Mitigation of Malware Proliferation in P2P Networks using Double-Layer Dynamic Trust (DDT) Management Scheme

Lin Cai and Roberto Rojas-Cessa*

Networking Research Laboratory, ECE Department, New Jersey Institute of Technology, University Heights, Newark, NJ 07102, USA;
**e-mail: rojas@njit.edu*

Abstract

Peer-to-peer (P2P) networking enables users with similar interests to exchange, contribute, or obtain files. This network model has been proven popular to exchange music, pictures, or software applications. These files are saved, and most likely executed, at the downloading host. At the expense of this mechanism, worms, viruses, and malware find an open front door to the downloading host and gives them a convenient environment for successful proliferation throughout the network. Although virus detection software is currently available, this countermeasure works in a reactive fashion, and in most times, in an isolated manner. In this paper, we consider a trust management scheme to contain the proliferation of viruses in P2P networks. Specifically, we propose a cooperative and distributed trust management scheme based on a two-layer approach to bound the proliferation of viruses. The new scheme is called double-layer dynamic trust (DDT) management scheme. Our results show that the proposed scheme bounds the proliferation of malware. With the proposed scheme, the number of infected hosts and the proliferation rate

Journal of Cyber Security and Mobility, 1–20.

are limited to small values. In addition, we show that network activity is not discouraged by using the proposed scheme.

Keywords: malware, peer-to-peer networks, P2P, trust management, virus proliferation.

1 Introduction

Perhaps the simplest service model of a connection between two Internet hosts is the one used in peer-to-peer (P2P) networking, where a host can perform the role of a client and a server.

Hosts in P2P networks have the potential of functioning as a data server and to be used as a part of a large distributed system for disseminating of information without the limitations of using a single host (interface). The distribution potential of these networks is currently under consideration for massive audience applications, such as IPtv [1, 2], where video sources rely on intermediate peers for further distribution of content. Furthermore, P2P networks allow a user with Internet access and an acceptable bandwidth to participate in complex and effective distribution environments, as proven by Napster [3] and Gnutella [4] for sharing music files.

A peer user, usually interested in the content available through P2P networks, pre-approves storing downloaded files, and most likely, executes them. This pre-disposition process leaves a front door for viruses to the local host and make peers vulnerable to malicious files that can affect the peers, the network, or both [8]. Furthermore, other users can be encouraged to download popular Internet files, therefore creating an incubating environment for viruses.

Several studies about virus proliferation have been presented [5, 6]. They consider a network topology and features that describe proliferation patterns of viruses. Among other properties, viruses tend to have a spreading rate in function to the network density. Analysis of virus proliferation models is beyond the scope of this paper.

Viruses or malware[1] have usually a specific destructive objective, whether they are aimed to damage the host computer, to retrieve user information that

[1] We refer to virus or malware interchangeably in this paper as they may show similar proliferation characteristics.

can be illegally profitable, or to affect communication resources (e.g. denial of service). Depending on the characteristics, viruses in a host may or may not affect other stored files.

The general countermeasure in a host against viruses is the use of an antivirus program, which tasks can be coarsely divided into detecting a computing threat and removing the threat from the host. The successful detection by this protection software is based on the knowledge of existing viruses and their properties or signature for identification. Therefore, a new virus can be unnoticeably hosted in a peer until the virus becomes known to the detection program. During this detection delay, the virus could be downloaded by another peer and spread throughout the network. Furthermore, after a virus is detected in a peer, the detection software may remove it. However, the information about this detection might be kept from other peers as the virus detection and removal may be information considered of only local significance.

Trust management schemes aim to distribute reputation information about peers in different networks scenarios to categorize the behavior and contribution of hosts to the P2P community [7]–[9]. A dynamic trust management scheme was proposed [10]. This scheme is based on localized trust evaluations and in dissemination of alert messages to prevent others peers from downloading a file from a suspicious peer. The scheme aims to limit the proliferation of malware under the assumption that there is no local file infection. In other words, when a virus-free peer downloads a file containing viruses, other existing files in the peer are not infected. However, viruses not only attempt to spread themselves but also to infect the other files in the P2P network, or to pursue further hardware and software damage at the host or network level. Although the authors didn't assign a name to the scheme in the paper, we call this scheme dynamic threshold management (DTM) in the remainder of this paper, for brevity.

In this paper, we discuss the performance of DTM under file infection and show that file infection has the potential to underscore proliferation countermeasures. To bound virus proliferation, we propose the double-layer dynamic trust (DDT) management scheme, which uses a two-layer trusting strategy aimed to contain the impact of the internal infection. The results show that the proposed trust management scheme is efficient for bounding the dissemination of viruses in P2P networks under viruses with infectious properties. The proposed scheme uses a rating messaging scheme, used to advertise the undergone experience of a peer after a download. We analyze the effect of the propagation delay on the system performance, and observe how delayed alerts benefit network infection as informed peers cannot prevent clean peers from downloading files from infected peers in a timely fashion. Furthermore, we show that the adoption of the proposed scheme has a negligible impact on the downloaded activity by peers.

