in table II) contain techniques that support accelerometers. However, the passkey techniques are not suitable as they also require a display. For a faster association, the designer can further eliminate techniques that require device discovery. At this stage, only two options are still feasible; depends on the sensitivity of communication, if security is required, the *Shake Well Before Use* approach [Mayrhofer and Gellersen 2007b; 2009] is the most appropriate option.

8. EMPIRICAL STUDIES

Up until now, we presented existing device association techniques. Many of the techniques were designed for/with specific requirements or limitations. A technique that fits for one scenario may not be adequate for another purpose. Thus, analysing between the techniques is not straightforward and can be challenging. To understand the usability of device association, researchers have conducted empirical studies on learning how users execute device association. In this section, we discuss three user

study methodologies that researchers conducted: *Preliminary*, *Comparative* and *User-Defined Action*.

8.1. Preliminary Studies

From a system's point of view, it is important to show that a device association technique works for its intended purpose. However, from a usability's point of view, the importance lies with whether the technique is usable by people (other than the designers themselves) as well as how they feel about the interaction. For the first step of understanding usability, researchers conduct preliminary (or informal) user studies in laboratory settings to determine people's performance (i.e. quantitative results) as well as their acceptance (i.e. qualitative results) of a technique. For example, Ayatsuka and Rekimoto [2005] reported small-scale preliminary user studies with five or less participants. Their goal was to investigate whether people understand and accept their tranStick concept.

Preliminary studies are confined within the testing technique. This type of study is limited, as people only experience one technique. It gives no indications of how well people perform and/or prefer using the technique compares to other existing ones. To understand usability differences between techniques, comparative studies are needed.

8.2. Comparative Studies

Over the past decade, researchers have demonstrated numerous device association techniques and standardisation bodies have also worked on improving protocols. While some of the techniques were motivated by technology such as limited hardware and interfaces, others were conceived by security or usability requirements. Upon recent years, new usability questions arose, such as amongst the methods that provide equivalent end result (e.g. similar security strengths), which of them is the most efficient? To answer such questions, researchers carried out comparative usability evaluations, where the participants first experience a group of techniques that associate the same devices and then evaluate the different techniques.

The need for comparative studies was first introduced by Uzun et al. [2007]. They focused on secure pairing schemes (hence, associating two devices) that are based on the *short authentication string (SAS) protocol* [Laur and Nyberg 2006; Vaudenay 2005]. They compared five interaction techniques:

— ***Compare-and-Confirm*** – both devices display a text and a user only confirms if both display the same text (hence, text comparison; e.g. MANA II [Gehrmann and Nyberg 2001; 2004] and MANA IV [Laur and Nyberg 2006]).
— ***Select-and-Confirm*** – one device displays a number, a user selects the same number from a list of random numbers on the second device. On the first device, the user is prompted whether the second device indicates a successful association.
— ***Copy-and-Confirm*** – a user copies a text displayed on one device and enters it into the second one, and at the end of the association, the first device prompts whether the association is successful (hence, character input; e.g. MANA I [Gehrmann and Nyberg 2001; 2004; Gehrmann et al. 2004]).
— ***Copy*** – similar to *Copy-and-Confirm*, but without the prompting at the end
— ***Choose-and-Enter*** – a user decides a random number as a passkey and enters it on both devices (hence, character input; e.g. MANA III [Gehrmann et al. 2004; Gehrmann and Nyberg 2004]).

Uzun et al. [2007] conducted the study in United States and Finland. For each location, they recruited 40 participants. Their participants were first given an introduction regarding the operation of the devices and the above five interaction techniques. The participants were then asked to perform the techniques, in a randomised order. Dur-

ing the study, the researchers collected the participants' *average completion time*; *fatal error rate* – a violation of a security goal (e.g. devices show different text but the user still confirms the text are identical, or choosing an easy-to-guess passkey, "0000" for example); and *total user error rate* – all other user errors other than fatal errors (e.g. accidentally pushing a wrong button).

The results of the study show that *Select-and-Confirm*, *Copy-and-Confirm* and *Choose-and-Enter* had non-zero fatal error rates, caused by users not strictly following the prescribed order of the interaction. The participants also negatively perceived the two latter techniques. Users perceived *Compare-and-Confirm* and *Select-and-Confirm* as easy to use, while *Copy* is difficult but inherently resistant to fatal errors. However, the users considered *Copy* to be more secure and more professional than the other two techniques. Based on the results, Uzun et al. [2007] formulated three guidelines: (1) default action must correspond to the safest choice; (2) user actions must be labeled using task-specific words; and (3) multi-step interactions should be avoided.

Besides text-based methods, Kumar et al. [2009b][4] later expanded the study with several other OOB channels (e.g. audio, computer vision, etc.). They compared thirteen secure pairing techniques. Amongst the techniques, number comparison was the overall winner with respect to error rates, completion time, ease-of-use and user preferences. When one device had a speaker and the other one had a microphone, audio pairing (e.g., HAPADEP [Soriente et al. 2008; Goodrich et al. 2009]) was the preferred method. The results show that for interface-constrained devices (e.g. headsets), BEDA Vibrate-Button [Soriente et al. 2007; 2009] was the best choice. Also, given a choice between the camera-based techniques (e.g. SiB [McCune et al. 2005; 2009] and Blinking-Lights [Saxena et al. 2006]), SiB is preferred due to its better usability.

Kobsa et al. [2009] emphasised that several issues existed in Kumar et al. [2009a]'s study (e.g. the set of participants was unbalanced, subjects' fatigue, uneven number of test cases, etc.). Instead, Kobsa et al. [2009] compared eleven pairing methods with a set of participants that was balanced by age, gender and prior experience with pairing devices. Concurrent to their study, Kainda et al. [2009] independently compared a set of fourteen secure pairing methods. Results from both studies showed that users achieved faster average completion time when using numerical-based methods than image-based or audio-based methods. Uzun et al. [2011] refined the study by only including techniques that enable "social pairing". Similar to the "Individual User" controllability described by Chong and Gellersen [2012], a social pairing scenario involves two different users establishing pairing between their respective devices. In other words, each user operates their own device, without the need of surrendering the possession of their devices. Their findings showed comparison-based methods over the visual channel are preferred by users. In contrast to Kobsa et al. [2009] and Kainda et al. [2009]'s findings, Uzun et al. [2011] suggested that, amongst their tested techniques, sentence comparison yields lower errors and is the most robust, fastest, as well as the users most preferred method.

While the above studies mainly focused on finding the most usable and secure method(s) amongst several existing approaches, Ion et al. [2010] took into account that the variety of situations in which pairing maybe used in real life. Instead of comparing techniques only, Ion et al. [2010] examined how users perceive the suitability of different techniques for different situations. In other words, would different situations affect people's preference of a pairing method? In their study, four techniques (*Select the Device*, *Take a Picture*, *Listen up*, and *Push the Button*) and three situations (*print a document*, *make a payment*, and *send electronic business cards*) were tested. Their findings showed that people do not always use the easiest or the most popular method.

[4]This study was first published in Kumar et al. [2009a]

People select techniques based on *data sensitivity*, *time constraints*, and *appropriateness for a particular social context*.

Extending the cardinality of devices (from pair to many), Kainda et al. [2010] evaluated secure device associations in group scenarios. Coordination and cooperation are required from all group members. Four group association techniques were tested, with variable group sizes between two to six members per group. Their results indicate that, on the contrary to conventional beliefs, group scenarios are less prone to failures, because group members help each other to overcome the weaknesses of struggling members. Hence, the success of a group association is the sum of group members' efforts. With the same motivation, Nithyanand et al. [2010] independently examined secure group association. Besides examining the interaction of different techniques, they also focused on the effect of techniques being controlled by a centralised group member (i.e. a *leader*) versus *peer-based*, where every member had the same duty. Five SAS-based techniques were tested with fixed numbers of people per group – either four or six per group. Overall, their results show that the technique of *peer-based verification with users entering the group size* achieved the best usability results, as well as the most robust against the simulated attacks in the study. They further discussed that requiring the users to examine the group size provides additional security. Their participants perceived that entering group size as more usable and secure than verifying group size.

