An Approach of Secure and Fashionable Recognition for Pervasive Face-to-Face Social Communications

Zheng Yan
The State Key Lab of ISN, Xidian University, China
Dept. of ComNet, Aalto University, Finland
zyan@xidian.edu.cn

Yu Chen
Swiss Federal Institute of Technology (EPFL)
CH-1015, Lausanne, Switzerland
yu.chen@epfl.ch

Peng Zhang
The Institute of Mobile Internet
Xian University of Posts and Telecommunications
Xi'an, China
pzhang@xupt.edu.cn

Abstract—**Pervasive social communications are instant social activities through communications based on mobile elements, e.g., via mobile ad hoc networks. Meanwhile, fashionable technology is becoming a trend in Human-Computer Interaction (HCI) design. It extends the traditional understanding of HCI by emphasizing aesthetic element. This paper investigates how to use fashionable technology in pervasive social communications. It presents a novel approach to realize secure recognition for pervasive face-to-face social communications based on MANET, local connectivity and fashionable technology. The social acceptance of this inter-disciplinary approach is explored through a small-scale user study.**

Keywords-trust, identity, fashionable technology, wearable computing,

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) has a good prospect of becoming a practical platform for instant social activities [1]. MANET is a collection of autonomous nodes that communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. A social group could be instantly formed based on MANET not only by people socially connected, but also those physically in proximity, such as groups for common instant social activities. For example, Groupon (http://www.groupon.com) provides daily digests of group purchase activities to users; eRideShare (http://www.erideshare.com/) helps people with similar driving routes to share car riding. People could chat with strangers nearby using mobile devices based on MANET first and then decide to meet with each other for a direct face-to-face contact, e.g., for the purpose of purchasing 'buy 3 pay 2' goods. This kind of thorough pervasive social communications is an essential and valuable complement for Internet social networking and traditional social communications.

Trust plays an important role in the pervasive social networking (PSN) for reciprocal activities among nearby strangers. It helps people overcome perceptions of uncertainty and risk and engages in behaviors that would not be possible without it. During the instant social activities, people are not necessarily acquaintances but more likely to be strangers. They generally talk with each other with nick names and build up initial trust based on MANET communications. This initial trust could motivate them to make an instant appointment for a face-to-face meeting. In such a situation, it is important to make a recognition mechanism for strangers to meet with each other in a secure way.

Mobile phone, as one major device for pervasive social communications, can be further developed to extend its functions into wearable devices for improving personal fascination and achieving sound social effects. Nowadays, aesthetics is becoming a key factor that influences a person to make a decision on a concrete action. Fashion has played as a social element to impress and attract people. Fashionable technology refers to the intersection of design, fashion, science and technology [2]. It integrates aesthetics and fashionable into functional technologies. Particularly, fashionable wearable represents the fashionable technology by using wearable devices, such as the devices attached to garments, accessories or jewelries. Recently, fashion industries are making efforts to combine fashion and high technologies together.

In practice, MANET provides a generic platform for pervasive social networking. Various instant social activities can be supported by this platform. For some social activities, after anonymous MANET based communications, people in proximity, but unfamiliar with each other would like to meet for further face-to-face contact. How to make unknown people to meet without mismatch and avoid troubles after MANET based communications? How to sustain their initially established trust through right recognition in crowds? How to preserve their privacy (e.g., still using nick names and hiding real names) but assure correct recognition in a secure and fashionable manner? How to fight against malicious persons who may personate somebody for face-to-face contact? In this situation, it is essential to provide an approach to let people who communicated before via pervasive social networking or other networks securely recognize with each other and meet in an easy way. However, literature still lacks an efficient, secure and convenient manner to recognize people in pervasive social communications.

This paper gives an answer to the above questions that haven't been solved in prior arts. We propose a novel approach to realize secure and fashionable recognition for pervasive face-to-face social communications based on MANET, local connectivity and fashionable technology. It is an inter-disciplinary technology and could open up a new research

978-1-4673-1430-5/12/$31.00

horizon on fashionable security. Concretely, a fashionable wearable device (FWD) (e.g., embedded into handbags, garments, accessories or jewelries) is applied with the assistance of its wearer's mobile device (e.g., a mobile phone) to provide a secure and fashionable way to recognize strangers for face-to-face social communications. The FWD is decorated with some displaying elements, e.g., Light Emitting Diode (LED) lights. The status of the LED lights is controlled by a corresponding mobile FWD application (MFA) executed in the FWD wearer's mobile device. The communication between the FWD and the MFA is securely paired, thus the information displayed or illustrated by the FWD can be controlled by the MFA. For example, the control signal between the FWD and MFA is transmitted through Bluetooth or other local connection methods.

For secure and fashionable recognition, we use the FWD to illustrate a pre-defined recognition protocol among strangers. The FWD plays as a displaying platform, in order to make short distance pervasive social communications obvious and attractive. The protocol could contain one or several rounds of 'argot' (i.e., a kind of code word) interaction in order to securely make the strangers recognize with each other in crowds. The successful execution of the recognition protocol is coordinated by the mobile devices based on MANET. That is the display of FWDs can be coordinated based on the control and communications of their corresponding MFAs.

