**Failures/Attacks and Adaptable Self-healing Defense in Networks**

Bharat Bhargava ([bbshail@purdue.edu](mailto:bbshail@purdue.edu))

CERIAS security center, Purdue University

**1. Abstract**

Attacks against networked systems are becoming more complex and powerful. Individual attackers can collaborate to cause more problems for the intruder-identification and defense mechanisms. Models for cooperation need to be studied along with adaptable defense mechanisms. We also need to characterize various types and models of attacks through experimental studies of detailed attack logs that are available from various intrusion detection systems (IDS). We thus plan to study the impact of collaborative attacks on throughput, data delivery, denial-of-service, and routing. This research will lead to guidelines for developing adaptable defenses that can deal with type, severity, timing, extent, duration, and collaboration present in attacks. We will study Internet as well as mobile ad hoc environments. Experimental studies will integrate ideas from networking, distributed systems, and security/reliability research and will answer questions about performance and implementation of large networks under multiple attacks. They will also provide us with empirical parameters and observations that can be used in peer to peer, cooperative systems, and large-scale applications.

**Intellectual Contribution:** Collaborative attacks are an emerging threat in the cyber space, but little is understood. Understanding, characterizing, and modeling them will bring insights into better defending against them. The intellectual merits of this project are:

* *Characterizing failures and attacks:* This research will contribute towards a comprehensive study and characterization of the type, duration, ordering, and impact of failures and attacks. It will benefit and contribute to better understating of how the networks of future will self heal and provide non-stop operational capability.
* *Identification of intruders:* Techniques to identify malicious nodes which give false information about distance to destination and claim to have the most recent routes in mobile ad hoc networks. The ideas of suspicion list, black lists and bypassing the misleading nodes will be investigated to provide algorithms for routing during black hole and wormhole attacks.
* *Modeling adaptable defense:* Theoretic models will be developed to help understand, analyze, and defend against attacks from a whole-system perspective. We are interested in answering questions such as: Which aspects of a networked system have a significant impact on its vulnerability, and how to tune system configurations or parameters to defend and improve security?
* *Adaptability to attacks:* The research in adaptability to failure will be extended for enhancing defense mechanism against various models and scenarios of attacks. The overheads of dealing with threats will correspond to the severity and timing of the attacks and the potential for damage to QoS and performance. Better models and specifications for adaptability will emerge based on guidelines derived from experimental studies and allow us to build future networks that are dynamically reconfigurable and autonomic.
* *Vulnerabilities and Safe/Secure Configurations:* The research will use attack graphs and causal graphs to model mischievous event ordering to identify defense events that can thwart progress towards unsafe operational modes. Coordinated defense events can be launched to protect the network and self heal wit dynamic reconfiguration.

**Industry Collaboration:** Experiments will be conducted on test beds or using simulation tools to study the impact of this work on self-healing of various aspects of networks. We will collaborate with our industry partner to develop specific experiments. One Ph. D student is working on these issues and will participate in research. We have built a reliable and adaptable distributed system called RAID which has demonstrated self-healing and tuning capabilities. The research received the best paper award in a database conference in 1988.

**Key Words**: Collaboration among Attacks; Adaptable Defense; Network Security; Experiments

# 2 Introduction

Security is a key challenge in network environments since most prominent protocols in use were designed without considering any prevention against miscreants. In particular, wired network environments like the Internet are faced with myriad of security attacks, including worms and viruses, denial-of-service (DoS), spam and phishing attempts, route manipulations, and domain name system (DNS) exploitations. Wireless networks, especially ad-hoc networks, also suffer from attacks such as denial-of-messages (DoM) where malicious nodes may prevent some honest ones from receiving broadcast messages, and replication attacks where adversaries insert hostile nodes into the network after obtaining secret information from

Captured nodes or infiltration. In addition wormhole and blackhole attacks along with collaboration among malicious nodes are problems.

The current approach to dealing with attacks is to deploy individualized security solutions. For example, anti-virus software is used to defend against worms and viruses, intrusion detection tools guard against scanning and DoS attacks, firewalls aim to protect against unwanted connection attempts, and mail filtering tries to foil spam and phishing attempts.

An important piece missing from the current research is an understanding of the coordination among attacks and/or the collaboration among various attackers. Attacks in Internet are so sophisticated that it is hard to imagine that individual attackers, even having taken over many machines, can launch complex and powerful attacks (i.e., without any coordination or collaboration between them). Many examples of likely coordinated attacks exist [40,42,43]. For instance, an illegal DNS zone transfer typically used to reveal the IP addresses of hosts present in an organization followed by scanning attempts to find vulnerable machines could involve coordination among attackers with varying expertise. The vulnerable machines could then initiate Web requests to download backdoors from sites hosted by the attacker and join attacker's army of machines. Similarly, spammers could collaborate with attackers in control of a set of Internet routers to get fake Internet routes installed. These routes can then be used to send spam and phishing emails without fear of detection. Yet another example of coordinated attack could occur in wireless ad-hoc networks, where various attacking machines could collude to incorrectly report routes. Unlike single and uncoordinated group attacks, coordinated attacks may cause more devastating impacts on the Internet or wireless environments as they combine efforts of more than one attacker. In mobile ad hoc network, identification of malicious activity is hard when one node misbehaves in route formation [3]. If multiple nodes act maliciously, simultaneously, or alternately, the schemes to deal with them will become very slow at most nodes.

