Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2013, Article ID 896187, 13 pages
http://dx.doi.org/10.1155/2013/896187

Research Article

An Efficient Patch Dissemination Strategy for Mobile Networks

Dawei Zhao,[1,2] Haipeng Peng,[1,2] Lixiang Li,[1,2] Yixian Yang,[1,2] and Shudong Li[3]

[1] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2] *National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[3] *College of Mathematics and Information Science, Shandong Institute of Business and Technology, Shandong, Yantai 264005, China*

Correspondence should be addressed to Haipeng Peng; penghaipeng@bupt.edu.cn

Received 8 June 2013; Accepted 5 July 2013

Academic Editor: Ming Li

Mobile phones and personal digital assistants are becoming increasingly important in our daily life since they enable us to access a large variety of ubiquitous services. Mobile networks, formed by the connection of mobile devices following some relationships among mobile users, provide good platforms for mobile virus spread. Quick and efficient security patch dissemination strategy is necessary for the update of antivirus software so that it can detect mobile virus, especially the new virus under the wireless mobile network environment with limited bandwidth which is also large scale, decentralized, dynamically evolving, and of unknown network topology. In this paper, we propose an efficient semi autonomy-oriented computing (SAOC) based patch dissemination strategy to restrain the mobile virus. In this strategy, some entities are deployed in a mobile network to search for mobile devices according to some specific rules and with the assistance of a center. Through experiments involving both real-world networks and dynamically evolving networks, we demonstrate that the proposed strategy can effectively send security patches to as many mobile devices as possible at a considerable speed and lower cost in the mobile network. It is a reasonable, effective, and secure method to reduce the damages mobile viruses may cause.

1. Introduction

The last decade has witnessed a surge of wireless mobile devices such as mobile phones, PocketPCs, netbooks, and tablet PCs. With the appearance and development of intelligent operating system, mobile devices are getting smarter and more functional. For example, they can connect to the Internet, receive and send emails and short messages (SMS)/multimedia messages (MMS), and connect to other devices for exchanging information and activating various applications. Meanwhile, these mobile devices also become the ideal targets of mobile virus because they are popular, designed to be open, programmable, and, general of purpose, and highly dependent on common software platforms such as Android, Symbian, Windows Mobile, and Linux.

Mobile networks, formed by the connection of mobile devices following some relationships among mobile users, provide good platforms for mobile virus spread. For example, an MMS-based worm named "Commwarrior" (http://www.f-secure.com/v-descs/commwarrior.shtml) can spread in MMS network which is formed based on the social relationships among mobile users. And a Bluetooth-based worm named "Cabir" (http://www.f-secure.com/v-descs/cabir.shtml) can spread in Bluetooth network which is formed according to the geographically positions of mobile devices. There have been extensive studies on modeling the virus/epidemic propagation [1–6] in complex networks which can be used to estimate the scale of a virus/epidemic outbreak before it actually occurs and evaluate the effect of new or improved countermeasures in restraining virus/epidemic propagation. And based on these studies, many network immunization strategies [7–10] have been proposed for restraining virus propagation by selectively immunizing some nodes based on the measurements of degree or betweenness. But it would be difficult for these strategies to deal with large-scale, decentralized, and dynamic

mobile networks. Intrusion detection technology [11] is another straight and effective means for the containment of mobile virus. However, the detection capabilities of most antivirus software are depend on the existence of an updated virus signature repository. Antivirus users are not protected whenever an attacker spreads a previously never encountered virus. In order to protect the mobile phones from the damage of new virus, service providers or security companies need to quickly identify the new virus, generate a signature, and disseminate patches to smart phones. Currently, most researches have been done on intrusion detection [11–13] and patch generation [14–16], while this paper aims to study the dissemination [17–20] of security patch in the wireless mobile network environment.

Due to the limited bandwidth of wireless networks, it is difficult to disseminate the security patches to all phones simultaneously and timely. And since the mobile network is always large-scale, decentralized, dynamically, and of unknown network topology, good patch dissemination strategy is necessary. Some strategies attempt to forward security notifications or patches based on the short-range communication capabilities of intermittently connected phones [17, 18]. These strategies select some important phones that can divide a Bluetooth-based network into different communities based on the contact time and frequency. Thereafter, they send security signatures to all communities based on the local detection. However, this method cannot ensure that users acquire patches in time. References [20, 21] presented a quick and efficient autonomy-oriented computing (AOC) [22, 23] based patch dissemination strategy, based on SMS that can be used in multiple forms of mobile network. But, this strategy still has the following deficiencies: (1) the number of patches disseminated is not determined at a time step. Especially, there may be many patches disseminated at the initial stage which can potentially cause network congestion [24, 25]; (2) a phone may receive the same patch from different neighbors more than once which may lead to network congestion and the waste of network resource. Therefore, it is still in high demand to develop a new strategy that can efficiently and quickly send security patches to as many phones as possible in the mobile network.

In this paper, we propose a patch dissemination strategy based on semi autonomy-oriented computing (SAOC) to restrain the mobile virus. For the AOC-based strategy, certain entities reside in some phones in the mobile network. They autonomously work with each other and move in the network based on their own autonomous behaviors. But in our SAOC-based strategy, a center is added to the AOC-based strategy to combine and analyze the information received from the entities. At each time step, each entity moves to the next location according to its own autonomous behavior and the information feedbacked from the center. Through many experiments involving both synthetic and real-world networks, we find that the proposed SAOC-based strategy can quickly send security patches to as many phones as possible in the mobile network with limited bandwidth which is also large-scale, decentralized, dynamically, and of unknown network topology. Besides, it can control the number of patches disseminated at each time step and make adjustment according to the network conditions. The selected phones, which receive the patches, are always the most important ones of the phones found by the entities at each time step for the virus propagation, and thus the virus propagation can be effectively restrained. The network congestion and the waste of the network resources can also be avoided because each phone receives the patch only once.

2. SAOC-Based Patch Dissemination Strategy

SMS/MMS messages and Bluetooth are becoming the two major propagation routes of mobile virus. Since SMS-based viruses are found more dangerous than Bluetooth-based viruses in terms of propagation speed and scope [20], we propose a semi autonomy-oriented computing (SAOC) based patch dissemination strategy to restrain the SMS-based virus propagation in this paper. For the autonomy-oriented computing (AOC) approach [20, 26], a group of computational entities are dispatched into a mobile network. They reside in some phones, autonomously work with each other, move from one phone to another, and update their local environment based on their own autonomous behaviors. However, in our SAOC-based approach, the entities no longer work full autonomously and a center is added to help the entities finish their tasks. At each time step, the center is responsible for combining and analyzing the information received from the entities, and each entity moves from its present position to a new one according to some rules, the information feedbacked from the center and the cooperation with other entities. We use a graph G to denote the mobile phones network formed according to the address books of mobile phones. Some definitions which are used to formulate the SAOC-based dissemination strategy are as follows.

Definition 1. A graph $G = \langle V, L\rangle$ is a mobile network formed according to the address books of mobile phones, where $V = \{v_1, v_2, \ldots, v_N\}$ is a set of phones and $L = \{\langle v_i, v_j\rangle | 1 \le i, j \le N, i \ne j\}$ is a set of undirected links (if v_i is in the address book of v_j, then there is a link between v_i and v_j, and v_i is called a friend of v_j). $N = |V|$ represents the total number of phones in the network.

Each phone v_i in G has two states $\langle phoneId, all\ friendIds\rangle$, where $phoneId$ denotes the identifier of v_i and $friendId$ is the identifier of the friend of v_i.

