Intrusion Detection in MANET using Neural Networks and ZSBT

D. Divya
Assistant Professor
Dept. of CSE
IFET College of Engineering
Villupuram

Abstract

Mobile ad-hoc network is a collection of mobile nodes that organize themselves into a network without any predefined infrastructure. The characteristics of MANET are dynamic topology; bandwidth and energy constrained and limited physical security. Due to the dynamic nature of the network, these networks can be easily vulnerable to attacks. Many type of attacks can threat the MANET and the classification of attacks are Black hole, Routing loops, Network partition, Selfishness, Sleep deprivation and Denial of Service. The MANET is mainly applied in military environments, personal area networking and emergency operations. This work provides a technique to improve the security level of MANET. The mechanism of intrusion detection is designed in MANET on the basis of artificial neural networks (ANNs) and Zone- Sampling Based Trace back algorithm (ZSBT) for detecting DOS attacks. Intrusion detection system is a type of security management system for computers and networks. The prevention mechanisms are thwarted by the ability of attackers to forge, or spoof, the source addresses in IP packets. By employing IP spoofing, attackers can evade from detection. But with the help of IDPF, the attacker node can be identified easily and it also has the ability to limit the IP spoofing capability. Artificial neural network and ZSBT modeling uses simulated MANET environments for detecting nodes under DOS attack effectively. But the ZSBT method works well for detecting DoS attacks in the network when compared with ANN methods.

Keywords

DOS attack, ANN, MANET, Intrusion detection, ZSBT, IDPF, IP spoofing.

1. INTRODUCTION

A MANET is a collection of mobile nodes that organize themselves into a network without any pre-defined infrastructure and mainly it is a dynamic network topology. The security goal of MANET includes availability, integrity, authentication, confidentiality and non-repudiation. Many types of attacks can threat the MANET such as Black hole, Routing loops, Network partition, Selfishness, Sleep deprivation and Denial of Services. This work mainly focuses on DOS attack. Therefore, nodes in MANETs are more vulnerable to DOS attacks. The attackers in MANET use IP spoofing to conceal their real identities and it becomes a challenging task to trace the remote attacker in MANET [1, 2]. Thus, the implementation of Zone Sampling-Based Trace back (ZSBT) algorithm is used for tracing DoS attackers in MANET and also improves the security level of MANET.

Intrusion detection systems (IDSs) [9] are the foremost tools for providing safety in computer and network system. There are many limitations in traditional IDSs like time consuming, regular updating, non adaptive, accuracy and flexibility. So a new IDS is designed which is inspired by Artificial Neural Network, that provides maximum security. It evaluates new IDS against the DOS attack and evaluates the performance of the new IDS and compares the results with traditional IDSs.

In a type of DOS attack, an intruder node injects a large amount of junk packets into the network and causes a denial in the services of the attacked node. ANN modeling and ZSBT method uses a simulated MANET environment for detecting nodes under DOS attack effectively. Artificial Neural Network is a Mathematical Model or Computational Model inspired by human biological neural structures. An artificial neural network is an interconnected group of nodes.

ANN and ZSBT method is used for the detection of DOS attack in the network. A method called “Trace back” is to be implemented here as an IDS. The network parameters have to be investigated to identify the existence of attacks in the network. The attacker spoofs the IP address of the other node and sends the packets with abnormal rate. This is known as IP spoofing [4]. So the IDS have to find the original DOS source node, if the DOS source node spoofs the IP. So the trace back alone is not enough to handle the DOS attack. So, “IDPF” (Inter Domain Packet Filters) is introduced to identify the spoofed nodes. This IDPF helps to find whether the IP is spoofed or not. If it is spoofed, then this method stops receiving the packets from the DOS packet’s path. By this way, the network is protected from such attacks [3].

But in the ZSBT method [5], a node forwards a packet along with the IP address and zone ID. By employing IP spoofing attackers can evade from detection. But with the help of Zone ID, the attacker node can be identified easily and the network is protected from such attacks.

2.RELATED WORK

D. E. Denning (1987) discusses the model of a real-time intrusion-detection expert system capable of detecting break-ins, penetrations, and other forms of computer abuses. The model is based on the hypothesis that security violations can be detected by monitoring a system's audit records for abnormal patterns of system usage. The model includes profiles for representing the behavior of subjects with respect to objects in terms of metrics and statistical models, and rules for acquiring knowledge about this behavior from audit records and for detecting anomalous behavior. The model is independent of any particular system, application environment, system vulnerability, or type of intrusion, thereby providing a framework for a general-purpose intrusion-detection expert system.

