Interference Detection and Prevention of Black Hole (Dos) Attack Using Honeypots

Rahul Diwate
B.E (Computer Engg.)
4thYear
B.D.C.O.E.

Surabhi Deshpande
B.E (Computer Engg.)
4thYear
B.D.C.O.E.

Shaktikala
B.E (Computer Engg.)
4thYear
B.D.C.O.E.

ABSTRACT
Due to rapid increase in networking throughput and security threat, much research is been done in the field of computer science. But security susceptibility grows every day. DoS attacks are the most prominent threat to the networks around the world. This paper gives an introduction to various DoS attacks present in today's Ad Hoc networks and proposes a method to prevent or counter these attacks against the networks by using honeypots that are deployed into the network to mislead and trap the attacker and thus providing a two layer security to the Ad Hoc networks. Computer networks and information technology on in the wake of intensive growth of use of the whole, we now rely deeply on our network for even the most basic functions. Even a small hindrance to the network just about paralyses us. But there are severe threats looming around, like Blackhole attack Rushing attack Wormhole attack and many more known and unknown attacks. These attack affect the network unfavorably thus creating a chaos all around. Thus NETWORK SECUTIRY has become the priority of all organizations. Many security measures have been taken to counter the security attacks. But these measures are not up to the mark. In this paper we are going to give a detail review about Networks and all the types of know DoS (Denial of service) present in the system. We also propose how a new methodology to counter these attack by providing a two layer security to the network by the use of HONEYPOTS. These honeypots help them to mislead the attacker to itself, exposes itself to the attack and gathers the information about the attacker, the type of attack and the purpose of the attack. Thus the gathered information helps us to counter the given type of attack.

Keywords
AdHoc, wireless network, DoS, honeypot, jamming. 802.11, network security.

1. INTRODUCTION
Denial of Service (DoS) attacks have become a major threat to current computer networks. These attacks were supposed to be some kind of games among the attackers. The attackers would launch DoS attacks against large organizations whose policies they disagreed. DoS attacks are illegal by law. Some companies would use this attack to slow down or knock out their competitors in the market. Known DoS can be anything related to network computing and service performance, such as link bandwidth, TCP connection buffers, application/service buffer, CPU cycles, etc. Ad hoc networks are envisioned as playing a significant role in mission critical communication for the military, utilities, and industry. An adversary may attempt to attack a victim ad hoc network to prevent some or all victim communication. Such denial-of-service (DoS) attacks have been considered in ad hoc wireless networks at several levels. A number of researchers have considered DoS where the attackers are internal members in the victim ad hoc network [1].

Ad hoc networks require the cooperation of peer nodes for their operation and are especially susceptible to such peer-based attacks. In this paper we consider encrypted victim networks in which the entire packet including headers and payload are encrypted and thus the attacker cannot directly manipulate any of the victim communication. In this case, the attacker must resort to external physical-layer-based DoS, also known as jamming. There are many known DoS attacks. We now focus on attacks against the routing protocol in ad hoc networks. These attacks may have the aim of modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. An attack may also aim at impeding the formation of the network, making legitimate nodes store incorrect routes, and more generally at perturbing the network topology. Attacks at the routing level can be classified into two main categories: incorrect traffic generation and incorrect traffic relaying. Sometimes these coincide with node misbehaviors that are not due to malice, e.g. node malfunction, battery exhaustion, or radio interference.

1.1 Incorrect Traffic Generation
This category includes attacks which consist in sending false control messages: i.e. control messages sent on behalf of another node (identity spoofing), or control messages which contain incorrect or outdated routing information. The network may exhibit Byzantine [2] behavior, i.e. conflicting information in different parts of the network. The consequences of this attack are degradation in network communications, inaccessible nodes, and possible routing loops.

1.1.1 Cache poisoning
As an instance of incorrect traffic generation in a distance vector routing protocol, an attacker node can advertise a zero metric for all destinations, which will cause all the nodes around it to route packets toward the attacker node. Then, by dropping these, the attacker causes a large part of the communications exchanged in the network to be lost. In a link state protocol, the attacker can falsely declare that it has links with distant nodes. This causes incorrect routes to be stored in the routing table of genuine nodes, also known as cache poisoning.

