A Comparison Study of Collaborative Strategies for Distributed Defense against Internet Worms based on Small-World Modeling

Hao Chen, Yu Chen*

[†]*Dept. of Electrical & Computer Engineering, SUNY - Binghamton, Binghamton, NY 13902*
{hchen8, ychen}@binghamton.edu

***Abstract*:[*] The prosperity of the Internet has made it attractive to hackers and malicious attackers. Internet worms have become one type of major threats to the network infrastructure. Distributed defense collaborating with single-point-deployed security applications over multiple network domains are promising. However, most of the reported collaborative schemes for distributed defense are application-specific. There is not much research that studies the general properties of variant collaborative schemes systematically. In this paper explores properties of general collaborative defense strategies from the perspective of complex system. A three-layered network modeling platform has been developed. Taking advantage of small-world network model, the platform consists of two network layers and one application layer. On top of it, an experimental comparison study of collaborative defense schemes has been conducted. Their performance and effectiveness facing signature-embedded worm attacks have been evaluated.**

Keywords: **Collaborative Distributed Defense, Internet Worms, Small world model.**

1. Introduction

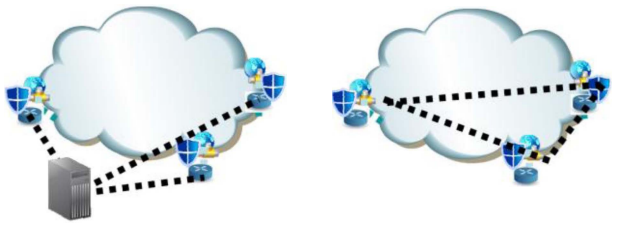
While the population of the Internet users has grown from 361 million in 2000 to 1.8 billion in 2009 [12], the Internet has become even more attractive to hackers. The *Information Security Forum* (ISF) report, entitled Threat Horizon 2010 [6], predicted an increase of Web 2.0 vulnerability, mobile malware, industrial espionage, and attacks from organized crime. Malicious activities such as *Distributed Denial-of-Service* (DDoS) attacks, turbo worms, e-mail spam, phishing and viruses have been identified as primary threats challenging the Quality-of-Service (QoS) that the ISPs provide to their users.

Securing network infrastructure has become one of the major concerns. Ideally, a comprehensive infrastructure security solution is expected to cover the entire network fabric. However, the prevalence of Internet renders this notion impractical and improbable due to the immeasurable scale and complexity of its infrastructure. It is more reasonable to limit deployment of infrastructure security applications to high threat targets, such as government agencies, financial institutions, health care facilities, and campus networks.

In recent years, efficient defense against distributed attacks has been a hot topic in network security community. Instead of establishing brand-new, dedicating systems, collaborating widely deployed, single-point network security applications for co-defense would be more feasible. Through collaboration, a security shield that covers infrastructure of multiple network domains could be built without significant modification. Besides keeping most of original functions, collaboration offers individual security applications wider views of dynamic situations around which may otherwise not be observed. It improves the resilience and confidence of participating security applications to handle sophisticated security problems in optimized strategies.

Existing collaborative schemes for distributed defense could be classified into either centralized or decentralized category. The most significant symbol of a centralized scheme lies in the use of a coordination daemon as shown in Figure 1(a). It could be a powerful multi-role server, or a dedicated server. Most likely, this server locates at one of participating network domains. Its major responsibilities include information collection, processing, analyzing, and distribution from/to individual nodes. This server may also conduct decision-making, either making decisions for all the participating nodes, or providing suggestions to those nodes for reference, depending on the detail mechanism for collaboration. The main advantages of centralized schemes are high accuracy and efficiency. Considering the overhead and scalability, centralized schemes have a distinct boundary for collaboration.

In contrast, the decentralized scheme is much flexible. It behaves similar to the manners of Peer-to-Peer (P2P) networks. This is due to the fact that most of decentralized schemes are developed on top of P2P network protocols.



(a) Centralized Collaboration (b) Decentralized Collaboration

Figure 1 Centralized and Decentralized collaboration

*Manuscript submitted to *the 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2010)*, Oct. 9 – 12, 2010, Chicago, Illinois, USA. Corresponding author: Yu Chen, Dept. of Electrical & Computer Eng., SUNY–Binghamton, Binghamton, NY 13902. E-mail: ychen@binghamton.edu, Tel.: (607) 777-6133, Fax: (607) 777-4464.

DOI 10.4108/icst.collaboratecom.2010.31

The P2P collaborative architecture gives decentralized schemes good scalability. Theoretically, any network node features compatible collaboration protocols could participate, so that the boundary of covered network could be loose. Rather than having a collaborative server in centralized scheme, each participating node takes responsibilities for collaboration, as shown in Figure 1(b), which brings more flexibility for self-management. Obviously, the cost for application is relatively low, since it does not require any modification in network beyond the installation of software.

It is important to have a comprehensive understanding of the behaviors of variant collaborative schemes. A deeper insight is critical for designers of network security system to adopt proper strategies that can match their requirements best for application. However, there are only few reported efforts that studied the collaborative behaviors of different schemes at the abstract level. Instead, most of the researches rather focused on application-specific solutions.

One main challenge in conducting such a behavioral study lies in the lack of methodology that is capable of presenting the networks in the abstractive level. In practice, many technical and/or non-technical issues make this task more complicated. Fortunately, this challenge could be handled through modeling technology. With the help of modeling, a virtual environment that mimics a simplified world could be set up [10]. After abstracting and scaling-down original problems, it is feasible to conduct further study on substantial behaviors.

In this paper, a three-layered network modeling platform has been developed for the establishment of such an abstract environment. The Internet layer at the bottom and the overlay network layer in the middle take the advantage of small-world network model for setup, while the application layer on the top focuses on the description of defense schemes. Based on this platform, a preliminary behavior study comparing different defense schemes has been conducted. The single-point defense scheme and its corresponding centralized and decentralized collaborative schemes are modeled. Through the adjustment of modeling parameters, different scenarios have been created for the evaluation of their impacts on network infrastructure security when facing signature-embedded worm attacks at the abstract level.