Definition 2. The center, denoted by C, contains two states $\langle id, task\rangle$, where id denotes its identifier and $task$ stores a series of its tasks.

Definition 3. Let e be an entity in a network G. Entity e is represented by a tuple $\langle id, phoneId, all\ friendIds, lifecycle, rule\rangle$, where id denotes the identifier of the entity; $phoneId$ represents the identifier of the phone resided by e; $friendId$ is the identifier of the friend of the resided phone; $lifecycle$ is the maximum time steps for an entity to reside on a phone; and $rule$ is a set which stores four local behaviors of an entity, including rational-move, rational-jump, random-jump, and wait.

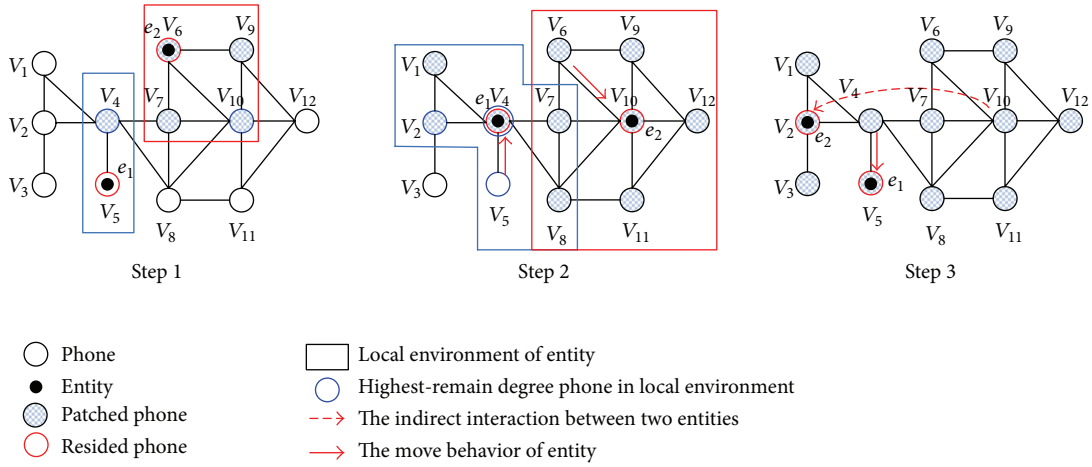


Figure 1: An example of the SAOC-based patch dissemination strategy.

Definition 4. The local environment and prelocal information of an entity are denoted by E_l and $preI_l$, respectively. If an entity e resides on phone v_i, its local environment and prelocal information are defined as $E_l(e) = \{v_i; \{v_j\}\}$ and $preI_l(e) = \{v_i's\ id\ \&\ v_i's\ all\ friendIds; \{v_j's\ id\ \&\ v_j's\ all\ friendIds\}\}$ respectively, where $\{v_j\}$ is the set of friends of v_i.

Definition 5. Remain degree of a phone denotes the number of friends who have not received the patches of a phone. A phone is regarded as its own friend.

At each time step, each entity sends its prelocal information searched in its local environment to the center. The center combines and analyzes the information received from all entities according to its *task*, and shares the analysis results which are called the postlocal information $postI_l(e)$ with each entity e, where $postI_l(e) = \{v_i's\ id\ \&\ v_i's\ remain\ degree; \{v_j's\ id\ \&\ v_j's\ remain\ degree\}\}$, $\{v_j\}$ is the set of friends of v_i resided by e. If two phones resided by two entities are friends or they have at least a same friend, we assume that these two entities can share their postlocal information. Each entity then moves to the next location (*targetId*) according to its *rule*. Algorithm 1 shows the detailed process of SAOC-based patch dissemination strategy.

The *task* of the center includes the following.

(1) Delete the *friendIds* who have received the patches from each phone's *all friendIds* in all the prelocal information.

(2) Compute each phone's remain degree and send the security patches to the first m phones with the highest-remain degree. (Therefore, the number of patches disseminated at each time step is controllable that can be adjusted according to the network conditions.) And record the *ids* of the phones who just received the patches.

(3) Delete the new patched *friendIds* from each phone's *all friendIds* and compute each phone's new remain degree.

(4) Send the postlocal information to the entity.

The main behaviors of each entity are as follows.

(1) Rational move: An entity moves to a phone with the highest-remain degree in its postlocal information or the shared postlocal information if it exists. If there exists more than one highest-remain degree phone, the entity will randomly choose one for residing in.

(2) Rational jump: the entity requests from the center a phone for residing in, if such phone exists.

(3) Random jump: an entity moves along the edges with a randomly-determined number of steps in order to avoid getting stuck in local optima.

(4) Wait: If an entity does not find any available phone for residing in, it will stay at its current position.

For example, as shown in Figure 1, two entities e_1 and e_2 reside in phones v_5 and v_6 at the initial phase of step 1, respectively. e_1 and e_2 begin to search their local environments and obtain the prelocal information as:

$$preI_l(e_1) = \{v_5\ \&\ v_5, v_4; \{v_4\ \&\ v_4, v_1, v_2, v_5, v_7, v_8\}\},$$

$$preI_l(e_2) = \{v_6\ \&\ v_6, v_7, v_9, v_{10}; \{v_7\ \&\ v_7, v_4, v_6, v_8, v_{10}; v_9\ \&\ v_9, v_6, v_{10}, v_{12}; v_{10}\ \&\ v_{10}, v_6, v_7, v_8, v_9, v_{11}, v_{12}\}\}. \quad (1)$$

When receiving $preI_l(e_1)$ and $preI_l(e_2)$, the center firstly deletes the phones' *id* that has been immunized from each phones' *friendIds* and computes the remain degree of each phone. Since there are no phones have been immunized, the remain degree of each phone will be $\{v_4\ \&\ 6; v_5\ \&\ 2; v_6\ \&\ 4; v_7\ \&\ 5; v_9\ \&\ 4; v_{10}\ \&\ 7\}$. In this

