RESEARCH REVIEW JOURNALS
Volume-03
Issue-11
November -2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Vulnerability Assessment of Routing Protocols in MANET

[*1]Kakkar Parveen, [2]Sharma Pooja & [3]Saluja Krishan

[*1]*Research Scholar, Computer Science & Engineering Department, IKGPTU, Kapurthala Punjab (India)*
[2]*Computer Science & Engineering Department, IKGPTU, Kapurthala, Punjab (India)*
[3]*Information Technology Department, University Institute of Engineering & Technology, Panjab University, Chandigarh (India)*

ARTICLE DETAILS

Article History
Published Online: 10 November 2018

Keywords
Denial of Service (DoS), Distributed Denial of Service (DDoS), Ad Hoc On-Demand Distance Vector Routing Protocol (AODV), Dynamic source Routing (DSR), MANET

[*]**Corresponding Author**
Email: parveen.daviet[at]gmail.com

ABSTRACT

Security is a weak link of network systems. The malicious usage and attacks have caused tremendous loss by impairing the functionalities of the computer networks. Among all network attacks, Denial of Service (DoS) and Distributed DoS (DDoS) attacks are two of the most harmful threats to network functionality. Mobile Ad Hoc networks are even more vulnerable to these attacks. Existing MANET routing protocols, such as Ad Hoc On-Demand Distance Vector Routing Protocol (AODV), do not provide enough security defense capacity. AODV is inherently vulnerable to many attacks viz. authentication, availability, integrity & confidentiality attacks. Major research efforts have been taken to solve this problem. But most of the proposed solutions are not feasible or practical for the operating MANETs.

1. Introduction

An ad hoc network is a collection of mobile nodes forming a temporary network without the aid of any centralized administration or standard support services [1]. Advances in wireless technology and portable computing along with demands for greater user mobility have provided a major impetus toward development of an emerging class of self-organizing, rapidly deployable network architectures referred to as ad-hoc networks. Ad-hoc networks are expected to play important role in future commercial and military settings where mobile access to a wired network is either ineffective or impossible. Potential applications for this class of network include instant network infrastructure to support collaborative computing in temporary or mobile environments, emergency rescue networks for disaster management, remote control of electrical appliance and mobile access to the global Internet. Furthermore, ad-hoc networks have the potential to serve as a ubiquitous wireless infrastructure capable of interconnecting many thousands of devices with a wide range of capabilities and uses.

A mobile Ad hoc network (MANET) is formed by a group of autonomous mobile nodes connected by wireless links, in which there is no backbone infrastructure [36]. The system may operate in isolation, or may have gateways to interface with a fixed network [49]. Ad hoc networks have no fixed routers; all nodes are capable of movement and can be connected dynamically in an arbitrary manner [47]. Usually, these nodes act as both end systems and routers at the same time. Nodes of these networks, which function as routers, discover and maintain routes to other nodes in the network. The topology of the ad hoc network depends on the transmission power of the nodes and the location of the Mobile Nodes, which may change with time. The nodes (a router with multiple hosts and wireless communications devices) are free to move about and organize themselves randomly. These nodes may be located in or on airplanes, ships, trucks, cars, or on very small devices, and there may be multiple hosts per router. As a result, the network wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. In general, Ad hoc networks are self-creating, self-organizing, and self-administrating networks. Hence, they offer unique benefits and flexibility for a variety of situations and applications. Because of these features, the Ad hoc networks are used where wired network and mobile access is either unproductive or not feasible. A few possible examples include: earthquake hit areas, where infrastructure is destroyed, military soldiers in a destructive environment; virtual classrooms, biological detection, tracking of rare animal, space exploration, and undersea operations.

Among the various research issues of MANET, security is considered the most difficult job. It demands attention to a number of new research challenges. Table 2 summarizes the security challenges in MANET in contrast to traditional systems. To address the security challenges, various solutions have been proposed. Survey of various security solutions for MANET have been provided in [4-7]. However, the need for an updated survey on MANET is desired. This research provides an updated account of currently available security solutions for MANET. The survey specifically ponders over the security solutions for routing, key management and intrusion detection in MANET. In addition, it provides a new classification for secure routing, key management and intrusion detection systems proposed in recent past for MANET.

