# Secure Device Pairing Methods: An Overview

Aatifah Noureen
Department of Information Technology,
Faculty of Computing and IT
University of Gujrat
Gujrat, Pakistan

Umar Shoaib
Department of Computer Science,
Faculty of Computing and IT
University of Gujrat
Gujrat, Pakistan

Muhammad Shahzad Sarfraz
Department of Computer Science,
Faculty of Computing and IT
University of Gujrat
Gujrat, Pakistan

***Abstract*—The procedure of setting up a secure communication channel among unfamiliar human-operated devices is called "Secure Device Pairing". Secure binding of electronic devices is a challenging task because there are no security measures and commonly trusted infrastructure. It opens up the doors for many security threats and attacks e.g. man in middle and evil twin attacks. In order to mitigate these attacks different techniques have been proposed; some level of user participation is required in decreasing attacks in the device pairing process. A comparative and comprehensive evaluation of prominent secure device pairing methods is described here. The main motive of this research is to summarize the cryptographic protocols used in pairing process and compare the existing methods to secure the pairing devices. That will help in selecting best method according to the situation, as the most popular or easy method, instead they choose different methods in different circumstances.**

***Keywords*—Device pairing methods; binding method; OOB channel; cryptographic protocols***

## I. Introduction

As the usage of mobile devices (cell-phones, PDA's, cameras and media players) is increasing, the need of spontaneous connection of two devices over a wireless connection has also become essential [1]. The main advantage of using wireless technologies like Wi-Fi or Bluetooth is that ad hoc communication can take place without the infrastructure or any overhead charges to the users [2]. There are many situations where devices interact with each other such as sharing files, photos and videos with the friends. It also includes editing the documents and reports cooperatively in a conference, and playing games with multiple players and exchanging of digital business cards. Sometimes, a single user controls both devices (e.g. communication between Alice's cell phone and her wireless headset or her PDA and a wireless printer) and sometimes two different users control their respective devices. (e.g. communication between A's and B's devices such as laptops/ PDAs or cell phones for professional or social reasons) [3].

But the heavy usage of these devices may carry many security risks. Sharing data with strangers and at public places (markets, parks and airports) may result in more concerns of security and privacy [4]. As the wireless radio communication channels can easily be eavesdropped and manipulated, which raises many threats. Evil Twin attack as shown in Fig. 1 and Man-in-the-Middle which is shown in Fig. 2 are the most common attacks [5].

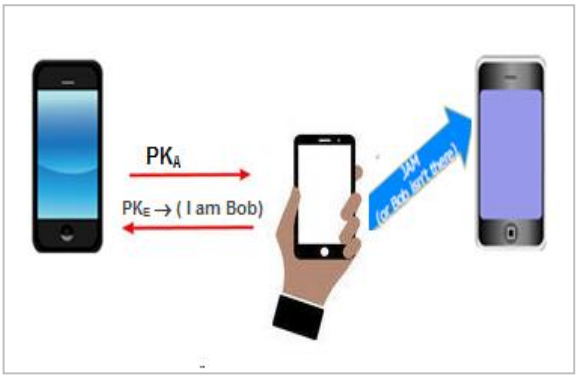


Fig. 1. Evil Twin attack.


Fig. 2. Man-in-the-Middle attack.

In order to minimize the chances of such attacks, the communication should be bootstrapped securely (i.e., devices should be "paired" securely). The procedure to set up a secure communication channel among unfamiliar human-operated devices is called "**Secure Device Pairing**" (for example, between two cell phones; between cell phone and a wireless headset; between PDA and an MP3 player). Enrolling a phone or a PDA into a home WLAN [6] and secure binding of electronic devices is challenging because we need to set up a security association with unfamiliar devices that don't have any common security infrastructure (i.e., no PKI or TTPs). And it is more difficult particularly when it is performed by ordinary users (don't have any technical knowledge) [7].

Device pairing method should be secure, intuitive, burden and error-free and inexpensive universal pairing method. It must give adequate clues and security to guarantee that right devices are paired [3]. If there is an attacker/intruder who tries

to attack, the user will be intimated with an error message so that the pairing process can be terminated [5].

The essential measures in order to ensure the security recommended by [8] are:

*1)* Secrecy through information hiding from unintended devices.

*2)* Integrity and authenticity through validation of data that it is in original form as sent by particular sender.

*3)* Demonstrative identification of devices that are interacting, communicating, and performing exchange in wireless medium of communication.

The aim of the attacker is to disturb or interrupt the communication breaching the security measures. These attacks are either active or passive attacks [9]. In active attack attacker directly participate in protocol and disrupt the communication of data, man in the middle, denial of service, Evil Twin, and data injection attacks are the example of active attacks as depicted in Fig. 1 and 2. While passive attack occurs when attacker is not directly involved in protocol, eavesdropping is an example of passive attack. In order to authenticate the communication, many protocols for secure device pairing are proposed that validate the devices. Mostly devices are based on OOB (Out-of-Band) channel which is an auxiliary data channel that can be used to check the essential's credibility of wireless connections) [7]. These channels are controlled and managed by the users which own and are operating the devices [10], [40]. These OOB channels can be utilized through acoustic, visual and the tactile senses [7].

