Technical Report

Department of Computer Science
and Engineering
University of Minnesota
4-192 EECS Building
200 Union Street SE
Minneapolis, MN 55455-0159 USA

TR 04-010

Monitoring of Wireless Networks for Intrusions and Attacks

Sandeep Karanth and Anand Tripathi

February 24, 2004

Monitoring of Wireless Networks for Intrusions and Attacks *

Sandeep Karanth and Anand Tripathi
Department of Computer Science
University of Minnesota, Minneapolis MN 55455

Abstract

Wireless networks based on IEEE 802.11 are becoming integral parts of any enterprise network. The inherent openness of these networks makes them a target for attackers. The coverage of wireless networks cannot be confined by walls or obstacles. The task of an enterprise network administrator is thus compounded by the introduction of wireless technology. Most of the attacks on wireless networks are due to vulnerabilities in the Medium Access Control (MAC) Layer. This fact drives the need for a MAC layer network monitoring system.

As part of the Konark project we have developed a mobile-agent based network monitoring system for the wired network. This system facilitates centralized viewing of network alerts through cooperating agents. The main contribution of this project is the development and deployment of an analysis and attack detection tool for 802.11 wireless networks. Events generated by this tool are correlated using Konark monitoring agents and the administrator is alerted. We focus on detection of MAC address spoofing, Denial of Service attacks and network misconfigurations. We also provide services to users and applications. This report describes the different modes in which network monitoring could be done in an enterprise network using such a tool. The trade-offs involved with each mode of operation is described too.

1 Introduction

One of the important tasks of a system administrator is to monitor networks to ensure proper system operation and protect system resources from being misused by intruders or attackers. This typically involves monitoring for inconsistencies in user activities, resource usage, system configuration, and enforcing security policies. A large enterprise network typically consists of hundreds of nodes and resources with varying amount of heterogeneity among them in terms of the hardware and software used. In the last few years, wireless networks are becoming integral components of any enterprise network. Most of these networks are based on the IEEE 802.11 standard [1]. The communication medium in wireless technology is an open broadcast medium. Further, it is very difficult to confine radio waves to a particular area as they pervade walls and obstacles. These reasons make it easier for attackers and war-drivers to identify wireless networks and launch attacks.

Most of the security vulnerabilities in wireless networks are in the Medium Access Control (MAC) sublayer. For attacks in the upper layers of the protocol stack there are well known detection tools available for the administrator [2]. There are wireless network analyzers for 802.11 wireless networks, but most of them require manual analysis to detect attacks. These analysis tools cannot detect attacks where MAC addresses are spoofed and are best used for detecting network misconfigurations and failures. Our objective is to provide a wireless network analysis system that will alert the administrator about possible attacks or misconfigurations with minimum latency.

We have developed a mobile-agent based network monitoring system (Konark) for centralized monitoring of networks. This monitoring system is based on the concept of co-operating agents and uses a publish-subscribe paradigm to achieve communication between monitoring agents in the system.

The main contribution of this work is to show the need for a MAC layer analysis tool for monitoring 802.11 based wireless networks. This project also shows different ways by which a layer-2 wireless monitoring tool can be integrated with an existing network monitoring system to enhance the monitoring capabilities of the system. We have developed a MAC layer

* This work was supported by National Science Foundation grant ANI 0087514.

based tool that is capable of detecting most attacks and misconfigurations in a wireless network. We have integrated this tool with an already existing network monitoring system making this system more comprehensive in terms of monitoring.

This report is organized as follows. In section 2, we provide an overview of the IEEE 802.11 standard with introduction to the different terms that will be used in the report. We discuss the potential threats to open wireless networks in section 3. This section then discusses details about the different modes in which the Konark monitoring system can be operated with a MAC layer analysis tool in place. Finally, this section discusses the different detection strategies used in the tool we have developed. Description of the experimental setup we have used is discussed in section 9. Related work is discussed in section 10. In section 11, we present conclusions and future work.

2 IEEE 802.11 Network Overview

IEEE proposes a protocol standard for wireless LANs called IEEE 802.11 [1]. This protocol operates at the Physical (PHY) and Medium Access Control (MAC) layers. 802.11 networks operates in one of the 2 modes: *infrastructure* mode and *ad-hoc* mode. In *ad-hoc* mode wireless clients can directly communicate with each other. However , in the *infrastructure* mode wireless clients communicate with a central base station called Access Point (AP). The access point acts as a bridge forwarding packets onto the appropriate network (wired or wireless). We concentrate on wireless LANs operating in the infrastructure mode in our work. At the MAC layer IEEE 802.11 implements CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance). Simultaneous transmissions are handled by the Binary Exponential Back-off algorithm. Hidden station problems are solved by exchange of RTS (Ready-To-Send) and CTS (Clear-To-Send) frames.

