American Journal of Scientific Research
ISSN 2301-2005 Issue 80 November, 2012, pp.155-163

http://www.eurojournals.com/ajsr.htm

Use of Honeypots along with IDS in Cluster-Based MANETs

Ali Mirzaei
MSc, Information Technology, E- Commerce
IT Department, Khajeh Nasir Toosi University of Technology, Tehran, Iran
E-mail: mirzaei@kntu.ac.ir
Tel: +98-912-6030115

Shahriar Mohammadi
PhD, Assistant Professor, Information Technology Department
Khajeh Nasir Toosi University of Technology, Tehran, Iran
E-mail: mohammadi@kntu.ac.ir
Tel: +98-912-2978284

Abstract

In comparison to traditional networks, MANETs are less secure and more vulnerable to threats, because of their natural characteristics. In this paper after an overview of security problems and vulnerabilities of MANETs, we will discuss about IDS and its necessity and applications in MANETs. Then we propose using a honeypot system along with IDS. And also we will propose architecture of a honeypot node to be used in MANET networks, based on honeypots in traditional wired networks.

Keywords: Network, MANET, security, network security, IDS, Honeypot

1. Introduction

Since 1970 that networks similar to MANETs created by DARPA (Defense Advanced Research Projects Agency) – named Mobile Packet Radio Networking or Mobile Mesh Networking for future military networks – it has been under development. And even today with all the technology advances and developments, there are still many problems to be solved in MANET networks. It needs more efficient routing protocols with better security handle, more energy efficient solutions, standardization and so on. MANETs are still facing many challenges. Both software and hardware parts need to be upgraded to a better level of functionality and reliability. In the security part, in addition to the old problems like a secure routing protocol, we should work on new technologies in parallel to achieve a better security performance. The idea of using an IDS system in networks is not a new paradigm. But using honeypots are relatively new rather than traditional IDSs. In this paper we will discuss about using a honeypot system along with the IDSs in a MANET network.

2. An Overview on MANETs

MANET (Mobile Ad hoc Network) is a wireless ad hoc network. Each node in a MANET is free to move independently in any direction, leaving the network and joining whenever it wants. Ad hoc in Latin means “for this purpose only”, and here it means no infrastructure. In MANETs we have no

infrastructure. So each node of the network must act like a router or switch to maintain the network functionality.

2.1. Main Characteristics

List of the main MANET characteristics:

- Wireless communication
- Self-configuration
- No infrastructure
- Each wireless terminal also acts as a router
- Multi hop dynamic routing is used to autonomously create communication routes between terminals witch cannot communicate directly. This happens when two nodes are not in the radio range of each other.

2.2. MANET Applications

MANET has developed by DARPA for military purposes in the first place. But today it has many applications beside military. For example it's the best choice for fire/safety and rescue operations, where probably there is no functional infrastructure available. In addition to military and safety operations, it has also applications in: (Kuldeep Sharma, Neha Khandelwal and Prabhakar.M, 2010)

- Transportations (VANET, Vehicular Ad hoc Network)
- Intelligent Transport Systems (ITS)
- Mobile commerce
- Sensor networks
- Medical service
- Personal Area Networks
- Robotics
- Surveillance systems and delivery systems for local information
- And so on

2.3. Vulnerability and Security Issues of MANETs

MANET networks have more vulnerabilities rather than wired networks or even other types of wireless networks with infrastructure. Here is a list of them:

(Goyal, Parmal and Rishi, 2011) (Zhang and Lee, 2004) (Rai, Tewari and Upadhyay, 2010)

- **Lack of pre-defined boundaries**

This vulnerability is originated from the nature of MANETs. In comparison to traditional wired networks, there is no clear line of secure boundary. In wired networks adversaries must get physical access to the network medium, or even pass through several lines of defense such as firewall and gateway before they can perform malicious behavior to the targets [3] but in MANETs there is no need to do anything to get access to the network medium, once the adversary positioned in radio range of any other node from the network, it automatically will be joined to the network and soon can communicate with other nodes.