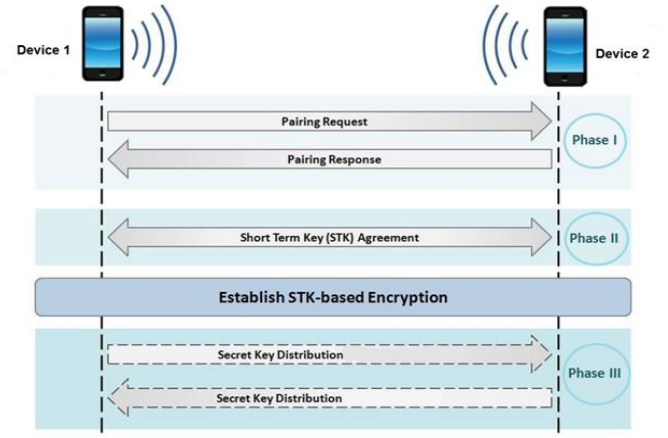


Fig. 3. Simple device pairing protocol.

Fig. 4. People are pairing devices.

Cryptographic protocol demonstrates the information sharing, establishment of connections and interaction in pairing process (Fig. 3) [11] while pairing method is described as the user orientation of pairing process [6], [41]. It will be clarified in later discussion that one cryptographic protocol can be combined in more than one pairing method.

The main goal of this research is to summarize the cryptographic protocols used in pairing process and compare the existing secure device pairing methods. That will help in selecting best method according to situation as people don't always use the most popular or easy method, instead they choose different methods in different circumstances, taking into account the sensitivity of information, time limitations, and the social convention suitable for a specific place and setting. The rest of the paper is organized as follows. Section 2 discusses the cryptographic protocols. In Section 3, the pairing methods are described in detail while the conclusion is discussed in Section 4.

## II. Cryptographic Protocols

Many cryptographic protocols are proposed by different researchers, some of these are discussed in this paper. In [11], a simple device pairing protocol like shown in Fig. 4 in which devices "A" and "B" interchange their public keys PKA and PKB through a channel which is not secure. Their resultant hashes, named H.PKA and H.PKB are exchanged through another media OOB channel.

To enhance the efficiency and functionality of protocols [14] has done some work in this field and proposed a modified version of SAS that requires three round communications and SAS message is computed through universal hash function. In different pairing methods users generate a random secret value that is used by both devices. Then the authenticating key exchange mechanism is performed. Password-Authenticated Key Exchange (PAKE) protocols are used for cryptography [15]. Improvements never stops [1], [16], recently suggested an updated and more efficient version of SAS protocol that is in use of many pairing methods.

## III. Pairing Methods

Fig. 5 is showing categorization of some pairing methods along with the process details. The detailed steps involved in each steps are also explained.

### A. Pairing Methods

The techniques to examine the available methods from user's perspective as categorized by the researchers in [6] are following:

#### 1) Input

The users generate information and enter on the user interfaces of their devices. For example, the Bluetooth pairing process requires its users to enter a passkey into the devices [17]. It includes:

*a)* *Compare and Confirm*: The devices display a 4, 6 or 8-digit number and the user compares these and then decides to enter. This is quite inefficient and time taking and having high error rate [17].

