International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 34281-34287

Mitigation of Session Hijacking in Mobile Ad hoc Networks

***1. K.Geetha**
Associate Professor
Department of Computer Science
Periyar Arts College,
Cuddalore
2. N.Sreenath
Professor
Department of Computer Science and Engineering
Pondicherry Engineering College,
Puducherry

Abstract- One of the attacks which severely affect the MANET is session hijacking attack. Session hijacking attacks occur by hijacking the session established between the source and destination. When the valid session is exploited, the unauthorized access gains the highly valuable and confidential information from the session. In Mobile Adhoc Networks (MANETs), the communication takes place mainly in emergency situations and highly confidential applications like military battle field. So, this attack is viewed seriously and solutions are provided to mitigate the effect of the attack by identifying the attack at an early stage. The detection method is tested with the Quality of Service (QoS) parameters which are essential parameters to determine the effective communication like packet delivery ratio, throughput, delay, jitter and control overhead. It is found that the mitigation algorithm works well in terms of the QoS parameters.

Keywords- MANET, Session hijacking attack, packet delivery ratio, throughput, delay, jitter, control overhead, QoS parameters

1. Introduction

Mobile Adhoc Networks play a vital role in ubiquitous computing. Due to the flexibility of the networks, these networks are now popular in usage. At the same time, they are vulnerable to a lot of attacks. One of the main attacks which occur in almost all the layers is session hijacking attack. These attacks generally arise by spoofing a nodes identity. So, they are difficult to identify. This paper presents an algorithm at the link layer as (LLD- Link Layer Detection) to identify the attack at an early stage. Since MANETs are used with multimedia communications, the data used here for transfer is multimedia data. The paper is organized as follows. Section 2 describes the related works Section 3 describes briefly the session hijacking attack. Section 4 explains the Link Layer Detection Method (LLD) to identify the attack at an early stage. The detailed analysis of the detection method with QoS parameters is explained in section 5. Section 6 concludes the paper.

2. Related Work

A Session hijacking attacks can be detected using sequence number analysis, transceiver finger printing and signal strength analysis [1]. Many of the existing methods use MAC sequence number to detect the session hijacking attack at MAC layer itself. J. Wright et al [2] proposed a method to detect session hijacking attacks using the MAC sequence number. In order to detect the session hijacking attack, a gap in the header frame was checked against the threshold; if it was beyond the given threshold session hijacking alarm was raised. But guessing the MAC sequence number by the attacker is possible in this case. Hall et al [3] proposed to identify the attack using received radio frequency finger printing (RFF). A profile of radio frequency finger printing was created and using wavelets and neural networks the finger prints were checked to match the profile. Session hijacking attacks were identified if there was difference. Gill Rupinder et.al [4, 5] used Received Signal Strength(RSS) and Round Trip Time values(RTT) to detect session hijacking attack. This method impressed very much since it has detected the session hijacking attack by checking the RSS and RTT values at frequent intervals. But false positives may arise due to the fact that the sudden variation in RSS and RTT values may be due to noise present in the signal or fading of the signals. Xia et al. [6] specified session id checking against session hijacking attacks. The session id was cryptographically protected. It should to be periodically refreshed with the encrypted session id. Session hijacking was detected if refresh was not done for a given period of time. This needs frequent refresh by the user. Long. et al. [7,8] proposed a method using continuous wavelet theory to identify the noise present in the signals received. A profile of signals were created for normal nodes and checked for matching in the abnormal attack situation that is during a difference in the signals received. The detailed coefficients of noise were calculated and checked against a threshold value. If noise was more, the attack presence was confirmed. Gill et al. [9] detected the intruder present in the network by specifying a node's normal behaviour with Radio waves frequency. Each frame received was checked against the specification. If there was any deviation from the normal behaviour the presence of intruder was identified. Dactsoitalo et al [10] used one time cookies to prevent the session hijacking attacks. One time cookies were sent to receiver. The cookies have to be reproduced as a security measure to prevent session hijacking attack. But, the attacker

may silently watch the communication and instead of hijacking the session, use the data later on.

3. Session Hijacking Attacks

Session hijacking attacks occur by hijacking the session established between the source and destination. When the connection is established between the nodes, the attacker spoofs the victims address and acts like the victim. He terminates or delays the communication which has been already established and takes away the connection. Now, the connection is established between the server and the victim. Without knowing the fact all the valuable information are communicated to the attacker by the server. The attack scenario is given in the figure 1. Initially, the Server and Client have established a session of communication. The attacker hijacks the session by knowing the address of the client.