A *Basic Service Set* (BSS) is a set of stations capable of communicating with each other. An ad-hoc network is called an *Independent Basic Service Set* (IBSS). In the infrastructure mode, many BSSs could be combined to form an *Extended Service Set* (ESS). The architectural component used to interconnect the BSSs to form an ESS is called a *Distribution System* (DS). An AP could be viewed as a station providing access to the DS and its services. IEEE does not define any standard for the DS.

Prior to data communication, wireless stations and APs must establish a relationship called *association*. The association process is a 2-step process involving three states. Management frames (Figure 4) need to be exchanged between the wireless station and the AP for transition between these states. A station keeps two state variables for each station it would like to communicate with. Note that we consider an AP to be a station too. The two state variables are Authentication state (values are unauthenticated or authenticated) and Associated state (values are unassociated and associated). The three states formed by these state variables are:

1. Unauthenticated and Unassociated
2. Authenticated and Unassociated
3. Authenticated and Associated

The state transition diagram between these 3 states is shown in figure 1.

APs could transmit *beacon* management frames at fixed intervals advertising themselves. The format of a typical beacon frame is shown in Table 2. A client listens to these beacon frames to decide as to which AP to associate with. *Service Set Identifiers* (SSIDs) are generally presented to the user in the beacon frames. A client may also send a *probe request* management frame (Table 8) to find an AP affiliated with a particular SSID. After a wireless client identifies an AP, the client and the AP perform authentication. Most networks implement MAC address based access control lists (ACL) with no explicit authentication protocol. This is called open authentication and is the default protocol in 802.11. IEEE 802.11 also defines a shared key based mutual authentication scheme. *Wired Equivalent Privacy* (WEP) protocol is designed to provide confidentiality in 802.11. Shared key authentication is based on a challenge-response protocol and WEP is used to encrypt the challenge text. Once a wireless client is successfully authenticated the AP moves from state 1 to state 2 (Authenticated and Unassociated state) and an *Association request* frame (Table 4) is sent by the client. The AP responds with an *Association response* frame and the client is now associated with the AP and could send data frames (Figure 3). Every frame has two frame control bits ”To DS” and ”From DS”. These bits indicate if the frame is entering the DS or exiting it. Both of these bits cannot be true at the same time. Management frames have both these bits reset. Frame formats and frame types in each class are listed in Appendix A.

A roaming user could associate with an AP closest to him/her in an ESS. When a wireless client wants to associate with another AP within the same ESS, authentication need not take place again. However, a reassociation needs to take place as the

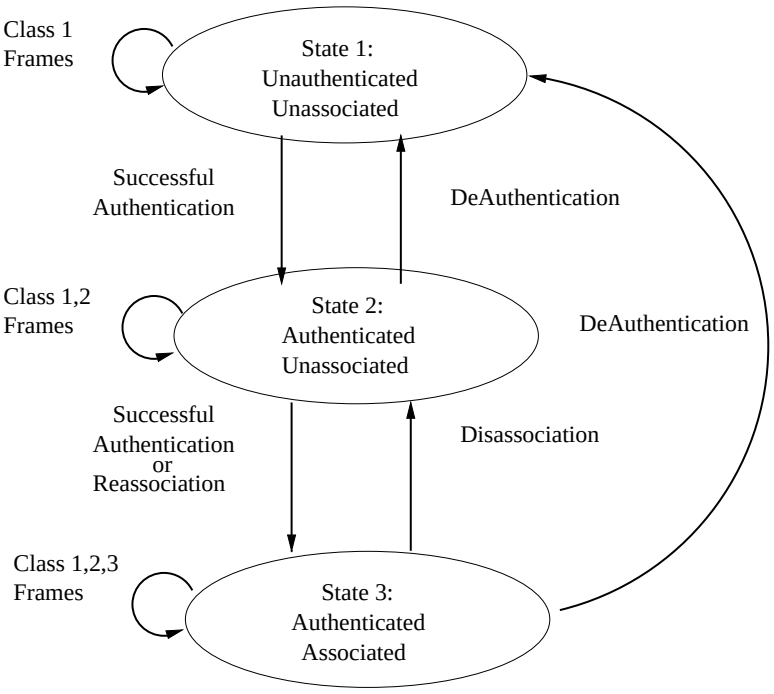

Figure 1. State Transition Diagram

association relationship changes. This is done by a *Reassociation request* and a corresponding *Reassociation response* from the AP. An AP could disassociate or deauthenticate a client using the *Disassociation* frame(Table 3) and the *DeAuthentication* frame(Table 11). A client could also request disassociation or deauthentication from an AP.