Results from comparative studies provide an indication of users' preferences and performance between the examined techniques. However, several drawbacks need to be considered. Studies that examined many methods at once can easily overwhelm the participants with fatigue and confusions [Ion et al. 2010]. The studies were often conducted in a lab environment. They fail to reflect applications in real life. Furthermore, the results only reflect the quality amongst the compared methods. Within this fast developing research area, new methods are often invented. To understand the differences between the old and new methods, each time a new method is created, another comparative study that includes the new methods is required. Hence, results from comparative studies can quickly become outdated. Although all of the studies above compared different user interaction techniques for associating devices, they were all motivated by usable security. The underlying meanings of the interaction techniques were never examined.

8.3. User-Defined Action Studies

Other than comparing a selection of existing techniques, an alternative approach to understand how people associate devices is via the *guessability study* methodology [Wobbrock et al. 2005]. On the contrary to comparative studies, guessability studies take a bottom-up approach. The studies first portray the participants with the *end effect* and then request them to perform its *cause* [Wobbrock et al. 2009]. This methodology aims to elicit *user-defined actions*, based on what people desire, and it evaluates only the inputs without prior learning or premeditation. In other words, letting users define their own methods for device association.

Kray et al. [2010] was the first to adopt this methodology for device association study. Their aims were to understand the gestures people produce for connecting a mobile phone to another phone, to a public display, or to a tabletop; hence, three conditions. During their study, real devices were used, but switched off. Their participants were asked to produce meaningful gestures spontaneously to trigger a set of twenty activities, such as "*... to send an item from the phone to the other device*", "*... to download an item from the other device to the phone*", etc. Each participant performed twenty gestures per condition (i.e. phone plus another device) and experienced all three conditions. Kray et al. [2010] then categorised the results based on four binary properties:

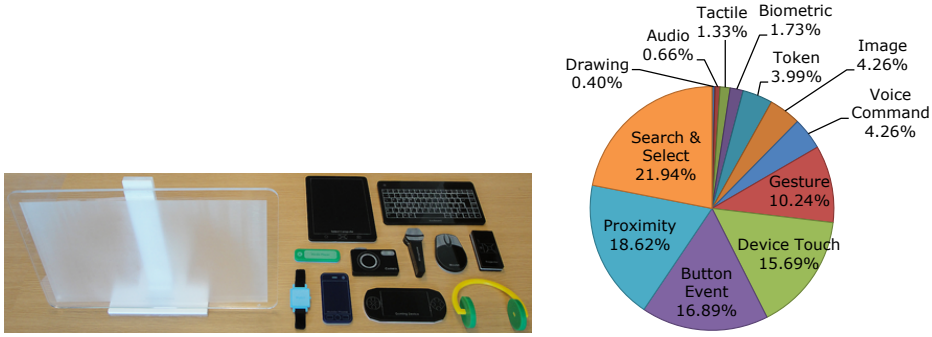

Fig. 12. (Left) The low-fidelity acrylic prototypes used in Chong and Gellersen [2011]. (Top row) A situated *interactive display*, a *tablet computer* and a *wireless keyboard*. (Second row) A *media player*, a *digital camera*, a *wireless microphone*, a *wireless mouse* and a *handheld projector*. (Bottom row) A *digital watch*, a *mobile phone*, a *gaming device* and *wireless headphones*. (Right) An illustration of the twelve categories in proportional to their overall occurrences.

distance, *touch*, *location* and *rotation*; and two attributes measured in time: *delay* and *duration*. More than 70% of the gestures incurred a change in relative distance; also more than 70% resulted in a change in the absolute location of the phone. Touch and rotation occurred less frequently. Only 20% of the gestures for phone-to-public display involved the two devices touching, while touch events occurred twice as frequent (39%) in the phone-to-phone and the phone-to-tabletop conditions. Also, about 50% of the gestures involved a rotation of the mobile phone. Overall, Kray et al. [2010] provided an analysis of the basic properties of gestures, which is useful for the design of future phones (e.g. choosing sensors that can recognise the gestures).

Ideally, a user should be able to associate wireless devices quickly, extemporaneously and without explicit instructions. Whereas Kray et al. [2010]'s study focused on finding gestures for various activities, Chong and Gellersen [2011] focused on one activity – associating wireless devices. They conducted a large-scale study on understanding, instead of only gestures and regardless of the limitations posed by the current hardware, the types of actions that people spontaneously produce to connect wireless devices. To avoid influences from existing interfaces, the use of real devices was prohibited. The study instead adopted low-fidelity "plastic" surrogates of twelve types of wireless devices (see Fig. 12). In total, thirty-seven combinations of devices were examined (with thirty pairings and seven combinations of three or more devices). The study results show twelve distinctive categories of user-defined actions (see Fig. 12). The top five categories have similar shares, and their sum dominates over 80% of the overall occurrences. Besides their dominance, the results also show their high coverage across different device combinations, but not a single category had achieved dominance in any of the combinations. Further examination shows that besides the existing techniques found in research or practice, people also have their own ideas of how devices should be associated. Although research had shown some intuitive techniques, for normal people the techniques might not be spontaneously obvious, for example *shaking*.

The results by Chong and Gellersen [2011] only represent scenarios where device associations were controlled by one operator. When multiple users are involved, device association is not just a simple extension of pairings. In social situations, people often want to connect their devices to share digital resources. To understand how groups of users associate devices, Chong and Gellersen [2013] conducted a follow-up study and extended the guessability study methodology for groups. Participants worked in groups of four and were asked to connect a predefined set of personal devices. Similar to the

Fig. 13. (Left) The plastic components used in Chong and Gellersen [2013]. The components represent (Top row) a *situated computer*, (Bottom, from left to right) a *bendable computer*, a *tablet*, a *mobile phone* and a *tiny computer*. (Right) A video screenshot of a recorded study session. A group of four participants sat around each other, while the experimenter (sitting in the back) mediated the session.

single-operator study, for each scenario, the experimenter allocated the participants with plastic components that represent personal devices (see Fig. 13). The participants took turns to suggest techniques for associating the devices. Results of the study show that many people conceptualise group association as a one-step procedure, instead of multiple pairings. People's expectation of how group association should be conducted is largely influenced by the *mobility* and *physicality* (such as size, affordance, etc.) of devices, as well as by the persons' prior knowledge of interaction with technology (such as from experience and media).

People often relate techniques for connecting devices should be similar to the interactions they previously learnt or encountered with other systems [Chong and Gellersen 2011; 2013]. As technology evolves, new interaction techniques are introduced, and people are continuously being exposed to them. This effectively influences people's conceptualisation of how technology should be manipulated. For example, a decade ago, multi-touch interaction was not common because very few hardware support the functionality. With the proliferation of smart phones and tablets, it is now applied in many applications. More people are getting familiar with new interaction techniques. So, people's expectation on the interaction for associating devices inherently changes over time. Results from guessability studies enlighten researchers and designers of the users' *current* conceptualisations. The knowledge learnt from guessability studies is intended to influence the current design of device association, which in turn will influence how people conceptualise device association in the future.

