Research on Information Dissemination Model for Social Networking Services

Ruzhi Xu[1], Heli Li[2], Changming Xing[3]

[12]School of Computer Science and Technology,Shandong University of Finance and Economics, Jinan, China

[3]School of Continue Education,Shandong University of Finance and Economics, Jinan, China

Email: lhl890104@163.com

Abstract

On the basis of characteristics of Social Networking Services (SNS), this paper modifies the traditional SEIR model by analyzing the influence of the information value and user behavior on information dissemination, and then the S-SEIR model on SNS is proposed. In S-SEIR model, the relevance of the information value and the rate of information audit are considered, and the influence of user behavior on he users number of each state also is researched. Simulation results show that: S-SEIR model can well simulate information dissemination process on social network.

Keywords

Social Networking Services (SNS); Information Dissemination; Information Value; User Behavior

Introduction

SNS (Social Networking Services) is a service which is oriented social network based on Web 2.0 technology. Nowadays, social networking applications have spread to all areas of society, and become a mass media tool with strong social influence. For example, companies can prove web brand promotion; government departments can collect their opinions and suggestions through the internet as well as internet users can share life information, just like shopping experience. All the convenience is owing to social network tools, such as Sina Weibo, the Renren network and Tianya Community etc. Social network has provided great facility by its quick, direct and wide range way of information dissemination. However, information dissemination on social network also is dispersive, massive and uncontrollable, which may lead to network public opinion crisis by spreading false or fake information. The “grab salt storm” caused by network rumors after 3.11 big earthquakes in Japan disrupted the normal order of life seriously. Research on propagation mechanism of information on social network can help us to make better use of the internet and analyze the mode of information dissemination.

Research on propagation mechanism of information began years ago, Kermark and Makendrick proposed the epidemic model of SIR with the application of dynamics method in 1927, which has provided an idea for the use of mathematical tools to study the propagation mechanism of infectious diseases. In 1991, Anderson and May added the Exposed state to SIR model and then built the SEIR model by analysis of the propagation patterns of a variety of infectious diseases. SEIR model can provide better description and simulation of the propagation mechanism of infectious diseases with multiple states. In recent years, a series of researches on propagation mechanism of information on network have been carried out using the methods of propagation mechanism of infectious diseases for references. For example, Yuan Hua and Chen Guoqing made extensions and amendments for SEIR model and established the E-SEIR model for e-mail viruses spread. The E-SEIR model discussed the influence of user behavior and anti-virus technology on E-mail virus diffusion. Hu Jieying and Zhang Wangcheng proposed the IM-SEIR model for Instant Messaging network to study the influence of probabilities of status transition on information dissemination.

On social network, which is based on social relations, the number of message insiders and information value has a significant influence on information dissemination. The more friends a user has the wider this piece of information disseminates. However, all the previous models assumed that the node passed messages to its neighbors in the same probability without consideration of the influence of information value and the number of "infected nodes" around every node. In recent social networks, users can choose to reject, browse or share it after receiving a message. So the existing mode of status transition does not be applied to social network. With the increase number of social network, user generally is active in

the multiple social networks simultaneously. The transmission of information between the different social networks also is frequent. The S-SEIR is proposed in this paper with the consideration of information value and user behavior through the analysis of information dissemination mode among different social networks. The S-SEIR model is adaptive to information dissemination characteristics on social network. The influence of correlation parameters on information dissemination is also discussed in this paper.

S-SEIR model build

Analysis of Propagation Mechanism of Information

With the increasing number of social networks, a user often is active in multiple social networks at the same time, which enhances the ability of proliferation information in social networks and the complexity of propagation mechanism of information. In social network, users read a published message from their friends and choose to share this message with the website or outside website with a certain probability. We consult paper of Yanchao Zhang to define users in social network as nodes and the relations between users as the edge between nodes. Information on social network spread along the edge between the nodes. The nodes of social network can be classified into four categories according to propagation mechanism of information, such as publication node, communication node, immune node and uninfected node. Publication node publishes the original information which needs to be audited by network administrators in social network. When the probability of information audit equals one, it means that this social network doesn't have audit mechanism. Communication node receives massage from its neighbor nodes and has the capacity to spread this message in or outside website. Immune node receives massage from its neighbors but without the ability to spread. Infected node does not receive or browse the information from its neighbor temporarily but has the opportunity to receive the message. Communication node and immune node collectively referred to as the infected nodes.

The transition of different state nodes in social network has relation with user behavior (such as browse, share in or outside website) and information value. The rules of information dissemination can be defined as follows:

(1) Information published from publication node needs to be audited by website administrator with a probability of φ.

(2) Information which has been audited is browsed by infected node with a probability of β.

(3) Infected node shares information to other social networks with a probability of δ_1, shares in the same social network with a probability of δ_2, and becomes immune node with a probability of δ_3.

Definition of Information Dissemination Model

We define the following notations according to the above analysis: N is the number of nodes in the network; S represents that node release information at time t and waiting for network administrators to audit; E represents the audited information waiting for neighbor nodes to browse; I represents the neighbor nodes browse information and becomes then infected nodes; R represents that information spreads into stagnation, or nodes become the immune nodes.

Considering the propagation mechanism of information on social network and learning from the SEIR model, the information dissemination model on SNS(S-SEIR) is shown in FIG.1:

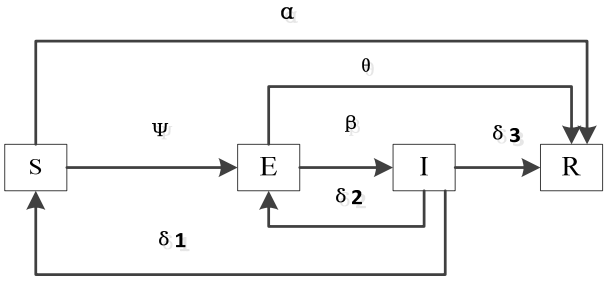


FIG.1 S-SEIR MODEL FOR INFORMATION DISSEMINATION

In FIG.1: the process of S—>E represents that information to be audited by network administrator after publication with a probability of Ψ; the process of $S—>R$ represents that the information is not approved and cannot spread with a probability of α; the process of $E—>R$ represents that there is no node browsing the approved information with a probability of θ; the process of $E—>I$ represents that node browses information and becomes infected with a probability of β; the process of $I—>S$ represents that node browses information and shares it outside this network with a probability of δ_1; the process of $I—>E$ represents that node browses information and shares it in the same network with a probability of δ_2; the process of $I—>R$ represents that node browses information and shares

then without sharing it with a probability of δ_3; for $\delta_1 + \delta_2 + \delta_3 = 1$.

We use *S(t), E(t), I(t)* and *R(t)* to denote the number of nodes respective in the state of Susceptible, Exposed, and Infected and Rejected at time t.

In S-SEIR model, *S(t)* is a continuous and derivable function at time *t*. There are $\varphi S(t)$ nodes receiving information per minute, $\alpha S(t)$ nodes cannot receive information and $\delta_1 I(t)$ a node browsing and sharing the information to the other sites, so at time $t + \triangle t$, Eq.1 is shown as follows:

$$S(t+\triangle t) - S(t) = \delta_1 I(t)\triangle t - \varphi S(t)\triangle t - \alpha S(t)\triangle t \quad (1)$$

From the above formula we obtain the following differential equations:

$$\frac{dS(t)}{dt} = -\varphi S - \alpha S + \delta_1 I \quad (2)$$

Similarly, other differential equations can be worked out and the corresponding differential equations of S-SEIR model are as follows:

$$\begin{cases} \frac{dS(t)}{dt} = -\varphi S - \alpha S + \delta_1 I \\ \frac{dE(t)}{dt} = \varphi S + \delta_2 I - (\beta + \theta)E \\ \frac{dI(t)}{dt} = \beta E - (\delta_1 + \delta_2 + \delta_3)I \\ \frac{dR(t)}{dt} = +\theta E + \alpha S + \delta_3 I \end{cases} \quad (3)$$

For the process of information publication to be audited is influenced by many factors, probability between two states cannot be showed with a constant number. Information value (V_0) affects the audit process. At the same time, the information has the characteristics of half-hearted so that the timeliness of the information value should also be taken into consideration. We use λ to denote characteristic scale factor of information timeliness. In order to build the S-SEIR model, we refer to paper of Xiaoyuan He to do the following definition:

Definition 1: transfer efficiency function $\varphi(t)$: the probability of information transfers from the publication state to audit state. $\varphi(t)$ refers to paper of Xiaoyuan He.

$$\varphi(t) = v_0 * e^{-\lambda t} \quad v_0 \in (0,1) \quad (4)$$

Model Simulation and Analysis of Impact Factors

Information dissemination on social network is influenced by many factors. In this section, we simulate and analyze several key factors affecting the process of information dissemination by changing different initial values. We analyze the information dissemination law in influence of different parameters by changing the parameter values.

Assuming that the number of users $N = 10000$, $S(0) = 10000$, $E(0) = 0$, $I(0) = 0$, $R(0) = 0$, in which time information has not started to spread.

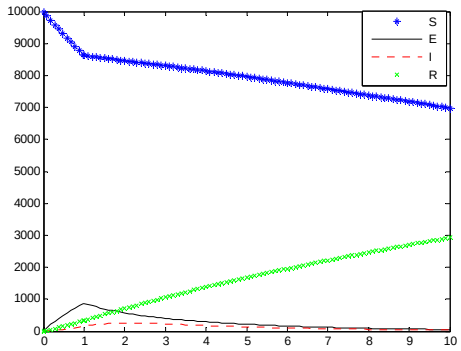
The Influence of Information Value v_0 on Information Dissemination

The unique nature of the information makes it difficult to evaluate. Information can be measured from multiple aspects, such as standard value, subjective value, actual value, etc. There is no unified measurement of information value. In this paper, we assume information value is a random number that between 0 and 1. Big number means high information value.

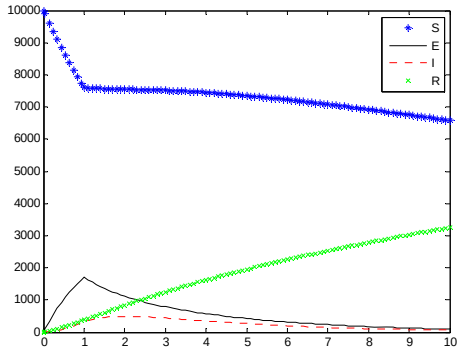
Reference to the parameter settings in paper of Hethcote H W., simulation uses parameters as follows: $\lambda = 4$, $\alpha = 0.03$, $\beta = 0.45$, $\theta = 0.1$, $\delta 1 = 0.4$, $\delta 2 = 0.4$, $\delta 3 = 0.2$, taking four sets values of information value (v_0): 0.12, 0.25, 0.5, and 0.75. The trend of *S(t)*, *E(t)*, *I(t)*, and *R(t)* as the time can be shown in FIG.2 .

As it can be seen from FIG.2, when v_0 is small, susceptible nodes reduce slowly and exposed nodes also increase slowly within a low range in the initial time of information dissemination. The above condition indicates that the probability of information audit is low. Conversely, exposed nodes show rapid growth trend in the initial time with v_0 increases, and then begin to decline until to 0 after a certain stage.

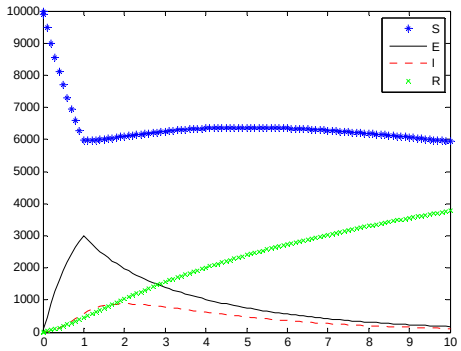
By observing the trend of *I(t)*, we draw a conclusion that the higher the value of v_0 is, more active the information will be in network and the higher degree trend the exposed nodes will reach. The maximum value of the number of exposed nodes increases as the value of v_0 increases within a certain range. The result indicates that information dissemination on social network is directly related to the ability to identify information of nodes when information is audited. The higher the value of information is, the more the number of exposed nodes reach.