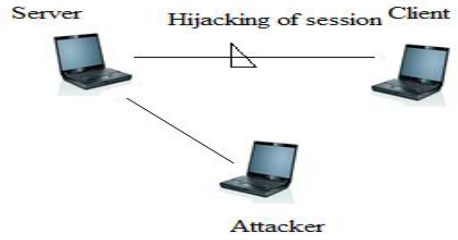

Figure1. Hijacking of Session

4. Proposed method- Link Layer Detection (LLD) Method

Detection methods which depend on the spoofable and predictable parameters like MAC sequence number are not reliable. The attackers can also guess these types of parameters if they are used for detection. In this detection method the unspoofable parameters like Received Signal Strength (RSS) and Round Trip Time (RTT) values are taken for detecting the session hijacking attack. The algorithm is divided in to three parts as 1. Monitor segment 2. Detection segment and 3. Response segment. The monitoring segment monitors the RSS values and RTT values continuously and keeps a profile of values. If there is any variation in the values the detection segment is called for the confirmation of the attack. The response segment provides the response to the attack. This algorithm is implemented in the source node which is sending the multimedia data (MS node). This is explained in the Figure 2.

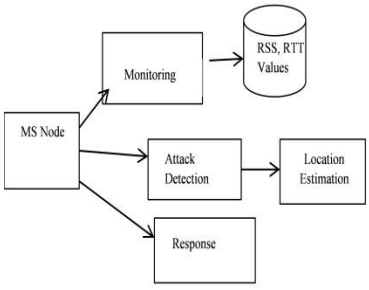

Fig 2. Segmented attack detection method-LLD

4.1 Algorithm

//Monitor the RSS and RTT values
Monitor _values:
Create a profile of RSS and RTT values
If sudden variation in RSS and RTT values
Proceed to attack confirmation

//Confirmation of Session hijack
i) Threshold-Check:
Attack _confirmation:
Separate noise and signal using Haar wavelet
F(t)=s(t)+n(t)
S(t) represents the signal with variations
Perform inverse transform of s(t) as s' the detail co efficient.
If s'- s > Threshold value the attack is present

ii) Signal fading check

Analyse the signal using Haar Wavelet and find the detailed co-efficient.

Find the carrier frequency ratio using the detailed co-efficient.

Find the signal fading with Doppler frequency shift.

If the fading is more than a threshold value then, the attack is confirmed.

4.2 Monitoring segment

RSS values are the measure of the received signal strength energy observed in the physical layer of the receiver's antenna [4]. The strength of radio frequency waves gets disturbed by the distance, shadowing and other object interferences. RTT values are the round trip time values. Before transmission, the source sends a RTS (Request To Send) frame to the receiver requesting positive control over the communication medium. The receiver acknowledges by CTS (Clear To Send) frame to the sender. The time between RTS and CTS is calculated as RTT.

The attacker uses the fake address of the MS node and sends a false de authentication message to the client in order to terminate the session. The client then, terminates the session with the MS node. This session is later used by the attacker. But, the client repeatedly tries to get reconnected with the MS node. The attacker has to repeatedly send the de authentication message periodically to the client.

Another variation of this approach is the attacker, may not de authenticate but, uses the same IP address of the client and simultaneously communicate with the MS node. In the MAC layer it cannot be identified.

4.3 Detection Segment

A profile of the received signal strength is maintained in a list. The profile is created with an attack free environment. The nature of the signal strength is thus will not vary a lot unless these signals are get distorted by distance, shadow fading, presence of noise etc. Otherwise the RSS will follow a consistent distribution [4]. In MANETs, mobility adds the fact that the RSS value will vary a lot where an adversary cannot guess this. Similarly a profile of Round trip time is also maintained by the monitor. A node can transmit data only when its Network Allocation Vector (NAV) is zero. The NAV value reveals the predicted time it will take to transmit

the frame from the sender to the receiver and the corresponding acknowledgment (ACK) frame to return from the receiver to the sender. The data transmission between the source and the destination takes place only after an RTS-CTS handshake/session. The profile of RSS and RTT values are maintained in the list by the monitor. Once there is a sudden jump in values, the presence of session hijacking attack is suspected. This is shown in Figure 3.

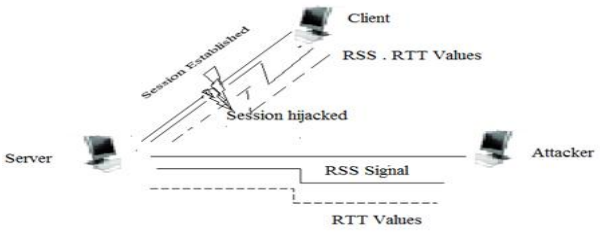

Fig3 Session Hijack Detection Scenario

The sudden change in the RSS signal and RTT values may be due to noise that present in the signal. So the variance of the values are taken and checked for change as,

$$\text{Var(s)}= \frac{\sqrt{(di \cdot m)^2}}{n} \quad (1)$$

$$\text{Var(t)} = \frac{\sqrt{(si-m)^2}}{n}$$

Where, m is the mean of the signal values n is the number of signals. s_i is the set of RSS signals of n numbers, d_i is the set of RTT values of n numbers.