- **Threats from Compromised nodes Inside the Network**

In wired networks one of the most dangerous attacks is the attacks performed by insiders. This kind of attack is harder to detect and prevent. Because of the lack of secure boundaries in MANETs, like we said before it's very easy for adversaries to get into the network, so after that they can act as insiders. Or they can use other nodes to perform an attack. The compromised nodes that used to be trusted can be more dangerous rather than newbies. Furthermore, because of the mobility of the ad hoc network, a compromised node can frequently change its attack target and perform malicious behavior to different node in the network, thus it is very difficult to track the malicious behavior performed by a

compromised node especially in a large scale ad hoc network. Byzantine failures are one good example of this kind of attacks. In a Byzantine failure a group of compromised nodes cooperate with each other so their malicious behavior cannot be detected. In a Byzantine attack may everything be seemed normal from node's viewpoint but it may actually be a byzantine behavior. [4]

- **Lack of Centralized Management**

This means we have no centralized management and monitoring facilities. This makes it very hard to address security problems in MANETs. Obviously it's very hard to monitor the traffic without centralized management and facilities, especially in large scale ad hoc networks with high density of nodes and highly dynamic topology. In addition to this, in MANET networks some decision making is cooperative and decentralized due to the lack of centralized management and authority. Also that's a good opportunity for adversaries to participate in decision makings or to manipulate or disorder group tasks.

- **The nature of cooperation in MANETs**

Most of operations like routing protocols and many other tasks in MANETs are based on cooperation between nodes and that's the nature of MANETs. That is because of the lack of centralized management and also the lack of infrastructure like switches or routers or DNS servers and so on like traditional networks. This is where the adversaries can abuse it. They can abuse of pre-assumed other nodes' trust in them and forward the modified packets with wrong data or just eavesdropping transmittal information.

- **Resource availability**

Providing secure communication in such a dynamic topology and changing environment to make the services available to all nodes in a reliable and secure manner is a major challenge. Developers created various security schemes and architectures.

- **Scalability**

Based on MANET characteristics the scale of the network is variable and non-predictable. Security mechanism should be capable of handling a large network as well as small ones.

- **Dynamic topology**

In MANETs each node can freely move in any direction and nodes are dynamically changing their positions and leaving the network or joining in any time. So in this situation, keeping the track of trust relationship and node membership poses a challenge in security of MANETs.

- **Limited power supply**

Since the nodes are mobile, they should use a power source like battery. So energy source of the nodes are provided by limited resources. This limitation may pose some security threats like selfness behavior from nodes. Like nodes restraining to forward packets when the power source is low.

- **Bandwidth constraints**

Bandwidth capabilities are variable in MANETs due to density of nodes and environmental characteristics like interference, signal attenuation effects or external noise and so on.

The nature of MANETs is based on cooperation of nodes together. So nodes should act like they fully trust each other. This makes it harder to establish a level of security.

2.4. Types of attacks in MANETs

There are many kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following two types: (Zhang and Lee, 2004)

- External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.
- Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

3. What is an IDS System?

Today IDS or IDPS (Intrusion Detection and Prevention System) seems to be almost necessary for every organization to monitor and improve their network security.

3.1. IDS Definition

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. (Scarfone and Mell, 2007)

4. Honeypots and Honeytokens

Beside of IDPS technologies and methods, we are observing emerge of honeypots and honeytokens as new security approach that take different path to identify and learn malicious behavior without taking any real damage.

4.1. Definitions

Honeypot concept is defined by Lance Spitzner : "A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource." [6] According to this definition and his paper, a honeypot or a honeytoken is a resource that we want the bad guys to interact with. It may be a computer or a digital entity like a credit card number, excel spreadsheet, PowerPoint presentation, or even a bogus login. So honeytokens are everything a honeypot is, except they are not a computer. No one should be interacting with them. Any interaction with a honeytoken implies unauthorized or malicious activity. (Spitzner, 2003)

The term honeytoken was first coined by Augusto Paes de Barros in 2003 on the honeypots mailing list. This term aptly described the concept, and as is often true when dealing with technologies, having a commonly accepted term makes the concept easier for others to understand and discuss. (Spitzner, Jully 2003)

4.2. Honeypot Advantages

Honeypots or honeytokens have advantages over traditional security mechanisms that includes: (Spitzner, 2003)

- **Small Data Sets**
  In comparison to organizations logging a large volume of events and activities, Honeypots just record something that is certainly suspicious activities.
- **Reduced False Positive**
  Any activity with honeypots is by definition unauthorized, making it extremely efficient at detecting attacks.
- **Catching False Negatives**
- **Encryption**
  No matter if the attacker is using some kind of encryption, because we just observe and capture the events and activities
- **Working in any IP environment**
  Compatible with any IP environment like new IPv6
- **Highly Flexible**
  Honeypots can be used in a vast variety of environments
- **Minimal Resources**
  Even in the large networks, we can use an old pc to do the job.

Like any other technologies, Honeypots also have disadvantages: (Spitzner, 2003)

- **Risk**

  Since we want our honeypot system to be almost openly accessible to attackers, there is a risk that attacker could use a honeypot system to attack other systems in our network.