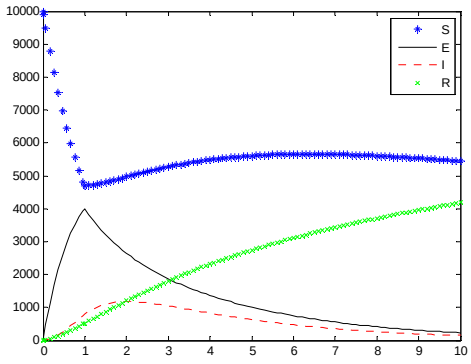
a v0=0.12



b v_0=0.25



c v_0=0.5



d v0=0.75

FIG.2 THE INFLUENCE OF INFORMATION VALUE ON INFORMATION DISSEMINATION

When the value of information is low (v_0 = 0.12), as is shown in figure a of FIG.2, the spread of the entire network is in "inactive" status and the information will eventually be lost in the “sea of information”. At the first time, the number of susceptible nodes decrease from 10000 to about 8500, and then the downward trend has a buffer with the increasing number of nodes which can share information. However, the number of exposed nodes only increases to 1000 and then begins to decline until close to 0, which indicates that the number of nodes which can receive approved information diminishes.

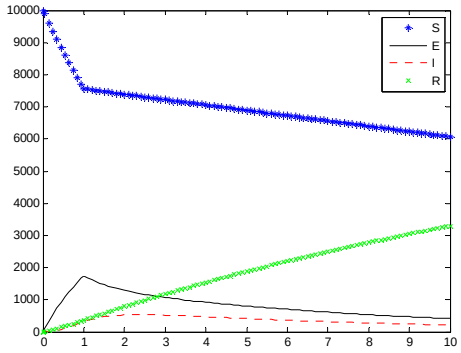
In FIG.2, the height of curve *I(t)* in figure d is higher than which in figure a, b and c, which indicates that the information has a high active degree in the network at this time. It means that more and more people have access to this information. However, facts show that if the number of information is overload, it will lead to information expansion. As a result, a part of users produce "immune" or even offensive to this information. So the rejected nodes will increase rapidly. For example, in the Renren network, if a user is sharing information so frequently that his/her friends may not have enough time to read or consider it as valueless information, and then his/her friends may shield this user or ignored the information.

Simulation results show that the transfer efficiency function which is determined by information value has influence on information audit. In a certain range, audit pass rate is positively correlated with information value. The bigger number the information value is, the more number exposed nodes reach, which is conducive to the spread of information, and the sooner the browsing nodes reach the maximum number.

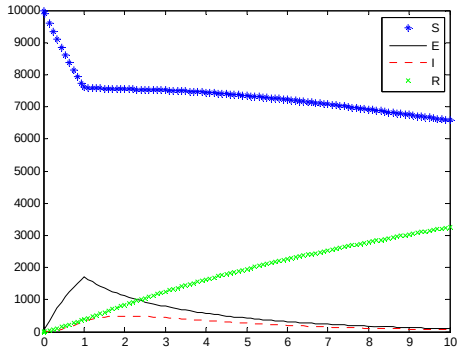
The Influence of User Behavior (δ1, δ2, δ3) on Information Dissemination

Simulation uses parameters as follows : v_0 = 0.25, λ = 4, α = 0.03, θ = 0.1, β = 0.45, taking four groups values of (δ_1, δ_2, δ_3): (0.1,0.8,0.1) , (0.4, 0.4, 0.2), (0.8,0.15,0.05) and (0.1,0.2,0.7) . The trend of S(t), E(t), I(t), and R(t) as the time can be shown in FIG. 3.

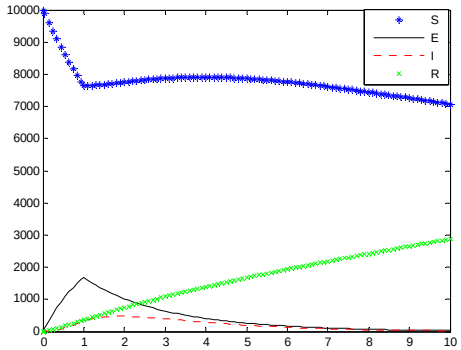
Simulation results of FIG. 3 show that user behavior affects the scale of information dissemination. Parameters δ_1 directly affects the number of publication nodes. In the previous figure a, b, and c, the number of publication nodes even increase in a short-term with the increment probability of sharing information outside website. However, the number of



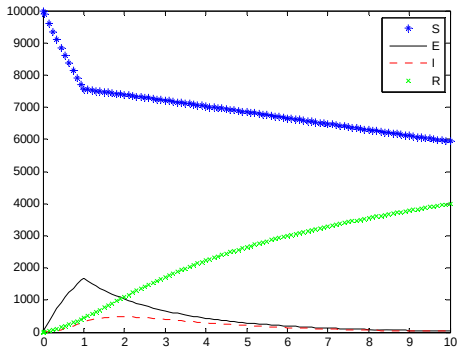
a δ_1=0.1, δ_2=0.8, δ_3=0.1



b δ_1=0.4, δ_2=0.4, δ_3=0.2



c δ_1=0.8, δ_2=0.15, δ_3=0.05



d δ_1=0.1, δ_2=0.2, δ_3=0.7

FIG. 3 THE INFLUENCE OF USER BEHAVIOR ON INFORMATION DISSEMINATION

publication nodes is inevitable to reduce with the large-scale spreading of information in the network.Parameter δ_3 has a certain impact on rejected nodes. By the previous figure c, b, and d, it can be seen that the changes in the value of the parameter δ_3 only slightly affect the number of rejected nodes. For social network, if most of users become uninterested in information and immune to it, then the information will be very difficult to continue to spread down, which is the so-called "a flash in the pan", or the message disappeared into the "sea of information".

Conclusions

Information dissemination on social network is affected by many factors. In this paper, we simulate dynamic of infectious diseases model and discuss the influence of information value and user behavior on information dissemination according to propagation mechanism on social network. The experiment results show that: within a certain range, information value is benefit to information audit when other parameters keep constant. The higher the value is the more broad scope of information spreads. The proportion of three ways of user behavior also affects information dissemination. The probability of sharing information is helpful for information dissemination. As there are many other uncertainties factors that affect the dissemination process, there is still improvement for this model. For example, the division of the information value also needs more empirical research to support, and the model should also consider the effect of network topology.

ACKNOWLEDGMENT

The project is funded by "Research on Marxism dissemination based on new media technology" (10JD710006) , which is a special mission project for Humanities and Social Sciences of Ministry of Education.

REFERENCES

Anderson R M, May R M. "Infectious diseases of humans dynamics and control." Oxford University Press, Oxford(1991).

Beretta E,Breda D. "Epidemic spreading of an SEIRS model in scale-free networks." Math Biosci Eng,vol.8,No.4 ,2011,pp.931-952.

EPHRAIM O. AGYINGI, DAVID S. ROSS, KARTHIK BATHENA "A model of the transmission dynamics of

leishmaniasis." Journal of Biological Systems, vol. 19,No.2,2011,pp.237-250.

Hethcote H W. "The mathematics of infectious disease." SIAM Review, vol.42, No.2,2000, pp.599-653.

Hua Yuan, Guoqing Chen "Simulation model of E-mail virus propagation and simulation of its influence factors." Computer Engineering and Design, vol.27,No.11,2006, pp.1914-1960.

Jieying Hu, Wangcheng Zhang "Research of Information dissemination model on Instant Message network." Science & Technology for China's Mass Media,No.1, 2012,pp.81-82.

Kieun Song;Sunjin Hwang;Yunsik Kim;Youngsik Kwak "The effects of social network properties on the acceleration of fashion information on the web." Multimedia Tools and Applications. 2012.

Mei Song, Wanbiao Ma, Yasuhiro Takeuchi. "Permanence of a delayed SIR epidemic model with density dependent birth rate." Journal of Computational and Applied Mathematics, vol. 201,No. 2,2007, pp. 389-394.

Sean Chester, Bruce M. Kapron, Gautam Srivastava, and S. Venkatesh "Complexity of social network anonymization." Social Network Analysis and Mining, 2012.

Yu Zhang and Tong Yu "Mining Trust Relationships from Online Social Networks," Journal of Computer Science and Technology, Vol. 27 ,No.3, 2012,pp. 492-505.

Xiaoyuan He, Xiaofeng Hu and Pi Luo "Modeling Method Research of Web Information Diffusion Based on Petri Net." Journal of System Simulation, Vol. 22 No. 3, 2010.

Yanchao Zhang, Yun Liu, Haifeng Zhang, Hui Cheng and Fei Xiong "The research of information dissemination model on online social network." Physica Sinica, 2011.

Zhien Ma, Wendi Wang and Yicang Zhou "Mathematical modeling study of the dynamics of infectious diseases." Science Press, Beijing, 2004.

Interior Design Framework Integrating Mixed Reality with the Multi-touch Tabletop Interface and Its Extension for Collocated and Remote Collaboration

Steven ZhiYing Zhou[*1,2], Jiaming Guo[3]

[*1,3]Dept. of Electrical Computer Engineering, National University of Singapore, Engineering 4, Singapore, 117542

[2]National University of Singapore (Suzhou) Research Institute, 377 Lin Quan Street, Suzhou Industrial Park, Jiang Su, People's Republic of China, 215123

[*1,2]elezzy@nus.edu.sg; [3]guo.jiaming@ nus.edu.sg

Abstract

This paper presents an interior design framework based on multi-touch table, which allows multiple users to work on. The information visualization is enhanced by 3D animation shown in a vertical display using the mixed-reality technology. Furthermore, the framework is extended to allow both collocated and remote collaboration, which is enabled by the combining of separated viewed mode and extended view mode. Moreover, a "sliding pass" touch gesture is designed for the extended mode, and a user avatar system is developed to solve the user awareness problem.

Keywords

CSCW; Mixed Reality; Multi-touch Table

Introduction

We are interested in both co-located collaboration [Hornecker 2008, Tobiasz 2009, Sadurai 2009, Cao 2010] and remote collaboration [Arroyo 2010, Tuddenham 2007, Perron 2006, Coldefy 2007] between groups using the large-scale multi-touch tabletop. Large multi-touch tabletop wall and displays is one of the most popular approaches devised for computer-supported cooperative work (CSCW) [Grudin 1994], since it offers intuitive interfaces for the team members to manipulate both shared and individual instances of data representations concurrently.

One of the most important factors in the implementation of multi-touch tabletop system for CSCW is the information visualization method. One of the related outstanding projects is Lark, presented by Matthew [Tobiasz 2009], an information visualization system for hierarchical data that supports co-located collaboration by integrating a representation of the information visualization pipeline in the shared workspace. However, many of the currently developed multi-touch tabletops confine its information visualization technology within 2D, which makes it difficult for workers to complete their work purely via the tabletop, especially for some design jobs. There are also some 3D visualization methods for multi-touch tabletop, for example, the FI3D project presented by Yu [Yu 2010]. However, most of them only support for single user instead of collaboration.

Besides, the physical constraint of most multi-touch tabletops may also bring problems for collocated collaboration. A few recent projects have investigated the possibility of physically extending the LCD based multi-touch tabletops by combining a few of LCD panels together to increase the physical size of the system such that more users can work together [Kim 2009, Wang 2008]. However, there are also some limitations with these approaches. For example, the boundaries of each LCD display explicitly divide the whole surface into small territories, which is not quite helpful for enforcing the integrity of the whole workspace. The boundaries may also cause problems when user's touch operations are across the boundaries.