Table 1. Research Issues in MANET

Physical Layer	Network Layer	Transport Layer	Application Layer
Antenna Design	Routing	Protocol Design	Service Discovery
Access Control	IP Address assignment		Data Management

Interference	Gateway		
MAC Addressing	Multicasting		
	Clustering		
Power Management			
QoS			
Standards			
Security			

Table 2: Some common DoS attacks [1].

Type of DoS Attack	Target	Exploited Vulnerability
Network Device Attack	Hardware Device (such as a Router)	Software bug in device's software
Operating System Level Attack	Operating System (OS Services)	Bug in OS software
Application Level Attack	Application Layer (Software Services)	Bug in victim software (usually identified through Port Scanning technique)
Data Flood Attack	Bandwidth or connection capacity of network	Limited bandwidth and server capacity to process requests (heavy traffic is sent towards victim to exhaust services)
Protocol Feature Attack	Protocol Services (mainly at network layer)	Limitation of a protocol such as IP address spoofing (Internet Protocol is a part of TCP/IP stack)

2. Distributed Denial of Service Attacks

In a Distributed Denial of Service (DDoS) attack, the attacker makes a huge impact on the victim by having multiplied power of attack derived by a large number of computer agents. It becomes possible for an attacker because he takes large number of computer machines under his control over the internet before applying an attack. In fact, these computers are vulnerable machines in the public network and attacker can exploit their weaknesses by inserting malicious code or some other hacking technique so that they become under his control. These compromised machines can be hundreds or thousands in numbers. They behave as agents of the attacker and are commonly termed as 'zombies.' The entire group of zombies is usually named as a 'botnet.' The size of botnet decides the magnitude of attack. For larger botnet (increased number of zombies in a botnet), attack is more severe and disastrous. Within a botnet, the attacker chooses 'handlers' which perform command and control functions and pass the instructions of attacker to zombies. The zombies directly attack on the victim. There is a group of zombies or agents under each handler. These handlers also pass the information received from zombies to attacker about the victim [2]. Therefore, handlers are the machines which directly communicate with attacker and zombies. As handlers and zombies are also compromised machines in the public network under attacker's control, the users of such machines are mostly unaware of the fact that there machines are being used as a part of some botnet. A typical architecture of DDoS attack is mentioned in Fig. 1. The attack employs client server technology and a stream of data packets is sent to the victim for exhausting its services, connections, bandwidth etc. The data flood attack type of DoS is mostly used in DDoS attacks.

Table 3: Classification of DDoS attacks—By exploited vulnerability [1].

Type of DDoS Attack	Target	Exploited Vulnerability	Method of Attack	Impact
UDP Flood Attack	Server or Network (Software Services/ Connection Capacity or Bandwidth)	Limited bandwidth and server capacity to process requests	Heavy traffic (UDP Packets) is sent towards victim with randomly selected destination port.	Victim replies with 'Destination Host Unreachable' packets. When it is kept busy continuously beyond processing capacity, it crashes. Network's bandwidth is also exhausted
ICMP Flood Attack	Network (Bandwidth)	Limited bandwidth	Heavy traffic (ICMP Packets) of 'Ping' requests is sent towards a machine on target network. They are sent directly or through Agents for larger impact.	Massive traffic is generated leading in bandwidth saturation.
TCP Flood Attack	Server or Network (Connection Capacity or Bandwidth)	Limited bandwidth and server capacity to process requests	Heavy TCP traffic (packets) of legitimate-like headers and random payload is sent towards victim.	Massive traffic is generated leading in bandwidth saturation and degradation of server's CPU consumption
Smurf Attack	Server or Network (Connection Capacity or Bandwidth)	Limited bandwidth and server capacity to process requests	Heavy traffic (ICMP Echo Packets) is sent towards victim with randomly selected destination port.	Massive traffic is generated leading in bandwidth saturation and degradation of server's CPU consumption (or it can even crash)