The recognition protocol is designed by users through their mobile devices during the pervasive social networking via MANET. If needed, those people unknown with each other can use their mobile devices to define how to recognize with each other if a face-to-face meeting is needed. (Note that photo or video sharing may not be preferred by some users who would like to keep their privacy by hiding any tracking clues and personal information). The protocol can be designed via MFA by indicating the identity and type of FWD for mobile device local pairing and the 'argots' used in each step of protocol, as well as their displaying style. The MFA provides a user interface to help users easily fulfill this design function.

The rest of the paper is organized as below. Section 2 briefly reviews related work in the field of fashionable and wearable technology, as well as secure pervasive social networking. Section 3 presents our approach. This is followed by the regonization protocol in Section 4. In Section 5, we explore the acceptance of the proposed approach through a small-scale user study. Finally, conclusion and future work are presented in the last section.

II. RELATED WORK

Several research groups have focused on social activities based on mobile ad-hoc networks. Stanford MobiSocial Group has developed Junction, a mobile ad hoc and multiparty platform for MANET applications [3]. Micro-blog [4], developed by SyNRG in Duke University, helps users to post micro-blogs tagged by locations and viewed by others. AdSocial [5], introduced by ETHz Systems Group, aims to provide a pervasive social communication platform. However, secure recognition for face-to-face meeting between strangers after pervasive social networking is not considered at all in these projects. Traditional centralized social networking systems (e.g., facebook) have not taken this issue into account. They cannot support instant social face-to-face meeting in a secure, easy and fashionable way, especially when users do not have internet connection, but with location proximity.

Our previous works, AdContRep [6] and AdChatRep [7] provide trust evaluation based on pervasive social communications via MANET. This evaluation solves the issue of establishing initial trust in instant social activities via ad hoc network communications. But it didn't touch the issues listed in Introduction to comprehensively support trustworthy recognition in instant face-to-face social communications, which could be demanded in many application scenarios.

On the other hand, wearable computing designs equipments and devices wearable by humans. The most common wearable items include clothes, shoes, bracelets, handbags, hats, gloves, and so on. Fashionable technologies go beyond wearable computing by emphasizing aesthetics.

MIT Media Lab is among early research institutes engaged in fashionable technologies. Romandic radio [8] and Music Jacket [9] were their early prototypes. Romandic Radio is a neckset that aims to mine ambient contextual information and send to users as notification. It gathers the ambient sound through microphones on the neckset and notifies users via audio messaging or tactile feedback on the body. Music Jacket aims to extend musical environment. It combines a normal Levi jean jacket with a fabric keyboard and a midi signal generator to produce a sound and applies speakers to amplify the sound. All the add-ons are embroidered inside the jacket.

Jacket has become a popular platform for developing fashionable technology due to its daily-use nature. Smart Jacket [10] is designed to control body temperature, enhance night visibility and monitor activity level. For example, some parts of the jacket glow in the evening to provide warning of safety, e.g., in traffic. Love Jackets [11] are a pair of jackets designed for social awareness. Once the pair finds each other, in at least 3-meter distance, facing each other, the two jackets beep and blink.

Women consider dresses as a symbol of femininity and fashion. Firefly Dress [9] and necklace uses conductive fabric to distribute power throughout the dress. The dress was attached with small lights, i.e., LEDs. When the wearer moves, the LEDs brush lightly against the fabrics power, creating a dynamic lightening effect. A more recent artifact is the Microsoft Printing Dress [12]. The printing dress enables wearer to enter their thoughts onto the fabric and wear them as a form of art displayed to the public. It is one of the pioneer works that integrates the fashionable technology with social networks.

Bags are among the top consumed fashionable accessories. It is thus natural to design technology-enhanced fashionable bags. Courtly bag [13] is a fashionable bag containing lights and sounds that can shine in dark and transmit information. LadyBag [14] is designed to notify missing items in the bag. All items in the bags, e.g., keys, phones are attached with RFID tags. Therefore, the bag keeps log of items in the bag. It shows the icons of missing items on the LED display of the bag. SEIL

bag is a handbag using a LED display and a flexible printed circuit board for safe bicycle riding. It displays important information such as turning and braking to travelers behind.

All the work mentioned above shed light on a novel means and materials for the fashionable technology. However, prior arts have not investigated the social value and usage of the fashionable technology, especially for social communications. Most of previous designs are standalone accessories, which cannot communicate with each other for security purpose. Most of them are very expensive and still in its infant stage. Our work, on the other hand, uses a Fashionable Wearable Device as an illustration platform. It coordinates with the wearer's mobile device in order to provide a fashionable way of secure social communications that can be easily accepted by mobile users in terms of aesthetics and functions.

