Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Intrusion Detection in 802.11 Wireless Local Area Networks

Mazda Salmanian, Julie H. Lefebvre,
Steve Leonard and Scott Knight

Defence R&D Canada – Ottawa
TECHNICAL MEMORANDUM
DRDC Ottawa TM 2004-120
July 2004

Canada

Intrusion Detection in 802.11 Wireless Local Area Networks

Mazda Salmanian
Julie H. Lefebvre
Defence R&D Canada – Ottawa

Steve Leonard
Scott Knight
Royal Military College of Canada

Defence R&D Canada – Ottawa

Technical Memorandum

DRDC Ottawa TM 2004-120

July 2004

Abstract

This paper presents a theoretical study of the wireless protocol defined by the IEEE 802.11 standard in order to identify characteristics or potential idiosyncrasies that could be used to enhance intrusion detection in a WLAN. The control, management, and data frames used to implement the media access control (MAC) functionality along with WLAN services and a state relationship that governs the exchange of frames between wireless stations provide useful insights into the signatures that identify security-related threats and intrusions.

The threat signatures obtained in this research clearly indicate the usefulness of IEEE 802.11 frames and the state relationship rules in helping to detect some of the known threats to WLANs. The frame types and information fields provide insights about the source of the transmission as well as the intent. The state relationship rules assist in the detection of situations that violate the procedures described in the 802.11 standard.

A number of common security-related threats are discussed and evaluated in experiments. The characteristics of the IEEE 802.11 standard are exploited to derive signatures for these threats in supporting intrusion detection in a WLAN [1].

Résumé

Cet article présente une étude théorique du protocole sans fil défini par la norme d'IEEE 802.11 afin d'identifier des caractéristiques ou des idiosyncrasies potentielles qui pourraient être employées pour supporter la détection d'intrusion dans un réseau sans fil.

La commande, gestion, et les trames de données utilisees dans l'implimentation du contrôle d'accès avec les services de reseaux sans fil et un rapport d'état qui régit l'échange des trames entre les stations sans fil fournissent des perspectives utiles des signatures qui identifient les menaces d'intrusions.

Les signatures de menace obtenues de cette recherche indiquent clairement l'utilité des trames d'IEEE 802.11 et les règles de rapport d'état en aidant à détecter certaines des menaces connues envers les réseaux sans fil. Les types de trames et les champs de l'information fournissent des perspectives au sujet de la source de transmission aussi bien que de l'intention. Les règles de rapport d'état aident à la détection des situations qui enfreindrent les procédures décrites par la norme 802.11.

Un certain nombre de menaces communes envers la sécurité sont discutées et évaluées dans les expériences. Les caractéristiques de la norme d'IEEE 802.11 y sont exploitées pour dériver les signatures de ces menaces afin de supporter la détection d'intrusion dans un réseau sans fil.[1].

This page intentionally left blank.

Executive summary

The flexibility, capability, and economics of wireless local area networks (WLANs) make them an attractive communication asset. They are, however, vulnerable to various types of intrusion-related attacks that can compromise the confidentiality, integrity, and availability of information and resources. Before WLANs gain widespread acceptance in the Department of National Defence (DND) and Canadian Forces (CF), it is necessary to understand the nature of these attacks and to develop techniques capable of detecting and guarding against intruders in a wireless environment.

This paper presents a theoretical study of the wireless protocol defined by the IEEE 802.11 standard in order to identify characteristics or potential idiosyncrasies that could be used to enhance intrusion detection in a WLAN. In this research, we have observed, tested, and documented threat signatures for intrusion detection in WLANs. The signatures aid in the detection of rogue access points and unauthorized stations that attempt to invade the LAN by probing (frame injection), illegal authentication, or associations. The methodology was developed by studying and analyzing the following concepts in the 802.11 standard: MAC sub-layer services, permitted frame types, and the state relationship rules that govern the exchange of the permitted frames. Based on the aggregate information from our laboratory testing, we have summarized the relevant frames and events that trigger intrusion alerts in a tabular format. Such a table can be exploited in scheduled audit scripts in WLANs to detect intruders of documented attacks.

We have recommended that a network administrator should ensure that wired equivalent privacy (WEP, or other link layer algorithms like Wi-Fi protected access, WPA) is enabled so that unintentional traffic (from higher layers such as Dynamic Host Configuration Protocol, DHCP, and Address Resolution Protocol, ARP) is encrypted before being released over the WLAN. Establishing a firewall to prevent this traffic from being broadcast over the wireless link is also important. We also observed that traffic was unintentionally transmitted from the AiroPeek stations sniffing or monitoring the WLAN. These frames are usually transmitted without a service set identifier, SSID - which is not standard compliant - and may be detected.

When an unauthorized station spoofs the MAC address, IP address, and computer name of an authorized station, its traffic is undetectable. In this case, both the legitimate and spoofing stations are unable to browse or transfer network files, thus creating a denial of service for the authorized station. We also explored taking an active approach to intrusion detection and noted that it is not suited to the 802.11 standard.

The threat signatures obtained in this research clearly indicate the usefulness of IEEE 802.11 frames and the state relationship rules in helping to detect some of the known threats to WLANs. The frame types and information fields provide insights about the source of the transmission as well as the intent. The state relationship rules assist in the detection of situations that violate the procedures described in the 802.11 standard.

Salmanian, M., Leonard, S., Lefebvre, J. H., Knight, S. 2004. Intrusion Detection in 802.11 Wireless Local Area Networks. DRDC Ottawa TM 2004-120, Defence R&D Canada - Ottawa.

Sommaire

La flexibilité, la capabilite, et l'aspect économique des réseaux locaux sans fil les rend une forme de communication attrayante. Ils sont, cependant, vulnérables à divers types d'attaques reliées à l'intrusion qui peuvent compromettre la confidentialité, l'intégrité et la disponibilité de l'information et des ressources. Avant qu'il y est une utilisation répandue des réseaux sans fil dans le département de la défense nationale et des forces canadiennes, il est nécessaire de comprendre la nature de ces attaques et de développer des techniques capables de détecter et de garder contre les intrusions dans un environnement sans fil.