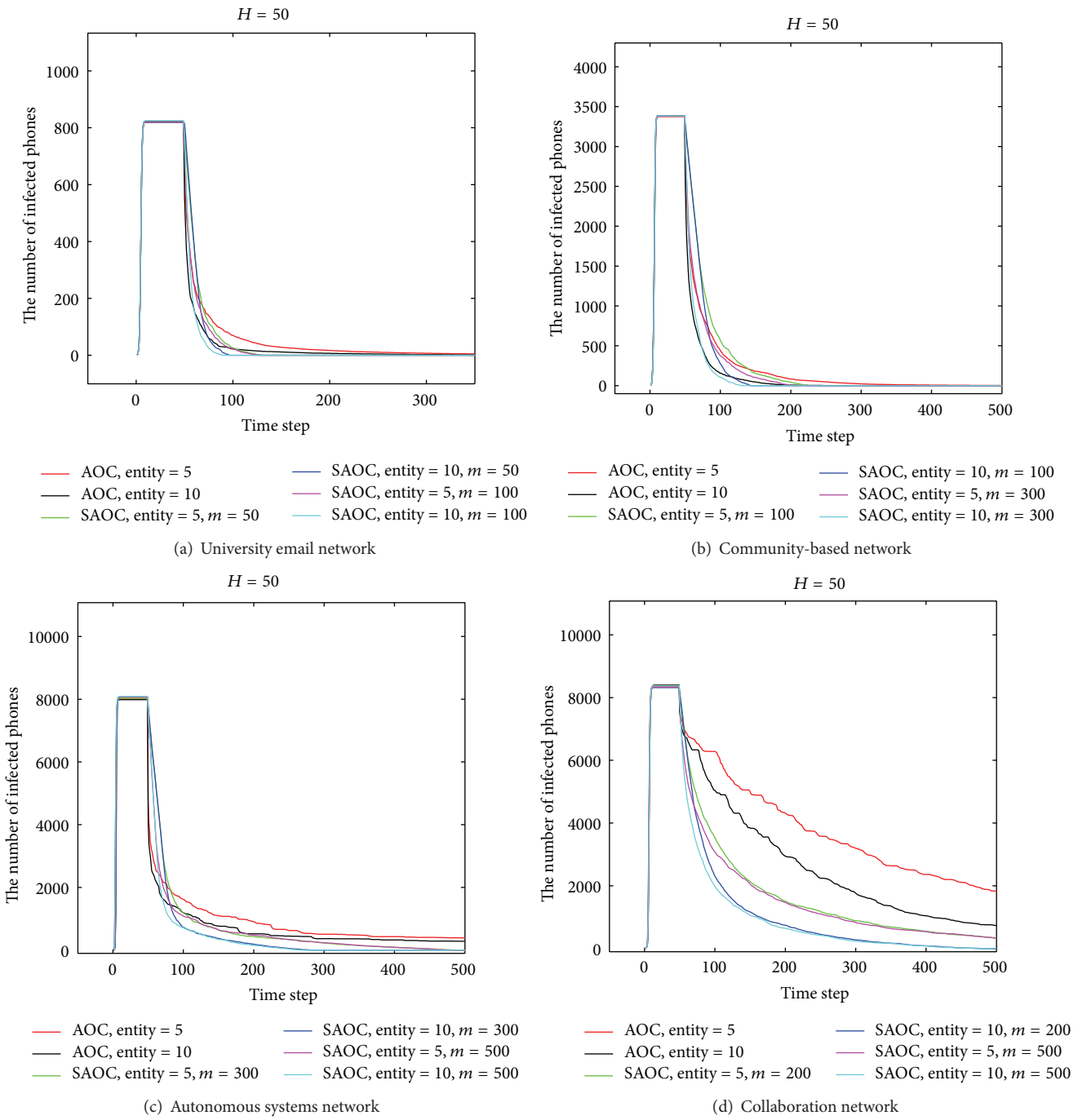


Figure 2: The number of infected phones over time.

moment, the center sends the security patches to the first 5 unimmunized phones (in this example, we assume that no more than $m = 5$ phones are immunized at each time step) with highest-remain degree, that is, $\{v_4, v_6, v_7, v_9, v_{10}\}$, and deletes these phones' *id* from each phones' *friendIds* and computes the new remain degree of each phone. The new remain degree will be sent to entities as their postlocal information, that is, $postI_l(e_1) = \{v_5 \,\&\, 1; \{v_4 \,\&\, 4\}\}$ and $postI_l(e_2) = \{v_6 \,\&\, 0; \{v_7 \,\&\, 1; v_9 \,\&\, 1; v_{10} \,\&\, 3\}\}$. When receiving the postlocal information, each entity will move to the phone which has the highest-remain degree in its postlocal information. Therefore, e_1 and e_2 move from v_5 to v_4 and from v_6 to v_{10}, respectively. In this step, these two entities perform the rational move relying on their own postlocal information. Step 2 will show the case of the movement of the entities relying on the shared postlocal information. In step 2, when e_1 and e_2 receive $postI_l(e_1)$ and $postI_l(e_2)$ from the center, they can share their postlocal

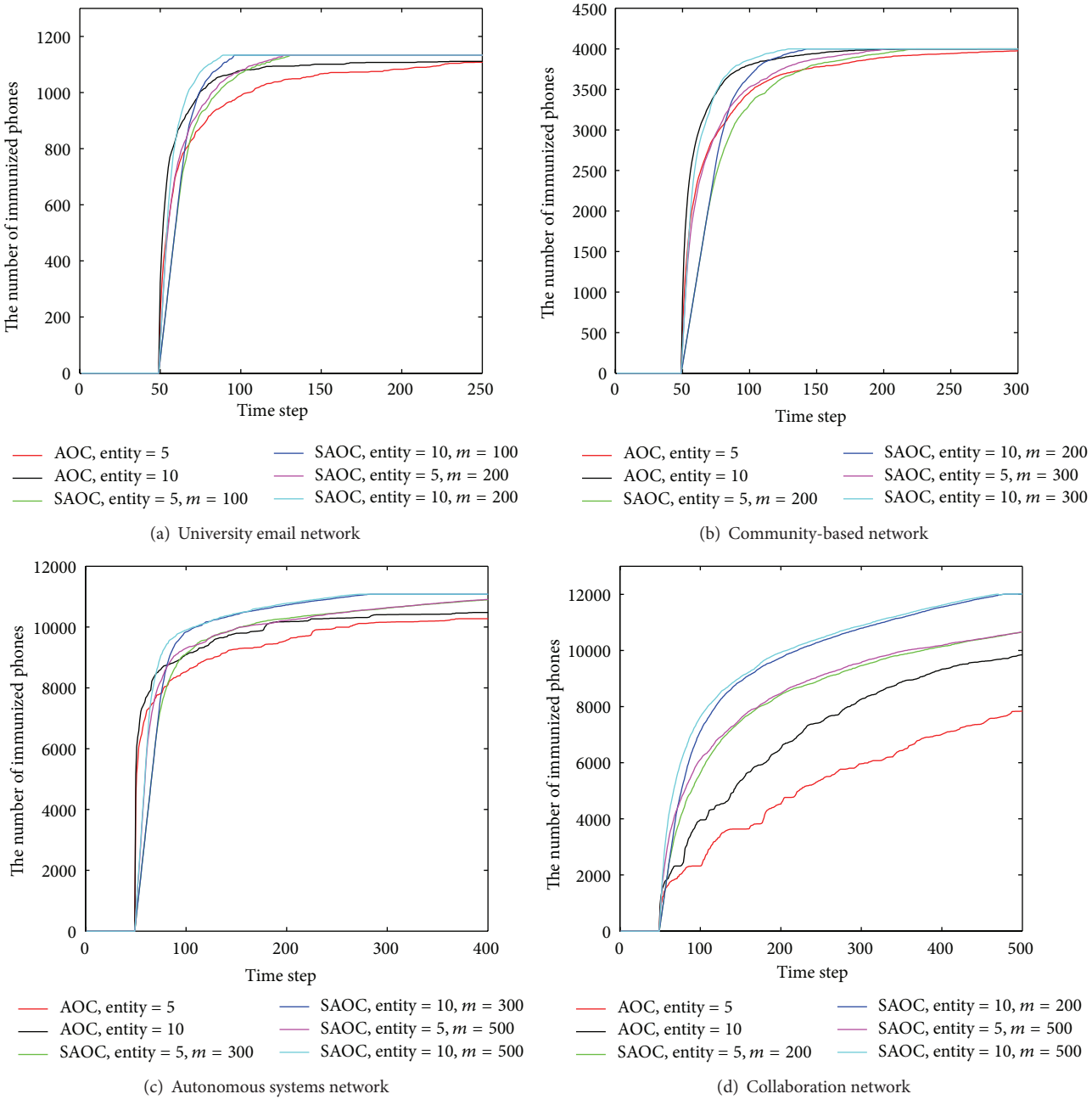


FIGURE 3: The number of immunized phones over time.