As for remote collaboration, several recent projects have investigated the possibility of building linked connections among geographically-separated tabletops to create a shared. For example, VideoWhiteboard [Tang 1991] and Clearboard [Ishii 1992] provided shared drawing surfaces to let users at different location simultaneously sketch objects. Escritoire [Ashdown 2005], RemotedDT [Esenther

2006] and ViCAT/TIDL [Hutterer 2006] provide remote collaborators with another shared workspace with movable interactive virtual objects so that remote collaborators can arrange the objects at different location but still get the same experience of collocated collaboration. Although Distributed Tabletops [Tang 2006] have improved the previous work and virtual objects can be moved and reoriented by any collaborators to suit different seating arrangement, the whole shared workspace is still relatively static to collocated users. User operations could only happen on individual objects. In reality, this approach may not always be suitable for remote collaborations because the collaborations task may be divided into different sub tasks and each collocated group can choose to focus on a certain sub-area of the whole shared workspace. Thus, user operations should be implemented to support local view manipulation.

Another important factor to ensure the effectiveness of remote collaboration is user awareness. This often means to provide different kinds of cues or indicators to remind a user of the physical existence of the remote collaborators. Embodiment of collaborator is an intuitive way to represent collaborator's activities in the reference space and to enforce user awareness. Recent researches show a high interest in video-based embodiments of collaborators. In Tang's VideoArms [Tang 2006], the image of collaborators' arms is captured digitally and redrawn at the remote location to mimic collaborators' body gesture. Several other projects [Pauchet 2007, Izadi 2007, Tang 2010] also adopt this method to enable remote user awareness. These researches all assume that only one participant at each workstation uses the remote collaboration systems. However, this may not always be true in reality. For example, in a design team that includes many designers located at different cities, one designer may occupy a single tabletop at one location whereas a few designers at another location may want to share a tabletop together. Tang's research [Tang 2010] also shows that attributing workspace activity to a remote collaborator is difficult when there is more than one remote collaborator and participants are sometimes confused about whom the hand belongs to when all collaborators have the same-side configuration.

In this article, we present a conceptual interior design frame-work – multi-touch mixed reality (MTMR) which integrates the usage of mixed reality (MR) [Milgram 1994] with the multi-touch tabletop interface, providing 3D spatial information to the designers. Moreover, the proposed MTMR system is extended to a networked collaborative interior design system with the client-server architecture in order to support both efficient collocated and remote collaborations. Besides, two modes of view – Separated View Mode (SVM) and Extended View Mode (EVM) – are implemented. The SVM is aimed to address the physical constraint problem in co-located collaboration and the EVM is aimed to provide independent views of shared workspace in remote collaboration. We also develop a user avatar system to improve user awareness in remote collaboration.

Interior Design Framework

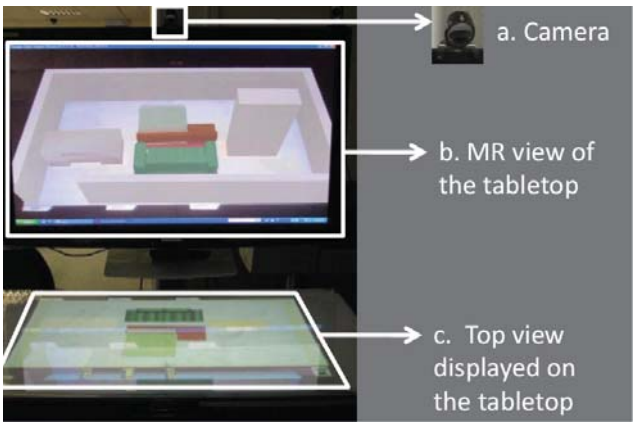


FIG. 1 OVERVIEW OF THE DESIGNER SIDE

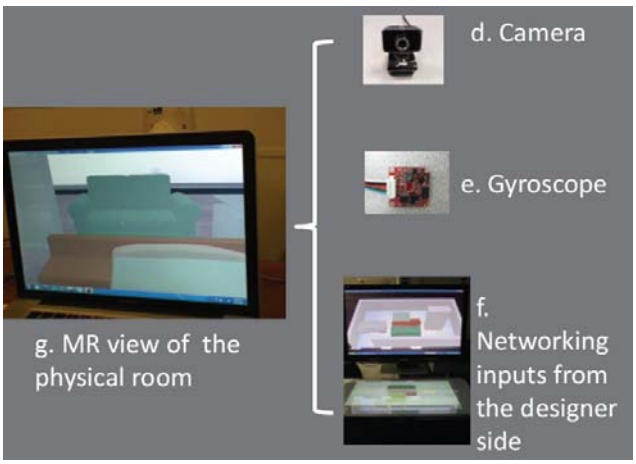


FIG. 2 OVERVIEW OF THE CLIENT SIDE

The MTMR design framework is divided into designer side (Fig. 1) and client side (Fig. 2). At the designer side, designers interact with the tabletop, and carry out design work on the top view of their design. Vertical display reflects the real-time 3D simulation of design perspective view, which provides designer better vision of their design. At client side, client resides at his/her remote home and receives designers' control messages. Client's computer will be able to interpret these control messages to construct the virtual view of the design output. The design output

which includes furniture and their orientation is combined with the camera-captured video to establish MR view. Detailed interactions at both sides are discussed in following sections.

Designer Side

The major parts of the designer side are the tabletop interface (Item *c* in Fig. 1) and the vertical display (Item *b* in Fig. 1). The tabletop interface works as both input and output device, while the vertical display shows the corresponding 3D MR view. The tabletop interface provides a multi-user multi-touch supported platform for collaborative work. Since it is convenient for the designers to carry out furniture arrangement work on 2D top views, the tabletop interface is chosen to provide the interactive environment. However, a top view alone may not provide 3D spatial information for the designers, thus the 3D MR view on the vertical screen can deliver complementary information.

Since the top view is limited in 2D, a 3D MR view of the design can provide important complementary information to the designers to review their work. The position, orientation and size of the virtual furniture contained in the tabletop display are passed through network to the computer connecting the vertical screen, where they are interpreted to construct and register 3D virtual furniture models. A camera mounted on top of the vertical screen (Item *a* in Fig. 1) captures live video of the design work going on the tabletop. This real-time video is mixed with the constructed 3D furniture models in such a way that these furniture models in the MR view align with their position, rotation and size seen in the top view. The final output is these 3D models appearing to stand on the tabletop (Fig. 4 and item *b* in Fig. 1). What is more, since the designers' operation is also captured in the video, they may look at the vertical screen while operating on the tabletop. This extra feature is expected to make the designers have the feeling that they are interacting with the 3D models directly, which would narrow the gap between the physical world and the virtual world.

Fig. 3 shows the GUI of the application at the designer side. Besides, several traditional touch gestures (translation, rotation, scaling) are implemented for touch operations. In summary, the application at the designer side supports functionalities in the following three aspects:

- Furniture model manipulation: The system provides the Model Catalogue and Trash Bin widgets for creating/deleting furniture models. Two one-finger gestures can be recognized for moving/sliding the models around inside the shared workspace and three two-finger gestures can be recognized for translating, rotating and scaling the models
- Workspace manipulation: In the shared workspace, a one-finger gesture can be used to move the entire workspace to any direction inside local workspace view. Three two-finger gestures can be used to translate, rotate and scale the entire workspace. In addition, a switchable mini-map widget is also designed for showing the area of the workspace that is visible in the local workspace.
- Two switchable collaboration modes: The system also provides both separated view mode (SVM) and extended view mode (SVM) to facilitate different collaboration needs which are switchable using the View Mode Switch widget. More details about these two modes will be provided later when collocated collaboration and remote collaboration on the MTMR system are introduced.

FIG. 3 THE DESIGN OF GUI AT THE DESIGNER SIDE

The development tool used here is MXR software development kit (SDK) which is the product of MXR Corporation (http://www.mxrcorp.com/). This SDK is built on the Torque Game Engine Advanced which is a popular commercial 3D game engine. Thus, the 3D virtual world simulation is mainly handled by TGEA source code. The modification is mainly done to facilitate creating MR effects.

The first part of 3D simulation implementation is importing 3D models for use (See Fig. 4 for example).

Furniture models used in this project are from the model database of another interior design software.

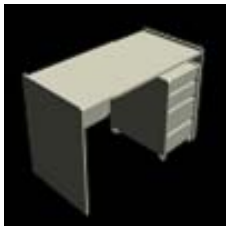


FIG. 4 PERSPECTIVE VIEW OF A FURNITURE MODEL SAMPLE

Since TEGA has its own static 3D data format dts, and the available models are in 3ds format, the first step of importing them is transferring the format using related software tool. When creating furniture models, properties such as size, location and orientation are retrieved from data sent from designer side to configure them.

The second part of 3D simulation implementation is collaboration.

FIG. 5 CALIBRATION INTERFACE

FIG. 6 CALIBRATION MARKER

Fig. 5 above shows the calibration interface. To finish the collaboration, a marker with pattern shown in Fig. 6 needs to be captured into the green ring. Then the centre of the marker will be labeled as origin (0, 0, 0), *x-y* plane is aligned with the marker's surface plane, and z axis point from the origin upwards.

For vertical display at designer side, marker is shown in the center of tabletop graphical interface. After collaboration, the marker is removed and the tabletop surface will be *x-y* plane. Thus, when *z* value of furniture model's coordinate is set to 0, the furniture will appear to be held on the tabletop as shown below.

For client side 3D simulation, the marker is placed at the center of the room floor such that the floor forms *x-y* plan. In this way, furniture models will appear to stand on the floor of the physical room.

After the coordinate system is set up, it is rather easy to match the top view design on tabletop with the 3D simulation at both vertical display and client side.

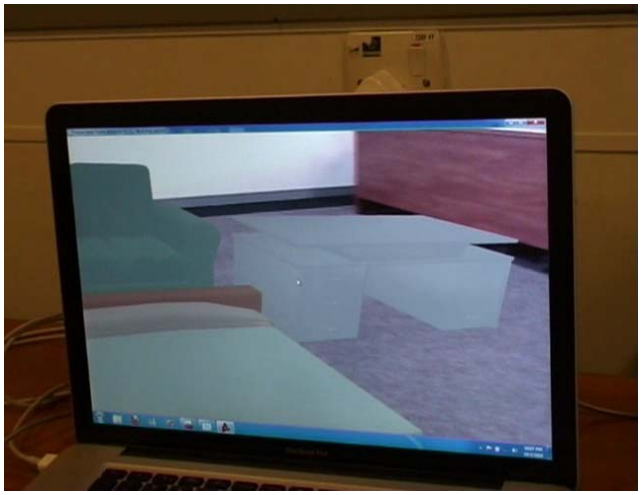
Client Side

At the client side, the implementation of MR (Item *g* in Fig. 2) is similar to the 3D MR view at the designer side. The client resides at his/her remote room and receives designers' control messages. These control messages, including the existence, position, orientation and size of the virtual furniture in the design plan, are passed to the client's computer through network (Item *f* in Fig. 2) to construct and update the client's MR view in real time. A camera (Item *d* in Fig. 2) captures live video of the client's room. This video is augmented with life-size virtual furniture models constructed according to the control messages. The difference is that at the designer side, the camera is fixed, while at the client side, the client is supposed to view the furniture layout from different perspectives with a rotatable camera. To match the perspectives of the virtual world and the physical world, an extra gyroscope (Item *e* in Fig. 2) is attached to the camera to measure its orientation. The measurement data is used to adjust the view point in the virtual world. Fig. 7 shows the same design (as in the top view in Fig. 1) viewed from three different perspectives at the client side by rotating the camera from left to right.