In this proposal, we propose to address issues of characterizing, modeling, and defense against coordinated/collaborative attacks for wired and wireless environments. From one perspective, attacks may be classified into the following two categories: *Multiple attacks* occur when a system is disturbed by more than one attacker. *Attacks in quick sequence* is another way to perpetrate a coordinated attack by launching sequential disruptions in small intervals (usually shorter than one second). The attacks may also be concentrated on a *group of nodes* or spread to a *different group of nodes* just for confusing the detection/prevention system in place. From another perspective, coordinated attacks can be classified into *short-lived* and *long-lived* attacks. We develop and enhance the science to develop self-healing networks through theoretical models, simulations and experiments.

## Research Problems and Directions

The following research problems and ideas are proposed:

* *Characterizing attacks in the Internet:* An understanding of the modi operandi of attacks is essential for defending the network environments. Data from thousands of Intrusion Detection Systems (IDSs) and various darknets will be characterized and correlated to determine: Who do the attackers target over short and long periods of time? What kind of attack vectors do various organizations witness and is there any correlation between the attack vectors at various organizations? Could future attacks be predicted based on attack sequences that have already been witnessed? Do the machines used in launching attacks stay the same over time?
* *Modeling attacks in the Internet:* Theoretic models will be developed to help understand, analyze and defend such attacks from a whole-system perspective. Some problems of particular interest are: Which aspects of a networked system have a significant impact on its security, and how to tune system configurations or parameters so as to improve security? Can we quantify the attackers’ gain in power because of their coordination? Can we quantify the gain, if any, of defender’s power because of the attackers’ coordination? As we will show through a preliminary result, novel stochastic models could be built for this purpose.
* *Identification of intruders and coordinated defense for the Internet:* Two systems to defend against coordinated and collaborative attacks will be developed. The goal of the first system, BehaviorAlert, is to reliably record behavior of Internet hosts in a timely fashion so servers and other Internet entities can prioritize trustworthy clients and refuse packets and connections from known miscreants. The second system, BGP-Wayback, named after the routing protocol used in the Internet, aims to prevent misuse of Internet routing to launch coordinated attacks. To accomplish its goal, it will capture, record, and analyze precise routing information required to apprehend cyber-criminals that exploit vulnerability in Internet routing.
* *Modeling and defending against attacks in mobile ad-hoc networks:* The research will involve dealing with a variety of attacks in AODV, DSR, DSDV protocols and exploring approaches that minimize communication and data structures at each node. The objective is to ensure that all nodes in ad hoc network do not get classified as suspicious. How distributed trust can be used to identify malicious nodes?

# 3 Characterizing Collaborative Attacks in the Internet

## 3.1 Problem Statement

An understanding of the mechanisms used in launching coordinated attacks is critical to devising adequate defense mechanisms. Little is known about coordinated attacks in the Internet. In particular, answers to following questions need investigation. Who do the attackers target over short and long periods of time? What kind of attack vectors do various organizations witness and is there any correlation between the attack vectors at various organizations? Could future attacks be predicted based on attack sequences that have already been witnessed? Do the machines used in launching attacks stay the same over time? For coordinated attacks, many factors have to be considered such as the type of attack, the severity of attack, the extent of attack, and the communication between attackers among many others. An appropriate way of measuring the full impact composed of each one of these factors is needed.

## 3.2 Related Work

## Many research works have characterized specific Internet attacks or phenomenon using one or more sources of data. For instance, work in [17] has characterized spammer behavior. Works in [1, 94] focus on specific worm outbreaks and work in [93] characterizes DoS attacks in the Internet. The Internet Motion Sensor Project [120] has analysed botnets [122] and malware in peer-to-peer networks has been characterized in [123, 124]. Very few works have focused on correlating various attacks. Among the few such efforts is work in [11] which used data from approximately 1700 intrusion detection systems (IDSs) logged by the Dsheild project to perform the first Internet-wide attack correlation. Using one month of attack data, they found that 20% of the attacking IPs attack multiple networks and contribute to 40% of the total attacks in their data set. They looked at attacker behavior only on the order of minutes and found that shared attackers attack different networks within a few minutes of each other. Further, they found that IDSs can be divided into small groups of 4-6 members which experience highly correlated attacks, whereas IDSs in different groups see uncorrelated attacks. In addition to short-term correlations of the type discussed in this work, we are interested in understanding correlations among Internet attacks on a much longer time scale, on the order of many months and even years. Further, the novelty of our approach lies in consolidating the multiple views offered by the darknet and IDS data.