III. SYSTEM DESIGN

A. *Example Scenario*

We name the system implementing the proposed approach as SecGemini. The name "Gemini" originates in astrology, which refers to the third sign of zodiac [17], with the support of another person taken inside. Gemini emblematizes the coordination between FWD and MFA. SecGemini provides a function for secure pervasive face-to-face social communications. SecGemini can be applied into such a scenario that strangers in vicinity communicate with each other in a digital way, for example via mobile ad hoc networks. After establishing initial trust, they would like to make an instant face-to-face meeting. The work presented in this paper provides a secure and fashionable approach to help them securely recognize with each other with fascination.

B. *SecGemini System Design*

The proposed system consists of two parts: FWD that is wearable and mobile FWD application (MFA) in a mobile device (e.g., a wearer's mobile phone). Taking aesthetics, prices and functions into account, we design an FWD, which can be a surface material or portable decoration of a handbag, a hat, clothes or many other kinds of wearable. There are two ways of information display in SecGemini: the information displayed on the FWD to the public and the information displayed in mobile device screen that is provided by the MFA. The MFA and FWD are paired in a secure way, e.g., by sharing a symmetric key. Thus, the MFA can uniquely control the display of paired FWD. The FWDs can coordinate their display through the communications of MFAs via MANET.

FWD is a fashionable wearable device embroidered with an LED panel with an array of LED lights, as shown in Figure 1. The colors of the LEDs can be customized upon need. Each light has two states: on or off. When all lights are off, the LED panel serves as a normal decoration. When the light is turned on, it can show one or multiple colors. When a certain signal is sent to the LED panel, the array can display meaningful information on the wearable that is decorated, serving as a blinking, shining and unique component of the wearable. Using arrays of LED saves implementation cost. It is one of the cheapest ways to display information. Obviously, other techniques can be adopted for wearable display purpose.

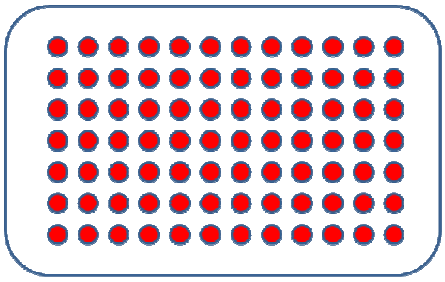

Figure 1: An example fashionable wearable device embroidered with an LED panel with an array of LED lights

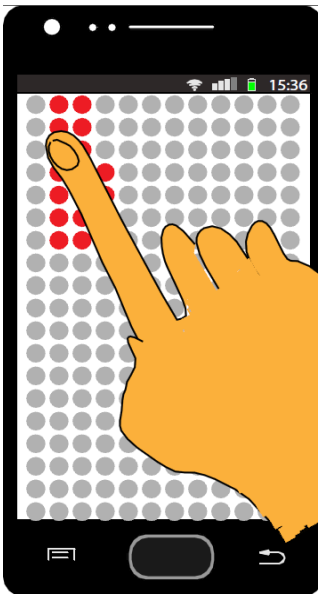

Figure 2: A touch screen UI to define an argot and its presentation style

MFA is a private mobile application in personal mobile device that can be used to design what is shown and how to show it on the paired FWD. It also serves as the remote controller of FWD. It can be one basic function of a pervasive social networking application (e.g., AdChatRep [7]) and used to design the recognition protocol. For example, the MFA provides a user interface to define the identifier and name of wearable (e.g., handbag, hat, T-shirt or jacket) used for recognition; the number of recognition steps, the argot used in each step of recognition and its order. For designing the argot, the MFA provides a wizard to allow its user to design how to present the argot on the LED panel. For example, the MFA emulates the LED panel of FWD. The user can define the argot by drawing on the surface of touch screen. He/she can also design a presentation style by customizing the wizard. The wizard also provides many templates to help users efficiently design the argot and its displaying style. Once the user confirms his/her design, the MFA saves the argot into the protocol.

FWD and MFA can communicate via Bluetooth or other short distance connectivity methods. Each FWD has a secret key. The MFA needs the key in order to pair up with the FWD. This design ensures the security of the proposed system. Therefore, only an authorized MFA can control the presentation of the FWD. Once successfully paired up, the MFA can send a signal to control the presentation of the FWD, i.e., the status of each LED light and its color and display style, as well as the music/tone attached to each argot. The FWD presentation can be designed by its wearer through the MFA user interface, e.g., via a touch screen, shown in Figure 2.

Two or multiple FWDs can coordinate with each other based on the communications among MFAs. For example, a series of argots can be displayed one by one (in an order) on the FWDs of different wearers aiming to recognize for a face-to-face meeting; different parts of one argot can be displayed in different wearers' FWDs for secure recognition. The argot could be a word, a picture, a symbol, and so on. A series of argots can be applied in the recognition protocol in order to achieve sound security.

