Vol. 5, No. 1 | January – June 2021

A QR Code Based Group Pairing Approach for Mobile Ad Hoc Networks

Yasir Arfat Malkani[1], Moez Ahmed Malik[1], Lachhman Das Dhomeja[2], Abdul Waheed Mahessar[2], Bisharat Rasool Memon[2]

Abstract:

Due to the rapid growth of small and smart hand-held devices, mobile ad hoc networks (MANets) are becoming very common nowadays. MANets may consist of a number of small hand-held devices having limited resources in terms of memory, battery and processing power. In order to provide services to the users, these devices are capable of communicating with each other through some radio technology, such as WiFi, Bluetooth or Infrared. Since radio channels are inherently vulnerable to various security threats, it requires that devices in MANets must establish a secure association amongst themselves before exchanging any sensitive information or data. The process of establishing a secure channel between two devices is referred to as device pairing or device association. Device pairing do not rely on traditional mechanisms for security due to the impulsive and ad hoc interactions among the devices. Due to this, researchers have proposed many approaches to deal with this issue; however, the issue of group pairing (i.e. secure association of more than two devices) is less addressed issue in the literature yet. There could be many scenarios (such as confidential office meetings, paring of group of home appliances in smart-homes, etc) of MANets, where secure group communications is desired. Consequently, this research focuses on this issue and proposes a QR (quick response) code based approach to establish a secure channel between a numbers of devices. The proposed system is implemented and tested on modern hand-held devices and a usability study of the implemented system is also carried out

Keywords: *Group Pairing; Mobile Ad hoc Networks; Security; Device Association; QR Code*

1. Introduction

Mobile Ad hoc Networks (MANETs) are emerged from distributed computing and mobile computing [1]. In recent years, MANETs have revolutionized the computing world through their enormous useful applications in varying sub-fields. The main goal of mobile ad hoc network is to provide services to its users anytime and anywhere and to achieve this goal, devices need to connect with each other spontaneously. Due to the wireless nature of Mobile Ad hoc Networks, these are vulnerable or open to various security attacks [2 – 4]. Also note that in Mobile Ad hoc Networks devices do not share security credentials a priori, so traditional security mechanisms cannot be applied to Mobile Ad hoc Networks. This raises the need of bootstrapping the security process before actual data transfer. This security bootstrapping process is referred as secure first connect or device paring in the literature. The issue of device pairing is not new in the field of Mobile Ad hoc Networks. Many researchers

[1]Institute of Mathematics & Computer Science (IMCS), University of Sindh, Jamshoro
[2]Department of Inforamtion Technology, University of Sindh, Jamsoro
Corresponding Author: Yasir Arfat Malkani (yasir.malkani@usindh.edu.pk)

have worked on it and proposed many solutions to it during last two decades. However, most of them have focused on only two device scenarios and there has been less focus on group device paring. Group device pairing refers to establish a secure channel between more than two devices.

As stated, achieving the goal of secure first connect is non-trivial task in Mobile Ad hoc Networks due to its open nature. Not only this, but the conventional methods to handle Man-in-the-Middle (MiTM) and eavesdropping attacks are also inapplicable due to their computational cost and fixed infrastructure requirements. Due to this, researches proposed various modern solutions to solve the problem of device pairing based on the concept of out-of-band (OOB) channels.

Out-of-band (OOB) channel refers to an additional or secondary location constrained channel that provides some additional security properties to establish a secure channel at a short distance. Some examples of OOB channel includes near-field-communication (NFC), infrared (IrDA), audio and visual channels, etc. So far, researchers have given many solutions to device pairing using these OOB channels, but these solutions are mainly for two-device scenarios. In contrast to these solutions, authors in [2] proposed an approach to device pairing called PoP (Proof-of-Proximity) framework that have combined various device pairing protocols into a generic system for providing usable and secure scheme for a larger set of device pairing scenarios including two-device and multiple devices scenarios.

Though, PoP framework is providing a generic solution to device pairing and is easy to use, but still it has limited support for group pairing (i.e: associating more than two devices securely over a short range wireless channel). In this research work, it is advocated that there could be many scenarios (such as confidential office meetings, paring of group of home appliances in smart-homes, etc) of MANets, where secure group communications are desired. As a result, in contrast to previous approaches [5 – 29] to device pairing, this research focuses on the issue of group pairing and proposes a scheme to build a secure channel between group of devices.

1.1 Research Contributions

The research contributions of this paper are listed below:

- The first and main contribution of this research work is the proposal of a QR (quick response) code based approach to group device pairing.
- The second contribution of this work is the implementation of the proposed group device pairing scheme.
- The third contribution of this research work is the conduct of a usability study of the proposed solution. The usability study is carried out to verify whether the proposed solution is user-friendly/usable or not.

2. Background

In this section, the basic terminologies and concepts related to the field of device pairing are presented followed by a comprehensive and detailed literature survey of the device pairing schemes.

2.1 Mobile Ad Hoc Network

A mobile ad hoc network (MANET) is a infrastructure-less network of mobile devices connected wirelessly that have capability of self-configuration and self-organization. In other words, a mobile ad hoc network is consisting of numerous small hand-held devices having limited resources in terms of memory, battery and processing power [30], [31]. In order to provide services to the users, these devices need to communicate with each other through some radio technology, such as WiFi, Bluetooth or Infrared.

2.2 Device Pairing

Device pairing refers to setup a connection between two unassociated devices in a secure manner prior to exchanging any information or

data using a short-range wireless technology, such as infrared, Bluetooth, WiFi, etc [24].

2.3 Device Pairing Protocol

Protocol refers to a set of rules governing the exchange of data or information over a communication channel and device pairing protocols refers to the approach or set of rules that are used to initiate a secure channel between two or more devices [2].

2.4 Out-of-Band Channel

In the literature of device pairing, out-of-band (OOB) or side channel refers to a secondary communication channel that is used to exchange some minimal security material (such as short password or random number) to initiate the pairing process. Some examples of OOB channels include audible voice, LED lights, bar codes, NFC technology, etc [2].