information with each other since they have the mutual friends v_7 and v_8. $postI_l(e_1)$, $postI_l(e_2)$ and the shared postlocal information are as follows:

$$postI_l(e_1) = \{v_4 \,\&\, 1; \{v_1 \,\&\, 0; v_2 \,\&\, 1; v_5 \,\&\, 1; v_7 \,\&\, 0; v_8 \,\&\, 0\}\},$$

$$postI_l(e_2) = \{v_{10} \,\&\, 0; \{v_6 \,\&\, 0; v_7 \,\&\, 0; v_8 \,\&\, 0; v_9 \,\&\, 0; v_{11} \,\&\, 0; v_{12} \,\&\, 0\}\},$$

$$postI_l(e_1) \cup postI_l(e_2) = \{v_1 \,\&\, 0; v_2 \,\&\, 1; v_4 \,\&\, 1; v_5 \,\&\, 1; v_6 \,\&\, 0; v_7 \,\&\, 0; v_8 \,\&\, 0; v_9 \,\&\, 0; v_{10} \,\&\, 0; v_{11} \,\&\, 0; v_{12} \,\&\, 0\}. \quad (2)$$

e_1 and e_2 will choose the first two phones with the highest-remain degree in the shared postlocal information as their target locations. Note that there are three phones can be resided and e_1 is residing in one of the highest-remain degree phone. In this case, we let e_1 continue from

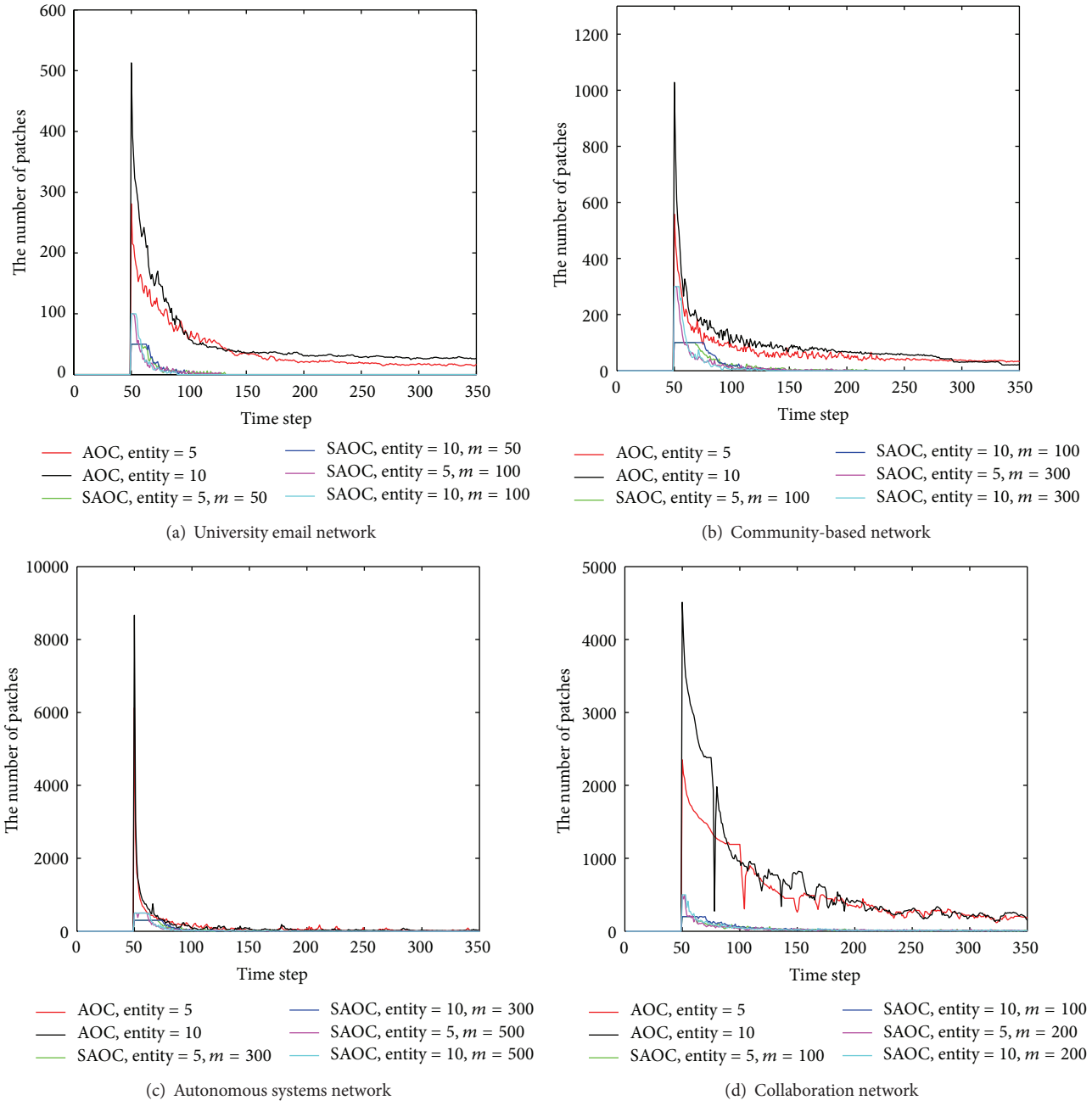


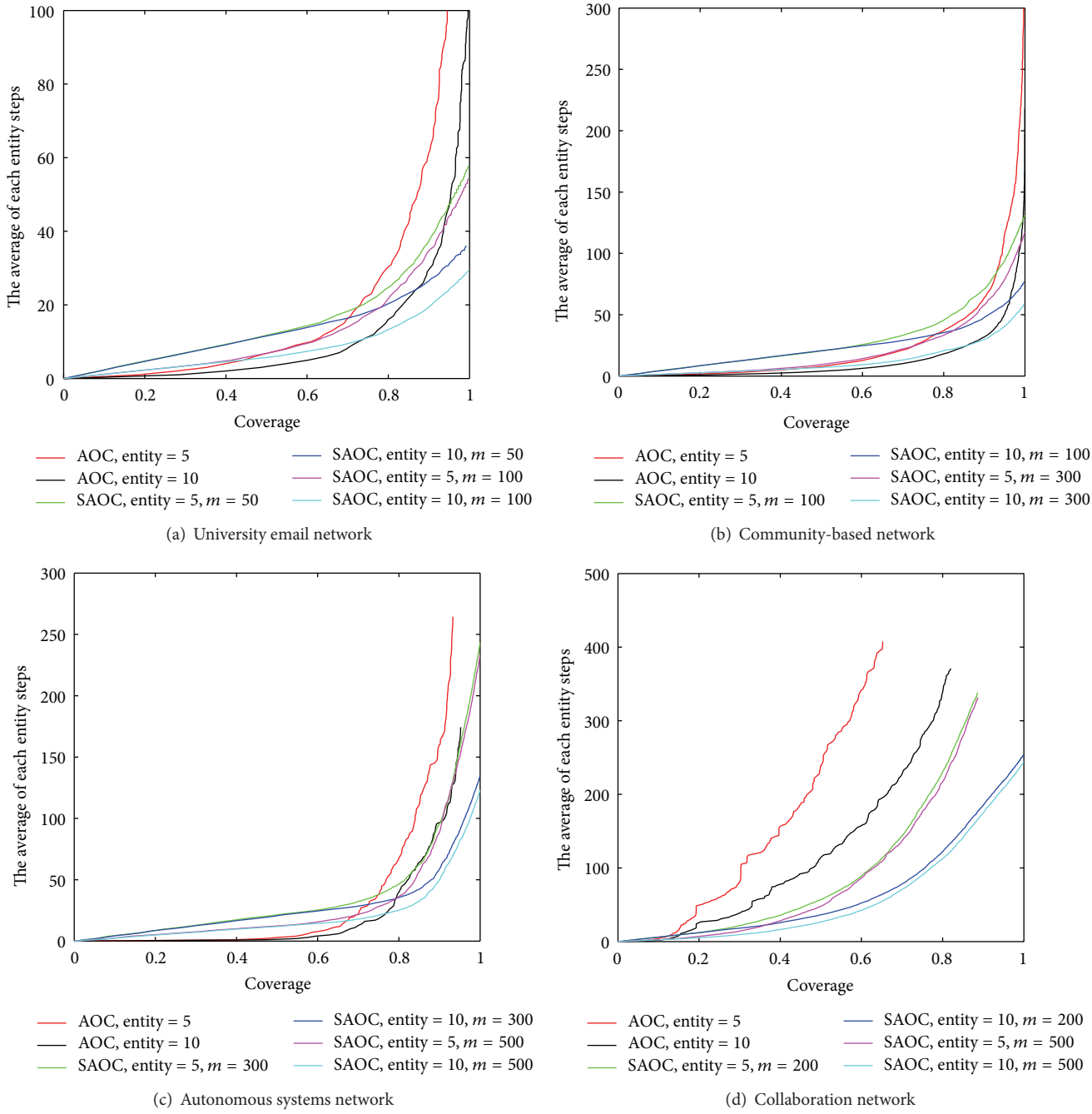
Figure 4: The number of patches over time.

