Study and Detection of Jamming attacks in Wireless Networks

Dr. Tejinderpal Singh Brar
Head and Associate Professor, Dept. of Computer Applications
Chandigarh Group of Colleges, Landran

Abstract--**The growing popularity of the 802.11-based Wireless LAN (WLAN) also increases its risk of security attacks. The new WLAN security standard, 802.11i, addresses most issues on user authentication and data encryption; however, it does not protect WLANs against Denial of Service (DoS) attacks. This paper presents a solution to detect and resolve Selective Jamming Attacks. To prevent these attacks various cryptographic schemes are implemented. The main goal of these systems is to prevent the preserved information at the wireless physical layer and allowed the safe transmission among communicated nodes although the jammer is present. We developed an experimental framework to demonstrate and quantify attacks against TCP and wireless Voice over IP (WVoIP) communications. Our study shows that such attacks can be easily launched, and cause service disruption.**

1. INTRODUCTION

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) 1 are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSs have become a necessary addition to the security infrastructure of nearly every organization. IDPSs typically record information related to observed events, notify security administrators of important observed events, and produce reports. Many IDPSs can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack's content. This publication describes the characteristics of IDPS technologies and provides recommendations for designing, implementing, configuring, securing, monitoring, and maintaining them.

The types of IDPS technologies are differentiated primarily by the types of events that they monitor and the ways in which they are deployed. Therefore, it is important for them to value the improvements brought by these new devices. In the same way, for the network and systems administrators, it would be interesting to assess the IDS/IPS to be able to choose the best before installing it on their networks or systems, but also to continue to evaluate its efficiency in operational method. Unfortunately, many false positives and false negatives persist in the new versions of the IDS/IPS, then, they brought improvements are not worthy of the continuous efforts of research and development in the domain of the detection and the prevention of

intrusion. In general, it is essentially due to the absence of efficient methods of assessment of the security tools, and of the IDS/IPS in particular.

2. TYPES OF INTRUSION DETECTION SYSTEMS

Several types of IDS technologies exist due to the variance of network configurations. Each type has advantages and disadvantage in detection, configuration, and cost. Mainly, there are three important distinct families of IDS: The types of IDPS technologies are differentiated primarily by the types of events that they monitor and the ways in which they are deployed.

2.1 Network-Based

A Network Intrusion Detection System (NIDS) is one common type of IDS that analyzes network traffic at all layers of the Open Systems Interconnection (OSI) model and makes decisions about the purpose of the traffic, analyzing for suspicious activity. Most NIDSs are easy to deploy on a network and can often view traffic from many systems at once. A term becoming more widely used by vendors is "Wireless Intrusion Prevention System" (WIPS) to describe a network device that monitors and analyzes the wireless radio spectrum in a network for intrusions and performs countermeasures which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity. It can identify many different types of events of interest.

It is most commonly deployed at a boundary between networks, such as in proximity to border firewalls or routers, virtual private network (VPN) servers, remote access servers, and wireless networks. The NIDS are also called passive IDS since this kind of systems inform the administrator system that an attack has or had taken place, and it takes the adequate measures to assure the security of the system. The aim is to inform about an intrusion in order to look for the IDS capable to react in the post. Report of the damages is not sufficient. It is necessary that the IDS react and to be able to block the detected doubtful traffics. These reaction techniques imply the active IDS.

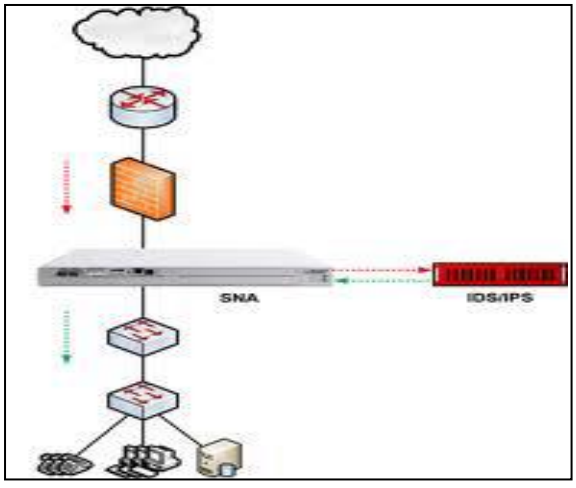

Figure 1: Location of IDS/IPS

According to the source of the data to examine, the Host Based Intrusion Detection System can be classified in two categories:

- The HIDS Based Application. The IDS of this type receive the data in application, for example, the logs files generated by the management software of the database, the server web or the firewalls. The vulnerability of this technique lies in the layer application.
- The HIDS Based Host. The IDS of this type receive the information of the activity of the supervised system. This information is sometimes in the form of audit traces of the operating system. It can also include the logs system of other logs generated by the processes of the operating system and the contents of the object system not reflected in the standard audit of the operating system and the mechanisms of logging. These types of IDS can also use the results returned by another IDS of the Based Application type.

Host-based intrusion detection systems (HIDS) analyze network traffic and system-specific settings such as software calls, local security policy, local log audits, and more. A HIDS must be installed on each machine and requires configuration specific to that operating system and software.

Host-Based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity. Examples of the types of characteristics a host-based IDPS might monitor are network traffic (only for that host), system logs, running processes, application activity, file access and modification, and system and application configuration changes. Host-based IDPSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

2.2 Network Behavior Anomaly Detection

Network behavior anomaly detection (NBAD) views traffic on network segments to determine if anomalies exist in the amount or type of traffic. Segments that usually see very little traffic or segments that see only a particular type of traffic may transform the amount or type of traffic if an unwanted event occurs. NBAD requires several sensors to create a good snapshot of a network and requires benchmarking and baselining to determine the nominal amount of a segment's traffic. The NIDS-HIDS combination or the so called hybrid gathers the features of several different IDS. It allows, in only one single tool, to supervise the network and the terminals. The probes are placed in strategic points, and act like NIDS and/or HIDS according to their sites. All these probes carry up the alerts then to a machine which centralize them all, and aggregate the information of multiple origins.

2.3 Wireless

A wireless local area network (WLAN) IDS is similar to NIDS in that it can analyze network traffic. However, it will also analyze wireless-specific traffic, including scanning for external users trying to connect to access points (AP), rogue APs, users outside the physical area of the company, and WLAN IDSs built into APs. As networks increasingly support wireless technologies at various points of a topology, WLAN IDS will play larger roles in security. Many

previous NIDS tools will include enhancements to support wireless traffic analysis. Some forms of IDPS are more mature than others because they have been in use much longer. Networkbased IDPS and some forms of host-based IDPS have been commercially available for over ten years. Network behavior analysis software is a somewhat newer form of IDPS that evolved in part from products created primarily to detect DDoS attacks, and in part from products developed to monitor traffic flows on internal networks. Wireless technologies are a relatively new type of IDPS, developed in response to the popularity of wireless local area networks (WLAN) and the growing threats against WLANs and WLAN clients.

3. WIRELESS ATTACKS

3.1 Cipher attacks:

Cipher attack is an attack model in cryptanalysis. In cipher attack, cryptanalyst gathers information data that is exchanged between two parties and decrypts the gathered data under an unknown key. Some of the cipher attacks are:

3.2 WEP attacks:

Wired Equivalent Privacy (WEP) is relatively trivial to defeat. There exist numerous attacks with WEP. It is first level of security, build into any wireless device. WEP security enabled devices works on the Wired Equivalent Privacy (WEP) algorithm. This WEP algorithm is designed and used to overcome the most security threats. The recipient with correct WEP address is the only one can decrypt information. Basically, this algorithm is designed to prevent unauthorized access on wireless networks. There are some security threats with this WEP, they are easy access, rouge access points, data tampering, masquerading. WEP algorithm has been broken for more than 10 years. So, this should not be used for securing our wireless networks.