2.5 Literature Review

In this section a compressive literature review on state-of-the-art device pairing schemes is presented. This literature review is divided into two sub-sections: the first sub-section describes the pairing schemes that are mainly proposed for establishing secure channel between two devices, while the second sub-section discusses the device pairing schemes, which could be used in group scenarios and allow to connect more than two devices securely.

2.5.1 Device Pairing Schemes for Two-Devices Scenarios

Due to the significance of device pairing in both mobile ad hoc and ubiquitous computing environments, there is an immense research work done on this topic and during the last two decades many device paring schemes and protocols have been proposed. In the literature of device pairing, the work done by Stajano and Aderson [20], [22] is considered as the first that attracted other researchers towards this domain. They [22] presented a policy-based mother-duckling (i.e. resurrecting duckling) security model, which uses plain-text to transfer security material (i.e. encryption key) over physical medium (i.e. wire) to establish the secure channel between the devices. The drawback of this approach is that it is difficult to carry cables all the time and exchange of encryption key in plain-text is vulnerable to dictionary attack [32]. Another limitation of this approach is that it requires that both devices should have similar type of physical interface/port.

Later on Blafanz et al. [19] extended the work of Stajano and Aderson and proposed the first wireless channel based solution to device pairing. They [19] used Infrared as an out-of-band channel to exchange the cryptographic material between two devices to initiate the pairing process. The limitation of this approach is that it requires line-of-sight between the two devices while performing the pairing process. Some other approaches similar to Balfanz et al. approach are also proposed [24], which use the laser or ultrasound channels as out-of-band channels to exchange the minimal cryptographic material to initiate the pairing process.

The device association approaches or mechanisms that are discussed above use wired and/or proximity constrained channels, however, some researchers have proposed device association approaches, which use sensors. These approaches mainly are based on the concept of shaking devices together. In this category, the very first approach is Smart-its-Friend [21]. Later on this approach [21] is modified by Lester et. al. [18], which is called Are You With Me. Are You With ME is followed by another similar approach [10] that uses the same concept of shaking devices together. Shake-Well-Before-Use [10] require from the user to shake the two devices simultaneously in order to pair them. Note that these schemes use accelerometers data to bootstrap the pairing process. The main drawback of these approaches is that practically it is not applicable to shake the two devices simultaneously all the time due to their large size or being fixed in ceilings or at walls. Another similar approach [16] is Shake-Them-Up, which instead of accelerometer data

exploits radio signals to bootstrap the secure device association process.

Later on AMIGO [11] - a radio based approach to device pairing - is proposed by Varshavsky et al.. They in fact extended the traditional Diffie-Hellman [32] key exchange approach for secure device association. Since the proposed approach exploits the WiFi access points data to pair the devices, it is not applicable to scenarios, where there is no WiFi (wireless fidelity) data is accessible to process.

Afterwards, Biometric technology is used as a location-limited side channel for device pairing. Biometric based OOB channels are combined with standard cryptographic primitives to accomplish the goal of secure first connect (i.e. device pairing). Biometric based approaches to device pairing are more attractive solutions, because they put little or no cognitive load/overhead on users [6], [8], [33]. In contrast to benefits of biometric based solutions, these also have some serious limitations. For example, these approaches need exhaustive calculations for pattern matching. Some researchers also proposed device pairing approaches based on NFC technology [12], [34]. NFC based approaches exploit magnetic field induction mechanism to bootstrap the secure pairing process. However, it is to be noted that NFC is an extremely short range technology among all other technologies that decreases its chances of applicability in device association scenarios where there devices are kept at some distance and also note that NFC is open to various attacks, such as data modification, corruption and eavesdropping [8].

Recently, some researchers have also proposed device pairing schemes, which are based on audio/video out-of-band channels. For example, See-is-Believing (SiB) [26] is one of them which uses camera and bar codes for device paring, while another approach called Loud-and-Clear (LaC) [14] uses microphone/speaker and display to establish the secure connection between two devices. SiB is inappropriate solution for the devices that do not have camera, while LaC is not a suitable solution for hearing-impaired users. HAPADEP is another audio based approach proposed by Sorient et al. [35]. The limitation of this approach [35] is that if users do not carefully listen to audio generated by devices, then the devices security may easily be compromised by false match. Apart from above approaches, some standard pairing technique, such as Bluetooth pairing [36], are also in operation, which uses PIN or password to connect the two devices securely, however, PIN code number is also vulnerable to exhaustive search attack and/or dictionary attack. By launching these attacks a four (04) digits PIN code could be broken down in less than 0.06 sec [37], [38]. Another limitation of Bluetooth pairing is that it requires human intervention to input the same PIN code / short password on both the devices to bootstrap the secure device association process.

While comparing all above discussed approaches with the approach proposed by Malkani [2], it is very clear that this is more standard and generic solution to device pairing. Malkani [2] called his developed approach as the proof-of-proximity (PoP) framework. The proposed approach [2] uses the common device capabilities, a discovery mechanism and several integrated device association schemes to provide a comprehensive support for a larger set of device association scenarios ranging from two-device settings to multiple device settings. The discovery system exploits or combines the best features of service location protocol (SLP) [39] and Universal Plug and Play (UPnP) [40] protocol. The readers, who are interested to know more about this approach can refer [2] for further reading.

In short, many device pairing approaches have been introduced by several researchers so far and each of them have their own advantages and disadvantages. Also note that above all approaches (excluding the [2], which has partial support for group pairing scenarios) are specially designed for pairing of two devices scenario. In next section, those pairing approaches are discussed, which are proposed

pairing of more than two devices and thus are suitable for group pairing scenarios.

2.5.2 Device Pairing Schemes for Group Pairing Scenarios

As stated earlier in introduction section, there is very less work done on group pairing and to the best of my knowledge I have found only two direct approaches to group pairing. The first one is proposed by Ming Li et al. [41] and second more recent approach to group pairing is proposed by Zhiping Jiang et al. [42]. Ming Li et al. [41] focused on the secure sensors' association problem in body area network (BAN). All the sensors are securely paired before the body area network is actually deployed. This group pairing approach is based on traditional symmetric-key cryptographic primitives. The body area network is developed to meet a larger range of applications (e.g. ubiquitous health monitoring system (UHM) [43] and emergency medical response system (EMS) [44]).