IEEE 802.11 is a MAC protocol and addressing is based on the 6-byte unique MAC address associated with each network interface card. A broadcast address is all 1s in the 6-byte address. Beacon frames and Probe request frames have broadcast addresses in their destination address field. It must also be observed that these addresses are sent in the clear as the management frames and MAC headers of any frame in 802.11 is not encrypted. 802.11 frames have sequence numbers that are 12 bits long ranging from 0-4095. A MAC frame could be fragmented. Fragmented frames have the same sequence number but will have different fragment numbers.

3 System Overview and Capabilities

The goals of any wireless monitoring system can be categorized broadly into, *Monitoring* objectives and *Service Provisioning* objectives. Monitoring objectives include monitoring the wireless network for possible attacks, detection and response to unauthorized use, and alerting administrators or users regarding possible network misconfigurations or failures. Services are provided to ubiquitous applications regarding proximity of users and user mobility patterns, to users regarding account usage and misconfigurations, and to service providers regarding usage patterns and network coverage.

4 Konark: A Mobile Agent based Network Monitoring System

This tool is integrated with Konark [3, 4, 5], an agent-based network monitoring system that facilitates dynamic extensibility of monitoring functions, active monitoring, easy integration of off-the-shelf components and distributed event correlation. Monitoring agents in Konark can be powered with monitoring capabilities in the form of detectors to parse and analyze log files and generate events. These agents are also capable of subscribing to events from other agents. With detection and subscription capabilities monitoring agents can make correlations and take appropriate actions or alert the administrator. The capabilities of these agents can be dynamically modified or extended. Controlling the Konark monitoring system is easy with an user friendly GUI.

Capabilities of Konark are enhanced by integrating this system with it. Events generated by this system are correlated with host-level Konark events to gain insight into an attacker's activity and origin. Correlated events can also be disseminated to aid in the service provisioning objectives of the system. We use the monitoring agents of Konark to generate events from the syslog file (logged by the AP) or any other alert file. APs could be geographically dispersed though they belong to the same ESS. Agents facilitate event correlation from dispersed sources.

5 Potential Threats

Wireless networks based on 802.11 are vulnerable to many attacks [6]. As part of this work we focus on the following threats:

1. MAC address spoofing.
2. Denial-of-Service attacks on wireless components.
3. Network misconfigurations or failures.

5.1 MAC address spoofing

Changing the MAC address of a wireless card is a very trivial task that can be performed by novice attackers too, as it can be done by software. Most wireless infrastructures use a MAC-based access control list to authenticate and let wireless clients associate. A simple command is all that is needed to spoof the MAC address and most drivers provide this facility. With a spoofed MAC address a malicious user could exploit the network in the following ways,

- A malicious user could change their MAC address and pose as a legitimate user to gain entry into the network. With packet sniffers for wireless networks available for free, coupled with the fact that MAC addresses are sent in the clear, it takes little effort for an adventurous attacker to sniff out legitimate MAC addresses and use them to gain access to the network. This is particularly easy where access points are configured for open authentication. Even with shared key authentication enabled it has been shown that WEP is not a safe encryption algorithm at any key size [7, 6].
- An attacker could advertise as a legitimate AP by using the MAC address of an AP and could get clients to connect with itself. We term these APs as *Fake APs*.
- An attacker could launch Denial-of-Service attacks by sending spoofed deauthenticate or disassociate frames to clients logged on to the network.

The above mentioned attacks are particularly easy with programs and libraries such as *macchanger* [8], *FakeAP* [9] and *LibRadiate* [10] readily available.

5.2 Denial-of-Service Attacks

In [11], it is shown that even with authentication mechanisms, wireless networks based on IEEE 802.11 standard are prone to denial-of-service attacks. This is mainly because management and control frames are not encrypted. We have already seen one kind of DOS attack where a malicious user constructs a deauthentication or a disassociation request and sends it to a client whom it wants to disconnect from the network. A client launching a DOS attack on an access point could repeatedly send authentication request frames in a short interval of time. An access point has to retain state after an authentication request by a client and before a client associates with it. A client could continuously flood the access point with authentication requests making the access point incapable of accepting more client requests. RTS and CTS control frames are used for collision avoidance in the 802.11 MAC protocol. RTS flood attacks could be conducted by continuously emitting RTS frames and denying other stations from using the medium.