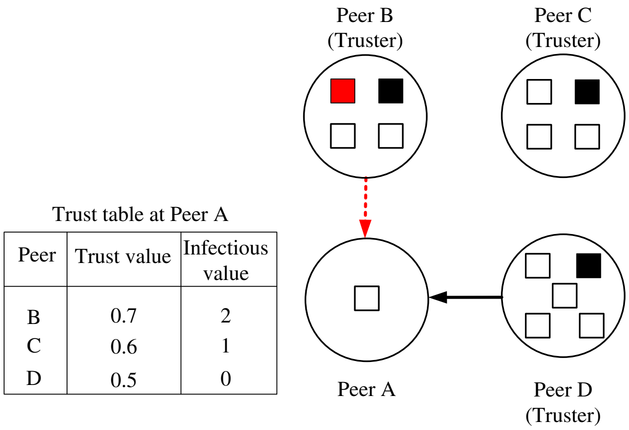
The remainder of this paper is organized as follows. Section 2 describes the proposed scheme based on dynamic trust management, the terms and the parameters for evaluation of peer trust, and the operation of the proposed management scheme in a P2P network. Section 3 presents the theoretical analysis of the number of infection peers under different trust management schemes. Section 4 presents a performance study of the proposed scheme, obtained through computer simulation. Section 5 presents our conclusions.

2 Double-Layer Dynamic Trust Management Scheme

In the two-layer approach of the DDT scheme, each peer has a trust table that keeps two main parameters. The first parameter, similarly to that used in DTM, is a trust value about the other peers. A trust value at peer A about peer B indicates the probability that a virus is downloaded from B by peer A. The higher the trust A has on B, the smaller the probability of downloading an infectious file.

Any peer in the system that is trusted by any other peer is called trustee and any peer that trusts a trustee is called truster. The second trust value in this table is designed to prevent internal infection, which is defined as the action of an infected file or malware of infecting other files in a host, This trust value is called the infectious value. The infectious value at peer A about peer B indicates the probability of internal infection from a file downloaded. The larger the infectious value is, the higher the probability of an infection from virus downloaded from B. This means that peer A would less likely to download a file from B.

The following is an example of how the proposed algorithm works. Let us consider that peer A wants a file and there are three possible trusters B, C, and D who have the desired file. Figure 1 shows this example. The black square in the figure represents the requested file, the red square in peer B represents a virus, which has infected the other files in peer B with probability P_I. In the



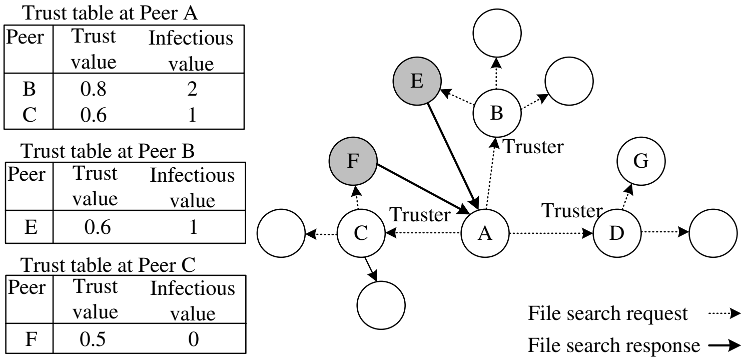
Trust table at Peer A

Peer	Trust value	Infectious value
B	0.7	2
C	0.6	1
D	0.5	0

Figure 1 Example of the proposed scheme using a double-layer trust management.

DTM scheme, peer A chooses the peer that has the highest trust value at A. Peer A then chooses peer B as the downloading source. In our proposed scheme, the higher the infectious value is, the larger the probability that an infection has occurred in the corresponding peer. Peer A then chooses a peer with the smallest infectious value from its eligible trustees. In this example, peer A selects peer D as the downloading source because D's infectious value is 0, which is the smallest among B, C, and D. In this way, the system guarantees that a peer performs a download from the most reliable source. Different from another schemes, we consider that a file can be infected by a file stored in the same peer. For example, as this figure shows, peer B has an infected file, which is different from the one requested by A. Therefore, if peer A had selected the sought file from peer B, this file may have been infected and all the files at peer A may become infected in turn.

As another example, let us consider that peer A wants a file and none of its three trusters, B, C, or D has that file, as Figure 2 shows. Peer B, C, and D forward the search request message to their trusters, consequently. Figure 2 shows that peer A finds the searched file in peers E and F, the grey colored ones. Peer A calculates the trust values on these two peers, which are $Tv(A, B) \times Tv(B, E) = 0.48$ and $Tv(A, C) \times Tv(C, F) = 0.3$. In the DTM scheme, peer A chooses the peer that has the largest trust value. Peer A then chooses peer E as the downloading source. In the proposed scheme, the larger the infectious value is, the larger the probability that an infection



Trust table at Peer A

Peer	Trust value	Infectious value
B	0.8	2
C	0.6	1

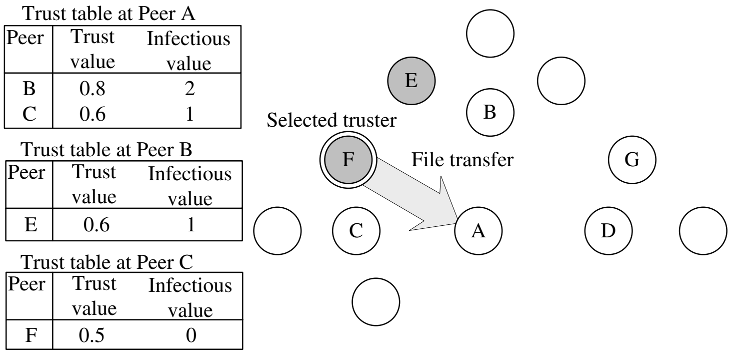
Trust table at Peer B

Peer	Trust value	Infectious value
E	0.6	1

Trust table at Peer C

Peer	Trust value	Infectious value
F	0.5	0

Figure 2 File search mechanism, from a peer to its trusters. Trusters forward the search request to their own trusters.