Zhiping Jiang et al. [42] proposed an approach - called NFV - to allow a group of modern hand-held devices equipped with a motion sensor to exchange data and information securely. In their proposed scheme a group of people or users put their hand-held devices on a table and wait for the group connection to be established. The proposed approach exploits vibration technology to establish the secure channel.

2.6 Justification of the Proposed Group Pairing Approach

As stated mobile ad hoc networks (MANets) are becoming common day by day. A MANetis consisting of a number of small hand-held devices having capability of interacting with each other wirelessly. Since wireless technology is inherently vulnerable to several security threats (such as eavesdropping, main-in-the-middle (MiTM) attack), it requires some mechanisms to provide secure communication between the devices. As stated in previous section, during the last two decades, many research efforts [20-45] have been made that address the issue of security in general and security of Mobile Ad hoc Networks (MANETs) in particular. Each of the solutions have their own trade-offs in terms of device heterogeneity, usability and applicability. From the literature survey, it is concluded that researchers have proposed and developed many scheme to secure the communication between any two devices, however the issue of secure group association is less addressed yet. We advocate that there could be many MANets scenarios where there is a need of secure group communication. Therefore, in this research we propose to develop some mechanism that facilitates to bootstrap the secure pairing process between a group of devices. The proposed approach is also compared with one of the recent approach [42] to group pairing. The comparative analysis is presented in section 5. The results show that the proposed approach to group pairing is more effective as compared to the prior [42] group pairing scheme.

3. The Proposed System

The main goal of this research work is to develop a device pairing scheme that allows the secure association of group of devices (i.e. two or more devices) in a mobile ad hoc network. Therefore, in subsequent sections, the high-level and low-level design of the proposed approach is presented followed by a message sequence diagram, which summarizes the overall approach.

3.1 High-level Design of the Proposed System

Figure-1 illustrates the high-level design of the proposed approach. In the proposed approach there are two types of roles for devices. The first role is of master device or group controller, while the other role is of an ordinary group member. The difference between these two roles is that apart from being used as an ordinary member, a group controller is also responsible for initiating a group pairing process by distributing the initial key through QR code. Note that in the

proposed approach QR code serves the purpose of out-of-band (OOB) channel. The brief description of the high-level design is given below:

It is assumed that the mobile phones intended to become the part of secure group communication must have cameras to read the QR code and are also having support for wireless interface to connect and exchange data or information with each other in a group setting.

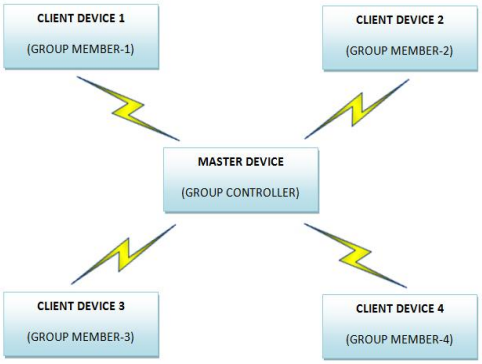

Figure-1: High-level architecture of the proposed system

In the proposed approach the master device first encodes some cryptographic material (i.e. a random short secret key) into a QR code and display it on its screen. Then, the user of every client device intended to become member of the group approaches the master device and reads the QR code (through the camera of his/her device) displayed on the master device to get the initial short secret key. Once the short secret key is obtained by the member device, it uses that short secret key to exchange the long term symmetric key in encrypted mode with the group controller through the normal in-band (i.e. WiFi) channel for further communication. Once the symmetric key is exchanged between the member device and group controller, it guarantees the secure communication between both of these devices. Consequently, later on group controller shares a common group key with group members in a secure way that ultimately results in secure group communication. The low-level and more technical discussion on the proposed approach is presented in subsequent sections.

3.2 Low-level Design of the Proposed System

In this section, the details of the proposed algorithm for group device pairing is presented preceded by the notations that could help in understanding the proposed algorithm.

Algorithmic Notations:

MD: Master Device (Group Controller)
GMD: Group Member Device
GCIK: Group Communication Initiation Key
MSG: Message
OTP: One Time Password
SGCK: Shared Group Communication Key

Step-1: (a) MD (Master Device) --> Generates GCIK (Group Communication Initiation Key)
(b) MD --> Generates SGCK (Shared Group Communication Key)
Step-2: MD --> Set MSG1:=Encode(GCIK)$_{QRCode}$
Step-3: MD --> Display(MSG1)
Step-4: GMD (Group Member Device) --> Read(MSG1)$_{MD}$
Step-5: GMD --> Set GCIK:= Decode(MSG1)$_{MD}$
Step-6: GMD--> Generate OTP (One Time Password)
Step-7: GMD --> Set MSG2:=Encrypt(OTP)$_{GCIK}$
Step-8: GMD --> Send(MSG2) to MD
Step -9: MD --> Set OTP$_{GMD}$:= Decrypt(MSG2)$_{GCIK}$
Step-10: MD --> Set MSG3:=Encrypt(SGCK) with OTP$_{GMD}$
Step-11: MD --> Send(MSG3) to GMD
Step-12: GMD --> Set SGCK := Decrypt(MSG3)
[Repeat steps 4 to 12 for every device intended to become part of the group communication]
Step-13: Return

Figure-2: The proposed algorithm for secure group device association

In figure-2, the proposed algorithm for secure group device pairing is presented. The description of each of the step of the algorithm is presented below:

In very first step, the master device (i.e. group controller or manager) generates a group communication initiation key (GCIK) that is a short secret key used to initiate the pairing process and a long term symmetric key, called shared group communication key (SGCK) that is actually used for group communication in a secure mode. Once the GCIK and SGCK are generated, the master device encodes GCIK only into a quick response (QR) code, while

keeps the SGCK with itself. QR code (i.e an array of black and white squares) is a special type of bar-code that could easily be read by mobile phones or other digital devices. QR codes are usually used for encoding short or limited information that could be read by any camera enabled device. After the encoding of GCIK within the QR code, it is displayed on the screen of master device.