C. *Secure Protocol in Pervasive Social Networking based on MANET*

Adopting a secure protocol in pervasive social networking is essential for negotiating a secure face-to-face recognition protocol. During the design of the recognition protocol, all messages exchanged between PSN users should be securely routed to their destinations and protected to be accessed by authorized users. Although secure protocol is not the main focus of this paper, we herein propose using a trust evaluation based security solution to provide effective security decision on data protection, secure routing and other network activities, as described in our past work [18]. Meanwhile, we suggest using a secure protocol based on a trusted computing platform to ensure trustworthy behaviors at each PSN user device as a remote user expected, as described in [19]. In order to control pervasive social communication data access, we apply an attribute-based encryption technology [20] to control data access in PSN based on a specified trust threshold and context attributes. It supports data broadcast or multicast in PSN can be only accessed by those users whose trust levels are above the threshold, and that satisfy the requirements specified in the context attributes. Detailed solution will be presented in another paper.

IV. SECURE RECOGNITION PROTOCOL

A. *Recognization Protocol Generation*

The recognition protocol can be generated through negotiation among potential users (FWD wearers) via secure PSN communications based on MANET. The MFA provides an easy user interface to instantly design a recognition protocol. The steps for recognition protocol generation are described below:

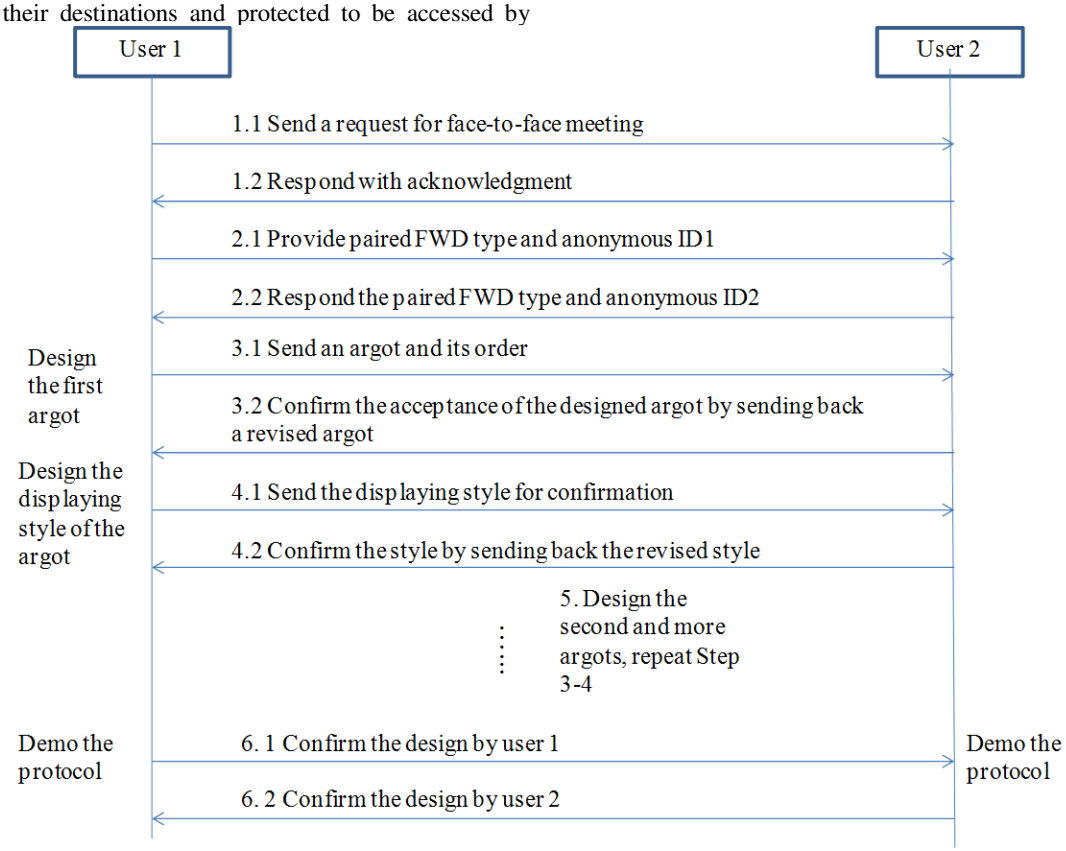

Figure 3: A recognition protocol generation procedure between two users

Step 1: Request and acknowledgment of protocol generation;

Step 2: Select a FWD for pairing and notify other parties;

Step 3: Negotiate an argot used in the recognition by indicating its order;

Step 4: Decide presentation style of the argot, e.g., flashing or blinking, color, and music attached to the argot.;

Step 5: Repeat Step 3-4 until the design is finished;

Step 6: Demonstrate the recognition protocol for final confirmation of each party. If the user doesn't satisfy the design, repeat Step 3-5.

The protocol can support recognition for two users or multiple users. A concrete recognition protocol generation procedure between two users is illustrated in Figure 3. An example recognition protocol generation procedure among multiple users is illustrated in Figure 4.