Trust table at Peer A

Peer	Trust value	Infectious value
B	0.8	2
C	0.6	1

Trust table at Peer B

Peer	Trust value	Infectious value
E	0.6	1

Trust table at Peer C

Peer	Trust value	Infectious value
F	0.5	0

Figure 3 File download mechanism, from the downloading source to the file requesting peer.

has occurred in the corresponding peer. Peer A then chooses the peer with the smallest infectious value from its possible trustees. The infectious value of peer E and F separately are $Iv(A,B) + Iv(B,E) = 3$ and $Iv(A,C) + Iv(C,F) = 1$. In this example, peer A selects peer F as the downloading source since its *Iv* is lower than that of peer E.

As Figure 3 shows, peer A downloads the file from peer F. When the downloading is finished, peer A checks whether or not the downloaded file has a virus. If peer A is not satisfied with the download, it sends a warning message to its trustees as shown in Figure 4. When the trustees receive the message, they update their trust value and infectious value about peer E, and they forward the message to their trustees until the time stamp expires.

Trust table at Peer A

Peer	Trust value	Infectious value
B	0.8	2
C	0.6	1

Trust table at Peer B

Peer	Trust value	Infectious value
E	0.6	1

Trust table at Peer C

Peer	Trust value	Infectious value
F	0.5	0

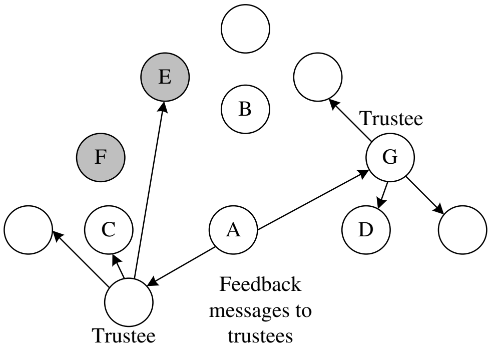


Figure 4 Feedback messages.

2.1 Trust Model

In the proposed trust management scheme, there are N peers, where each peer has a trust table with $2 \times (N - 1)$ entries. The trust value and the infectious value in the trust table are used to select the downloading source. The trust model has the following major components:

- **Trust table.** The trust table in peer i is denoted as $T(i)$. The trust value of peer i on peer j, is denoted as $T_v(i, j)$, where $T_v(i, j) \in [-1, -1]$. For example, $T_v(i, j) = -1$ means that peer i does not trust peer j and any filed downloaded from j would be expected to be a virus with probability 1.0. On the other hand $T_v(i, j) = 1$ means that peer i trusts peer j and any file downloaded from j is expected to be innocuous with probability 1.0. Therefore, in the selection of the downloading source, peer j has the top priority to become the downloading source. Peer i updates its trust table after downloading a file from peer j by re-evaluating the trust and infectious values about peer j according to the experienced interactions with peer j, and these are represented as the ratio of downloads of clean files and all downloads from peer j. We define *social distance* as the number of peers that a message would traverse to reach a given peer. For example, if a peer forwards a file search request from a truster to its trustee, the social distance that the request travels is two.

- **Infectious value.** The second value in $T(i)$ is the infectious value I_v that represents the possible internal infection degree of peer j. The larger the value of I_v, the larger the probability that the peer contains a virus. If there are several trustees those trust value is larger than the threshold for an acceptable trust value, the peer with the smallest I_v is selected as the downloading source. Peer i updates $T(i)$ if it receives an alert from its trustee, peer j.
- **Antivirus software.** In this paper, it is considered that a peer counts with virus-detection software. A successful virus detection indicates that a peer has downloaded an infected file, and the antivirus software can identify the file. Therefore, peer i detects a virus with probability $P_d(i)$.
- **Internal infection.** If a clean peer (whose files are virus free), downloads a file containing viruses, other existing files in this peer can possibly get infected with probability P_I. An infected download is defined as a download of a file containing a virus.
- **Propagation delay.** The propagation delay is the time it takes to download a file or the time that a ranking message takes to travel from one peer to another. The units of the propagation time in this paper a fixed period of time, called time slot. In this paper, we assume that a download takes a time slot. Also, we assume that the time that takes for a ranking message to be sent to a peer is one time slot. The propagation delay between peer i and peer j is denoted as $d(i, j)$.

2.2 Management Scheme

The trust management scheme works as follows. When peer i searches for file f, it checks the local file's reputation in the file record. If the file's reputation value is found at the database and is above the acceptable reputation threshold, Th_R, then the peer proceeds to find the file source.

The values held by a peer are updated after different actions take place. These are described as follows.

File Search. A peer i sends a request for file f to all trustees whose trust value is above the admissible threshold value Th_T (i.e., trustable trustees). Peer i chooses the peer that has the largest T_v and the lowest infectious value among those who have a copy of the requested file. If the file is not available from peer i's trustable trustees, the peer sends a recursive query for f to all trustees. In this query, the receiving trustee searches for the requested file among its own trustees. This process is performed recursively until either a fruitful search is achieved or there are no more trustees to query. After a recursive query, if peer k is introduced to i, new values are calculated: $T_v(i,k) = T_v(i,j) \times T(j,k)$, and $I_v(i,k) = I_v(i,j) + I_v(j,k)$, then the peer proceeds to the selection of a downloading source.