The rest of this paper is organized as follows. Section 2 provides a brief review on the reported efforts in distributed defense schemes for network infrastructure security. The developed three-layered modeling platform is introduced in Section 3. Then section 4 focuses on the description of our modeled worm-based attack and defense. Section 5 expresses the operation details of how the simulation experiments have been conducted. On top of it, we analyze the results for the overall performance evaluation of applying multi-domain collaboration for distributed defense. Section 6 concludes our work.

2. Related Work

In network security systems, it is common at the abstract level on that multiple end-hosts work collaboratively against attacks [15, 16, 19, 23]. A blacklist is exchanged among the potential victims to mitigate the threat. Usually a two-stage operation is conducted for distributed defense, which includes local detection and global collaboration.

There are two popular collaboration schemes. Schnackenberg *et al*. proposed a centralized coordinative scheme called CITRA [22] for network intrusion detection in 2001. A central coordinator responds for coordinating countermeasures based on a complete view of the network. Janakiraman *et al*. [13] introduced a decentralized defense scheme for network intrusion prevention. Information is shared among trusted peers to guard the network against intrusion. The subscription-based group communication is conducted over a P2P architecture, which brings excellent scalability.

For collaborative detection at the victim end, some more advanced techniques have been developed. Beyond focusing on certain detectable facts at the same domain, the emergence of cross-class detection [21] and multi-domain alter correlation [33] are able to link these detectable facts to some deliberate essentials for further analysis. With the help of cross-class detection, hosts can monitor and share information of different attacks. Meanwhile, the multi-domain alter correlation can even aggregate alters that possess common feature values. Instead of only focusing on traffic volume, researchers have extended the anomaly detection to frequency domain, in which the traffic distribution has been considered as random signals and its energy distribution in different frequency bands has been analyzed [4, 28, 36].

Beyond collaboration at the victim end, deploying network security systems into network fabric increases the initiative of defense system. Gamer *et al*. [9] extended their research to achieve a coordinated collaboration among independent systems for anomaly-based attack detection. Their approach combines an in-network deployment of neighboring detection systems with information exchanging. Working in a self-organized manner, however, each network node makes decision independently.

Taking advantages of the P2P network, researchers attempted to address the major challenges in large scale collaboration: the scalability and avoidance of central point of failure [32]. They merged multi-dimensional correlation for collaborative intrusion detection [33], and developed a self-protecting and self-healing collaborative intrusion detection architecture for the trace-back of fast-flux phishing domains [34].

A Distributed Change-point Detection (DCD) scheme was proposed to detect DDoS attack over multiple

network domains [30], [29]. Distributed information is collected through Change Aggregation Tree (CAT) for centralized analysis and decision-making [27]. Another collaborative approach was designed to detect and stop DDoS attacks at the intermediate network [31]. To achieve this purpose, detection nodes are deployed at both victim and source ends for collaborative detection [35]. In a more ambitious approach based on the DefCOM [18] scheme, the collaborative nodes are deployed all over the network. Not only the victim end and the source end, the intermediate network is also included [20].

The Internet could be considered as a complex system. All network activities, including attack and defense could be treated as subsets of it. From this perspective, it is practical to study the behaviors of network security activities using complex system models. The earliest effort using complex system for the modeling of distributed network defense schemes was proposed in 2001 [8]. However, not much other similar research has been reported since then, to the best of our knowledge. Different from their proposal of only describing a preliminary agent-based model without concrete experiments, this paper presents our efforts in a specific evaluation based on a more deliberate three-layered network model.

3. Small-World Network Based Modeling Platform

Many network security applications are based on traffic monitoring. The more traffic information is obtained, the more confident security applications are. In order to achieve the best performance, security applications are preferable to be deployed at the gateway of the intended networks. In practice, it has been a trend to integrate traffic monitoring functions into routers for a simple solution. Nowadays, many advanced commercial-available routers are security enhanced. Not only software applications are implemented, hardware based applications are also embedded for advanced security improvement.

Essentially, distributed collaborative security defense is set up on top the cooperation of their corresponding network devices. The upper-level application chooses the countermeasure, while the lower-level agent supports its execution. Special channels are reserved for this collaboration, in order to avoid the interference with normal traffic. In this section, taking advantage of small-world network theory, an abstract three-layer platform is built for this modeling study.

3.1 Small World Network

The real Internet is a scale-free network [2]. A scale-free network is a network whose degree distribution approximately follows the power law [3]. Most nodes in a scale-free network have only one or two links, while only a few nodes have a large numbers of links. These small portion numbers of nodes act as hubs responding for the connection of the whole network.

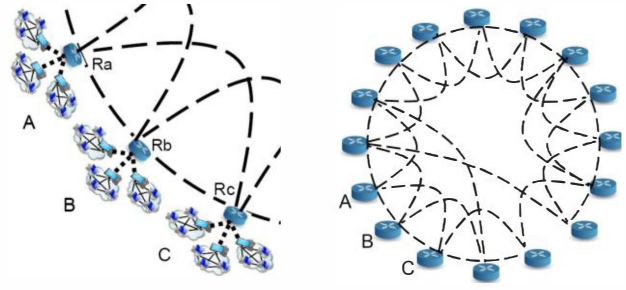
Figure 2 (a) represents a segment of Internet in logic. With the connection to router R_a, R_b, and R_c respectively, end hosts belonging to different network domain A, B, and C are able to communicate with each other. In addition, multiple logic links among R_a, R_b, and R_c make the communication more efficient by choosing optimal paths. For example, directly forwarding packets from domain A to C through the shortest links between R_a and R_c without passing R_b. Therefore, routers R_a, R_b, and R_c play critical roles as gateway hubs bringing local network A, B and C together to form a larger network.

The theory of small-world network well describes a simplified scale-free network. A small-world network is a network being mostly local-connected but with a few global connections. In fact, many real-world networks could be well described using small-world network models, such as cells [14], social networks [25], World-Wide Web [11] and the Internet [1]. Watts and Strogatz model is the most famous small-world network model. It is a random graph generation model that produces graphs with short average path lengths and high clustering [26]. It is the foundation of our modeling platform.