Cet article présente une étude théorique du protocole sans fil défini par la norme d'IEEE 802.11 afin d'identifier les caractéristiques ou les idiosyncrasies potentielles qui pourraient être employées pour supporter la détection d'intrusion dans un réseau sans fil. Dans cette étude, nous avons observé, examiné, et documenté les signatures de menaces de détection d'intrusion dans un réseau sans fil. Les signatures assistent à la détection des points d'accès et stations non-autorisées qui essayent d'envahir le reseau en sondant (injection de trames), authentifications illégales, ou associations illégales. La méthodologie a été développée en étudiant et en analysant les concepts suivants de la norme 802.11 : Des services sous-couche du contrôle d'accès, des types de trames autorisés, et les règles de rapport d'état qui régissent l'échange des trames autorisés. Basé sur l'information globale de notre essai en laboratoire, nous avons récapitulé les trames et les événements appropriés qui déclenchent des alertes d'intrusion dans un format tabulaire. Une telle table peut être exploitée en manuscrits programmés d'audit dans un réseau sans fil pour détecter les intrusions d'attaques déjà documentées.

Nous avons recommandé qu'un administrateur de réseau devrait s'assurer que le WEP (ou d'autres algorithmes de couche de lien comme WPA) soit utilisé de sorte que le trafic involontaire (des couches plus élevées telles que le Protocole de Configuration Dynamique d'Hote et le Protocole de Resolution d'Addresse) soit chiffré avant d'être libéré en réseau. L'établissement d'un mur de protection pour empêcher ce trafic d'être diffusé sur un lien sans fil est également important. Nous avons également observé que le trafic était involontairement transmis des stations d'Airopeek reniflant ou surveillant le réseau sans fil. Ces trames sont habituellement sans l'Identificateur de Services de Base – ce qui n'est pas conforme au standard - et peuvent être détectées.

Quand une station non-autorisée masquerade l'Addresse du Contrôle d'Acces, l'addresse IP, et le nom d'un ordinateur autorisé, son trafic est alors indétectable. Dans un tel cas, les stations légitimes et ceux qui masqueradent sont incapables soit de passer en revue ou de transférer des dossiers en réseau, de ce fait créant un refus de service pour la station autorisée. Nous avons également exploré une approche active envers la détection d'intrusion et avons noté qu'elle n'est pas convenue à la norme 802.11.

Les signatures de menace obtenues lors de cette recherche indiquent clairement l'utilité des trames d'IEEE 802.11 et les règles de rapport d'état en aidant à la detection de certaines menaces connues envers les réseaux sans fil. Les types de trames et les champs de l'information fournissent des perspectives au sujet de la source de transmission aussi bien que de l'intention. Les règles de rapport d'état aident à la détection des situations qui enfreindrent les procédures décrites par la norme 802.11.

Salmanian, M., Leonard, S., Lefebvre, J. H., Knight, S. 2004. Intrusion Detection in 802.11 Wireless Local Area Networks. DRDC Ottawa TM 2004-120, R & D pour la défense Canada - Ottawa.

Table of contents

List of figures

List of tables

Acknowledgements

Many sincere thanks to Mr. Kellett for his comments and to Mr. Montreuil for translation of the Executive summary.

This page intentionally left blank.

1. Introduction

The flexibility, capability, and economics of wireless local area networks (WLANs) make them an attractive communication asset. They are, however, vulnerable to various types of intrusion-related attacks that can compromise the confidentiality, integrity and availability of information and resources. Before WLANs gain widespread acceptance in the Department of National Defence (DND) and Canadian Forces (CF), it is necessary to understand the nature of these attacks and to develop techniques capable of detecting and guarding against intruders in a wireless environment.

The Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard defines a widely accepted and implemented medium access control (MAC) and physical layer specification for WLANs. This standard has been criticized for inadequate and flawed security provisions that expose WLANs to a variety of security threats [1- 3] ranging from passive eavesdropping to highly intrusive masquerading. These threats have behaviours (identifiable signatures) that may be distinguishable with the attributes defined in the 802.11 MAC that also manages the wireless medium. Threat signatures derived from these attributes could be used in support of a WLAN intrusion detection system (IDS).

Sections 2 and 3 provide a brief overview of the background information supporting this area of research. Section 3 follows with a discussion of state of the art in current research activities and WLAN IDSs. Section 4 provides a detailed evaluation of the IEEE 802.11 standard from the perspective of determining information and idiosyncrasies that can be used to enhance intrusion detection in WLANs. Section 5 describes the laboratory set-up and tests conducted in order to evaluate the effectiveness of the information proposed in Section 4. Section 6 concludes this research with a discussion on the achievement of goals.

2. The Infrastructure Mode

The Infrastructure Mode, as opposed to the Ad Hoc Mode, is the mode of operation considered in this paper. In infrastructure mode, a Basic Service Set (BSS) consists of one or more wireless stations and an access point. The access points in Figure 1 provide connectivity to a wired distribution system (DS), providing the capability to send information from one BSS to another and creating an Extended Service Set (ESS) [4]. The type of connectivity depicted in Figure 1 is often used to extend a wired network to mobile users or remote networks. As a result, a WLAN can potentially provide a means by which intruders can infiltrate a wired network.