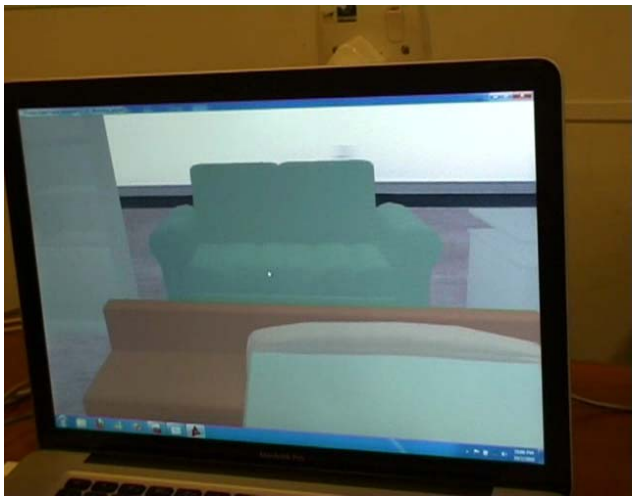
Collocated Collaboration and Remote Collaboration Using MTMR System

In the case of interior design, when the room is large, it needs more than one designer to collaborate. When the team of designers is large, the MTMR system with only one tabletop is not enough. It is important for the MTMR system to support distributed tabletops for collocated collaboration when the team of designers are in the same place and remote collaboration when they locate in different places. As mentioned in the introduction, the limited physical size is often a reason to cause unpleasant experience when too many collocated collaborators crowd around the same tabletop. As for remote collaboration, user awareness

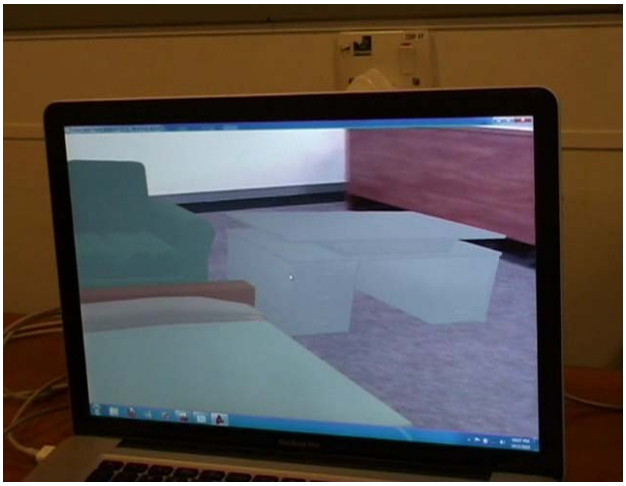
is an important factor to ensure the effectiveness of the collaboration.



(A)



(B)



(C)

FIG. 7 (A)-(C) SHOW THE DESIGN AT THE CLIENT SIDE FROM THREE DIFFERENT PERSPECTIVES BY ROTATING THE CAMERA FROM LEFT TO TOP

Motivated by these problems, the proposed MTMR system is extended to a networked collaborative interior design system with the client-server architecture to allow efficient collocated and remote collaborations. The system provides an independent shared workspace for each collaboration task.

Network Architecture

Fig. 8 shows the architecture of the networked MTMR system. The overall system consists of a single server application named "SAPP" running on an "always-on" PC with known IP address and several instances of the client application named "CAPP" running on several workstations located at different places. At each workstation, the client application runs on the multi-touch tabletop and the augmented 3D application named "3DAPP" runs on the vertical display.

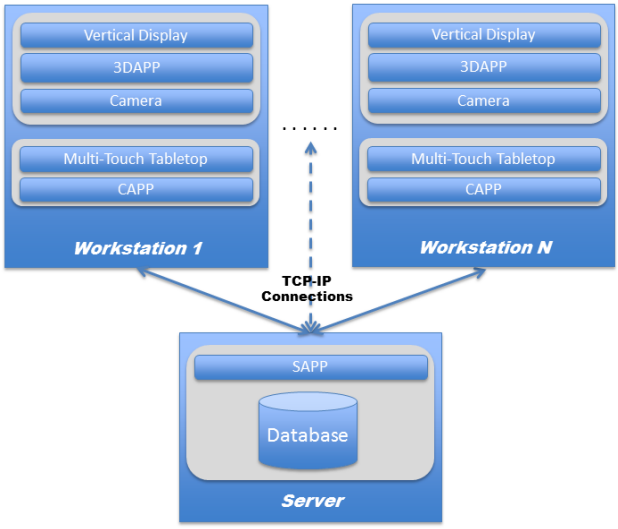


FIG. 8 NETWORK ARCHITECTURE OF THE DISTRIBUTED MTMR SYSTEM

In this networked system, the server application is designed as a data synchronization manager and communication coordinator. It is mainly responsible for storing project information, keeping track of session information and directing messages among different clients. For each project, it maintains an individual file keeping records of the project meta-data and project scene data. Meta-data includes information that will help server application initialize a new session. Project scene data mainly consists of a list of data structure that represents all objects in the scene. The major attributes that are used to describe each object are object index, type, position, rotation and scale.

Separated View Mode and Extended View Mode

(A) TABLE 1

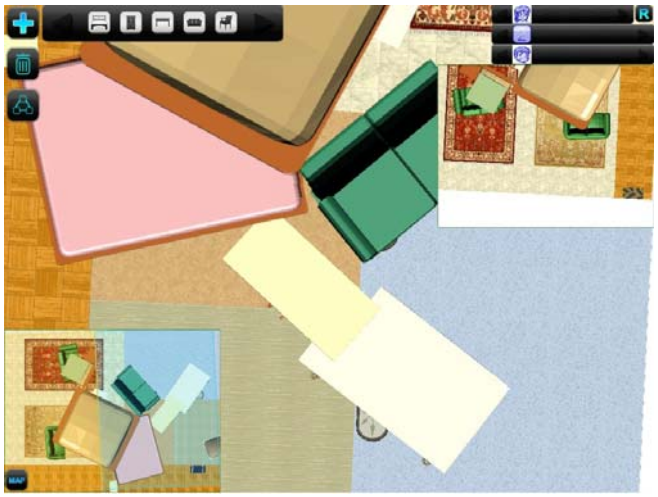
(B) TABLE 2

FIG. 9 A SCREENSHOT OF THE CLIENT APPLICATION RUNNING IN SVM

The system also provides two different collaboration modes to facilitate different collaboration needs, which is enabled switchable by the View Mode Switch widget.

In Separated View Mode (SVM) (See Fig. 9), each multi-touch tabletop can have its own view range of the shared workspace. Workspace manipulation on tabletop A does not affect the view range of tabletop B. But furniture model manipulation on tabletop A is synchronized with the shared workspace and is reflected at other tabletops. In order to keep the integrity of the furniture models in the shared workspace, each model can only be manipulated by the users at the same tabletop. This mode is suitable for most remote collaboration tasks.

In Extended View Mode (EVM) (See Fig. 10), two multi-touch tabletops are virtually concatenated together so that a larger single multi-touch tabletop surface can be constructed just by putting the two tabletops side by side. Both workspace manipulations and furniture model manipulations are synchronized with each other. Workspace and all objects inside the shared workspace can be manipulated by users at different tabletops at the same time. This mode is the most suitable for overcoming the physical constraint of collocated collaboration.



(A) TABLE 1

(B) TABLE 2

FIG. 10 A SCREENSHOT OF THE CLIENT APPLICATION RUNNING IN EVM

A New Touch Gesture for Collaboration in EVM

Assume that a team of designers are collaborating in EVM, and one designer working on one tabletop wants to pass an object to another designer working on another tabletop. Traditional touch gestures cannot achieve this. Thus, a sliding gesture is implemented to improve user experience when they are collaborating in EVM.

We achieve this in three steps. Firstly, the simple

translation gesture is recognized, and the speed of the touched item is estimated. Whenever a translation happens on the item, the intrinsic speed is estimated by dividing the displacement with time difference. The new estimated speed is calculated by taking the average of the intrinsic speed and the previous estimated speed. Secondly, when the finger is removed from the item, the estimated speed is then used as the start value of the sliding animation. The animation is played to indicate the sliding operation and the speed is reduced in a quadratic curve. Finally, when the object is passing through the boundary of one tabletop and entering another, the server application plays data synchronization, simulating that the object is seamlessly passing between two virtually concatenated tabletops.

User Avatar System

FIG. 11 A SCREENSHOT OF THE USER AVATAR SYSTEM AT TABLE 1

In order to solve the user awareness problems in remote collaboration, a user avatar system enabling following functionality is implemented (See Fig. 11):

- A list widget for showing the icons of all workstations that have joined in the current project.
- A list widget for displaying the avatars of all participants that are registered on a selected workstation.
- A mini view widget for displaying the remote workspace view of a selected remote workstation.
- It is able to display a user's avatar on the object that the user is currently touching on.
- It provides a short animation to enlarge the user avatar of an object that a user touches in the mini view widget.

The main benefit of the user avatar system is that it allows a user easily recognizes the existence and manipulation of another remote user without having any interfering effects on this user's own manipulation.

Example User-Case Scenario

MTMR system is a conceptual design framework that utilizes an enhanced information visualization method (3D MR) to improve users' experience on indoor spatial information rendering, which is believed to be helpful for interior design. Besides, the application at client side provides an opportunity for the client to view the temporary design easily and intuitionally.

Moreover, the extension of the MTMR system for collocated and remote collaboration is aimed to solve the problems such physical limitation of single tabletop and remote user awareness which are common in currently developed multi-touch tabletop based CSCW projects.

To show the use of our system, we describe a scenario in which a large designer team, whose members are located in different places, is carrying out an interior design for a remote client. We will explain how our design features are used as we follow how the designer team carries out the design work.

Communication between Designer and Client

Suppose that a designer team works in Singapore, carrying out an interior design job for a client in China. The client needs the design team to send the detailed information about the room, such as its height, width and shape. Using the proposed MTMR system, members of the designer team can do the job by co-located collaboration or remote collaboration on the distributed tabletop (introduced later). After the initial design is completed, the design team sends the client the information about the design, and then, the client can use the proposed application at the client side to view the vivid live video of the current design on his laptop, which offers the client an opportunity to give instant and helpful feedback.

3D MR

During the design, the designer may need to take into account the effects of the furniture's height played on the room. Without the vertical display in our system, it is difficult for the designers to achieve this because

most tabletop displays can only provide 2D information (the height and the width). Although by adding a rotation gesture and the relative object rendering with respect to the slant and tilt direction, it is possible to implement 3D simulation in the tabletop display, this newly added gesture will make impossible the collocated collaboration on a single tabletop or distributed tabletop in EVM mode. This is because certain designer's manipulation using the slant and tilt gesture will always distract others who share the same workspace from their work.

Thus, the vertical display and its 3D MR simulation is a reasonable way for the designer to view the 3D spatial information of their design. It won't lead to any distraction to others, since the rendering of the perspective view has no effects on the manipulation workspace.

Collocated and Remote Collaboration

Suppose that there is the designer team includes six designers, four in Singapore are in charge of placing the furniture; another two in Hong Kong are in charge of paining the floor. The four in Singapore need two tabletops, one displays the eastern part of the room and the other western part. These two tabletops are in EVM which enlarges the workspace to allow them to work concurrently. If one designer finds that the furniture object which is under manipulation of his colleague, is also suitable for the space he is in charge of, he can ask his colleague to pass the object via the sliding gesture.

The two in Hong Kong and in charge of painting floor only need one tabletop. Since the placing of furniture has great effect on the final outlook of the floor, they need to remotely collaborate with the four in Singapore. However, instead of EVM, SVM is activated in the tabletop because they need a whole view of room to efficiently paint the floor. Sometimes, the manipulation of the furniture may distract their painting. When this happens, the user avatar system provides them with information about who are manipulating the distracting furniture so that they can call the corresponding designer in Singapore to stop for a while via the speech communication system.

Conclusions

We have developed MTMR, a conceptual interior design framework which integrates MR with the multi-touch tabletop interface, to provide an intuitive and efficient interface for collaborative design and an augmented 3D view to users at the same time. Moreover, we have extended the MTMR system for both collocated and remote collaboration.

ACKNOWLEDGMENT

The authors would like to acknowledge the financial support from the National University of Singapore (Suzhou) Research Institute under the grant number **NUSRI R-2012-N-002**.