Figure 2 (b) illustrates a classic small-world network. This modeled network consists of finite numbers of nodes. Each node represents a network domain. Let's assume that each network domain has only one outlet to the Internet. Actually, it is true in many cases. The dashed lines represent logic links among different networks domains over Internet at the abstract level. The graph in Figure 3 shows an example generated with the specific approach that we employed to construct such a small-world network. The whole network contains 50 nodes. Each node is connected to 2 nearest neighbors and has the probability of 0.175 to add another edge. Small-world networks set up the basic topology for our intended network layers.

3.2 Structure of Three-layered Modeling Platform

As demonstrated in Figure 4, the platform that we developed for the modeling of collaborative schemes consists of three layers. From the bottom to the top, they



(a) A segment of Internet in logic **(b) A simplified network representation**

Figure 2 Illustrations of Logic Networks

are the Internet layer, overlay-network layer and application layer, respectively. The development of bottom two layers is inspired by the Watts and Strogatz small-world network model. The Internet layer models an abstract Interment environment in general, while the overlay network layer models a dedicating environment for the running of different collaborative schemes. Finally, the application layer focuses on the description of defense schemes.

As shown in Figure 4, each solid node in the bottom Internet layer represents a network domain participating collaborative defense and the hollow nodes are network domains that do not participate in the collaboration. The dashed lines present the physical network topology. The middle overlay network layer consists of those network domains that participate in collaborative defense. The solid lines in this layer represent the logic connections among these nodes.

In this model, link weight is adopted as the metric of distance between nodes. One hop is the minimal distance between any neighboring network domains. For example, in Figure 4, nodes A and B, nodes B and C are adjacent respectively, so that the weight of $Link_{ab}$ and $Link_{bc}$ are one. Meanwhile, the weight of $Link_{ac}$ is two.

However, their link weights may not remain the same when corresponding nodes are mapped to the bottom Internet layer. Though Node A' and B' still appears to be adjacent, Node B' and C' are four hops away from each others, so the weight of $Link_{b'c'}$ is four. As illustrated by Figure 4, there are three other network domains on the path from B' to C'.

In the Internet layer, the six-degree-of-separation theory [17] points it out that the average width of a large scale network is six. Specific to the Internet, relative research [29] has statistically verified that more than 99% of network domains in Internet could be reached within six hops. In our work, the weight assigned to the associated links follows normal distribution.

The top layer is the application layer, which is a conceptual layer where we define defense schemes. This layer focuses on the behavior description of participant network domains in an abstract manner. As shown in Figure 4, stars represent security applications deployed on top of corresponding network domains. The cloud generalizes the defense schemes organizing these applications for reaction.

Three types of defense schemes are described in this layer: the single-point defense scheme, centralized and decentralized collaborative defense schemes. All three defense schemes are applied to the same constellation of security applications, but with different concentration on network coverage. The first single-point scheme concentrates on the protection of individual network domains. Each security applications work independently. The other two collaborative schemes, instead, concentrate on the protection of a wide range network area. Through multi-domain collaboration, valuable information is shared among individual security applications for the improvement of overall performance.

4. Internet Worm Attack and Defense

Based on above developed modeling platform, a preliminary study comparing three different defense schemes has been conducted to investigate their performance against a typical Internet worm attack. This section describes the following two parts: modeling a worm attack, and modeling corresponding defense schemes.

4.1 Modeling a Worm Attack

Featuring self-duplication and automatic propagation, Internet worms are truly autonomous during attack. They are able to spread over the network, breaking into end hosts and replicating. It is extremely challenging to prevent Zero-day worms. In addition, worms themselves

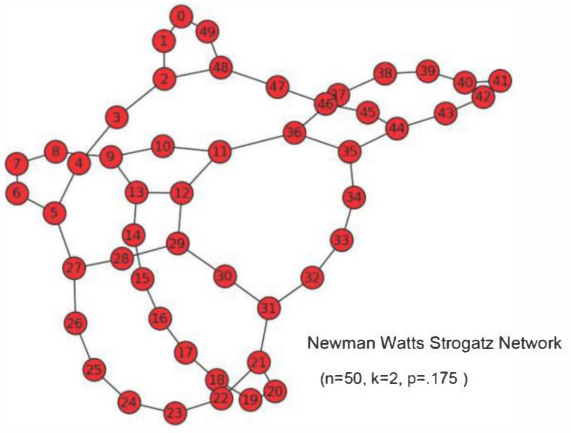


Figure 3. An example of small-world based network.

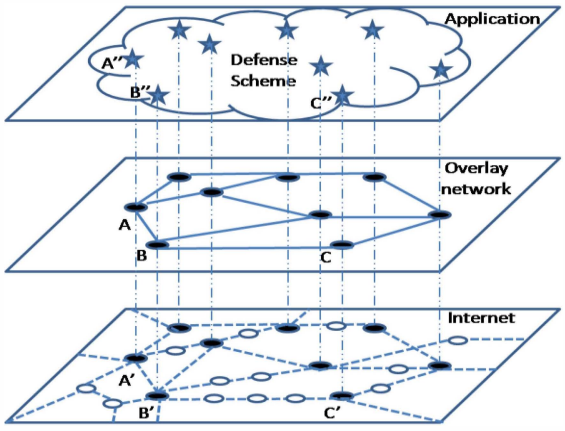


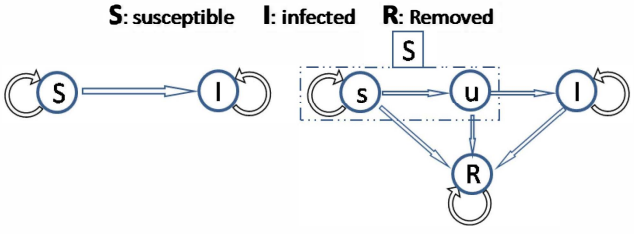
Figure 4. Structure of Three-layered Network Model.

are good carriers for other malicious attacks. Some sophisticated worm attacks intend to propagate stealthily so as to survive for further actions, such as remote control of infected hosts for launching DDoS attacks.