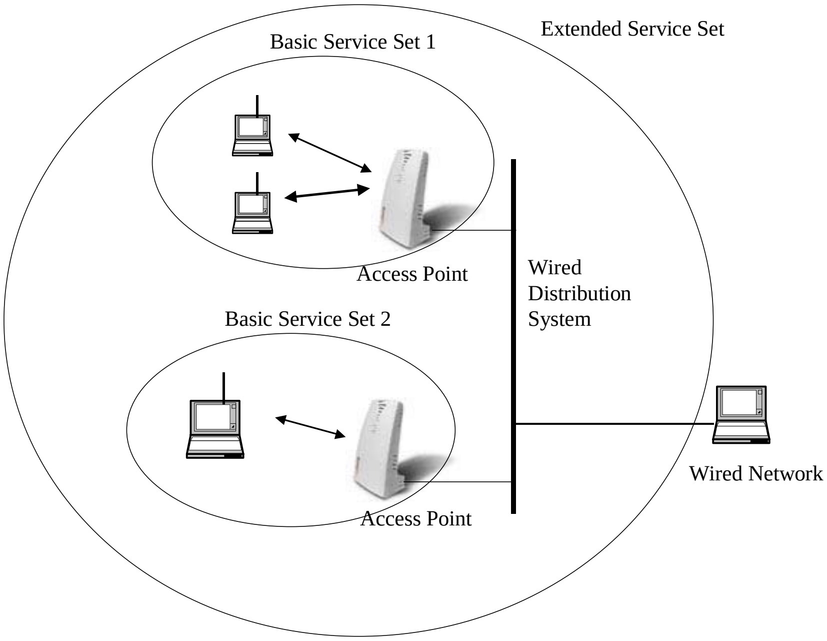

Figure 1. *Infrastructure Mode*

Before a wireless station can become part of a BSS, it must first establish an association with the access point controlling the BSS. Once the association process has been completed, the wireless station is considered part of the BSS and may utilize the distribution system of the BSS and the ESS. The association process is important in infrastructure-based 802.11 WLANs and its description will serve to identify some of the unique characteristics of these WLANs. There are three steps involved in the association process shown in Figure 2:

1. Finding the access point,

2. Authentication, and

3. Association.

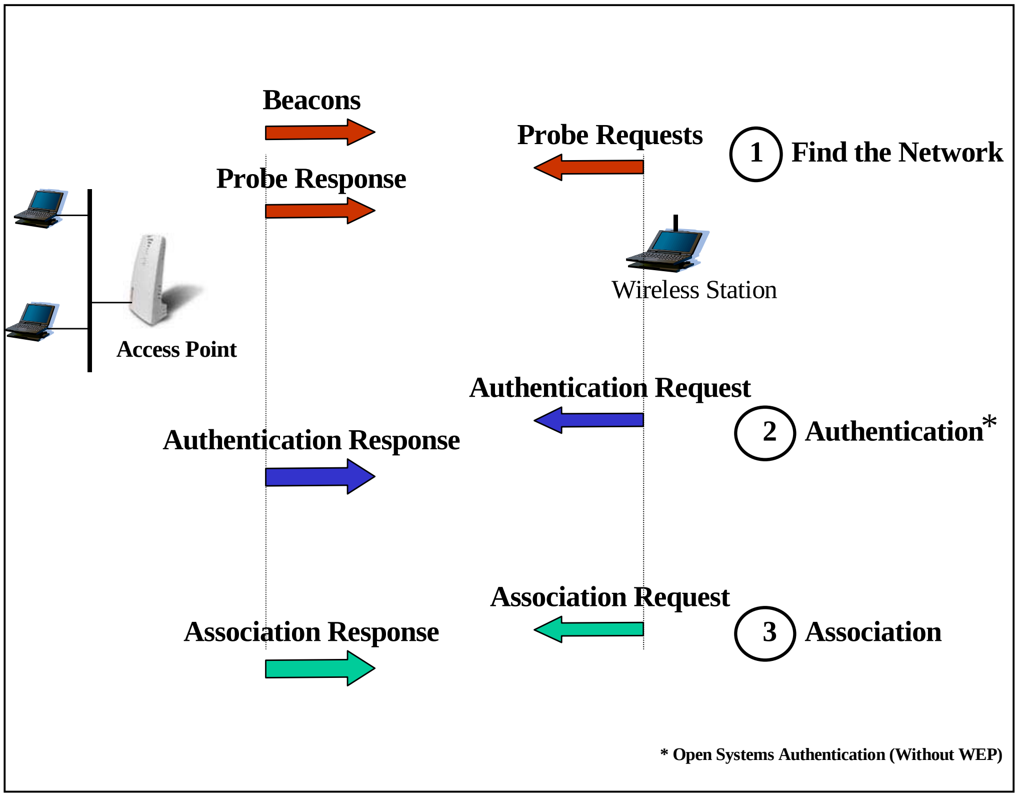

Figure 2. *Three Steps in Association Process*

There are two methods used for finding the network. The first involves the access point transmitting a Beacon frame that contains the network name - referred to as the Service Set Identifier (SSID). In the second method, wireless stations transmit a Probe Request frame that contains the SSID of the required network [5].

Once the wireless client has found the proper access point, the next step in the association process involves authentication. It is necessary for the access point to authenticate the wireless station. The wireless station initiates this step by transmitting an Authentication Request to the access point. The response from the access point depends upon the authentication scheme implemented in the WLAN.

If the authentication process is successful, the wireless station will send an Association Request to the access point and if the access point has room for additional stations, it will reply with a positive Association Response [6].

3. Intrusion Detection in WLANs

A great deal more research has been done on IDSs for wired networks than for wireless networks. There exists a requirement for intrusion detection techniques or systems that can detect threats unique to a WLAN. A wired-based IDS placed behind an access point may be successful in identifying threats to a WLAN from a connected wired LAN but it is incapable of detecting wireless threats. In addition, from the perspective of a wired network, a wireless intruder that has successfully established an association with an authorized access point is considered a legitimate member of the ESS and, potentially, a connected wired network. The additional OSI layer 2 functionality incorporated into IEEE 802.11 WLANs through the exchange of special management and control frames provides security-related indications that are not visible to an IDS functioning primarily at layer 3 and above. To provide adequate protection to an ESS, a combination of wire- and wireless-based IDSs may be required to operate together to provide overall protection.

There are a number of commercial and free packet capturing tools that could be used to support WLAN intrusion detection activities. All of these tools are capable of monitoring wireless traffic and, depending on the tool, providing a meaningful interpretation to an administrator or analyst. With increased research activity and interest in WLANs, it is anticipated that the number of WLAN security-related products will continue to rise with additional products available by the time this research is presented. The following is a selection of currently available products [7]: AirDefense [8], WildPackets AiroPeek [9], Network Associates Sniffer Wireless [10], Network Instruments Network Observer [11], Ethereal [12], and Airsnort [13].

