Procedure Dynamic Network and Prevent Mobile Typically
Extension

Priti Naik
M.E.4th sem (wireless communication and computing)
G. H. Riasoni Collage of Engineering, Nagpur

Abstract: Prevent and mobile is taken spread from dynamic networks and mobile networks is used number of times results of mobile users. In a mobile network mobile and prevent can use security data lose no. of modifications and remote finding this problem a two-layer network procedure is presented use simulating prevent propagation in Bluetooth and SMS. The two models is analyzed for controlling the mobile prevent propagation and change distribution methods taken on the techniques is autonomy-oriented computing (AOC). Then these method is not taken the hybrid prevent that disseminate i.e. both BT and SMS models. We introduce an innovative model called a Hybrid prevent detection model. The hybrid mobile can be distributed end-to-end messaging services in personal social communications and short-range wireless communication services it is increasingly the target of propagating prevent through the Bluetooth and Wi-Fi and security in mobile networks. In a mobile user and prevent security loss modify depletion of battery power remote models and accessing security short message and call history log An algorithm is design the extension power in a dynamic network with no use to redetect the community in the dynamic network which may significantly improve the security of assessment in a large-scale dynamic network.

Index Terms: Mobile networks AOC; Adaptive Dissemination; Bluetooth; SMS/MMS, Dynamic Network model.

Introductions

In the model of researchers prevent and security potential damages of user use different methods [4] are used to take the dynamic network of prevent propagation. Useful propagation methods are used to test different estimate the results of out supporting messages it applications in reality and use new improved methods[3] for restraining prevent propagation modern thinks there privies some models to characterize and predict the infection dynamics of mobile viruses. In the mobile computing, mobile phone security is an important research topic[4]. It is of particular concern as it associates to the security of personal information now accumulated on the Smart phone. Today most of the users and businesses utilize smart phones [1] [2] as communication tools but also as a means of planning and managing their work and private life. In the companies, these technologies are able to cause the profound modifications in the organization of the information[5] systems and consequently they have become the source of new risks. Definitely, smart phones gather and accumulate a growing amount of responsive information to which access must be inhibited to defend the isolation of the user and the intellectual property of the company[6].

In recent years, the worldwide market for smart phones has grown dramatically. Smartphone users can now perform many online tasks, including web browsing, document editing, multimedia streaming, Internet banking, and share the documents from one mobile to another through Bluetooth and SMS services[7]. Our work is aimed to gain further insights into how human behaviours affect the propagation mobile viruses and automatically detect and delete the malwares before enter into the mobile operating system based on the methodology of Autonomy-Oriented Computing (AOC) [13]. The recent research mobile network prevent propagation is divided number of models different researchers model the prevent propagation to find the stand points of a large-scale out source data to. Mobile network prevent propagation in a mobile network is different domains is biological prevent propagation four similar methods (susceptible-infected-susceptible method (SIS), susceptible-infected-recovered method (SIR)[8] susceptible-exposed infected-recovered method (SEIR), and susceptible-infected-Direc ted-removed method (SIDR)) used to describe biological prevent propagation and used dynamic network prevent propagation. There are two model life of research on mobile network changes
1. **Existing system:**

We introduce some virus defense methods [9] including abnormal detection technologies and patch dissemination strategies for restraining virus propagation in mobile networks. We incorporate related research on human mobility and operational behavior into our model in order to provide a computational model for characterizing and simulating the propagation dynamics of mobile viruses. The characteristics of mobility patterns described by our model are consistent with statistical results from the real-world.

### A. VIRUS DETECTION MODEL

In the existing research a two-layer network model is used for differentiating BT-based and SMS-based viruses, which proliferate via Bluetooth and Short/Multimedia Message Services correspondingly. In this model, instead of using the contact [10] probabilities in a homogeneous model, the viruses are triggered as a result of human behaviors. There are two categories of the human behavior: one is operational behavior and another one is mobile behavior considered in the individual-based model. The main objective of this work is to provide how the human behaviors concern the propagation dynamics of mobile viruses. This model considers the user behaviors in the mobile networks additionally [11] an adaptive dissemination strategy is designed by extending local reactive behaviors of entities. The objectives of this work are as follows:

- By using the two-layer network propagation model, to uncover some key factors in deciding mobile virus dissemination.
- The impacts of the operational patterns and mobility patterns are examined in the mobile virus dissemination.
- The two methods are investigated for preventing virus dissemination in mobile networks. There are two methods such as preimmunization and adaptive patch distribution strategies drawing on the methodology of AOC [12].

![MMS/SMS Model](image)

### B. HYBRID VIRUS DETECTION METHOD

In the research to increase the efficiency of the restraining the propagation of hybrid viruses, an innovative method is proposed which is called a Hybrid [13] virus detection model. A hybrid malware can develop both messaging and short-range wireless communication services to spread. It is essential to have a mathematical model by analyzing the mixed behaviors of long-range infectivity pattern from dissemination through messaging service and ripple-based infectivity pattern from propagating through short-range wireless communication. In this work, a new analytical model is proposed for examine the speed and harshness for dissemination the hybrid malware that targets SMS and BT in an efficient manner. This analytical model based on the differential equations works more effectually and it act as a quick reference to collect estimated knowledge of propagation speed and sternness of hybrid malwares with a variety of settings [14].

\[
I(t) + S(t) = I_{BT}(t) + I_{SMS}(t) + S(t) = N,
\]

and

\[
\frac{dI(t)}{dt} = \frac{dI_{BT}(t)}{dt} + \frac{dI_{SMS}(t)}{dt}
\]
HYBRID VIRUS DETECTION DESIGN