Once the GCIK is displayed on the screen of master device, any other device/mobile phone intended to become the part of group communication need to access this QR code first. In this regard, the user of the member device need to approach the master device and read the QR code through the camera of member device. Then, the member device decodes the QR code to obtain the GCIK. After obtaining the GCIK, the member device generates its own one-time-password (OTP) key and encrypts it with GCIK and send it back to the master device through ordinary in-band wireless channel for further communication between them in a confidential/encrypted mode. This process (i.e. step - 4 to step - 12) is repeated for each device that intended to become the part of group communication.

Note that once SGCK is shared, the group pairing is achieved and hence the group member devices could securely communicate with each other using standard symmetric cryptographic primitives.

3.3 Message Sequence Diagram

In order to understand the proposed group pairing approach at high-level, a message sequence diagram is presented in figure-3. This message sequence diagram itself is self-explanatory and shows all the same steps that are explained in previous sections.

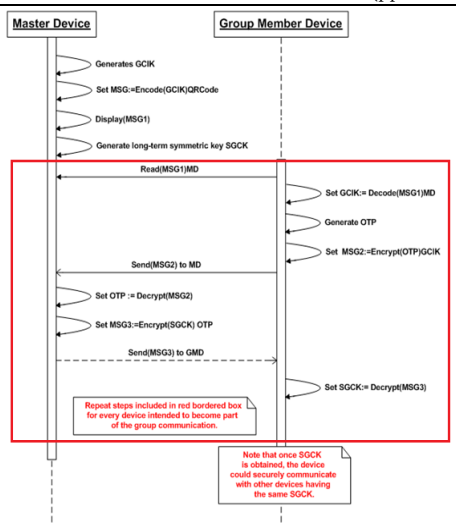

Figure-3: Message sequence diagram of the proposed approach

4. System Implementation and Testing

In order to validate or verify the viability of a theoretical solution, it is always desired to implement the system in real word and test it. Consequently, the proposed system is also implemented and tested in real-world scenarios.

The proposed approach/algorithm is implemented and tested using a Laptop that works as a WiFi hotspot and mobile phones running the Android operating system and coding is done using Android studio. Following mobile phones are used in implementation and testing phase:

- Samsung J5 (android 5.1 / 1.2 GHz quad core / 1.5 GB RAM)
- Samsung Mega (android 4.2 / 1.7 GHz dual core / 1.5 GB RAM)
- Qmobile Qtab x50 (android 4.2.2/1.2 Quad core / 1 GB RAM)

The reason to choose Android based mobile phones is that Android is an open source operating system and most of the modern mobile phones support it. Android studio IDE, as shown in figure-4, is installed

on a Corei7 machine with 8GB RAM with 3.6 GHz processing power and having Windows 7 operating system running on it.

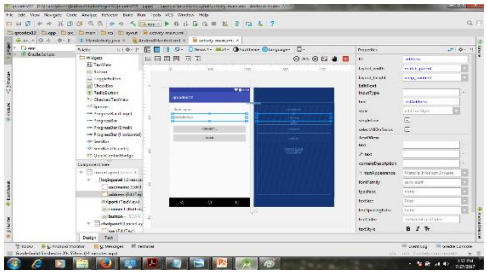

Figure-4: Android studio IDE

4.2 System Testing

In this section the working mechanism of the proposed system is demonstrated through some real-world test scenarios, which are prepared for testing the implementation of the proposed system.

The figures 5 to 8 show the snapshots taken during the testing of the proposed system after successful implementation. Figure-5 shows the Laptop that is used as WiFi hotspot and three mobile phones in which middle one is the master device (i.e. group controller) and other two are clients (i.e. group member devices).

Figure-5: Device involved in system testing

Figure-6: Client 1 reading QR code to obtain GCIK

Figure-6 illustrates the situation when client1 (i.e. group member device) scans the QR code from the master device in order to obtain the GCIK. Client1 once receives the GCIK, it generates its OTP and sends it to the master device encrypted with GCIK through WiFi channel.

Figure-7 shows the situation when client2 (i.e. group member device) scans the QR code from the master device in order to obtain the GCIK. Client2 once receives the GCIK, it generates its OTP and sends it to the master device encrypted with GCIK through WiFi channel.

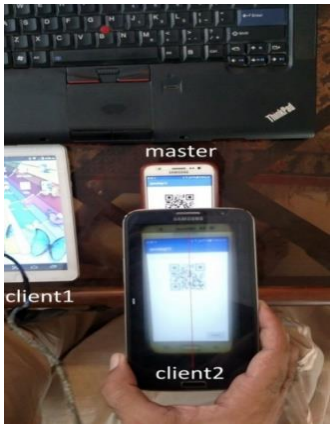

Figure-7: Client 2 reading QR code to obtain GCIK

(a) (b) (c)

Figure-8: Sample of logs generated on each device involved in pairing process

(a) Master Device (Group Controller)
(b) Client-1 (Group Member Device)
(c) Client-2 (Group Member Device)

Figure-8 shows the three snapshots taken after successful pairing of group of devices. Figure-8 (a) shows the log generated at master device during the pairing process, while the Figure-8 (b) and Figure-8 (c) show log/text generated on client 1 and client 2 devices respectively. It could be seen in figures 8 (b) and 8 (c) that both of the devices are exchanging information/data between themselves through a chat application, which is developed to test the secure communication between group members after successful pairing. This testing procedure is repeated several times to make sure that the system working well and is reliable. After system testing, a usability study of the developed system is performed and the details of that study are discussed in next section (i.e. results and discussion) in detail.

5. Results and Discussion

In order to meet the aims and objectives of this research work, we proposed a group device association scheme for mobile ad hoc networks (MANETs). The proposed scheme is implemented, tested and its usability evaluation is also performed to confirm that the proposed system is user-friendly and practically a usable solution for group device association scenarios.