Fraggle Attack	Server or Network (Connection Capacity or Bandwidth)	Limited bandwidth and server capacity to process requests	Heavy traffic (UDP Echo Packets) is sent towards victim with randomly selected destination port.	Massive traffic is generated leading in bandwidth saturation and degradation of server's CPU consumption (or it can even crash)
Protocol Exploit Attack	Server (Connection Capacity)	Protocol feature (e.g., three-way handshake for TCP SYN attack)	Heavy traffic of spoofed SYN signals is sent towards victim. The ACK signals is not acknowledged by attacker.	Server waits for final acknowledgment for certain time. Buffer capacity is limited, hence it results in full queue buffer. New requests can not be processed
Malformed Packet Attack	Server (Processing Capacity)	Limited processing capability of server	Malicious packets are sent towards victim with manipulated entries in IP address fields	Server can not process malicious packets and can completely crash if traffic is too heavy

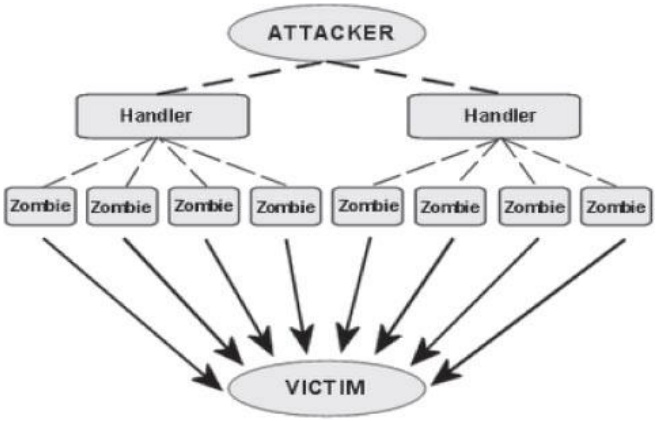

Figure 1: Architecture of DDoS Attacks

3. Secure Routing in MANET

Routing is one of the major concerns in MANET. The frequent changes in the network make it very difficult to maintain a consistent path from source to destination. Three types of routing protocols for MANET have been proposed in literature. The proactive protocols (DSDV, WRP, and OLSR etc.) are based on repeated advertisement of routing information to neighboring nodes. The reactive protocols are based on on-demand discovery of routing path (ADOV, DSR, TORA etc.). The hybrid protocols (ZRP) are combination of proactive and reactive approaches. Secure routing in MANET is a thorny job and requires dealing with various types of network layer attacks as discussed in previous section. Various secure routing approaches have been proposed in literature. Surveys on secure routing protocols have been provided in [9-12]. However, most of these surveys discuss the routing protocols proposed before 2005. They classify the secure routing protocols as preventive and reactive approaches. An updated classification of currently available security solutions can be done as follows:

- Protocols based on exploiting routing header information to identify malicious activities in the network
- Protocols based on cryptographic technique to protect routing header
- Protocols exploiting redundancy of routing Layers
- Protocols based on trust information to identify malicious activities in the network
- Protocols that maintain anonymity of routing entities.