3.3 WPA-PSK dictionary attack:

WPA stands for Wi-Fi Protected Access, is the security protocol and security certification program developed by the Wi-Fi Alliance. This WPA also prone to many security problems. The weak point in WPA PSK is its passphrase. Users often choose to configure short passphrase, dictionary based passphrases leaving them vulnerable to attack. Attackers can capture the packets on air during the key exchange of a client for joining the wireless network. Then performing the offline dictionary attack on the passphrase.

3.4 WPA/TKIP:

TKIP protocol was designed by the IEEE 802.11i task group and Wi-Fi Alliance as to replace the WPA without requiring the replacement of legacy hardware. TKIP is not considered as secure and deprecated in the 2012 revision of 802.11 standards. The TKIP attacks works in a similar way to WEP chopchop attack and can provide the clear text but doesn't expose the key. This attack severe can be reduced with a short keying time of 120 seconds or less. However, WPA2/AES would be the recommended solution. And it is recommended that sites can use a more robust authentication mechanism such as EAP/TTLS, PEAP, etc.

4. DETECTION TYPES

4.1 Signature-Based Detection

An IDS can use signature-based detection, relying on known traffic data to analyze potentially unwanted traffic. This type of detection is very fast and easy to configure. However, an attacker can slightly modify an attack to render it undetectable by a signature based IDS. Still, signature-based detection, although limited in its detection capability, can be very accurate.

4.2 Anomaly-Based Detection

An IDS that looks at network traffic and detects data that is incorrect, not valid, or generally abnormal is called anomaly based detection. This method is useful for detecting unwanted traffic that is not specifically known. For instance, anomaly based IDS will detect that an Internet protocol (IP) packet is malformed. It does not detect that it is malformed in a specific way, but indicates that it is anomalous.

4.3 Stateful Protocol Inspection

Stateful protocol inspection is similar to anomaly based detection, but it can also analyze traffic at the network and transport layer and vender-specific traffic at the application layer, which anomaly-based detection cannot do. False Positives and Negatives It is impossible for an IDS to be perfect, primarily because network traffic is so complicated. The erroneous results in an IDS are divided into two types: false positives and false negatives. False positives occur when the IDS erroneously detects a problem with benign traffic. False negatives occur when unwanted traffic is undetected by the IDS. Both create problems for security administrators and may require that the system be calibrated. A greater number of false positives are generally more acceptable but can burden a security administrator with cumbersome amounts of data to sift through. However, because it is undetected, false negatives do not afford a security administrator an opportunity to review the data.

IDPSs cannot provide completely accurate detection; they all generate false positives (incorrectly identifying benign activity as malicious) and false negatives (failing to identify malicious activity). Many organizations choose to tune IDPSs so that false negatives are decreased and false positives increased, which necessitates additional analysis resources to differentiate false positives from true malicious events. Most IDPSs also offer features that compensate for the use of common evasion techniques, which modify the format or timing of malicious activity to alter its appearance but not its effect, to attempt to avoid detection by IDPSs. Most IDPSs use multiple detection methodologies, either separately or integrated, to provide more broad and accurate detection. The primary classes of detection methodologies are as follows:

Signature-based, which compares known threat signatures to observed events to identify incidents. This is very effective at detecting known threats but largely ineffective at detecting unknown threats and many variants on known threats. Signature-based detection cannot track and understand the state of complex communications, so it cannot detect most attacks that comprise multiple events.

Anomaly-based detection, which compares definitions of what activity, is considered normal against observed events to identify significant deviations. This method uses profiles that are developed by monitoring the characteristics of typical activity over a period of time. The IDPS then compares the characteristics of current activity to thresholds related to the profile. Anomaly-based detection methods can be very effective at detecting previously unknown threats. Common problems with anomaly-based detection are inadvertently including malicious activity within a profile, establishing profiles that are not sufficiently complex to reflect real-world computing activity, and generating many false positives.

Stateful protocol analysis, which compares predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Unlike anomaly-based detection, which uses host or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. It is capable of understanding and tracking the state of protocols that have a notion of state, which allows it to detect many attacks that other methods cannot. Problems with stateful protocol analysis include that it is often very difficult or impossible to develop completely accurate models of protocols, it is very resource-intensive, and it cannot detect attacks that do not violate the characteristics of generally acceptable protocol behavior.