Commercial IDS products and support tools are based on proprietary information and offer little insight into how they accomplish their advertised capabilities. The research presented here is offered as a contribution to an open-source solution to the WLAN intrusion detection problems. In this research, we identify the attributes of IEEE 802.11 that can provide threat signatures in support of a WLAN-specific intrusion detection system.

4. An Analysis of the IEEE 802.11 Protocol

The review of the 802.11 standard results in the identification of three broad categories whose information enhances intrusion detection in WLANs:

1) MAC sub-layer services,
2) Permitted frame types in an 802.11-based WLAN,
3) The state relationship rules - that govern the exchange of the permitted frames.

In evaluating the information in these categories, it is also desirable for the network to notify illegal or unauthorized activity - activity that could compromise the confidentiality, integrity, and availability of information and resources. A WLAN IDS must be capable of collecting observable or auditable events, analyzing them, and determining the intruders' cause or motive [14] by correlating the results. This report concentrates on the type of information that has sufficient value for a WLAN IDS to observe and audit.

4.1 MAC Sub-layer Services

There are nine services offered by the MAC sub-layer. These services provide the additional functionality required by the wireless architecture that is over and above that of wired Ethernet. These services relate to critical steps involved in joining and leaving a WLAN. The ability to monitor and collect tangible information in support of a security evaluation is critical to a WLAN IDS. In a WLAN, events are visible by the presence of specific wireless frames. The frame format associated to these services is listed in Figure 3. In a WLAN, potential security events are related to the following services:

1. Association
2. Re-association
3. Disassociation
4. Authentication
5. Pre-authentication - authentication with an access point in a neighbouring BSS prior to a re-association as a station moves into the new BSS
6. De-authentication
7. Distribution - the process by which frames are exchanged in an ESS
8. Integration - information interaction from a WLAN to a wired LAN
9. Privacy - the WEP[1] Protocol is implemented to provide encryption and decryption capabilities

[1] The security analysis of WEP, WPA, and other 802.11 algorithms are subjects of another DRDC Technical Memorandum that is in progress.

These services are implemented through an exchange of specific and identifiable frames as determined by the rules outlined in the 802.11 standard.

4.2 Permitted Frame Types

The 802.11 standard defines three categories of frames types permitted for exchange between wireless devices:

a) Data frames

b) Control frames

c) Management frames

One way to perform intrusion detection is to follow any abnormalities in a specific MAC sub-layer service, such as authentication, by filtering the standard message exchanges to find messages from an intruder. The messages involved in such services are generally Control and Management frames. Table 1 provides a summary of the analysis results obtained for messages of specific services. Only the frame types that are useful in the detection of certain security events are presented. The explanation of these frame types and their associated security events is presented below. This tabular summary of frame types is very important in a WLAN intrusion detection system that collects, monitors, and correlates pertinent information to alert a network administrator.

***Table 1.** Analysis Results of Permitted Frame Types*

Useful Frame Types	Security Event
Beacon frames	Useful in detecting rogue access points.
Probe Request frames	Useful in detecting rogue stations and network probing.
Authentication Request and Response frames	Useful in detecting authentication events such as failed authentication attempts.
Association Request and Response frames	Useful in detecting association events such as illegal associations and failed association attempts.
Re-association Request and Response frames	Useful in detecting re-association events such as illegal associations and failed re-association attempts.
De-authentication frames	Useful in detecting authentication events such as the voiding of an authentication relationship.
Disassociation frames	Useful in detecting association events such as the voiding of an association relationship.
Useful Frame Fields	**Comments**
Type and Sub-type fields	Useful in identifying frame types.
WEP field	Useful in identifying data frames that are not encrypted.
Address fields	Useful in identifying rogue stations and rogue access points.
Sequence Control field	Useful in detecting unauthorized frame injection.
SSID field of Beacon frames	If the SSID is identified in the Beacon frames, the access point may allow unwanted associations.

SSID field of Probe Request frames	If the SSID is blank, then the station is looking for any access point that is broadcasting its SSID. This could indicate probing activity.
Status Code field	Provides an indication of the success or failure of authentication, association, and re-association events.
Reason Code field	Provides a reason for de-authentication or disassociation events.

Another way to perform intrusion detection is to filter the contents of the frame fields for indications of an intruder. Table 1 also presents a summary of frame fields that are useful in detecting intruders. For example, the frame type/subtype (of the Frame Control Field) carries the information that associates the message to a specific MAC sub-layer service. Some of these frame types along with certain fields within the frames provide useful information for intrusion detection, as summarized in Table 1.

The Type and Subtype Fields of the **Frame Control** Field are used to indicate the specific type of frame being transmitted. This information may be used to help identify potential security-related threats. For instance, a noticeable increase in de-authentication frames indicates a potential intruder attempting to infiltrate a WLAN. The WEP sub-field of the Frame Control Field provides an indication that WEP has or has not been used to encrypt the frame body. The **Address** fields provide a means by which unauthorized stations and unauthorized access points can be identified based on the MAC addresses they contain.

The **SSID** field is the unique network name assigned to a BSS. An access point can be configured to be silent or continuously transmit its SSID using the Beacon frame type. A Beacon frame can broadcast the SSID so that wireless stations can detect the presence of the access point. If the access point is set up for such broadcasts then it will respond with its SSID to any Probe Requests that have a blank SSID field. This probing response could lead to authentication and associations with undesirable or unauthorized stations.

Since Beacon frames are, by default, automatically and continually transmitted by access points, they are useful in detecting the presence of rogue access points (i.e. an unauthorized access point security event). The source address field of Beacon frames can be used to identify foreign or unauthorized access points. Since these Beacon frames can contribute to the identification of the unauthorized access point security event, the principle that detectable security events should be observable or auditable is upheld. As a result, Beacon frames are considered useful frame types in enhancing intrusion detection in WLANs.

The Address field of the MAC header can be used to detect Probe Requests from unauthorized stations. Thus, detection of unauthorized station security events (i.e. rogue stations) is made via Probe Request frames by identifying its corresponding Address field of the MAC header. Probe Requests cycling through all available channels may indicate that a station is conducting network scanning. This sort of scanning activity is considered a security event depending on the motive or intent of the scanning station.