3.1 Protocols Based on Routing Header Information

Some secure routing protocols are based on exploiting routing header information to identify malicious activities in the network. In this direction, [13] proposes a solution that identifies routing anomalies using the sequence number field of the routing packet. In routing protocols, a sequence number field defines the last packet received from a node. In case of normal routing operations, subsequent packets must have a higher sequence number. If a packet sequence number is less than previously received packet, misbehaviour is suspected. In the proposed approach, two small tables are maintained by every node on the network. These tables help in recognizing the sequence number changes. The first table keeps the sequence number of the last packet sent to other nodes on the network. The second table contains the sequence number of the last received packet by a node. During route discovery, once a RREQ reaches the destination, a RREP is generated. The RREP carries the last packet sequence number received from the source. By comparing the sequence number carried in the reply packet with the one maintained in local tables, any sequence number inconsistencies can be identified. [14] proposes an anomaly detection approach based on a dynamic training model. The proposal is based on the fact that during a black hole attack, the attacking node changes sequence number of the RREP to a considerably large value. Hence, a black hole attack can be recognized by analyzing the distribution of the sequence number in normal and anomalous state of the network. A feature vector is devised that comprises of number of sent routing requests, number of replies, average difference of sequence number when the request was sent and when it is received. Using a training data set, an attack model is devised. The mean value of the feature vector is calculated using the training data. The Euclidean distance of an input sample from the mean vector is calculated. If the distance is larger than a threshold value, it is classified as a black hole attack. At repeated intervals, the model is updated using previous interval data as a training

dataset. [15] proposes a scheme called DPRAODV to detect black hole attack based on the sequence number of RREP packets. If the sequence number is higher than a threshold, the node is marked as blacklisted. In this case, an ALARM message is generated to notify other nodes. To penalize the black listed node, the routing tables of the node are neither updated nor are their messages forwarded. To calculate the threshold value, the difference between sequence number of RREP packet and the value in the routing table is first calculated. The average of this difference value is set to the threshold value. The threshold value is updated as soon as a new RREP is received. In this way, the model detects the black hole as well as prevents the attack in some cases.

3.2 Cryptography Based Approaches

The techniques of cryptography have also been used to provide integrity, privacy and non-repudiation of the routing messages. Secure Ad hoc On-Demand Distance Vector routing (SAODV) is an asymmetric cryptographic approach that is based on signing the non-mutable fields of AODV routing request headers. Intermediate nodes verify that the fields have not changed before creating a reverse route. After verification, the node broadcasts the request to neighboring nodes. Similar procedure is applied during the RREP message. Authenticated Routing for Ad hoc Networks (ARAN) is a public key cryptography approach for providing secure routing in MANET. Every node has a certificate issued by a trusted third party. For route discovery, a node generates a request packet called RDP comprising of the IP of the destination, source certificate, a nonce and current time, signed by the source private key. The intermediate nodes verify the signature using the previous node's certificate (that is carried along with the request), sign the received message with their private key and append their own certificated with the message and rebroadcast. The destination generates a reply REP along the reverse route. The REP is signed by a node before it is forwarded to next node. The next node will verify the signature using the certificate of the previous node. Secure Routing Protocol (SRP) is a symmetric key approach based on establishing a security association between source and destination using a shared key. The shared key is set up using the other party's public key. All the communications are then encrypted and decrypted using the shared key. Ariadne provides security over the DSR protocol using TESLA protocol. During route discovery, the source node generates a routing request. The request among other things comprises of a hash chain and a message authentication code (MAC). MAC is computed over the initiator, destination, id of the message and the time interval fields. The hash list is initialized with the MAC. The intermediate node appends its own address to the list of nodes (as in DSR). The node id of intermediate node is then appended to the current hash value and the hash value is recomputed. The MAC code of the whole packet is also recomputed and appended to the MAC field. Using the node list field of DSR, the destination verifies the integrity of the packet by comparing the hash value specified in the packet with its computed value. endairA[16] is an inspiration of Ariadne protocol that instead of verifying the request, verifies the route reply messages. During route discovery, the request contains the identifier of source, destination and the generated request. Intermediate node appends their identifier to the packet and rebroadcast. When the packet reaches the destination, a route reply is generated and sent back through the reverse route. The reply comprises of the id of source and destination, the accumulated route and a digital signature. Intermediate nodes processing the reply verify the signature and ensure that next and preceding nodes are its neighbors. If the verification is done successfully, the intermediate node also signs the reply packet and forward to the next node. Another inspiration of Ariadne is APALLS [17] that is designed for providing non-reputable secure routing in MANET. The protocol assumes a network with a web server and certifying authority at the backend. During route discovery, RREQ includes digital signature of source, per-hop hash and an optional list of black listed nodes. Intermediate nodes verify the signature of the routing request. The destination node performs various consistency checks and then a reply RREP is generated. In case of any active attack in the network, a non-repudiable proof (signed packet of the attacker) is also generated.