9. CONCLUSION

Much research work on spontaneous device association has focused on enabling users to establish connections in a secure manner. However, the outlook of users, such as the user interaction involved in an association process, was often neglected. As the process involves users, it is crucial for researchers to understand the underlying user's model of process. Through surveying existing work, we realised that conceptual models are frequently implied rather than explicit in the design of techniques. Our effort here is to bring the conceptual models to the foreground. We presented a comprehensive overview of existing interactive techniques for spontaneous device association; we summarised usability attributes of the techniques (see Table I–IV) to aid comparison, and reviewed user studies on device association reported in the literature. In essence, this article covers state of the art from the spectrum of user interaction for spontaneous device association.

The current state of this research field has yet to mature. Although many individual research work examined specific issues, researchers have omitted the general picture of device association. There are fundamental issues that are in dire need of attention.

Below, we outline several open challenges that researchers must consider in order for this research field to advance.

9.1. Understand People

In spontaneous interaction scenarios, opportunities for associating devices arise upon users' desire. The process is triggered by some form of user interaction and executes with the help of users. For any association to be successful, it relies on its users' ability to operate the system correctly; hence, *usability* has a great impact. A crucial design goal is to make association techniques practical and usable. For us to achieve this goal, it becomes obvious that we need good understanding of users. Although obvious, through our survey, we realised that this was often overlooked by researchers. In many occasions, usability was an afterthought; researchers were often motivated to design new techniques based on new technology, and then thought of how users can support the technology. Usability is a crucial aspect and needs attention since the start of design [Chong and Gellersen 2012]. By designing for people, the design would be practical and usable.

To complement designing for users, researchers also need to evaluate with users. Technology-driven research often lacks rigorous user evaluation. Many of the literature we surveyed did not include a user study to collect usability measures; hence, their usability flaws are still unknown. In section 8, we revealed several methodologies researchers took for studying users in device association. For this field to advance, more studies and new methodologies for understanding users are needed.

9.2. Group Association

As shown in our summary tables (see tables I–IV), majority of the existing techniques were designed for pairing two devices. In scenarios where the cardinality increases (i.e. three or more devices), the procedure for device association becomes more complicated. Adopting a method that was designed for pairing to establish a group association (i.e. users connect two devices at a time, until every device is connected) costs more work for the users [Chong and Gellersen 2010; 2012]. Besides more work, there are several issues researchers must also consider.

In group scenarios, system designers need to decide whether a network should be fully connected (i.e. every device is connected to everyone else) or devices only need to connect to the closest neighbours. Having a group network means that there needs a mechanism for access control. Access control can be maintain either by a group leader or every group member who shares the same duty [Kainda et al. 2010; Nithyanand et al. 2010]. In addition, designers also need to consider the actions people would intuitively perform as a group to establish an association [Chong and Gellersen 2013].

After a network is formed, new members may want to join the network. Designers also need to consider how latecomers can associate with devices that are already connected. For example, two groups may want to combine into one. One simple way is to gather everyone to freshly form a new group network. Alternatively, Valkonen et al. [2006] suggested the concept of nominating *gatekeepers*. Each group nominates a representative (i.e. the gatekeeper). The gatekeepers associate amongst each other. Their association essentially symbolises an association between the groups. Thereafter, the members from the different groups can communicate with one another via the gatekeepers, and hence, the connection of the gatekeepers bridges the groups.

Besides allowing new members to join, we also need to consider members leaving. As discussed earlier, disconnecting devices from an existing group is crucial. When a member leaves permanently, from a system's point of view, all shared secrets known by the leaving member (such as encryption keys) should be re-negotiated. However, for users, this step should be as seamless as possible. The users only need a confir-

mation that the leaving members has left correctly, while the system executes the rest of the procedure. Another functionality that needs attention is revocation of a device [Valkonen et al. 2006]. In an extreme case where a group expels a member, the system designers need to consider how decisions should be made, whether it should be democratic, where every member votes, or dictated by a group leader. In any case, all group members must be informed.

Group association is inherently a social activity. Kuo et al. [2008] examined the social dynamics of multi-user group association and identified social and situational aspects. Their work demonstrated that protocol designs are situation dependent, and no single solution is appropriate for all situations.

9.3. Get Out of the Lab

All existing empirical studies we surveyed were conducted in controlled lab environments. The results of those studies reveal interesting trends in people's preferences for certain types of actions (or techniques) for associating devices. However, to observe how device association emerges as part of people's everyday life, it is important to study the use of various techniques in a real-world context. Immediately, some questions arise: what factors influence people's choice of device association techniques in real-life spontaneous interaction scenarios? How do people cope with device association when they are in a rush (such as limited time and under pressure) [Saxena and Uddin 2009b]? What influences the adoption of a new association technique? When we take device association out of the lab, it is no longer just asking for people's performance and preferences, but instead asking for how device association affect and assist people's lives. So far, we have not found any studies that explore device association in the wild. We believe that this is an important next step for researchers to understand how device association can be applied.

9.4. Usability vs. Security

Although this article focused mainly on usability and user interaction, security in device association is equally fundamental. For many years in research, there is an extensive ongoing debate about the effects and tradeoffs between security and usability. Often, to secure a system, users need to spend more effort. Although secure, the users might not understand the necessity and the underlying principle of spending such effort, so instead they see security as burdensome. Users themselves have their own expectations of security. Kindberg et al. [2004] showed that users' perceived security needs not necessarily be aligned with the real security. Convenience and social issues are as equally important as security and trust issues in systems design. The goal is therefore to have a balance of satisfying the needs and desires of users, as well as providing adequate technical supports to ensure the established communication meets a certain security standard.

9.5. Device Dissociation

While device association is the process of establishing a virtual connection, *device dissociation* is the process of terminating (i.e., disconnecting) an established virtual connection of linked devices.

With traditional cable connections, devices can simply be disconnected by physically unplugging the cable. However, with wireless devices, the metaphor of plugging/unplugging cables no longer applies. Throughout this paper, we surveyed numerous user interaction techniques for associating devices. However, research has often neglected the process of users terminating a virtual connection. At the end of a session, when a connection is no longer needed, users may want to disconnect their devices. This helps to avoid sending information unintentionally. For example, in a group

network that involves three or more devices, the system needs an assuring method that only the members that no longer want to participate are disconnected, while the connection remains for the rest of group.

What approaches are appropriate for dissociating devices? Researchers seldom consider the issues when the connection is no longer needed or discuss the process of disconnecting wireless devices. At the minimum, every connection has a common user action which enforces dissociation. A user can simply disconnect devices by switching them off or taking them out of the vicinity of the network. By doing so, the connected devices can no longer communicate, and thus forcing the connection to terminate. However, if a user takes a device away only for a brief moment, like accidentally stepped away, designers need to consider whether the user should re-associate the device. A system that requires frequent re-association can inherently affect its overall usability.

For any spontaneous device association, users perform an action to trigger the association. The same action can be applied for dissociation. For example, SyncTap requires a user pushing buttons simultaneously [Rekimoto et al. 2003a; Rekimoto 2004]. By repeating this action after a connection is built, it can terminate the connection. On the other hand, shaking [Bichler et al. 2007; Holmquist et al. 2001; Kirovski et al. 2007b; 2007a; Mayrhofer and Gellersen 2007b; 2009] is not so straightforward. Some people may perceive shaking as mixing things (e.g., mixing cocktails). Although a system can employ shaking for disconnecting devices, from a user's point of view, is shaking conceptually a logical action for dissociating devices (i.e., shaking to "unmix" things)? Alternatively, researchers can examine whether the inverse of an association technique is suitable for dissociation. For example, people have suggested the use of a throw gesture, like throwing an object, towards a target device for association [Chong and Gellersen 2011] or Ayatsuka and Rekimoto [2005]'s tranStick (plugging tokens); by mirroring the action, the inverse (i.e., the act of pulling a device away from a connected peer device or unplugging a token) can be used for dissociation. Lastly, a user can perform a separate unrelated action that explicitly indicates dissociation. In summary, we envision three types of dissociation: (1) using an identical action for both connecting and disconnecting devices, (2) using symmetrical actions, where one denotes association and its inverse denotes dissociation, and (3) using an explicit unrelated action for dissociation.