In infrastructure mode, the exchange of authentication, association, or re-association frames (Figure 1) is required in order for the access point to authenticate and associate wireless stations. An access point must authenticate a wireless station before association can take place. The **Status Code** field [4] can provide useful information in support of intrusion detection. For instance, failed authentication attempts due to challenge failure are reflected in the Status Code field with a value of 15 and may be useful in detecting intrusion attempts.

The frame body (see Figure 3) of De-authentication and Disassociation Frames contains a **Reason Code** field that identifies the reason for de-authentication or disassociation. These reason codes can also provide valuable insights in detecting potential intruders. Table 2 [4] lists the possible reason codes that may be used in intrusion detection. A large number of de-authentication or disassociation frames with reason codes 6, 7 or 9 may indicate attempts by an unauthorized station to infiltrate a WLAN.

Table 2. *A Subset of Reason Code Values*

Reason Code	Description
6	Class 2 frame received from non-authenticated station
7	Class 3 frame received from non-associated station
9	Station requesting association or re-association is not authenticated with responding station

These status/reason codes along with frame types and their fields provide characteristics that can be used to build signatures for intrusion detection. A visual summary of this information is presented in Figure 3.

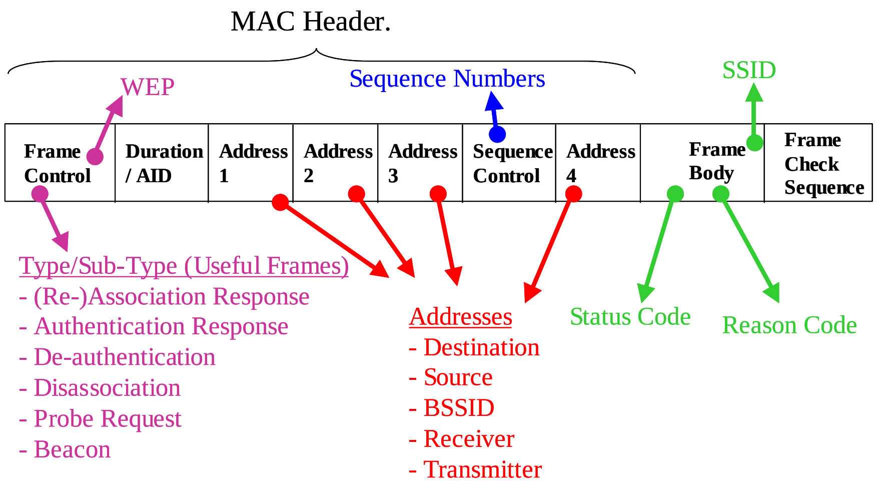

Figure 3. *Data Frame Format*

4.3 Wireless Station State Relationships

The provisions of the MAC sub-layer services described above are facilitated by the exchange of 802.11 frames and are dependent upon a state relationship that exists between wireless stations. Each wireless station maintains two state variables for each wireless station with which direct communication is required [4]. For the Infrastructure Mode of operation, direct communication is required between wireless stations and access points. The two state variables are called the Authentication State and the Association State and together they define three possible states depicted in Figure 4. The state that exists between the station and the access point determines the type of frames that may be exchanged between these stations.

State 1 is the most restrictive state in that only Class 1 frames (see Table 3) can be transmitted between stations. As the relationship escalates to State 3, with successful authentication and association, all classes of frames are permitted. Violation of this state relationship will result in the receiving station generating De-authentication or Disassociation frames [4]. These frames would include a Reason Code field that would explain the cause of the event. In a sense, a new security event exists related to the violation of the state relationship rules. This characteristic is useful in identifying the presence of unauthorized stations in the broadcast segment of an access point.

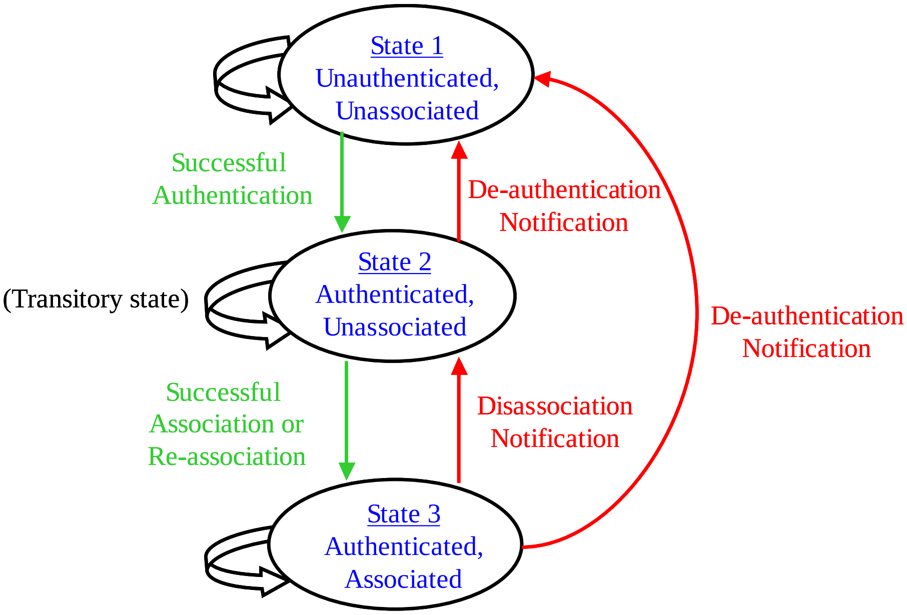

Figure 4. *State Relationships [1] [4]*

Table 3. *Classes of Frames Permitted in each State*

Class	**Frames**[2]	**Permitted in State(s)**
1	Request to Send (RTS)	**1,2,3**
	Clear to Send (CTS)	
	Acknowledgement (ACK)	
	Probe Request	
	Probe Response	
	Beacon	
	Authentication	
	De-authentication	
2	Association Request	**2,3**
	Association Response	
	Re-association Request	
	Re-association Response	
	Disassociation	
3	Power Save Poll (PS-Poll)	**3**
	Data Frames	

In addition to analyzing the potential usefulness of MAC sub-layer services, permitted frame types, and the state relationship rules for intrusion detection in WLANs, we have tested and validated their utility.