3.3 Protocols Exploiting Redundancy of Routing Layers

These protocols make use of redundancy (multiple routing paths, routing protocols etc.) to ensure the delivery of a routing message through a safe path. [13] propose a solution in which the source node verifies the authenticity of the RREP initiator through network redundancy. It is an extension over AODV protocol. During route discovery, the node waits for more than one RREP through different paths. From the redundant paths, the source extracts common hops and then constructs a safest path to route the message. A slightly different strategy has been used in SPREAD[18]. The original routing message is first decomposed into small shares using threshold secret sharing algorithm. Multiple paths towards the source are then determined using an on- demand routing algorithm. The routes are selected keeping into consideration the security levels of the node. The shares of the message are then transmitted towards the destination through these routes. At the destination, different shares of the message are then combined to generate the original message. By using the threshold secret sharing algorithm, it is ensured that if some share gets corrupted by malicious nodes, the whole message can still be reconstructed. [19] proposes a scheme that employs multiple routing protocols. As different routing protocols are prone to different types of attacks, the idea proposed is to switch the routing protocol upon a particular type of attack detected on the network. The solution detects three types of attacks: black hole, routing table overflow and sleep deprivation torture attack. The black hole attack is detected by watch dog functionality. A node that transmits a message to next node monitors that if it is correctly forwarded by the next node or not. The routing table overflow attack occurs when the nodes along a route sends unnecessarily acknowledgment to the source. By sending a threshold value for the number of acknowledgement packets, this attack can be detected. The sleep deprivation torture occurs when during route discovery a node sends multiple route replies to the source, thus consuming the resources of the source. The approach adopted for the routing overflow attack detection can also be applied for detecting this type of attack. Once an attack is detected, switching of the routing protocol is done. If there is a black hole attack detected on the network, the algorithm tries

to switch to On-demand Secure Routing Protocol (OSRP); otherwise Secure Link State Routing Protocol (SLSP) is selected.

3.4 Protocols Based on Trust Models

These approaches are based on maintaining trust information about other nodes on the network. Un-trusted nodes are disregarded during routing operation. [20] proposed an association based routing approach where the most secured route is selected based on the node's trust value. The algorithm extends the DSR protocol. A node maintains the trust value of other nodes based on the packets exchanged and dropped by the nodes. Associations between nodes are thus defined. The association value can be un-known (low trust), known (nodes have exchanged some messages and have moderate trust) and companion (high trust levels as nodes have exchanged lot of message in past). During route discovery, multiple route replies are received from the nodes, as in DSR. The route replies are sorted by trust ratings. The most trusted route is then selected by the source node based on the trust values of the intermediate nodes. [21] proposed a trust model for secure routing. The trust vector is based on nodes experience, knowledge and recommendation of some other node x in the network. The experience is defined as the ratio of the number of packets forwarded by x to the number of packets transmission x is responsible for. The knowledge parameter is the probability that the data packet will be successfully transmitted between the nodes. The recommendation parameter is based on the recommendation information about x provided by other nodes of the network. Based on these parameters, a trust routing scheme has been proposed. During route discovery, a node sends the trust information about preceding node along with route request. This ensures the spread of trust information across the whole network. Using the available trust information, the proposed approach ensures the selection of a route with the highest trust value. [22] presents a secure routing scheme using trust levels. The ratio of the 'difference between beacons received and transmitted' to the 'beacons received by the node' is calculated. Based on this ratio, the nodes are sorted in descending order. The first one third of the nodes in the list is classified as ally, the next one third as associate and the last as acquaintance. During routing, a node selects the best neighbor (with the same trust level) and sends it the packet. The neighbor then selects the best node (with the same trust level) and propagates the request ahead. This process continues until the packet is received by the destination.