So far, we found no research that investigates user interaction for dissociating devices. We hope to see research on this topic in the near future.

9.6. Final Remarks

Currently, we are witnessing a proliferation of wireless devices. More information will be shared, and number of opportunities for connecting devices inherently increases. As devices evolve, they come in different forms, shapes and sizes. In the near future, we anticipate and foresee a high demand of intuitive techniques for connecting various types of devices. Although research of device association has been ongoing for many years, our current understanding of the field is still limited. More research into understanding people is needed for designers to devise usable techniques. To help shape the future, this article presented an overview of the current situation of device association and outlined possible future directions. Finally, the work we presented is only a first step of unifying the research of user interaction for spontaneous device association. We hereby invite all researchers to extend this work and draw out new dimensions.

ACKNOWLEDGMENTS

Thanks to Jonathan McCune, Enrico Rukzio and Dominik Schmidt for giving us reprint permission and the original images for Fig. 3 (p.8), Fig. 4 (p.10) and Fig. 9 (p.15), respectively. Thanks to Jin Nakazawa

for pointing out the importance of disconnecting devices. Finally, we gratefully thank the reviewers and the associate editor, Jonathan Grudin, for their reading and valuable feedback. Ming Ki Chong was supported by Overseas Research Students Awards Scheme (ORSAS). Parts of this work have been carried out within the scope of *u'smile*, the Josef Ressel Center for User-Friendly Secure Mobile Environments. We gratefully acknowledge funding and support by the Austrian Christian Doppler Gesellschaft, A1 Telekom Austria AG, Drei-Banken-EDV GmbH, LG Nexera Business Solutions AG, and NXP Semiconductors Austria GmbH.

REFERENCES

Yuji Ayatsuka and Jun Rekimoto. 2005. tranSticks: physically manipulatable virtual connections. In *Proceedings of the SIGCHI conference on Human factors in computing systems (CHI '05)*. ACM, New York, NY, USA, 251–260. DOI:http://dx.doi.org/10.1145/1054972.1055008

Dirk Balfanz, Glenn Durfee, Rebecca E. Grinter, D. K. Smetters, and Paul Stewart. 2004. Network-in-a-box: how to set up a secure wireless network in under a minute. In *Proceedings of the 13th conference on USENIX Security Symposium - Volume 13 (SSYM'04)*. USENIX Association, Berkeley, CA, USA, 15–15. http://dl.acm.org/citation.cfm?id=1251375.1251390

Dirk Balfanz, D.K. Smetters, Paul Stewart, and H. Chi Wong. 2002. Talking to strangers: Authentication in ad-hoc wireless networks. In *Proceedings of the 2002 Network and Distributed Systems Security Symposium (NDSS'02)*.

Michael Beigl. 1999. Point & Click - Interaction in Smart Environments. In *Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing (HUC '99)*. Springer-Verlag, London, UK, 311–313. http://dl.acm.org/citation.cfm?id=647985.743710

Daniel Bichler, Guido Stromberg, Mario Huemer, and Manuel Löw. 2007. Key generation based on acceleration data of shaking processes. In *Proceedings of the 9th international conference on Ubiquitous computing (UbiComp '07)*. Springer-Verlag, Berlin, Heidelberg, 304–317. http://dl.acm.org/citation.cfm?id=1771592.1771610

Robert Biddle, Sonia Chiasson, and P.C. Van Oorschot. 2012. Graphical passwords: Learning from the first twelve years. *ACM Comput. Surv.* 44, 4, Article 19 (Sept. 2012), 41 pages. DOI:http://dx.doi.org/10.1145/2333112.2333114

Bluetooth Special Interest Group. 2006. Simple Pairing Whitepaper (Revision V10r00). (2006).

Anthony Brown, Richard Mortier, and Tom Rodden. 2013. MultiNet: Reducing Interaction Overhead in Domestic Wireless Networks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 1569–1578. DOI:http://dx.doi.org/10.1145/2470654.2466208

Ileana Buhan, Bas Boom, Jeroen Doumen, Pieter H. Hartel, and Raymond N. J. Veldhuis. 2009. Secure pairing with biometrics. *Int. J. Secur. Netw.* 4 (February 2009), 27–42. Issue 1/2. DOI:http://dx.doi.org/10.1504/IJSN.2009.023424

Ileana Buhan, Jeroen Doumen, Pieter Hartel, and Raymond Veldhuis. 2007. Secure Ad-Hoc Pairing with Biometric: SAfE. In *Proceedings of the First International Workshop on Security for Spontaneous Interaction (IWSSI 2007)*. 450–456.

Claude Castelluccia and Pars Mutaf. 2005. Shake them up!: a movement-based pairing protocol for CPU-constrained devices. In *Proceedings of the 3rd international conference on Mobile systems, applications, and services (MobiSys '05)*. ACM, New York, NY, USA, 51–64. DOI:http://dx.doi.org/10.1145/1067170.1067177

Chia-Hsin Owen Chen, Chung-Wei Chen, Cynthia Kuo, Yan-Hao Lai, Jonathan M. McCune, Ahren Studer, Adrian Perrig, Bo-Yin Yang, and Tzong-Chen Wu. 2008. GAnGS: gather, authenticate 'n group securely. In *Proceedings of the 14th ACM international conference on Mobile computing and networking (MobiCom '08)*. ACM, New York, NY, USA, 92–103. DOI:http://dx.doi.org/10.1145/1409944.1409957

Ming Ki Chong. 2009. *Usable Authentication for Mobile Banking*. Master's thesis. Department of Computer Science, University of Cape Town.

Ming Ki Chong and Hans Gellersen. 2010. Classification of Spontaneous Device Association from a Usability Perspective. In *Proceedings of the Second International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU 2010)*. 1–7.

Ming Ki Chong and Hans Gellersen. 2011. How users associate wireless devices. In *Proceedings of the 2011 annual conference on Human factors in computing systems (CHI '11)*. ACM, New York, NY, USA, 1909–1918. DOI:http://dx.doi.org/10.1145/1978942.1979219

Ming Ki Chong and Hans Gellersen. 2012. Usability classification for spontaneous device association. *Personal Ubiquitous Comput.* 16, 1 (Jan. 2012), 77–89. DOI:http://dx.doi.org/10.1007/s00779-011-0421-1

Ming Ki Chong and Hans W. Gellersen. 2013. How Groups of Users Associate Wireless Devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 1559–1568. DOI:http://dx.doi.org/10.1145/2470654.2466207

Ming Ki Chong, Fahim Kawsar, and Hans Gellersen. 2011. Spatial co-location for device association: the connected object way. In *Proceedings of the 2011 international workshop on Networking and object memories for the internet of things (NoME-IoT '11)*. ACM, New York, NY, USA, 21–26. DOI:http://dx.doi.org/10.1145/2029932.2029941

Ming Ki Chong and Gary Marsden. 2009. Exploring the Use of Discrete Gestures for Authentication. In *Proceedings of the 12th IFIP TC 13 International Conference on Human-Computer Interaction: Part II (INTERACT '09)*. Springer-Verlag, Berlin, Heidelberg, 205–213. DOI:http://dx.doi.org/10.1007/978-3-642-03658-3_27

Ming Ki Chong, Gary Marsden, and Hans Gellersen. 2010. GesturePIN: using discrete gestures for associating mobile devices. In *Proceedings of the 12th international conference on Human computer interaction with mobile devices and services (MobileHCI '10)*. ACM, New York, NY, USA, 261–264. DOI:http://dx.doi.org/10.1145/1851600.1851644

W.R. Claycomb and Dongwan Shin. 2009. Secure device pairing using audio. In *Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on*. 77 –84. DOI:http://dx.doi.org/10.1109/CCST.2009.5335562

Lynne Coventry. 2005. *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly Media, Chapter 10 Usable Biometrics, 175–197.