REFERENCES

Ashdown, M. and Robinson, P. E. "A Personal Projected Display." IEEE MultiMedia, vol.12, no. 1 ,pp. 34-42, 2005.

Arroyo, E., Righi, V., Blat, J. and Ardaiz, O.. "Distributed Multi-touch Virtual Collaborative Environments." Proceedings of the International Symposium on Collaborative Technologies and Systems, May 17-May 21, Barcelona, Spain, 2010.

Cao, X., Lindley, S. E., Helmes, J. and Sellen, A.. "Telling the Whole Story: Anticipation, Inspiration and Reputation in a Field Deployment of Telltable." Proceedings of the ACM Conference on Computer Supported Cooperative Work, Feb. 6-Feb. 10, Savannah, GA, USA, 2010.

Coldefy, F. and Lous-dit-Picard, S.. "DigiTable: an Interactive Multiuser Table for Collocated and Remote Collaboration Enabling Remote Gesture Visualization." Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Jun. 17-Jun. 22, Minneapolis, MN, USA, 2007.

Esenther, A. and Ryall, K. "RemoteDT: Support for Multi-Site Table Collaboration." Proceedings of Int. Conf. Collaboration Technologies, 2006.

Grudin, J.. "Computer-Supported Cooperative Work: History and focus." Computer, vol. 27, no. 5, pp. 19-26 1994.

Hornecker, E., Marshall, P., Dalton, N. S. and Rogers, Y.. "Collaboration and Interference: Awareness with Mice or Touch Input." Proceedings of the ACM Conference on Computer Supported Cooperative Work, Nov. 8-Nov. 12, San Diego, CA, USA, 2008.

Hutterer, P., Close, B. S. and Thomas, B. H. "Supporting Mixed Presence Groupware in Tabletop Applications." Proceedings of TABLETOP, 2006.

Ishii, H. and Kobayashi, M.. "ClearBoard: a seamless medium for shared drawing and conversation with eye contact." Proceedings of ACM SIGCHI Conference on Human Factors in Computing Systems, Jun. 7-Jun. 7, Monterey, California, USA, 1992.

Izadi, S., Agarawal, A., Criminisi, A. and Winn, J., Blake, A. and Fitzgibbon, A.. "C-Slate: exploring remote collaboration on horizontal multi-touch surfaces." Proceedings of IEEE Tabletop, 2007.

Kim, M., Cho, Y. and Park, K. S.. "Design and Development of a Distributed Tabletop System using EBITA Framework." Proceedings of the 4th International Conference on the Ubiquitous Information Technologies & Applications, (2009) Dec. 20-Dec. 22, 2009.

Milgram, P. and Kishino, F.. "A Taxonomy of Mixed Reality Visual Displays." IEICE Transactions on Information Systems, vol. 77, no. 12, 1994.

Pauchet, A. et al. "Mutual awareness in collocated and distant collaborative tasks using shared interfaces." Proceedings of INTERACT, 2007.

Perron, R. and Laborie, F.. "Augmented Tabletops, an Incentive for Distributed Collaboration." Proceedings of the First Annual IEEE International Workshop on Horizontal Interactive Human-Computer System, Jan. 5-Jan. 7, Toulouse, France, 2006.

Sadurai, S., Kitamura, Y., Subramanian, S. and Kishino, F.. "A Visibility Control System for Collaborative Digital Table." Journal of Personal and Ubiquitous Computing. Vol. 13, no. 8, pp. 619-632, 2009.

Tang, A., Pahud, M. and Inkpen, K.. "Three's company: understanding communication channels in three-way distributed collaboration." Proceedings of CSCW, 2010.

Tang, A., Neustaedter, C. and Greenberg, S. "VideoArms: embodiments for mixed presence groupware." Proceedings of British-HCI, 2006.

Tang, J. C. and Minneman, S.. "VideoWhiteboard: video shadows to support remote collaboration." Proceedings of ACM SIGCHI Conference on Human Factors in Computing Systems, Apr. 28-May 2, New Orleans, Louisiana, USA, 1991

Tobiasz, M., Isenberg, P. and Carpendale, S.. "Coordinating Co-located Collaboration with Information Visualization." IEEE Transactions on Visualization and Computer Graphics, vol. 15, no. 6, pp. 1065-1072, 2009.

Tuddenham, P. and Robinson, P.. "Distributed Tabletops: Supporting Remote and Mixed-Presence Tabletop Collaboration." Proceedings of the Second Annual IEEE International Workshop on Horizontal Interactive Human-Computer System, Oct. 19-Oct. 26, 2007.

Wang, X. and Maurer, F.. "Tabletop AgilePlanner: A Tabletop-Based Project Planning Tool for Agile Software Development Teams." Proceedings of 3rd IEEE International Workshop on Horizontal Interactive Human Computer Systems, Oct. 1-Oct. 3, 2008.

Yu, L., Svetachov, P., Isenbery, P., Everts, M. H. and Isenberg, T.. "FI3D: Direct-Touch Interaction for the Exploration of 3D Scientific Visualization Spaces." IEEE Transactions on Visualization and Computer Graphics, vol. 16, no. 6, pp. 1613-1622, 2010.

EMA as a Physical Method for Extracting Secret Data from Mobile Phones

[1]Driss Aboulkassimi, [2]Jacques Fournier, [1]Laurent Freund, [2]Bruno Robisson and [2]Assia Tria

[1]Département "Systèmes et Architectures Sécurisés", Ecole Nationale Supérieure des Mines de Saint Etienne, France

[2]Laboratoire "Systèmes et Architectures Sécurisés", CEA-LETI Minatec, France

[1]lastname@emse.fr; [2]firstname.lastname@cea.fr

Abstract

Today's mobile phones have diverse functions and features such as calling, Internet surfing, game playing, banking, storage of personal and professional data. Given that these devices run an increasing amount of added value applications, the number of the software attacks on them has drastically increased. This study shows that the mobile platforms, especially their constituent components running security-related applications, could also be good targets for hardware attacks where sensitive data stored in the mobile phone are extracted using physical methods. This article discusses the feasibility and presents the results of a technique involving the extraction of secret keys by using the Electromagnetic Analysis (EMA) on software implementations of the Advanced Encryption Standard (AES) running on Java mobile phones. Obtaining these keys can be used for forensic purposes or to recover encrypted data that could have been enciphered using such keys.

Keywords

AES; Electromagnetic Attacks; Java Mobile Phones; Secret Keys.

Introduction

Until recently, security was not one of the priorities of mobile phone designers, except for some specific products principally intended to certain categories of business users and governments. Apart from the IMEI (International Mobile Equipment Identity) or SIM (Subscriber Identity Module) lock protections, the security was based principally on the smart card (SIM) for some features like network authentication, key derivations or for storing the mobile phone contacts of the user. With the advent of multi applicative smart phones, there is a growing need for security: for applications handling personal or professional data and information about the user's activities; for uses such as Internet shopping, game playing and banking. It has become crucial to ensure a consistent level of security in all the constituents of the mobile terminal in order to close all the possible attack routes.

The study presented in this article focuses on the analysis of hardware techniques that can be used to extract sensitive data from modern mobile phones. We target the secret key used in encryption algorithms like the AES that can be used for encrypting data or for network authentications. In this paper, we describe how a technique, called ElectroMagnetic Analysis (EMA), used on smart card like devices, can be adapted to a Java-based smart phone in order to extract information about the AES key used in some "off-the-shelf" implementations.

In this paper, we first provide a review of data extraction techniques that have already been presented for mobile devices. Then we present the AES and the Correlation Electro-Magnetic Analysis (CEMA) on AES. The mobile Java platform used in our experiments is discussed in order to explain in which conditions the analysis was done. Next, the experimental set-up, technical difficulties met and proposed solutions are explained. Spectral Density based Approach (SDA) and Template based Resynchronisation Approach (TRA), two approaches implemented to "remove" the misalignments obtained on the measurements, are described and compared. Two AES implementations are then analysed using CEMA and the results are presented. Finally countermeasures are discussed in order to protect software cryptographic libraries against such attacks.

Previous Research & Existing Techniques

Modern mobile phones like those called smart phones are multi applicative, multi function devices that increasingly manipulate and store personal and professional data. Unfortunately for user privacy and fortunately for forensic investigation, to extract these sensitive data, several invasive, semi-invasive and non-invasive physical techniques exist and can be adapted to wireless platforms.

An example of an invasive attack is the dump of the

Flash memory of the mobile device. This technique first consists in physically extracting the Flash memory (M. Breeuwsma, 2007), and then reading its content by using a Flash memory chip programmer. One of the disadvantages of this technique is that it can be destructive. This technique also requires a software driver and the right memory content interpretation (K. Kim, 2007). Neither is trivial when the data-sheets of the Flash memories are not available.

Flash memory dumps can also be done via the JTAG port (Joint Test Action Group, IEEE Std 1149.1, 2001). In this case it can be classified as a semi-invasive attack. The JTAG interface is a hardware module added to a device for testing analogue and digital integrated circuits. It can also be used for debugging software. In (M. Breeuwsma, 2005), the authors show that the JTAG port access can be exploited to extract data from the Flash memory of mobile devices. Related works are reported in (S. Willassen, 2005), where the authors managed to dump the Flash memory of an "old" mobile phone.

To test the efficiency of this technique on a smart phone, a commercial probe from Amontec (JTAGKEY) was chosen for its compatibility with the ARM11 processor of our targeted mobile device. The probe was connected to the JTAG port through a PCB (Printed Circuit Board) as illustrated in Fig. 1, that was designed specially to be adapted to the physical board's constraints of our mobile device.

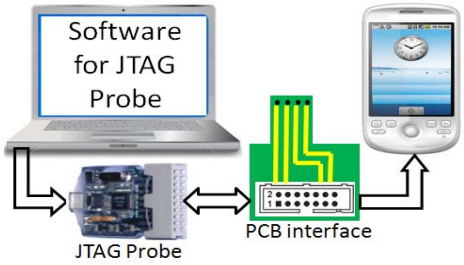


FIG. 1. JTAG PORT ACCESS ON MOBILE PHONE

Unfortunately, the "logical" connection could not be established between the probe and the processor. The performed manipulations allowed us to conclude that JTAG port access of the smart phone under test is protected (disabled) by the manufacturer. This shows that reading the phone's contents via the JTAG port is not as trivial as it was on older generations of mobile phones and that further investigations, which may lead to more invasive setups, would be needed to successfully implement this attack. To preserve the integrity of the mobile device that may be used in forensics proceedings, another physical technique for extracting secrets data was investigated.

This non-invasive technique is based on a category of attacks called "side channel attacks" (P.C. Kocher, 1996). This technique allows the extraction of sensitive data like the secret keys of encryption algorithms (for example the Advanced Encryption Standard - AES). It exploits the fact that some physical attributes such as the power consumption, the electromagnetic radiation or the duration of computation of the chip depend on its internal computations. Successful secret key extractions using the electromagnetic channel (a technique called Electro-Magnetic Analysis or EMA) have been reported in (K. Gandolfi, 2001) on smart cards and in (C. Gebotys, 2005) on a Java-based PDA (Personal Digital Assistant). To our best knowledge, this approach has not yet been tested on modern mobile phones and in this respect, we studied the efficiency of an EMA on a software AES running on the high-speed processor of a smart phone. The success of our attack is reported in section III. Given that on such platforms the AES can be used for server authentication protocols (like in PSK TLS) or to encrypt confidential information, the recovery of such secret keys can be useful for forensic and data recovery purposes, but can also put the user's privacy at stake if performed by a malevolent attacker.