- **Limited Field of View**

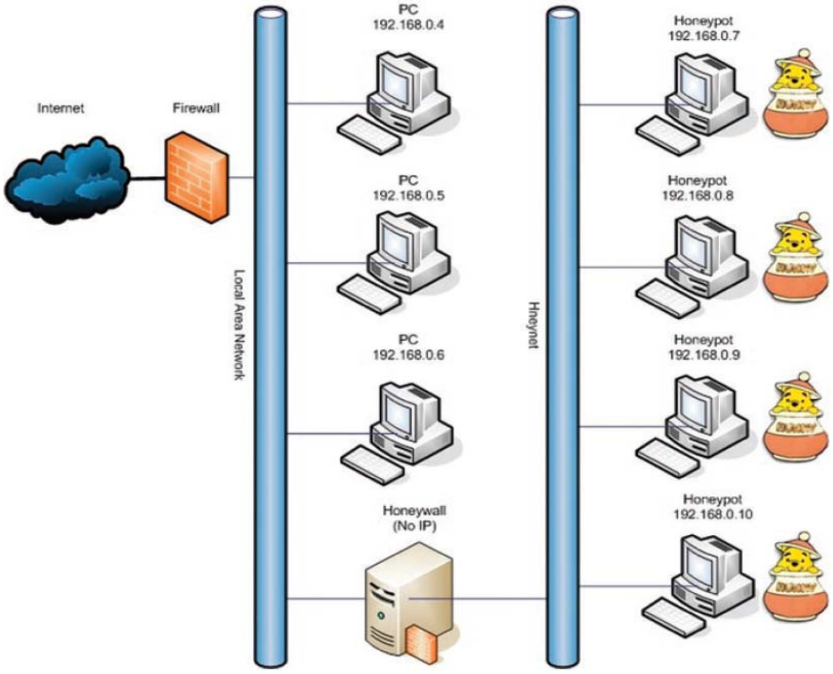
  Honeypots only can see and capture activities that target the honeypot systems. They can't monitor other parts of the networks.

4.3. Honeypots in a Traditional Network

Figure 1 is demonstrating the general scheme of a honeypot in a honeynet using a honeywall and a firewall for the network. This is a classical honeypot deployment.

Each of honeypot systems are an independent solution grouped together in a honeynet and separated from other parts of the network via a honeywall. Honeywall acts like a firewall for our network. Since honeypot systems are intended to be accessible by attackers, black hats may fully access them and use them to launch attacks like DoS or what else against the other non-honeypot systems of our network or even other systems on the Internet. So it's very important to protect other parts of the network from Honeynet by putting it behind a honeywall.

Figure 1: A Honeynet (Barfar and Mohammadi, 2007)



Honeywalls would do two major tasks:

- **Data Control**

Honeywall is used to limit the amount of malicious traffic passing through honeywall by limiting the number of connections in a period of time, limiting the volume of traffic or either limiting the bandwidth. It will reduce the risk of using our honeypot systems to attack other systems on the Internet or our non-honeypot systems.

- **Data Capture**

In addition to data control, honeywalls would do another job and that's monitoring and capturing almost all traffic entering or leaving the honeywall to analysis the attacker's behavior and gather information about attacker's tactics.

Honeywall used in figure 1 is a layer two device, acting like a switch, letting it to connect the honeynet to the production network logically, and having the same range of IP addresses. Since the honeywall is a layer two bridging device, it has no MAC address, no routing of packets, nor any TTL decrement, making it nearly impossible for an attacker to detect it. (Spitzner, 2003), (Barfar and Mohammadi, 2007)

4.4. Honeypots/Honeytokens in MANETs

There are many proposed architecture for IDS/IPS systems in MANETs. But what we discuss here is to use Honeypots along with IDS systems in MANET networks to improve security against the insider attacks.