Lynne Coventry, Antonella De Angeli, and Graham Johnson. 2003. Usability and biometric verification at the ATM interface. In *Proceedings of the SIGCHI conference on Human factors in computing systems (CHI '03)*. ACM, New York, NY, USA, 153–160. DOI:http://dx.doi.org/10.1145/642611.642639

W.K. Edwards. 2006. Discovery systems in ubiquitous computing. *Pervasive Computing, IEEE* 5, 2 (april-june 2006), 70 – 77. DOI:http://dx.doi.org/10.1109/MPRV.2006.28

Christian Gehrmann, Chris J. Mitchell, and Kaisa Nyberg. 2004. Manual authentication for wireless devices. *RSA CryptoBytes Technical Newsletter* 7, 1 (2004), 29–37. http://www.rsa.com/rsalabs/cryptobytes/Spring_2004_Cryptobytes.pdf

Christian Gehrmann and Kaisa Nyberg. 2001. Enhancements to Bluetooth baseband security. In *Proceedings of Nordsec 2001*.

Christian Gehrmann and Kaisa Nyberg. 2004. *Security for Mobility*. IEE, Chapter 9 Security in personal area networks, 191–230.

Michael T. Goodrich, Michael Sirivianos, John Solis, Claudio Soriente, Gene Tsudik, and Ersin Uzun. 2009. Using audio in secure device pairing. *Int. J. Secur. Netw.* 4 (February 2009), 57–68. Issue 1/2. DOI:http://dx.doi.org/10.1504/IJSN.2009.023426

Michael T. Goodrich, Michael Sirivianos, John Solis, Gene Tsudik, and Ersin Uzun. 2006. Loud and Clear: Human-Verifiable Authentication Based on Audio. In *Proceedings of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS '06)*. IEEE Computer Society, Washington, DC, USA, 10–. DOI:http://dx.doi.org/10.1109/ICDCS.2006.52

Roswitha Gostner. 2009. *Spatially Aware User Interfaces for Spontaneous Interaction*. Ph.D. Dissertation. Lancaster University.

Saul Greenberg, Nicolai Marquardt, Till Ballendat, Rob Diaz-Marino, and Miaosen Wang. 2011. Proxemic interactions: the new ubicomp? *interactions* 18, 1 (Jan. 2011), 42–50. DOI:http://dx.doi.org/10.1145/1897239.1897250

Dominique Guinard, Sara Streng, and Hans Gellersen. 2007. RelateGateways: A User Interface for Spontaneous Mobile Interaction with Pervasive Services. In *Mobile Spatial Interaction Workshop in conjunction with ACM International Conference on Human Factors in Computing Systems*.

Keisuke Hachisuka, Teruhito Takeda, Yusuke Terauchi, Ken Sasaki, Hiroshi Hosaka, and Kiyoshi Itao. 2005. Intra-body data transmission for the personal area network. *Microsyst. Technol.* 11, 8 (Aug. 2005), 1020–1027. DOI:http://dx.doi.org/10.1007/s00542-005-0500-1

Alina Hang, Gregor Broll, and Alexander Wiethoff. 2010. Visual design of physical user interfaces for NFC-based mobile interaction. In *Proceedings of the 8th ACM Conference on Designing Interactive Systems (DIS '10)*. ACM, New York, NY, USA, 292–301. DOI:http://dx.doi.org/10.1145/1858171.1858224

Tobias Hesselmann, Niels Henze, and Susanne Boll. 2010. FlashLight: Optical Communication Between Mobile Phones and Interactive Tabletops. In *ACM International Conference on Interactive Tabletops and Surfaces (ITS '10)*. ACM, New York, NY, USA, 135–138. DOI:http://dx.doi.org/10.1145/1936652.1936679

Ken Hinckley. 2003. Synchronous gestures for multiple persons and computers. In *Proceedings of the 16th annual ACM symposium on User interface software and technology (UIST '03)*. ACM, New York, NY, USA, 149–158. DOI:http://dx.doi.org/10.1145/964696.964713

Ken Hinckley, Gonzalo Ramos, Francois Guimbretiere, Patrick Baudisch, and Marc Smith. 2004. Stitching: pen gestures that span multiple displays. In *Proceedings of the working conference on Advanced visual interfaces (AVI '04)*. ACM, New York, NY, USA, 23–31. DOI: http://dx.doi.org/10.1145/989863.989866

Lars Erik Holmquist, Friedemann Mattern, Bernt Schiele, Petteri Alahuhta, Michael Beigl, and Hans-Werner Gellersen. 2001. Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts. In *Proceedings of the 3rd international conference on Ubiquitous Computing (UbiComp '01)*. Springer-Verlag, London, UK, UK, 116–122. http://dl.acm.org/citation.cfm?id=647987.741340

Iulia Ion, Marc Langheinrich, Ponnurangam Kumaraguru, and Srdjan Čapkun. 2010. Influence of user perception, security needs, and social factors on device pairing method choices. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. ACM, New York, NY, USA, Article 6, 13 pages. DOI: http://dx.doi.org/10.1145/1837110.1837118

Yohei Iwasaki, Nobuo Kawaguchi, and Yasuyoshi Inagaki. 2003. Touch-and-Connect: A Connection Request Framework for Ad-Hoc Networks and the Pervasive Computing Environment. In *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PERCOM '03)*. IEEE Computer Society, Washington, DC, USA, 20–. http://dl.acm.org/citation.cfm?id=826025.826372

Anil Jain, Lin Hong, and Sharath Pankanti. 2000. Biometric identification. *Commun. ACM* 43, 2 (Feb. 2000), 90–98. DOI: http://dx.doi.org/10.1145/328236.328110

Jeff Johnson and Austin Henderson. 2002. Conceptual Models: Begin by Designing What to Design. *interactions* 9, 1 (Jan. 2002), 25–32. DOI: http://dx.doi.org/10.1145/503355.503366

Ronald Kainda, Ivan Flechais, and A. W. Roscoe. 2009. Usability and security of out-of-band channels in secure device pairing protocols. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*. ACM, New York, NY, USA, Article 11, 12 pages. DOI: http://dx.doi.org/10.1145/1572532.1572547

Ronald Kainda, Ivan Flechais, and A. W. Roscoe. 2010. Two heads are better than one: security and usability of device associations in group scenarios. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. ACM, New York, NY, USA, Article 5, 13 pages. DOI: http://dx.doi.org/10.1145/1837110.1837117

Tim Kindberg and Armando Fox. 2002. System Software for Ubiquitous Computing. *IEEE Pervasive Computing* 1 (January 2002), 70–81. Issue 1. DOI: http://dx.doi.org/10.1109/MPRV.2002.993146

Tim Kindberg, Abigail Sellen, and Erik Geelhoed. 2004. Security and Trust in Mobile Interactions: A Study of Users Perceptions and Reasoning. In *UbiComp 2004: Ubiquitous Computing (Lecture Notes in Computer Science)*, Nigel Davies, Elizabeth Mynatt, and Itiro Siio (Eds.), Vol. 3205. Springer Berlin / Heidelberg, 196–213. http://dx.doi.org/10.1007/978-3-540-30119-6_12