Post-download update. If the download of f is determined to be clean, $T_v(i,j) = \alpha T_v(i,j)$, where α is the rate of the trust value growth, $\alpha > 1$, while $I_v(i,j)$ remains unchanged. If the download of f is determined infected:

$$\begin{aligned} T_v(i,j) &= \delta T_v(i,j) \\ I_v(i,j) &= I_v(i,j) + 1 \\ F(i,f_l) &= F(i,f_l) + 1 \end{aligned}$$

where δ is the rate of the trust value degradation and $1 > \delta > 0$. During this phase, if $T_v(i,j) < th_w$, where th_w is the threshold to trigger a warning process, peer i issues warning messages to all its trusters. In this way, peers exchange critical information about other interacting peers. A warning message has the following format: $\{ID, vj, f_m, \Delta, d\}$, where *ID* is the warning identification number, v_j is the identification of the peer that served as the source of a threatening file, f_m is the file's name, Δ is the decrement of the trust value at peer i, and d is the maximum number of truster hops the warning message is allowed to propagate.

Post-warning updates. After receiving a warning message from peer k about peer j, peer i updates the trust values. If $T_v(i,k) > Th_T$:

$$\begin{aligned} T_v(i,j) &= T_v(i,j) - \Delta T_v(i,j) \\ I_v(i,j) &= I_v(i,j) + \frac{(d-1)}{d} \\ F(i,f_l) &= F(i,f_l) + \frac{(d-1)}{d} \\ \Delta &= \Delta\frac{(d-1)}{d}. \end{aligned}$$

Because the forwarding of the warning message is bound by d, this value is also updated as $d = d - 1$. If the updated $d > 1$ and $\Delta T_v(k, i) > th_w$, peer i sends a warning message to its trusters with the updated values.

3 Analysis

We use probability to analyze proliferation of malware over a P2P network and develop a recursive formula to calculate the number of infected peers in the P2P network.

Let's consider a distributed trust management system with n legitimate peers and m infected peers uniformly distributed in the network. Each legitimate peer has v trusters in average. Total number of peers in the network is $n + m$. Let $I(t)$ represent the number of infected peers in the P2P network at time t. Therefore, $I(0) = m$. Let $H(t)$ represent the number of legitimate peers in the P2P network at time t. Therefore, $H(t) + I(t) = n + m$ and $H(0) = n$. Let the probability of each peer to perform a download at time slot t be p. Then, the total number of downloads in a time slot are $(n + m) \times p$. The probability of downloading from peer carrying a virus at time slot t is $\gamma(t)$, where $\gamma(0) = I(0)/(n + m)$. Let r the probability of requesting a malicious file of peer r at time slot t is $q(r, t)$. The total number of files in the network is M, and among them, M_f files are infected. Therefore, we get $q(r, t) = \frac{M_f}{M}$.

The average number of infected peers of a P2P network, without using a trust management scheme at time $t + 1$ can be expressed as:

$$\begin{cases} I(t+1) = I(t) + \displaystyle\sum_{i=1}^{n-I(t)} p \times \left((1 - q(i,t)) \times \frac{I(t)}{n+m} + q(i,t)\right) \\ q(i,t) = \dfrac{M_f}{M} \end{cases} \tag{1}$$

where, $0 \leq I(t) \leq (n + m)$.

The probability of downloading a file from a malicious peer by a P2P network is reduced by using warning messages. Let $N(i, t)$ denote the number of malicious peers recorded by peer i at time slot t. $G(i, t)$ denotes number of legitimate peers in the view of peer i at time slot t, and $G(i, t) = n + m - N(i, t)$.

Suppose that at time slot t, a truster peer of peer i, peer k, downloads an infected file from peer j, peer k then sends a warning message to its trustees if the malicious file is detected. Each warning message contains the downloading information such as name of the file, and the ID of peer j. The average number of infected peers at time slot $t + 1$ can be expressed as

$$\begin{cases} I(t+1) = I(t) + \displaystyle\sum_{i=1}^{n-I(t)} p \\ \qquad \times\left((1 - q(i,t)) \times \dfrac{I(t) - N(i,t)}{n + m - N(i,t)} + q(i,t)\right) \\ N(i,t+1) = N(i,t) + \displaystyle\sum_{k=1}^{v} p \\ \qquad \times\left((1 - q(k,t)) \times \dfrac{I(t) - N(k,t)}{n + m - N(k,t)} + q(k,t)\right) \\ q(i,t) = \dfrac{M_f}{M} \end{cases} \tag{2}$$

where, $0 < N(i,t) < I(t) < (n + m)$.

Since $N(i,t) > 0$, $\frac{I(t)}{n+m} > \frac{p\times(I(t)-N(i,t))}{n+m-N(i,t)}$. We can see that the proposed trust management scheme reduces the growth rate of the number of malicious peers in the network.

When file reputation (FR) is used in DDT scheme, $F(i,t)$ denotes the number of malicious peers recorded by peer i at time slot t. The average number of infected peers can be expressed as:

$$\begin{cases} I(t+1) = I(t) + \displaystyle\sum_{i=1}^{n-I(t)} p \times ((1 - q(i,t)) \\ \qquad \times \dfrac{(I(t) - N(i,t))}{n + m - N(i,t) + q(i,t))} \\ N(i,t+1) = N(i,t) + \displaystyle\sum_{k=1}^{v} p \times ((1 - q(k,t)) \\ \qquad \times \dfrac{(I(t) - N(k,t))}{n + m - N(k,t) + q(k,t))} \\ q(i,t) = \dfrac{M_f - F(i,t)}{M} \\ F(i,t+1) = F(i,t) + \displaystyle\sum_{k=1}^{v} p \\ \qquad \times\left((1 - q(k,t)) \times \dfrac{(I(t) - N(k,t))}{n + m - N(k,t)} + q(k,t)\right) \end{cases} \tag{3}$$

where $0 < F(i,t) < M_f$, and $0 < N(i,t) < I(t) < (n + m)$.