Zhenhai Duan and Xin Yuan provide a method called IDPF to control IP spoofing. The Distributed Denial of Services (DDOS) attack is a serious threat to the legitimate use of the Internet. Prevention mechanisms are thwarted by the ability of attackers to forge, or spoof, the source addresses in IP packets. By employing IP spoofing, attackers can evade detection and put a substantial burden on the destination network for policing attack packets. This paper proposes an inter-domain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. A key feature of our scheme is that it does not require global routing information. IDPFs are constructed from the information implicit in BGP route updates and are deployed in network border routers. The conditions under which the IDPF framework works are established correctly in that it does not discard packets with valid source addresses. Based on extensive simulation studies, it is shown that even with partial deployment on the Internet; IDPFs can proactively limit the spoofing capability of attackers. In addition, they can help localize and efficient method to deal with the origin of an attack packet to a small number of candidate networks.

S. Yu, W. Zhou and R. Doss proposes a novel trace back method for DDOS attacks that is based on entropy variations between normal and DDOS attack traffic, which is fundamentally different from commonly used packet marking techniques. In comparison to the existing DDOS trace back methods, the proposed strategy possesses a number of advantages—it is memory non-intensive, efficiently scalable, robust against packet pollution, and independent of attack traffic patterns. The results of extensive experimental and simulation studies are presented to demonstrate the effectiveness and efficiency of the proposed method. Our experiments show that accurate trace back is possible within 20 seconds (approximately) in a large-scale attack network with thousands of zombies [7].

Sunita Sahu & Shishir K. Shandilya has emerged as a new frontier of technology to provide any where, any time communication in MANET. Because of its deployment nature, MANETs are more vulnerable to malicious attack. The absolute security in the mobile ad hoc network is very hard to achieve because of its fundamental characteristics, such as dynamic topology, open medium, limited power and limited bandwidth. The prevention methods like authentication and cryptography techniques alone are not able to provide the security to these types of networks. Therefore, efficient intrusion detection must be deployed to facilitate the identification and isolation of attacks. This paper provides various intrusion detection techniques in MANET and analyzes their fruitfulness.

Center Track is used for finding the source of forged Internet Protocol (IP) datagram's in a large, high-speed network is difficult due to the design of the IP protocol and the lack of sufficient capability in most high-speed, high capacity router implementations by R. Stone. Typically, not enough of the routers in such a network are capable of performing the packet forwarding diagnostics required for this. As a result, tracking-down the source of a flood-type denial-of-service (DOS) attack is usually difficult or impossible in these networks. Center Track is an overlay network, consisting of IP tunnels or other connections that is used to selectively re-route interesting datagram directly from edge routers to special tracking routers. The tracking routers or associated sniffers, can easily determine the ingress edge router by observing from which tunnel the datagram arrive. The datagram can be examined, then dropped or forwarded to the appropriate egress point.

DOS/DDOS attacks constitute one of the major classes of security threats in the Internet today. The attackers usually use IP spoofing to conceal their real location. The current Internet protocols and infrastructure do not provide intrinsic support to trace back the real attack sources. The objective of IP Trace back is to determine the real attack sources, as well as the full path taken by the attack packets. Different trace back methods have been proposed, such as IP logging, IP marking and IETF ICMP Trace back (ITrace). H. C. J. Lee and V. L. L. Thing proposed an enhancement to the ICMP Trace back approach, called ICMP Trace back with Cumulative Path (ITrace-CP). The enhancement consists in encoding the entire attack path information in the ICMP Trace back message. Analytical and simulation studies have been performed to evaluate the performance improvements. The enhanced solution provides faster construction of the attack graph, with only marginal increase in computation, storage and bandwidth.