The idea of trust relationship is used [100, 4] to limit the number of clones a malicious node and defend against sybil attacks. However, no coordinated model is discussed in these works. In RIP of Internet [2], the detection of invalid routing announcements has been suggested. The response after detection and how to defend against such attacks remains a challenge. In [38], a stochastic model of coordinated internal and external attacks is used to study the characterization of attacks and defenses. In [53, 54], Data Routing Information (DRI) Table and Cross Checking are used to identify multiple black hole nodes cooperating as a group. In [14], general intrusion detection scheme for detecting local anomalies caused by adversaries is discussed. In [63], An on-demand routing protocol is proposed for ad hoc wireless networks to provide resilience to byzantine failures caused by individual or colluding nodes. In [40], a signature-based model is used to detect coordinated attacks. In [78], examination of differences observed between unused address blocks is used to detect distributed blackhole placement. In [79], clustering and merging functions are used to recognize alerts that correspond to the same occurrence of an attack and create a new combined alert. In [83], a coordinated system using multicast, annotated topology information, and blind detection techniques to detect Distributed DoS attacks is discussed. In [101], Hidden Markov Models are used to detect coordinated attacks. In [57], many cyber attacks that consist of mutliple sub-attacks have studied. The coordinated attacks are a strict superset of these multistep attacks. Further, we are interested in 1) classifying different types of coordinated attacks in the Internet using IDS data, 2) creating taxonomy of prevalent methods of launching coordinated attacks, and 3) modeling coordinated attacks.

## 3.3 Proposed Work and Sample Research Task

The goal is to characterize attacks occurring in the Internet using intrusion logs from thousands of IDSs and using the darknet data. We plan to characterize attacks and by gaining an understanding of the mechanisms their perpetrators use. Toward this goal, we will use logs from multiple sources. Our first source of data includes intrusion data from a large number of intrusion detection systems (IDSs). In collaboration with Prof. Minaxi Gupta at Indiana University,we have already acquired 1.5 years of data from the Dshield project [91] which contains voluntarily submitted intrusion logs from about 2000 IDSs from all over the world. Dr Gupta is in the process of acquiring data from the myNetWatchman project [92], which also contains IDS logs from over a thousand IDSs. Our second source of data includes darknet data, which is essentially a capture of packets directed at unused IP address ranges. Such packets are malicious or misdirected by their very nature and many organizations and universities are beginning to advertise their unused address ranges to contribute toward understanding attacker behavior. An example of a project that collects darknet data is the Internet Motion Sensor Project [120]. REN-ISAC center [121] at Indiana University is beginning to collect darknet data through a strategic alliance of many universities. The research involves correlating data from these two very diverse sources to infer attacker behavior over a period of time. In preliminary findings using five months of Dshield data, we observe:

- A significant percentage of attacking machines continue to be active month after month. The networks to which these machines belong continue to stay active in even higher percentages. This indicates that blacklisting offending machines and networks could be viable defense.

- Upwards of 90% attackers are active only for a day in any given month. The same is true of the subnets that these machines belong to.

The research task is to investigate if any patterns exist in how attacking machines are rotated. We plan to study who these machines attack against over long periods of time, where they are geographically, who they belong to, which attack vectors they use, and if any correlations exists among the organizations being attacked. The output of this research will offer insights into defending against organized Internet crime.

Another task is to identify and classify multiple attacks.Examples of attacks include replication attacks [33], sybil attacks [34, 35], spam attacks, phishing attacks, worms and viruses, DNS-related attacks, routing-related attacks, denial-of-messages (DoM) attacks [36], and denial-of-service (DoS) attacks [110, 111, 112]. The research invovles comprehensive feature analysis encompassing feature detection and feature extraction toward a robust classification of coordinated attacks. This will require a mechanism for learning the patterns of the attacks based on adaptive learning algorithms [114, 115, 119] such as fuzzy logic [56]. The approach is to classify the attacks in some order such as a hierarchy. Three possible categories are as follows:

1. **Independent:** Attacks in this category have no knowledge of other attacks. But this type of attacks can be launched at the same time as other attacks.
2. **Collaborative**: Attacks in this category can be launched simultaneously. From high-level functional point of view (e.g., target of the attack, which could be contents of email, files stored on the server, or the access logs of users, etc), we further identify the relationships between the launched attacks and classify the attacks as: i) overlapping, ii) non-overlapping, and iii) fully-overlapping*.* Attacks may target different parts of the network and be launched together to deplete the resources of defenders.

From low-level technical point of view (e.g. techniques employed by attackers, such as packet spoofing, packet eavesdropping, etc), attacks can be categorized into: attacks that may overtake each other, attacks that may diminish the effects of each other, attacks that damage each other, attacks that may expose other attacks, attacks that may be launched after each other, and attacks that may target different areas of the network

1. **Replicated**: The replication attack is an attack with which adversaries can insert additional replicated hostile nodes into the network after obtaining some secret information from the captured nodes or by infiltration [5, 6]. Thus, the replicated nodes are likely to have the shared secrets with the uncompromised neighboring nodes. Encrypted communication links are established between the replicated node and the nodes in the original network. As the result, the compromise of even a single node might allow an adversary to gain partial or even full control of the network by cloning the nodes and deploying them into the original network.

**Sample Experiment**

Coordination parameters have been studied in a different context other than attacks in Internet and wireless networks [105, 106, 117, 118]. We propose to identify parameters for classifying coordinated attacks. We plan to conduct experiments to determine the coordination parameters.

**Objectives:** We plan to conduct experiments and simulations to identify the conditions when two or more attackers coordinate to cause more damage. We also conduct experiments to identify essential coordination parameters.