4.5. The Main Advantage of Honeypots in MANETs

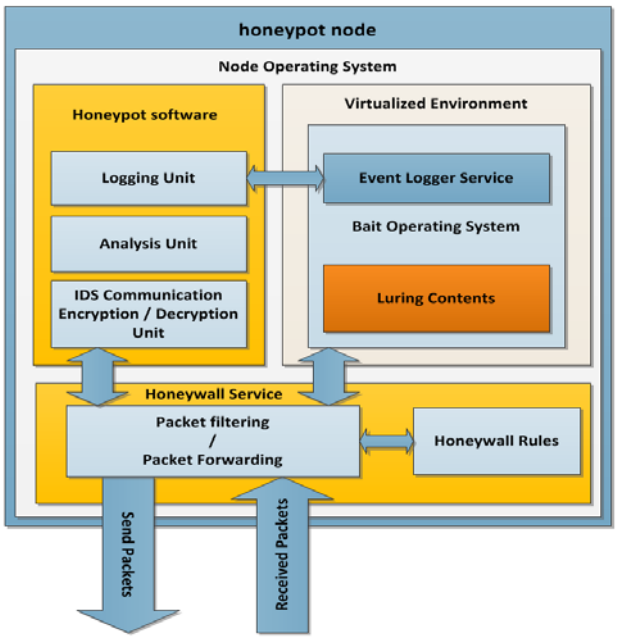
As we discussed before MANETs are cooperative networks by their own nature. It means that nodes in a MANET fully trust each other. Based on this, MANETs are so vulnerable from this point (Threats from Compromised nodes Inside the Network). So who should do the trust management and detect and identify the malicious behavior and bad nodes?

Basically IDS systems are designed for MANETs to do the job. They don't fully trust all nodes and they monitor and analysis the network activities or host activities to detect intrusion and generate alarm messages. But like enterprise networks, by using honeypots along with IDS, we go further to detect and also to understand the attacker's goal and to learn new malicious activity methods and even more. It seems like a lost chain for MANET networks.

5. Proposed Model for Honeypot Node in MANETS

And here is our model, shown in figure 2. A honeypot node is a node acting as a honeypot system in a MANET network. We have all the elements appeared in a classic deployment here with little differences.

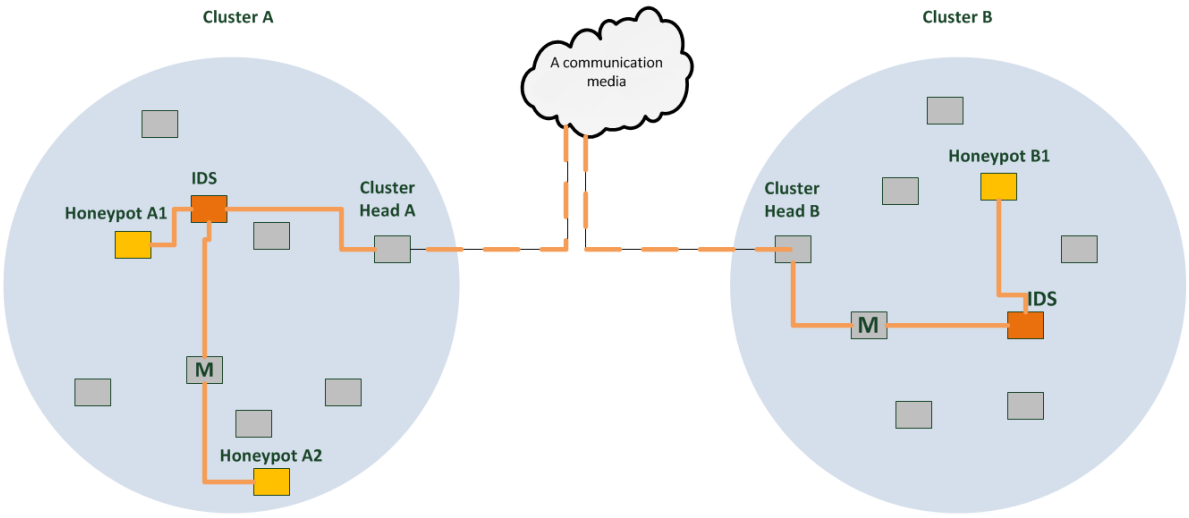
Figure 2: Internal block view of a proposed honeypot node for MANETs



- **Node Operating System:** it's simply an operating system running in the node. This operating system should consist of a virtualization program allowing the guest operating system to run.
- **Bait Operating System:** A bait operating system is a guest OS running in a virtualized environment containing the luring contents and a service to log all the activities and report it to logging unit in the honeypot software. This service is named Event Logger Service in figure 2.
- **Luring Contents:** this is actually the contents we think an attacker ask for it. This may be the information he is interested in. and obviously it is kind of fake information. It may be the information appearing as a higher security level or something like that. Maybe a fake structure of files and folders that seems to be something important.
- **Honeypot Software:** a piece of software doing the job of logging and analysis of input data from Event Logger Service, running in the Bait operating system. Honeypot software also does communications to IDS system using encryption and decryption through Honeywall service. We use encryption/decryption to communicate to IDS system, because of MANET characteristics. It's obviously a necessity to use some methods of hiding traffic between honeypot nodes and IDS, and protecting it from eavesdropping and possibly modifying. So we use encryption/decryption methods to provide confidentiality and integrity of traffic between honeypot nodes and IDSs.