5. INTRUSION PREVENTION SYSTEM

The intrusion prevention is an amalgam of security technologies. Its goal is to anticipate and to stop the attacks [2]. The intrusion prevention is applied by some recent IDS. Instead of analyzing the traffic logs, which lies in discovering the attacks after they took place, the intrusion prevention tries to warn against such attacks. While the systems of intrusion detection try to give the alert, the intrusion prevention systems block the traffic rated dangerous. Over many years, the philosophy of the intrusions detection on the network amounted to detect as many as possible of attacks and possible intrusions and to consign them so that others take the necessary measures. On the contrary, the systems of prevention of the intrusions on the network have been developed in a new philosophy "taking the necessary measures to counter attacks or detectable intrusions with precision ".

In general terms, the IPS are always online on the network to supervise the traffic and intervene actively by limiting or deleting the traffic judged hostile by interrupting the suspected sessions or by taking other reaction measures to an attack or an intrusion. The IPS functions symmetrically to the IDS; in addition to that, they analyze the connection contexts, automatize the logs analysis and suspend the suspected connections. Contrary to the classic IDS, the signature is not used to detect the attacks. Before taking action, The IDS must make a decision about an action in an appropriate time. If the action is in conformity with the rules, the permission to execute it will be granted and the action will be executed. But if the action is illegal an alarm is issued. In most cases, the other detectors of the network will be informed with the goal to stop the other computers from opening or executing specific files.

Unlike the other prevention techniques, the IPS is a relatively new technique. It is based on the principle of integrating the heterogeneous technologies: firebreak, VPN, IDS, anti-virus, anti-

Spam, etc. Although the detection portion of an IDS is the most complicated, the IDS goal is to make the network more secure, and the prevention portion of the IDS must accomplish that effort. After malicious or unwanted traffic is identified, using prevention techniques can stop it. When an IDS is placed in an inline configuration, all traffic must travel through an IDS sensor. When traffic is determined to be unwanted, the IDS do not forward the traffic to the remainder of the network. To be effective, however, this effort requires that all traffic pass through the sensor. When an IDS is not configured in an inline configuration, it must end the malicious session by sending a reset packet to the network. Sometimes the attack can happen before the IDS can reset the connection. In addition, the action of ending connections works only on TCP, not on UDP or internet control message protocol (ICMP) connections. A more sophisticated approach to IPS is to reconfigure network devices (e.g., firewalls, switches, and routers) to react to the traffic. Virtual local area networks (VLAN) can be configured to quarantine traffic and limit its connections to other resources. The IPS allows the following functionalities [8]:

- Supervising the behaviour of the application
- Creating rules for the application
- Issuing alerts in case of violations
- Correlating different sensors to guarantee a better

Protection against the attacks.

- Understanding of the IP networks
- Having mastery over the network probes and the logs analysis
- Defending the vital functions of the network carrying out an analysis with high velocity.

