Wi-net: Model based hypothesis on secure packet classification and prevention of jammers

R. Baskarane[1], A.Akila[2]
[1]Head of the department (cse), Christ College of Engineering and Technology, Pondicherry.
Mobile: 9443657917
[2]Final year M.Tech (cse), Christ College of Engineering and Technology, Pondicherry.
Mobile: 9566952455.

ABSTRACT

The wireless network (wi-net) abscond it vulnerable to its intentional attacks, mainly called as jamming attack. The intentional attack can be of Denial of service attack on the network. This paper addresses the problem of selective jamming attack in wireless network. Different model assumptions are used to make the wireless network to be an efficient model and consist of different wireless network via wireless links. The security of network has several issues related to the wireless medium; network can be made secured by using several network security basics such as firewall, sniffers and routers. Packet classification is the process of data flow in the network router. Adversary can classify packet in real time before the transmission completed. Ability of the adversary in classifying a packet *m* depends on the implementation of encoder, interleaver and modulator and vice versa. Finally the different model assumptions are made, the concept of jamming attack, network security basics and real time packet classification.

Keywords: wi-net, jamming attack, security issues, real time packet classification.

INTRODUCTION

Wireless network built upon a shared medium that makes it easy for adversaries to conduct radio interference, or jamming, attacks that effectively cause a denial of service of either transmission or reception functionalities. Attacks can easily be accomplished by an adversary by either bypassing MAC-layer protocols or by emitting a radio signal targeted at jamming an exact channel.

In this paper the different jamming attacks that are be employed against a network. An attention to the challenges associated with detecting jamming. To cope with jamming, two dissimilar but complementary approaches are focused. One approach is to just retreat from the interferer, which may be accomplished by any spectral evasion (channel surfing) or spatial evasion (spatial retreats). The next approach is to compete more actively with the interferer by adjusting resources, such as power levels and communication coding, to achieve communication in the presence of the jammer.

The process of categorizing the packets into “flows” in an Internet router is called packet classification. All packets belonging to the same flow follow a predefined rule and are processed in a parallel manner by the router. Packet classification is wanted for non best-effort services, such as firewalls and quality of service, services that need the capability to differentiate and isolate traffic in dissimilar flows for suitable processing. There are different services such as packet filtering, policy routing, and accounting and billing, traffic rate limiting, traffic shaping etc. Packet classification can be done on a distinct field or on several fields. For example, all packets with the same starting place and target IP addresses may be defined to form a flow [1].

Packet classification is an essential function in firewalls, intrusion detection mechanisms and monitoring architectures. Network elements assuming this technique operate on packet flow to cover access control. A huge variety of multi-fields packet classification technique were reported in literature but it remains not easy to find a packet classification solution that represent a good tradeoff between classification times, fast updates, memory requirements and scalability to huge cumulative database[2].

There are several reasons for some network to get mistreated by viruses, malware, worms and other security threats. Most general reasons for such security attacks in miniature sized companies are not using appropriate, certified versions of Antivirus software. And of course using dangerous sites also download hazardous malware when network is not appropriately secured, which infects the whole network.

When some network uses non authentic, non licensed or fractured versions of antivirus and comparable software, they do not update the latest virus signature file to defend the system till date. When new viruses are launched, this software doesn’t have most recent viruses threats defined in their signature files, hence it exposes the complete network to these virus threats, and more frequently or may not network does get infected.

MODEL ASSUMPTION

a) Adversary Model

An algorithm calculates its competitiveness against different adversary models. For deterministic algorithms, the adversary is the similar, the adaptive offline adversary. For randomized online algorithms competitiveness can depend upon the adversary model used.

The three common adversaries are the unaware adversary, the adaptive online adversary, and the adaptive offline adversary.

The unaware adversary is sometimes referred to as the feeble adversary. This adversary knows the algorithm's code, but does not get to know the randomized outcome of the algorithm.

The adaptive online adversary is sometimes called the average adversary. This adversary must make its individual judgment before it is allowed to know the judgment of the algorithm.

The adaptive offline adversary is sometimes called the burly adversary. This adversary knows everything, even the random number generator. This adversary is so strong that randomization does not help against him.

b) Network Model

Nodes may communicate directly if they are within the range and indirectly via multi-hops. Nodes can communicate with different modes.

Unicast is the term used to describe communication where a piece of information is sent from one point to another.