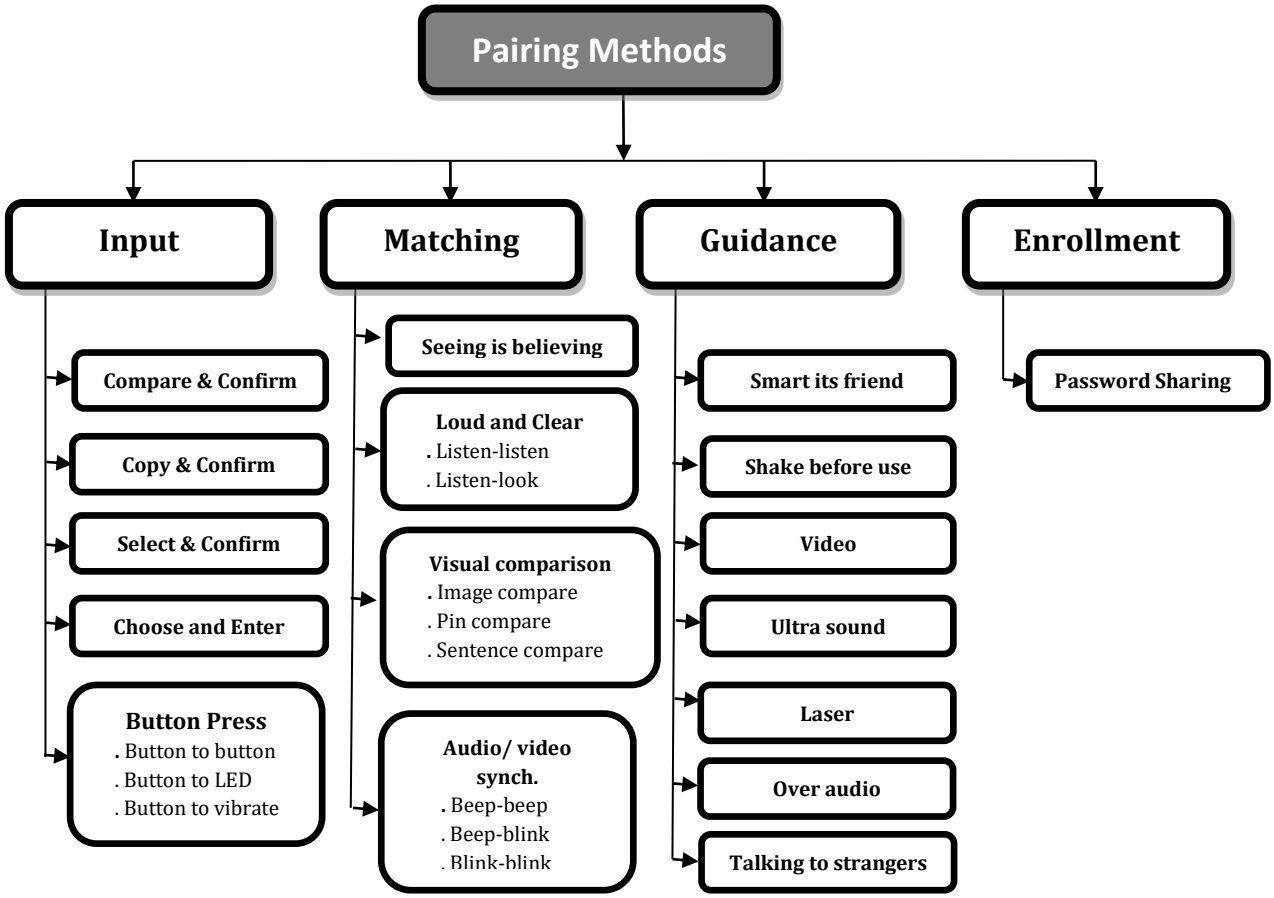


Fig. 5. Categories of pairing methods

*b)* *Select and confirm*: In this method a device shows one number and the other device show a series of numbers from which user selects the matching one to confirm the offer [18].

*c)* *Copy and confirm*: The number is copied by user from one device to another [19].

*d)* *Choose and enter*: In this four or eight-digit number is randomly chosen and then entered by user into each device. Its security is considerably weak due to user's choice. [17]

*e)* *Button press*:

- Button to button: As name shows this method is based on pressing specific buttons to establish pairing connection. In random time interval user has to press the button simultaneously on both devices A and B. The devices are encoded with instructions to start timer when first button is pressed and then calculate secret key in the time interval between first button press on device A and second button press on another device B. 3 bits' secret key is generated in every time interval [19], [39].
- Button to LED: In this approach a button is pressed on device A on the basis of display message generated by device B. The device B chooses a key, express it into a code and transfer it in form of display flashes on device A then user press a button in response and timer is started just like previous method in which sharing key bits are calculated by device [20].
- Button to vibrate: The users enter a button on device B when device A vibrates. Acceptation and rejection on device A is also based on output of device B [19].
- Button to Beep: This is another approach that is suitable for the situation where LED or display facility is not available instead a device has speaker only. Similarly, in previous method the device B selects a key convert it into appropriate coding format and transmit to other device A, that has a button, where user hears a beep and response through pressing button with random time interval [21].

**Pros of input methods:**

These methods are simple, easy to use and easy to understand.

**Cons of input method:**

- Devices must have a keyboard/keypad
- Humans are not good random number/string generators
- High error rate

- Not highly secure.

*2) Matching*

The users perform comparison of the output of devices in order to establish or reject a connection. For example, many wireless sensors ask the users compare the numeric values which are displayed on the connecting devices in order to check whether these numbers are similar or not. It includes:

*a) Seeing is believing*: Device display a barcode and user have to take snap shot with device A then reject or accept the outcome on B on the basis of output appeared on A. It has limitations as all devices don't have big displays to show two-dimensional bar codes. All devices don't have good quality cameras. Placing the devices sufficiently close and aligning the camera may not always be possible [22].

*b) Loud and clear*: The vocalized sentences and audio OOB channel are used in combination to exchange information on wireless channel [23].

- Listen-Listen: As three-word sentence is vocalized on both devices and user tries to configure their resemblance, if they appear to be similar the final response is added in two connecting devices separately. Two Speakers are required on both devices [24].
- Listen-Look: As name showed the listening occurs on one end and sighting on other. Device A show three-word sentence while at the other end three words sentence is spoken by device B and user inputs the decision after comparing both sentences. One speaker and a display is required on both devices [23].

*c) Visual Comparison based*

- Image Compare: A visual pattern is presented by both the devices then user is required to make a comparison. If both patterns accurately matched the decision is entered on both devices by user. Hash and colorful flag [25], snowflake, and random arts visual [26] are common example of this method. Its applicability requires high resolution devices on both ends such as PDAs, laptops and few specific cellphones [27].
- Pin Compare: A five-digit number appeared on two connecting devices, the user has to compare them and ultimate decision is entered by him/her at both ends [17].
- Sentence Compare: Three word sentences are appeared on device A and B where user make comparison and enter the final decision (accept/reject) on both devices [27], [36].

*d) Audio/video synch*

In this technique Beep-Beep, Beep-Blink and Blink-Blink methods are used. In this technique, users compare simple audio and visual patterns for syncing [21].

- Beep-beep: It requires devices to have a speaker.
- Beep-blink: It requires devices to have a LED and a basic speaker.
- Blink-blink: It requires devices to have a LED.

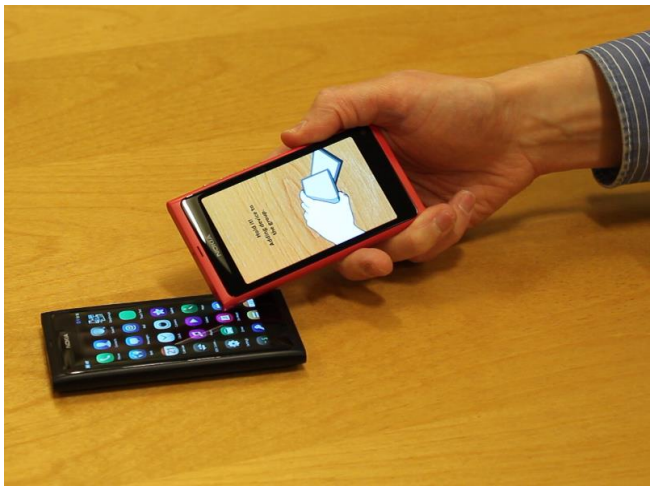

Fig. 6. Touching device to add it to the group.