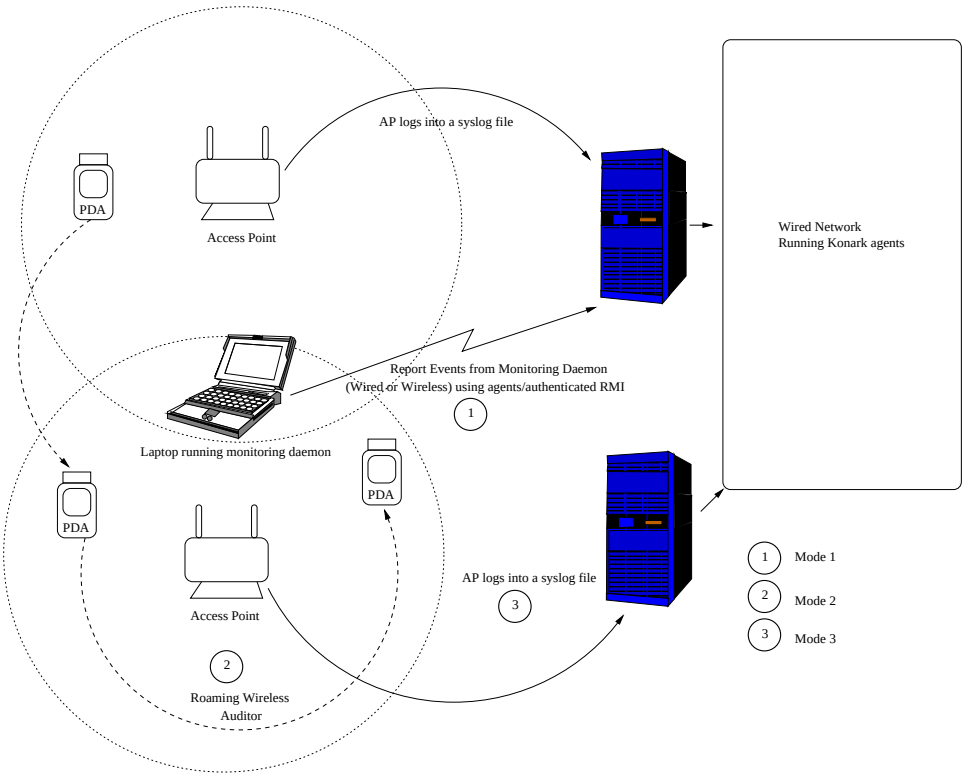

Figure 2. Modes of Operation

5.3 Network misconfiguration or Failures

Access points could fail, shutting off services for clients. As wireless equipment becomes inexpensive, it becomes easy for unauthorized users to establish their own access points. The problem with such rogue access points is that they may not conform to an organizations security policies. Organizations having wireless infrastructure could have policies regarding acceptable signal strengths, encryption, supported rates etc. For example, an organization could have a policy whereby certain sensitive access points need to have encryption and authentication enabled. There is always a possibility of policy violation in huge organizations where a large number of network components need to be maintained. Such misconfigurations and policy violations need to be reported.

6 Modes of Operation

The Konark network monitoring system can operate in 3 modes with wireless network monitoring tools in place. The figure 2 illustrates these modes of operation. In the first mode of operation, we install notebook PCs/laptops/PCs with wireless cards at strategic points in the network to get entire wireless network coverage. These hosts run a monitoring daemon that analyzes packets from the wireless medium and generates events. For the monitoring daemon to analyze packets a packet capturing software has to be running on the host under root privileges. A packet capturing program is going to put the card in RFMON (monitoring) mode and thus through the wireless card no transmissions can take place. The monitoring daemon has configurable options and the detection capabilities of the daemon can be altered. This daemon analyzes packets, makes correlations and generates an alert file.

These hosts could have an additional interface through which they could connect to the wired LAN. If they are connected to a wired network, a Konark monitoring agent is sent to these machines to generate events after reading the alert file written by the daemon. However if they do not have a wired network connection we need switch from RFMON mode to normal mode and transmit any events generated. This switching has to be done at certain intervals of time depending on the number of events generated by the monitoring daemon. However, events generated by the daemon are sent through the same wireless

Attack/Misconfigurations	Mode 1 (Dedicated notebooks/PCs)	Mode 2 (PDAs)	Mode 3 (AP logs)
MAC spoofing	Possible	Not possible	Possible in some cases (2 identical clients associated with different APs in an ESS)
DOS Attacks	Possible	Not possible	Possible in some cases (Cannot detect forced deauthentiction/disassociation)
Network Misconfigurations /Failures	Possible	Possible	Possible in some cases (Cannot detect rogue APs)

Table 1. Capabilities in each mode of operation

medium which may not be safe. To avoid this the daemon would request the Konark system to send an agent to collect the events generated by it when it switches to normal mode. Konark monitoring agents are developed using the Ajanta mobile-agent programming framework. Ajanta [12] provides tamper-proof mechanisms for securing data on agents. An alternate design would be for the daemon to launch an agent and send the events gathered by it to an administrator. Existing Konark agents provide for authenticated RMI. Agents also provide support for disconnected operations. With these capabilities a third alternative would be, to have agents running on the monitoring daemon gathering events, and transmitting them using authenticated RMI at intervals of time to subscriber agents on the wired network. This event transmission takes place when the daemon changes from RFMON to normal mode.