The usability evaluation test equipment are the same as used during system implementation and testing. The only difference is that during the usability testing, we allowed the test participants to use their own smart phones so that more realistic working of the proposed system could be analyzed. In the usability evaluation seventy two (72) participants are recruited to use the developed system and provide their feedback about it and also rate the developed system on 7-point likert-type-scale [45], [46].

Table-1: Usability evaluation participants' demographic data

	Nos.	%age
Gender:		
Male	57	79%
Female	15	21%
Age:		
18 – 23	52	72%
24 – 28	15	21%
29 or above	5	7%
Last Qualification:		
Intermediate	16	22%
BS/MSc/MCS or Equivalent Degree	46	64%
MS/M.Phil	8	11%
PhD or above	2	3%
Occupation:		
Teaching	6	8%
Student	58	81%
Other	8	11%

As stated earlier, the usability evaluation of the developed system is conducted by recruiting seventy two (72) participants. The usability evaluation participants are either students, teachers or employees of University of Sindh, Mehran University of Engineering & Technology and Liaquat University of Medical and Health Sciences, Jamshoro. The demographic data of the participants is provided in table-1, which is self-explanatory and requires no more description.

5.1 Usability Evaluation Results

This section presents the results that are obtained by analyzing the data gathered during the usability evaluation. In order to collect the usability data, two (02) questionnaires (i.e. pre-test questionnaire and post-test questionnaire) are used. In pre-test questionnaire usability evaluation participants are asked to provide

their demographic information, while post-test questionnaire is used to record the participants rating scores for four (04) usability evaluation questions with regard to the developed system. The user rating is carried out through seven-point likert scale in which each participant is asked to provide their ratings by selecting the score in the range 1 to 7. One is considered as the least score, while seven indicates the highest or the most satisfactory score. Microsoft Excel package is used to store and process the collected data for analysis purposes.

Figure-9: Usability evaluation participants while using the developed system in small groups (i.e. 4 members in each group)

Figure-10: Usability evaluation participants while using the developed system in larger groups (i.e. 10 members in group)

Figures 9 and 10 show some random snapshots taken during the usability study. In usability study, total fourteen (14) groups are formed consisting of overall seventy two (72) members. First twelve (12) groups are consisting of four (04) members in each, while the 13th group is consisting of ten (10) members and the 14th group is consisting of fourteen (14) participants. The reason to increase the numbers in group 13 and 14 is to test whether the proposed solution is workable in scenarios where number of users increase and decrease time-to-time.

The charts or graphs in figure 11 to figure 16 show the results of usability evaluation for first ten (10) groups having four (04) participants in each group. Every usability participant is provided four different questions through the post-test scenario questionnaire and asked to provide the rating for each of them.

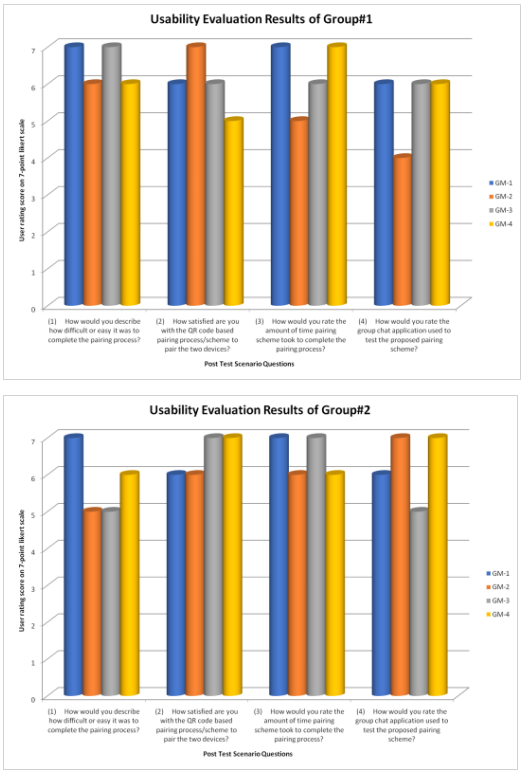

Figure-11: Usability evaluation scores as given by participants of groups #1 and #2

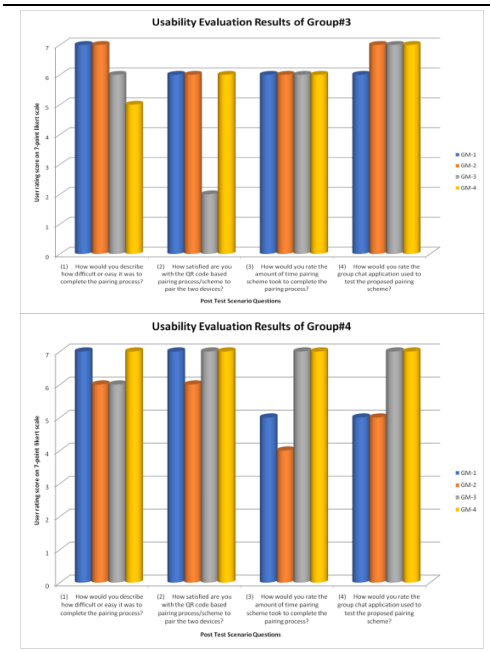

Figure-12: Usability evaluation scores as given by participants of groups #3 and #4

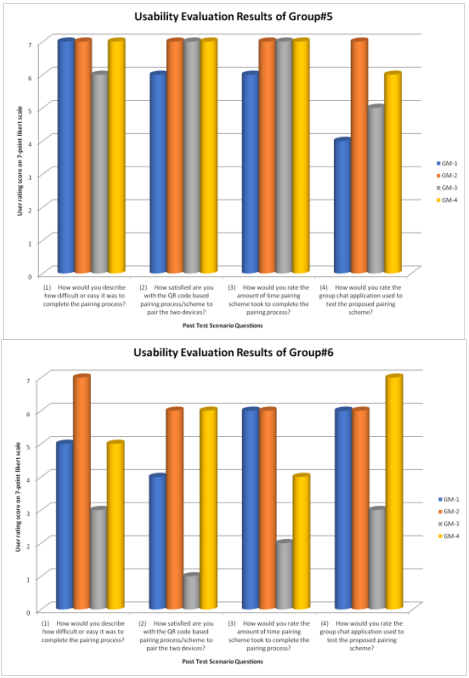

Figure-13: Usability evaluation scores as given by participants of groups #5 and #6