**Performance Metrics:**

How many nodes in the network are attacked by the coordinated attacks?

How many nodes in the network are infected by the coordinated attacks?

What is the effect of collaboration attacks on packet flow and recovery time?

What parameters can be used for adaptability to attacks?

Can the coordinated attacks cause more damage to computer networks and systems? If yes, under what conditions?

Can coordinated attacks leave more traces and evidences than individual attacks?

**Variable Parameters:** number of attackers, number of concurrent coordinated attacks, number of nodes in network, and number of distinct types of attacks involved. Other parameters for attack classification are: type, timing, severity and strength of attack, extent of attack, familiarity and role of attacker, communication between attackers, and attack and defense strategies.

**Method:**

a. Use a combination of different parameters to identify the attacks and find the essential parameters. We will use feature extraction to learn the patterns of the attacks based on learning algorithms and fuzzy logic [56].

b. After the essential parameters are identified, we will build a robust and precise classification model to classify attacks, using learning algorithms such as SVM [108].

c. Utilize the experimental tools such as DETER and EMIST [8, 107, 113] to do real-world evaluation of the attacks and generate real-world data. We plan to build the database for at least 5,000 coordinated attacks.

d. Build another database for evidence and trace analysis by running experiments and simulations. We will identify the attacks first, then order the coordinated attacks based on the amount of traces and evidences.

**Observations and Directions for Conclusions**

Based on the data from experiments, we like to tune the attack parameters for which adaptability defense mechanisms need to be developed. Administrators can understand the severity of the attacks, know the probability of tracing back the attackers and collecting evidences, and use this value to determine how much manpower to assign to the corresponding attack.

**3 Summary:**

Adaptability and self-healing algorithms and protocols can be developed based on a series of experiments. The costs will involve monitoring of network and evaluating the extent of vulnerabilities and strengths of attacks and impact of failures in a run-time system. Dynamic reconfiguration ideas and virtualization technologies will be used to see which self-healing schemes can provide the best results. More details can be provided in an extended document.