This is the most powerful mode of operation as all of the mentioned monitoring objectives can be achieved in this mode. At the same time, this approach is the most expensive in terms of cost and computation. Strategically placing these monitoring daemons to get entire network coverage is not trivial.

In the second mode of operation, the above mentioned daemon will be running on a PDA or an handheld device. An administrator has to take a walk through the campus where the wireless LAN is deployed. The daemon generates alerts on the terminal. We would like to provide off-loading of events from the hand-held to the wired network too. The functions of the daemon are scaled down. This is one of the weakest modes of operation. This mode of operation cannot detect DOS attacks and other attacks that require online monitoring. It is however useful for identifying network misconfigurations and failures.

Most APs in an ESS are connected by a wired DS. APs can log information about packets going through them in a syslog file. Monitoring agents are sent to parse these files and generate alerts. This mode of operation is the least expensive as it uses the existing infrastructure. But this mode is not as powerful as mode 1. We will not be able to detect forced deauthentication attacks, rogue APs, fake APs or do any kind of sequence number analysis in this mode. The capabilities of the 3 modes of operation are summarized in Table 1.

7 Detection Logic and Response

We detect most of the attacks conducted by MAC spoofing using a sequence number analysis technique as discussed in [13]. It is observed that the sequence number field in a 802.11 frame is put in by the firmware. The sequence number field (Figure 3) in a frame is a 12 bit field that has a value between 0 and 4095. As each frame is emitted by a wireless station (client or an access point), the sequence number is incremented by 1 and it wraps around at 4095. Thus it is highly unlikely that sequence numbers of 2 stations having the same MAC address are identical. By observing sequence numbers in frames we can detect any MAC address spoofing going on in the network. An assumption made here is that both the legitimate wireless station and the faking one are on the network at the same time.

Analysis of packets is intensive in computing. The monitoring daemon analyzes packets by taking packets from the packet capturing tool. This may cause the packet capturing tool to drop packets if the analyzer is working at a slower pace. Due to such limitations of the tools we use to capture packets for sequence number analysis, we may have to fix a threshold for the sequence number difference. If this threshold is small then we may get a lot of false positives. We have chosen a tolerance of 20 i.e., we conclude that malicious activity is going on in the network if we happen to see frames from the same source having sequence numbers differing by more than 20 values. But now the question arises as to how can we detect attackers who gain access to the network in a time frame disjoint to that of the legitimate user?. We implement a policy where we

specify likely times when we expect to see activity from a particular user and flag off alerts when we observe MAC activity of the user during other times. We also provide notification to the owner of the wireless client when he/she associates with the network. We get this information from the syslog file (mode 3) or by observing associate requests and responses (mode 1). In this way, an user is aware about his usage pattern and can notify the network administrator if there is any discrepancy.

There is also a possibility in an Extended Service Set (ESS) having many access points that a legitimate user connects to one access point and the malicious user to another that are out of range of each other. In such a scenario, we need some kind of distributed correlation to be done. Our monitoring daemon is present in many locations to get complete network coverage. Konark monitoring agents can subscribe to associate request events and make correlations. Our monitoring daemon records authentications and associations along with the sequence number of the frame and also the time of logging. The centralized correlation detectors could check overlapping time intervals of these events from the same source and raise alerts to the administrator. Other than notification to the user about suspected MAC spoofing, repeated instances of such MAC spoofing with the same address would lead to the MAC address to be blacklisted and removed from the access control list of the ESS.

Access points emit beacon frames advertising their presence to clients who would like to logon to the network. Like any other wireless station an access point increments a sequence number and puts it in each frame it is going to transmit. An attacker who tries to spoof the access point's MAC address and advertises himself as a legitimate portal into the network will have an out-of-order sequence number field from the authentic access point. Our monitoring daemon will record beacon frames and probe responses with their sequence numbers and generate events in case of mismatch. Again monitoring agents could make higher correlations to detect fake access points that are out of range with the authentic one. Every beacon frame is not logged, instead we record beacon frames/probe responses at particular intervals.

Disassociate/Deauthentication requests can be sent either by an access point removing a wireless clients or a wireless client can request disassociation from an access point. When a malicious client sends such a frame to disassociate another client it would fake as an access point. Comparing the sequence number of this frame with the last frame sent by the access point we can infer that a faking client had launched an attack. Authentication floods on an access point can be detected by the monitoring daemon through traffic analysis and packet type count. We could also detect such flood attacks by analyzing the syslog file generated by the AP.