2. PROPOSED METHOD

In the system we are implementing a two layer network model for spreading virus through Bluetooth and SMS/MMS channel. The spreading of viruses is addressed by the operations of human behaviors such as mobile behavior and operational behavior [3] we examine two strategies to avoid virus in mobile phones Preimmunization and changes Dissemination strategies through the methodology of Autonomy-Oriented Computing (AOC) [1] In this method it can automatically detect the prevent before when virus enter into the smart phones [15]

1. AUTONOMY-ORIENTED COMPUTING

Autonomic computing alludes to the self-managing physical models of sharing computing resources, changes to irregular changes while beating existences difficulty to operators and users [13] this methods finally goal is to develop computer network size of admirations to overcome the efficient growing different waves of computing systems management and to decrease the obstacle that complexity stances to further growth The system makes conclusion on its own, using high-level policies;

it will constantly check and enhance its status and automatically modify itself to changing conditions. An autonomic computing framework is collected of autonomic components (AC) interacting with each other[16]

AUTONOMY-ORIENTED COMPUTING

2. Calculating prevent propagation power in dynamic network

It is difficulty evaluate the risk of prevent propagation number of security models in dynamic network models the network[17] size is large it is difficult to compute the propagation power of the entire network second the risk of prevent propagation changes number of times to the change of the network model a large amount of computation is required to same type the propagation risk after each change we propose a usably algorithm to compute the propagation power of security in large data dynamic networks based on dynamic community search algorithm which can speed model the propagation risk of virus in communicate network[16]

2.1. Add a new node Adding a new node in the network can modify commutations model two models for prevent the propagation power of the community has to calculating First when a new node is not connected to any different nodes in the network is added a new combinations is added to the dynamic network [18]

Algorithm 1 AddNode

Input : $F_t$ represented value of propagation Energy of the community in time t, and community structure and new node u

Output: $F_{t+1}$ represented the upload value of propagation energy of the community in time $t+1$ and the new community structure

If $(d_u == 0)$ then
    Remain $F_t$ unchanged
    Update $C^{t+1} = C^t \cup \{u\}$
Else
    Recalculated F for the community which u Join in
    Update $F_{t+1} = F_t + \Delta F$
Update \( C^{t+1} = (C^t \setminus C) \cup (C \cup \{U\}) \)
End if

### 2.2. Add a new edge
Adding the edge is different ways dependent on structures. We calculate the prevent propagation power of communications after each change which may one of the two different cases then the two nodes is connected a new edge number of the same community the new edge is add same commutations the two nodes is a new edge number of different communities a new internal edge is added which may cause two different models the original community model remains constant and keep the value of prevent propagation power[20]

**Algorithm 2 AddEdge**

**Input:** \( F_t \) represented value of propagation energy of the community intime t, and community structure and new edge u

**Output:** \( F_{t+1} \) represented the upload value of propagation energy

Of the community in time t+1 and the new community structure
If (\( C(i) \neq C(j) \)) then
Recalculate F for the community which I and j in
Update \( F_{t+1} = F_t + \Delta F \)
Else if (either I (or j) is one degree) then
Recalculate F for the community which changes
Update \( F_{t+1} = F_t + \Delta F \)
End if
Endif

### 2.3. Delete an edge
Compared above two cases removing an edge is less time. When an edge is deleted from the dynamic network model we calculate the prevent propagation power based on different models then two nodes of the edge delete different communities models the overall value of propagation power remains unchanged[21]

**Algorithm 3 DeleteEdge**

**Input:** \( F_t \) represented value of propagation energy of the community time t, and community structure and edge u to be removed

**Output:** \( F_{t+1} \) represented the uploaded value of propagation energy of the community in time t+1 and the new community structure

K=1:
If (node 1’s degree is 1)
\( C^{t+1} = C \setminus C(i) \cup (C(i) \cup \{i\}) \)
Else
While (\( N(i) \) is not empty) do
\( S(k) = \{ \text{nodes have connection with nodes which don’t in } C(i) \} \)
K=k+1:
Endwhile
End if

Let every S(i) Consider its best communities:
Recalculate F for all the communities changes
Update \( F_{t+1} = F_t + \Delta F \)
Update C^{t+1}

### 4. Relationship between propagation power and virus infection
The prevent propagation speed of expertly we change the relationship two propagation speed \( \nu \) and prevent propagation power \( F \) in basic model is firstly use three basic models as input of graph G to take the corresponding prevent propagation speed \( \nu \) and these calculate the corresponding propagation power \( F \).
then to simplify the simulation the time taken for a node to infect another node is take this assumption different results.[23]

3. CONCLUSION
A two-layer network model is used for replicating and analyzing the propagation dynamics of SMS-based and BT-based viruses to alleviate the viruses and malwares in the mobile networks. This model characterizes two categories of the human behaviors: such as operational behavior and mobile behavior for examining and uncovering the propagation mechanisms of mobile viruses the virus content of data’s enter into the smart phones through Bluetooth and SMS channels it automatically filter the virus and data separately and delete the virus but not the data we propose the new concept of prevent propagation power quality risk of eatery propagation is influenced by dynamic network model Preventive model is taken advance

4. Future work
To next generations to improve the proposed models dependents should be made to improve the algorithm for computing prevent propagation power so that the efficiency of calculation can increase without compromising the accuracy This is support in android smart phones and efficiently detect and delete the virus of the content before enter into the mobile operating system This method is based on the differential equations works more resourcefully and could act as a speedy reference to collect estimated knowledge of propagation speed and sterness of hybrid mobiles with different of settings of contagion results and average node degrees is generated social network.

7. REFERENCES