Table 4: Summary of secure routing protocols for MANET

Protocol	Techniques	Base Routing Protocol	Attack addressed	Brief Description
	Sequence Number Inconsistencies Multiple Routing Paths	AODV	Black Hole	Identify the anomalies by checking the sequence no of subsequent sent and received messages are larger than previous values Construct the safest path based on multiple path information from received multiple route replies.
	Dynamic Learning	AODV	Black Hole	An attack model is devised by analyzing the distribution of sequence number difference in normal and anomalous case.
DPRAODV	Limit on sequence Number of RREP	AODV	Black Hole	The Sequence number of RERP is compared against a threshold to identify the black hole attack
ARAN	Sign the request pkt	None	Modification, Fabrication & Impersonation	Digitally sign the routing messages using private key that are verified by next node using certificates
SRP	Encryption	ZRP	Modification, Fabrication & Impersonation	Establish security association using public key and then encrypt the communication using public key.
Ariadne	MAC, Hashing	DSR	Wormhole Attack, Modification, Fabrication	Using Hash chain & MAC list, verify the integrity of the messages using route request.
endairA	MAC, Hashing	DSR	Route Modification	Verify the integrity of route reply messages.
APALLS	Digital Signature	DSR	Non Repudiation	Intermediate nodes do verification using certificates, Non repudiation is achieved by assigned message from attacker
SEAD	Threshold secret sharing Algorithm	None	Eavesdropping, colluding attack, Modification	Splitting the message into multiple shares and reconstructs at the destination
	Multiple routing	SLSP,OSRP	Black hole, Sleep Deprivation and routing table overflow attack	Decides the routing algorithm based on the type of attack.
	Trust Models based on packet drop	DSR	Selective Packet drop attack	An optimal path is chosen based on the degree of association of node with neighbors
	Trust Model based on experience, knowledge recommendation	DSR, AODV	Black hole	Trust information is carried along with the routing request and ensure the selection of route with highest trust

	Trust Model based on beacons	NTP	Black hole	Trust is maintained based on beacons transmitted/received and trust routing is performed by selecting the best node in the same trust level

4. Conclusion & Future Scope

MANETs have risen in prominence in recent years due to the requirement for heterogeneous devices to be networked together seamlessly. However, there are many challenges to this network environment such as power constraints and lack of computational resources available for security functions. This ensures that this environment is vulnerable to many attacks such as DoS. Such attacks can withstand some common defense mechanisms like firewalls. In this paper we have investigated the vulnerability of Routing protocols in MANET. Firstly on the behalf of exploited vulnerability, common DDoS attacks are identified & further classified. Then the architecture of DDoS attack was discussed. Comprehensive survey of secure routing protocols was carried out. After survey we learnt that foremost DDoS Attack in MANET is the flooding attack and the most vulnerable protocol among all is AODV. In the future scope we will propose a noval technique to detect & mitigate the flooding attack against the vulnerability of AODV.