Failure of access points that advertise by means of beacon frames can easily be determined by missing beacons. Some networks may implement a policy where by access points do not advertise beacon frames. To detect failure of such access points the monitoring daemon sends probe requests when it switches out of RFMON mode and waits for probe responses from the access point to check for liveness. AP logs can also be analyzed for liveness of APs. Configuration parameters from beacon frames are analyzed to see if access points are configured according to the norms of the network. Signal strengths are analyzed to ensure network liveness and coverage.

Our monitoring daemon can sniff out presence of rogue access points by comparing it with a baseline network configuration which is fed to the system before startup. It is not enough if we monitor only the beacon frames as rogue access points may not transmit beacon frames. It is essential that we monitor other frames too (Probe requests/responses) and look out for MAC addresses in the frame that are not known in the baseline. This baseline network configuration should be extensible as the network configuration changes (access points are installed or removed). In case of any misconfigurations or failures, the administrator could be alerted to take necessary action.

8 Service Provisioning Objectives

Apart from failure and attack detection we provide services to users and applications. Ubiquitous applications generally require user proximity detection and tracking. Since we log user associations with access points we can determine the proximity of the user to the access point. This kind of service would use existing infrastructure without the need for GPS tracking. Such a service is useful in a small geographic area that is entirely covered by the same wireless network. Konark supports a publish-subscribe paradigm. Association events could be gathered from the monitoring daemon by the Konark monitoring agents and appropriate applications could subscribe to these events. Association events could be gathered from the AP logs (syslog) as well. Triangulation methods could be used to get a more precise location of the user.

Repeated DHCP denials, frequent disassociations and reassociations with the same access point and unknown frame transmittals by a client could mean errors in the client's configuration or brute force attacks. To improve the wireless service to the client, such events could be notified to the owner of the wireless client.

9 Experimental Setup

We conducted experiments on the Computer Science department wireless LAN to evaluate the system. The department has many APs installed on different floors of the building to form an ESS. The APs are mainly Cisco Aironet Access Points [14] (340 and 350 series) with software release 12 and above. The wireless network in the department has an open authentication scheme based on a MAC address ACL. Encryption is not enabled in the APs as key distribution is a tedious task. Users who want to use the network have to get their wireless card MAC address registered with the system administrator.

We used three notebook PCs to simulate attack scenarios and detect them. All the notebooks were using Cisco Aironet 340/350 series wireless cards. The PCs were running different Linux flavors with aironet drivers. MAC spoofing can be done at the command line using the *ifconfig* tool on these notebooks. The monitoring daemon used *Kismet* [15] as the packet capturing software and *Ethereal* [16] as the packet analyzer. The daemon itself was written in C++. To run Kismet and capture packets the card has to be run in monitoring mode (RFMON). This requires root privileges on the notebook PCs.

We could spoof the MAC address of an already registered card and gain access to the network. The monitoring daemon detected this misuse by sequence number analysis when both the legitimate client and the faking client were connected to the network. We detected fake and rogue APs by generating attack traces and feeding it to the daemon. We will extend these experiments by using available attack tools like FakeAP [9] in the near future. DOS attacks were simulated by manually constructing attack traces. We have identified packet injection libraries like LibRadiate [10] that could be used to actually conduct such attacks.

APs in the department network broadcast beacon frames every 100 milliseconds. Our monitoring daemon was slow in processing every beacon frame. A slow daemon was causing Kismet to drop packets randomly. Hence we had to fine tune our daemon to analyze one in ten beacon frames so that we have control on the packets that are being dropped.

APs can be configured to log events in a log file. We had logs of APs written to syslog files. Konark agents were made to parse these syslog files and generate events. Facilitating syslog file parsing by monitoring agents was a rather simple task (addition of patterns) because of the dynamic extensibility support provided by the Konark framework. Simple detectors were written in Java and installed on monitoring agents to correlate events generated by parsing the log file. Monitoring agents are capable of storing these events in MySQL databases to facilitate communication between co-operating agents or to support archiving.

To support the roaming auditor mode of operation, we will install the components of the system on a handheld device such as a Zaurus PDA. Packet capture and analysis tools like Kismet are already available for such handheld devices.

10 Related Work

IEEE 802.11 [1] standard was formed in 1997 as a physical and MAC layer protocol for wireless networks. The security vulnerabilities in wireless networks and the WEP protocol were exposed by many researchers [6, 17, 7]. A security framework called Robust Security Network (802.1X) has been proposed by the IEEE. In [11] a security analysis of this framework is given. It has been noted that this framework does not provide solutions to many DOS attacks.