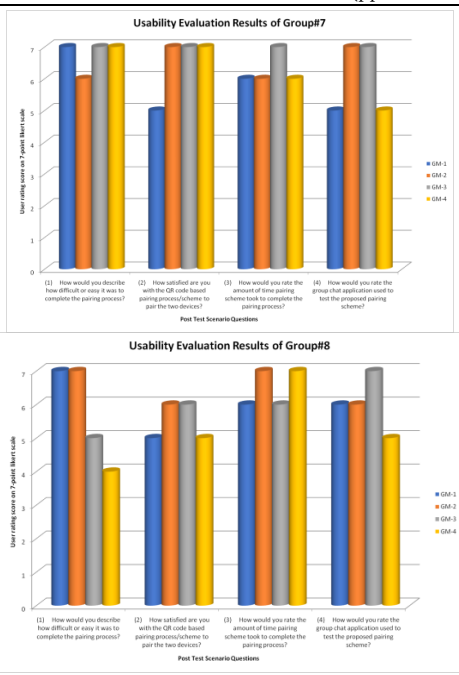

Figure-14: Usability evaluation scores as given by participants of groups #7 and #8

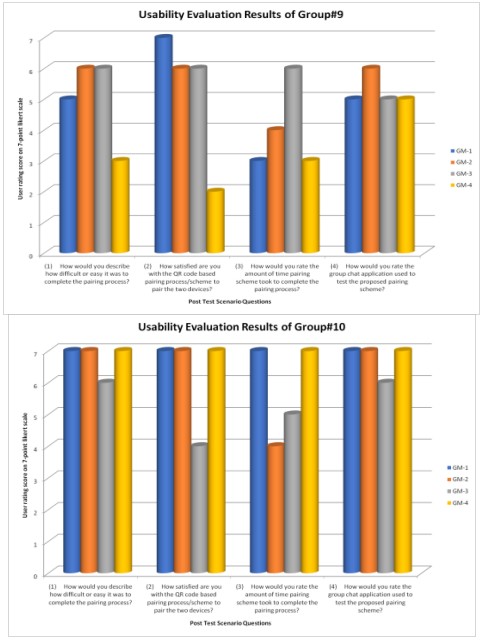

Figure-15: Usability evaluation scores as given by participants of groups #9 and #10

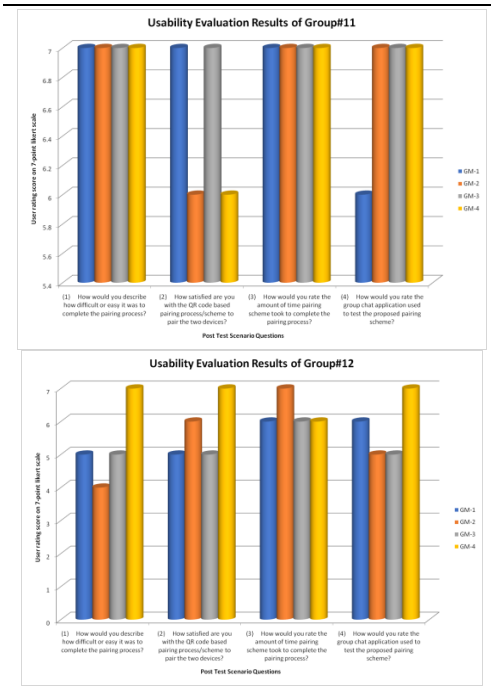

Figure-16: Usability evaluation scores as given by participants of groups #11 and #12

The charts or graphs in figures 17 and 18 show the results of usability evaluation for last two groups.

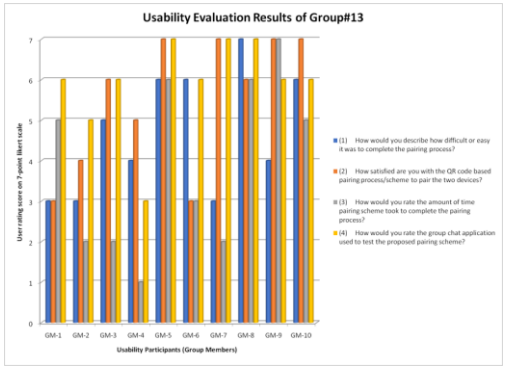

Figure17: Usability evaluation scores as given by participants of groups #13

Figure-17 refers to the results of group 13, where ten (10) participants performed the task of group pairing and provided their usability score as per their experience. Similarly, figure-18 shows the results obtained from group 14, which is consisting of fourteen (14) group members. Again in this setting, every usability participant is provided four different questions through the post-test scenario questionnaire and asked to provide the rating for each of them.

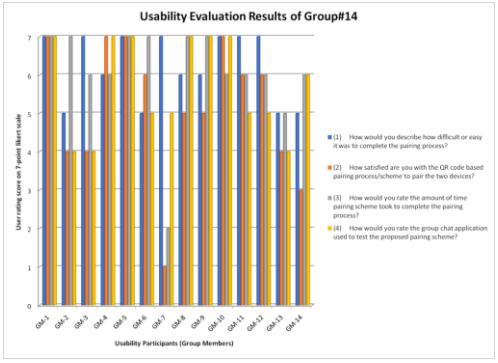

Figure-18: Usability evaluation scores as given by participants of groups #14

The chart shown in figure-19 provides the overall summary of the usability evaluation results. This chart shows the mean and standard deviation of all scores as provided by all of usability participants and as discussed/shown in figures 11 to 18.