1.1.2 Message Bombing and other DoS Attacks
The attacker can also try to perform Denial of Service on the network layer by saturating the medium with a storm of broadcast messages (message bombing), reducing nodes good put and possibly impeding nodes from communicating. (This is not possible under hybrid routing protocols, where nodes cannot issue broadcast communications [3]. The attacker can even send invalid messages just to keep nodes busy, wasting their CPU cycles and draining their battery power. In this case the attack is not aimed at modifying the network topology in a

certain fashion, but rather at generally perturbing the network functions and communications.

1.2 Incorrect Traffic Relaying

Network communications coming from legitimate, protocol-compliant nodes may be polluted by misbehaving nodes.

1.2.1 Blackhole Attack

An attacker can drop received routing messages, instead of relaying them as the protocol requires, in order to reduce the quantity of routing information available to the other nodes. This is called blackhole attack by Hu et al. [4], and is a "passive" and a simple way to perform a Denial of Service. The attack can be done selectively (drop routing packets for a specified destination, a packet every n packets, a packet every t seconds, or a randomly selected portion of the packets) or in bulk (drop all packets), and may have the effect of making the destination node unreachable or downgrade communications in the network.

1.2.2 Wormhole Attack

The wormhole attack [5] is quite severe, and consists in recording traffic from one region of the network and replaying it in a different region. It is carried out by an intruder node X located within broadcast range of legitimate nodes A and B, where A and B are not themselves within broadcast range of each other. Intruder node X merely tunnels control traffic between A and B (and vice versa), without the alteration presumed by the routing protocol – e.g. without stating its address as the source in the packets header – so that X is virtually invisible. This results in an extraneous inexistent A - B link which in fact is controlled by X. Node X can afterwards drop tunneled packets or break this link at will. Two intruder nodes X and X′, connected by a wireless or wired private medium, can also collude to create a longer (and more harmful) wormhole.

The IEEE 802.11b standard includes a scheme called WEP (Wired Equivalent Privacy) to secure communications. It uses the RC4 stream cipher coupled to an Initialization Vector for encryption, and the CRC-32 checksum for integrity check. WEP employs a 40-bit or 64-bit secret shared key, providing no infrastructure for key management. As its name implies, WEP offers a protection similar to that of an unsecured wired network, and therefore a quite low level of security (the Air Snort program can easily crack WEP keys). Despite its weakness, WEP may be considered useful as a deterrent against casual snoopers. The vulnerabilities of WEP have been fixed in WPA (Wi-Fi Protected Access). WPA uses IEEE 802.1X authentication, providing port-based network access control capability, with a standard EAP (Extensible Authentication Protocol).

Following table will give you the transitory information regarding various types of attacks that effect the network.

Table.1: DoS attacks and their effects on the network

Types of DoS attacks			**Conflicting routes**	**Connectivity loss**	**Message loss**
Incorrect Traffic Generation	Incorrect HELLO generation	ID spoofing	X	X	X
		Link spoofing	X	X	
	Incorrect TC generation	ID spoofing	X	X	X
		Link spoofing	X	X	
	Incorrect MID/HNA generation		X	X	X
	ANSN attack			X	X
Incorrect Traffic Relaying	Message tampering		X	X	
	Blackhole attack			X	X
	Replay attack		X	X	X
	Wormhole attack			X	
	MPR attack			X	X
Message bombing and other DoS attacks				X	X

2. LITRATURE REVIEWED

In the year 2011 G. Thamilarasu, S. Mishra and R. Sridhar Institute of Technology has published a paper named "Improving Reliability of Jamming Attack Detection in Ad hoc Networks" they focus on jamming type DoS attacks at the physical and MAC layers in 802.11 based ad hoc networks. Collisions in wireless networks occur due to varying factors such as jamming attacks, hidden terminal interferences and network congestion. They first investigate the problem of diagnosing the presence of jamming, then evaluate the detection mechanism using cross-layer information obtained from physical and link layers to differentiate between jamming and congested network scenarios. By correlating the cross-layer data with collision detection metrics, they can distinguish attack scenarios from the impact of traffic load on network behavior. Through simulation results we demonstrate the effectiveness of our scheme in detecting jamming with improved precision.in ad hoc networks.