There are many wireless network monitoring and intrusion detection tools [18, 19]. Some of these tools can be integrated with Snort [2] and other intrusion detection tools. But most of these tools do not deal with network misuse or attacks involving spoofing of MAC addresses. These tools do not account for distributed attacks too. Techniques to detect spoofing of MAC addresses has been presented in [13]. Usage patterns in university networks have been studied in detail in [20] using information from packet capturing tools and syslog files.

11 Conclusions and Future Work

Wireless network deployment is increasing as it provides a lot of convenience for roaming users at lower costs. But this convenience comes at the cost of security. Further many security issues are not addressed and are left as open issues in the IEEE 802.11 standard. Higher level authentication and security schemes like the 802.1X framework do raise the security standards but do not account for many attacks (DOS attacks for example). Robust security mechanisms are not the only thing required to secure wireless networks. Strict security policy enforcement is also equally important in an organization deploying wireless networks. We have developed a MAC layer monitoring tool and integrated it with an mobile-agent based monitoring system. We have shown as a proof of concept that such a tool is quite effective in detecting various kinds of attacks and misconfigurations in a IEEE 802.11 based wireless network .

In the future, we would like to find out more cost efficient ways of analyzing packets as the need for a MAC layer based intrusion detection system for the wireless medium becomes a must. As thin clients like handheld devices become more popular we would like to investigate methodologies for building intrusion detection systems that work efficiently in environments constrained by power and computation. We would also like to customize Ajanta agents to run on handhelds and wearable computers. As pervasive applications come into existance we would like to provide more services to these applications and study the security issues associated with it.

12 802.11 Frame formats

12.1 Frame Classes

1. Class 1 frames (permitted from within States 1, 2, 3):
    - Control Frames
        - Request To Send (RTS)
        - Clear To Send (CTS)
        - Acknowledgement (ACK)
        - CF-End + ACK
        - CF-End
    - Management Frames
        - Probe Request/Response
        - Beacon
        - Authentication
        - DeAuthentication
        - Announcement traffic indication message
    - Data Frames
        - Data : Both ToDS and FromDS bit reset (false)
2. Class 2 frames (if and only if authenticated; allowed from within State 2, 3):
    - Management Frames
        - Association Request/Response
        - Reassociation Request/Response
        - Disassociation
3. Class 3 frames (if and only if associated; allowed from within State 3):
    - Management Frames
        - Deauthentication
    - Control Frames
        - PS-Poll
    - Data Frames
        - Data : Either ToDS or FromDS FC bits may be set

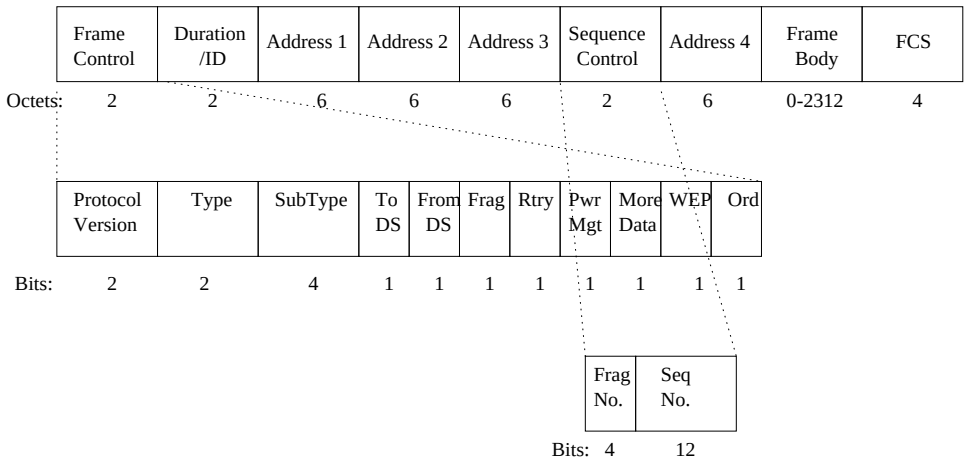

Figure 3. Generic MAC frame format

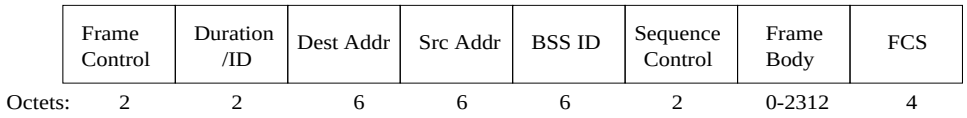

Figure 4. Generic Management frame format

Order	Information	Remarks
1	TimeStamp	
2	Beacon Interval	
3	Capability Information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	Frequency Hopping parameters
7	DS Parameter Set	Direct Sequence Parameters
8	CF Parameter Set	
9	IBSS Parameter Set	
10	TIM	