[2] Frames associated with the PCF or IBBS operation are not included.

5. Laboratory Tests and Discussions

A wireless network consisting of an access point and a wireless station was set up to determine typical behaviour patterns for each device. Another wireless station using the AiroPeek [9] WLAN protocol analyzer program was used to capture the traffic generated by the wireless station and the access point. The traffic consisted of the 3 categories of permitted 802.11 frames - namely Control, Management and Data frames. The resulting traffic from this scenario helped establish normal traffic patterns associated with typical WLAN devices. The following WLAN scenarios were used to evaluate the effectiveness of the proposed research in detecting some of the more common WLAN threats. Our observations are noted below.

5.1 Scenario 1: Normal WLAN Traffic

Both the access point and the wireless station were operated in the same broadcast segment in order to determine how these devices interact. A desktop computer was connected to the access point by an Ethernet cable in order to make the required configuration changes at the access point. It was interesting to note the number of higher layer queries (i.e. DHCP, ARP, SMB, NetBIOS Name Service) that were transmitted by the access point. These frames were broadcast throughout the BSS and could provide unintentional insights into the composition and services of the connected wired network. Network administrators should be aware of such activity and ensure that WEP, or other link layer algorithms like WPA, are enabled to ensure the encryption of any traffic before it is transmitted over the WLAN. Establishing a firewall to prevent some of this traffic from being broadcast over the wireless link is also important. On the other hand, the absence of such frames from an access point may be considered unusual and, as a result, could be used to flag changes in the normal behaviour of an access point. Such an indicator may be useful in detecting rogue access points that may not be connected to a wired network.

5.2 Scenario 2: Access Point Re-configuration

In this scenario, we observed the effect of access point re-configuration and the state relationships on a wireless station that was connecting to the access point. For States 1 and 3, using the access point’s management interface, we made the following configuration changes to look for potential re-initialization idiosyncrasies:

- turning on/off the broadcast SSID,
- turning on/off WEP,
- changing channels, and
- restarting the access point.

Configuration changes made at the access point had no effect on the State 1 station. The only interaction noted between the two State 1 devices was when the access point broadcasted the

SSID. When proper authentication is not enforced, an access point broadcasting its SSID allows any station to associate with it. Moreover, even with proper authentication enforced, an access point in broadcast mode responds to Probe Requests with blank SSIDs, whereas an access point that does not broadcast its SSID only responds to Probe Requests that contain the proper SSID. This highlights the importance of properly configuring the access point in accordance with the security goals of the WLAN. This information can be used by an IDS to generate alerts if the examination of the SSID field in Beacon frames from authorized access points determines that a valid SSID is present. The alert would warn to turn off the broadcast. With the SSID broadcast off, another alert could result from examination of blank SSID field in Probe Request frames.

We were unable to stabilize the network and freeze the station in State 2 to perform the configuration changes. The authentication and association processes are sequential by nature and happen quickly. It was difficult to authenticate a wireless station and prevent its association with the access point to keep it in State 2.

With configuration changes in State 3, the sequence of frames leading up to the association was consistent with the 802.11 standard. An associated station that was not configured with the network SSID was unable to re-establish an association if the SSID were not broadcasted by the access point. The frames following association were not defined by the standard but were related to higher layer services such as DHCP and ARP and were treated as data frames within the standard. Following the assignment of an IP address by the access point, a Ping Request was sent to the station confirming the new IP address. After the access point was restarted, the station was de-authenticated causing the association process to be repeated. When WEP was turned on, the access point voided the association relationship with the station. The station did not attempt to re-associate with the access point since it could no longer satisfy all the capability requirements (i.e. privacy) identified in the Probe Response frames. When WEP was again turned off, the station was able to successfully associate.

5.3 Scenario 3: Detecting Wireless Sniffers

The card on the wireless sniffer was configured to accept all network traffic that passed within range of the station regardless of the intended recipient. A station operating in *monitor mode* can capture frames on any channel from different networks without being associated with a particular network [13][15]. This mode of operation is unique to WLANs and may be considered an enhanced version of the *promiscuous mode* available in wired networks, which requires an association with the network [13][15].

An AiroPeek station operates in monitor mode and, in theory, should not transmit any frames since it is not associated with any network. Despite this, we observed that traffic was transmitted from the AiroPeek stations. Although the sniffing program takes over the operation of the wireless card by suppressing normal 802.11 behaviour (i.e. no Probe Requests), traffic related to higher layer services (i.e. DHCP requests) leaked out. In this case, many of the transmitted DHCP request frames made reference to reserved IP addresses and contained hostname and MAC address information. In addition, this traffic was packaged in 802.11 data frames and was broadcasted without an SSID - which is not standard compliant.

Such traffic indicates the presence of a sniffing program operating in the broadcast segment and an IDS program may exploit this.

5.4 Scenario 4: Detecting Active Probing

Wardriving is defined as roaming around scanning the airwaves to find WLANs with the aim of gathering network intelligence. In this experiment, NetStumbler was installed on a wireless station to conduct network probing. NetStumbler operates by sending out Probe Requests; this made it possible for the station with the AiroPeek program to observe this activity and capture the address of the transmitting station, as well as any patterns in traffic that could be used to detect the use of this program.

The NetStumbler program was only successful in detecting the presence of the WLAN when the access point was broadcasting the SSID in its Beacon frames. In such cases, the NetStumbler station attempted to establish an association with the access point by exploiting the lack of security defined in the 802.11 standard for networks that were broadcasting their SSID. Such networks are obliged to respond to Probe Requests that contain a blank SSID.

One of the Sub-Network Access Protocol (SNAP) frames initiated by the NetStumbler station contained a unique text string (“intentionally blank”) that could also be used to detect a version of the program. This SNAP frame from the station is designed to invoke a SNAP frame from the access point that contains the access point’s name.