Description of the AES and Principle of Electromagnetic Analysis

Side channel analysis, as a non-invasive method for extracting data like secret encryption keys, exploits the fact that some physical values such as the power consumption, the electromagnetic radiation or the duration of computation of the chip depends on its internal computations. It is of particular concern since it does not destroy the physical integrity of the circuit and it can be quickly mounted with cheap equipment. The main requirement for carrying such an analysis is that the attacker has to be able to measure several times (in practice, from hundreds to millions), the same cryptographic elementary operation with different operands. These measurements have to be done in the same conditions. In particular, the elementary operations have to be performed at the same time. In our analysis, we opted for the EM waves as physical characteristic to study because we could locally target the relevant chip. Using a characteristic like power consumption would have been tricky in the sense that there are too many sources of parasitic noise on a complex system board like that of a mobile phone.

Description of the AES

The AES is an iterative algorithm that performs encryption on data blocks of 128 bits as input and output, using key sizes of 128, 192 or 256 bits respectively in 10, 12 or 14 rounds according to the size of the key. The algorithm includes two separate processes: one for the key scheduling to derive the round keys from the initial secret key and the second one for data encryption. Decryption is also divided into two separated processes: the first one is for the inverse key scheduling and the second one is for the data decryption. In this paper, key sizes of 128 bits are used and we consider the encryption scenario. The structure of the AES-128 (referring to the AES using keys of 128 bits) is illustrated in Fig. 2. Each round key Ki is derived iteratively from the previous one as described in (NIST, 2001).

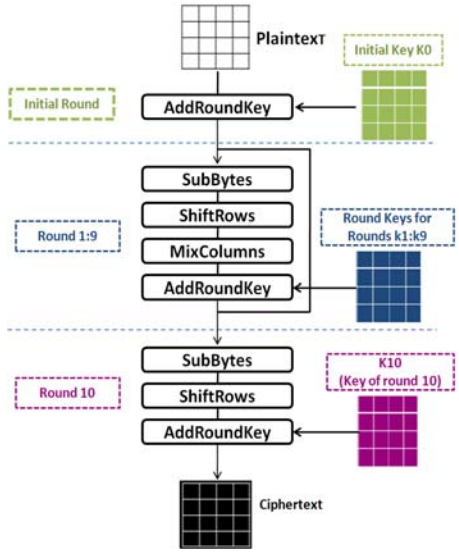


FIG. 2. AES ALGORITHM

AES Softwar Implementation

Lots of AES software implementations exist and, to develop a cryptographic Java Micro Edition (Java ME) application (since it is the system used on our device under test), developers have the choice among:

- Developing their own implementation according to the cryptographic algorithm specifications.
- Using a commercial or an open source implementation, e.g. the Bouncy Castle library .
- Using a manufacturer's implementation, e.g. the JSR 177.

The first approach requires development work without the help of any external commercial library. Consequently, neither a virus, nor a Trojan is possible. The second one has the advantage of using all the knowledge of an expert company or community. But royalties must sometimes be paid or open source license rules have to be followed. The last one seems to be the best solution in terms of performance and security because the manufacturer is responsible for the implementation. However the JSR 177 is today only available for very few mobile phones.

In this paper we only investigated about the first and the second scenarios, using a 32-bit processor as targeted hardware platform. In order to optimize the code size and the performances of our own AES implementation, we chose to combine the SubBytes and ShiftRows operations into one operation, implemented as a lookup table of 8 x 32 bits. In the Bouncy Castle library, the "fast algorithm" version of the AES has been chosen: three of the AES operations (SubBytes, ShiftRows and MixColumns) are grouped into one operation using a lookup table of 8 x 32 bits.

Principle of Correlation Electro Magnetic Analysis

The acquisition set-up is illustrated in Fig. 3. It consists of an EM probe, an oscilloscope, the trigger mechanism described below and a PC. The acquisition of the EM curves is performed as follows.

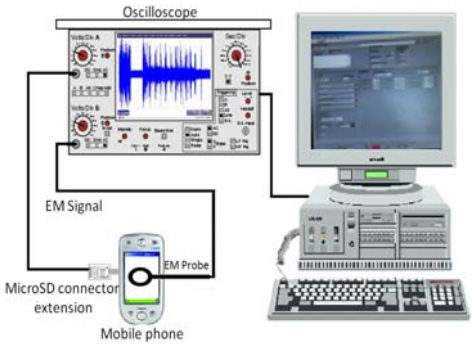


FIG. 3. EXPERIMENTAL SET-UP

The mobile phone executes, in a stand-alone mode, a large number (typically hundreds) of AES encryptions. At the beginning of each encryption, a signal is triggered as explained in a later section. This signal launches the oscilloscope which acquires the EM curves measured through the EM probe.

A "sleep time" is introduced between two encryptions. This sleep time provides the necessary time for the oscilloscope to send the EM curves to the PC that stores them.

Correlation Electromagnetic Analysis (CEMA) is an EMA technique based on the statistical analysis of the correlation between the EM waves measured during an AES computation and the data processed (secret key). An approach to CEMA would consist in the

following steps:

- **Step1.** Measure the EM emanation. Let d be a set of D different plain texts for encryption d = (d_1 ,...,d_D). To each di is associated an EM curve t_i = ($t_{i,1}$,..., $t_{i,T}$) of T points each.
- **Step1b.** (optional) Modify mathematically the EM curves to obtain a set of t'_i = ($t'_{i,1}$,..., $t'_{i,T'}$) of T' points.
- **Step2.** Choose intermediate results of the executed algorithm f(d, k) with k being a small part of the key (also called "guessed key"). Let K be the set of all the possible values of k.
- **Step3**. Compute some intermediate values $v_{i,j}$ = $f(d_i, k_j)$ for i = 1, …,D and j = 1, …,K.
- **Step4.** Correlate the intermediate values with the EM waves. Hamming-distance or Hamming-weight models (E. Brier, 2004) consumption models may be used.
- **Step5.** Compare the measured EM values T (or the modified ones T') with these theoretical EM values. The result is a matrix R of size K x T.

The line index of the highest values of the R is the index of the key actually used (correct key guess). The straightforward place for an attacker to find the secret key is during the first round (DPA Book, 2007). Therefore, the intermediate values used in Step3 are computed according to the SubBytes outputs' Hamming weights.

Setting up the EM Acquisition Bench

Unlike EMA on "classical" targets such as smart cards, we have faced two major difficulties. The first one is the choice of the experimental set-up that is slightly different from those classically described in the literature for smart cards. The second one is due to the complexity of the software running on the smart phone. As the AES is running inside a Java Virtual Machine (JVM), which is a complex software, the elementary operations of the AES were not always executed at the same time (i.e. they were not synchronized). The main requirement for EMA was not thus readily met. In order to overcome this difficulty, two techniques have been tested and compared. Before performing CEMA on a mobile phone, several points have to be first considered for the experimental set-up:

- Choice of the AES software implementation.
- Generation of a trigger signal to synchronize the software on the mobile phone with our acquisition platform.
- Choice of the EM probe.
- Physically accessing the phone's chip inside the mobile phone.
- Software for automatic acquisitions of EM traces.

The first point has been discussed previously. Concerning the forth point, the battery has been removed and the power supply was provided through wire connections. We shall now detail the three remaining points.

Trigger Signal

In order to signal to the oscilloscope that the EM wave acquisition can begin, a trigger signal, synchronized with the software running on the smart phone, has to be generated. This signal must be sent just before starting the AES encryption. Since all Java ME applications are executed in a sand box, we cannot have direct input/output accesses during the AES execution itself. The external inputs/outputs on a mobile phone are the screen, the loudspeaker and connections like http/SMS/Bluetooth and file access. The best solution we found that guaranteed an acceptable response delay was to access to a file stored on an external micro-SD card.

To facilitate the access to the micro-SD's PINS (Fig. 4), a special extension for the micro-SD's connector has been manufactured Our tests showed that in order to obtain a trigger signal, a simple open file instruction (Algorithm in Fig. 5) can be used to activate the PIN 2 of the micro-SD interface thus providing a deterministic trigger signal.

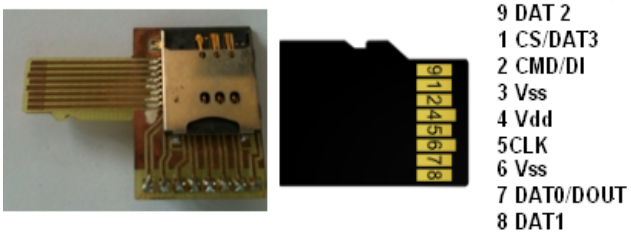


FIG. 4. MICRO SD CARD PINOUTS

```
public void trigger() {
   try {
         FileConnection file;
         file=Connector.open(file:///SDCard/myfile.txt);
         fclose(file); }  }
```

FIG. 5. ALGORITHM FOR MICRO SD TRIGGER

Choice of EM Probe

The choice of the probe is crucial to perform a successful analysis based on EM measurements (E. De Mulder, 2010). Some EM probes used to perform CEMA on smart card like devices are described by Mounier et al. in (B. Mounier, 2012). We first considered using some of the latter probes. However, as such probes (with diameters ranging from 70µm to 250µm) were too small with respect to the phone's die size (≈1cm²), we had problems finding a proper position for the probe and making sure that we were measuring the relevant EM waves. We rapidly concluded that such probes were not appropriate for performing EM analysis on the phone's chip. From there we focused on probes large enough to "cover" the phone's chip. (C.K.Kim, 2008) describes the successful implementation of an EMA on an FPGA executing the ARIA algorithm (which is a fast symmetric key algorithm derived from the AES) using a "commercial" probe which has a diameter of 25mm and a bandwidth of 30MHz to 3GHz. For setting up our analysis on the phone's chip, we chose the same commercial probe equipped with a pre amplifier.

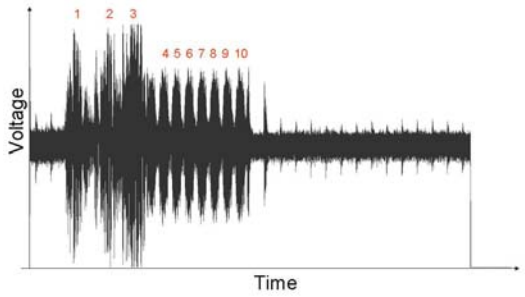


FIG. 6. EM CURVES CAPTURED BY HOMEMADE PROBE

Measurements were made on the phone's chip during the execution of our software AES using the chosen commercial probe. As shown in Fig. 7, the execution of the ten rounds of the AES could clearly be seen with a high signal to noise ratio.

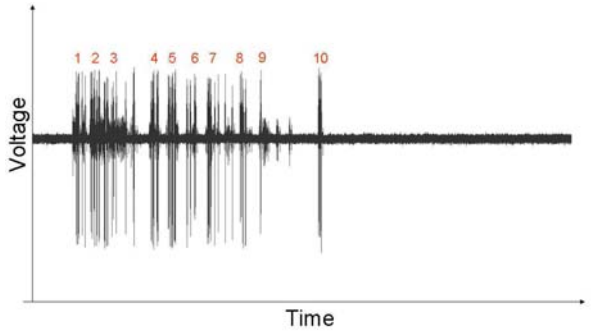


FIG. 7. EM CURVES CAPTURED BY COMMERCIAL PROBE

In order to illustrate the efficiency, and added value, of this commercial probe in our set-up, we performed the same measurements but this time using a home made probe (a solenoid coil of ten loops of diameter 1cm). A measurement made with the homemade probe is illustrated in Fig. 6 showing that a lower signal to noise ratio was obtained compared to when the commercial probe was used.

Automatic Acquisition Sequence

Table I sums up the characteristics and parameters of the equipment and conditions used during the acquisition phase. The 16 bytes of the text to encrypt are chosen by randomly changing only 1 byte, according to the attacked secret key byte. Other bytes are kept fixed in order to reduce measurement noise.