# 4 References (Detailed-Not all are used in this proposal)

1. D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the Slammer Worm," IEEE Security and Privacy journal, Aug 2003
2. Dan Pei, Dan Massey, Lixia Zhang, Detection of Invalid Routing Announcements in the RIP Protocol", GLOBECOM, December 2003
3. W. Wang, Y. Lu, and B. Bhargava , On Security Study of Two Distance Vector Routing Protocols for Mobile Ad Hoc Networks in Proceedings of IEEE International Conference on Pervasive Computing and Communications (PerCom'03), Dallas-Fort Worth, Texas, March, 2003
4. Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, and Abraham Flaxman, "SybilGuard: Defending Against Sybil Attacks via Social Networks." Proceedings of ACM SIGCOMM Conference, September 2006.
5. H. Chan, A. Perrig, and D. Song. Random key pre-distribution schemes for sensor networks. In Proc. of 2003 IEEE Symposium on Research in Security and Privacy, Orland, Florida, USA, January 2003.
6. H. Fu, S. Kawamura, M. Zhang, and L. Zhang. Replication attack on random key pre-distribution schemes for wireless sensor networks. In Proc. of the 6th IEEE Information Assurance Workshop, West Point, New York, USA, June 15–17, 2005.
7. S. Kawamura and H. Fu. Blom-based Q-composite: A Generalized Framework of Random Key Pre-distribution Schemes for Wireless Sensor Networks. Tech. Rep. #06-01, Oakland University, Oakland, MI, February 2006.
8. Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebar, Ian Pratt and Andrew Warfield , Xen and the Art of Virtualization, In the Proceedings of the ACM Symposium on Operating Systems Principles (SOSP), October 2003
9. G. Vigna, S. Eckmann, and R. Kemmerer. The stat toolsuite. In Proceedings of DISCEX, 2000.
10. V. Yegneswaran, P. Barford, and J. Ullrich. Internet intrusions: Global characteristics and prevalence. In Proceedings of ACM SIGMETRICS, 2003.
11. Sachin Katti, Balachander Krishnamurthy and Dina Katabi, Collaborating Against Common Enemies, ACM Internet Measure Conference (IMC) 2005.
12. M. Srivastava, “Wireless Sensor & Actuator Network Security: A User’s Perspective”, ACM Workshop on Security of Ad Hoc and Sensor Networks, October 2004.
13. D. Wagner, “Sensor Network Security: Breakthroughs, Game-changers, and Open Problems”, ACM Workshop on Security of Ad Hoc and Sensor Networks, October 2004.
14. W. L. Du, L. Fang, P. Ning, “LAD: Localization Anomaly Detection for Wireless Sensor Networks”, In Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, April 2005.
15. “Information security: Where the dangers are,” Wall Street Journal (online), July 2005,http://online.wsj.com/public/article/SB112128442038984802-w4qR772hjUeqG%T2W0FIcA3\_FNjE\_20060717.html.
16. Y. Rekhter, T. Li, and S. Hares, “A border gateway protocol 4 (BGP-4),” IETF RFC 4271, 2006.
17. Ramachandran and N.Feamster, “Understanding the network-level behavior of spammers,”in ACM SIGCOMM, 2006.
18. S. Murphy, “BGP security vulnerabilities analysis,” IETF RFC 4272, 2006.
19. S. Kent, C. Lynn, and K. Seo, “Secure border gateway protocol (S-BGP),” IEEE Journal on Selected Areas in Communications, vol. 18, no. 4, pp. 582–592, 2000.
20. R. White, “Securing BGP through secure origin BGP (soBGP),” The Internet Protocol Journal, vol. 6, no. 3, pp. 15–22, 2003.
21. Y. C. Hu, A. Perrig, and D. Johnson, “Efficient security mechanisms for routing protocols,” in Internet Society Network and Distributed System Security Symposium (NDSS), 2003.
22. Y. C. Hu, A. Perrig, and M. Sirbu, “SPV: Secure path vector routing for securing BGP,” in ACM SIGCOMM, 2004.
23. L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. H. Katz, “Listen and whisper: Security mechanisms for BGP,” in NSDI, 2004.
24. T. Wan, E. Kranakis, and P.C. van Oorschot, “Pretty secure BGP (psBGP),” in Internet Society Network and Distributed System Security Symposium (NDSS), 2005.
25. J. Karlin, S. Forrest, and J. Rexford, “Pretty good BGP: Improving BGP by cautiously adopting routes,” in IEEE ICNP, 2006.
26. “Routeviews project,” http://www.routeviews.org.
27. “Spamhaus home page,” http://www.spamhaus.org.
28. “Dsheild project,” http://www.dsheild.org.
29. “my—NetWatchman home page,” http://www.mynetwatchman.com.
30. “Snort home page,” http://www.snort.org.
31. R. Mahajan, D. Wetherall, and T. Anderson, “Understanding BGP misconfiguration,” in ACM SIGCOMM, 2002.
32. V. Paxson, “End-to-end routing behavior in the Internet,” in IEEE/ACM Transactions Of Networking, Pages 601-615, 1997.
33. J. Newsome, E. Shi, D. Song and A. Perrig, “The Sybil Attack in Sensor Networks: Analysis and Defenses”, In Proceedings of 3th International Symposium on Information Processing in Sensor Networks, Pages: 259-268, Berkeley, California, 2004.
34. Q. H. Zhang, P. Wang, D.S. Reeves, P. Ning, “Defending against Sybil Attacks in Sensor Networks”, In Proceedings of the 2nd International Workshop on Security in Distributed Computing Systems conjunction with the 25th International Conference on Distributed Computing Systems , Pages: 185-191, Columbus, OH, June 2005.