5.5 Scenario 5: Detecting Spoofing and Infiltration

Spoofing, also known as masquerading, involves an intruder changing the identity of his or her wireless station to look like an authorized station of a network. Spoofing can be achieved by changing the MAC address of a wireless station to that of an authorized WLAN station. Such authorized MAC addresses can be obtained by monitoring network traffic. In addition to spoofing the MAC address, additional features can be spoofed, including the computer name and the IP address. The AiroPeek WLAN analyzer was used to look for traffic anomalies that indicated the presence of a spoofing station.

A station using only MAC address spoofing was able to associate with the access point and obtain a unique IP address. Both the spoofed and spoofing stations were able to operate concurrently in the network with the access point indicating only one association and IP address in its status window. However, it was possible to distinguish some of the traffic based on computer names.

A station spoofing both the MAC address and computer name was also able to associate with the access point. In this case, traffic between the spoofing and legitimate station could not be distinguished based solely on the computer name. However, both stations were assigned a unique IP address and the presence of such traffic could be used to indicate spoofing.

When the station spoofed the MAC and IP address and computer name, no distinction could be made between the traffic. In this case, both the legitimate and spoofing stations were unable to browse or transfer network files, creating a denial of service situation for the legitimate station. Once the legitimate station shut down, the spoofing station again had full access to network resources with no indication in network traffic that the station was not legitimate. In this case, there was no DHCP frame sent by the spoofing station to the access point following association. Since the spoofing station was using a static IP address, there was no requirement to request an IP address through the DHCP process. This skipping of the DHCP process was used to indicate the presence of a station spoofing the IP address in a DHCP-based WLAN. The only exception in the generation of a DHCP frame noted in a DHCP-based WLAN was when a station is de-authenticated or disassociated for a relatively short period. For example, when a minor configuration change is made at the access point, DHCP frames are not exchanged to request an IP address. Although not scalable, assignment of static IP addresses in a WLAN has value in exploiting the DHCP process to detect intruders.

5.6 Scenario 6: Detecting Rogue Access Points

A rogue access point is an unauthorized access point introduced into the broadcast segment of a WLAN. A rogue access point configured with the right network ID (SSID) will cause wireless stations in close proximity to attempt to associate with it since the signal strength will generally be greater.

The presence of rogue access points operating in a broadcast segment can be detected by observing the Beacon frames that all access points must transmit as defined in the 802.11 standard. The source address contained in these frames may be compared to known authorized access point addresses. This source address comparison may also be performed on association responses sent from rogue access points to authorized stations. Beacon and association response frames can provide an indication that a rogue access point is in operation.

5.7 Summary

Based on the aggregate information from our laboratory testing, we have summarized the relevant frames and events that trigger intrusion alerts. They are sorted and summarized based on related security tests in Table 4.

Table 4. *Relevant Frames and Trigger Events*

Security Tests	Relevant Frames	Trigger Event
a. Rogue Station Detection	Probe Request Frames	Probe Request frame from an unauthorized station.
b. Rogue Access Point Detection	Beacon Frames	Beacon frame from an unauthorized access point.

c. Illegal Association Detection	Association and Re-association Response Frames	Association or Re-association Response frames sent to unauthorized stations by authorized access points. Association or Re-association Response frames sent to authorized stations from unauthorized access points.
d. Sniffing Station Detection	Broadcast 802.11 Data Frames	802.11 Data frames that are broadcast without an SSID.
e. Spoofing and Infiltration Detection:		
(1) MAC Spoofing Detection	DHCP Frames following Association or Re-association Response Frames	A DHCP frame sent by a station following association or re-association that does not contain the authorized station's name.
(2) MAC and Name Spoofing Detection	Ping Request Frames from access point	A change in the IP address assigned to an authorized station as reflected in the Ping Request frame sent to the station by the access point.
(3) Static IP or IP Spoofing Detection	Association or Re-association Response Frames	The absence of a DHCP frame from a station following association or re-association, if the station has not recently been de-authenticated or disassociated.

One may suggest that instead of taking a passive approach to intrusion detection - by monitoring frame types and fields for indicators related to security events - it may be better to take a more active approach to intrusion detection. For example, if a frame could be broadcast from the access point that would actively invoke a response from a sniffing station, the response would then alert its presence. The invoking frame would violate the state relationship rules of the sniffing station, and, therefore, any mandatory response from the sniffing station could be used to detect its presence. Nevertheless, according to the 802.11 standard, such (active) messages will invoke a mandatory response only if they are sent to a unicast address; they cannot be sent to a broadcast address for active intrusion detection. Since a sniffing station would most likely be a covert one, whose address is unknown to the AP, such an active approach would most likely be ineffective. Even if the AP could successfully scan the unicast address space looking for rogue APs - a resource intensive and no doubt fruitless task given the wide range of possible unicast addresses - there is no reason that the intruder would not find some way to ignore the standard and fail to respond. Active probing requires the cooperation of the intruder and the element of surprise; it is unlikely to catch anyone who is determined to get around it.

6. Conclusion

In this research, we have observed, tested, and documented threat signatures for intrusion detection in WLANs. The signatures aid in the detection of rogue access points and unauthorized stations that attempt to invade the LAN by probing (frame injection), illegal authentication, or associations. The methodology was developed by studying and analyzing the following concepts in the 802.11 standard: MAC sub-layer services, permitted frame types, and the state relationship rules that govern the exchange of the permitted frames. Based on the aggregate information from our laboratory testing, we have summarized the relevant frames and events that trigger intrusion alerts in a tabular format. Such a table can be exploited in scheduled audit scripts in WLANs to detect intruders of documented attacks.

We have observed that during normal traffic testing many 802.11 data frames from the access point contained higher layer (i.e. DHCP, ARP, etc.) messages. A network administrator should be aware of such activity and ensure that WEP, or other link layer algorithms like WPA, are enabled so that this traffic is encrypted before being released over the WLAN. Establishing a firewall to prevent some of this traffic from being broadcast over the wireless link is also important. We also observed that traffic was unintentionally transmitted from the AiroPeek stations sniffing or monitoring the WLAN. These frames are usually transmitted without a SSID - which is not standard compliant - and may be detected.

