ISSN:0975-9646

Modelling & Detaining Mobile Virus Proliferation over Smart phones

Ashwini Gour,Jagdish Pimple ,Somesh Gangotri

Department of CSE
Nagpur Institute of Technology
RTMNU, Nagpur, MH, India.

***Abstract*— The devices with the Android operating system has been on the rise with the increase malware threat for mobile phones functionality. In a mobile network, viruses and malwares can cause privacy leakage, extra charges, battery power depletion, remote listening and accessing private short message and call history logs etc[3]. Furthermore, they can also scrape wireless servers by sending lot of spam messages or track user positions through GPS. Because of the potential damages of mobile viruses, it is important to gain a deep understanding of the propagation mechanisms of mobile viruses. In this paper, we propose a two layer network model for simulating virus propagation if apps are installed on a device. It addresses the behaviour of virus propagation and restrains it, also determine factors of virus propagation in mobile networks and analyses the virus in the device. The presence of viruses in an application will be reported and hence, avoided by further users of the same app. Network immunization is the most effective techniques to restrain virus propagation in complex networks. We observe two strategies to avoid virus propagation, i.e., Preimmunization and Adaptive Dissemination strategies represent on the methodology of Autonomy-Oriented Computing (AOC) [1][6]. So that by using the method it can automatically detect and delete both Bluetooth and SMS virus before enter into the Smartphone operating system.**

***Keywords*— Mobile devices, Smartphone, malware, Preimmunization and Adaptive Dissemination, Autonomy-Oriented Computing (AOC).**

I. INTRODUCTION

In recent years, the smart phones worldwide market has grown dramatically. Smartphone users perform many online tasks, including web browsing, document editing, multimedia streaming, Internet banking, and share the documents from one mobile to another through Bluetooth, SMS services and through social applications like whatsapp, facebook. Simultaneously, the increasing use of Smartphone in life and business has been attracting the attention of malware writers, who aims to theft data confidentiality, integrity, and the ability to use handheld services. Mobile malware is rapidly becoming a serious threat. In this paper, we survey the current state of mobile malware in the wild and analyze the incentives behind 46 pieces of iOS, Android, and Symbian malware that spread in the wild from 2009 to 2012. We also use this data set to evaluate the activeness of techniques for preventing and identifying mobile malware. We also examine the incentives that cause non-malicious Smartphone to publish root exploits and survey the availability of root exploits. Examples of the most infamous threats to mobile phones include the Skull and Mabir worms, targeting at android phone applications. These are malware or viruses or cell-phone worms, which are malicious codes that act susceptibility in cell-phone software and spread in networks through current services such as Bluetooth and Short / Multimedia Messaging Service (SMS/MMS). A user can be automatically exciting for numerous SPAM messages generated by the worm and the phone battery will be quickly exhausted. Many studies reported the damages of mobile viruses [9], [10]. Other reported worm damages extend from robbery user data and privacy to destroying hardware.

Different Surveys:

From year 2004 to 2008, the types of mobile malware have increased significantly in numbers. As of March 2008, FSecure has counted 401 varieties of mobile malware in the world, and McAfee has counted 475 kinds of mobile malware. Overall, in 2012 the number of known malicious samples for Android is more than eight times. Hence, the mobile malware various includes leaking of user privacy, extra service charges by automatically sending expensive multimedia messages or making long-distance calls, and battery power depletion.

In several existing methods some will not be able to detect new viruses due to the limitation of antivirus knowledge. Our work focuses that the device initially affording the application can provide the feedback to the server which enhances further devices not installing that particular app. In order to make sure that users timely update their own detection databases, the smart phones are disseminated with the notifications or patches by the service providers or security companies. Some strategies attempt to forward security notifications or patches based on the short-range communication capabilities of connected phone but their impact will be affected by human mobility patterns and inter contact frequencies among phones. It would be difficult to acquire signature files in a timely manner. In the meantime, other dissemination strategies have also been used to distribute patches and the difficulty remains when dealing with a large-scale or highly dynamic network. Thus, we propose a new strategy that can efficiently forward patches to as many phones as possible, even in large-scale and/or dynamically evolving networks.

This Malware can also be termed as all kind of intrusions that is disastrous to the computer software and hardware system. The malware is created by malware writers for different reasons and purposes ranging from challenges to

productive commercial gain, destruction to punishment among others. Hence, its growth is tremendously alarming in volume and its expansion rate is also cannot be overlooked due to its damages. Through different media if once malware gets itself into the system like copying of files from external devices onto the system and mostly by downloading files from the internet, it checks the susceptibilities of the system and infects the system if the system is terrifically vulnerable. The involvement for the rate of malware spread today is a global paradox, especially as its spreading capacity is twice over the internet which is a means of global communication.

Valid proliferation models can be used as test beds to:

1) Measure the scale of a malware outbreak before its occurrence in reality and

2) Check out new and/or improved remedies for governing virus propagation.

In this paper, we propose a two-layer network model for characterizing viruses, for which Bluetooth , installing apps and SMS Services, is the propagating medium in order to address the above mentioned shortcomings. In our proposed model, viruses are triggered as a result of human behaviours, instead of the contact probabilities in a uniform model. Here, the two operational behaviour and mobile mobility are focused in our individual-based model. Different from existing work that focuses the effects of network structures on virus propagation; our work is aimed to gain further insights into how human behaviours affect the propagation dynamics of mobile viruses and to avoid further misuse of the same.