Table 2. Beacon Management Frame body

Order	Information	Remarks
1	Reason code	Reason for disassociation

Table 3. Disassociation Frame body

Order	Information
1	Capability information
2	Listen interval
3	SSID
4	Supported rates

Table 4. Association Request Frame body

Order	Information
1	Capability information
2	Status code
3	Association ID (AID)
4	Supported rates

Table 5. Association Response Frame body

Order	Information
1	Capability information
2	Listen interval
3	Current AP address
4	SSID
5	Supported rates

Table 6. Reassociation Request Frame body

Order	Information
1	Capability information
2	Status code
3	Association ID (AID)
4	Supported rates

Table 7. Reassociation Response Frame body

Order	Information
1	SSID
2	Supported rates

Table 8. Probe Request Frame body

Order	Information	Remarks
1	TimeStamp	
2	Beacon Interval	
3	Capability Information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	
7	DS Parameter Set	
8	CF Parameter Set	
9	IBSS Parameter Set	

Table 9. Probe Response Frame body

Order	Information	Remarks
1	Authentication algorithm number	
2	Authentication transaction sequence number	
3	Status code	Not present if open authentication
4	Challenge text	Not present if open authentication

Table 10. Authentication Frame body

Order	Information	Remarks
1	Reason code	Reason for deauthentication

Table 11. Deauthentication Frame body

References

[1] IEEE: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications (1997)

[2] Roesch, M.: Snort - Lightweight Intrusion Detection for Networks. In: 13^{th} Systems Administration Conference - LISA. (1999)

[3] Tripathi, A., Koka, M., Karanth, S., Pathak, A., Ahmed, T.: Secure multi-agent coordination in a network monitoring system. In: To appear in, Software Engineering for Large-Scale Multi-Agent Systems, Springer, LNCS #2603 (2003)

[4] Tripathi, A., Ahmed, T., Pathak, S., Pathak, A., Carney, M., Koka, M., Dokas, P.: Active Monitoring of Network Systems using Mobile Agents. In: Networks 2002, a joint conference of ICWLHN and ICN 2002. (2002) 269–280

[5] Tripathi, A., Ahmed, T., Pathak, S., Carney, M., Dokas, P.: Paradigms for Mobile Agent-Based Active Monitoring of Network Systems. Technical report, Department of Computer Science, University of Minnesota (2001) Available at URL `http://www.cs.umn.edu/Ajanta`.

[6] Arbaugh, W., Shankar, N., Wan, Y.: (Your 802.11 Wireless Network has No Clothes) Technical Report, Department of Computer Science, University of Maryland, College Park, Maryland 20742.

[7] Walker, J.: Unsafe at any key size: An analysis of the WEP encapsulation (2000) Technical Report 03628E, IEEE Standards 802.11 Committee.

[8] Changer, M.: (A gnu/linux utility for viewing/manipulating the mac address of network interfaces) Available at `http://www.alobbs.com`.

[9] FakeAP: (Black alchemy weapons lab) URL `http://www.blackalchemy.to/project/fakeap/`.

[10] Schiffman, M.: Radiate 802.11b frame handling (2002) http://www.packetfactory.net/projects/radiate/.

[11] Mishra, A., Arbaugh, W.A.: An initial security analysis of the IEEE 802.1X standard (2002) Technical Report CS-TR-4328,UMIACS-TR-2002-10 University of Maryland.

[12] Karnik, N., Tripathi, A.: Security in the Ajanta Mobile Agent System. Software - Practice and Experience **31** (2001) 301–329

[13] Wright, J.: (Detecting Wireless LAN MAC Address spoofing) Available at URL `http://www.linuxsecurity.com/articles/documentation_article-6585.html`.

[14] Cisco: (Cisco aironet access point software configuration guide) Available at URL `http://www.cisco.com`.

[15] Kismet: (802.11 wireless network sniffer) Available at URL `http://www.kismetwireless.net`.

[16] Ethereal: (A network analyzer) Available at URL `http://www.ethereal.com`.

[17] Borisov, N., Goldberg, I., Wagner, D.: Intercepting Mobile Communications: The Insecurity of 802.11. `http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html` (2001)

[18] AirDefense: (Air defense gaurd and air defense rogue watch) Available at URL `http://www.airdefense.net`.

[19] Widz: (Wireless intrusion detection system) Available at URL `http://www.packetstormsecurity.com/wireless/widzv1-0.zip`.

[20] Kotz, D., Essien, K.: Analysis of a campus-wide wireless network. In: Proceedings of MOBICOM 2002. (2002)