TABLE I ACQUISITION CONDITIONS AND EQUIPMENTS CHARACTERISTICS

Equipment	Characteristics
Target Circuit	RISC Processor, 32bits Clock frequency: 370Mhz
Oscilloscope	Lecroy 3Ghz, resolution 200 s/div Sampling frequency 1GSamples/s
EM Probe	30MHz-30GHz bandwidth
PC	Xeon 2.67 Ghz, RAM 12Go
Soft scope Driving	Labview interface Ethernet connection with oscilloscope
Plain texts to Encrypt	2000 random plain text changing only one of 16 the bytes

Analyzing the measured EM Curves: Handling the Misalignments

The following initial observations highlight the difficulty of interpreting the electromagnetic field of the execution of a Java program on a mobile phone. Several explanations can be derived from the Fig. 8 that describes the workflow from editing a Java program to executing it on the processor. Java is a compiled language.

Compilation techniques do a static analysis of the source code in order to reduce the execution time. Moreover, Java is intended to let application developers "write once, run anywhere". For that purpose, the Java Virtual Machine (JVM) interprets the Java byte code, issued from the compilation step. The portability is performed by the availability of a JVM for classical computer architectures. In parallel to the Java interpreter process, the execution of the just-in-time (JIT) compiler process raises concerns described later. The haphazard phenomena that appear on mobile phones are usually not present in the case of the more deterministic Java (smart) cards.

First, the "Garbage Collector" has been identified as

one of these phenomena. The garbage collector consists in automatically cleaning the memory. The problem is that this process is launched in an uncontrolled way from a user point of view. Therefore, some EM curves are not exploitable (like in Fig. 9) because the signal is indistinguishable from noise. As the garbage collection consumes power and thus increases the electromagnetic radiation of the chip, the curves where the "Garbage Collector" is triggered are discriminated simply by computing their temporal average. The average of such curves appears to be 20% higher than those curves without garbage collector.

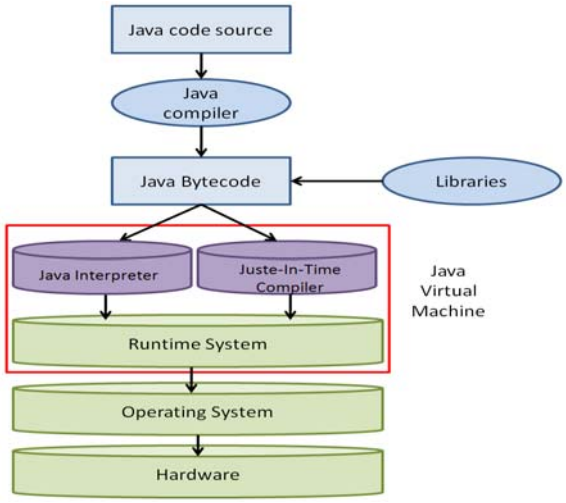


FIG. 8. JAVA PROGRAMME EXECUTION

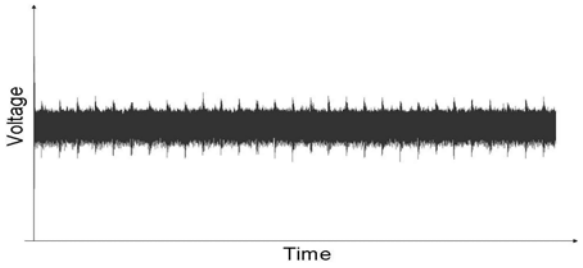


FIG. 9. CURVE ACQUIRED DURING GARBAGE COLLECTION: NO AES VISIBLE

Second, the "Just-In-Time-Compiler" was identified as a possible problem. Indeed, the "Just In Time Compiler" is an optimization executed by the virtual machine to dynamically speed-up the multiple execution of a set of instructions. It consists in compiling the instructions on the fly during their first execution. This phenomenon is visible in Fig. 7 where the first round is longer than the following ones.

These two issues introduce EM curves' misalignments. The temporal shift (Fig. 10) among EM curves varies between 0 and 110 ms and may impact the CEMA.

Third, the Java operating system is multi-threaded, consequently daemon processes could introduce additional delays. In order to find a workaround to all the EM curves' misalignments issues, a timing synchronization methodology based on the detection of the beginning of the first round was investigated. The statistical analysis failed due to temporal shift between instructions within the round itself. To solve this problem two successful solutions are described namely SDA and TRA.

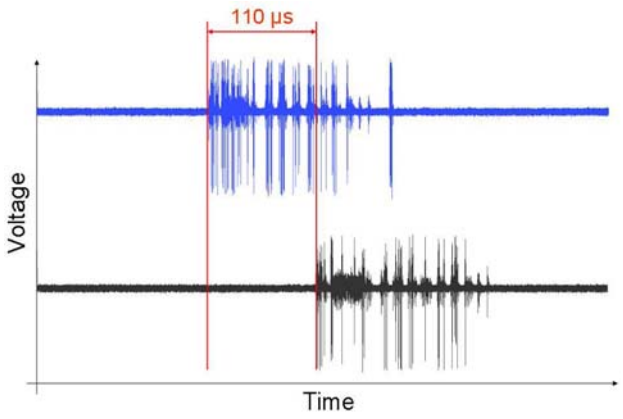


FIG. 10. MISALIGNMENT BETWEEN EM TRACES

EMA with Spectral Density Based Approach:

Such misalignments could also be due to random delays that could be introduced as a countermeasure in AES hardware and software implementations. Several techniques in signal processing exist and could be exploited, such as in (Jasper G, 2011) and (N. Homma, 2006). Another synchronization technique consists in performing the correlation not in the temporal domain but in the frequency domain. This technique is based on the fact that the Power Spectrum Density (PSD) of a "shifted signal" and the PSD of a "not shifted signal" are the same. In (C.C. Tiu, 2005), the authors show the efficiency of such an EM analysis on a very high speed embedded system. In (Zhang, P., 2009), the authors show that even if random delays are introduced, the CEMA attack in the frequency domain is still efficient on a program executed without a virtual machine on a processor running at less than 12 MHz. Unlike previous researches, our paper shows the efficiency of CEMA on a AES Java program executed on a virtual machine on a high speed circuit (400MHz). (O. Schimmel, 2010) exploits the simulation of the power consumption by using CPA (Correlation Power Analysis). Their analysis in the frequency domain allowed them to find the secret key.

We have performed on our own implementation of the AES, the EM attack in the frequency (or spectral) domain. It consists in computing the PSD of the EM curves in the optional **step 1b** described previously (with the Hamming Weight as the model for the EM

signal). The result of the correlation is represented in Fig. 11 for one key-byte where the correlation factor of the correct key guess is distinguishable from the others. With this result, the efficiency of the CEMA attack has been shown on our AES J2ME implementation with resynchronisations performed in the spectral domain.

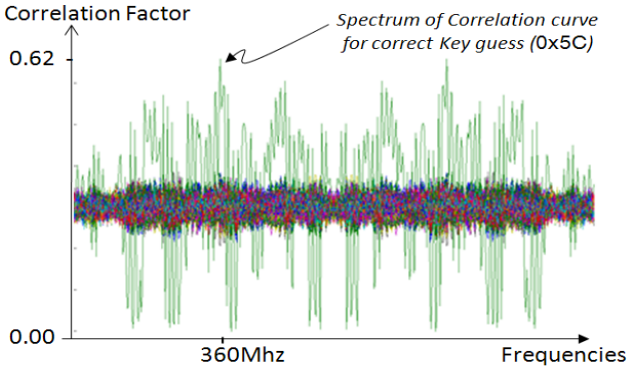


FIG. 11. CORRELATION RESULT FOR ONE KEY BYTE IN THE FREQUENCY DOMAIN

EMA Using Template Resynchronisation Approach:

During our experiments, we observed that the EM signature corresponding to the SubBytes parts of our AES implementation were very similar. It can be explained by the fact that the SubBytes are implemented as a LUT (Look-Up-Table), i.e. an access to an array, and that this access emits a characteristic EM signature. We use this property in order to resynchronize our curves.

The proposed approach consists first in developing a piece of code of a LUT access. Its signature is then measured and defined as the reference pattern (or "template") (Fig. 12).

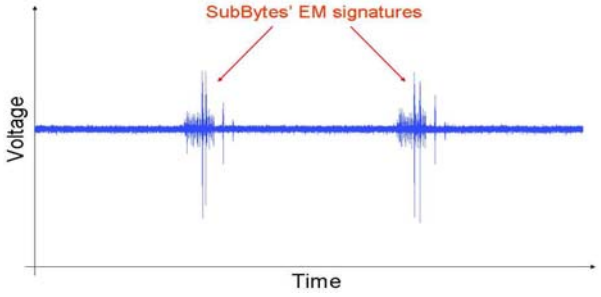


FIG. 12. ZOOM ON SUBBYTES SIGNATURES

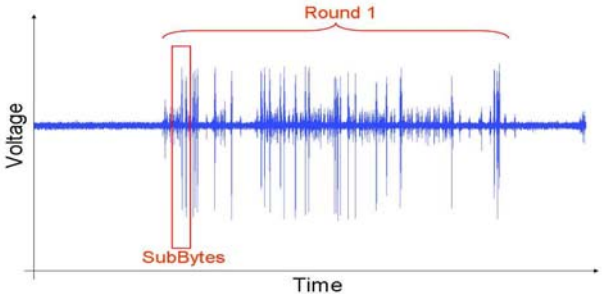


FIG. 13. IDENTIFICATION OF EM SIGNATURE OF LUT ACCESS

Then, the optional **step 1b** described previously has consisted in extracting the pieces of curves similar to such a template in the whole set of the raw EM curves (as represented in Fig. 13).

The sliding window technique correlation has been used to extract these pieces of curves. Thanks to this technique, each byte of the key used by our own implementation of the AES has been recovered with only 256 EM curves (Fig. 14). The correlation factor is about 72%. Using more curves increases the contrast between the correlation curve for the correct guess compared to the other 255 wrong guesses (Fig. 14).

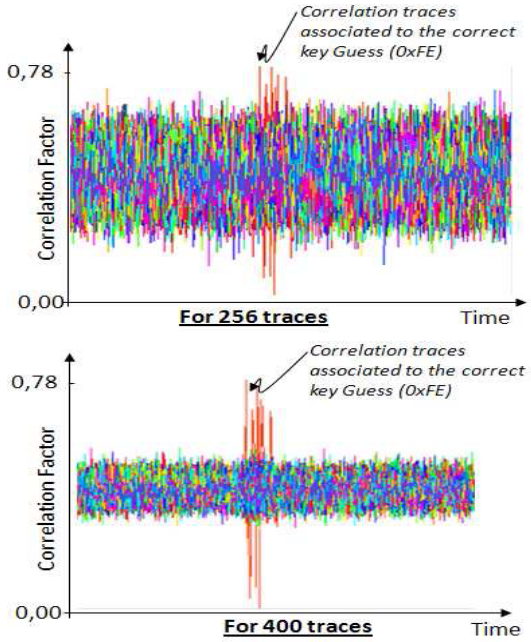


FIG. 14. CORRELATION RESULT FOR ONE KEY BYTE

Comparison between SDA and TRA

With the previously described results, it has been proven that SDA and TRA are efficient techniques to manage desynchronisation introduced by a mobile phone's JVM during an EMA. The differences between both methodologies are summarized in Table II. As shown in this table, the SDA needs to select curves without "Garbage Collector" while the selection is automatically realized by the SubBytes operation identification technique of the TRA. An important point to note is that the first one requires four times more curves than the second one. On the opposite, the second one needs to build a template (i.e. the signature of a particular operation) before performing the attack. The real disadvantage in the first one is the number of samples (millions) compared to the second one (hundreds). Consequently more computer resources are necessary to perform the DSP and to apply the CEMA.

TABLE II : COMPARISON BETWEEN THE TWO PROPOSED APPROACHES

	SDA	TRA
Number of curves	20800	4096
Sorting curves	yes	no
Number of samples/curve	1 Million	600
Computing time	28h	1h

We showed that CEMA on our AES implementation on a mobile phone is also possible despite "irregularities" introduced by the JVM. By comparing both proposed approaches, the fastest has been identified. The next interesting challenge was to attack a 'commercially used' AES implementation using TRA.