35. B. Parno and A. Perrig and V. Gligor, “Distributed Detection of Node Replication Attacks in Sensor Networks”, In Proceedings of IEEE Symposium on Security and Privacy, Pages: 49-63, May 2005.
36. J. McCune, E. Shi, A. Perrig and M. K. Reiter, “Detection of Denial-of-Message Attacks on Sensor Network Broadcasts”, In Proceedings of IEEE Symposium on Security and Privacy, Pages: 64-78, May 2005.
37. S. Staniford-Chen and et. al. GrIDS – A graph-based intrusion detection system for large networks. In 19th National Information Systems Security Conference, 1996.
38. X. Li and S. Xu, “A Stochastic Modeling of Coordinated Internal and External Attacks,” submitted to Dependable Systems and Networks (DSN) 2007. Availble at [http://www.cs.utsa.edu/~shxu/dsn07-sub.pdf](javascript:ol('http://www.cs.utsa.edu/~shxu/dsn07-sub.pdf');)
39. R. Albert, H. Jeong, and A. Barabasi. Error and attack tolerance of complex networks. Nature,406:378482, 2000.
40. Jiahai Yang, Peng Ning, X. Sean Wang, and Sushil Jajodia. *CARDS: A distributed system for detecting coordinated attacks*. In Proceedings of IFIP TC11 Sixteenth Annual Working Conference on Information Security, pages 171 -- 180, Aug 2000..
41. R. Ortalo, Y. Deswarte, and M. Kaaniche. Experimenting with quantitative evaluation tools for monitoring operational security. IEEE Trans. Softw. Eng., 25(5):633–650, 1999.
42. J. García, F. Autrel, J. Borrell, Y. Bouzida, S. Castillo, F. Cuppens et G. Navarro. Preventing coordinated attacks via alert correlation . 9th Nordic Workshop on Secure IT Systems (NORDSEC 2004). Finland, Nov 2004.
43. M. Little and C. Ko, **Detecting coordinated attacks in tactical wireless networks using cooperative signature-based, MILCOM 2005, Oct 2005**
44. N. Bailey. The Mathematical Theory of Infectious Diseases and Its Applications. 2nd Edition. Griffin, London, 1975.
45. R. Chinchani, A. Iyer, H. Ngo, and S. Upadhyaya. Towards a theory of insider threat assessment. In 2005 International Conference on Dependable Systems and Networks (DSN’05), pages 108–117, 2005.
46. P. Ammann, D. Wijesekera, and S. Kaushik. Scalable, graph-based network vulnerability analysis. In Proceedings of the 9th ACM conference on Computer and communications security (CCS’02), pages 217–224, 2002.
47. H. Wang, C. Guo, D. Simon, and A. Zugenmaier. Shield: vulnerability-driven network filters for preventing known vulnerability exploits. In Proceedings of the ACM SIGCOMM 2004, pages 193–204, 2004.
48. BerkeleyDB download page, http://search.cpan.org/dist/BerkeleyDB/.
49. R. Albert and A. Barabasi. Statistical mechanics of complex networks. Reviews of Modern Physics, 74:47–97, 2002.
50. P. Erdos and A. Renyi. On the evolution of random graphs. Publications of the Mathematical Institute of the Hungarian Academy of Sciences, 5:17–61, 1960.
51. I. F. Akyildiz and X. Wang. A Survey on Wireless Mesh Networks. *IEEE Communications Magazine*, 43(9):S23–S30, 2005.
52. Global Mobile Information Systems Simulation Library web page, http://pcl.cs.ucla.edu/projects/glomosim/
53. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks,” ICWN’03, Las Vegas, NV, USA, Jun. 2003
54. Sanjay Ramaswamy, Huirong Fu, and Kendall E. Nygard, “Effect of Cooperative Black Hole Attack on Mobile Ad Hoc Networks,” ICWN’03, Las Vegas, NV, USA, Jun. 2005.
55. Christoph L. Schuba, Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spafford, Aurobindo Sundaram, Diego Zamboni. Analysis of a Denial of Service Attack on TCP,IEEE Symposium on Security and Privacy,1997
56. L. A. Zadeh, Fuzzy logic = computing with words, IEEE Transactions on Fuzzy Systems, Vol. 4, No 2, pp. 104-111, 1996.
57. S. Cheung, U. Lindqvist, M. Fong, "Modeling Multistep Cyber Attacks for Scenario Recognition", DARPA Information Survivability Conference and Exposition (DISCEX III), pp. 284-292, Apr. 2003.
58. Srdjan Capkuny, Levente Butty´an, and Jean-Pierre Hubaux, “Self-Organized Public-Key Management for Mobile Ad Hoc Networks,”, IEEE Transactions on Mobile Computing, Jan 2003.
59. Vesa Kärpijoki, “Security in Ad hoc Networks,” <http://www.tcm.hut.fi/Opinnot/Tik-110.501/2000/papers/karpijoki.pdf>.
60. Janne Lundberg, “Routing Security in Ad Hoc Networks,” <http://citeseer.nj.nec.com/cache/papers/cs/19440/http:zSzzSzwww.tml.hut.fizSz~jluzSznetseczSznetsec-lundberg.pdf/routing-security-in-ad.pdf>
61. Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu, and Lixia Zhang, “Self-securing Ad Hoc Wireless Networks,” <http://www.cs.ucla.edu/~jkong/publications/ISCC02.pdf>.
62. Lidong Zhou and Zygmunt J. Haas, “Securing Ad Hoc Networks,” IEEE Network Magazine, vol. 13, no. 6, Nov./Dec. 1999
63. Baruch Awerbuch, David Holmer, Cristina NitaRotaru, and Herbert Rubens, “An On-Demand Secure Routing Protocol Resilient to Byzantine Failures,” In ACM Workshop on Wireless Security (WiSe) in conjunction with MobiCom 2002, Atlanta, Georgia, September 28, 2002
64. Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Network,” IEEE Communications Magazine, vol. 40, no. 10, Oct. 2002.
65. S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” 6th MobiCom, Boston, MA, Aug. 2000
66. M. Just, E. Kranakis, and Tao Wan, “Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks,” <http://www.scs.carleton.ca/~kranakis/Papers/adhocnow03.pdf>
67. K. Sanzgiri, B. Dahill, D. LaFlamme, B. N. Levine, C. Shields, and E. Belding-Royer,"A Secure Routing Protocol for Ad Hoc Networks". IEEE Journals on Selected Areas in Communications Special issue on Wireless Ad hoc Networks, March, 2005.
68. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions,” IEEE Wireless Communications, Vol. 11, No. 1, pp. 38-47, Feb. 2004.
69. CERT Coordination Center. “mstream” Distributed Denial of Service Tool, May 2, 2000. CERT Incident Note N-2000-05.
70. F. Cuppens and R. Ortalo. LAMBDA: A language to model a database for detection of attacks. In H. Debar, L. M´e, and S. F. Wu, editors, *Recent Advances in Intrusion Detection (RAID 2000)*, volume 1907 of *LNCS*, pages 197–216, Toulouse, France, Oct. 2–4, 2000
71. P. G. Neumann and P. A. Porras. Experience with EMERALD to date. In *Proceedings of the Workshop on Intrusion Detection and Network Monitoring*, Santa Clara, California, Apr. 9–12, 1999.
72. P. Ning, S. Jajodia, and X. S. Wang. Abstraction-based intrusion detection in distributed environments. *ACM Transactions on Information and System Security*, 4(4):407–452, Nov. 2001.
73. P. A. Porras, M.W. Fong, and A. Valdes. A mission-impactbased approach to INFOSEC alarm correlation. In A.Wespi, G. Vigna, and L. Deri, editors, *Recent Advances in Intrusion Detection (RAID 2002)*, Volume 2516 of *LNCS*, Pages 95–114, Zurich, Switzerland, Oct. 16–18, 2002.
74. L. Hu and D. Evans, .Using directional antennas to prevent wormhole attacks,. In Proceedings of Network and Distributed System Security Symposium (NDSS), 2004.
75. O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M.Wing. Automated generation and analysis of attack graphs. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, pages 273–284, Oakland, California, May 12–15, 2002.
76. S. J. Templeton and K. Levitt. A requires/provides model for computer attacks. In *Proceedings of the 2000 New Security Paradigms Workshop*, pages 31–38, Ballycotton Co., Cork, Ireland, Sept. 18–21, 2000.
77. Computer Emergency Readiness Team.http://www.us-cert.gov/.
78. E. Cooke, M. Bailey, D. Watson, F. Jahanian, and D. McPherson. Towards understanding distributed blackhole placement. In The 2nd Workshop on Rapid Malcode (WORM) Fairfax, Virginia, October 29, 2004.
79. F. Cuppens and A. Miege. Alert correlation in a cooperative intrusion detection framework. In IEEE Symposium on Security and Privacy, 2002
80. N. Habra, B. L. Charlier, A. Mounji, and I. Mathieu.ASAX : Software architecture and rule- based language for universal audit trail analysis. In ESORICS, 1992.
81. L. T. Heberlein, B. Mukherjee, and K. N. Levitt. Internet security monitor: An intrusion detection system for large-scale networks. In Proceedings of the 15th National Computer Security Conference, 1992.
82. J. Hochberg, K. Jackson, C. Stallings, J. McClary, and J. DuBois, D.and Ford. NADIR: An automated system for detecting network intrusions and misuse. In Proceedings of Computers and Security 12(1993)3, 1993.
83. A. Hussain, J. Heidemann, and C. Papadopoulos. COSSACK: Coordinated Suppression of Simultaneous Attacks. In DISCEX, 2003.
84. D. Moore, C. Shannon, G. Voelker, and S. Savage. Internet Quarantine: Requirements for Containing Self-Propagating Code. In INFOCOM, 2003.
85. W. Wang, B. Bhargava, Y. Lu, and X. Wu, Defending against Wormhole Attacks in Mobile Ad Hoc Networks, Wireless Communications and Mobile Computing (WCMC), vol. 6, issue 4, pp. 483-503, June 2006.
86. A. Snapp and et. al. Distributed intrusion detection system - motivation, architecture, and an early prototype. In Proceedings of the 14th NCSC, 1991.
87. E. Spafford and Z. D. Intrusion detection using autonomous agents. In Computer Networks, Volume 34, 2000.
88. [L. Qian](http://ieeexplore.ieee.org/search/searchresult.jsp?disp=cit&queryText=(lijun%20qian%3cIN%3eau)&valnm=Lijun+Qian&reqloc%20=others&history=yes),  [N. Song](http://ieeexplore.ieee.org/search/searchresult.jsp?disp=cit&queryText=(%20ning%20song%3cIN%3eau)&valnm=+Ning+Song&reqloc%20=others&history=yes) and [X. Li](http://ieeexplore.ieee.org/search/searchresult.jsp?disp=cit&queryText=(%20xiangfang%20li%3cIN%3eau)&valnm=+Xiangfang+Li&reqloc%20=others&history=yes).  Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path. IEEE WCNC, 2005.
89. D. Liu and P. Ning. Establishing pairwise keys in distributed sensor networks. In Proc. of the 10th ACM Conference on Computer and Communications Security (CCS’03), pages 52–61, Washington, D.C., USA, October 2003.
90. Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing Security in Wireless Ad HocNetwork,” IEEE Communications Magzine, Vol. 40, No. 10, October 2002.