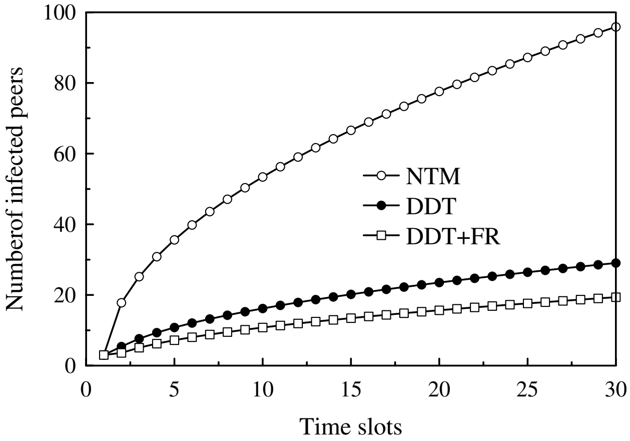


Figure 5 Theoretical estimation of proliferation of viruses in DDT, DDT+FR, and without a trust management scheme, NTM.

Therefore, the average number of infected peers in the DDT scheme with FR is smaller than that of using the DDT scheme alone.

3.1 Simulation Study of the DDT Scheme with and without Warning Messaging

We modeled a network with 100 peers, and three malicious peers. The total number of files is 150, and 10 of them are viruses. The downloading probability p is 0.2. We randomly select 10 peers as the number of trustees for each peer as initial condition. In Figure 5, NTM indicates the performance of DDT with no propagated messages and no trust management scheme. From this figure, we can see that the DDT scheme, combined with file reputation, limits the number of infected peers in 30 peers within 30 time slots.

4 Performance

We simulated a P2P network using a mesh topology, with 100 peers randomly placed as active peers in the mesh. An active peer is a host that forwards, stores, or requests files to or from the other peers. The network has 150 existing files with several copies for each file. Files (and copies) are distributed randomly with a uniform distribution among peers. From these files, we set 60% of

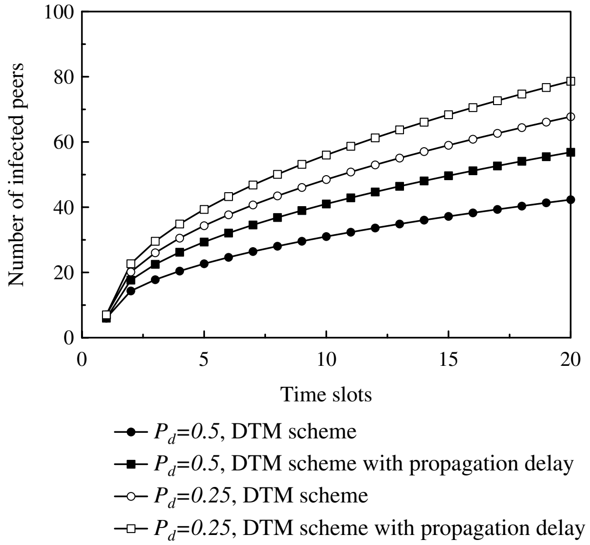


Figure 6 Proliferation of malware using T_v and $P_d = \{0.25, 0.5\}$, with no local infection and alert delay.

them as popular files (i.e., requested with high frequency). Among all files, 10 randomly selected files are designated as malware (i.e., virus). After a host downloads a malicious file, there is a probability of detecting it, which is denoted as P_d. Here, we consider that the minimum time for an event (e.g., a download or a transmission of an alert from one peer to another in the network) is a fixed amount of time or time slot. We evaluated the total number of infected peers at each time slot.

Figure 6 shows the performance of the DTM scheme measured in the number of infected peers, where only a trust value per peer is used. In this scheme, the trust value of a peer is evaluated by considering the recorded downloads of a truster from its trustees. This figure also considers when downloading a file and the broadcasting of peers' trust values to trusters, and $P_I = 0$. The figure shows two curves, one with $P_d = 0.5$, and $P_d = 0.25$. Because the number of infected peers changes significantly from time slot to time slot, the curve for $P_d = 0.25$ converges to 70 infected peers after 20 time slots, while the curve for $P_d = 0.5$ converges to 50 peers after the same time. This shows that the management scheme cannot bound the malware proliferation efficiently.

This figure shows the performance of the DTM scheme with $P_I = 0.0$ in a network. This figure shows that for peers with antivirus software with

$P_d = 0.5$, the number of infected peers is 45 after a long period of time (or until the number of downloads reaches 800), and for $P_d = 0.25$, the maximum number of infected peers approaches 70 after 750 downloads. These results show that the delay on disseminating the alert messages allows more high-risk downloads, allows the proliferation of malware.

Figure 7 shows the proliferation of the DTM scheme, as in the two cases above but, however, with infection probability ($P_I = 0, 0.25, 0.5$). This case considers no propagation delay for the messaging system, and $P_d = 0.5$. This figure shows that the infection property of viruses increase the effectiveness of malware proliferation, and even with $P_d = 0.5$, all peers in the network would end up infected after 1200 downloads.

Figure 8 shows the degree of proliferation of malware using the DTM scheme and our proposed DDT scheme, where I_v is used, under $P_d = 0.5$ with no propagation delay in the distribution of the alert messages. This figure shows the spreading of the malware in the number of infected hosts per time slots. In this figure, the performance of the DTM scheme decreases as the *PI* increases. On the other hand, with the proposed DDT scheme, the impact of the infection probability is also noticeable but this impact is significantly lower, making the proposed scheme more effective.