*3) Guidance*

The users perform a physical action (touch, point, proximate) on devices to direct them to discover each other. For example, the users are required to bring devices closer to each other as shown in Fig. 6 to establish a connection in Android Beam. It includes the following:

*a) Smart it's Friends*: The user shake both devices together that results in a secret pattern transmission between two devices [28].

*b) Shake well before use*: The two axis accelerometer is required on both devices and the devices are shaken to establish a pairing connection by user just like 'smart its friends' method. But it's not usable for bulky or large fixed position devices [29].

*c) Ultrasound*: Ultrasound is used as OOB channel but it is quite expensive and rarely used method [20].

*d) Laser based*: Laser transceiver is required on both devices through which laser beam could be used for pairing process [29].

*e) Video*: device B displays a blinking pattern and the user capture a video of this pattern with device A then on the basis of A's output user accept or reject the offer on device B [16], [41].

*f) Over audio*: This method is preferably used by the devices that do not possess any common wireless channel. An audio protocol of cryptographic message is transmitted that is then closely monitored by user to avoid any third party interruption. Microphone and speaker should be present in both devices [30].

*g) Talking to stranger*: This method depends on infrared (IR) communication and doesn't require user involvement, except in initial setup [11].

- Problems in using talking to stranger: Finding and turning on IR ports.

IR is invisible to humans; man in middle attack is still possible.

*4) Enrollment*

The users set a password for the devices first which is then shared with the devices that are intended to be connected.

*a) Password sharing*: This is used when users have to make Wi-Fi hotspot like a code is generated on the admin which is shared with the devices which require connecting with the network.

*5) Others*

*a) Resurrecting Duckling*: The first attempt to resolve the pairing issues was resurrecting duckling by [31]. It was based on standard cables and physical interfaces but its usability was limited up till 1990's, today it is totally obsolete because of devices' variation and diversity. In this method infrared technology was used. IR works as the OOB channel in pairing process. The user only initiates the setup then it works itself but IR is replaced now with other more efficient and easy to use technologies like Bluetooth [31], [38], [42].

TABLE I. SUMMARY OF DEVICE PAIRING METHODS (INPUT AND MATCHING)

| | | | | Device Requirements | | User Actions | | |
|---|---|---|---|---|---|---|---|---|
| **Pairing Method** | | | **OOB Channel** | **Sending Device** | **Receiving Device** | **Phase I: Setup** | **Phase II: Exchange** | **Phase III: Out Come** |
| **Input** | Compare and confirm | | Visual | Display + user-input | Keypad + user-input | None | Enter value displayed by sending device into receiving device | Abort and accept on sending device based on receiving device decision |
| | Copy and confirm | | | | | | | |
| | Select and confirm | | | | | | | |
| | Choose and enter | | Tactile | User input on both devices | | None | Select random value and enter it into each devices | None |
| | Button press | Beep press | Tactile Visual + tactile Acoustic + tactile | User input+ vibration/Led/beep | User output + one button | Touch or hold on both devices | For each signal on sending device press button on receiving device | Abort and accept on sending device based on receiving device decision |
| | | Led press | | | | | | |
| | | Vibrate press | | | | | | |
| | | Button press | tactile | One button on both + user output on one | | Touch or hold on both devices | Simultaneous press button on both devices, wait and repeat until output signal | None (unless synch. error) |
| **Matching** | Seeing is believing | | Visual | Display + user-input | Photo camera + user-output | None | Align camera on receiving device with displayed barcode on sending device, take picture | Abort and accept on sending device based on receiving device decision |
| | Loud and clear | Listen listen | Acoustic/ Acoustic + visual | User input on both/speaker on both/ display on one + speaker on other | | None | Compare:<br>Two vocalizations<br>Displayed phrase with vocalization | Abort and accept on both device |
| | | Listen look | | | | | | |
| | Visual comparison based | Sentence compare | visual | Display + user input on both | | None | Compare:<br>Two images<br>Two numbers<br>Two phrases | Abort and accept on both device |
| | | Image compare | | | | | | |
| | | Pin compare | | | | | | |
| | Audio/video synch. | Beep beep | Visual/audio/ audio + visual | User input on both: Beeper on each/ Led on each/beep on one and Led on other | | None | Monitor synchronized Beeping/blinking/beeping & blinking | Abort on both devices if no synchrony |
| | | Blink blink | | | | | | |
| | | Blink beep | | | | | | |

TABLE II. SUMMARY OF DEVICE PAIRING METHODS (GUIDANCE AND ENROLLMENT)

| | | | Device Requirements | | User Actions | | |
|---|---|---|---|---|---|---|---|
| **Pairing Method** | | **OOB Channel** | **Sending Device** | **Receiving Device** | **Phase I: Setup** | **Phase II: Exchange** | **Phase III: Out Come** |
| **Guidance** | Over audio | Acoustic | Speaker + user-input | Microphone + user-output | None | Waiting for signal from receiving device | Abort and accept on sending device |
| | Laser | Laser | Laser transceiver on both devices | | Align both devices | Waiting for signal from sending device | Abort and accept on receiving device |
| | Smarts its friend | Tactile + motion | 2-axis accelemeters on both + user input on one | | Hold both devices | Shake both devices together until out-put signal | None (unless synch. error) |
| | Shake before use | | | | | | |
| | Video | visual | Led + user input | User output + light detector / video camera | None | Initiate transmittal of OOB data by sending device, Align camera on receiving device | Abort and accept on sending device based on receiving device decision |
| | Talking to strangers | IR | IR ports on both | | Find, align and activate IR ports | None | None |
| **Enrollment** | Password sharing | visual | Display + user input | Keyboard + user input | None | Enter secret key on receiving device | Abort and accept on sending device |
| **Others** | Resurrecting duckling | Cable | Hardware port on and a cable | | Connect cable to devices | None | None |