We propose a two-layer network propagation model that accounts for the behaviour of users (i.e., operational and mobility patterns) in mobile networks. Based on our model, we examine the performance of a preimmunization strategy that draws on the methodology of autonomy-oriented computing (AOC) in restraining mobile virus propagation. We design an adaptive dissemination strategy by extending local reactive behaviours of entities.

The remainder of this paper is organized as follows: Section 2 surveys the propagation of mobile malwares and their type. Section 3 surveys the present and future incentives for writing mobile malwares. Section 4 presents a two-layer network model for simulating virus propagation, model and processes involved. Section 5 discusses the methodology of computing, different strategies and techniques. Section 5 highlights the major contributions. Section 6 examines the conclusion of the proposed propagation model.

II. LITERATURE SURVEY

In what follows, the related work on mobile virus and their propagation models is reviewed first. Next, some virus defense methods that contain abnormal detection technologies for restraining virus propagation in mobile networks are introduced here.

A. Smartphone Malwares

The Smartphone virus, Cabir, was developed in 2004 by the virus writing group. It can self-replicate but does no damage to the phones. Now a day more than a hundred mobile viruses have come into existence, many of which contain susceptible codes and cause various damages to the smart phones. The smart phones virus growth is very fast, as compared to the virus from the computer and Internet world. Such suddenly growth of smart phones will provide a productive ground for the malware to spread. An affected smart phone can cause severe compensation for both the users and the cellular service provider. In case of users, the damage may contain the loss or theft of private data, the interference of normal smart phone usage and also economic losses (e.g., the virus may secretly use the SMS/MMS services).In the cellular infrastructure side, the mobile viruses present a serious effect of Denial of Server.

B. Types of Viruses

There are many ways to categorize Smartphone viruses. These Smartphone viruses are categorized based on the targets that the virus attacks (e.g. the call centre, the cellular base station) [10]. Instead of focusing on what the viruses seek to attack or achieve, we choose to categorize the Smartphone viruses based on the multiple infection vectors that the virus enters and/or exits the device. The benefit of our approach is that it provides a generic view on how a virus penetrates into a Smartphone and how easily it can spread in the Smartphone population. We have identified the categories of infection vectors for Smartphone virus, which are listed in Table 1 [8] gives some descriptive viruses at present in existence for each infection vector. Below, we will describe these infection vectors in more detail.

TABLE 1.

TYPES OF SMARTPHONE VIRUSES BASED ON INFECTION VECTOR

Infection Vector	**Examples**
Cellular Network	CommWarriors, Mabir
Bluetooth	CommWarriors
Internet	Skulls, Doomboot
USB	Mobler, Crossover
Peripherals	Cardtrap

C. Virus Propagation through BT and SMS

According to the communication channels of mobile viruses, the viruses fall into two categories namely: BT-based viruses (e.g., Cabir, Lasco) and SMS-based viruses (e.g., TXSBBSpy, Zombie, and Commwarrior). SMS-based viruses can send copies of themselves to all phones that are recorded in address books, by means of photos forwarding, videos, and short messages, etc. The propagation of SMS-based malwares follows a long-range spreading pattern that is similar to the spreading of viruses in computer, especially like worm propagation in e-mail networks thus, the operational behaviour of users is important in SMS-based virus propagation. Users with awareness about the viruses risk will not likely be infected even if they receive attachment. In order to study SMS-based virus propagation, we consider certain the operational patterns, such as if the users open a virus attachment or not. BT-based virus is a local-contact driven virus since it infects other phones only through Bluetooth and Wi-Fi devices within a given radio range. Similar to contact based diseases as in humans (e.g., SARS and H1N1), the propagation of a BT-based virus

follows a spatially localized spreading pattern. Epidemic modelling is one of the most common approaches for studying such virus propagation. It assumes that individuals are homogeneous in a host community, each having an equal likelihood contact with others. Also, epidemic modelling is applied on some studies to analyse the propagation dynamics of a BT-based virus.

In this work, we incorporate related research on human mobility and operational behaviour into our model in order to provide a computational model for characterizing and simulating the propagation dynamics of mobile viruses. The traits of mobility patterns described by our model are consistent with statistical results from the real-world traces, i.e., local bounded mobility areas, power-law travelling distances, and inter contact times.

D. Defense Strategies against Mobile Viruses

Some countermeasures such as anomaly detection technologies have been proposed to protect users' private information from being revealed to different users. Although these abnormal detection technologies can help directly protect phones from being affected by certain viruses, it is not easy to detect new viruses because the monitoring technologies must first be trained to recognize normal and abnormal operational behaviours. If any new virus produces some patterns (e.g., a series of system calls), these monitoring technologies cannot detect such virus. Hence, challenging to detect a worm outbreak at the early stage unless both users and security companies frequently update their detection classifiers. Like, Bose et al. discriminated some of the malicious behaviours from normal operations by training a classifier based on the method of support vector machines. Cheng et al. have provided an approach to detecting both single-device and system-wide abnormal behaviours by collecting and sending communization data to remote servers in order to reduce the detection burden of phones.