These results are also shown in terms of the number of downloads. Figure 9 shows the proliferation of malware using the DTM scheme and the DDT

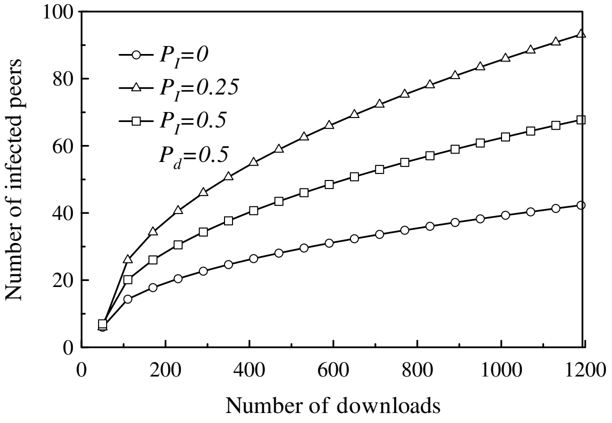


Figure 7 Proliferation of malware using DTM scheme, with $P_d = 0.5$ and considering infection probability $P_I > 0$.

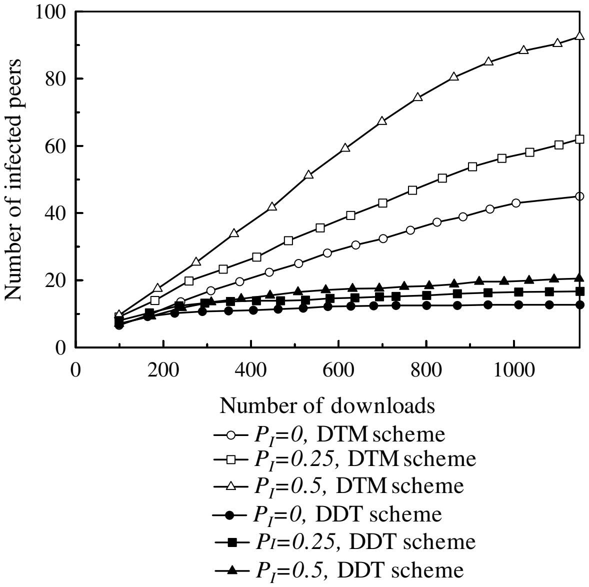


Figure 8 Proliferation of malware using the proposed DDT scheme with $Pd = 0.5$ and different P_I values in time slots.

scheme under $P_d = 0.5$ with propagation delays for the alert messages. The curves for different P_I, as in Figure 8, show a similar performance. The proposed scheme bounds it. In the case of a high P_I value, or $P_I = 0.5$, the number of infected peers drops from 100 peers as in the case of the DTM scheme to close to 30 peers in the DDT scheme.

Figure 10 shows the performance of both the DTM and the proposed schemes, measured as the number of infected peers per number of downloads in the network under different P_I values in an infectious environment. The proposed trust management scheme uses file reputation, labeled FR in the figure, with and without I_v. Curves a) to d) show that infectious viruses inhibit the effectivity of the DTM scheme as all peers in the network eventually get infected. This occurs because peers may be isolated after viruses have infected some peers. Curves e) to h) show that when file reputation is used, without recurring to I_v, the number of infected peers is bounded as the number of infected files is smaller than the total number of peers in the network. The proliferation is bounded because a peer can now identify a file coming from a peer with a record of no infections, in a proactive way. Curves i) to l) show

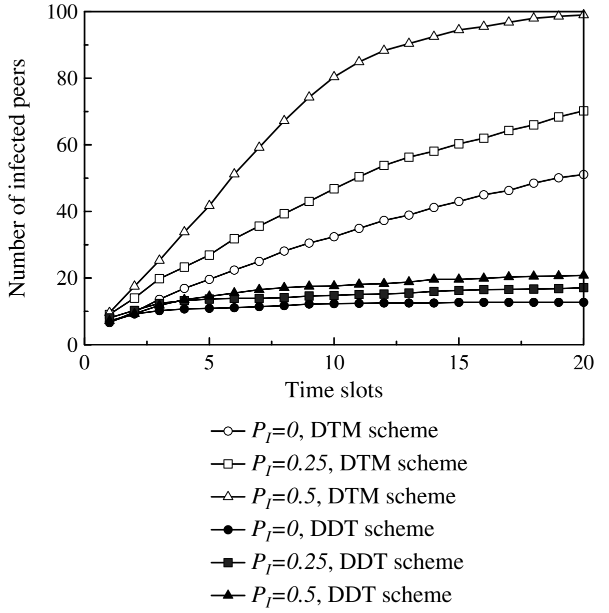


Figure 9 Proliferation of malware using the proposed DDT with $Pd = 0.5$ and different P_I values.