References

1. Mitrokotsa, A., and Douligeris, C., Denial-of-Service Attacks. Network Security: Current Status and Future Directions, Wiley Online Library, Chapter 8, 117–134 (2006).
2. Zhang, L., Yu, S., Wu, D., and Watters, P., A Survey on Latest Botnet Attack and Defense, Proceedings of IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 53–60 (2011).
3. Mishra, A., Gupta, B. B., and Joshi, R. C., A Comparative Study of Distributed Denial of Service Attacks, Intrusion Tolerance and Mitigation Techniques, Proceedings of IEEE European Intelligence and Security Informatics Conference (EISIC), 286– 289 (2011).
4. Ghazali, K. W. M., and Hassan, R., ‘‘Flooding distributed denial of service attacks—A review,’’ J. Comput. Sci., 7: 1218– 1223 (2011).
5. Beitollahi, H., and Deconinck, G., Denial of Service Attacks: A Tutorial, Electrical Engineering Department (ESAT), University of Leuven, Technical Report: 08-2011-0115 (2011).
6. Information WeekSecurity: hhttp://www.informationweek.comi (2012).
7. Business Insider: hhttp://articles.businessinsider.comi (2011).
8. SecureList: hhttp://www.securelist.comi (2012).
9. Prolexic Technologies: ‘‘Prolexic Attack Report Q1 2013,’’ hhttp://www.prolexic.comi (2013).
10. Conti, M., Chong, S., Fdida, S., Jia, W., Karl, H., Lin, Y. D., Mahonen, P., Maier, M., Molva, R., Uhlig, S., and Zukerman, M., ‘‘Research challenges towards the future internet,’’ Comput. Commun., 34: 2115–2134 (2011).
11. Chao-yang, Z., DoS Attack Analysis and Study of New Measures to Prevent, Proceedings of IEEE International Conference On Intelligence Science and Information Engineering (ISIE), 426–429 (2011).
12. Ahlawat, N., and Sharma, C., ‘‘Classification and prevention of distributed denial of service attacks,’’ Int. J. Adv. Eng. Sci. Technol., 3: 52–60 (2011).
13. Badishi, G., Herzberg, A., Keidar, I., Romanov, O., and Yachin, A., An Empirical Study of Denial of Service Mitigation Techniques. IEEE Symposium on Reliable Distributed Systems (SRDS), 115–124 (2008).
14. Subhashini, K., and Subbalakshmi, G., ‘‘Tracing sources of DDoS attacks in IP networks using machine learning automatic defence system,’’ Int. J. Electron. Commun. Computer. Eng., 3: 164–169 (2012).
15. Lin, S. C., and Tseng, S. S., ‘‘Constructing detection knowledge for DDoS intrusion tolerance,’’ Expert Syst. Appl., 27: 379– 390 (2004).
16. Wang, Y., Lin, C., Li, Q. L., and Fang, Y., ‘‘A queuing analysis for the denial of service (DoS) attacks in computer networks,’’ Comput. Network, 51: 3564–3573 (2007).
17. Douligeris, C., and Mitrokotsa, A., ‘‘DDoS attacks and defense mechanisms: Classification and state-of-the-art,’’ Comput. Network, 44: 643–666 (2004).
18. Aissani, A., and Achour, M. Y., Evaluation of the Severity of DoS Attacks on Computer Networks, Proceedings of IARIA 2nd International Conference on Performance, Safety and Robustness in Complex Systems and Applications (PESARO), 8–13 (2012).
19. Mirkovic, J., and Reiher, P., ‘‘A taxonomy of DDoS attack and DDoS defense mechanisms,’’ ACM SIGCOMM Comput. Commun. Rev., 34: 39–53 (2004).
20. Abliz, M., and Znati, T., New Approach to Mitigating Distributed Service Flooding Attacks, Proceedings of IARIA 7th International Conference on Systems (ICONS), 13–19 (2012).
21. Sen, J., Chowdhury, P. R., and Sengupta, I., A Mechanism for Detection and Prevention of Distributed Denial of Service Attacks, Distributed Computing and Networking, Lecture Notes in Computer Science (Springer-Verlag), 4308: 139–144 (2006).
22. Kang, S. H., Park, K. Y., Yoo, S. G., and Kim, J., ‘‘DDoS avoidance strategy for service availability,’’ Cluster Comput., 16: 241–248 (2013).
23. Lee, Y., and Lee, Y., Detecting DDoS Attacks with Hadoop, ACM CoNEXT Student Workshop (2011).
24. Beitollahi, H., and Deconinck, G., ‘‘Analyzing well-known countermeasures against distributed denial of service attacks,’’ Comput. Commun., 35: 1312–1332 (2012).
25. Tariq, U., Hong, M., and Lhee, K., A Comprehensive Categorization of DDoS Attack and DDoS Defense Techniques, Advanced Data Mining and Applications, Lecture Notes in Computer Science (Springer-Verlag), 4093: 1025–1036 (2006).
26. Peng, T., Leckie, C., and Ramamohanarao, K., ‘‘Survey of network-based defense mechanisms countering the DoS and DDoS problems,’’ ACM Comput. Surv., 39: 1–42 (2007).
27. Ying, Z., ‘‘Distributed denial of service attack principles and defense mechanisms,’’ Advances in Natural Science (CS Canada), 4: 15–17 (2011).