Different from wired networks (e.g., computer networks), it is almost impossible to send patches to all phones simultaneously and timely. Thus, we need new strategies to efficiently disseminate security notifications or patches to as many phones as possible with a relatively lower communication cost before a new virus spreads to a large population. In order to reduce communication redundancy, strategies that send patches based on Bluetooth is utilized. After which they send security signatures to all communities based on the local detection. However, this method cannot ensure that users acquire patches in time.

In this paper, we examine the performance of an AOC-based preimmunization strategy that selects some highly-connected phones and prevents a virus from turning into an epidemic. Furthermore, AOC-based dissemination strategy is designed that distributes security notifications or patches to smart phones with a low communication redundancy, in order to restrain virus propagation before it causes further infections.

III. PROBLEM STATEMENT

The motivation for writing mobile malware is as follows.

A. *Present Incentives*

1) Novelty Changes

Some malware can cause mischief or damage in such a way that appears to amuse the author. For example, the wallpaper of infected devices are changed by Ikee, and sent anti religion text messages from Android phones. Number of malware fall into this category and no other.

2) Selling User Information

Mobile operating system APIs provide apps with large amounts of user's data. The applications can also query the device APIs for the user's location, list of contacts, browser and downloaded history, installed applications, and IMEI number (the unique device identifier). Advertising or marketing companies might be willing to purchase users' locations, browsing histories, and lists of installed applications to improve their behavioural profiling and product targeting. We still cannot know for sure why malware collects this data; we contemplate that for financial gain this type of data is being sold by malware distributors.

3) Stealing User Credentials

Credentials could be used directly by malware authors for greater financial gain, but financial fraud can be difficult to perpetrate and requires specialization. People use Smartphone for shopping, banking, e-mail, and other activities that require passwords and payment information. Banks rely on cell phones for two-factor authentication. Users may also save payment credentials and authentication in text documents on their devices (for example, to use phone as a password manager), which in turn makes the device a target for credential theft.

4) Premium-Rate Calls and SMS

Premium-rate cost call or SMS is charged to the sender's phone bill. Calls of premium rate can cost several dollars per time, and SMS messages of premium-rate can cost several dollars per SMS. In Android and Symbian devices, malware tries to completely hide premium-rate SMS messages from the user. Premium-rate SMS attacks could in turn is feasibly go unnoticed until the user's next phone bill.

5) SMS Spam

SMS spam is used for commercial advertising and spreading phishing links. Commercial spammers are incentivized to use malware to send SMS spam because sending SMS spam is illegal in most countries. Furthermore, the use of SMS may lend more authenticity to spam than e-mail because phone contacts are often more intimately acquainted than e-mail contacts. 8 of the malicious Symbian and Android applications send SMS spam.

6) Search Engine Optimization

Many web sites rely on search engines for traffic congestions, which makes web site owners desire high visibility in search engine results. Search engines rank the web sites as per how relevant each web site is to a given search term. An engine's perception of relevance is announced by the rate at which users click on the web sites for a search term.

7) Ransom

Malware can be a tool for blackmail. For example, the desktop Trojan Kenzero stole the user's browser history, published it publicly on the Internet alongside the person's name, and then demanded 1500 yen to take down the person's browser history. There has not yet been any mobile malware that seriously threatens or publicly embarrasses the user for profit, but one piece of mobile malware has sought a ransom.

B. *Future Incentives*

This section discusses incentives that will motivate future mobile malware. Mobile malware has not yet exhibited evidence of these motivations.

1) Advertising Fraud Click

Advertisers pay advertising networks if users view or click on ads. In turn, advertising networks pay the web sites that host this. Numerous web sites, advertising networks, defraud advertisers and non-malicious networks use desktop malware to load and click on advertisements [16, 17]. If undetected, click fraud generates a few cents (or even dollars) per instance of fraud. The attacker will directly benefit from the fraud by receiving some portion of the fraudulent payment. Furthermore, competitors may lower their advertising bids after seeing a lower return on investment, causing the cost of advertisements to go down [18].

2) Invasive Advertising

Many legitimate applications use advertisements to earn money while providing the application to users for free. There are two main reasons for an attacker to display advertisements with malware. First, the attacker may want to advertise goods or services that are illegal or of a nature that legitimate advertising companies prohibit. An attacker might do this to advertise his own products or to create a black market. Second, the attacker may simply want to collect revenue from displaying legitimate advertisements. The attacker may be able to generate more revenue with invasive advertising practices by displaying advertisements to users more often or in such a way that users accidentally click on them. This is not considered click fraud because it capitalizes on users' legitimate clicks instead of automated clicks. However, these invasive advertising practices are against legitimate networks' terms of service. Antivirus reports did not include enough information to determine the nature of those web requests. However, adware exists for desktop machines, and we expect to see it in mobile applications as well.

3) In-Application Billing Fraud

Android and iOS support in-application billing, which allows a user to purchase a virtual item from an application using the payment account associated with the Android Market. Users can buy items such as game credits and music from applications without directly providing the application with payment information. We predict that in-application billing may become a target of fraud in the future. First, the implementations of in-application billing protocols could include bugs that allow malware to charge users for items without their approval. Second, malicious applications could use social engineering, click jacking, or phishing attacks to trick users into accidentally or unknowingly approving in-application purchases.