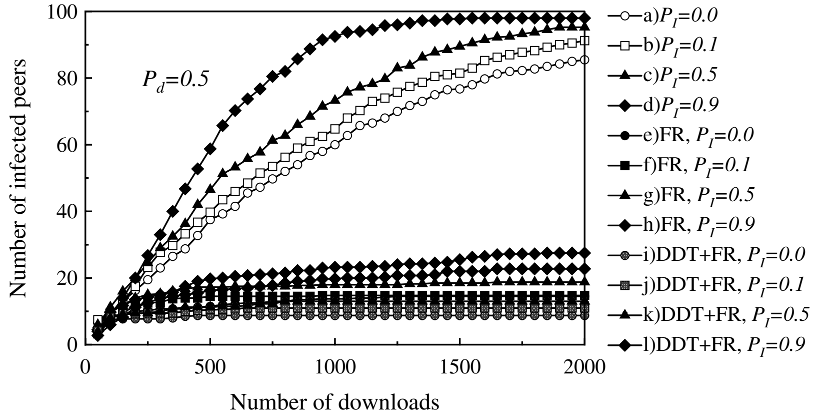


Figure 10 Comparison of proliferation of viruses using T_v only and with the proposed scheme.

that the use of a file reputation value in combination with I_v, which is updated based on warning messages among peers, has the highest performance as the number of infected peers decreases to an average of 10. The warning messages then are also used to identify peers with trustable values but that may contain

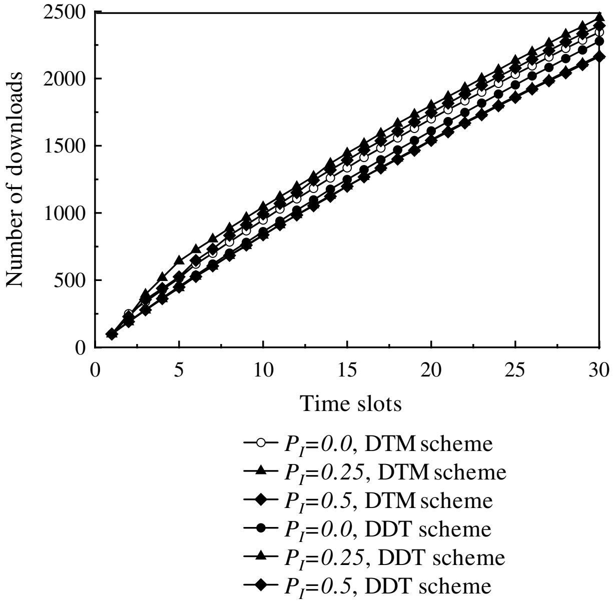


Figure 11 Download activity of the network using the proposed DDT scheme.

infected files. This is shown under the highest P_I values, $P_I = 0.9$, as the number of infected peers of l) is smaller than those of h).

Increasing the number of trust parameters in the management systems creates the risk of discouraging the download activity. We evaluated the download activity of the network using the same conditions as above. Figure 11 shows the download activity of a network using the DDT scheme, in downloads per time slot. The results show that the download activity with different P_I values, which impacts I_v for each peer, has no significant changes. This means that the proposed approach does not discourage network activity.

5 Conclusions

Trust management is a promising strategy to bound the proliferation of malware on peer-to-peer networks that can work jointly with virus detection systems. In this paper, we showed that the use of a single trust value per peer has deficiencies in bounding the proliferation of malware. In most cases, it is highly probable that the majority of peers become infected. By using extra information, based on the infectious value, where the consideration of a peer having hosted an infected file, the proliferation of malware becomes bounded more effectively. By using computer simulation of a mesh peer-to-peer network, we have shown the improvement of this proposed approach. Furthermore, considering that trust parameters to bound proliferation have the potential of discouraging download activity in P2P networks, we studied the impact of using our proposed DDT scheme. We showed that our approach has little impact on the download activity of the network.

References

[1] X. Xu, Y. Wang, S.P. Panwar, and K.W. Ross. A peer-to-peer video-on-demand system using multiple description coding and server diversity. *Proc. IEEE International Conference on Image Processing (ICIP)*, pp. 1759–1762, October 2004.

[2] X. Hei, C. Liang, J. Liang, Y. Liu, and K.W. Ross. A measurement study of a large-scale P2P IPTV system. *IEEE Transactions on Multimedia*, 9(8): December, 2007.

[3] M. Macedonian. Distributed file sharing: Barbarians at the gate? *IEEE Computer*, 33(8): 99–101, August 2000.

[4] Y. Wang, X. Yun, and Y. Li. Analyzing the characteristics of gnutella overlays. *Proc. IEEE IV International Conference in Information Technology*, pp. 1095–1100, April, 2007.

[5] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: Analysis and defences. *IPSN, Proceedings of the 3rd international symposium on Information processing in sensor networks*, pp. 259–268, April, 2004.

[6] L.-C. Chen and K.M. Carley. The impact of countermeasure propagation on the prevalence of computer viruses. *IEEE Trans. on System, Man, and Cibernetics*, 34(2): 823–833, April 2004.

[7] E. Damiani, D.C. Vimercati, S. Paraboschi, P. Samarati, and F. Violante. A reputation-based approach for choosing reliable resources in peer-to-peer networks. *Proc. of the 9th ACM Conference on Computer and Communications Security (CCS)*, Washington, DC, pp. 207–216, November 2002.

[8] S. Marti and H. Garcia-Molina. Limited reputation sharing in P2P systems. *Proc. of the 5th ACM Conference on Electronic Commerce*, New York, NY, pp. 91–101, May 2004.

[9] J. Shin, T. Kim, Taehoon, and S. Tak. A reputation management scheme improving the trustworthiness of P2P networks. *Proc. IEEE International Conference on Convergence and Hybrid Information Technology*, pp. 92–97, August, 2008.

[10] X. Dong, W. Yu, and Y. Pan. A dynamic trust management scheme to mitigate malware proliferation in P2P network. *Proc. IEEE International Conference on Communications 2008*, Beijing, China, pp. 1605–1609, May 2008.

[11] E.K. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim. A survey and comparison of peer-to-peer overlay network schemes. *IEEE Comm. Survey and Tutorial*, 7(2): 72–93, March, 2005.