Various strategies have been adopted to achieve fast propagation, such as exploring security holes, increasing scanning rate with different scanning schemes [7, 24]. The propagation of most Internet worms shows certain similarity. After a short period of modest increase, the number of infected network domains presents an exponential growing. Once reaching the maximum infection, the corresponding curve trends to be flat, if there is no effective way for containment. At that time, a wave of worm attack enters a saturate state.

We modeled the worm attack as follows. Assume there is only one type of worm in the whole process. The infection of network domains follows the simple classical epidemic model (SI model) as shown in Figure 5 (a). Participant nodes in the interested space have two states: "Susceptible (S)" and "Infected (I)". They are all initialized to be susceptible to the attack. One of the participant nodes is randomly selected as the first infected node. Most likely, worms propagate to all the neighbor nodes from the current infected node. This propagation follows the network topology at the Internet layer as shown in Figure 4. For a small chance, it may propagate any nodes within the space directly.

The SI model only considers the attack under pure infection mode. With the engagement of all kinds of defense efforts, worms may be detected and contained. Consequently, network domains may be immune from this attack, regardless their current status either in susceptible or infected state. The adapted SIR model depicts such an infection/recovery scenario as shown in Figure 5 (b). A "Removed (R)" state is introduced. Once entering the "Removed" state, the current network domain is recovered and become invulnerable to the worm. We also adjusted the "Susceptible (S)" state in the original SI model to "susceptible (s)" and "under-attacking (u)" sub-states for the clarification of different situations when a susceptible network domain enters "Removed" state.



(a) Pure Infection mode (SI model) **(b) Adapted Infection /Recovery Mode (SIR model)**

Figure 5 Infection/Defense modes

4.2 Modeling Defense Schemes

The adaptive SIR model also describes the basic behaviors of individual security applications. We assume the immunity of network domains to worm attacks results from the reaction of security applications. Each security application plays as an agent for reaction. Although individual defense behaviors may vary, the collective behaviors determine the overall effectiveness.

Single-point defense scheme is inefficient facing fast propagation, wide spread and stealth Internet worms. For example, considering the security applications modeled in the application layer of Figure 4, network domains A′, B′ and C′ adopts different security applications A″, B″ and C″, respectively. While B″ has detected the signature of a worm on network B′, neither A″ nor C″ has detected that network A' has been infected. Since all the applications work individually, the successful detection at B″ does not imply that other network domains can get any benefit. Their collective behavior shows that the overall reaction efficiency of security applications running under the single-point defense scheme is low. It highly depends on the performance of each individual.

In contrast, collaborative defense can significantly improve the effectiveness. Benefiting the earlier alarm and assistance from B″, C″ can start and optimize its defense in advance, and A″ will realize what happened and start to contain the maliciousness so as to minimize the negative impact.

The on-the-fly collaboration runs seamlessly without human intervention. As the result, corresponding network domains are all saved from the attack. The overall reaction effectiveness of participants running under the collaborative scheme is higher. Their performance is correlated and significantly impacted by the first agent reacting to the attack. Theoretically, the larger the numbers of network domains involve and the wider the area they span for co-defense, the higher the probability would be for prompt detection.

Due to the different collaborative strategies, centralized and decentralized schemes have been proposed as the improvement on top of the single-point defense scheme. The individual behaviors of the participant agents remain the same, but obviously their collective behaviors are changed. In this study, we will focus on different defense behaviors with or without collaboration.

The collaborative defense of participant agents running under the decentralized scheme behaves similar to social network activities. Besides defending individually, they interact with peers for information sharing and decision making. This type of collaboration is flat, no agent is dominative. We assume that all agents only collaborate with their neighbors and all neighbors have the same significance to each other. On one hand,

each agent still makes decision individually, but takes the reference from its neighbors under consideration, such as: issuing an alarm for the worm attack. On the other hand, each agent acts as a relay that efficiently passes the proper information to others, such as: spreading the issued worm alarm to its peers. Individual agents are highly flexible in collaboration.

In the centralized scheme, all the collaborative activities run under a root-leaves structure. A centralizer acts as the root that is in charge of the whole collaboration. It may locate in any of the participating network domains. This centralizer has reliable communication with all the participants. Security applications act as leaves, collecting and pre-screening useful information to the root. Through the analysis of gathered information, corresponding feedback is returned from the root to all the leaves. Obviously, the overall efficiency of agents running under this scheme is more consistent than what the decentralized scheme can achieve.

5. Experiments and Performance Evaluation

This section presents the simulation results and the performance evaluation of this preliminary comparison study. The simulation experiment is discussed in detail, including the basic assumptions, parameters, and attack-and-defense operations. Through the analysis of simulation results, the performance of both centralized, decentralized collaboration schemes for distributed defense and the single-point scheme for individual defense have been evaluated.

5.1 Simulation Setup

In simulation, the operation of attack and defense is relatively independent from each other. According to the platform shown in Figure 4 earlier, the simulation of a worm attack is conducted in the Internet layer. The propagation of worms spreads through the paths defined in this layer. Their targets are those susceptible interested network domains (solid nodes). The propagation does not stop as long as any susceptible node has not been compromised in the interested network space.

The simulation of defense is carried out in the overlay network layer. The whole constellation of security applications applied to this layer act as agents. They take the defense schemes from the upper layer to protect the corresponding network domains mapped in the lower layer. The collaboration among agents follows the topology defined in this layer. The defense countermeasure will not stop until either all the solid nodes in the Internet layer are alarmed or all the nodes are immune from the worm, depending on the detail setup for simulation.

The appearance of the first infected node triggers the worm attack towards the interested network area. This node is randomly selected from the interested network domains in the Internet layer at the beginning of the simulation. After that, worms propagate following the described modeling approach.

Meanwhile, the location of the centralizer is also randomly assigned to one of the participant network domains. Through the association with its related defense agent, it records all the shortest paths from the related agent to all the other agents as defined in the overlay network layer. The structure for centralized collaboration is set up during the initialization of simulation.

The first alarm for worm detection from a defense agent triggers the whole defense reaction. This triggering event is associated with the progress of worm propagation. With the propagation of worms through the network space, the probability of being detected also grows. The worm packets are detectable once corresponding signatures have been identified [5].