4) Governments

Governments may use mobile phones to monitor citizens and their activities. Unlike the majority of other incentives discussed in this paper, government spying is not motivated directly. This type of monitoring could be performed on a large scale (e.g., China's Internet monitoring) or targeted at known dissidents or suspected criminals. It could incorporate GPS tracking, audio and video recording, monitoring of e-mail and SMS messages, and extracting lists of contacts. The government threat model is significantly more powerful than the criminal threat model. Markets and review processes cannot be trusted because governments can compel the responsible agencies to publish it. Government agents also can gain physical access to targets' phones to install monitoring software.

5) E-Mail Spam

Desktop malware uses compromised hosts to send e-mail spam for advertising and phishing. There are three ways for malware to send spam from infected hosts:

1. Malware can send spam from the user's e-mail account, for example by abusing a logged-in browser session. However, it is hard for mobile malware to manipulate a user's e-mail account.
2. Malware can make SMTP connections to spam recipients' Mail eXchange (MX) servers if the network permits outgoing traffic on port 25
3. Malware can launder spam through open proxies. In many cases, this only requires an outgoing HTTP request. Mobile malware can do this, although mobile phones typically have less bandwidth than desktops. Desktop machines are more attractive as spam clients, so we do not expect to see e-mail spam as a major motivating factor for mobile malware.

6) Distributed Denial of Service

To perpetrate distributed Denial of Service (DDoS) attacks, botnet owners command large groups of compromised Machine to simultaneously send requests to servers. DDoS attacks can be launched for ransom, amusement, cyberwar fare, or as a paid service to others. Traditional DDoS attacks are difficult to stop because of their distributed nature, but one approach is for the server to block the IP addresses of visitors that behave anomalously. Consequently, each attacking machine is limited to a small number of fraudulent requests. This would not be an effective defense mechanism against mobile-based DDoS attacks because cellular networks assign new IP addresses. If that rate of IP assignment is not fast enough, mobile malware can force the assignment of a new IP address from the cellular network by resetting the data connection.

7) NFC and Credit Cards

Mobile phones are beginning to incorporate Near Field Communication (NFC), which allows short, paired transactions with other NFC-enabled devices in close

proximity.NFC can be used for commerce (i.e., accepting credit card transactions), social networking (e.g., sharing contact information), device configuration (e.g., automatically configuring Wi-Fi), and more. We predict that NFC will become a popular target for malware due to the ease with which financial transactions can occurs using NFC. Malware that is capable of using NFC has the potential ability to surreptitiously read and interact with NFC enabled devices placed close to the phone (e.g., in a pocket), such as credit cards or personal identification cards.

IV. PROPOSED APPROACH

In the system we are implementing a two layer network model for spreading virus through Bluetooth and SMS/MMS channel. The operation of human behaviors such as mobile behavior and operational behavior [3] addresses the spreading of viruses. Moreover we examine two strategies to avoid virus in mobile phones. i.e., Preimmunization and Adaptive Dissemination strategies through the methodology of Autonomy-Oriented Computing (AOC) [1].In this method it can automatically detect the virus before when virus enter into the smartphones and delete it.

A. *Autonomy-Oriented Computing*

Autonomic computing alludes to the self-managing physical appearance of distributed computing resources, adapting to irregular changes while beating intrinsic difficulty to operators and users [6]. Started by IBM in 2001, this enterprise finally aims to develop computer systems capable of self-management, to overcome the quickly growing difficulty of computing managements of system, and to reduce the obstacle that complexity indicates to further growth. Using high-level policies the system makes conclusion on its own and it will frequently check and enhance its status automatically so that it can modify itself to changing conditions. An autonomic computing framework is collected of autonomic components (AC) interacting with each other .

B. Modeling Mobile Virus Propagation

In this section, first a two-layer network model for simulating mobile virus spreading through different communication channels is introduced. Next, we present detailed propagation processes on mobile application viruses. The work presented in this section is an extension of the work in Modeling and Restraining the Propagation of Mobile Viruses. Based on the analysis of propagation mechanisms, a primary factor contributing to virus propagation lies in operations of users after infected messages are received from the network through the applications being installed on the device. If users have enough knowledge they will not open suspicious messages and their phones will not be easily infected. Mobility patterns play a key role in virus propagation because as these viruses can only infect local neighbors (whether or not they know these neighbors) within a certain range. This can evaluate the impact of operational behavior on mobile virus proliferation in social related networks, and also the effects of mobile behavior on the virus and other virus propagation in geographical contact networks.