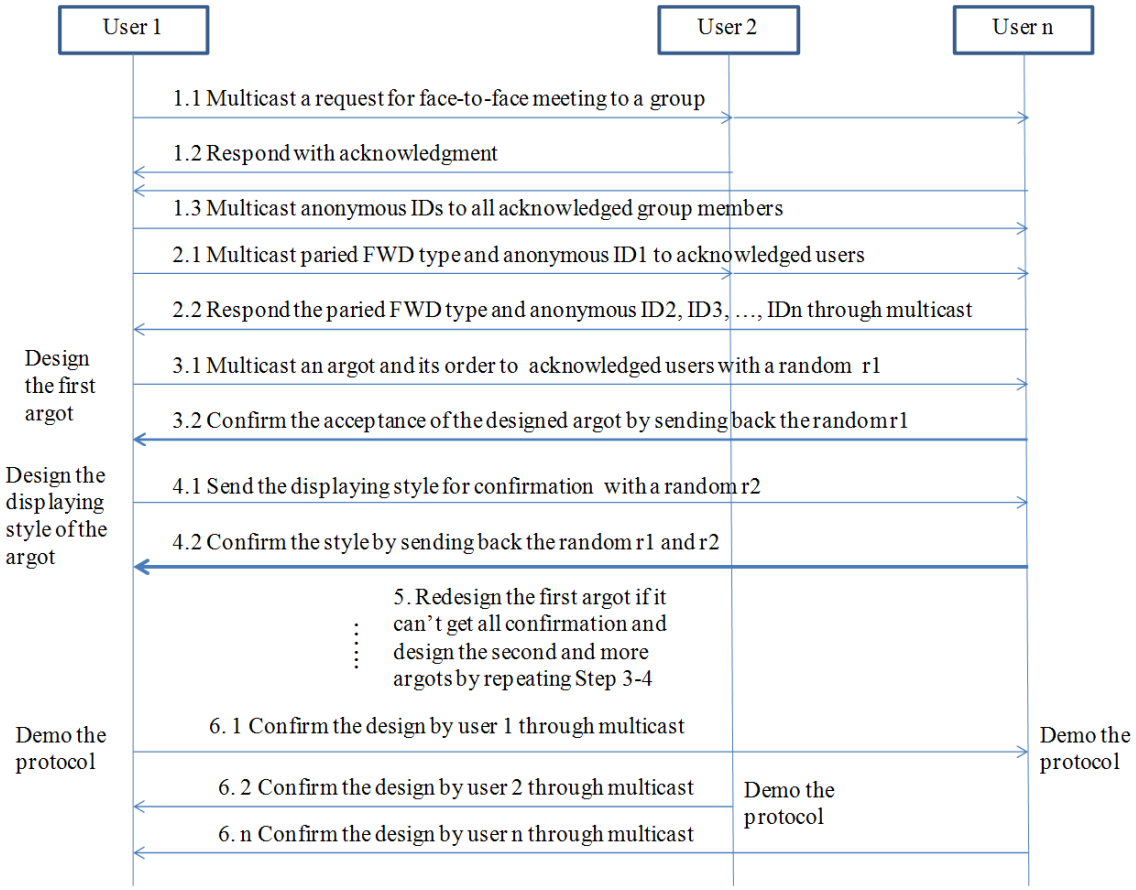

Figure 4: An example recognition protocol generation procedure among multiple users

In Fig. 3, User 1 would like to make an instant face-to-face meeting with another user (User 2). In this case, User 1, as an inviter of the meeting, may use his/her mobile device with MFA to initiate the procedure for generating the recognition protocol by sending a request for a meeting to User 2 and receiving an acknowledgment from the mobile device of User 2. Then User 1 performs a process of exchanging the information for the recognition protocol with User 2. This exchanging process may comprise: providing to User 2 a first pair of parameters which may comprise an identifier of a FWD carried by User 1 and an anonymous identifier (such as nickname) of User 1; and getting from User 2 a response with a second pair of parameters which may comprise an identifier of a FWD carried by User 2 and an anonymous identifier (such as nickname) of User 2. From the perspective of User 1, a negotiation of an argot with User 2 may be made, for example, by sending an original argot and its order designed by User 1 to User 2; receiving a response with a confirmed argot from the second apparatus, which may comprise the original argot, a revised argot or a reply argot; sending an original presentation style of the confirmed argot designed by User 1 to User 2; and receiving a response with a confirmed presentation style from User 2, which may comprise the original presentation style or a revised presentation style. Thus it can be seen that User 2 may accept the argot as originally designed by User 1, or revise the received argot from User 1, or even design a new argot as a reply argot of the received argot from User 1. As shown in Fig.3, a second or more argots may be designed through a negotiation between User 1 and User 2.

Obviously, User 2 may initiate the procedure for generating the recognition protocol by receiving a request for the meeting from User 1 and sending an acknowledgment to User 1. Then

User 2 may perform a process of exchanging the information for designing the recognition protocol with User 1.