EMA on Bouncy Castle's AES

Bouncy Castle is an open source lightweight library used by Java applications that need cryptography. It supports standards like Transport Layer Security, Public Key Infrastructure and Certificate Management Protocol. In our experiments, we targeted the AES library in Bouncy Castle. To begin, a first acquisition was made. Visually, only 6 "patterns" were seen, which at first seemed in contradiction with our implementation (Fig. 15) where the 10 AES rounds could be seen. The challenge was to find the key without any knowledge of the source code. We made the hypothesis that the implementation of the SubBytes could be the same as on a 32-bit processor architecture, i.e. an 8x32 LUT. Therefore the template previously defined for our implementation, when using the TRA method, could be used for the identification of the Bouncy Castle's SubBytes function operation.

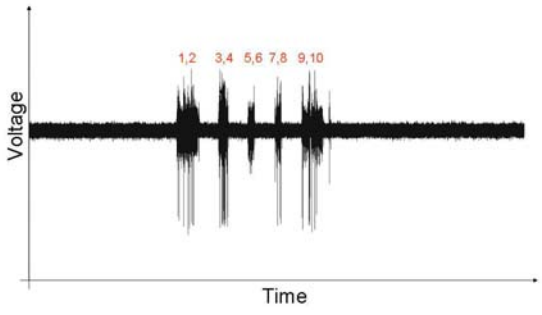


FIG. 15. EM CURVE OF BOUNCY CASTLE'S AES

Processings have been made in this manner and it has been discovered that the CEMA succeeds with only 250 curves (for each byte of key) with a correlation factor of 77% (Fig. 16).

This study demonstrates that an EM attack is possible without knowing the source code of an external library. This kind of attack could be dangerous because it could be generalized to all Java AES implementations on a 32-bit processor where a 8 x 32 LUT is used to implement the SubBytes operation.

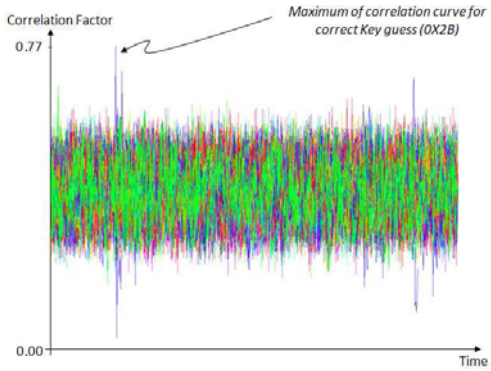


FIG. 16. CORRELATION RESULT FOR BOUNCY CASTLE AES (FOR ONE KEY BYTE)

Discussion on Countermeasures

CEMA like attacks, which we have adapted to mobile phones, have been implemented on devices like smart cards for some time now. In the later field, countermeasures against such attacks have been thoroughly studied. In this section we provide an overview of such countermeasures that mobile phone manufacturers could integrate to protect cryptographic calculations against CEMA like attacks. Among these techniques we distinguish among countermeasures implemented on the hardware level, the software level, in the packaging and on the applicative side:

- **Hardware countermeasures**: Those are features defined at the technological or architectural levels of the chip design to leverage the impact of the attacks on the chip itself. In the design phases of the mobile phone chip, the manufacturer may integrate hardware secure IP blocks like those proposed in (M. Agoyan, 2011). Another approach could be to adopt technologies like multi-rail encoding (R. Soares, 2008). Since CEMA needs synchronised EM traces, it is also possible to use random noise generator blocks (D. Page, 2003), that create EM perturbations and generate noise.
- **Software countermeasures**: This approach is based on the modification of the ciphering algorithm in the low level "driver" libraries or in the higher-level application software layers. Data masking (M-L. Akkar, 2001) is one of these software techniques where the input data and the

sensitive keys handled are "randomised" by adding a random value. Like in the hardware case, software random delays can be added within the AES software implementation (D.Naccache, 2005).

- **Packaging countermeasures**: Those are security features that can be added either in the way the chips are embodied into their package or the way the whole phone is packaged at the PCB board level. Such techniques are commonly used in point of sales terminals, (PCI/PIN, 2011). For example, sensors can be integrated to detect any illegal opening of the device's encasing and thus limit the physical access to the telephone's chips.
- **Applicative countermeasures**: Those are tweaks that can be added in the way applications use the sensitive routines so that attackers do not have a total control over the attack(s) he is carrying, thus reducing the chance for the attack to succeed. Concerning smart phones, hardware and packaging countermeasures may have a too high impact on their cost and their development cycle unless for cases where performance is important, in which case having dedicated hardware accelerators might be cost efficient.

Conclusion

In this paper we present what is, to our best knowledge, a first published study on physical attacks against modern mobile phones. Because such terminals now manipulate and store more and more private and confidential data, it has become vital to develop techniques to measure the resistance of such devices against physical attacks like those typically used in the smart card industry. Such techniques can either be used to measure to what extent a user's privacy is guaranteed or be used as a forensics method for unearthing encryption keys used to cipher data stored inside the phone. We first rapidly explored techniques like the use of JTAG probes without any success. We then set up a test bench and adequate analysis tools to successfully perform CEMA against the AES of the Bouncy Castle library. This shows that such libraries have to embed countermeasures against such attacks. Future work might consist in testing the technique against AES running on other smart phone's software platforms or against other cryptographic libraries like RSA or in setting up other powerful semi-invasive techniques like fault attacks.

ACKNOWLEDGMENT

The experiments were done on the MicroPackS platform and funded by the Secure Communications Solutions (SCS) cluster's FUI AAP10, project Calisson2.

REFERENCES

B. Mounier, A-L. Ribotta, J. Fournier, M. Agoyan and A. Tria, EM probes characterisation for security analysis, in 'Cryptography and Security: From Theory to Applications', pp 248-264, LNCS 6805, March 2012.

C.C. Tiu, A new frequency-based side channel attack for embedded Systems. MS thesis, Dept. of Electrical and Computer Eng., Univ. of Waterloo, 2005.

C. Gebotys,S. Ho and A. Tiu. EM Analysis of Rijndael and ECC on a PDA, Technical Report:CACR 2005-13, Dept of Electrical and Computer Engineering, 2005.

C.K. Kim, M. Schlaffer and S.J. Moon, Differential Side Channel Analysis Attacks on FPGA Implementations of ARIA, in ETRI Journal, vol. 30, num. 2, April 2008.

D. Naccache, P. Q. Nguyen, M. Tunstall and C. Whelan. Experimenting with faults, lattices and the DSA. In the proceedings of PKC 2005, LNCS 3386, pages 16-28, 2005.

D. Page. Defending against cache based side channel attacks. Information Security Technical Report, 8(1):3044, 2003.

E. Brier, C. Clavier and F. Olivier. Correlation power analysis with a leakage model. In Proceedings of CHES 2004, LNCS 3156, August 2004.

E. De Mulder, Electromagnetic Techniques and Probes for Side- Channel Analysis on Cryptographic Devices, PhD thesis, Arenberg Doctoral School of Science, Engineering & Technology, KUL, November 2010.

http://www.amontec.com/jtagkey-tiny.shtml, Last accessed, January 2013

IEEE Std 1149.1-2001. "IEEE standard test access port and boundaryscan architecture description", http://standards.ieee.org/reading/ieee/stdpublic/description/testtech/1149.1-2001 desc.html; July 23, 2001.

Jasper van Woudenberg, M. Witteman and B. Bakker. Improving diferential power analysis by elastic alignment. In the proceedings of CT-RSA 2011, pp 104-109, 2011.

jcp.org/aboutJava/communityprocess/final/jsr177/index.html, last accessed, January 2013

K. Gandolfi, C. Mourtel and F. Olivier, Electromagnetic analysis: concrete result, in the proceedings of CHES 2001, LNCS 2162 , pp. 251-261, Springer-Verlag, 2001.

K. Kim, D. Hong, K. Chung, and Ryou, "Data Acquisition from Cell Phone using Logical Approach", Proceedings of World Academy of Science, Engineering and Technology. Vol. 26. December 2007.

M. Agoyan, S. Bouquet, J. Fournier, B. Robisson, A. Tria, J-M. Dutertre and J-B. Rigaud, Design and characterisation of an AES chip embedding countermeasures, in IJIEI, Vol. 1, Nos. 3/4, 2011.

M. Breeuwsma, M. de Jongh, C. Klaver, R. Van der Knijff and M. Roeloffs, "Forensic Data Recovery from Flash Memory", Small Scale Digital Device Forensic Journal, Vol. 1, No. 1, 2007.

M. Breeuwsma, Forensic imaging of embedded systems using JTAG (boundary-scan), Digital Investigation, vol. 3, ed. 1, March 2006

M-L. Akkar and C. Giraud. An implementation of DES and AES, secure against some attacks, in the proceedings of CHES 2001, LNCS 2162, pp.309-318, 2001.

National Institute of Standards and Technology (NIST), Announcing the advanced encryption standard (AES), FIPS Publication, vol. 197, 2001.

N. Homma, S. Nagashima, Y. Imai, T. Aoki, and A. Satoh, Highresolution side-channel attack using phase-based waveform matching. CHES 2006, LNCS .4249, pp.187-200.

O. Schimmel, P. Duplys, E. Boehl, J. Hayek, R. Bosch, and W. Rosenstiel. Correlation power analysis in frequency domain. In proceedings of COSADE 2010.

P.C. Kocher, Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, in proceedings of Crypto'96, LNCS 1109, pp. 104-113, 1996.

PCI security standards council Payment Card Industry / PIN TransactionSecurity / Point of Interaction / Modular Security Requirements, version 3.1, October 2011.

R. Soares, N. Calazans, V. Lomné, P. Maurine, L. Torres and M. Robert. Evaluating the robustness of secure triple track logic through prototyping, in the Proceedings of SBCCI'08, ACM, pp.193-198, 2008.

S. Mangard, E. Oswald and T. Poop, DPA Book, April 2007

S. Willassen. "Forensic analysis of mobile phone internal memory". In IFIP Int. Conf. Digital Forensics, pp 191-204 (2005).

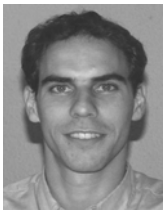
www.bouncycastle.org, last accessed, January 2013

Zhang, P., Deng, G., Zhao, Q., and Chen, K. EM Frequency Domain Correlation Analysis on Cipher Chips. In Proceedings of the 2009 First IEEE international Conference on information Science and Engineering.

Driss Aboulkassimi (S'09) received his engineering degree from the University of Montpellier. In 2010 he joined the Secure Architectures and Systems (SAS) lab, a joint team between the CEA-Leti and the Ecole Nationale Supérieure des Mines de St Etienne (ENSMSE. His research interests are security aspects of embedded systems.

Jacques Fournier worked 8 years for smart card manufacturer Gemalto before joining the CEA's SAS team in 2009 to work on smart card security, HW cryptographic accelerators and secure mobile systems. He graduated from SUPELEC, holds an MSECE from Georgia Tech and has a PhD from the Uni. of Cambridge.

Laurent Freund has been a lecturer in computer science at the ENSMSE for 14 years. He joined the SAS team 5 years ago. His research interests are mobile programming and secure mobile & embedded systems. He holds a Masters degree and a PhD from the Uni. of Evry.



Bruno Robisson studied electrical engineering at the Ecole Normale Supérieure de Cachan and received his PhD from University Paris VI in 2001. Since then, he has been a researcher at the CEA-Leti and joined the SAS team in 2005.. His main research topics are side channel attacks and development of secure cryptographic hardware.

Assia Tria is Research Director Habilited (HDR) by the French Ministry of Research. She received her PhD from University of Montpellier. She joined Gemalto in 1996 as a product engineer and then as a chip security expert. In 2005 she moved to the CEA-Leti to manage the SAS laboratory.