Tim Kindberg and Kan Zhang. 2003a. Secure Spontaneous Device Association. In *UbiComp 2003: Ubiquitous Computing (Lecture Notes in Computer Science)*, Anind Dey, Albrecht Schmidt, and Joseph McCarthy (Eds.), Vol. 2864. Springer Berlin / Heidelberg, 124–131. http://dx.doi.org/10.1007/978-3-540-39653-6_9

Tim Kindberg and Kan Zhang. 2003b. Validating and Securing Spontaneous Associations between Wireless Devices. In *Information Security (Lecture Notes in Computer Science)*, Colin Boyd and Wenbo Mao (Eds.), Vol. 2851. Springer Berlin / Heidelberg, 44–53. http://dx.doi.org/10.1007/10958513_4

Tim Kindberg, Kan Zhang, and Narendar Shankar. 2002. Context Authentication Using Constrained Channels. In *Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02)*. IEEE Computer Society, Washington, DC, USA, 14–. http://dl.acm.org/citation.cfm?id=832315.837553

Darko Kirovski, Michael Sinclair, and David Wilson. 2007a. The Martini Synch: joint fuzzy hashing via error correction. In *Proceedings of the 4th European conference on Security and privacy in ad-hoc and sensor networks (ESAS'07)*. Springer-Verlag, Berlin, Heidelberg, 16–30. http://dl.acm.org/citation.cfm?id=1784404.1784407

Darko Kirovski, Michael Sinclair, and David Wilson. 2007b. The Martini Synch: Device Pairing via Joint Quantization. In *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*. 466 –470. DOI: http://dx.doi.org/10.1109/ISIT.2007.4557269

Alfred Kobsa, Rahim Sonawalla, Gene Tsudik, Ersin Uzun, and Yang Wang. 2009. Serial hook-ups: a comparative usability study of secure device pairing methods. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*. ACM, New York, NY, USA, Article 10, 12 pages. DOI: http://dx.doi.org/10.1145/1572532.1572546

Gerd Kortuem, Christian Kray, and Hans Gellersen. 2005. Sensing and visualizing spatial relations of mobile devices. In *Proceedings of the 18th annual ACM symposium on User interface software and technology (UIST '05)*. ACM, New York, NY, USA, 93–102. DOI: http://dx.doi.org/10.1145/1095034.1095049

Christian Kray, Daniel Nesbitt, John Dawson, and Michael Rohs. 2010. User-defined gestures for connecting mobile phones, public displays, and tabletops. In *Proceedings of the 12th international conference on Human computer interaction with mobile devices and services (MobileHCI '10)*. ACM, New York, NY, USA, 239–248. DOI:http://dx.doi.org/10.1145/1851600.1851640

Arun Kumar, Nitesh Saxena, Gene Tsudik, and Ersin Uzun. 2009a. Caveat eptor: A comparative study of secure device pairing methods. In *Proceedings of the 2009 IEEE International Conference on Pervasive Computing and Communications*. IEEE Computer Society, Washington, DC, USA, 1–10. DOI:http://dx.doi.org/10.1109/PERCOM.2009.4912753

Arun Kumar, Nitesh Saxena, Gene Tsudik, and Ersin Uzun. 2009b. A comparative study of secure device pairing methods. *Pervasive Mob. Comput.* 5 (December 2009), 734–749. Issue 6. DOI:http://dx.doi.org/10.1016/j.pmcj.2009.07.008

Cynthia Kuo, Ahren Studer, and Adrian Perrig. 2008. Mind your manners: socially appropriate wireless key establishment for groups. In *Proceedings of the first ACM conference on Wireless network security (WiSec '08)*. ACM, New York, NY, USA, 125–130. DOI:http://dx.doi.org/10.1145/1352533.1352553

Sven Laur and Kaisa Nyberg. 2006. Efficient Mutual Data Authentication Using Manually Authenticated Strings. In *Cryptology and Network Security (Lecture Notes in Computer Science)*, David Pointcheval, Yi Mu, and Kefei Chen (Eds.), Vol. 4301. Springer Berlin / Heidelberg, 90–107. http://dx.doi.org/10.1007/11935070_6

Sven Laur and Sylvain Pasini. 2008. SAS-based group authentication and key agreement protocols. In *Proceedings of the Practice and theory in public key cryptography, 11th international conference on Public key cryptography (PKC'08)*. Springer-Verlag, Berlin, Heidelberg, 197–213. http://dl.acm.org/citation.cfm?id=1793774.1793791

Jonathan Lester, Blake Hannaford, and Gaetano Borriello. 2004. "Are You with Me?" Using Accelerometers to Determine If Two Devices Are Carried by the Same Person. In *Pervasive Computing (Lecture Notes in Computer Science)*, Alois Ferscha and Friedemann Mattern (Eds.), Vol. 3001. Springer Berlin / Heidelberg, 33–50. http://dx.doi.org/10.1007/978-3-540-24646-6_3

David Liddle. 1996. Bringing Design to Software. ACM, New York, NY, USA, Chapter Design of the Conceptual Model, 17–36. DOI:http://dx.doi.org/10.1145/229868.230029

Felix Xiaozhu Lin, Daniel Ashbrook, and Sean White. 2011. RhythmLink: securely pairing I/O-constrained devices by tapping. In *Proceedings of the 24th annual ACM symposium on User interface software and technology (UIST '11)*. ACM, New York, NY, USA, 263–272. DOI:http://dx.doi.org/10.1145/2047196.2047231

Yue-Hsun Lin, Ahren Studer, Hsu-Chin Hsiao, Jonathan M. McCune, King-Hang Wang, Maxwell Krohn, Phen-Lan Lin, Adrian Perrig, Hung-Min Sun, and Bo-Yin Yang. 2009. SPATE: small-group PKI-less authenticated trust establishment. In *Proceedings of the 7th international conference on Mobile systems, applications, and services (MobiSys '09)*. ACM, New York, NY, USA, 1–14. DOI:http://dx.doi.org/10.1145/1555816.1555818

Y.A. Malkani and L.D. Dhomeja. 2009. Secure device association for ad hoc and ubiquitous computing environments. In *Emerging Technologies, 2009. ICET 2009. International Conference on*. 437 –442. DOI:http://dx.doi.org/10.1109/ICET.2009.5353132

Nicolai Marquardt, Robert Diaz-Marino, Sebastian Boring, and Saul Greenberg. 2011. The proximity toolkit: prototyping proxemic interactions in ubiquitous computing ecologies. In *Proceedings of the 24th annual ACM symposium on User interface software and technology (UIST '11)*. ACM, New York, NY, USA, 315–326. DOI:http://dx.doi.org/10.1145/2047196.2047238

Rene Mayrhofer. 2008. Ubiquitous Computing Security: Authenticating Spontaneous Interactions. (15 September 2008). Habilitation thesis, University of Vienna.

Rene Mayrhofer, Jurgen Fuss, and Iulia Ion. 2013. UACAP: A Unified Auxiliary Channel Authentication Protocol. *IEEE Transactions on Mobile Computing* 12, 4 (April 2013), 710–721. DOI:http://dx.doi.org/10.1109/TMC.2012.43

Rene Mayrhofer and Hans Gellersen. 2007a. On the Security of Ultrasound as Out-of-band Channel. In *Proceedings of the 21th International Parallel and Distributed Processing Symposium: Workshop on Security in Systems and Networks*.