The future wireless ad-hoc networks transactions are expected to become one of the primary types of flows. Transactions require only a small number of packets to complete. Hence, providing optimal (shortest path) routes to such transactions consumes more energy than the actual data transfer. Conventional shortest path routing protocols are, thus, unsuitable for routing transactions. In this paper, a novel architecture, called TRANSFER is proposed by A. Helmy for transactions routing in large-scale wireless ad hoc networks. In our approach, the aim is to reduce the total energy consumption by transactions as opposed to finding shortest path routes. Our architecture uses a hybrid approach, in which each mobile node obtains information about nodes in its proximity (zone), up to R hops away, using a proactive link-state protocol. Beyond the proximity, the novel notion of contacts is introduced that act as shortcuts to reduce the degrees of separation between the source of the transaction and the destination. An efficient on-demand protocol for contact selection is proposed that does not assume knowledge of location information. Contacts are used during transactions and queries to discover valid routes in an energy-efficient manner. Extensive simulations are used to evaluate the performance of our protocol in terms of energy consumption and success rate. Then the architecture to flooding, dynamic source routing (DSR), zone-routing protocol (ZRP) are compared and two power-aware schemes. Our results show substantial power savings for our contact-based protocol, especially for large ad hoc networks.

3.METHODOLOGY

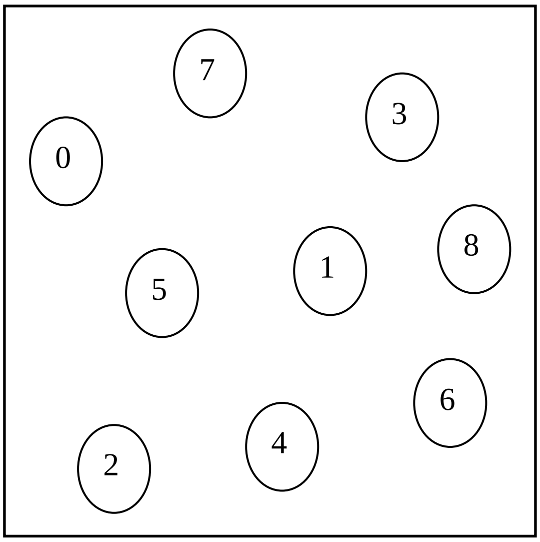
To design the model following steps must be taken:

1. Network creation and routing
2. DOS attack implementation
3. Parameter selection
4. NS2 simulation
5. ANN and ZSBT based IDS implementation

1. Network creation and routing

In this module, the nodes are created in the network. The nodes in the network are configured with type of channel, data structure to be used, size of the data structure, type of routing protocol, and other necessary parameters. GOD- General Operations Director is to be created which gives reference to all the necessary c++ files for all nodes. A network topology is to be created by deploying all nodes in different areas or locations in the simulation area, and ensure that all the nodes are in the coverage area. The nodes should be mobile nodes, since the network is MANET. The nodes are provided with mobility to move randomly across the network.

Figure. 1 A Sample Network Topology (sample network)

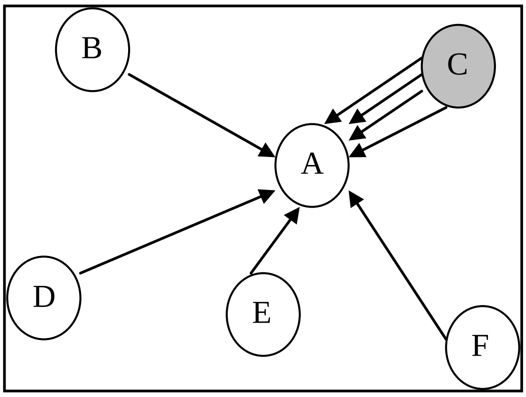


But in the ZSBT method, the network is partitioned into several zones and assigns unique Zone ID for each zone. Thus with the help of Zone ID, the attacker node can be easily identified.

2. DOS attack implementation

In a type of DOS attack, an intruder node injects a large amount of junk packets into the network. This action consumes a significant portion of network resources and causes a denial the services that attacked node could provide for other nodes. A typical DOS attack is shown in Fig. 2, where node A is a host node and host C is the intruder.

Figure. 2 DOS attack, Intruder C bombards the host node A with extra packets (DOS attack)



The intruder sends extra junk packets to the node A. Because of handling huge traffic, the node A exhausts its resources such as bandwidth and energy. This results in inability of node A to serve other nodes such as B, D, E and F fairly and degrades the network performance.

In this module, DOS is to be implemented across the network. All the nodes are configured with some threshold packet flow rate (example: packet flow rate = 5).