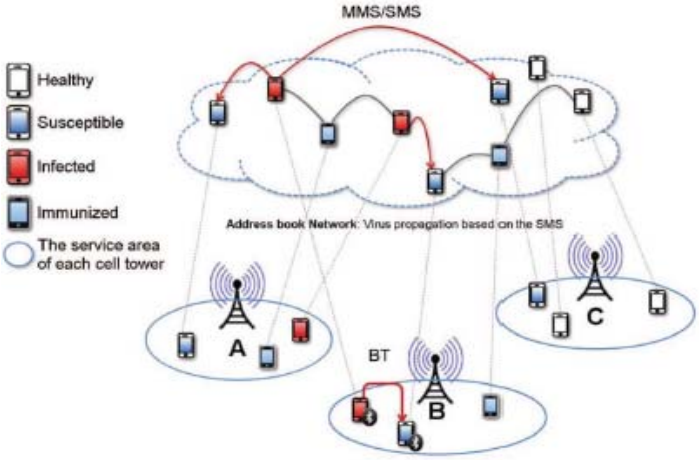

Fig 1: A two-layer network model for simulating mobile virus propagation. The network of cell towers (e.g., A, B, and C) is built based on geographical information, whereas the social relationship network is constructed from the address books of mobile users [1].

C. *Two-Layer Network Propagation Model*

The basic ideas behind our two-layer network proliferation designing are shown in Fig1. The lower layer represents a geographically based cell tower network. In this layer BT-based viruses spreads to various positions of mobile phones as shown. The upper layer corresponds to a logical network constructed from the address books of phones. SMS-based viruses propagate in this layer following the social relationships among mobile users and interaction proceeds.

D. *The Structure of Geographical Network*

Mobile phones connect with each other through wireless signals provided by cell towers. Users with their phones can travel in a geographical network, moving from lattice to another based on their mobile behavior. The same or different towers provide the basic wireless signals in these two lattices. The propagation processes of BT-based and SMS-based viruses can be simulated in a geographical contact network and a social related network, respectively.

E. *The Structure of Logical Network*

A logical relationship network among mobile users can emerge from the address books of mobile phones. In such a network, the various nodes correspond to phones and links and show the communications among them. Different from virus propagation through Bluetooth that is only capable of affecting nearby phones, some viruses may spread through SMS (e.g., Zombie). Hence, they can also attack remote phones. Therefore, SMS-based viruses potentially spread as fast as consider to worms in email networks.

F. *SMS- Based Propagation Process*

Social relationships are embodied in mobile networks based on the address books of smart phones. If a phone is infected by this type of virus, it automatically sends its copies to other phones as per the address book of the infected phone. When users gets a suspicious message from other devices, based on their own security awareness they

opens or delete according to the knowledge about the risks of mobile viruses. Therefore, the security awareness of mobile users is one of the dominant factors that describe SMS based virus propagation. In our model, one type of operational behaviour is simulated, i.e., whether or not a user opens a suspicious message. In order to better characterize the SMS based virus propagation, following is assumed:

- If a user opens an infected message, the phone of this user is infected and automatically sends viruses to all phones based on its address book;
- If a user does not open an infected message, its assume that the one with higher security awareness can deletes this infected message;
- An infected phone sends out viruses to other phones only once, and the infected phone cannot send out viruses anymore;
- If a phone is patched (immunized), it will not send out any viruses even if a user opens an infected message.

G. *BT- Based Propagation Process*

Different from SMS-based viruses, if a phone is infected with BT-based virus, then it automatically searches another device through available Bluetooth services within a certain range, and then replicates the BT-based virus to that phone. Therefore, users' contact frequency and mobility patterns which play key roles in BT-based virus propagation. In our model, we integrate a stochastic local infection dynamics among phones with the mobile behaviour of each user in a geographical network, taking into account prior research on human mobility.

Based on our analysis, a smart phone can avoid a BT-based attack by turning off the Bluetooth service. However, SMS based viruses often propagate through the trust relationships among friends. Previous experiments also show that SMS-based viruses are more dangerous than BT-based viruses in terms of propagation speed and scope. In this section, we describe two strategies to restrain SMS-based virus propagation.

V. METHODOLOGY

Although we have used a homogenous model to simulate BT-based virus propagation in each tower, users' different travelling patterns will cause different dynamic spreading processes. Several studies have found that users' travelling patterns play a key role in virus propagation, similar to contact-based epidemics (e.g., SARS) in humans. Fig. shows three mobility patterns of users. The more accurate the mobility patterns of users are, the better predicting results about virus propagation will be. Based on existing studies, characteristics of mobility observed from the real-world data are:

- The traveling distances of a user follow a truncated power-law distribution
- People move with a probability at each time;
- People trend to devote most of the time to only a few locations in their daily life where they can meet a lot of other people;

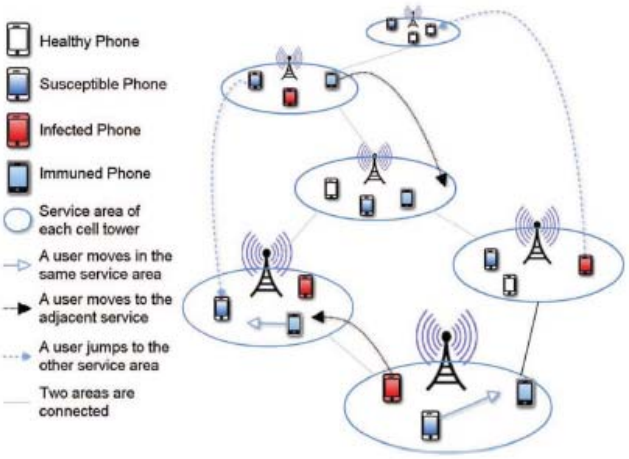

Fig 2 : The mobility patterns of users in a geographical network, which can be affected by BT virus propagation[1].