moving. Therefore, e_1 and e_2 move from v_4 to v_5 and v_{10} to v_2, respectively. Table 1 presents the detailed patch dissemination process of Figure 1 based on our SAOC-based patch dissemination strategy.

3. Experimentation and Validation

3.1. Static Networks. A mobile network is constructed based on the address books of smart phones, which reflects the social relationship among mobile users in real world situations. Here, we use some benchmark networks (university email network, autonomous systems network, and collaboration network) to reflect the relationship structures in the real world. Table 2 shows the structure and degree of four networks. University email network [27], autonomous systems network [28], and collaboration network of Arxiv High Energy Physics category [29] are real-world networks. Community-based network is a synthetic network with four communities based on the GLP algorithm [30].

We use the four networks shown in Table 2 to evaluate the efficiency of the proposed SAOC-based patch dissemination strategy in restraining the SMS-based virus. For the SMS-based virus propagation model, we assume the following.



(a) University email network

(b) Community-based network

(c) Autonomous systems network

(d) Collaboration network

FIGURE 5: The average of each entity steps with respect to coverage rate.

(1) If a user receives a message from his friend, he may open or delete this message determined by his security awareness [20, 31, 32]. The security awareness of different users in this paper is consistent with that used by [20] and follows a normal distribution, $N(0.5, 0.3^2)$.

(2) If a user opens a virus message, he is infected and will automatically send the virus message to all his friends.

(3) An infected phone sends the virus to his friends only once, after which the infected phone will not send out virus any more.

(4) If a phone has received the patch, it will not send out virus even if the user opens an infected message again.

At some point, we deploy a few entities into a mobile network. These entities reside in the phones with the highest degree which are found by the AOC-based immunization strategy [26]. Each entity then moves according to

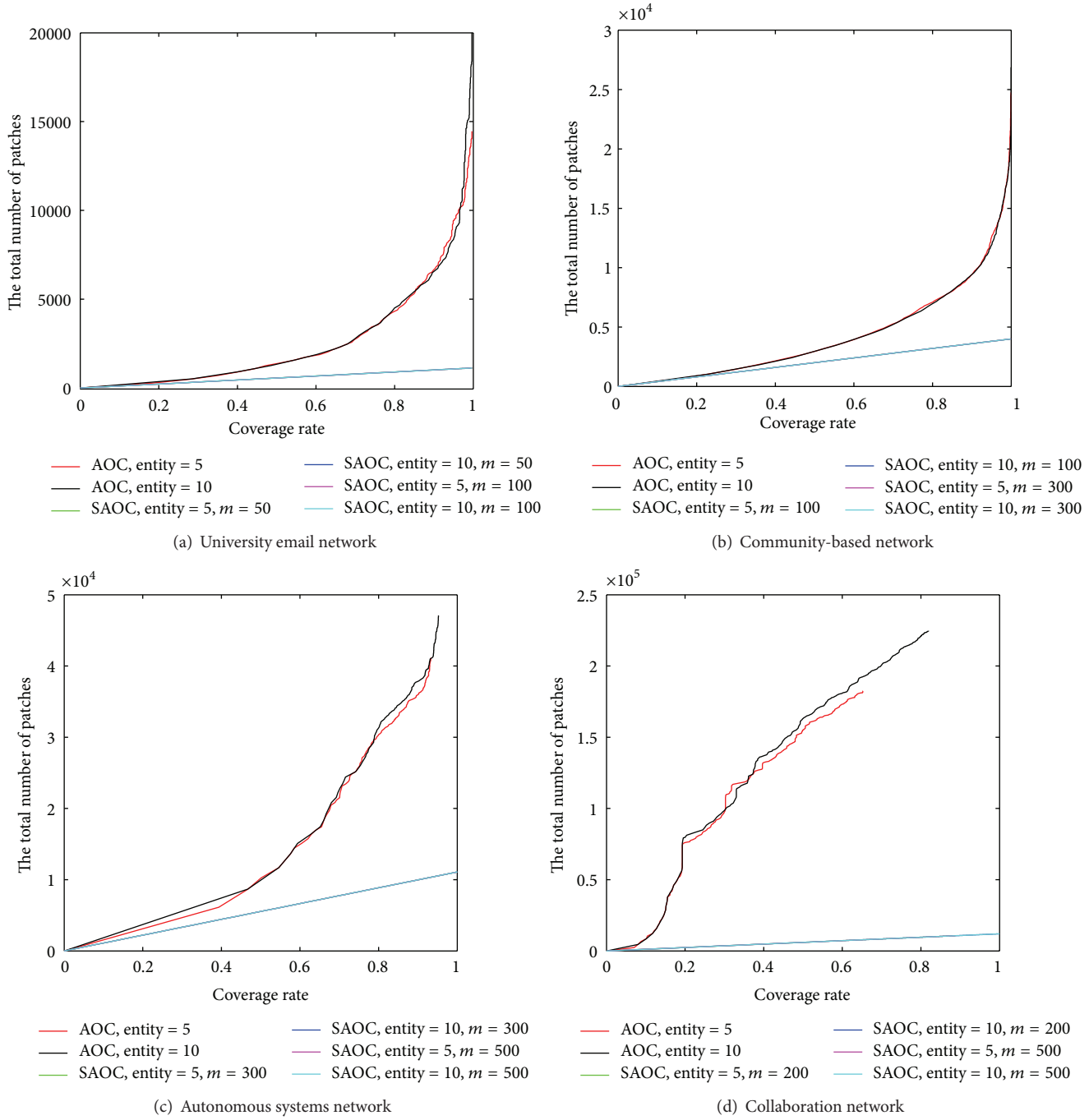


Figure 6: The number of patches with respect to coverage rate.

Algorithm 1. We compare the efficiency of our SAOC-based dissemination strategy with the AOC-based dissemination strategy [20] by different indexes in the above static benchmark networks.