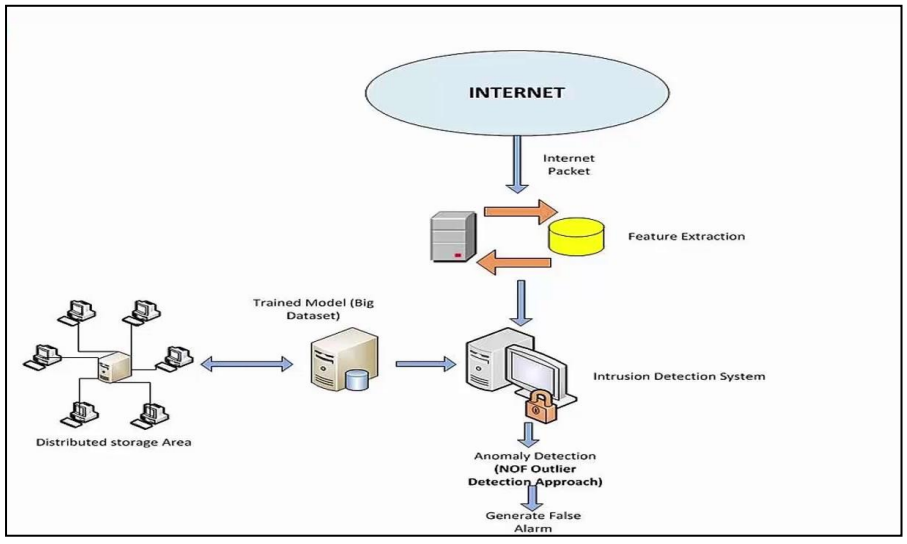

Figure 2: Intrusion Detection Systems

6. Implementation

Proposed system uses Network Simulator 2.34 tool in which front end is tcl and back end is c++. Here two protocols are used. TCP protocol is used for establishing reliable connection and AODV routing protocol is used for finding routing path for data packets. The RTS/CTS mechanism enabled at MAC layer. The transmission rate is 11Mbps for every link. The continuous, random, targeted RREQ these jammers are kept between the communicated pairs. But due to flooding feature of AODV the random jammer fails in disturbing route path.

- Implementation of wireless node in NS-2 with AODV.
- Implementation of jamming attack with selective transmission.
- Implementation of packet classification for wireless traffic.
- Implementation of packet hiding for real packet.
- Detection of jamming attack and analysis with throughput.

7. Results

The result is generated in terms of various graphs PSR, PDR, Jamming probability versus number of packets jammed and jamming probability versus throughput. PSR graph is linear, now due to jamming attack is implemented as ddos.o in Makefile.in as configured. The PDR graph is non-linear. Now when we are performing classification of the real packets from jammed packet at that time we are calculating the number of packets jammed and the throughput of the proposed system which is decreases due to attack from the jammer. At the last step we are hiding the real packets by using cryptographic schemes such as Hash based encryption and DES algorithm. In hash based encryption we are sending the packet or message in encrypted format with hash based value that is pre-shared before actual communication starts and at the receiver side the message is decrypted with the help of hashing value. In DES algorithm at the sender side input is given as plain text and 64 bit key from that the cipher text of 64 bit block is generated. Now at the receiver side DES decryption consists of the encryption algorithm with the same key but reversed key schedule. In this way proposed system avoids the jamming attack over wireless network with great security.