Fig.4 illustrates a recognition protocol generation procedure among multiple users. In Fig.4, User 1, as an inviter of the meeting initiates the procedure for generating the recognition protocol by multicasting a request for a meeting to a group of users; receiving respective acknowledgments from multiple other users; and multicasting respective anonymous identifiers of User 1 and the multiple anonymous IDs of acknowledged other users to all acknowledged users. Then User 1 performs a process of exchanging the information for the recognition protocol with the multiple users. This exchanging process may comprise: multicasting to the multiple users a first pair of parameters which may comprise an identifier of a FWD carried by User 1 and an anonymous identifier of User 1; and obtaining respective pairs of parameters from the multiple users through multicast, where the second pair of parameters may comprise an identifier of a FWD carried by its user and an anonymous identifier of the user. From the perspective of User 1, a negotiation of an argot with the multiple users may be made, for example, by multicasting an argot and its order designed by User 1 to the multiple other users with a first security parameter (such as a random r1 shown in Fig.4); receiving respective confirmations of the argot from the multiple users along with the first security parameter; multicasting a presentation style of the argot designed at User 1 to the multiple users along with a second security parameter (such as a random r2 shown in Fig.4); and receiving respective confirmations of the presentation style along from the multiple users with the first security parameter and the second security parameter. Using the first security parameter and the second security parameter can ensure the negotiation security that a user providing an acknowledgement is the user with whom User 1 wants to have the face-to-face meeting and that the confirmed presentation style corresponds to the confirmed argot. Similarly, a second or more argots may be designed through negotiations among multiple users, as shown in Fig.4.

Correspondingly, User 2, … , User n shown in Fig.4 may respectively initiate the procedure for generating the recognition protocol. Taking User 2 as an example, the procedure for generating the recognition protocol may be initiated by User 2 by receiving a request for a meeting from a User 1 through multicast. Then User 2 may perform a process of exchanging the information for the recognition protocol with other acknowledged users.

B. Protocol execution

Secure recognition for pervasive face-to-face social communications can be realized by executing the recognition protocol. When the users unknown with each other are in the watching distance, the MFA can warn its users with a sound and a specific show in FWD. When a user confirms starting recognition (e.g., through a voice control), the MFA starts to run the protocol by showing the first argot (or one part of argot if only one argot is designed) in FWD; the other user(s) got the notification of the first argot show through MFA communications, their FWDs respond with the second argot (or other parts of the argot) presenting in the same style in order to attract people to see with each other. If the argots match the design through the verification of both user and MFA, the MFA controls FWD to present next argot (or combined argots) at the same time based on the protocol design. This coordinated presentation continues and repeats until the unknown users can safely recognize with each other. For a simple example, the first argot is a blinking heart, the second one is two blinking hearts and the third one is two blinking hearts with an arrow passing through them.

V. SECURITY ANALYSIS AND DISCUSSION

The proposed approach provides a fashionable way to achieve secure recognition. We discuss its advantages with regard to security and other properties as below:

Fashionable: This approach provides a fashionable and secure method to help strangers in vicinity to meet with each other after digital communications and based on initially established trust. It offers recognition security by enhancing social fascination. This research opens a new horizon of fashionable security study. Our work is a primary attempt to transfer virtual security and anonymity into a live physical meeting by making use of the advance of fashionable technology. The purpose is to attract people to have a try.

Secure/safe: The security of this approach lies in the fact that the argots and their showing style and order are instantly designed by the users through a secure communication way via MANET. Other unrelated persons or parties can't get the details of the recognition protocol, thus they can't personate the protocol. The correctness of protocol execution is verified by both the users and their MFA. When User 2 find User 1 whose FWD shows the first argot, but User 2 suddenly doesn't like to meet with him/her before confirming to start the recognition, User 2 can withdraw the meeting by sending a cancel signal to User 1 with his/her MFA. In this case User 1 has no idea who is User 2 in crowds. In addition, we can synchronize the display of the first argot in order to provide equal security for all involved users. Particularly, the recognition protocol is generated based on secure communications in MANET. The communication messages are encrypted and can be only accessed by the authorized users, e.g., whose trust level exceeds a threshold. MANET communication threats (such as eavesdropping, man-in-middle attack and message dropping) can be overcome by applying trust evaluation based security management in data access control and network routing.

Privacy enhancement: the execution of the recognition protocol is based on anonymous identites used in the protocol design. There is no need for users to disclose their real identities. The secure recognition protocol ensures that they are the people who would like to meet.

Easy identification: By applying fashionable technology with the coordination of a mobile device and its application, it is easy for users to recognize with each other.

Low cost: Adopting the array of LED lights can reduce the cost of the proposed approach and its application system.

VI. PILOT STUDY

We performed a small-scale user study on the social acceptance of the SecGemini system with the proposed approach. We showed the low fidelity prototypes to a total of 23 university students (47.8 % female) in China. The participants ranged in age from 21-24 years. We showed the participants the SecGemini system design, its user interface design and the design for recognition protocol generation. We then asked them to provide their feedback on whether SecGemini is useful in a number of scenarios as described in Table I.