A. *Goals and Modelling Process of Autonomy-Oriented Computing*

AOC has three goals [10].The first goal is to reproduce life-like behaviour in computation. With complete knowledge of the fundamental mechanism, simplified life-like behaviour can be used as model for a general-purpose problem solving technique. Replication of behaviour is not the end, but rather the means, of these computational algorithms; the second goal is to understand the essential mechanism of a real-world complex system by hypothesizing and frequent experimentation. The conclude product of these simulations is a progress understanding of or explanations to the real working mechanism of the modelled system; the third goal affairs the rise of a problem solver in the absence of human intervention. To build an AOC-based model, the following is a list of common steps:

- Observe macroscopic behaviours of a natural system;
- Design entities with desired synthetic behaviours as well as an environment where entities reside;
- Observe macroscopic behaviours of the artificial system;
- Validate the behaviours of the artificial system against the natural counterpart;
- modify (ii) in view of (iv);
- Repeat (iii)-(v) until satisfactory;
- Find out a model/origin of (i) in terms of (ii) or apply the derived model to solve problems.

From the above steps, we note that an AOC system mainly contains a population of autonomous entities and the rest of the system is referred to as the environment. Concentrating on entity and environment, the construction of an AOC model involves three phases (see Figure 3). The first phase, natural system identification, can be viewed as the precursor to actual systems modelling and concerns the selection of an appropriate analogy from the natural and physical world. There are two tasks involved: identify desired system behaviours and identify system parameters.

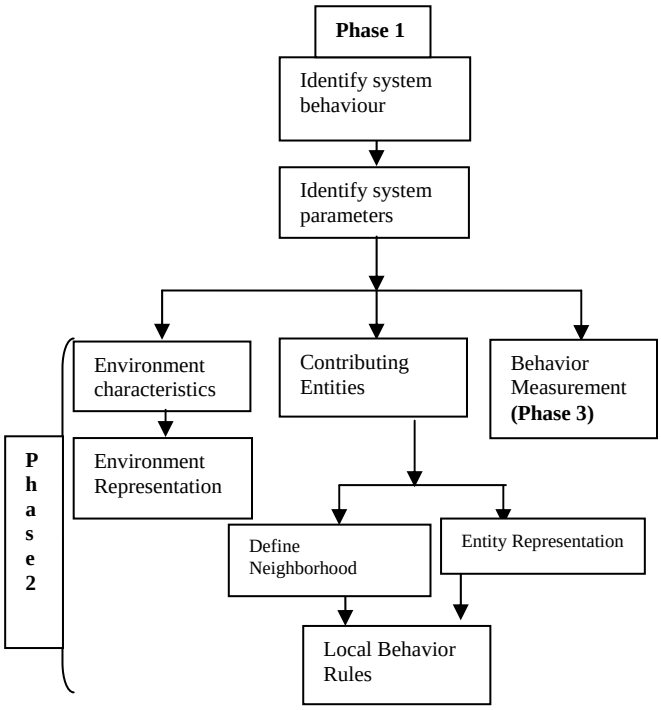

Fig 3: block diagram of major components of Aoc model

The right analogy is the key to the success of the AOC-based system which interprets itself through its behaviours. After the choice of appropriate analogy, and details like the total entities to run and time to run the simulation need to be decided. The second phase is the artificial system construction, includes total number of elements present in the AOC-based system. This phase is further divided into two major sub-phases: autonomous entity modelling and environment modelling. The identify contributing entities task is the first and the most important task in which the designers are required to choose the level of detail to be modelled. The define neighbourhood task provides a certain measurement (e.g., distance) in the solution space within which local interactions can occur and local information collection is possible. The *define entity representation* task handles how to characterize an entity, that also focus on its states and goals etc. The last task concerning the entities, *define local behaviours and behavioural rules*, defines the ways in which an Autonomous entity reacts to various data which has been collected within its neighbourhood and the ways in which it adapts its local behaviours and behavioural rules. The tasks that concern the environment are *identifying environment characteristics* and *define environment representation*. The former task concerns the role the environment plays in conveying the knowledge shared between the autonomous entities. The latter task addresses the characterization of the environment. The third phase is the performance measurement, which is concerned about the evaluation criteria for comparing the artificial system manifested by the AOC-based system. This relates to problem-solving and provides an indication to modify the current set of individual behaviours and behavioural rules.

B. *Adaptive Patch Dissemination Strategy*

However, only if the viruses have already propagated (e.g., Melissa), then we detect certain viruses and then allocate patches or antivirus programs into networks. The security notifications or patches cannot be sent to all users simultaneously due to the network bandwidth constraints. Therefore, we propose an adaptive dissemination strategy based on the methodology of AOC in order to efficiently send security notifications or patches to most of phones with a relatively lower communication cost.