In the year 2012 Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, Kuang-Yuan Tung, Department of Computer Science and Engineering they proposed a work on "Intrusion detection system" with the increasing amount of network throughput and security threat, the study of intrusion detection systems (IDSs) has received a lot of attention throughout the computer science field. Current IDSs pose challenges on not only capricious intrusion categories, but also huge computational power. Though there is a number of existing literatures to IDS issues, they attempt to give a more elaborate image for a comprehensive review. Through the extensive survey and sophisticated organization, they propose the taxonomy to outline modern IDSs. In addition, tables and figures we summarized in the content contribute to easily grasp the overall picture of IDSs.

In the year 2013 Michael Beham, Marius Vlad, Hans P. Reiser(Institute of IT-Security and Security Law University of Passau, Germany) compared the performance of existing nested-virtualization solutions and analyze the impact of the

performance overhead on VMI-based intrusion detection and honeypot systems.In earlier studies we saw the intrusion detection systems and honeypot architectures based on virtual machine introspection (VMI). These systems directly benefit from the use of virtualization technology.

In the year 2013 Luís M. L. Oliveira, Joel J. P. C. Rodrigues, Amaro F. de Sousa published a paper named "Denial of service mitigation approach for IPv6-enabled smart object networks". Denial of service (DoS) attacks can be defined as any third-party action aiming to reduce or eliminate a network's capability to perform its expected functions DoS attacks are even more troublesome in smart object networks because of two main reasons. First, these devices cannot support the computational overhead required to implement many of the typical counterattack strategies. Second, low traffic rates are enough to drain sensors' battery energy making the network inoperable in short times.

In the year 2013 Constantin Musca, Emma Mirica, Razvan Deaconescu of Department of Computer Science and Engineering University "Politehnica" of Bucharest have discussed about the most delicate problem in the information security domain, which is detecting unknown attacks which are known as zero-day attacks In this paper they have presented methods for isolating the malicious traffic by using a honeypot system and analyzing it in order to automatically generate attack signatures for the Snort intrusion detection/prevention system.

In the year 2013 Sounak Paul, Bimal Kumar Mishra department of Computer Science and Engineering has proposed solutions for the following problems: 1. It should be capable of understanding definition of malicious and legitimate traffic. 2. Signature must be flexible enough to defend against the worms that change their appearance in every infection. 3. It should take care of system resource such as CPU time of generating signature and comparing them with network traffic. 4. Signature must be wide enough to detect zero day attacks.

3. CURRENT SYSTEM

To prevent DoS attacks there are many prevailing methods which are used. Intrusion detection methods are basically classified into three categories: Signature-based Detection, Anomaly-based Detection and Stateful Protocol Analysis. There methods are widely used and are known to majority of population. But these detection methods lack few in some or the other way. Signature-based is ineffective to detect unknown attacks, has little understanding to states and protocols and is time consuming to maintain knowledge. The Anomaly-based detection has weak profiles accuracy due to observed events being constantly changed, unavailable during rebuilding of behavior profiles and difficult to trigger alerts in right time. Stateful Protocol Analysis is unable to inspect attacks looking like benign protocol behaviors and might incompatible to dedicated OSs or APs.

4. SUGGESTED SYSTEM

In this paper we propose use of honeypots in the Ad Hoc network to provide a double layer security to the network and reduce the effect of DoS attacks on a network. The honeypots acts as the first layer of security and the base nodes are the second layer of security. The honeypots acts like trap for the attackers and help to gather all the information about the attacker, type of attack and the methods used. The attacker get trapped in the honeypot or the honeynodes assuming that the nod is the important part of the network. And thus giving the network time to detect and counter the DoS attack.