Basically, our simulation process follows the adaptive SIR model as show in Figure 5(b). Those event-triggered activities could be well manageable under a Finite State Machine (FSM) mechanism. The simulation is executed with a discrete time scale. The execution time of each activity is scaled to one or multiple time slots. The complete worm propagation procedure consists of three phases: online probe, data transmission and local infection. For simplicity, we just assume that the time delay for one node infection is one unit time slot.

Considering that transferring 100k data in 100M/bps takes 1 *ms*, while infecting a node takes a few seconds. It is obvious that the infection time is dominative in a simple worm propagation scenario. From the perspective of defenders, the time for alarm spreading is expected to be short due to the utilization of reserved channel for collaboration. However, the overhead that resulted from the collaboration among different agents is non-trivial.

To describe the variable security vulnerabilities that network domains possess, we randomly assigned the resistant time of each network domain to worm attack from 1 – 3 unit time slots, following the normal distribution. It means that the most vulnerable network domains would be infected in one unit time, and the least vulnerable network domains would also be infected in 3 time slots, if there is no available defense.

At the defenders' side, assume the time delay of information exchange is one unit time for collaboration between adjacent agents in decentralized scheme, or between agents and centralizer in centralized scheme. The collaborative activities include alarm spreading, and advanced knowledge sharing which includes the updated signatures. It is also assumed that the execution time for all the local activities is one unit time, including the alarm issuing, the advanced knowledge issuing, relying determining and knowledge updating. Except the original agent issuing the alarm or other advanced knowledge, all the other agents have to receive the updated knowledge

and finish the update processing in order to contain worms in their network domains.

Although it may be disputable that worm signatures are generated and ready for spread just one unit time later after the worm alarm is issued in our simulation, it does not affect the relative defending trends after the knowledge update processing is finished in local agents. The only difference lies on the start point for reaction along the time axle during simulation.

5.2 Experimental Results and Discussion

According to the above description, we conducted extensive simulation experiments on worm attack-and-defense atop the modeling platform. The sample of the first set simulation consists of 200 security applications in the overlay layer. Mapping to the Internet layer, they correspond to 200 intended network domains. Taking advantage of Watts-Strogatz network function, we generated a small-world network environment for the Internet layer with n = 200, k = 2, p = 0.4. The average distance between any two adjacent nodes is 5.514, which is acceptable for the number representation of un-intended network domains in between them along the way. Since the nodes in overlay network are usually tightly connected in logic, their average distance between any pair of adjacent nodes should be shorter. Thus, we increase the link probability for setting up the topology of Overlay network layer, as n = 200, k = 2, p = 0.6.

5.2.1 Simple SI Model

Figure 6 demonstrates the modeled the worm propagation without any defense. The X axis represents the time ticks. The Y axis represents the number of network domains (nodes). The red line represents the increasing trend of worm infection over all of the network domains. The line that consists of small dots records the total number of infected nodes. The green line represents the decreasing of susceptible nodes due to the increase of infected nodes. The blue spots at the bottom indicate the number of newly infected nodes in each time unit.

In order to present a clear view of their variation, we used the log scale of the representation of values in Y axis. The number of infection nodes stays small at the both ends, but it is large in the middle. This is because the exponential increase of worm propagation usually happens in the middle with respect to the whole progress.

Figure 7 shows the alarm spreading after the worm attack is detected. The purple line across through the end-to-end from the left-bottom to the right-up represents the referred number of infected nodes. It is identical to the red infection line in Figure 6. The shape is different because Y axis is normal scaled, which represents the number of alarmed nodes. One difference between the centralized and the de-centralized collaborative schemes is that the knowledge update or alarm generated by the center server is sent to each agent to contain the worms, not by itself.

In this simulation, it is assumed that when 60% of the network domains have been infected, the worm is detected and the first alarm is generated. In Figure 7, the blue cubic box on the purple curve marks this point. Referring to the X axis, it is time for issuing the first alarm from that agent. The red line represents the agents working under single-point defense scheme, the blue and green lines represent agents working under centralized and decentralized defense schemes, respectively.

As expected, the red line is almost flat during the whole simulation period since none of the peer agent is expected to be able to share the alarm. For centralized and decentralized schemes, the alarm quickly spreads to all the defense agents through the topology built in the overlay network layer. This topology models the paths for collaboration. It is obvious that centralized scheme is more efficient for alarm spreading with the same set of collaborative nodes and the same network topology.