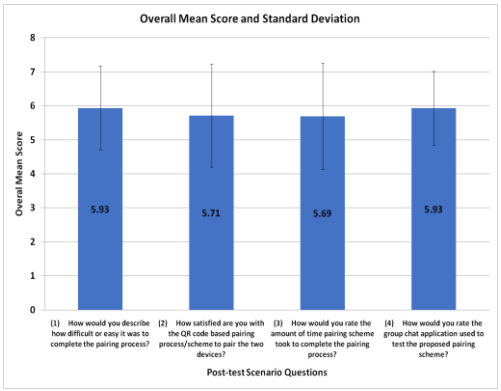

Figure-19: Overall mean and standard deviation of all the scores as given by usability evaluation participants

Nielsen. et al. [45] has indicated that while performing usability evaluation experiments through a seven-point likert scale, if one gets the mean score that is equals to 5.6 or above it,

the produce or system under evaluation could be considered as usable and acceptable for use. Note that the last chart (figure 5.11) shows that for each of the usability question/parameter, the mean score is above 5.6. Consequently, the developed system is considered as one of the good and usable solution for the scenarios where there is need of associating more thatn two devices in mobile ad hoc networks (MANETs).

5.2 Comparative Analysis

This section presents the comparative analysis of the proposed developed system with prior work on group device association. As stated in literature review section, there is very less work done on group devices assocation and hence we found only one work [42] that is closely relevant to the proposed system.

Table-2: Comparative analysis of the proposed approach with prior work on group device paring

Approach to group device association	Maximum supported distance between devices while initialing pairing	Out-of-Band (OOB) channel used
NFV: Near Field Vibration Based Group Device Pairing (Zhiping Jiang et al., 2015) [12]	Upto 40 cm (15.748 inches)	Vibrator and motion/vibrator detector sensor
The Proposed Approach	Upto 50.8 cm (20 inches)	QR (quick response) code and camera

Consequently, the proposed system is compared with it [42] and the comprasion results are shown in table 5.4. From table 5.4, it could be seen that the prposed systme is more better in terms of distance requied for initiating the pairing process. Also note that the work proposed by Zhiping Jiang et al. best performs only when they use plastic table / surface [42], however in our proposed approach there is no any restriction of surface type is imposed.

6. Conclusion

Mobile Ad hoc Networks (MANETs) are becoming common day by day. Devices in a MANET interact with each other through a wireless channel, which requires secure association between the communicating partners prior to exchanging any information or data. The concept of establishing secure association between two or more devices in close proximity is known as device paring. One of the less addressed aspect of device pairing is the association of more than two devices (i.e. also known as group pairing). In this paper, a solution to the issue of group pairing in MANets is presented. The outcome of the proposed research can be used in various scenarios of MANets where secure and spontaneous interaction among a group of devices is desired, such as smart conference halls and meeting rooms, etc. The most important and major contribution of this work is the proposal and development of a QR code based system that allows the pairing of a group of devices. The other two contributions of this research work are (a): a comprehensive and detailed literature survey of device pairing that could help the newbie researchers to understand the device paring domain in a very quick manner, and (b) the conduct of a usability evaluation of the proposed solution to verify whether the proposed solution is user-friendly or not. The usability evaluation results were also positive and the results indicated that the proposed system is working very well in real world scenarios and is one of the usable and acceptable solution from users point of view.

AUTHOR CONTRIBUTION*:* In this paper, Yasir Arfat Malkani and Lachman Das Dhomeja conceived the idea of the paper. Further, Yasir Arfat Malkani and Moez Ahmed Malik jointly performed the system Implementation and conducted usability study with some support from Lachhman Das Dhomeja. Abdul Waheed Mahesar and Bisharat Rasool Memon helped in literature survey and to refine/improve the system and also supported in writing the paper.

DATA AVAILABILTY STATEMENT: There is no any third party data is used in this research. However, the raw (usability study) data collected as part of this research is available (if required).

CONFLICT OF INTEREST: None

FUNDING: No any funding received and used for this research.

REFRENCES

[1] Y. A. Malkani and L. Das Dhomeja, "Secure device association for ad hoc and ubiquitous computing environments", International Conference on Emerging Technologies, Islamabad, Pakistan, 2009, pp. 437-442, doi: 10.1109/ICET.2009.5353132..

[2] Y. A. Malkani, "A proof-of-proximity framework for device pairing in ubiquitous computing environments," A Univ. Sussex DPhil thesis, 2011.

[3] M. Qabulio, Y. A. Malkani, and A. Keerio, "On Node Replication Attack in Wireless Sensor Networks," vol. 34, no. 4, pp. 413–424, 2015.

[4] M. Qabulio, Y. A. Malkani, and A. Keerio, "A framework for securing mobile wireless sensor networks against physical attacks", 2016 International Conference on Emerging Technologies (ICET), Islamabad, Pakistan, 2016, pp. 1-6, doi: 10.1109/ICET.2016.7813265.

[5] N. Saxena, Md. Borhan Uddin, and J. 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, 56--67. DOI:http://dx.doi.org/ 10.1145/1408664.1408672

[6] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, "Feeling is Believing : a location limited channel based on grip pattern biometrics and cryptanalysis," no. 2.

[7] N. Saxena and J. Voris, "Pairing devices with good quality output interfaces," Proc. - Int. Conf. Distrib. Comput. Syst., pp. 382–387, 2008.

[8] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, "Secure Ad-hoc Pairing with Biometrics: SAfE," Proc. 1st Int. Work. Secur. Spontaneous Interact. (IWSSI '07), pp. 450–456, 2007.

[9] C. Soriente, G. Tsudik, and E. Uzun, "BEDA: Button-enabled device association," Int. Work. Secur. Spontaneous Interact., 2007.

[10] R. Mayrhofer and H. Gellersen, "Shake Well Before Use: Authentication Based on Accelerometer Data," Pervasive Comput., pp. 144–161, 2007.

[11] A. Varshavsky, A. Scannell, A. LaMarca, and E. de Lara, "Amigo: Proximity-Based Authentication of Mobile Devices," pp. 253–270, 2007.

[12] E. Haselsteiner and K. Breitfuß, "Security in Near Field Communication (NFC) Strengths and Weaknesses," Semiconductors, vol. 11, no. 71, p. 71, 2006.