TABLE III. EFFECT OF AGE, GENDER AND EXPERIENCE ON AVERAGE TASK PERFORMANCE TIME

| **Methods** | **By age group** | | | **By gender** | | **By experience** | |
|---|---|---|---|---|---|---|---|
| | 18-25 | 26-40 | Above 40 | female | male | experienced | Non experienced |
| Pin-compare | 10 | 12 | 18 | 18 | 16 | 14 | 19 |
| Image- compare | 11 | 15 | 21 | 20 | 18 | 19 | 17 |
| Sentence-compare | 08 | 13 | 33 | 21 | 20 | 17 | 28 |
| Over audio | 13 | 18 | 30 | 25 | 25 | 23 | 29 |
| Listen look | 13 | 19 | 40 | 29 | 26 | 23 | 38 |
| Seeing is believe | 16 | 28 | 49 | 42 | 32 | 36 | 50 |
| Listen listen | 18 | 38 | 57 | 57 | 25 | 37 | 58 |
| video | 19 | 39 | 43 | 45 | 39 | 40 | 49 |
| Led Press | 30 | 50 | 96 | 64 | 70 | 60 | 88 |
| Beep press | 20 | 76 | 93 | 72 | 68 | 71 | 75 |
| Vibrate press | 50 | 96 | 108 | 110 | 97 | 93 | 86 |

### B. Summary of the Methods

Tables 1 and 2 summarize our discussion by comparing the existing device pairing methods. The following terminologies are used:

*a)* *Sending/Receiving Device*: It is applied to all those methods in which one direction uses OOB channel.

*b)* *User-input*: Any way of user input.

*c)* *User-output*: Any way of output.

*d)* *Phase I*: Setup: In the startup method user performs an action.

*e)* *Phase II*: Exchange: In this user acts as a part of the protocol.

*f)* *Phase III*: Outcome: user performs the actions in order to finish the method.

### C. Average Task Performance Time of Different Methods

In [32] comparison between different device pairing methods based on Task performance time is elaborated in Fig. 7.

Effect of age, gender and experience on average task performance time of different methods is shown above in Table 3.

Fig. 8, 9 and 10 are graphical representation of effect of age, gender and experience on average task performance time.

- "PIN-Compare < Image-Compare < Listen-Look < See-Believe < Video"
- "PIN-Compare < Sentence-Compare < Over-Audio < Listen-Listen"
- "Listen-Look < Listen-Listen < LED-Press"
- "Video < LED-Press < Beep-Press"

Fig. 7. Comparison based on task performance time.

### D. Factors affect the Binding Methods

There are different factors that influence the preferences of users for the binding methods. So, binding methods must be robust and flexible, so that the users can adapt them according to the requirement and situation [33], [37].

*a)* Physicality: The size and shape of the devices influence on the ways user how users do interaction to bind the group. The devices whose surface area is small are not easy to interact and give commands. On the other hand, users prefer less movement for massive devices [6].

*b)* Device affordance also influences how users conceptualize the interaction [34].

*c)* Place and the social setting influence user preferences for designing binding methods [33].

*d)* Robustness in real-life conditions is also very important to consider [35]. There are many methods that can work well theoretically or with mock-ups, but not in reality. The applications which are involved in multiple entities are like distributed systems which are complex.

*e)* Situation: Touch-based are high-speed and expressive. This method enables the better awareness of in the formation of the group. The group members can understand easily the touching actions but the users may not be in the close proximity like sitting around a table in a conference room. The users may not feel comfortable to use these methods [34], [43].

### E. Best Pairing Method According to Situation

In Table 4, some pairing methods are suggested according to the devices interface and functionality.

### F. Guidelines for the Device Developers

Following are the guidelines for the developers to keep in mind when designing or developing a device for the enhanced usability and security of devices [6].

*a)* To meet user's needs and demands there are other factors that should be taken into account like social situation and user perception, just security and usability focus is insufficient to address phenomenon.

*b)* Actual security that is guaranteed by developer should be consistent with user perception for security needs. To attain this objective there should be cancelation option, dual confirmation, stop buttons, and other control options.

*c)* It is very obvious and natural that human mind maps and system designs may mismatch. To address the mismatches between actual system designing and user perceived mental models, the default security option is necessary to deal with sensitive data like credits cards issued by banks or other confidential reports, etc.

*d)* Another issue may be the differences among users' personal preferences. As some people like listening and other may like taking pictures so there should be option in devices to use different pairing methods.

*e)* Situations also differ so it is necessary to design methods according to the different situations.