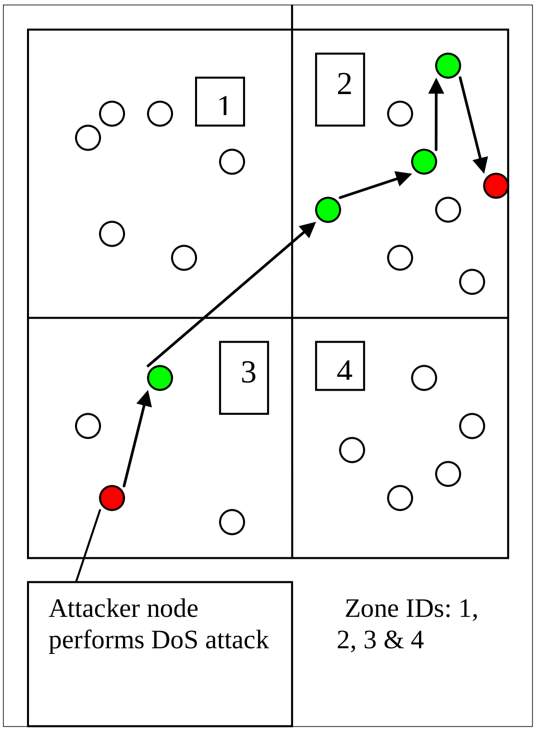


Figure. 3 DOS attack is implemented in the network with Zone ID

If a node sends packets to another node, the receiver node checks the packet flow rate of the sender that is the number of packets, packet sending frequency and intention of the sender.

If the rate is below the threshold value (example: if the rate below 5), then the receiver simply continues the communication; If it exceeds, then the receiver node fails responding to other nodes. So here, a node is to be created with abnormal rate. That is this node contacts the destination node with abnormal rate (greater than 5) and denies the services of the destination node.

And the DOS source node may spoof the IP address of the other node in the network in order to make difficult to find the source node. But with the help of Zone ID, the source of the attacker node can be easily identified. When compared with ANN, ZSBT method works well for detecting DOS attacks in the network.

3. Parameter selection

In a network, the DOS attack can be detected with the help of following parameters:

Packet loss (PL): It calculates the average number of packets dropped in every time frame on the links from destination to host node.

Packet Sending (PS): It calculates the average number of packets that are sent between two nodes and shows the traffic load of host nodes.

Packet Receiving (PR): It calculates the average number of packets received in every time frame.

Energy Consumption (EC): DOS attack may exhaust the battery power of destination node. It measures the amount of energy every node consumes in every time frame.

These parameters have to be analyzed. Therefore, a sample communication is to be performed between two nodes. The sender node is configured as DOS source node, and the sender node sends the packet with abnormal rate to the receiver. And one more communication between two nodes is to be made. These two nodes are normal nodes.

Then, the number of packets sent between two nodes (PS), number of packets dropped (PL), number of packets received (PR), and the total energy consumption (EC) are to be evaluated between two normal nodes and between the DOS source and receiver node.

The analysis results are to be plotted as X-Graphs and the results are to be compared. Based on the comparison, the communication between DOS source and destination consumes more resources than the normal one.

4. NS2 Simulation

Here the simulation was carried out using NS-2. The network is constructed with several nodes and ensures that every node is connected at-least to one node via mobile agents.

The mobile agents serve as a communication agent between nodes. The configuration of MANET in NS-2 is shown in Table I.

Table I. MANET configuration in NS-2

Parameter	Definition
Protocol	Ad hoc on Demand Distance Vector(AODV)
Mac layer	IEEE 802.11
Transmission range	250 m
Node placement	Random
Simulation area	500*500
Minimal speed	1 m/s
Maximal speed	10 m/s
Size of data packets	512 bytes
Simulation time	400 s
Number of node	25
Parameter	PL, PS, PR and EC
Version NS-2	NS-2.34(under Red hat Linux)

5. ANN and ZSBT based IDS implementation

An ANN and ZSBT based IDS are to be implemented to act against DOS attack. A method called **"Trace back"** is implemented here as an IDS. The attacker spoofs the IP address of the other node and sends packets with abnormal rate. So the IDS have to find the original DOS source node, if the DOS source node spoofs the IP. So the trace back alone is not enough to handle the DOS attack. So **"IDPF" (Inter Domain Packet Filters)** is used to identify the spoofed nodes.