If the variance is more, the presence of session hijacking is assumed. However the variation may be due to the presence of noise.

4.4 Confirmation of Attack

In order to confirm the presence of the attack, the signal fading is computed. First the signal is analysed using Haar wavelet as a filter. The signal is checked against the fade margin value, if the permissible fading is exceeded, the session hijacking attack is confirmed.

Generally, the fading of RF signals are not linear with respect to distance, but they are inversely proportional to the square of the distance between the node and the sender [4]. The fading of signals may occur due to noise or some added energy present in the signal. This is allowed up to a threshold value. Different sources will have the allowed fading values differently. Here, the signal is filtered first using Haar wavelet and checked for the fading.

4.4.1 Wavelet Theory and Signal Analysis

The term "wavelet" (originally called wavelet of constant shape) was introduced by J. Morlet [12]. These are functions used to localize a given function in space and time. A family of wavelets can be constructed from mother wavelets. The discrete wavelet transform is used in this as the signals are represented as discrete samples.

The Haar wavelet is the simplest wavelet. For any signals represented by 2^n values,

2^n -1 differences and sum are produced. It is very much used in finding the sudden jump in signal values.

Example for Haar wavelet transforms

Let the signals be,

f= (8, 6, 10, 12, 8, 6, 5, 5)

f can be decomposed into (a1|d1)

a- approximation co-efficient and

d- detailed co-efficient with the formula as

$ai=(f(2i-1)+f(2i))/\sqrt{2}$

$di=(f(2i-1)-f(2i))/\sqrt{2}$

i takes the values from 1 to n/2

$$f=(8,6,10,12,8,6,5,5) \xrightarrow{\text{H:1st level}} (7\sqrt{2},11\sqrt{2},7\sqrt{2},5\sqrt{2},\sqrt{2},-\sqrt{2},\sqrt{2},0)$$

The inverse transform can be performed by

$$f'=[(a1+d1)/\sqrt{2},(a1-d1)/\sqrt{2},.....,(an/2+dn/2)/\sqrt{2},(an/2-dn/2)/\sqrt{2})]$$

a1: $7\sqrt{2}$ $11\sqrt{2}$ $7\sqrt{2}$ $5\sqrt{2}$

d1: $\sqrt{2}$ $-\sqrt{2}$ $\sqrt{2}$ 0

f: 8 6 10 12 8 6 5 5 .

i) **Separating noise in a signal**

When a signal is traveling a distance it will be contaminated by added noise. The signal is represented as,

Contaminated Signal =original signal + noise

f(t)=s(t)+n(t) (2)

The noise can be separated by threshold method [13] by transforming the contaminated values which have magnitudes which lie below a threshold value tn<Ts. For de-noising these values are set to zero and inverse transform is performed. The threshold value is calculated as

Ts= $\sigma\sqrt{2\log n/n}$ where

σ is the standard deviation of the signal,

n is the number of signals.

All values of noise included signals below the threshold value is taken as noise parameters n and an inverse transform of signal (s') is performed to obtain the approximation of the signal(s)

If Inverse(s') - s > specified threshold value the attack is present.

We find the variance of noise n as

$$\text{Var(n)}= \frac{\sqrt{(ni-m)^2}}{n} \quad (3)$$

Where, m is the mean of noise values.

ii) Signal Fading

The equation (2) can be written as,

$f(t) = n(t) + \Delta m.\ u(t-t0)$ (4)

where u(t) is the unit step located at unknown time instance t0.

Δm is the jump amplitude. It can be assumed to be derived from the path loss as

the distance from the genuine node to the MS node is $d_0(t)$ and distance from attacker node is $d_1(t)$

$$\Delta m = x1 - x0 + \mu \log 10(d1(t0)) - \mu \log 10(d0(t0))$$

Where x1, x0 are path loss constants. $\mu \log_{10} d$ represents the path loss as a function of the distance d between the sender and the receiver. The source can compute the approximate distance with the receiver using the formula [4]

Distance = (Speed of RF waves in air X (RTT / 2))

It is assumed that the speed of RF waves is a constant. The mobile node is assumed to be moving with constant speed. By calculating the distance from where the signal is generated, the location of the attacker can be identified.

Wavelet is used to analyse the signals and find the difference in the signals.

The wavelet transform is generally a decomposition of the original signal into a set of basic wavelet functions.