TABLE I. SCENARIOS

Scenarios
1) Right now you are at a shopping center alone, and a product you want is on sale under a condition that ´buy 3 pay 2´. However, you only need one. You want to ask your neighbor(s), whom you don't know, via your mobile phone whether he/she wants to share the discount with you. You would like to meet somebody face-to-face you are unknown for concrete discussions about purchase share after MANET chat. **Do you think SecGemini is helpful for you in this scenario?**
2) After shopping, you want to watch Avatar in a movie theater. The ticket price is 13.8e. However, if you buy a packet of 5 tickets, it will be 8.6e for each. You want to share the ticket packet cost with your neighbor(s) whom you don't know. You inquire and discuss whether he/she wants to share the discount with you via your mobile phone After MANET based instant social chatting, you think it is necessary to meet some guys you preferred to share a packet ticket cost. **Do you think SecGemini is helpful for you in this scenario?**
3) After the movie, a lot of people are leaving the theatre. You want to watch a figure skating competition quite far away. You would like to take a taxi and think about sharing a ride. You discuss with your neighbors nearby via your mobile phone whether he/she wants to share the ride with you. Of course, you need to meet some guys you preferred to share a ride face-to-face for further discussion or call a taxi together. **Do you think SecGemini is helpful for you in this scenario?**

Additionally, we conducted a survey to evaluate the perceived usefulness, perceived ease of use, interface, playfulness and user attitude in terms of SecGemini. The participants were asked to express their agreement on the statements listed in Table II. A 5-point Likert scale was applied. Our interview was designed based on the TAM model (Technology Acceptance Model) and its extension, which indicates that usefulness, ease of use and playfulness lead to user acceptance [15, 16]. This theory also indicates that good interface leads to better perceived usefulness and ease of use; playfulness causes better acceptance (attitude). Finally, we interviewed the participants in order to get their additional comments. After the test, each participant was awarded a small gift.

TABLE II. INTERVIEW STATEMENTS

Purpose	**Interview Statements**
Perceived ease of use	Q1: I think it is easy for me to recognize a person I don't know with the help SecGemini.
	Q2: I think It is easy for me to use SecGemini to design a recognition protocol for pervasive social communications.
	Q3: I think it is convenient for me using SecGemini to recognize a person I preferred to meet although I don't know him or her before.
Perceived Usefulness	Q4: SecGenimi can help me design my preferred recognition way for face-to-face meetings.
	Q5: SecGemini assists me to find a person in crowds in a safe way.
	Q6: SecGemini is a useful and helpful application.
Interface	Q7: LED display provides a fashionable and attractive way for meeting recognition.
	Q8: SecGemini has a good design on LED display.
	Q9: SecGemini provides a good user interface for recognition protocol design.
Playfulness	Q10: SecGemini is an interesting application.
	Q11: SecGemini is an exciting application.
	Q12: SecGemini provides a joyful way for secure social communications.
Attitude	Q13: I would like to use SecGemini.
	Q14: SecGemini is very cool.
	Q15: SecGemini offers me a way of outstanding in crowds.

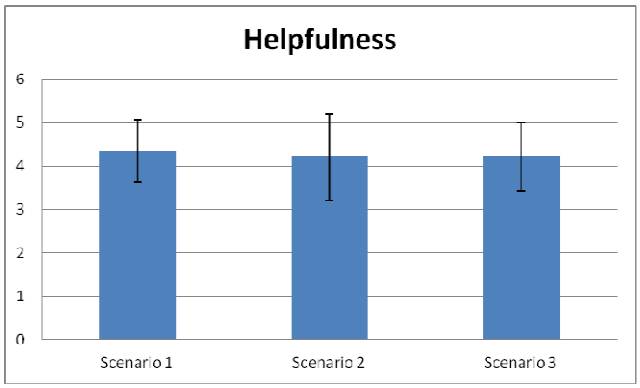

Figure 5: Helpfulness of SecGemini

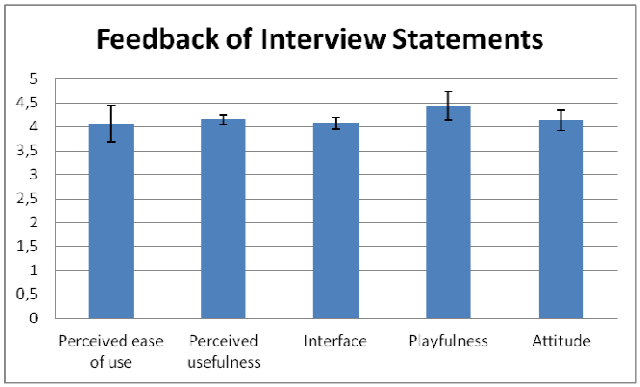

Figure 6: Feedback of interview statements

The result in Fig.5 showed that SecGemini is a very helpful application that can aid unknown people to recognize with each other for physical face-to-face contact after digital communications in a number of scenarios. SecGemini has satisfactory evaluation scores (over 4) with regard to perceived ease of use, perceived usefulness, interface, playfulness and user attitude, shown in Fig.6. We got the highest average scores (>4.4) in terms of playfulness. We notify that the participants thought SecGemini is an interesting, exciting and joyful application for secure social communications. Based on the TAM, we can conclude that SecGemini was well accepted by the participants. Regarding user interface design, the feedback is not as good as other items. We will further improve it by applying easily accepted technologies such as voice-control to guide MFA execution and improve user experience.