C. *Malware Attack Technique*

1) *First Technique on Mobile Phone***:** Malware, in this case creates a new process to execute its malicious code and compromise the cell phone. Here user operations are required, for example when a user downloads software on an internet or opens a received message from another user. The newly created process includes program descriptor, that describes the address content, execution state and security context, which is different from that of the invoked parent process. In this technique, an attack is launched by the cell phone malware through legally installed application. A good example is a cardblock Trojan, which is a cracked version of a legitimate Symbian application called instansis. It allows a user to create SIS archive. Cardblock blocks the MMC memory card and detect the subdirectories under system (SDI attack) [12].

2) Second Technique: Malware, here redirects the program flow of a legitimate application (e.g. messaging activities) to execute its malicious code within a legitimate security context. Open Source based OS and application a framework like Android smart phones is the major target of this kind of malware attack.

3) *Malware method of Propagation:* The basic method of propagation of malware is either self-propagation or user interaction. A malware like worm does not require any user intervention before its execution occur. It is capable of copying itself and causing occasional execution without the intervention of host program or its user. Virus is a user-interaction oriented malware that always looks for a host program for its execution and consequent infection. Other malware might not require any of these methods for its propagation, but may adopt internet medium for their spreading. Mobile malware on the other hand, adopt mobile phone network on the internet in order to propagate itself, but this action is usually curtailed by the internally built defence mechanism in the network mobile phone. Another opportunity for mobile malware to propagate is through the direct pair-wise communication resources i.e. Bluetooth, Wi-Fi, and Infrared.

D. *Malware Detection Techniques*

The task of detecting malware can be categorized into analysis, classification, detection and eventual containment of malware. Several classification techniques have been used in order to classify malware according to their instances and this has made it possible to recognize the type and activities of a malware and new variant. Analysis of malware has to do with identifying the instances of malware by different classification
schemes using the attributes of known malware characteristics. Malware detection has to do with the quick detection and validation of any instance of malware in order to prevent further damage to the system. The last part of the job is containment of the malware, which involves effort at

stopping escalation and preventing further damages to the system. Malware detection technique has been classified according to the following:

1) *Feature Selection:*

In Machine Learning applications, a large number of extracted features, some of which redundant or irrelevant, present several problems such as - misleading the learning algorithm, over-fitting, reducing generality, and increasing model complexity and run-time. These adverse effects are even more crucial when applying Machine Learning methods on mobile devices, since they are often restricted by processing and storage-capabilities, as well as battery power. Applying fine feature selection in a preparatory stage enabled to use our malware detector more efficiently, with a faster detection cycle.

2) *Using Machine Learning for Behavioural Analysis:*

The evaluation of Machine Learning classifiers is typically split into two subsequent phases: training and testing. In the first phase, a training-set of games and tools feature vectors is provided to the system. These feature vectors are collected during the activation of both game and tool applications. The representative feature vectors in the training set and the real class of each vector (as game/tool) are assumed to be known and enable to calibrate the detection algorithms (such as a Decision Trees, or Bayesian Network). By processing these vectors, the algorithm generates a trained classifier. Next, during the testing phase, a different collection (the testing-set) containing both game and tool applications feature vectors is classified by the trained classifier. In the testing phase, the performance of the classifier is evaluated by extracting standard accuracy measures for classifiers. Thus, it is necessary to know the real class of the feature vectors in the test-set in order to compare it real class with the class that was derived by the trained classifier.

E. *Strategy Output*

The software has been built based on the techniques and different apps when installed are processed on it. The following figures show the implementation of the mentioned model in the application. It reminds the fact that the applications being installed by the users on the android devices is processed, scanned and the feedback is taken back from the user.

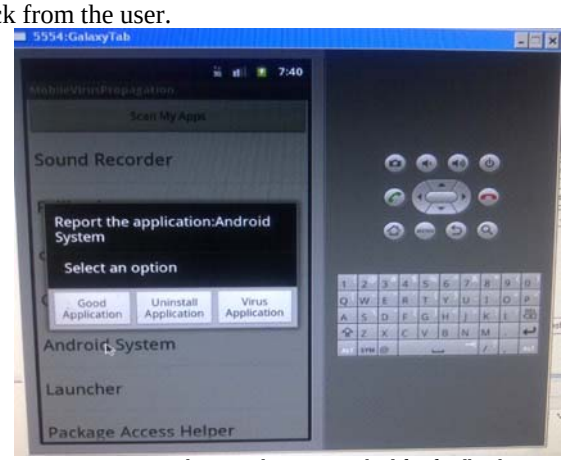

Fig 4: Figure showing the user is asked for feedback.

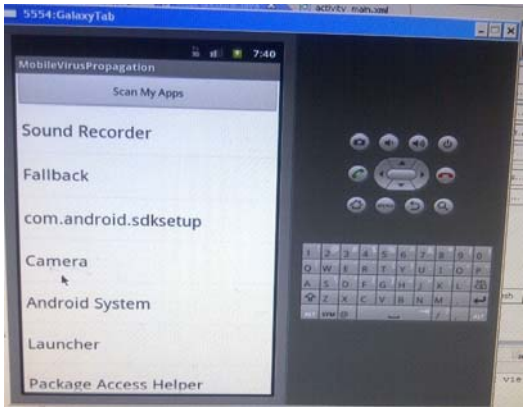

Fig 5: Figure showing the running apps in device.