Broadcast is the term used to describe communication where a piece of information is sent from one point to all other points. For encrypting broadcast message, symmetric keys are shared among the receivers.

Multicast is the term used to describe communication where a piece of information is sent from one or more points to a set of other points.

c) Communication Model

Spread spectrum is used to transmit the signal which occupies minimum number of bandwidth to send information. The main advantage of using spread spectrum is anti-jamming, message privacy. To protect wireless transmission from jamming spread spectrum uses several techniques.

Direct sequence spread spectrum is frequently used spread spectrum and simple to understand. Direct sequence modulation is done by modulating the carrier wave with digital sequence that has a bit ranges higher than that of the message to be sent.

Frequency hopping spread spectrum is an arguably better among the family of spread spectrum. Frequency hopping is more complex than direct sequence system. A frequency hopping system is to retune the transmitting carrier frequency to a pseudo randomly determined frequency value. In this way it keeps on popping up a different frequency in pseudo random pattern.

NETWORK SECURITY BASICS

a) Network traffic

Network traffic control is the process of supervising, prioritizing, scheming or sinking the network traffic, particularly Internet bandwidth, used by network administrators, to shrink congestion, latency and packet loss. This is part of bandwidth management. In order to use these tools successfully, it is essential to measure the network traffic to decide the causes of network congestion and attack problem particularly.

b) DDoS attacks

Denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make network resource unavailable to its intended users. The means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the efforts of one or more people to indefinitely interrupt or suspend services of a host connected to the Internet.

c) Intrusion detection system

An intrusion detection system (IDS) is a device or software applications that monitors system behavior for malicious activity or policy violations and produces information to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and coverage attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting obtainable threats, and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.

NEED FOR NETWORK SECURITY

Network security is flattering more and more essential as people use up more and more time connected. Compromising network security is frequently much easier than compromising physical or local security, and is much more general.

- Increasing online communication

- Personal and responsive information shared over network.

a) Authentication

Authentication is the process of shaping whether someone or something is, in fact, who or what it is declared to be. In confidential and communal computer networks (including the Internet), authentication is normally done through the use of logon passwords. Knowledge of the password is assumed to assurance that the user is genuine. Each user registers originally, using an assigned or self-declared password. On each succeeding use, the user must know and use the existing password. The disadvantage in this system for transactions that are important (such as the exchange of money) is that passwords can often be stolen, by chance revealed, or forgotten.

b) Authorization

Authorization is the procedure of giving someone agreement to do or have something. In multi-user computer systems, a system administrator defines for the system which users are permitted access to the system and what constitutional rights of use. Assuming that someone has logged in to a system, the system may desire to recognize what resources the user can be given during this session. Thus, authorization is sometimes seen as both the preliminary setting up of permissions by a system administrator and the actual checking of the permission values that have been set up when a user is getting right to use.

c) Authentication vs. Authorization

It is easy to mystify the method of authentication with that of authorization. In many host-based systems, the two mechanisms are performed by the similar physical hardware and, in some cases, the identical software.

Authentication is the mechanism whereby systems may firmly recognize their users. An authentication system may be as easy (and insecure) as a plain-text password demanding system or as complicated as the Kerberos system described elsewhere in these documents. In all cases, however, authentication systems depend on some exclusive bit of information known only to the entity being authenticated and the authentication system -- a shared secret. Such information may be a classical password, some physical property of the individual (fingerprint, retinal vascularization pattern, etc.), or some derived data. In order to confirm the identity of a user, the authenticating system classically challenges the user to give his exclusive information (his password, fingerprint, etc.) -- if the authenticating system can prove that the shared secret was presented suitably, the user is considered authenticated.

Authorization, by contrast, is the method by which a system determines what level of contact a particular authenticated user should have to protect resources prohibited by the system. For example, a database management system might be intended so as to provide certain specified individuals with the capability to recover information from a database but not the ability to modify data stored in the database, while giving other individuals the ability to change data.

Authentication and authorization are somewhat tightly-coupled method authorization systems depend on protected authentication systems to make sure that users are who they maintain to be and thus prevent unauthorized users from gaining admittance to secured resources.

MEASUREMENT METHODS

a) Passive versus Active Measurement

The passive approach uses several strategies to monitor the traffic as it passes by. These devices can be extraordinary purpose devices such as a Sniffer, or they can be build into other devices such as routers, switches or end node hosts. Examples of such build in techniques include Remote Monitoring (RMON), Simple Network Monitoring Protocol (SNMP) and net flow competent devices. The passive monitoring devices are polled occasionally and information is collected to review network performance and status.