28. Loukas, G., and Oke, G., ‘‘Protection against denial of service attacks: A survey,’’ Comput. J., 53: 1020–1037 (2010).
29. Kumar, A. R., Selvakumar, P., and Selvakumar, S., Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment—A Survey on DDoS Attack Tools and Traceback Mechanisms, Proceedings of IEEE International Advance Computing Conference (IACC), 1275–1280 (2009).
30. Aamir, M., and Arif, M., ‘‘Study and performance evaluation on recent DDoS trends of attack & defense,’’ Int. J. Inf. Technol. Comput. Sci., MECS Publisher, 5: 54–65 (2013).
31. Ferguson, P., and Senie, D., Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing, RFC 2827 (2000).
32. Mirkovic, J., and Reiher, P., ‘‘D-WARD: A source-end defense against flooding denial-of-service attacks,’’ IEEE T Depend Secure, 2: 216–232 (2005).
33. Wang, H., Jin, C., and Shin, K. G., ‘‘Defense against spoofed IP traffic using hop-count filtering,’’ IEEE ACM T Network, 15: 40–53 (2007).
34. Eddy, W., TCP SYN Flooding Attacks and Common Mitigations, RFC 4987 (2007).
35. Gupta, B. B., Agrawal, P. K., Joshi, R. C., and Misra, M., Estimating Strength of a DDoS Attack Using Multiple Regression Analysis, Communications in Computer and Information Science (Springer), 133: 280–289 (2011).
36. Gupta B. B., Agrawal, P. K., Mishra, M., and Pattanshetti, M. K., On Estimating Strength of a DDoS Attack Using Polynomial Regression Model, Communications in Computer and Information Science (Springer), 193: 244–249 (2011).
37. Shannon, C. E., ‘‘A mathematical theory of communication,’’ ACM Mob. Comput. Commun. Rev., 5: 3–55 (2001).
38. Carl, C., Kesidis, G., Brooks, R. R., and Rai, S., ‘‘Denial-of-service attack-detection techniques,’’ IEEE Internet Computing, 10: 82–89 (2006).
39. Lung-Yut-Fong, A., Levy-Leduc, C., and Cappe, O., ‘‘Distributed detection/localization of change-points in high dimensional network traffic data,’’ Stat. Comput., 22: 485–496 (2012).
40. Li, L., and Lee, G., ‘‘DDoS attack detection and wavelets,’’ Telecommun. Syst., 28: 435–451 (2005).
41. Lu, W., and Ghorbani, A. A., ‘‘Network anomaly detection based on wavelet analysis,’’ EURASIP J. Adv. Sig. Pr. (2009).
42. Moore, D., Voelker, G. M., and Savage, S., Inferring Internet Denial-of-Service Activity, Proceedings of Usenix Security Symposium (2001).
43. Feinstein, L., Schnackenberg, D., Balupari, R., and Kindred, D., Statistical Approaches to DDoS Attack Detection and Response, Proceedings of IEEE DAPRA Information Survivability Conference and Exposition, 303–314 (2003).
44. Blazek, R. B., Kim, H., Rozovskii, B., and Tartakovsky, A., A Novel Approach to Detection of Denial-of-Service Attacks via Adaptive Sequential and Batch-Sequential Change-Point Detection Methods, Proceedings of IEEE Workshop on Systems, Man, and Cybernetics Information Assurance, 220–226 (2001).
45. Wang, H., Zhang, D., and Shin, K. G., Detecting SYN Flooding Attacks, Proceedings of IEEE 21st Annual Joint Conference on Computer and Communication Societies (INFOCOM), 1530–1539 (2002).