Figure 2 shows the average numbers of infected phones over time when 5 and 10 entities are deployed into the networks from the time step of 50. At each time step, no more than m patches can be sent in SAOC-based strategy that is, up to m phones can be immunized at each time step in SAOC-based strategy. Obviously, the earlier and the more the patch is disseminated, the shorter the propagation duration will be. Figure 3 shows the average number of immunized phones over time when the entities are deployed into the networks from 50. Since we set a limit on the size of m to avoid the network congestion, the effect of SAOC-based strategy is inferior to the AOC-based one at the initial phase after the deploying of the entities when m is small. But simulation results show that the SAOC-based strategy can recover all the

```
(1) For each entity e
        search the local environment E_l(e) and obtain pre-local information preI_l(e);
        send preI_l(e) to the center;
    End
(2) For center C
        perform a series of task according to its task;
    End
(3) For each entity e
        compute targetId based on the post-local information or the shared post-local information;
        If targetId is not null Then
            Rational move to targetId;
        Else if e.lifecycle < 1 Then
            request the center a targetId;
            If receive a targetId Then
                Rational jump to targetId;
            Else if not receive a targetId Then
                Random jump to targetId;
        Else
            Wait;
        End
    End
```

Algorithm 1: The process of SAOC-based patch dissemination strategy.

infected phones and immune all the phones faster than the AOC-based one even if m is relatively small. Figure 4 shows the number of the patches disseminated at each time step. We find that the number of the patches disseminated at each time step in AOC-based strategy is much more than that of the SAOC-based one. Figure 4 also shows the main inadequacies of AOC-based strategy; that is, too many patches are sent at certain times which may lead to network congestion and a phone may receive the patch from different neighbors more than once which causes the waste of network resources. However, in our SAOC-based strategy, the number of patches disseminated at each time step is controllable that can be adjusted according to the network conditions, and a phone receives the patch only once.

Figures 5 and 6 show the average number of steps of each entity and the total number of patches disseminated corresponding to the coverage rate, respectively. The coverage rate is defined as $N_{\text{immunized}}/N$, where $N_{\text{immunized}}$ represents the total number of immunized phones that are patched by the center and N represents the total number of phones in the network. In Figure 5, each entity in SAOC-based strategy needs to move a bit more steps than that in the AOC-based strategy when the coverage rate is small due to the limitation on m. But in the case of achieving a significant amount of coverage rate, the number of steps of each entity needed to move is much smaller in SAOC-based strategy than that in AOC-based strategy. In Figure 6, we can see that the total number of patches disseminated is much smaller in SAOC-based strategy than in AOC-based strategy to attain the same coverage rate.

From the simulations performed above, we can see that the SAOC-based dissemination strategy can efficiently send security patches to as many phones as possible with considerable speed and relatively lower cost in the static networks.

3.2. Dynamically Evolving Networks. In this section, we evaluate the efficiency of SAOC-based dissemination strategy in dynamically evolving networks since the structure of a network is changing in the real world. We assume that the initial network contains 1000 phones with $\langle k \rangle = 8$. Three different patterns of network evolving are considered as follows: (1) the network scale will grow to 4000; (2) 50 or 100 phones are added into the network at each step from the time step of 20; (3) the network degree, $\langle k \rangle$, will remain unchanged or change from 8 to 18, respectively. We use the SIR [33–35] model to characterize the SMS-based virus propagation in dynamically evolving networks. SIR is the most basic and well-studied epidemic spreading model. In the SIR model, the elements of a network are divided into three compartments, including susceptibles (S, those who can contract the infection), infectious (I, those who have contracted the infection and are contagious), and recovered (R, those who have recovered from the disease). At each time step, we assume that a susceptible phone becomes infected with a probability λ if it is directly connected to an infected phone. Meanwhile, if an infected phone receives the patch, it will become to be recovered from the infected state.

Simulation results shown in Figure 7 indicate that when selecting the appropriate number of patches disseminated at each time step, our SAOC-based strategy can send security patches to as many phones as possible and reduce the damages of mobile virus in the dynamically evolving networks with various complex evolving patterns.

4. Conclusion

In this paper, we propose an efficient SAOC-based patch dissemination strategy to restrain the SMS-based mobile

Table 1: The detailed process of Figure 1 based on SAOC-based patch dissemination strategy.

Entity ⟶	**Center**	⟶ **Entity**	
Pre-local information	Analytical information	Post-local information	Movement
Step 1:			
Entity e_1:		**Entity** e_1:	
V_5 & V_5, V_4	V_4 & $V_4, V_1, V_2, V_5, V_7, V_8$ & 6 & 4	V_5 & 1	$e_1: V_5 \to V_4$
V_4 & $V_4, V_1, V_2, V_5, V_7, V_8$ ⟶	V_5 & V_5, V_4 & 2 & 1	V_4 & 4 ⟶	
Entity e_2:	V_6 & V_6, V_7, V_9, V_{10} & 4 & 0	**Entity** e_2:	
V_6 & V_6, V_7, V_9, V_{10}	V_7 & $V_7, V_4, V_6, V_8, V_{10}$ & 5 & 1	V_6 & 0	
V_7 & $V_7, V_4, V_6, V_8, V_{10}$	V_9 & V_9, V_6, V_{10}, V_{12} & 4 & 1	V_7 & 1	$e_2: V_6 \to V_{10}$
V_9 & V_9, V_6, V_{10}, V_{12}	V_{10} & $V_{10}, V_6, V_7, V_8, V_9, V_{11}, V_{12}$ & 7 & 3	V_9 & 1	
V_{10} & $V_{10}, V_6, V_7, V_8, V_9, V_{11}, V_{12}$ ⟶	Store immune phones: $V_4, V_6, V_7, V_9, V_{10}$	V_{10} & 3 ⟶	
Step 2:			
Entity e_1:		**Entity** e_1:	
V_4 & $V_4, V_1, V_2, V_5, V_7, V_8$	V_1 & V_1, V_2, V_4 & 2 & 0	V_4 & 1	
V_1 & V_2, V_1, V_4	V_2 & V_2, V_1, V_3, V_4 & 3 & 1	V_1 & 0	
V_2 & V_1, V_2, V_3, V_4	V_4 & $V_4, V_1, V_2, V_5, V_7, V_8$ & 4 & 1	V_2 & 1	
V_5 & V_5, V_4	V_5 & V_5, V_4 & 1 & 1	V_5 & 1	e_1 and e_2 share their post-local informations, then $e_1: V_4 \to V_5$ $e_2: V_{10} \to V_2$
V_7 & $V_7, V_4, V_6, V_8, V_{10}$	V_6 & V_6, V_7, V_9, V_{10} & 0 & 0	V_7 & 0	
V_8 & $V_8, V_4, V_7, V_{10}, V_{11}$ ⟶	V_7 & $V_7, V_4, V_6, V_8, V_{10}$ & 1 & 0	V_8 & 0 ⟶	
Entity e_2:	V_8 & $V_8, V_4, V_7, V_{10}, V_{11}$ & 2 & 0	**Entity** e_2:	
V_{10} & $V_{10}, V_6, V_7, V_8, V_9, V_{11}, V_{12}$	V_9 & V_9, V_6, V_{10}, V_{12} & 1 & 0	V_{10} & 0	
V_6 & V_6, V_7, V_9, V_{10}	V_{10} & $V_{10}, V_6, V_7, V_8, V_9, V_{11}, V_{12}$ & 3 & 0	V_6 & 0	
V_7 & $V_7, V_4, V_6, V_8, V_{10}$	V_{11} & $V_{11}, V_8, V_{10}, V_{12}$ & 3 & 0	V_7 & 0	
V_8 & $V_8, V_4, V_7, V_{10}, V_{11}$	V_{12} & $V_{12}, V_9, V_{10}, V_{11}$ & 2 & 0	V_8 & 0	
V_9 & V_9, V_6, V_{10}, V_{12}	Store immune phones: $V_1, V_2, V_4, V_6, V_7, V_8, V_9, V_{10}, V_{11}, V_{12}$	V_9 & 0	
V_{11} & $V_{11}, V_8, V_{10}, V_{12}$		V_{11} & 0	
V_{12} & $V_{12}, V_9, V_{10}, V_{11}$ ⟶		V_{12} & 0 ⟶	
Step 3:			
Entity e_1:		**Entity** e_1:	
V_2 & V_2, V_1, V_3, V_4	V_1 & V_2, V_1, V_4 & 0 & 0	V_2 & 0	
V_1 & V_2, V_1, V_4	V_2 & V_2, V_1, V_3, V_4 & 1 & 0	V_1 & 0	
V_3 & V_3, V_2	V_3 & V_3, V_2 & 1 & 0	V_3 & 0	
V_4 & $V_4, V_1, V_2, V_5, V_7, V_8$ ⟶	V_4 & $V_4, V_1, V_2, V_5, V_7, V_8$ & 1 & 0	V_4 & 0 ⟶	end
Entity e_2:	V_5 & V_5, V_4 & 1 & 0	**Entity** e_2:	
V_5 & V_5, V_4	Store immune phones: $V_1, V_2, V_3, V_4, V_5, V_6, V_7, V_8, V_9, V_{10}, V_{11}, V_{12}$	V_5 & 0	
V_4 & $V_4, V_1, V_2, V_5, V_7, V_8$ ⟶		V_4 & 0 ⟶	