In addition, the user interview after user survey provided us interesting implications: a) We found other potential use cases of SecGemini such as dating, making friends, healthcare support for the elder, customer pick-up at the airport and potential business needs for a secure face-to-face meeting; b) The system should be improved for a better user experience on multi-person recognition. Some participants thought recognizing more than one person could be difficult at the same time; c) Some participants thought that the system has a big potential market. It can be extended for other purposes.

VII. Conclusion and Future Work

This paper proposed a novel approach to realize secure and fashionable recognition for pervasive face-to-face social communications based on MANET, local connectivity and fashionable technology. It contributes to the literature in three folds: a) it presents a novel fashionable approach for secure recognition in pervasive face-to-face social communications, thus provides a valuable extension for current Internet social networking and traditional social communications; b) it opens a new horizon of fashionable security study by integrating inter-disciplinary technologies, such as fashionable technology, wireless communication technology and mobile terminal technology, etc; c) the social acceptance of the proposed approach and its application system has been verified through a small scale pilot study based on the TAM model.

For future work, we will carry out further user studies based on a prototype system in order to improve the current design, investigate user needs and explore other potential applications.

Acknowledgments

The authors would like to thank Prof. Valtteri Niemi's valuable comments on the work described in this paper.

References

[1] A. Ahtiainen, et al. "Awareness networking in wireless environments: means of exchanging information", IEEE Vehicular Technology Magazine, 4(3), pp. 48-54, 2009.

[2] S. Seymour, Fashionable Technology: The Intersection of Design, Fashion, Science, and Technology, Springer Publishing Company, Incorporated, 2008

[3] Junction. Harvard MobiSocial Group. http://openjunction.org/

[4] MicroBlog, http://synrg.ee.duke.edu/microblog.html

[5] P. Stuedi, O. Riva, G. Alonso, "Demo abstract ad hoc social networking using MAND", retrieved from http://www.iks.inf.ethz.ch/publications/files/mobicom08_demo.pdf

[6] Z. Yan, Y. Chen, "AdContRep: a privacy enhanced reputation system for MANET content services", UIC2010, LNCS 6407, pp. 414-429, Xi'an, China, Oct. 2010.

[7] Z. Yan, Y. Chen, "AdChatRep: a reputation system for MANET chatting", SCI2011 in UbiComp2011, pp. 43-48, Beijing, China, Sept. 2011.

[8] N. Sawhney, C. Schmandt, "Nomadic radio: scaleable and contextual notification for wearable audio messaging", In Proceedings of the SIGCHI conference on Human factors in computing systems: the CHI is the limit (CHI '99). ACM, New York, NY, USA, pp. 96-103, 1999.

[9] M. Orth, R. Post, E. Cooper, "Fabric computing interfaces", In CHI 98 conference summary on Human factors in computing systems (CHI '98). ACM, New York, NY, USA, 331-332, 1998.

[10] L.E. Dunne, S.P. Ashdown, E. McDonald, "'Smart Systems': Wearable Integration of Intelligent Technology", In International Center for Excellence in Wearable Computing and Smart Fashion Products, Cottbus, Germany, Dec 9-11, 2002

[11] Love Jackets. http://www.5050ltd.com/loveRedux.php

[12] Microsoft Printing Dress. http://research.microsoft.com/pubs/149519/The_Printing_Dress.pdf

[13] Courtly bag. http://www.5050ltd.com/courtlyBags.php

[14] EDAG Light Car. http://www.automobilesreview.com/auto-news/geneva-motor-show-edag-light-car-sharing-concept-car/43410/

[15] F.D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology" MIS Quarterly, 13(3), pp. 319-340, 1989.

[16] V. Venkatesh, H. Bala, "Technology acceptance model 3 and a research agenda on interventions", Decision Sciences, 39(2), pp. 273–315, 2008.

[17] Oxford Dictionary. http://oxforddictionaries.com/definition/Gemini

[18] Z. Yan, P. Zhang, T. Virtanen, "Trust evaluation based security solution in ad hoc networks", The Seventh Nordic Workshop on Secure IT Systems, NordSec 2003, Gjovik, Norway, 10, 2003.

[19] Z. Yan, "Security via trusted communications", Book Chapter for Handbook on Communications and Information Security (ed. Peter Stavroulakis, Mark Stamp), Springer, pp. 719-746, 2010.

[20] S. Muller, S. Katzenbeisser, C. Eckert, "Distributed attribute-based encryption", In: Proceedings of the 11th Annual International Conference on Information Security and Cryptology, pp. 20–36, 2008.