The first step to understanding honeypots is defining what a honeypot is. This can be harder than it sounds. Unlike firewalls or Intrusion Detection Systems, honeypots do not solve a specific problem. Instead, they are a highly flexible tool that comes in many shapes and sizes. They can do everything from detecting encrypted attacks in IPv6 networks to capturing the latest in on-line credit card fraud. It is this flexibility that gives honeypots their true power. It is also this flexibility that can make them challenging to define and understand. As such, I use the following definition to define what a honeypot is [6].

"A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource."

This is a general definition covering all the different manifestations of honeypots. We will be discussing in this paper different examples of honeypots and their value to security. All will fall under the definition we use above, their value lies in the bad guys interacting with them. Conceptually almost all honeypots work the same. They are a resource that has no authorized activity, they do not have any production value. Theoretically, a honeypot should see no traffic because it has no legitimate activity. This means any interaction with a honeypot is most likely unauthorized or malicious activity. Any connection attempts to a honeypot are most likely a probe, attack, or compromise. While this concept sounds very simple (and it is), it is this very simplicity that give honeypots their tremendous advantages

5. SYSTEM ARCHITECTURE AND ALGORITHM

A honeypot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers. These honeypots or honeynodes are placed into the network such a way that they seem to be the authentic node or the most valuable node of the network thus attracting the attacker to attack on these honeynodes. The trapped attacker is unaware that he is attacking the honeynodes. These nodes detect the type of attack, the purpose of the attack and helps to locate the attacker without compromising the authentic node. If the honeynodes gets compromised still it gives the authentic nodes in the network to prevent attack by changing the protocols and frequency of the network.

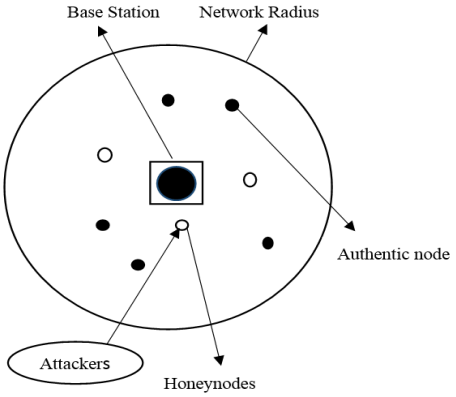

Fig. 3 System Architecture

Algorithm

1. If (Attack detected= true) then
2. If (Node is a honeynode) then
3. Inform base station of attack
4. Continue communications to deceive attacker
5. End.
6. Change frequency of operation
7. Else
8. If (node is a base station) then
9. If (honeynode has informed of attack) then
10. Select frequency to jump using dynamic selection
11. Inform nodes to switch to this frequency
12. Change frequency of operation
13. Else
14. Find the node that did not respond
15. If (any node did not respond) then
16. Broadcast frequency change command
17. Change frequency of operation
18. End

6. CONCLUSION

By this paper we have studied different types of Denial of Service (DoS) attacks that are present today, which effect the Ad Hoc Networks adversely. Also we found that with the help of this methodology honeypots can help to deceive the attacker and help us to reduce the hostile effect of DoS attacks on the Ad Hoc network. It gives the main network time to get knowledge about the type of attack, purpose of the attack and to change the protocols and frequencies at which it is working by using various intrusion detection methods. Thus creating a dual layer protection in the Ad Hoc network.

7. REFERANCE

[1] Hu, Y.-C., Perrig, A. A survey of secure wireless ad hoc routing. IEEE Security & Privacy Magazine. v. 02, n. 3, (May–Jun. 2004), pp. 28–39

[2] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine general's problem. ACM Transactions on Programming Languages and Systems, 4(3):382–401, 1982.

[3] Srđan Čapkun, Jean-Pierre Hubaux, and Markus Jacobsson. Secure and privacy-preserving communication in hybrid ad hoc networks. Technical Report IC/2004/10, Swiss Federal Institute of Technology Lausanne (EPFL), Lausanne, Switzerland and RSA Laboratories, Bedford, MA, USA, 2004.

[4] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In Proceedings of the 8th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '02), September 2002.

[5] Security in ad hoc networks: basic mechanismshttp://perso.crans.org/raffo/papers/phdthesis/thesisch4.html

[6] Honeypot (computing)http://en.wikipedia.org/wiki/Honeypot_(computing)