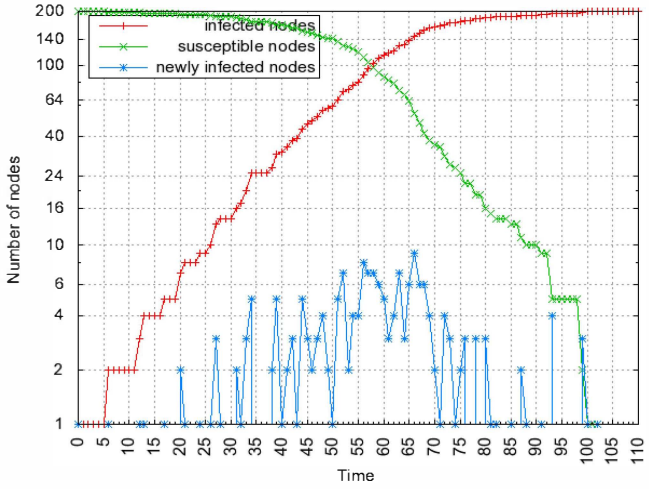


Figure 6 Pure Worm Infections without Containment

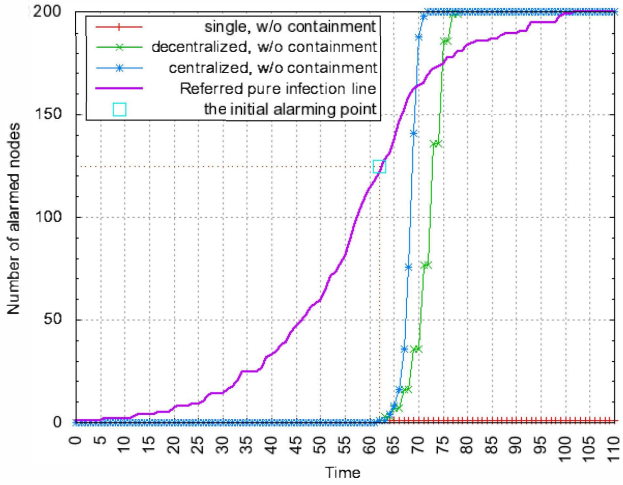


Figure 7 Alarming for Worm Attack

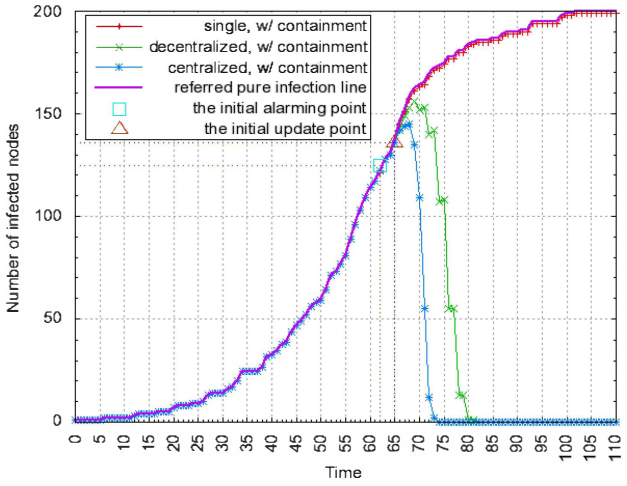


Figure 8. Trends of Infected Nodes with Containment.

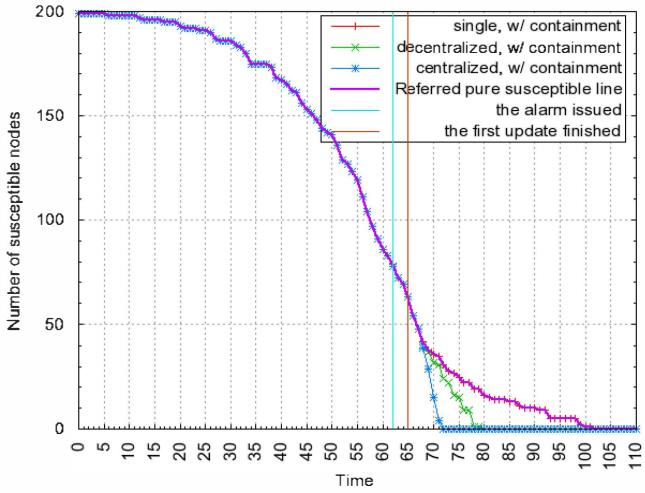


Figure 9. Trends of Susceptible Nodes with Containment.

5.2.2 The SIR Model

For further insight of the impact of different defense schemes, we simulated the defeat scenario. Once a worm attack has been detected and an alarm has been issued, the security agent continues to update its knowledge base and spread the newly generated signatures to peers for worm containment. Through sharing the signatures database, other agents can effectively prevent the attack.

Figure 8 presents the scenario of worm containment. The curves reflect the number of infected nodes along the time. The referred pure infection line and the initial alarming point remain the same with previous examples for consistency. The difference is that the initial update point is introduced, which represents the time point when first agent has finished knowledge updating and is ready for worm containment. The trend of red line that represents the defense running under single-point scheme almost keeps the same with the purple referred pure infection line. Since only one node is alarmed and become immunity from the attack, all other nodes still vulnerable and get infected.

Two collaborative defense schemes show much better containing efficiency. As observed, the trends of blue and the green lines turn down sharply after a small delay. The blue line represents the number of infected nodes under the centralized scheme, while the green line represents that under the decentralized scheme, respectively. Finally, the former touches the ground at the 74th tick, and the latter touches down at the 82th tick in this case.

From another perspective, the decreasing trend of susceptible nodes along the time also supports observation that collaborative schemes are efficient in defense. As illustrated in Figure 9, the first and second vertical lines from the left to the right represent the initial alarm time line and the initial update time line as described in the previous example. The trend lines regarding different defense schemes are overlapped at most of time. The interested points is that two lines with respect to the centralized and decentralized schemes divert shortly after they pass the initial update line, and quickly diminish to zero at the 74th and the 82th tick, respectively. This quick diminishment is due to the efficient signature database update of both collaborative schemes. Before being attacked by the worm, they have already been immunity.

To reveal the overall efficiency of different defense schemes against worm attack, we further explored the ratio between the immune and infected nodes in our simulation. Figure 10 gives an alternative view for this exploration. The immunity ratio is defined as:

$$\frac{number\ of\ immune\ nodes - number\ of\ infected\ nodes}{total\ number\ of\ nodes}$$

At the beginning of the simulation, none of node is infected nor immunity from the worm, so the immunity ratio is zero. Without effective containing measures, the quick propagating worms quickly pulls the immunity ratio down to negative and finally locks it to the fully infected

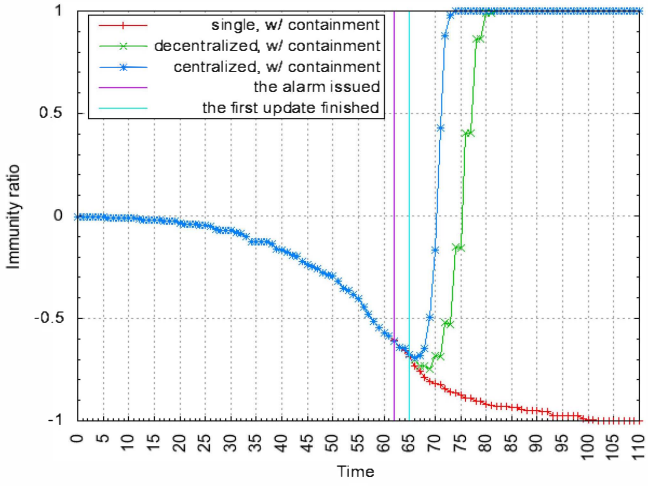


Figure 10. Overall Defense Efficiency.

status at -1, or -0.995 in terms of single-point defense scheme. However, this ratio could also be pulled up with the efforts of proper countermeasures. As observed in Figure 10, the trend lines corresponding to two collaborative schemes quickly rise up and finally enter full immune status at 1. In fact, the trends really depend on two facts: the efficiency of collaboration and the detection delay of worm.