When an unauthorized station spoofs the MAC and IP addresses, and computer name of an authorized station, its traffic is undetectable. In this case, both the legitimate and spoofing stations were unable to browse or transfer network files creating a denial of service for the authorized station. We also explored taking an active approach to intrusion detection and noted that it is not suited to the 802.11 standard.

The threat signatures obtained in this research clearly indicate the usefulness of IEEE 802.11 frames and the state relationship rules in helping to detect some of the known threats to WLANs. The frame types and information fields provide insights about the source of the transmission as well as the intent. The state relationship rules assist in the detection of situations that violate the procedures described in the 802.11 standard.

The IEEE 802.11b standard has been criticized for inadequate security provisions that have resulted in producing exploitable vulnerabilities and compromising the confidentiality, integrity, and availability of information. However, the standard also contains information that can be used to support WLAN-specific intrusion detection. The additional OSI layer 2 functionality incorporated into IEEE 802.11 WLANs, through the exchange of special management and control frames, provides security-related indications that are not visible to an IDS functioning primarily at layer 3 and above. As a result, it is necessary to incorporate special monitoring techniques capable of dealing with the uniqueness of WLANs. Although the research presented here highlights the usefulness of layer 2 and layer 3 monitoring, it is but a small sampling of the effort necessary to elevate intrusion detection capabilities to that comparable with wired networks. The development of a WLAN IDS that can be operated in conjunction with a wire-based IDS will greatly improve the overall protection and security of an ESS.

7. References

1. S. Leonard, “Intrusion Detection in Wireless Local Area Networks”, Master’s Thesis, Department of Electrical and Computer Engineering, Royal Military College of Canada, April 2003.
2. M. Sutton, “Hacking the Invisible Network”, iALERT White Paper, iDefense Labs, 10 July 2002.
3. B. Fleck, J. Dimov, “Wireless Access Points and ARP Poisoning”, Cigital Inc., 22 October 2001.
4. LAN MAN Standards Committee of the IEEE Computer Society, “ANSI/IEEE Std 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, 1999.
5. W. Arbaugh, N. Shankar, J. Wan, “Your 802.11 Wireless Network Has No Clothes”, University of Maryland, 30 March 2001.
6. S. Weatherspoon, “Overview of IEEE 802.11 Security”, Intel Technology Journal Q2, 2000.
7. P. Morrissey, D. Advani, “Sneak an Airopeek at WLAN Stats”, Network Computing, 27 May 2002.
8. AirDefense: WLAN Intrusion Protection and Management System, http://www.airdefense.net/products/index.shtm.
9. Wildpackets AiroPeek WLAN Analyzer, http://airopeek.com/products/airopeek, http://www.wildpackets.com/airopeek.
10. http://www.sniffer.com/products/sniffer-wireless
11. http://www.networkinstruments.com/
12. http://www.ethereal.com/faq.html
13. Airsnort Home Page, http://airsnort.shmoo.com .
14. D. Dobrotka, “Intrusion Detection on Wireless Network.” SANS Institute Intrusion Detection FAQ, 8 October 2002.
15. Airsnort FAQ, http://airsnort.shmoo.com/faq.html#Q3

List of symbols/abbreviations/acronyms/initialisms

ACL	Access Control List
AES	Advanced Encryption Standard
BSS	Basic Service Set
CF	Canadian Forces
COFDM	Coded Orthogonal Frequency Division Multiplexing
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
CRC	Cyclical Redundancy Check
DA	Destination Address
DCF	Distributed Coordination Function
DND	Department of National Defence
DR	Detection Rate
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
ESS	Extended Service Set
ETSI	European Telecommunications Standard Institute
FHSS	Frequency Hopping Spread Spectrum
FNR	False Negative Rate
FPR	False Positive Rate
IBSS	Independent Basic Service Set

ICV	Integrity Check Value
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IFS	Inter-frame Space
ISM	Industrial, Scientific and Medical
IV	Initialization Vector
MAC	Media Access Control
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PAN	Personal Area Network
PCF	Point Coordination Function
PLCP	Physical Layer Convergence Protocol
PMD	Physical Medium Dependent
PPK	Per Packet Key
RTS	Request to Send
SA	Source Address
SAT	Security-Auditor Tool
SNAP	Sub-Network Access Protocol
SSID	Service Set Identifier
TA	Transmitter Address
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
WECA	Wired Equivalent Compatibility Alliance
WEP	Wired Equivalent Privacy

WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

Intrusion Detection in 802.11 Wireless Local Area Networks

4. AUTHORS (Last name, first name, middle initial)

Salmanian, M., Leonard, S., Lefebvre, J. H., Knight, S.

5. DATE OF PUBLICATION (month and year of publication of document)

September 2004

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

20

6b. NO. OF REFS (total cited in document)

15

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)

5B36

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)

N/A

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC Ottawa TM 2004-120

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

N/A

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(X) Unlimited distribution
(   ) Distribution limited to defence departments and defence contractors; further distribution only as approved
(   ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
(   ) Distribution limited to government departments and agencies; further distribution only as approved
(   ) Distribution limited to defence departments; further distribution only as approved
(   ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

N/A

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

This paper presents a theoretical study of the wireless protocol defined by the IEEE 802.11 standard in order to identify characteristics or potential idiosyncrasies that could be used to enhance intrusion detection in a WLAN. The control, management, and data frames used to implement the media access control (MAC) functionality along with WLAN services and a state relationship that governs the exchange of frames between wireless stations provide useful insights into the signatures that identify security-related threats and intrusions.

The threat signatures obtained in this research clearly indicate the usefulness of IEEE 802.11 frames and the state relationship rules in helping to detect some of the known threats to WLANs. The frame types and information fields provide insights about the source of the transmission as well as the intent. The state relationship rules assist in the detection of situations that violate the procedures described in the 802.11 standard.

A number of common security-related threats are discussed and evaluated in experiments. The characteristics of the IEEE 802.11 standard are exploited to derive signatures for these threats in supporting intrusion detection in a WLAN.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

WLAN, 802.11, IDS, intrusion detection system