In the analytical information v_i & $v_{j1}, \ldots, v_{jk}$ & n_1 & n_2 of the center, v_i is the identifier of a phone, $v_{j1}, \ldots, v_{jk}$ the friends of v_i, n_1 the first computed remain degree of v_i, and n_2 the second computed remain degree of v_i. The identifiers in red indicate the phones that have received the patches in the previous steps. The identifiers in blue indicate the phones that will receive the patches in the current step. The no more than 5 red numbers in each step refers to the unimmunized phones with the highest-first computed remain degree.

virus. The advantages of our SAOC-based strategy could be described as follows:

(1) it sends security patches to as many phones as possible at a considerable speed and lower cost in the mobile network with limited bandwidth which is also large-scale, decentralized, dynamically evolving, and of unknown network topology;

(2) it can control the number of patches disseminated at each time step and make adjustment according to the

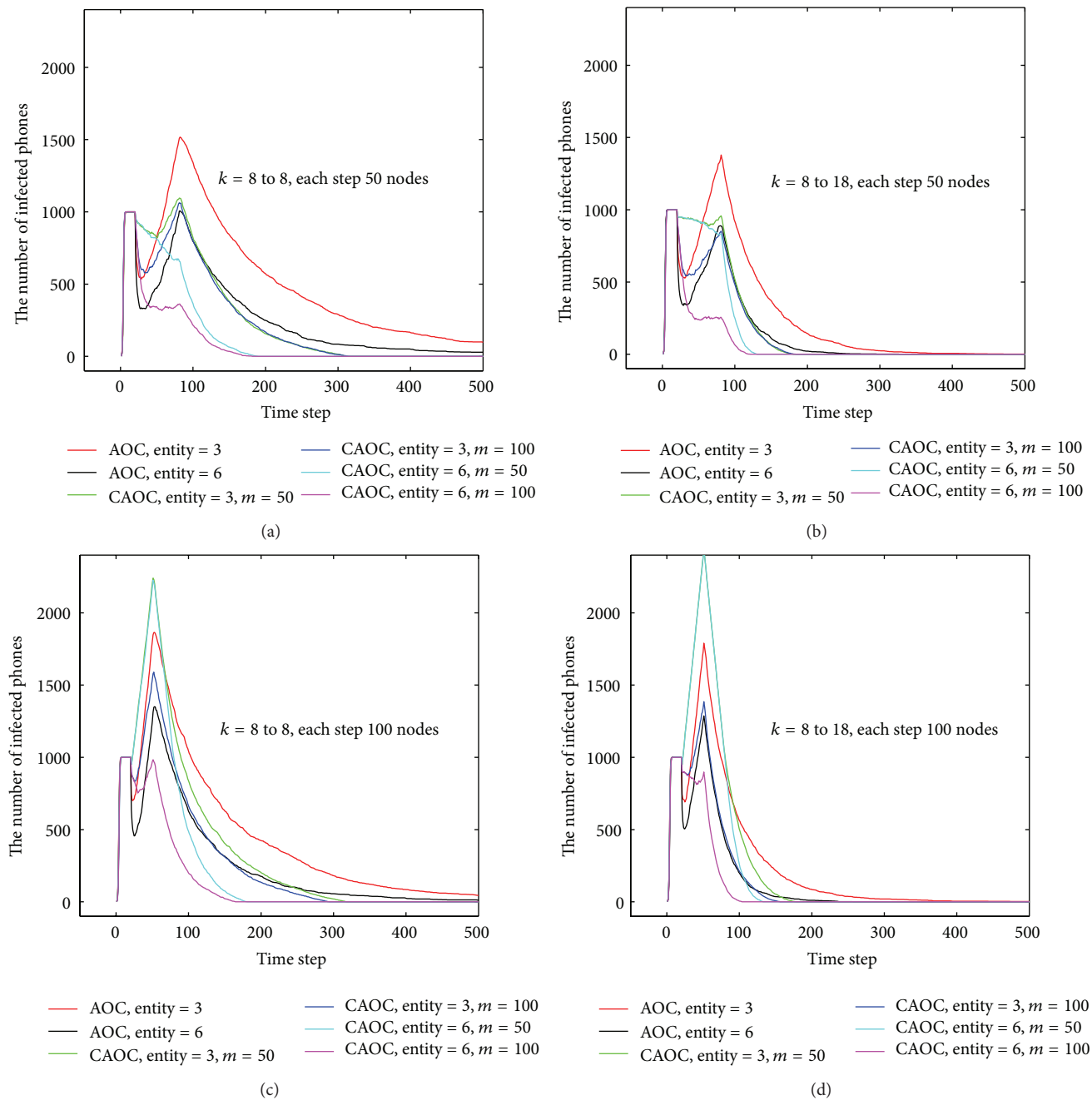


FIGURE 7: The number of infected phones over time in different dynamicin-evolving networks. (a) 50 phones are added into the network at each step, and the average degree $\langle k \rangle$ maintains 8; (b) 50 phones are added into the network at each step, and the average degree $\langle k \rangle$ increases from 8 to 18; (c) 100 phones are added into the network at each step, and the average degree $\langle k \rangle$ maintains 8; (d) 100 phones are added into the network at each step, and the average degree $\langle k \rangle$ increases from 8 to 18.

network conditions. Thus the network congestion can be avoided;

(3) the selected phones which receive the patches are always the most important ones of the phones found by the entities at each time step for the virus propagation, and thus the virus propagation can be effectively restrained;

(4) each phone receives the patch only once, which is beneficial to avoiding the network congestion and the waste of network resource.

In summary, the SAOC-based patch dissemination strategy is a reasonable, effective, and secure method to send security patches in mobile networks and reduce the damages mobile viruses cause.

Table 2: The structures of networks.