VI. CONCLUSION

In this paper, a two-layer network model for analysing the spreading of SMS-based and BT based viruses [3] is shown. Mobile handsets devices are victim to malwares due to their flexible communication and computation abilities, and resource constraints. This is support in android Smartphone and accurately detects and deletes the virus of the content before enter into the mobile operating system. It after utilising the apps provides the feedback so that the next user will know about the app. Future work can be enhanced the virus content of data's enter into the Smartphone through Bluetooth and SMS channels it automatically filter the virus and data separately and delete the virus but not the data. The result shows that the Smartphone in spreading of viruses via different apps is being protected. As Android malware evolves hence the effectiveness of these types of measures will decrease. But, these techniques are still valuable as they raise the bar of entry for repackaged and newly launched malware. The presented detection techniques are viable with the large scale testing requirement to find real world performance. The understanding of interactions between human behaviours and the propagation dynamics of mobile viruses would be helpful to send security notifications to multiple users in order to improve their security awareness, which can in turn to play a key role in restraining virus propagation.

References

[1] Chao Gao and Jiming Liu, "Modeling and Restraining Mobile Virus Propagation," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL.12, NO.3, MARCH 2013.

[2] C. Gao, J. Liu, and N. Zhong, "Network Immunization with Distributed Autonomy-Oriented Entities," IEEE Trans. Parallel and Distributed Systems, vol. 22, no.7, pp. 1222-1229, July 2011.

[3] C,Gao and J.Liu, " Modeling and Predicting the Dynamics of Mobile Virus Spread Affected by Human Behavior", Proc. IEEE 12th Int'l Symp. A World of Wireless, Mobile and Multimedia Networks (WoWMoM '11), pp, 1-9, 2011.

[4] D. Balcan, V. Colizza, B. Goncalves, H. Hu, J. Ramasco, and A. Vespignani, "Multiscale Mobility Networks and the Spatial Spreading of Infectious Diseases," Proc. Nat'l Academy of Sciences of USA, vol. 106, no. 51, pp. 21484-21489, 2009.

[5] D.-H. Shi, B. Lin, H.-S. Chiang, and M.-H. Shih, "Security Aspects of Mobile Phone Virus: A Critical Survey," Industrial Management and Data System, vol. 108, no. 4, pp. 478-494, 2008.

[6] J.Liu, "Autonomy-Oriented Computing(AOC): The Nature and Implications of a Paradigm for Self-Organized Computing."Proc. Fourth Int'l Conf.Natural Computation(ICNC '08),pp.3-11,2008.
[7] X. Meng, P. Zerfos, V. Samanta, S.H. Wong, and S. Lu, "Analysis of the Reliability of a Nationwide Short Message Service," Proc. IEEE INFOCOM, pp. 1811-1819, 2007.
[8] J.Cheng, S.H.Y. Wong,H. Yang, and S.Lu,"Smartsiren Virus Detection and Alert for Smartphones,"Proc.Fifth Int'l Conf.Mobile Systems, Applications, and Services(MobiSys '07),pp.258-271,2007.
[9] H.Kim, J.Smith, and K.G. Shin, "Detecting Energy-Greedy Anomalies and Mobile Malware Variants," Proc. Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys 08), PP.239-252, 2008.
[10] L.Xie, H.Song, T. Jaeger, and S.Zhu, "A Systematic Approach for Cell-Phone Worm Containment," Proc.17th Int'l World Wide Web Conf.(WWW '08), pp. 1083-1084,2008.
[11] Jiming Liu, Xiaolong Jin, Kwok ching Tsui, " Autonomous Oriented Computing(AOC): Formulating Computational Systems with Autonomous Components." IEEE Trans on system, man and cybernetics,pp.879-902,nov 2005.
[12] Vinit B. Mohata,Dhananjay M. Dakhane, Ravindra L.Pardhi," MOBILE MALWARE DETECTIONTECHNIQUES", International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 4 No. 04, 2229-3345,Apr 2013.
[13] J. Balthrop, S. Forrest, M.E.J. Newman, and M.M. Williamson, "Technological Networks and the Spread of Computer Viruses," Science, vol. 304, no. 5670, pp. 527-529, 2004.
[14] R. Pastor-Satorras and A. Vespignani, "Epidemic Spreading in Scale-Free Networks," Physical Rev. Letters, vol. 86, no. 14, pp. 3200-3203, 2001.
[15] Adebayo, Olawale Surajudeen, Mabayoje, Amit Mishra, Osho luwafemi, "Malware Detection, Supportive Software Agents and Its Classification schemes", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.6, November 2012.
[16] B. Miller, P. Pearce, C. Grier, C. Kreibich, and V. Paxson. What's Clicking What? Techniques and Innovations of Today's Clickbots. In DIMVA, 2011.
[17] N. Daswani and M. Stoppelman. The anatomy of Clickbot. A. In Proceedings of the _rst conference on First Workshop on Hot Topics in Understanding Botnets, pages 11{11. USENIX Association, 2007.
[18] N. Daswani, C. Mysen, V. Rao, S. Weis, K. Gharachorloo, and S. Ghosemajumder. Online advertising fraud. Crimeware: Understanding New Attacks and Defenses, 2008.
[19] http://en.wikipedia.org/wiki/Mobile_virus