The passive approach does not expand the traffic on the network for the measurements. It also measures real traffic. However, the polling necessary to gather the data and the traps and alarms all produce network traffic, which can be considerable. Further the amount of data gathered can be considerable particularly if one is doing flow analysis or trying to capture information on all packets.

The active approach provides clear control on the making of packets for measurement scenarios. This includes manage on the nature of traffic making, the example techniques, the timing, frequency, scheduling, packet sizes and types, numerical quality, the path and function chosen to be monitored. Being active implies testing what you want, when you need it. Emulation of scenarios is uncomplicated and checking if Quality of Service (QoS) or Service Level Agreements (SLAs) are met is comparatively simple.

b) LAN versus WAN Measurement

The terms Local Area Network (LAN) is a universal explanation of geographic size of the network and to some amount, the protocols in use. The short form LAN tends to be used to submit to a network that encompasses a distinct room or a building at distances calculated in meters. A LAN is most often used to attach computer workstations and servers. Physical Layer protocols that are high speed and broadcast across short distances are used in LANs. Examples of LAN are: ethernet, fast, Wi-Fi.

The short form WAN is used to refer to networks straddling much areas larger than a LAN does and often include circuits provided by a telecommunications mover or a private leased line. Protocols that can broadcast across longer distances measured in kilometers are used to build WANs. Examples of Physical Layer protocols used to build WANs include: X.25, Frame Relay.

JAMMING ATTACKS

There are several dissimilar attack strategies that an opponent can use to jam wireless communications. While it is unreasonable to cover all the potential attack models that might continue to exist, in this paper an analysis is made on a wide range of jammers that have reputable to be effective.

a) Constant jammer

The constant jammer repeatedly emits a radio signal, and can be implemented using a waveform creator that continuously sends a radio signal [7] or a ordinary wireless device that incessantly sends out arbitrary bits to the channel without following any MAC-layer in a good manners [4].

Normally, the fundamental MAC protocol allows rightful nodes to send out packets only if the channel is inactive. Thus, a constant jammer can efficiently prevent justifiable traffic sources from getting grip of a channel and sending packets.

b) Deceptive jammer

Instead of sending out arbitrary bits, the deceptive jammer continually injects standard packets to the channel without any slit between successive packet transmissions. As a result, a normal communicator will be deceived into believing there is a justifiable packet and be duped to stay behind in the accept state. For example, in Tiny OS, if a foreword is detected, a node remains in the accept mode, regardless of whether that node has a packet to send or not. Even if a node has packets to send, it cannot control to the send state because a constant tributary of incoming packets will be detected.

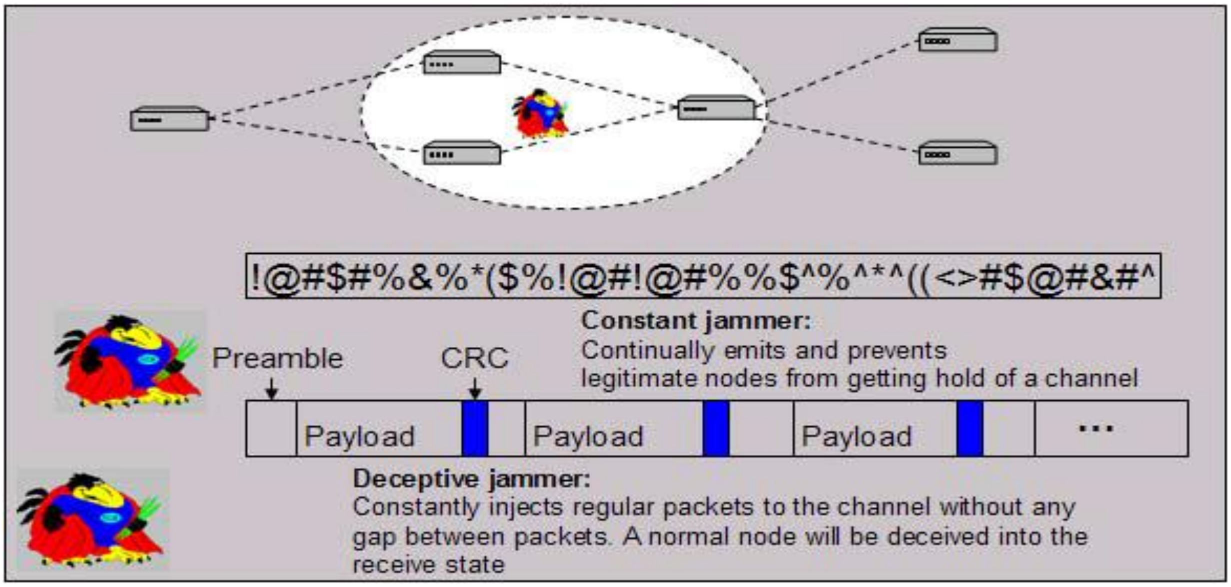
!@#$#%&%*($%!@#!@#%%$^%^*^((<>#$@#&#^
Constant jammer:
Continually emits and prevents legitimate nodes from getting hold of a channel
Preamble
CRC
Payload
Payload
Payload
...
Deceptive jammer:
Constantly injects regular packets to the channel without any gap between packets. A normal node will be deceived into the receive state