The trace back method monitors the packet flow from the node. If the rate is abnormal, then it avoids to receiving the packets from the node (the receiver node identifies the node by seeing the IP address of the sender node in packet's header information. Packet's header information contains all info about the sender including IP) and denies the services to the particular node. But in case of ZSBT method sender node forwards packet along with the IP address and Zone ID.

At the same time, the IDPF starts to find the source node of the attacker. IDPF sends the inquiry packet (normally a request packet), to ask about the node's abnormal flow. If the node is not a source node, then it simply gives the NO answer. So the IDPF knows that the IP is spoofed. So the IDPF stops receiving the packets from the DOS packet's path. Both the method stops further receiving of DOS packets from that path. The source of the attacker can be easily identified with the help of Zone ID.

Thus the ZSBT method works well when compared with ANN. Because in ANN method, all nodes have to be searched in order to find the source node of the attacker. Thus the network is protected from DOS attacks.

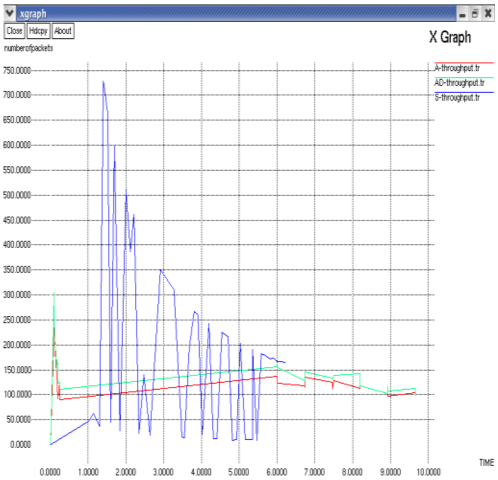
4.RESULT ANALYSIS

The analysis results are to be plotted as X-Graphs and the results are to be compared. Based on the comparison, the communication between DOS source and destination consumes more resources than the normal one.

Fig. 4 provides the performance of throughput using ANN and ZSBT method. Throughput indicates rate of communication per unit time. Throughput in these experiments is evaluated for all these routing protocols for varying node mobility and nodes. So for a network if a throughput is high then rate of communication is also high.

Throughput indicates rate of communication per unit time. Throughput in these experiments is evaluated for all these routing protocols for varying node mobility and nodes. So for a network if a throughput is high then rate of communication is also high.

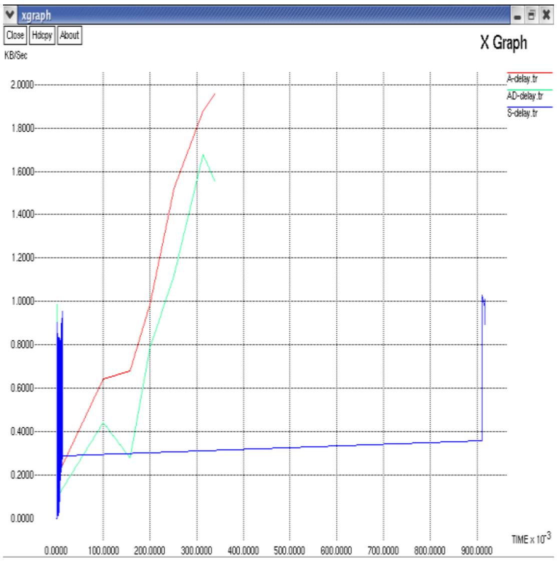
Figure. 4 Comparison of throughput using ANN and ZSBT method



Generally for a network, throughput must be high then only it is said to be an optimized network. Before attack detection the throughput is low whereas after attack detection the throughput is high while comparing with ANN method.