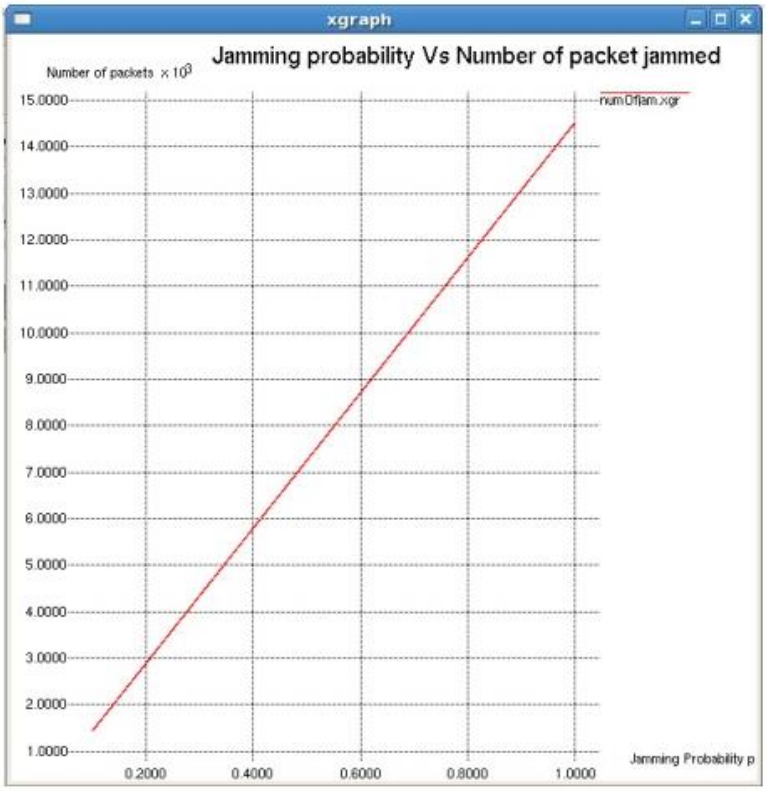

Figure 3: Jamming probability Vs Number of packets Jammed

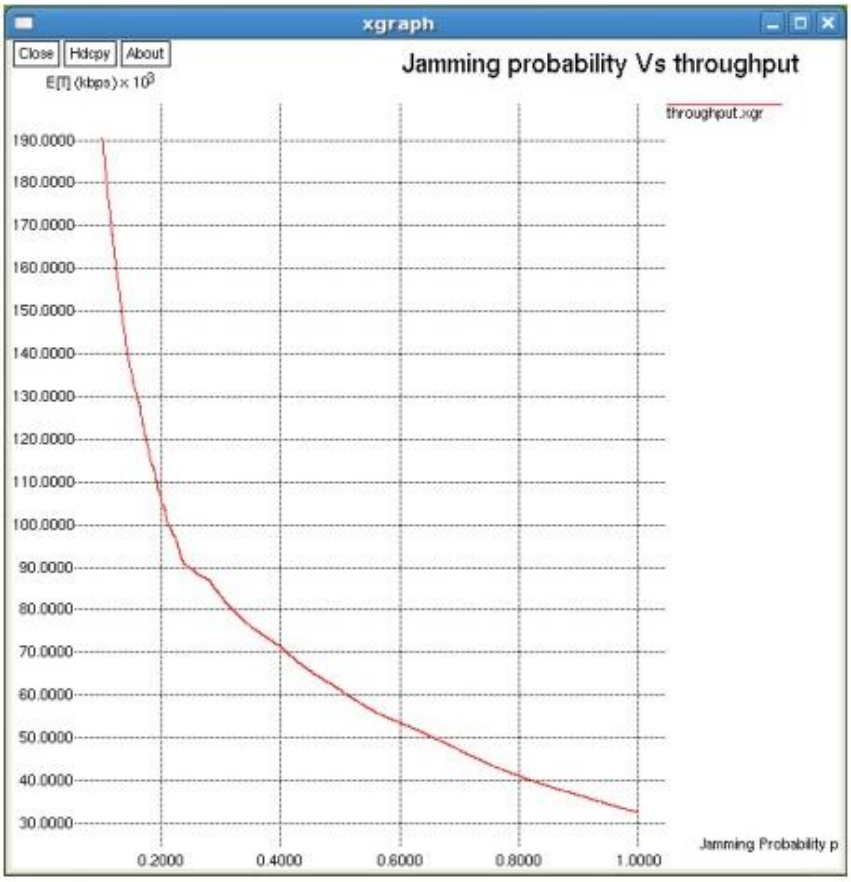

Figure 4: Jamming probability Vs throughput

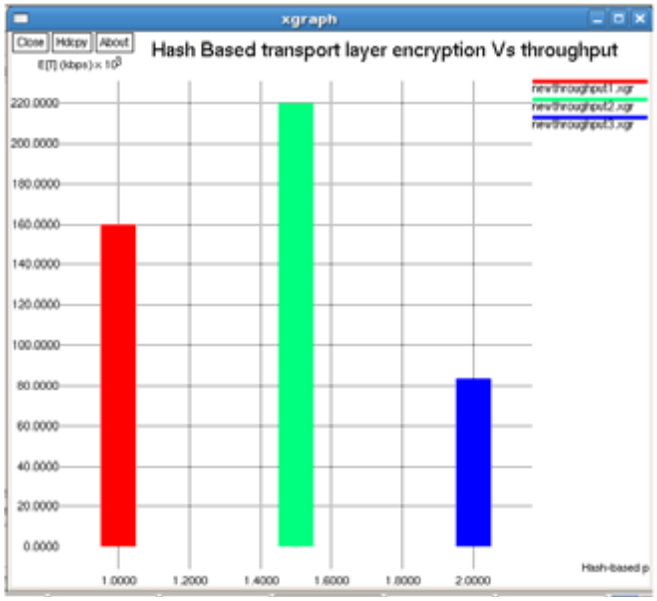

Figure 5: Encryption Vs throughput

8. CONCLUSION

This paper provides solution for jamming attack over wireless network. In this paper the internal threat model is considered, in which jammer is part of network and he is aware of network secrets and protocol specification. Jammer can perform classification in real time by decoding first few bytes of the transmitted packet. To prevent real time packet classification various schemes are developed. These schemes combine cryptographic primitives such as strong hiding commitment scheme with physical-layer characteristics so as to transform jammer to random one. We also measured how each jammer fared by their effect on the packet send ratio and packet delivery ratio. We analyse the security of our method and quantified their computational and communication overhead. This study has proved that both the intrusion detection systems and the intrusion prevention systems still need to be improved to ensure an unfailing security for a network. They are not reliable enough (especially in regard to false positives and false negatives) and they are difficult to administer. Yet, it is obvious that these systems are now essential for companies to ensure their security.

9. REFERENCES

- Amoroso, E.: Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response. Intrusion.Net Books (1999)

- Denning, D.: An Intrusion-Detection Model. IEEE Transactions on Software Engineering 13(2), 118-131 (1986)

- Denault, M., Gritzalis, D., Karagiannis, D., Spirakis, and P.: Intrusion Detection: Approach and Performance Issues of the SECURENET System. Computers and Security 13(6), 495-507 (1994)

- Crying wolf: False alarms hide Newman attacks, Snyder & Thayer Network World, 24/06/02, http://www.nwfusion.com/techinsider/2002/0624security1.html

- F. Cikala, R. Lataix, S. Marmeche", The IDS/IPS. Intrusion Detection/Prevention Systems ", Presentation, 2005.