Rene Mayrhofer and Hans Gellersen. 2007b. Shake well before use: authentication based on accelerometer data. In *Proceedings of the 5th international conference on Pervasive computing (PERVASIVE'07)*. Springer-Verlag, Berlin, Heidelberg, 144–161. http://dl.acm.org/citation.cfm?id=1758156.1758168

Rene Mayrhofer and Hans Gellersen. 2009. Shake Well Before Use: Intuitive and Secure Pairing of Mobile Devices. *IEEE Transactions on Mobile Computing* 8 (June 2009), 792–806. Issue 6. DOI:http://dx.doi.org/10.1109/TMC.2009.51

Rene Mayrhofer, Hans Gellersen, and Mike Hazas. 2007. Security by spatial reference: using relative positioning to authenticate devices for spontaneous interaction. In *Proceedings of the 9th international conference on Ubiquitous computing (UbiComp '07)*. Springer-Verlag, Berlin, Heidelberg, 199–216. http://dl.acm.org/citation.cfm?id=1771592.1771604

Rene Mayrhofer and Roswitha Gostner. 2007. Using a spatial context authentication proxy for establishing secure wireless connections. *J. Mob. Multimed.* 3 (September 2007), 198–217. Issue 3. http://dl.acm.org/citation.cfm?id=2010548.2010550

Rene Mayrhofer and Martyn Welch. 2007. A Human-Verifiable Authentication Protocol Using Visible Laser Light. In *Proceedings of the The Second International Conference on Availability, Reliability and Security*. IEEE Computer Society, Washington, DC, USA, 1143–1148. DOI:http://dx.doi.org/10.1109/ARES.2007.5

Jonathan M. McCune, Adrian Perrig, and Michael K. Reiter. 2005. Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication. In *Proceedings of the 2005 IEEE Symposium on Security and Privacy*. IEEE Computer Society, Washington, DC, USA, 110–124. DOI:http://dx.doi.org/10.1109/SP.2005.19

Jonathan M. McCune, Adrian Perrig, and Michael K. Reiter. 2009. Seeing-Is-Believing: using camera phones for human-verifiable authentication. *Int. J. Secur. Netw.* 4 (February 2009), 43–56. Issue 1/2. DOI:http://dx.doi.org/10.1504/IJSN.2009.023425

Elena Meshkova, Janne Riihij?rvi, Marina Petrova, and Petri M?hnen. 2008. A survey on resource discovery mechanisms, peer-to-peer and service discovery frameworks. *Computer Networks* 52, 11 (2008), 2097 – 2128. DOI:http://dx.doi.org/10.1016/j.comnet.2008.03.006

Anthony Nicholson, Ian Smith, Jeff Hughes, and Brian Noble. 2006. LoKey: Leveraging the SMS Network in Decentralized, End-to-End Trust Establishment. In *Pervasive Computing (Lecture Notes in Computer Science)*, Kenneth Fishkin, Bernt Schiele, Paddy Nixon, and Aaron Quigley (Eds.), Vol. 3968. Springer Berlin / Heidelberg, 202–219. http://dx.doi.org/10.1007/11748625_13

Rishab Nithyanand, Nitesh Saxena, Gene Tsudik, and Ersin Uzun. 2010. Groupthink: usability of secure group association for wireless devices. In *Proceedings of the 12th ACM international conference on Ubiquitous computing (Ubicomp '10)*. ACM, New York, NY, USA, 331–340. DOI:http://dx.doi.org/10.1145/1864349.1864399

Duck Gun Park, Jin Kyung Kim, Sung Jin Bong, Jung Hwan Hwang, Chang Hee Hyung, and Sung Weon Kang. 2006a. Context Aware Service Using Intra-body Communication. In *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications*. IEEE Computer Society, Washington, DC, USA, 84–91. DOI:http://dx.doi.org/10.1109/PERCOM.2006.17

Duck Gun Park, Jin Kyung Kim, Jin Bong Sung, Jung Hwan Hwang, Chang Hee Hyung, and Sung Weon Kang. 2006b. TAP: touch-and-play. In *Proceedings of the SIGCHI conference on Human Factors in computing systems (CHI '06)*. ACM, New York, NY, USA, 677–680. DOI:http://dx.doi.org/10.1145/1124772.1124873

Shwetak N. Patel, Jeffrey S. Pierce, and Gregory D. Abowd. 2004. A gesture-based authentication scheme for untrusted public terminals. In *Proceedings of the 17th annual ACM symposium on User interface software and technology (UIST '04)*. ACM, New York, NY, USA, 157–160. DOI:http://dx.doi.org/10.1145/1029632.1029658

Chunyi Peng, Guobin Shen, Yongguang Zhang, and Songwu Lu. 2009. Point&Connect: intention-based device pairing for mobile phone users. In *Proceedings of the 7th international conference on Mobile systems, applications, and services (MobiSys '09)*. ACM, New York, NY, USA, 137–150. DOI:http://dx.doi.org/10.1145/1555816.1555831

Ramnath Prasad and Nitesh Saxena. 2008. Efficient device pairing using "Human-comparable" synchronized audiovisual patterns. In *Proceedings of the 6th international conference on Applied cryptography and network security (ACNS'08)*. Springer-Verlag, Berlin, Heidelberg, 328–345. http://dl.acm.org/citation.cfm?id=1788857.1788877

Gonzalo Ramos, Kenneth Hinckley, Andy Wilson, and Raman Sarin. 2009. Synchronous Gestures in Multi-Display Environments. *HumanComputer Interaction* 24, 1-2 (2009), 117–169. DOI:http://dx.doi.org/10.1080/07370020902739288

Jun Rekimoto. 2004. SyncTap: synchronous user operation for spontaneous network connection. *Personal Ubiquitous Comput.* 8 (May 2004), 126–134. Issue 2. DOI:http://dx.doi.org/10.1007/s00779-004-0262-2

Jun Rekimoto, Yuji Ayatsuka, and Michimune Kohno. 2003a. SyncTap: An Interaction Technique for Mobile Networking. In *Human-Computer Interaction with Mobile Devices and Services (Lecture Notes in Computer Science)*, Luca Chittaro (Ed.), Vol. 2795. Springer Berlin / Heidelberg, 104–115. http://dx.doi.org/10.1007/978-3-540-45233-1_9

Jun Rekimoto, Yuji Ayatsuka, Michimune Kohno, and Hauro Oba. 2003b. Proximal Interactions: A Direct Manipulation Technique for Wireless Networking. In *INTERACT '03*. IOS Press, 511–518.

Jun Rekimoto, Takashi Miyaki, and Michimune Kohno. 2004. ProxNet: Secure Dynamic Wireless Connection by Proximity Sensing. In *Pervasive Computing (Lecture Notes in Computer Science)*, Alois Ferscha and Friedemann Mattern (Eds.), Vol. 3001. Springer Berlin / Heidelberg, 213–218. http://dx.doi.org/10.1007/978-3-540-24646-6_15

Nitesh Saxena, Jan-Erik Ekberg, Kari Kostiainen, and N. Asokan. 2006. Secure Device Pairing based on a Visual Channel (Short Paper). In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*. IEEE Computer Society, Washington, DC, USA, 306–313. DOI:http://dx.doi.org/10.1109/SP.2006.35

Nitesh Saxena and Md. Borhan Uddin. 2009a. Blink 'Em All: Scalable, User-Friendly and Secure Initialization of Wireless Sensor Nodes. In *Proceedings of the 8th International Conference on Cryptology and Network Security (CANS '09)*. Springer-Verlag, Berlin, Heidelberg, 154–173. DOI:http://dx.doi.org/10.1007/978-3-642-10433-6_11

Nitesh Saxena and Md. Borhan Uddin. 2009b. Secure Pairing of "Interface-Constrained" Devices Resistant against Rushing User Behavior. In *Proceedings of the 7th International Conference on Applied Cryptography and Network Security (ACNS '09)*. Springer-Verlag, Berlin, Heidelberg, 34–52. DOI:http://dx.doi.org/10.1007/978-3-642-01957-9_3