[91] http://www.dshield.org/

[92] http://www.mynetwatchman.com/

[93] D. Moore, G. M. Voelker, and S. Savage, Inferring Internet Denial-of-Service Activity, Usenix Security Symposium 2001.

[94] D. Moore, C. Shannon, J. Brown, Code-Red: a Case Study on the Spread and Victims of an Internet Worm, ACM/USENIX IMW 2002.

[95] M. Gupta, M.H. Ammar, and M. Ahamad, Trade-offs Between Reliability and Overheads in Peer-to-Peer Reputation Tracking, Elsevier Computer Networks journal, Volume 50, Pages 501-522, August, 2005.

[96] H. Yu, J. Rexford, and E. Felten, A distributed reputation approach to cooperative Internet routing protection, IEEE Workshop on Secure Network Protocols (NPSec), 2005.

[97] The International PGP home page, http://www.pgpi.org/.

[98] The Bamboo distributed hash table, <http://www.bamboo-dht.org/>.

[99] J. Kephart and S. White. Directed-graph epidemiological models of computer viruses. In IEEESymposium on Security and Privacy, pages 343–361, 1991.

[100] Douceur, J. (2002). The Sybil Attack. 1st International Workshop on Peer-to-Peer Systems (IPTPS '02) , February 2002.

[101] D. Ourston, S. Matzner, W. Stump, and B. Hopkins. Coordinated internet attacks: responding to attack complexity. Journal of Computer Security. Vol 12, Issue 2, 2004, pp 165-190.

[102] S. Marti, T. J. Giuli, K. Lai, and M. Baker, .Mitigating routing misbehavior in mobile ad hoc networks,. in Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking, 2000.

[103] H. Yang, X. Meng, and S. Lu, .Self-organized network-layer security in mobile ad hoc networks,. in Proceedings of ACM Workshop on Wireless Security (WiSe), 2002.

[104] Y. Hu, A. Perrig, and D. Johnson, .Packet leashes: A defense against wormhole attacks in wireless ad hoc networks,. in Proceedings of IEEE INFOCOM, 2003.

[105] Roussev, V., Dewan, P., Jain, V. “Composable Collaboration Infrastructures Based on Programming Patterns”. In Proceedings of the 2000 ACM Conference on Computer-Supported Cooperative Work (CSCW). Dec 2000, Philadelphia, PA.

[106] J. Herlocker, J. Konstan, L. Terveen, and J. Riedl. Evaluating collaborative

filtering recommender systems. ACM Transactions on Information Systems, 22(1):5–53, January 2004.

[107] DETER: A Laboratory for Security Research, <http://www.isi.edu/deter/>

[108] N. Cristianini and J.Shawe-Taylor. An Introduction to Support Vector Machines and other kernel-based learning methods. Cambridge University Press, 2000

[109] W.Wang and B.Bhargava. Visualization of Wormholes in Sensor Networks, in Proceedings of ACM Workshop on Wireless Security (WiSe), October 2004.

[110] A. Habib, S. Fahmy, and B. Bhargava. Monitoring and Controlling QoS Network Domains, ACM/Wiley International Journal of Network Management, Vol. 15, Issue 1, Pages 11-29, Jan- Feb 2005.

[111] A. Habib, M. Hefeeda, B. Bhargava. ``Detecting Service Violations and DoS Attacks,” in Proceedings of Network and Distributed System Software (NDSS 2003), San Diego, February, 2003.

[112] A. Habib, S. Fahmy. S. Avasarala, V. Prabhakar and B. Bhargava, On Detecting Service Violations and Bandwidth Theft in QoS Network Domains, in Elsevier Science Journal of Computer Communication, Vol. 26, No. 8, pp. 861 - 871, 2003

[113] EMIST Tool Suite, <http://www.cs.purdue.edu/homes/fahmy/software/emist/>

[114] B. Bhargava and J. Riedl. A Formal Model for Adaptable Systems for Transaction

Processing, IEEE Transactions on Knowledge and Data Engineering, Vol. 4, No. 1, 1989,

pp. 433–449.

[115] B. Bhargava, S. Browne. “Adaptable recovery Using Dynamic Quorum Assignments,” in

Proceedings of the Sixteenth International Conference on Very Large Data Bases (VLDB),

Brisbane, Australia, Aug. 1990.

[116] J. Steffan, M. Schumacher. Collaborative Attack Modeling. 17th ACM Symposium

on Applied Computing (SAC 2002), Special Track on Computer Security, Madrid, Spain,

March 10-14, 2002

[117] T. Jaeger and A. Prakash, Requirements of Role-based Access Control for Collaborative

Systems, in Proc. of the First ACM Workshop on Role-based Access Control ,

Gaithersburg, MD, Nov. 1995.

[118] P. Dewan, V. Mashayekhi, and J. Riedl. Infrastructure and tools for collaborative software

engineering. In Tom Malone, Gary Olson, and John Smith, editors, Coordination Theory

and Collaboration Technology. Lawrence Erlbaum Associates, 2001.

[119] B. Bhargava, K. Friesen, A. Helal, and J. Riedl. Adaptability experiments in the RAID

distributed database system. In Proceedings of the IEEE Symposium on Reliability in

Distributed Systems, Huntsville, Alabama, October 1990.

[120] The Internet Motion Sensor Project, <http://ims.eecs.umich.edu/>.

[121] REN-ISAC Web page, <http://www.ren-isac.net/>.

[122] Evan Cooke, Farnam Jahanian, and Danny McPherson, “The Zombie Roundup:

Understanding, Detecting, and Disrupting Bots”, USENIX/ACM Internet Measurement

Conference (IMC), 2005.

[123] Andrew Kalafut, Abhinav Acharya, and Minaxi Gupta, “A Study of Malware in Peer-to-

peer Networks”, USENIX/ACM Internet Measurement Conference (IMC), 2006.

[124] Seungwon Shin, Jaeyeon Jung, and Hari Balakrishnan, “Malware Prevalence in KaZaA

File-Sharing Network”, USENIX/ACM Internet Measurement Conference (IMC), 2006.

[125] Vinod Yegneswaran, Paul Barford, and Somesh Jha, “Global Intrusion Detection in the

DOMINO Overlay System”, ISOC Network and Distributed System Security Symposium

(NDSS) 2004.

[126] Y. Hu and A. Perrig and D. Johnson. Rushing Attacks and Defense in Wireless Ad Hoc

Network Routing Protocols. Proc. of the 2003 ACM workshop on Wireless Secuity, 2003