The second set of simulation exhibits the impact of variable alarming times to the overall worm defense, as shown in Figure 11. The X axis lists a range of different ratio of the compromised network domains in percentage, at which the first alarm is issued. The Y axis represents the alarm correlated infection rate when the first alarm reaches all the agents. For consistency, all the experimental configurations are same as the previous examples. This set of simulation studies the different compromised node ratio from 0.0 to 0.99 with an interval of 0.02. In order to achieve a refined output, every data point in Figure 11 is the average of 5 experiments. Intuitively, the early the alarm is issued, the lower the correlated infection rate would be, if no further containing action follows up. From the top down, the infection rate of decentralized scheme is higher than that of centralized scheme under the same alarming rate. It is obvious that both infection rates trend to full when the compromised ratio moves from 0 to 99%.

Furthermore, we have compared the infection rate and the corresponding containment. They become flat even the first alarm being continuously postponed. It is due to the reaction of containment. After alarm and the following update signatures are shared, more and more security agents are capable of containing the worm. They lower infection rate of the network space.

We also have evaluated the scalability of collaborative defense schemes. The configuration remains the same, except with different number of collaborative nodes for

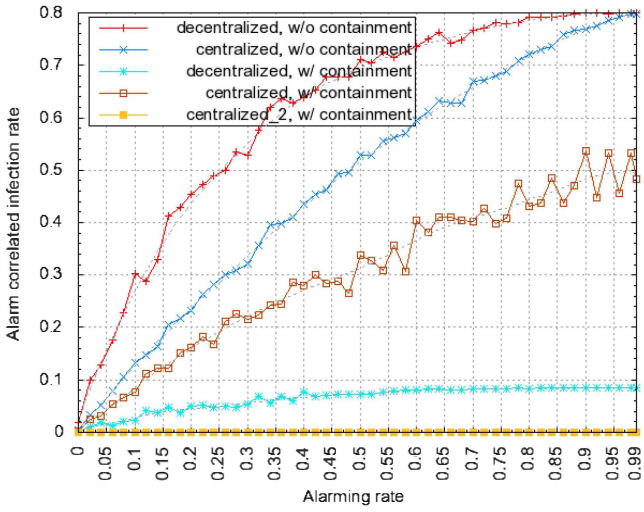


Figure 11 Correlated Infection Rate with Variable Compromised Node Ratio

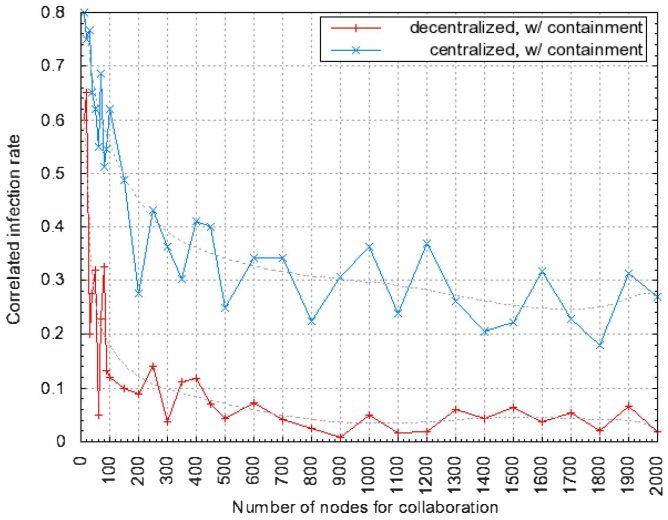


Figure 12 Correlated Infection Rate under Different Collaborative Scales

operation each time. Figure 12 presents the simulation results. Number of nodes was from 10 to 2000. According to the simulation result, although the vibration of infected rate is still obvious, they trend to flat when the collaboration scale is great than 200 nodes. The correlated infection rate of centralized scheme is higher than that of decentralized scheme when both are under the same simulation conditions.

6. Conclusion

This paper reports our efforts of a comparison study on the characteristics of different collaborative defense schemes against the Internet worm attacks. Based on the small-world network model, our experimental results have verified that both centralized and decentralized collaborative schemes can effectively improve the system performance comparing to single-point defense scheme. Based on a survey of related work, most reported research is application-dependable and specific problem based solution. Our work provides a new insight of collaborative strategies on a higher abstract level.

References

[1] R. Albert, H. Jeong, and A.-L. Barabási, "Internet: Diameter of the World-Wide Web," *Nature,* vol. 401, pp. 130-131, 9 September 1999.

[2] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature,* vol. 406, pp. 378-382, 27 July 2000.

[3] A.-L. Barabási and E. Bonabeau, "Scale-Free Networks," *Scientific American,* vol. 288, pp. 50-59, 2003.

[4] H. Chen and Y. Chen, "A Novel Embedded Accelerator for Online Detection of Shrew DDoS Attacks," in *Networking, Architecture, and Storage, 2008. NAS '08. International Conference on*, 2008, pp. 365-372.

[5] H. Chen, D. H. Summerville, and Y. Chen, "Two-stage decomposition of SNORT rules towards efficient hardware implementation " in *7th International Workshop*

on Design of Reliable Communication Networks, 2009 (DRCN 2009) Washington, DC 2009, pp. 359 - 366

[6] J. Creasey, "Threat Horizon 2010," *ISF 08 04 03,* 2008.

[7] R. Dantu, J. Cangussu, and A. Yelimeli, "Dynamic Control of Worm Propagation," in *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)*, 2004, pp. 419-423.

[8] D. Frincke and E. Wilhite, "Distributed network defense," in *IEEE Workshop on Information Assurance and Security*, West Point, NY, 2001, pp. 236-238.

[9] T. Gamer, M. Scharf, and M. Schöller, "Collaborative Anomaly-Based Attack Detection " in *Lecture Notes in Computer Science*. vol. 4725, ed: Springer Berlin / Heidelberg, 2007, pp. 280-287.