Fig.1. Constant and Deceptive jammers (Referred from 5).

c) Random jammer

Instead of constantly transferring out a radio signal, a random jammer alternates between resting and jamming. Particularly, following jamming for a while, it turns off its radio and enters a "resting" mode. It will carry on jamming after resting for some time. During its jamming phase, it can perform like either a constant jammer or a deceptive jammer. This jammer model tries to take energy protection into deliberation, which is particularly important for those jammers that do not have infinite power supply.

d) Reactive jammer

The three models discussed above are active jammers in the sense that they challenge to block the channel irrespective of the traffic pattern on the channel. Active jammers are frequently effective because they keep the channel active all the time. In the following section, these methods are comparatively simple to detect. A different approach to jamming wireless communication is to make use of a reactive strategy. The reactive jammer stays quiet when the channel is inactive, but starts transmitting a radio signal as soon as it senses activity on the channel. One advantage of a jammer is that it is harder to detect.

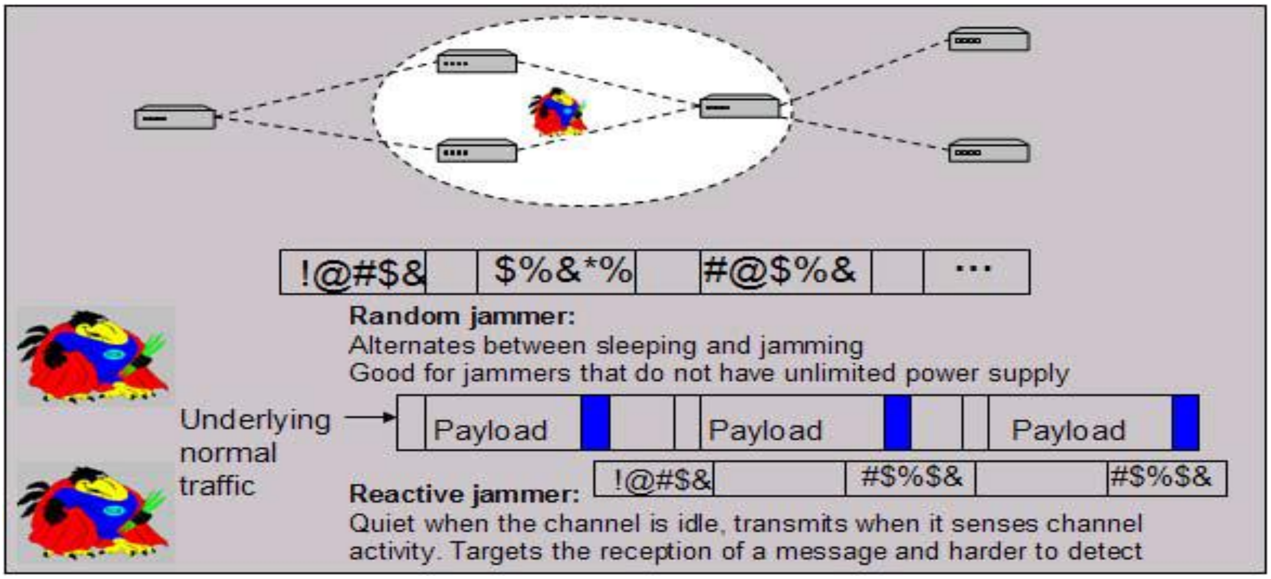
!@#$&
$%&*%
#@$%&
...
Random jammer:
Alternates between sleeping and jamming
Good for jammers that do not have unlimited power supply
Underlying normal traffic
Payload
Payload
Payload
Reactive jammer:
!@#$&
#$%$&
#$%$&
Quiet when the channel is idle, transmits when it senses channel activity. Targets the reception of a message and harder to detect