- Helman, P., Liepins, G., Richards, W.: Foundations of Intrusion Detection. In: Proceedings of the IEEE Computer Security Foundations Workshop V (1992)

- Hervé Debar and Jouni Viinikka, "Intrusion Detection,: Introduction to Intrusion Detection Security and Information Management", Foundations of Security Analysis and Design III, Reading Notes in to Compute Science, Volume 3655, 2005. pp. 207-236.

- Hervé Debar, Marc Dacier and Andreas Wespi, "IN Revised Taxonomy heart Intrusion Detection Systems", Annals of the Telecommunications, Flight. 55, Number,: 7-8, pp. 361-378, 2000.

- Herve Schauer Consultants", The detection of intrusion…" Presentation: excerpt of the course TCP/IP security of the Cabinet HSC, March 2000.

- ISS Internet Risk Impact Summary - June 2002.

- Janne Anttila", Intrusion Detection in Critical Ebusiness Environment ", Presentation, 2004.

- Juels and J. Brainard. "Client puzzles: A cryptographic countermeasure against connection depletion attacks (Periodical style-Accepted for publication)", *the network and distributed System Security Symposium,* to be published.

- K. Manojkumar, M. Vinothkumar, and Dr. G. TholkappiaArasu, "An Analysis on Denial of Service attacks and packet defending methodologies in wireless sensor network".

- Langin, C. L. A SOM+ Diagnostic System for Network Intrusion Detection. Ph.D. Dissertation, Southern Illinois University Carbondale (2011)

- L. Lazos, S. Liu and M. Krunz. "Mitigating control channel jamming attacks in multi-channel ad hoc networks (Periodical style-Accepted for publication)", *the second ACM conference on wireless network security,* to be published.

- Lunt, T.: Automated Audit Trail Analysis and Intrusion Detection: A Survey. In: Proceedings of the 11th National Computer Security Conference, Baltimore, pp.65-73 (1988)

- Lunt, T.: A Survey of Intrusion Detection Techniques. Computers and Security 12, 405-418 (1993)

- Vaccaro, H., Liepins, G.: Detection of Anomalous Computer Session Activity. In: Proceedings of the 1989 IEEE Symposium on Security and Privacy (1989)

- Young, C.: Taxonomy of Computer Virus Defense Mechanisms. In: The 10th National Computer Security Conference Proceedings (1987)