Nitesh Saxena, Md. Borhan Uddin, and Jonathan Voris. 2008. Universal device pairing using an auxiliary device. In *Proceedings of the 4th symposium on Usable privacy and security (SOUPS '08)*. ACM, New York, NY, USA, 56–67. DOI:http://dx.doi.org/10.1145/1408664.1408672

Adin Scannell, Alexander Varshavsky, Anthony LaMarca, and Eyal De Lara. 2009. Proximity-based authentication of mobile devices. *Int. J. Secur. Netw.* 4 (February 2009), 4–16. Issue 1/2. DOI:http://dx.doi.org/10.1504/IJSN.2009.023422

Dominik Schmidt, Fadi Chehimi, Enrico Rukzio, and Hans Gellersen. 2010. PhoneTouch: a technique for direct phone interaction on surfaces. In *Proceedings of the 23nd annual ACM symposium on User interface software and technology (UIST '10)*. ACM, New York, NY, USA, 13–16. DOI:http://dx.doi.org/10.1145/1866029.1866034

Dominik Schmidt, Julian Seifert, Enrico Rukzio, and Hans Gellersen. 2012. A cross-device interaction style for mobiles and surfaces. In *Proceedings of the Designing Interactive Systems Conference (DIS '12)*. ACM, New York, NY, USA, 318–327. DOI:http://dx.doi.org/10.1145/2317956.2318005

Bruce Schneier. 1999. Inside risks: the uses and abuses of biometrics. *Commun. ACM* 42 (August 1999), 136–. Issue 8. DOI:http://dx.doi.org/10.1145/310930.310988

Khoovirajsingh Seewoonauth, Enrico Rukzio, Robert Hardy, and Paul Holleis. 2009. Touch & connect and touch & select: interacting with a computer by touching it with a mobile phone. In *Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '09)*. ACM, New York, NY, USA, Article 36, 9 pages. DOI:http://dx.doi.org/10.1145/1613858.1613905

Claudio Soriente, Gene Tsudik, and Ersin Uzun. 2007. BEDA: Button-Enabled Device Pairing. In *Proceedings of the First International Workshop on Security for Spontaneous Interaction (IWSSI 2007)*. 443–449.

Claudio Soriente, Gene Tsudik, and Ersin Uzun. 2008. HAPADEP: Human-Assisted Pure Audio Device Pairing. In *Proceedings of the 11th international conference on Information Security (ISC '08)*. Springer-Verlag, Berlin, Heidelberg, 385–400. DOI:http://dx.doi.org/10.1007/978-3-540-85886-7_27

Claudio Soriente, Gene Tsudik, and Ersin Uzun. 2009. Secure pairing of interface constrained devices. *Int. J. Secur. Netw.* 4 (February 2009), 17–26. Issue 1/2. DOI:http://dx.doi.org/10.1504/IJSN.2009.023423

Frank Stajano and Ross J. Anderson. 1999. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In *Proceedings of the 7th International Workshop on Security Protocols*. Springer-Verlag, London, UK, 172–194. http://dl.acm.org/citation.cfm?id=647217.760118

J. Suomalainen, J. Valkonen, and N. Asokan. 2009. Standards for security associations in personal networks: a comparative analysis. *Int. J. Secur. Netw.* 4 (February 2009), 87–100. Issue 1/2. DOI:http://dx.doi.org/10.1504/IJSN.2009.023428

Colin Swindells, Kori M. Inkpen, John C. Dill, and Melanie Tory. 2002. That one there! Pointing to establish device identity. In *Proceedings of the 15th annual ACM symposium on User interface software and technology (UIST '02)*. ACM, New York, NY, USA, 151–160. DOI:http://dx.doi.org/10.1145/571985.572007

Ersin Uzun, Kristiina Karvonen, and N. Asokan. 2007. Usability analysis of secure pairing methods. In *Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security (FC'07/USEC'07)*. Springer-Verlag, Berlin, Heidelberg, 307–324. http://dl.acm.org/citation.cfm?id=1785594.1785635

Ersin Uzun, Nitesh Saxena, and Arun Kumar. 2011. Pairing devices for social interactions: a comparative usability evaluation. In *Proceedings of the 2011 annual conference on Human factors in computing systems (CHI '11)*. ACM, New York, NY, USA, 2315–2324. DOI:http://dx.doi.org/10.1145/1978942.1979282

Jukka Valkonen, N. Asokan, and Kaisa Nyberg. 2006. Ad Hoc Security Associations for Groups. In *Security and Privacy in Ad-Hoc and Sensor Networks (Lecture Notes in Computer Science)*, Levente Buttyn, Virgil Gligor, and Dirk Westhoff (Eds.), Vol. 4357. Springer Berlin / Heidelberg, 150–164. http://dx.doi.org/10.1007/11964254_14

Alex Varshavsky, Adin Scannell, Anthony LaMarca, and Eyal De Lara. 2007. Amigo: proximity-based authentication of mobile devices. In *Proceedings of the 9th international conference on Ubiquitous computing (UbiComp '07)*. Springer-Verlag, Berlin, Heidelberg, 253–270. http://dl.acm.org/citation.cfm?id=1771592.1771607

Serge Vaudenay. 2005. Secure Communications over Insecure Channels Based on Short Authenticated Strings. In *Advances in Cryptology CRYPTO 2005 (Lecture Notes in Computer Science)*, Victor Shoup (Ed.), Vol. 3621. Springer Berlin / Heidelberg, 309–326. http://dx.doi.org/10.1007/11535218_19

C.N. Ververidis and G.C. Polyzos. 2008. Service discovery for mobile Ad Hoc networks: a survey of issues and techniques. *Communications Surveys Tutorials, IEEE* 10, 3 (quarter 2008), 30–45. DOI:http://dx.doi.org/10.1109/COMST.2008.4625803

Roy Want, Andy Hopper, Veronica Falcão, and Jonathan Gibbons. 1992. The active badge location system. *ACM Trans. Inf. Syst.* 10, 1 (Jan. 1992), 91–102. DOI:http://dx.doi.org/10.1145/128756.128759

Marc Simon Wegmüller. 2007. *Intra-Body Communication for Biomedical Sensor Networks*. Ph.D. Dissertation. ETH Zurich.

Wi-Fi Alliance. 2007. Wi-Fi protected setup specification v1.0. (January 2007).

Andrew D. Wilson and Raman Sarin. 2007. BlueTable: connecting wireless mobile devices on interactive surfaces using vision-based handshaking. In *Proceedings of Graphics Interface 2007 (GI '07)*. ACM, New York, NY, USA, 119–125. DOI:http://dx.doi.org/10.1145/1268517.1268539

Jacob Otto Wobbrock. 2009. TapSongs: tapping rhythm-based passwords on a single binary sensor. In *Proceedings of the 22nd annual ACM symposium on User interface software and technology (UIST '09)*. ACM, New York, NY, USA, 93–96. DOI:http://dx.doi.org/10.1145/1622176.1622194

Jacob O. Wobbrock, Htet Htet Aung, Brandon Rothrock, and Brad A. Myers. 2005. Maximizing the guessability of symbolic input. In *CHI '05 extended abstracts on Human factors in computing systems (CHI EA '05)*. ACM, New York, NY, USA, 1869–1872. DOI:http://dx.doi.org/10.1145/1056808.1057043

Jacob O. Wobbrock, Meredith Ringel Morris, and Andrew D. Wilson. 2009. User-defined gestures for surface computing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. ACM, New York, NY, USA, 1083–1092. DOI:http://dx.doi.org/10.1145/1518701.1518866

T. G. Zimmerman. 1996. Personal area networks: near-field intrabody communication. *IBM Syst. J.* 35 (September 1996), 609–617. Issue 3-4. DOI:http://dx.doi.org/10.1147/sj.353.0609

Received .; revised .; accepted .