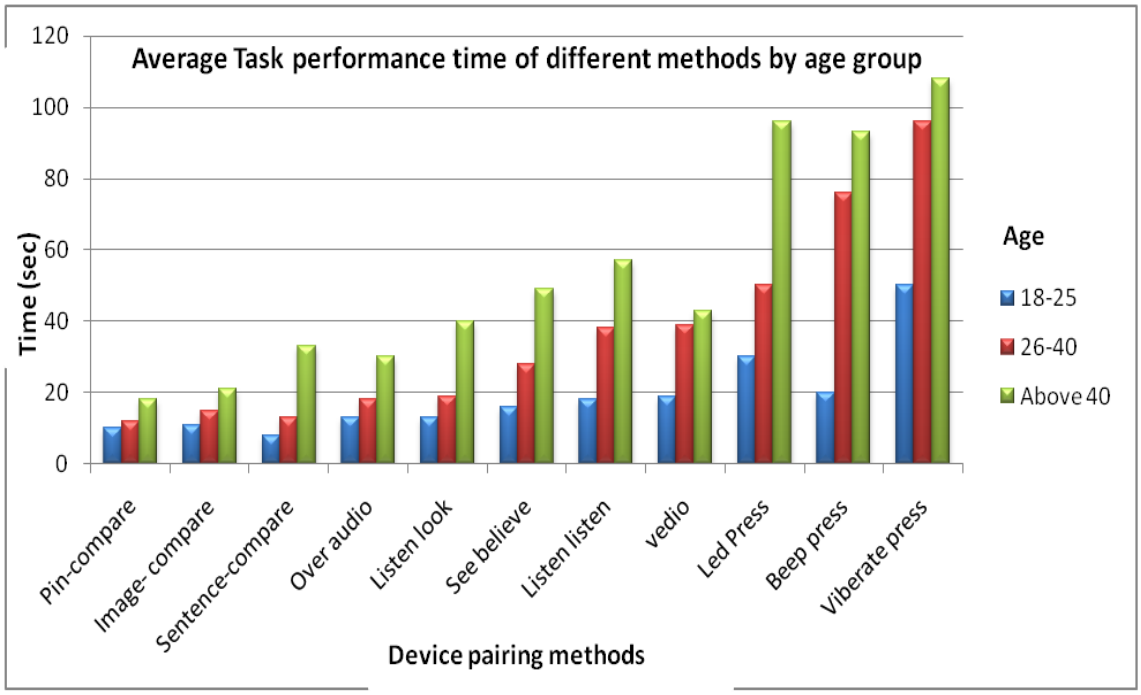


Fig. 8. Comparison based on task performance time.

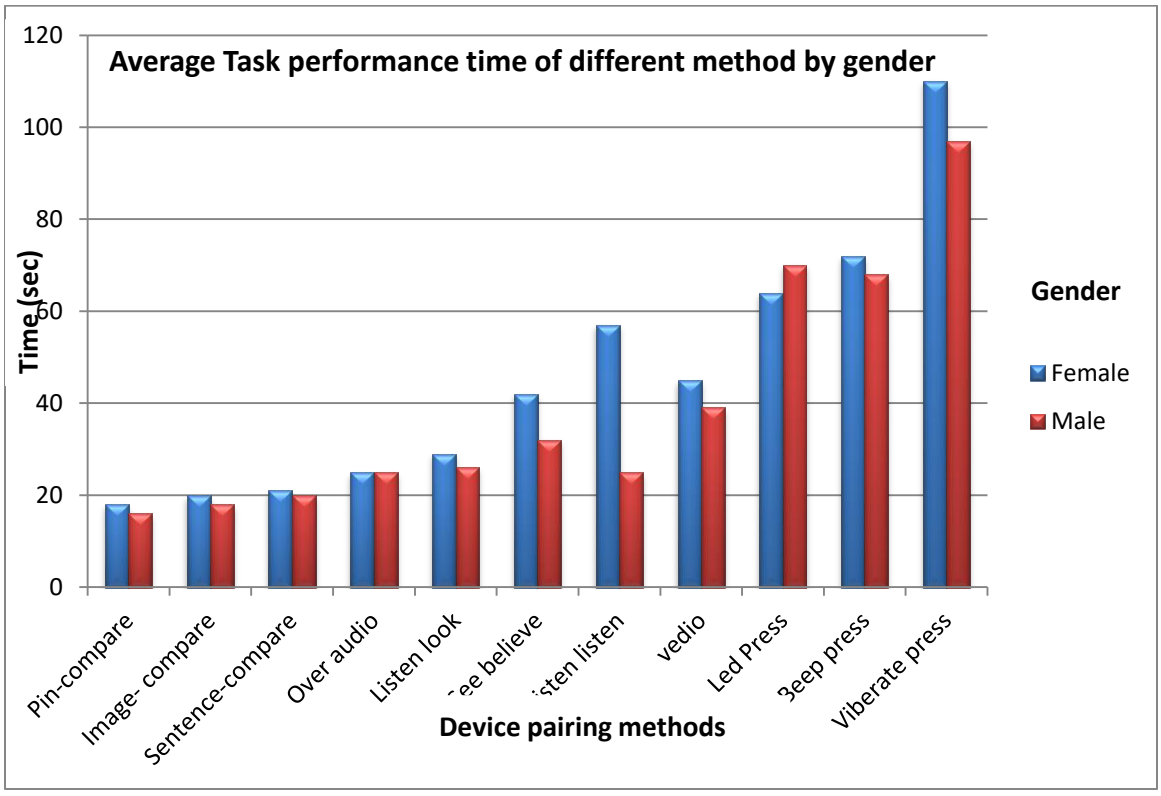


Fig. 9. Effect of age group on task completion time.