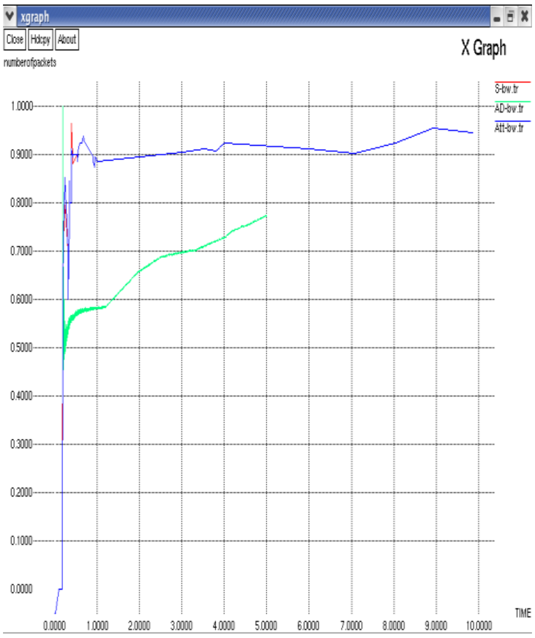
But when compared with Artificial Neural Network, ZSBT (Zone Sampling Based Method) method works well for detecting attacks in the network.

Figure. 5 Comparison of delay using ANN and ZSBT method



It shows the performance of delay before and after the attack. Before attack detection delay is high and after detection delay is low. So, this graph provides better performance.

Figure. 6 Comparison of bandwidth using ANN and ZSBT method



It provides the performance of bandwidth before and after attack. Generally, for a network during transmission of packets the bandwidth consumption will be high. After attack detection, dropping of unwanted and unauthorized packets will take place. So, bandwidth consumption will be low. Thus, for a better network bandwidth consumption must be low.

5.CONCLUSION

Thus the Artificial neural network and ZSBT method based IDS are used for the detection of DOS attacks in MANET environment. The MANETs are mainly applied in personal area networking, military environments, civilian environments and emergency operations. Using a simulation, it is shown that the model can be utilized for the detection of DOS attacks. Because of the dynamic nature of the network, it can be easily vulnerable to attacks such as DOS. Analyze these parameters for each node in the network to detect attacks and its impacts. This method is known as trace back. Trace back alone is not enough to identify the spoofed nodes. So, IDPF is introduced to identify spoofed nodes and prevent network from further attacks. Thus, the ZSBT method produces better results with the help of Zone ID rather than ANN method.

REFERENCES

[1] S.Yu, W.Zhou and R.Doss, Weijia Jia, “Traceback of DDoS Attacks Using Entropy Variations” IEEE transactions on parallel and distributed systems, March 2011.

[2] Sunita Sahu & Shishir K. Shandilya, “A Comprehensive Survey on Intrusion Detection in MANET” International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 305-310, December 2010.

[3] Mofreh Salem, Amany Sarhan, Mostafa Abu-Bakr, “A DoS Attack Intrusion Detection and Inhibition Technique

for Wireless Computer Networks", ICGST- CNIR, Volume (7), Issue (I), July 2007.

[4] Zhenhai Duan, Xin Yuan and Jaideep Chandrashekar, "Controlling IP Spoofing Through Inter Domain Packet Filtering" In proc. IEEE INFOCOM 2006.

[5] Xin Jin, Yaoxue Zhang, Yi Pan and Yuezhi Zhou, "ZSBT: A Novel Algorithm for Tracing DoS Attackers in MANETs", EURASIP Journal onWireless Communications and Networking Volume 2006.

[6] A.Helmy, "Contact-extended zone-based transactions routing for energy-constrained wireless ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 54, no. 1, pp. 307–319, 2005.

[7] Y. Kim and A. Helmy, "SWAT: small world-based attacker traceback in Ad-hoc networks," in Proceedings of IEEE Infocom Poster/Demo Session (INFOCOM '05), Miami, Fla, USA, March 2005.

[8] H. C. J. Lee, V. L. L. Thing, Y. Xu, and M.Ma, "ICMP traceback with cumulative path, an efficient solution for IP traceback," in Proceedings of 5th International Conference on Information and Communications Security (ICICS '03), pp. 124–135,Huhehaote, China, October 2003.

[9] Y.Zhang, W.Lee and Y.Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", Wireless Networks, vol 9 no.5,pp. 545-556,2003.

[10] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP Traceback," in Proceedings of the ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM '00), pp. 295–306, Stockholm, Sweden, September 2000.

[11] R. Stone, "CenterTrack: an IP overlay network for tracking DoS floods," in Proceedings of 9th USENIX Security Symposium, pp. 199–212, Denver, Colo, USA, August 2000.

[12] D.E.Denning, "An intrusion-detection model," IEEE Transactions on Software Engineering, vol. SE-13, no.2, pp. 222-232, February 1987.