	Nodes	Edges	$\langle k \rangle$
University email network	1133	5451	9.62
Community-based network	4000	16855	8.42
Autonomous systems network	11080	31538	5.69
Collaboration network	12008	237010	39.47

Acknowledgments

This paper was supported by the National Natural Science Foundation of China (Grant nos. 61202362, 61070209, 61121061, and 61272402), the Asia Foresight Program under NSFC Grant (Grant no. 61161140320), and the Specialized Research Fund for the Doctoral Program of Higher Education (Grant no. 20120005110017).

References

[1] P. Wang, M. C. González, C. A. Hidalgo, and A.-L. Barabasi, "Understanding the spreading patterns of mobile phone viruses," *Science*, vol. 324, no. 5930, pp. 1071–1076, 2009.

[2] S.-M. Cheng, W. C. Ao, P.-Y. Chen, and K.-C. Chen, "On modeling malware propagation in generalized social networks," *IEEE Communications Letters*, vol. 15, no. 1, pp. 25–27, 2011.

[3] G. Yan and S. Eidenbenz, "Modeling propagation dynamics of bluetooth worms (Extended version)," *IEEE Transactions on Mobile Computing*, vol. 8, no. 3, pp. 353–367, 2009.

[4] P. De, Y. Liu, and S. K. Das, "An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 8, no. 3, pp. 413–425, 2009.

[5] C. Toma, "Advanced signal processing and command synthesis for memory-limited complex systems," *Mathematical Problems in Engineering*, vol. 2012, Article ID 927821, 13 pages, 2012.

[6] E. G. Bakhoum and C. Toma, "Specific mathematical aspects of dynamics generated by coherence functions," *Mathematical Problems in Engineering*, vol. 2011, Article ID 436198, 10 pages, 2011.

[7] Y. Chen, G. Paul, S. Havlin, F. Liljeros, and H. E. Stanley, "Finding a better immunization strategy," *Physical Review Letters*, vol. 101, no. 5, Article ID 058701, 2008.

[8] W.-J. Bai, T. Zhou, and B.-H. Wang, "Immunization of susceptible-infected model on scale-free networks," *Physica A*, vol. 384, no. 2, pp. 656–662, 2007.

[9] R. Cohen, S. Havlin, and D. Ben-Avraham, "Efficient immunization strategies for computer networks and populations," *Physical Review Letters*, vol. 91, no. 24, Article ID 247901, 4 pages, 2003.

[10] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Physical Review E*, vol. 65, no. 5, Article ID 056109, 14 pages, 2002.

[11] D. Samfat and R. Molva, "IDAMN: an intrusion detection architecture for mobile networks," *IEEE Journal on Selected Areas in Communications*, vol. 15, no. 7, pp. 1373–1380, 1997.

[12] T. S. Yap and H. T. Ewe, "A mobile phone malicious software detection model with behavior checker," in *Web and Communication Technologies and Internet-Related Social Issues—HSI 2005*, vol. 3597 of *Lecture Notes in Computer Science*, pp. 57–65, 2005.

[13] J. Cheng, S. H. Y. Wong, H. Yang, and S. Lu, "SmartSiren: Virus detection and alert for smartphones," in *Proceedings of the 5th International Conference on Mobile Systems, Applications and Services (MobiSys '07)*, pp. 258–271, June 2007.

[14] A. Smirnov and T.-C. Chiueh, "Automatic patch generation for buffer overflow attacks," in *Proceedings of the 3rd Internationl Symposium on Information Assurance and Security (IAS '07)*, pp. 165–170, August 2007.

[15] S. Sidiroglou and A. D. Keromytis, "Countering network worms through automatic patch generation," *IEEE Security and Privacy*, vol. 3, no. 6, pp. 41–49, 2005.

[16] W. Cui, M. Peinado, H. J. Wang, and M. E. Locasto, "ShieldGen: automatic data patch generation for unknown vulnerabilities with informed probing," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 252–266, May 2007.

[17] F. Li, Y. Yang, and J. Wu, "CPMC: an efficient proximity malware coping scheme in smartphone-based mobile networks," in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM '10)*, pp. 1–9, March 2010.

[18] G. Zyba, G. M. Voelker, M. Liljenstam, A. Méhes, and P. Johansson, "Defending mobile phones from proximity malware," in *Proceedings of the 28th Conference on Computer Communications (INFOCOM '09)*, pp. 1503–1511, April 2009.

[19] M. H. R. Khouzani, S. Sarkar, and E. Altman, "Dispatch then stop: optimal dissemination of security patches in mobile wireless networks," in *Proceedings of the 49th IEEE Conference on Decision and Control (CDC '10)*, pp. 2354–2359, December 2010.

[20] C. Gao and J. Liu, "Modeling and restraining mobile virus propagation," *IEEE Transactions on Mobile Computing*, vol. 12, no. 3, pp. 529–541, 2013.

[21] C. Gao and J. Liu, "Modeling and restraining mobile virus propagation," *IEEE Transactions on Mobile Computing*, 2013.

[22] J. Liu, "Autonomy-Oriented Computing (AOC): the nature and implications of a paradigm for self-organized computing," in *Proceedings of the 4th International Conference on Natural Computation (ICNC '08)*, pp. 3–11, October 2008.

[23] J. Liu, X. Jin, and K. C. Tsui, *Autonomy Oriented Computing (AOC): From Problem Solving to Complex Systems Modeling*, Springer, New York, NY, USA, 2005.

[24] M. Li and W. Zhao, "Asymptotic identity in min-plus algebra: a report on CPNS," *Computational and Mathematical Methods in Medicine*, vol. 2012, Article ID 154038, 11 pages, 2012.

[25] M. Li and W. Zhao, "Representation of a stochastic traffic bound," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1368–1372, 2010.

[26] C. Gao, J. Liu, and N. Zhong, "Network immunization with distributed autonomy-oriented entities," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1222–1229, 2011.

[27] R. Guimerà, L. Danon, A. Díaz-Guilera, F. Giralt, and A. Arenas, "Self-similar community structure in a network of human interactions," *Physical Review E*, vol. 68, no. 6, Article ID 065103, pp. 651031–651034, 2003.

[28] J. Leskovec, J. Kleinberg, and C. Faloutsos, "Graphs over time: densification laws, shrinking diameters and possible explanations," in *Proceedings of the 11th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 177–187, ACM, August 2005.

[29] J. Leskovec, J. Kleinberg, and C. Faloutsos, "Graph evolution: densification and shrinking diameters," *ACM Transactions on Knowledge Discovery from Data*, vol. 1, no. 1, pp. 1–41, 2007.

[30] T. Bu and D. Towsley, "On distinguishing between internet power law topology generators," in *Proceedings of the 21st IEEE International Conference on Computer and Communications (INFOCOM '02)*, pp. 638–647, 2002.

[31] C. C. Zou, D. F. Towsley, and W. Gong, "Modeling and simulation study of the propagation and defense of internet e-mail worms," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 2, pp. 106–118, 2007.

[32] C. Gao, J. Liu, and N. Zhong, "Network immunization and virus propagation in email networks: experimental evaluation and analysis," *Knowledge and Information Systems*, vol. 27, no. 2, pp. 253–279, 2011.

[33] T. J. Norman Bailey, *The Mathematical Theory of Infectious Diseases and Its Applications*, Griffin, London, UK, 2nd edition, 1975.

[34] D. J. Daley and J. Gani, *Epidemic Modelling: An Introduction*, Cambridge University Press, Cambridge, UK, 2000.

[35] O. Diekmann and J. A. P. Heesterbeek, *Mathematical Epidemiology of Infectious Diseases*, John Wiley & Sons, New York, NY, USA, 2000.