Fig.2. Random and Reactive jammers (Referred from 5)

REAL TIME PACKET CLASSIFICATION

There are a number of network services that have need of packet classification, such as routing, admittance control in firewalls; policy- based routing, condition of differentiated behavior of service, and traffic billing. In each case, it is essential to establish which flow an incoming packet belongs to so as to establish — for example — whether to promote or filter it, where to promote it to, what class of service it should obtain, or how much should be charged for transporting it. The classification function is performed by a flow classifier (also called a packet classifier) which maintains a set of rules, where each flow obeys at least one rule. The rules classify which flow a packet belongs to based on the contents of the packet header(s). For example, a flow could be distinct by particular standards of source and destination IP addresses, and by particular transport port numbers. Or a flow could be basically defined by a destination prefix and a range of port values. A number of dissimilar types of rules are used in practice. This paper describes a method for fast packet classification based on an almost arbitrary set of rules. Here it focuses only on the problem of identifying the class to which a packet belongs.

The mainly well-known form of packet classification is used to route IP data grams. In this case, all the packets intended to the set of addresses described by an ordinary prefix may be considered to be part of the same flow. Upon arrival to a router, the header of each packet is examined to decide the Network-layer destination address, which identifies the flow to which the packet belongs. Until newly, longest-prefix corresponding for routing lookups could not be done at high speeds. Now that several fast steering lookup algorithms have been developed awareness has turned to the more common problem of packet classification.

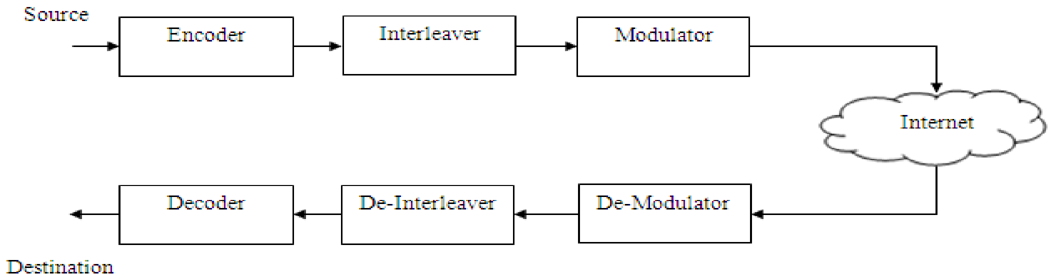

Fig.3. Generic communication system diagram

CONCLUSION

In the wireless network though the raising technology factors are tremendously increasing the solutions are observed and monitored. There are also some issues related to jamming attacks are mainly addressed. Considerably an assumption is made based on the models in which the jammer takes responsibility over the network. The network services are used to make the network more secure and prevent the packets from jamming attacks. Network security is used to prevent and monitor unauthorized access, misuse adopted by network administrator. Different measurement methods are deployed to measure the network traffic in wireless medium. The jammer inject standard packet to the channel without slit between packet transmissions over the wireless communication network.

REFERENCES

[1]. “Algorithms for Packet Classification” Pankaj Gupta and Nick McKeown, Stanford University.

[2]. “A two-level packet classification” Ons Jelassi, Olivier Paul INT, National Institute of Telecommunication Evry, France.

[3]. “Packet Classification using Hierarchical Intelligent Cuttings” Pankaj Gupta and Nick McKeown Computer Systems Laboratory, Stanford University

[4]. W. Xu et al., “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,” MobiHoc ’05: Proc. 6th ACM Int’l. Symp. Mobile Ad Hoc Net and Comp., 2005, pp. 46–57.

[5]. “A Survey on Jamming Attacks and Countermeasures in WSNs” ieee communications surveys & tutorials, vol. 11, no. 4, fourth quarter 2009.

[6]. “Packet Classification on Multiple Fields” Pankaj Gupta and Nick McKeown Computer Systems Laboratory, Stanford University

[7]. W. Xu et al., “Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service,” Proc. 2004 ACM Wksp. Wireless Security, 2004, pp. 80–89.