[13] BTSIG, "Simple Pairing Whitepaper," Bluetooth Spec. Interes. Gr., vol. 1, no. 1, p. 23, 2006.

[14] M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun, "Loud and Clear : Human-Verifiable Authentication Based on Audio 1 Introduction 2 Related Work," Elements, pp. 1–16, 2006.

[15] N. Saxena, J. Ekberg, K. Kostiainen, and N. Asokan, "Secure Device Pairing based on a Visual Channel (Short Paper) ∗," pp. 2–7, 2006.

[16] C. Castelluccia, "Shake Them Up!," ACM/Usenix Mobisys, pp. 51–64, 2005.

[17] A. Pathan, Security of self-organizing networks: MANET, WSN, WMN, VANET. 2016.

[18] J. Lester, B. Hannaford, and G. Borriello, "'Are You with Me?' – Using Accelerometers to Determine If Two Devices Are Carried by the Same Person," pp. 33–50, 2004.

[19] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to Strangers: Authentication in Ad Hoc Wireless Network," Proc. 9th Netw. Distrib. Syst. Secur. Symp., pp. 46–56, 2002.

[20] F. Stajano, "The resurrecting duckling—what next?," Secur. Protoc., pp. 204–214, 2001.

[21] L. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl5, and H.-W. Gellersen, "Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts," Ubicomp 2001 Ubiquitous Comput. SE - 10, vol. 2201, pp. 116–122, 2001.

[22] F. Stajano and R. J. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," Proc. 7th Int. Work. Secur. Protoc., pp. 172–194, 2000.

[23] M. K. Chong, R. Mayrhofer, and H. Gellersen,

"A survey of user interaction for spontaneous device association," ACM Comput. Surv., vol. 47, no. 1, p. 8, 2014.

[24] S. Mirzadeh, H. Cruickshank, and R. Tafazolli, "Secure device pairing: A survey," IEEE Commun. Surv. Tutorials, vol. 16, no. 1, pp. 17–40, 2014.

[25] Y. A. Malkani, "A Generic Framework for Device Pairing in Ubiquitous Computing Environments," Int. J. Netw. Secur. Its Appl., vol. 4, no. 2, pp. 1–20, 2012.

[26] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-Is-Believing: using camera phones for human-verifiable authentication," Int. J. Secur. Networks, vol. 4, no. 1/2, p. 43, 2009.

[27] C. Soriente, G. Tsudik, and E. Uzun, "Secure pairing of interface constrained devices," Int. J. Secur. Networks, vol. 4, no. June, p. 9, 2009.

[28] R. Prasad and N. Saxena, "Efficient device pairing using 'human-comparable' synchronized audiovisual patterns," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5037 LNCS, pp. 328–345, 2008.

[29] N. Saxena and M. B. Uddin, "Automated device pairing for asymmetric pairing scenarios," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5308 LNCS, pp. 311–327, 2008.

[30] J. Loo, J. Mauri, and J. Ortiz, Mobile ad hoc networks: current status and future trends. 2016.

[31] S. Al-Sultan, M. Al-Doori, … A. A.-B.-J. of network and, and undefined 2014, "A comprehensive survey on vehicular ad hoc network," Elsevier.

[32] E. Hellman, "New Directions in Cryptography," 1976.

[33] R. M and A. Jain, "Biometrics : The Future of Identification It is too early to predict where , how , and in which form reliable biometric," Technology, pp. 46–49, 2000.

[34] K. Seewoonauth, E. Rukzio, R. Hardy, and P. Holleis, "Touch {&} connect and touch {&} select: interacting with a computer by touching it with a mobile phone," MobileHCI '09 Proc. 11th Int. Conf. Human-Computer Interact. with Mob. Devices Serv., p. 1, 2009.

[35] C. Soriente, G. Tsudik, and E. Uzun, "HAPADEP: Human-Assisted Pure Audio Device Pairing," in Information Security, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 385–400.

[36] D. Sangster, C. Dreher, … J. N.-U. P., and undefined 2016, "Systems and methods for pairing bluetooth devices," Google Patents.

[37] C. Soriente, G. Tsudik, and E. Uzun, "Information Security," vol. 5222, no. September 2008, 2008.

[38] J. P.-N. S. Publication and undefined 2017, "Guide to bluetooth security," nvlpubs.nist.gov.

[39] E. G.-I. I. Computing and undefined 1999, "Service location protocol: Automatic discovery of IP network services," ieeexplore.ieee.org.

[40] 278 DY Cheng - US Patent App. 09/742 and undefined 2002, "UPnP enabling device for heterogeneous networks of slave devices," Google Patents.

[41] L. Ming, Y. Shucheng, L. Wenjing, and R. Kui, "Group Device Pairing based Secure Sensor Association and Key Management for Body Area Networks BT - INFOCOM, 2010 Proceedings IEEE," pp. 1–9, 2010.

[42] Z. Jiang, J. Han, W. Xi, and J. Zhao, "NFV: Near Field Vibration Based Group Device Pairing," 2016, pp. 129–140.

[43] E. Jovanov, A. Milenkovic, C. Otto, and P. C. De Groen, "A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation," vol. 10, pp. 1–10, 2005.

[44] K. Lorincz et al., "Sensor Networks for Emergency Response: Challenges and Opportunities," Pervasive Comput., vol. 3, no. 4, pp. 16–23, 2004.

[45] Xiaopeng Li, Qiang Zeng, Lannan Luo, and Tongbo Luo. 2020. "T2Pair: Secure and Usable Pairing for Heterogeneous IoT Devices". In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20). Session 1E: Cyber Physical Systems November 9–13, 2020, New York, NY, USA, pg: 309–323.

[46] J. Nielsen, J. L.-C. of the ACM, and undefined 1994, "Measuring usability: preference vs. performance," dl.acm.org.

[47] A. Seffah, M. Donyaee, R. B. Kline, and H. K.

Padda, "Usability measurement and metrics: A consolidated model," Softw. Qual. J., vol. 14, no. 2, pp. 159–178, Jun. 2006.