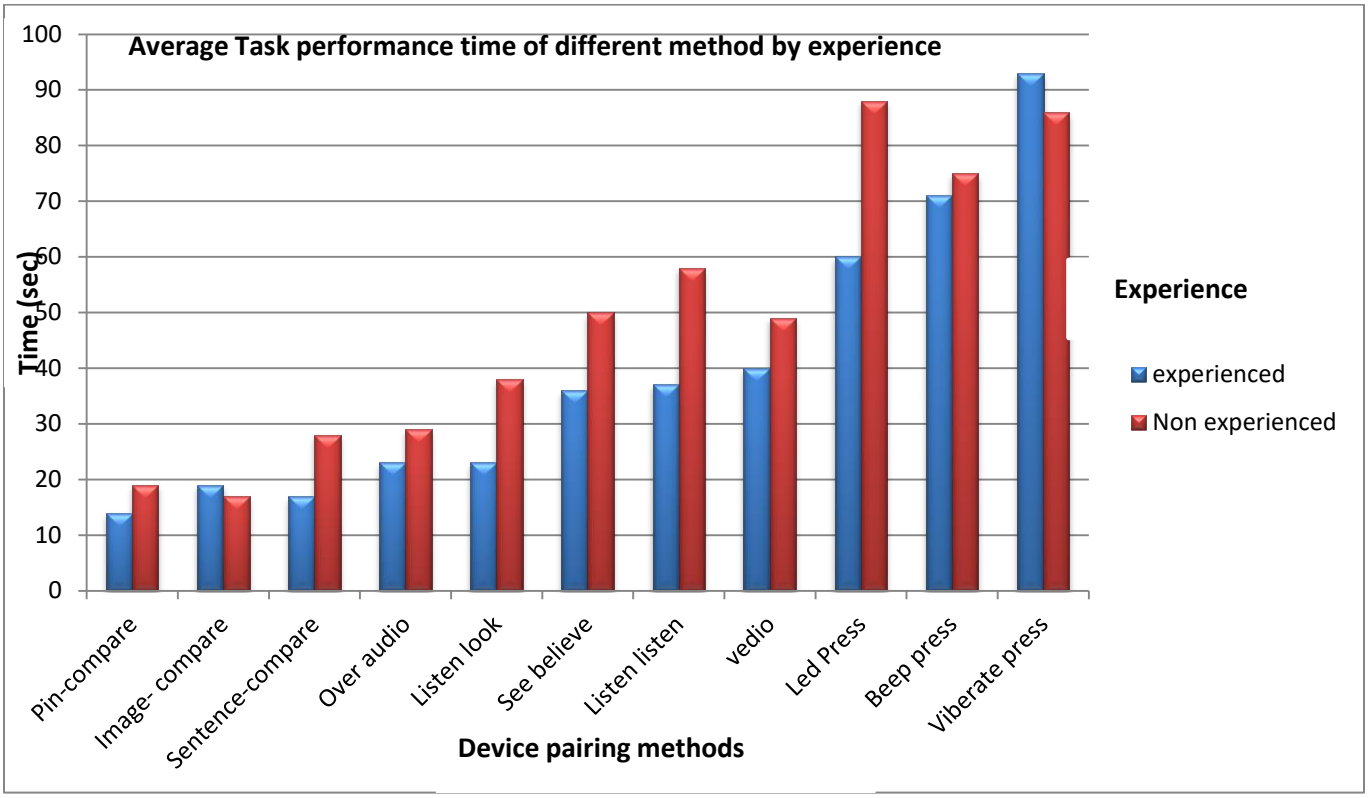


Fig. 10. Effect of experience on task completion time.

TABLE IV. BEST PAIRING METHOD ACCORDING TO SITUATION

| **Pairing method** | **Devices interface and functionality** |
|---|---|
| Button press methods | For interface-constrained devices |
| HAPADEP | When at least one device has no display but has an audio interface |
| Comparison based methods | Both devices have a display |
| Listen-Look | There is display on one side only audio output on other |
| Over-Audio | One side has audio output while only input on other side |

## IV. CONCLUSION

This study described different pairing methods for the devices which are secure. Our study points to some methods that can be performed best according to devices interface and functionality and some that should be avoided altogether. It helps to figure methods which are not suitable for different subgroups of people with respect to age, gender, and the previous experience.

## REFERENCES

[1]. Saxena, Nitesh, and Md Borhan Uddin. "Automated device pairing for asymmetric pairing scenarios." *Information and Communications Security*. Springer Berlin Heidelberg, 2008. 311-327

[2]. Li, Li, et al. "The applications of wifi-based wireless sensor network in internet of things and smart grid." *Industrial Electronics and Applications (ICIEA), 2011 6th IEEE Conference on*. IEEE, 2011.

[3]. Uzun, Ersin, Nitesh Saxena, and Arun Kumar. "Pairing devices for social interactions: a comparative usability evaluation." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011.

[4]. Kindberg, Tim, Abigail Sellen, and Erik Geelhoed. "Security and trust in mobile interactions: A study of users' perceptions and reasoning." *UbiComp 2004: Ubiquitous Computing*. Springer Berlin Heidelberg, 2004. 196-213.

[5]. Halevi, Tzipora, and Nitesh Saxena. "Acoustic Eavesdropping Attacks on Constrained Wireless Device Pairing-Final."

[6]. Jokela, Tero, et al. "Connecting devices for collaborative interactions." *interactions* 22.4 (2015): 39-43.

[7]. Soriente, Claudio, Gene Tsudik, and Ersin Uzun. "Secure pairing of interface constrained devices." *International Journal of Security and Networks* 4.1-2 (2009): 17-26.

[8]. Han, Jun, et al. "MVSec: Secure and Easy-to-Use Pairing of Mobile Devices with Vehicles (CMU-CyLab-14-006)." (2014).

[9]. Goyal, Priyanka, Sahil Batra, and Ajit Singh. "A literature review of security attack in mobile ad-hoc networks." *International Journal of Computer Applications* 9.12 (2010): 11-15.

[10]. Kainda, Ronald, Ivan Flechais, and A. W. Roscoe. "Secure and usable out-of-band channels for ad hoc mobile device interactions." *Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices*. Springer Berlin Heidelberg, 2010. 308-315.]