Figure 3 is demonstrating communications between honeypot nodes and IDSs and also IDSs together in a cluster-based MANET.

Figure 3: Honeypot nodes, IDS nodes and communications between them in a cluster-based MANET



In figure 3 the orange lines are encrypted channels that IDSs and honeypot nodes use them to communicate with each other. See the nodes marked M in cluster A and also in cluster B are acting as intermediate nodes to transmit the encrypted data, so they cannot read or modify the packets contents.

Note that communication between two nodes in different clusters should be done through the cluster heads. This communication could be done via Internet or other communication media. And because there are other packets sending and receiving between these two cluster heads, so the orange line is dashed (in figure 3), as there are other packets passing through the same path.

- **Honeywall Service:** this is the most important element. This service is running in the Honeypot node operating system and acts like a honeywall gateway in a traditional honeynet wired network. But it just acts for one honeypot not a group of them. Actually in this model we have one honeywall for each honeypot node.

All the inbound and outbound traffic of the honeypot node is passing through Honeywall service. Honeywall (like in classical deployment) will capture these packets. But in traditional wired networks, a honeywall would capture all the traffic, because almost all the passing traffic was suspected to be malicious. Of course there was some exception for these. Like the traffic of monitoring software or the normal packets generated by honeypot systems to stay on the network. But all the other traffic was considered as malicious because there was no useful service running on the honeynet network, and also no one was aware of existence of such system on the network. But here the situation is different.

Packets entering to the honeywall may be from one of these:

- Packets are coming from a random node going to another destination, using our honeypot node as an intermediate. This happens in MANETs when two communicating nodes are not in their radio range. These packets just need to be forwarded to the next node based on the routing protocol currently in use.
- Packets have the honeypot IP address as its destination: these packets are two types:
  a) The source IP address is an IDS node: in this case, after checking with honeywall rules to be ensured the sender is actually an IDS, honeywall send the packet to honeypot software to be decrypted and be used by honeypot software.
  b) The source IP address is not an IDS node: in this case the honeywall, after checking with honeywall rules will capture a copy of the packet and send it transparently to the bait operating system. And the further activities can be logged and more analysis can be done over there.
- Honeywall **Rules:** using this unit, let us to configure the honeywall in a more flexible way by defining packet filtering rules. Adding, deleting and changing rules to fit the network environment situations.

By using honeypot nodes we hope to reduce the insider attacks, which is the biggest problem of security concerns in MANETs.

6. Conclusion and Future Works

Security in MANET networks are more complicated than networks with infrastructure and all the facilities associated with them. The main security issue in the MANETs based on its nature are insider attacks. In this paper we attempted to reduce the risk of these kinds of attacks and use a method to learn new malicious tactics used by adversaries, by suggesting the use of honeypots in MANET networks. After discussing the security issues of MANETs and their vulnerabilities, we talked about advantages and disadvantages of honeypots in networks. Then we proposed a model of a honeypot node to be used in MANETs. As our future work we will concentrate on realizing the proposed model in a specific platform to develop a sample for simulation and more evaluations.

References

[1] Kuldeep Sharma, Neha Khandelwal, Prabhakar.M, 2010, “An Overview Of security Problems in MANET”, *PSRC - Planetary Scientific Research Center Proceeding*.

[2] Priyanka Goyal, Vinti Parmar, Rahul Rishi, January 2011, “MANETs: Vulnerabilities, Challenges, Attacks, Application”, *IJCEM Journal of Computational Engineering & Management*,, Vol. 11.

[3] Yongguang Zhang and Wenke Lee, 2004, “Security in Mobile Ad-Hoc Networks”, Ad Hoc Networks Technologies and Protocols (Chapter 9), USA, Springer, 2004, pp. 249-264

[4] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, 2010, “Different Types of Attacks on Integrated MANET-Internet Communication”, *International Journal of Computer Science and Security (IJCSS)*, Volume (4): Issue (3) , pp. 265-274.

[5] Karen Scarfone, Peter Mell, February 2007, “Guide to Intrusion Detection and Prevention Systems (IDPS)”, NIST Special Publication 800-94, U.S. Department of Commerce.
[6] Lance Spitzner, 2003-07-17, “Honeytokens: The Other Honeypot”.
[7] Lance Spitzner, 2003, “Honeypots: Catching the Insider Threat”, Honeypot Technologies Inc.
[8] Arash Barfar and Shahriar Mohammadi, June 2007, “Honeypots: Intrusion deception”, *ISSA, The Global Voice of Information Security,* pp. 28-31.