[12] P. Dhungel, X. Hei, K.W. Ross, and N. Saxena. The pollution attack in P2P live video streaming: Measurement results and defenses. *Proc. Sigcomm P2P-TV Workshop*, pp. 323–328, August 2007.

[13] A. Cheng and E. Friedman. Sybilproof reputation mechanisms. *Proceedings of the ACM SIGCOMM Workshop on Economics of Peer-to-Peer Systems*, pp. 128–132, November, 2005.

[14] P. Resnick and R. Zeckhauser. Trust among strangers in internet transactions: Empirical analysis of eBay's reputation system. *Advances in Applied Microeconomics: The Economics of the Internet and E-Commerce*, pp. 127–157, November 2002.

[15] L. Xiong and L. Liu. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering*, pp. 843–857, July 2004.

[16] P. Herrmann. Trust-based procurement support for software components. *Proc. 4th International Conference of Electronic Commerce Research*, pp. 505–514, November, 2001.

[17] K. Walsh and E.G. Sirer. Fighting peer-to-peer SPAM and decoys with object reputation. *Proc. Third Workshop on the Economics of Peer-to-Peer Systems (P2PECON)*, pp. 138–143, Auguest, 2005.

[18] G. Theodorakopoulos and J.S. Baras. On trust models and trust evaluation metrics for ad hoc networks. *IEEE Journal on Selected Areas in Communications*, pp. 318–328, February, 2006.

[19] K. Hwang, M. Cai, Y.K. Kwok, S. Song, and Y. Chen. DHT-based security infrastructure for trusted internet and grid computing. *International Journal of Critical Infrastructures*, pp. 654–662, December, 2006.

[20] S. Song, K. Hwang, and Y.K. Kwok. Trusted grid computing with security binding and trust integration. *Journal of Grid Computing*, pp. 53-73, June, 2005.

[21] S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in P2P networks. *Proc. 12th International World Wide Web Conference*, pp. 785–791, November, 2003.

[22] X. Zhang and H.H. Chen. Analysis of virus and antivirus spreading dynamics. *Proc. IEEE Global Communications Conference*, pp. 871–875, November, 2005.

[23] P. Li, Z. Wang, and X. Tan. Characteristic analysis of virus spreading in ad hoc networks. *Proc. IEEE Workshop in Computational Intelligence and Security*, pp. 538–541, March, 2008.

[24] R. Kumar, D.D. Yao, A. Bagchi, K.W. Ross, and D. Rubenstein. Fluid modeling of pollution proliferation in P2P networks. *Performance Evaluation Review*, pp. 335–346, June, 2006.

[25] B.F. Cooper and H. Garcia-Molina. Peer to peer data trading to preserve information. *ACM TOIS*, pp. 133–170, April 2002.

[26] B. Horne, B. Pinkas, and T. Sander. Escrow services and incentives in peer-to-peer networks. *Proc. 3rd ACM Conference on Electronic Commerce*, pp. 85–94, October, 2001.

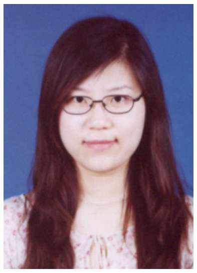
[27] B. Yang and H. Garcia-Molina. Ppay: Micropayments for peer-to-peer systems. *Proc. 10th ACM Conference on Computer and Communications Security (CCS)*, pp. 300–310, October, 2003.

[28] L. Mekouar, Y. Iraqi, and R. Boutaba. Peer-to-Peer's most wanted: Malicious peers. In *International Computer Networks Journal, Special Issue on management in Peer-to-Peer Systems: Trust, Reputation and Security*, 50(4):545–562, March, 2006.

[29] O. Kwon, S. Lee and J. Kim. FileTrust: Reputation management for reliable resource sharing in structured peer-to-peer networks. *IEICE Transactions Communication*, pp. 826–835, April 2007.

[30] C. Xie, G. Chen, and A. Vandenberg. Analysis of hybrid P2P overlay network topology. *Computer Communications*, 31(2):190–200, February 2008.

Biography



Lin Cai received the B.S. degree in telecommunication engineering from Nanjing University of Posts and Telecommunications, Nanjing, China. She received the M.S. degree in electrical engineering from Beijing University of Posts and Telecommunications, Beijing, China. She received Ph.D. degrees in electrical engineering from the New Jersey Institute of Technology, Newark, NJ. She is the recipient of the Hashimoto Fellowship for her Ph.D. dissertation from the New Jersey Institute of Technology. Her research interests include security, privacy and trust in Distributed networks (P2P networks).

Roberto Rojas-Cessa received the Ph.D. degree in electrical engineering from Polytechnic Institute of New York University, Brooklyn, NY. Currently, he is an Associate Professor in the Department of Electrical and Computer Engineering, New Jersey Institute of Technology. He has been involved in the design and implementation of application-specific integrated-circuits (ASIC) for biomedical applications and high-speed computer communications, and in the development of high-performance scalable packet switches and reliable switches. He was part of the team designing a 40 Tb/s core router for Coree, Inc, in Tinton Falls, NJ. His research interests include high-speed switching and routing, fault tolerance, quality-of-service networks, network measurements, and distributed systems. His research has been funded by the U.S. National Science Foundation and private companies. He has served on several technical committees for IEEE conferences and as a reviewer and panelist for the U.S. National Science Foundation and the U.S. Department of Energy. He was a Visiting Professor at Thammasat University, Rangsit, Thailand. He is a senior member of IEEE and a member of ACM.