[11]. Balfanz, Dirk, et al. "Talking to Strangers: Authentication in Ad-Hoc Wireless Networks." *NDSS*. 2002.

[12]. Laur, Sven, and Sylvain Pasini. "Sas-based group authentication and key agreement protocols." *Public Key Cryptography–PKC 2008*. Springer Berlin Heidelberg, 2008. 197-213.

[13]. Guo, Hua, et al. "Cryptanalysis of simple three-party key exchange protocol." *Computers & Security* 27.1 (2008): 16-21.

[14]. Saxena, Nitesh, et al. "Secure device pairing based on a visual channel."*Security and Privacy, 2006 IEEE Symposium on*. IEEE, 2006.

[15]. Uzun, Ersin, Kristiina Karvonen, and Nadarajah Asokan. "Usability analysis of secure pairing methods." *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2007. 307-324.

[16]. Kuo, Cynthia, Jesse Walker, and Adrian Perrig. "Low-cost manufacturing, usability, and security: an analysis of bluetooth simple pairing and Wi-Fi protected setup." *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2007. 325-340.

[17]. Soriente, Claudio, Gene Tsudik, and Ersin Uzun. "BEDA: Button-enabled device association." (2007).

[18]. Kumar, Arun, et al. "Caveat eptor: A comparative study of secure device pairing methods." *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on*. IEEE, 2009.

[19]. Prasad, Ramnath, and Nitesh Saxena. "Efficient device pairing using "human-comparable" synchronized audiovisual patterns." *Applied Cryptography and Network Security*. Springer Berlin Heidelberg, 2008.

[20]. McCune, Jonathan M., Adrian Perrig, and Michael K. Reiter. "Seeing-is-believing: Using camera phones for human-verifiable authentication."*Security and privacy, 2005 IEEE symposium on*. IEEE, 2005.

[21]. Goodrich, Michael T., et al. "Loud and clear: Human-verifiable authentication based on audio." *Distributed Computing Systems, 2006. ICDCS 2006. 26th IEEE International Conference on*. IEEE, 2006.

[22]. Laur, Sven, and Kaisa Nyberg. "Efficient mutual data authentication using manually authenticated strings." *Cryptology and Network Security*. Springer Berlin Heidelberg, 2006. 90-107.

[23]. Perrig and D. Song, "Hash visualization: a new technique to improve real-world security," in International Workshop on Cryptographic Techniques and E-Commerce, 1999.

[24]. A. M. Ellison and S. Dohrmann, "Public-key support for group collaboration," ACM Transactions on Information and System Security (TISSEC), vol. 6, no. 4, pp. 547–565, 2003

[25]. Kumar, Arun, et al. "Caveat eptor: A comparative study of secure device pairing methods." *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on*. IEEE, 2009.

[26]. Holmquist, Lars Erik, et al. "Smart-its friends: A technique for users to easily establish connections between smart artefacts." *Ubicomp 2001: Ubiquitous Computing*. Springer Berlin Heidelberg, 2001.

[27]. Mayrhofer, Rene, and Hans Gellersen. "Shake well before use: Intuitive and secure pairing of mobile devices." *Mobile Computing, IEEE Transactions on*8.6 (2009): 792-806.

[28]. Soriente, Claudio, Gene Tsudik, and Ersin Uzun. "HAPADEP: human-assisted pure audio device pairing." *Information Security*. Springer Berlin Heidelberg, 2008. 385-400.

[29]. F. Stajano and R. J. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks.In Security Protocols Workshop, 1999.

[30]. Kobsa, Alfred, et al. "Serial hook-ups: a comparative usability study of secure device pairing methods." *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, 2009.

[31]. Kainda, Ronald, Ivan Flechais, and A. W. Roscoe. "Security and usability: Analysis and evaluation." *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*. IEEE, 2010

[32]. Chong, Ming Ki, and Hans Gellersen. "How users associate wireless devices." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2011.

[33]. Shoaib, U., Ahmad, N., Prinetto, P., & Tiotto, G. (2012). A platform-independent user-friendly dictionary from Italian to LIS. In *LREC* (Vol. 12, pp. 2435-2438).

[34]. Ahmad, Nadeem, Umar Shoaib, and Paolo Prinetto. "Usability of Online Assistance from Semiliterate Users' Perspective." *International Journal of Human-Computer Interaction* 31.1 (2015): 55-64

[35]. Shoaib, U., Ahmad, N., Prinetto, P., & Tiotto, G. (2014). Integrating multiwordnet with Italian sign language lexical resources. *Expert Systems with Applications*, *41*(5), 2300-2308.

[36]. Gull, Ratab, Umar Shoaib, Saba Rasheed, Washma Abid, and Beenish Zahoor. "Pre Processing of Twitter's Data for Opinion Mining in Political Context." Procedia Computer Science 96 (2016): 1560-1570.

[37]. Liaqat, Misbah, Victor Chang, Abdullah Gani, Siti Hafizah Ab Hamid, Muhammad Toseef, Umar Shoaib, and Rana Liaqat Ali. "Federated cloud resource management: Review and discussion." Journal of Network and Computer Applications 77 (2017): 87-105.

[38]. Rahman, A., Sarfraz, S., Shoaib, U., Abbas, G., & Sattar, M. A. (2016). Cloud based E-Learning, Security Threats and Security Measures. Indian Journal of Science and Technology, 9(48).

[39]. Irfan, Muhammad-Naeem, Catherine Oriat, and Roland Groz. "Model Inference and Testing." Advances in Computers 89 (2013): 89-139.