[10] D. M. Gorman, J. Mezic, I. Mezic, and P. J. Gruenewald, "Agent-Based Modeling of Drinking Behavior: A Preliminary Model and Potential Applications to Theory and Practice," *American Journal of Public Health,* vol. 96, pp. 2055-2060, 2006.

[11] B. A. Huberman and L. A. Adamic, "Internet: Growth dynamics of the World-Wide Web," *Nature,* vol. 401, p. 131, 9 September 1999.

[12] Internetworldstats.com. (2009, *World Internet Usage and Population Statistics*. Available: http://www.internetworldstats.com/stats.htm

[13] R. Janakiraman, Waldvogel, M., Zhang, Q., "Indra: A peer-to-peer approach to network intrusion detection and prevention," in *Proceedings of 12th IEEE Workshops on Enabling Technologies,Infrastructure for Collaborative Enterprises (WETICE)*, Los Alamitos, 2003.

[14] H. Jeong, B. Tombor, R. Albert, Z. N. Oltvai, and A.-L. Barabási, "The large-scale organization of metabolic networks," *Nature,* vol. 407, pp. 651-654, 5 October 2000.

[15] J. Kannan, L. Subramanian, I. Stoica, and R. H. Katz, "Analyzing cooperative containment of fast scanning worms," in *Proceedings of the Steps to Reducing Unwanted Traffic on the Internet Workshop*, Cambridge, MA, 2005, pp. 3-3.

[16] M. Allman, E. Blanton, V. Paxson, and S. Shenker, "Fighting Coordinated Attackers with Cross-Organizational Information Sharing," in *The Fifth Workshop on Hot Topics in Networks (HotNets '06)*, Irvine, CA, 2006.

[17] S. Milgram, "The Small World Problem," *Psychology Today,* vol. 2, pp. 60-67, 1967.

[18] J. Mirkovic, M. Robinson, and P. Reiher, "Alliance formation for DDoS defense," in *Proceedings of the 2003 workshop on New security paradigms*, Ascona, Switzerland, 2003, pp. 11-18.

[19] D. Moore, C. Shannon, G. M. Voelker, and S. Savage, "Internet Quarantine: Requirements for Containing Self-Propagating Code," in *IEEE Infocom*, San Francisco, CA, USA, 2003.

[20] G. Oikonomou, J. Mirkovic, P. Reiher, and M. Robinson, "A Framework for a Collaborative DDoS Defense," in *Computer Security Applications Conference, 2006. ACSAC '06. 22nd Annual* Miami Beach, FL 2006, pp. 33-42

[21] H. Ringberg, A. Soule, and M. Caesar, "Evaluating the Potential of Collaborative Anomaly Detection," in *In submission*, 2009.

[22] D. Schnackenberg, Holliday, H., Smith, R., Djahandari, K., Sterne, D, "Cooperative intrusion traceback and response architecture (CITRA)," in *Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX)*, 2001, pp. 56-58.

[23] A. Soule, H. Larsen, F. Silveira, J. Rexford, and C. Diot, "Detectability of Traffic Anomalies in Two Adjacent Networks," in *Lecture Notes in Computer Science*. vol. 4427/2007, ed: Springer Berlin / Heidelberg, 2007, pp. 22-31.

[24] A. Wagner, T. Dubendorfer, B. Plattner, and R. Hiestand, "Experiences with worm propagation simulations," in *Proceedings of the 2003 ACM workshop on Rapid malcode*, Washington, DC, USA, 2003, pp. 34-41.

[25] S. Wasserman and K. Faust, *Social network analysis: methods and applications*. Cambridge: Cambridge University Press, 1994.

[26] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature,* vol. 393, pp. 440-442, 4 June 1998.

[27] Y. Chen and K. Hwang, "Collaborative Change Detection of DDoS Attacks on Community and ISP Networks," in *the IEEE International Symposium on Collaborative Technologies and Systems (CTS'06)*, Las Vegas, NV., USA, 2006, pp. 401-410.

[28] Y. Chen and K. Hwang, "Spectral Analysis of TCP Flows for Defense against Reduction-of-Quality Attacks," in *the 2007 IEEE International Conference on Communications (ICC'07)*, lasgow, Scotland, 2007, pp. 24-28.

[29] K. H. Y. Chen, and W.-S. Ku, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," *IEEE Transactions on Parallel and Distributed Systems,* vol. 18, pp. 1649 -1662 December 2007.

[30] W.-S. K. Y. Chen, and K. Hwang, "Distributed Change-Point Detection of DDoS Attacks: Experimental Results on DETER Testbed," in *DETER Community Workshop on Cyber Security Experimentation and Test, in conjunction with USENIX Security Symposium (Security' 07)*, Boston, MA, 2007, pp. 7-7.

[31] G. Zhang and M. Parashar, "Cooperative defence against DDoS attacks," *J Res Pract Inf Technol* vol. 38, pp. 69-84, 2006.

[32] C. V. Zhou, S. Karunasekera, and C. Leckie, "A Peer-to-Peer Collaborative Intrusion Detection System," in *13th IEEE International Conference on Networks, Jointly held with the IEEE 7th Malaysia International Conference on Communication*, Kuala Lumpur, Malaysia, 2005, p. 6.

[33] C. V. Zhou, C. Leckie, and S. Karunasekera, "Decentralized multi-dimensional alert correlation for collaborative intrusion detection," *J. Netw. Comput. Appl.,* vol. 32, pp. 1106-1123, 2009.

[34] C. V. L. Zhou, C. Karunasekera, and S. T. Peng, "A Self-Healing, Self-Protecting Collaborative Intrusion Detection Architecture to Trace-Back Fast-Flux Phishing Domains " *IEEE NOMS Workshops 2008. ,* pp. 321 - 327 7-11 April 2008.

[35] Z. Zhou, D. Xie, and W. Xiong, "A P2P-Based Distributed Detection Scheme against DDoS Attack " in *First International Workshop on Education Technology and Computer Science, 2009. ETCS '09.*, Wuhan, Hubei 2009, pp. 304 - 309

[36] L. Zonglin, H. Guangmin, Y. Xingmiao, and Y. Dan, "Detecting distributed network traffic anomaly with network-wide correlation analysis," *EURASIP J. Adv. Signal Process,* vol. 2009, pp. 1-11, 2009.