The wavelet function can be represented as

$$\psi_{s,r}(t) = (1/(\sqrt{s}))\psi((t-r)/s$$

Where $\psi(t)$ is the mother wavelet, s, r is represent the dilation (scaling) and transition parameters. The application of this family of wavelets to discrete signal requires discretization of the translation and distortion parameters. Discrete Wavelet transform (DWT) is the simple and most efficient discretization method where

$s=2^j$ $r=k.2^j$

That is, $\psi_{j,k}(t) = 1/\sqrt{2^j}\,(\psi((t-k2^j)/2^j))$

$$\psi_{j,k}(t) = 2^{-j/2}(\psi(2^{-j}t-k)) \quad (5)$$

is the wavelet function transformed from the mother wavelet function ψ (t)[8]

With scale j , time t and k the coefficients of the wavelet.

The Haar wavelet's mother wavelet, can be derived as [15]

$\psi(t)$ = 1, if 0 <=t <1/2
-1 if ½ <=t <1
0 otherwise

The wavelet transform can be expressed linearly for (3) as [8],

$$d_f(j,k) = d_n(j,k) + d_s(j,k)$$

d_s(j, k) are the detailed wavelet coefficients of the step function[8]

from (4),

$$s(t) = \Delta m.u(t - t0)$$

From [8]

$$Let I_\psi(t) = \int_{-\infty}^{t} \psi(u)du$$

$$d_s(j,k) = -\Delta m.2^{j/2} I_\psi(t02^{-j} - k) \quad (6)$$

From (2) and (6),

Signal to noise ratio[7] w= $(|ds(j, k)|)^2$/var (n)) (7)

= $\Delta m^2 2^j I(0)^2$/var(n)

The signal to noise ratio follows the Rayleigh distribution after filtering at the receiver's end [14].

The variance in the signal can be obtained by considering a Doppler shift in the frequency domain, which gives the fading of signals as,

$$fa = 1/(\prod wm\sqrt{1-((wc-w)/wm)^2}) \quad (8)$$

The fading of signals are allowed with in a fade margin [16] denoted by threshold. The fading of signals is given in terms of Doppler shift. The carrier frequency can have a shift from wc and wm. Where w represents the carrier frequency, wm represents the maximum carrier frequency of signal. The waveform can have a frequency shift in the range wc and wm. If fa is beyond specified value session hijacking attack is confirmed.

4.5. Response Segment

The duty of the response segment is to close the connection with the session hijacker once it is detected. The detection segment continuously checks for the presence of attack. If there is no session hijack the signal values and the round trip time values will not vary very much. Under the presence of hijack attack, these values show large variation. After the confirmation of the attack, the session will be closed with the malicious node

5. QoS ANALYSIS

The session hijacking attacks is a serious attack, which cannot be detected easily. However, the QoS parameters show the variation in packet delivery ratio, control overhead/node, throughput, end to end delay and jitter. The variations are studied and graphs are drawn. AODV protocol is chosen as a routing protocol to study the performance of the various QoS parameters. A simulation is carried out using the Network Simulator 2.

The simulation parameters are shown in table 1.

Table 1. Simulation Parameters

Number of Nodes	150
Simulation Area	1000 m X 1000 m
Buffer Size (Queue Length)	50 Pkts
Packet Size	1024 bytes
Application Traffic	Video traffic – evalvid
Simulation time	200 Secs
Number of Connections	150
Connection duration (secs)	20
Data Intervel	0.01,0.02,0.03,0.04,0.05,0.06,0.07 ,0.08,0.09,1.00
Connection	10,20,30,40,50,60,80,100,120,140 ,150
Protocol used	AODV

i) Packet Delivery Ratio

The PDR shows how stable are the networks in delivering data. The behaviour of the network with PDR is shown in the Figures 4 (a) Packet Delivery Ratio: Packet delivery ratio is an important metric to be considered while measuring any network performance. PDR is measured by computing the

ratio of the number of packets delivered to the number of packets sent from the source [17]

PDR= Number of packets delivered/Number of packets sent

This is one of the main QOS in measuring the performance of the network. The network is stable and a maximum of 99% of packets are delivered to the receiver. The AODV protocol determines the route on demand only. With 40 connections, the MANET shows the best performance. The packet delivery is almost consistent to an average of 92%. .

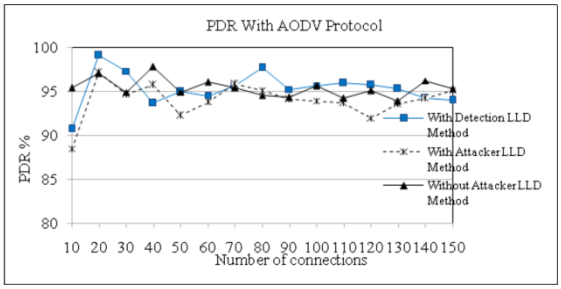

Fig 4(a). LLD Method - PDR-AODV Protocol

The LLD method detects the session hijacking attack at an early stage itself, by continuously monitoring the RTS and CTS signals. When session hijacking is detected, the connection is re- established immediately. The PDR will not be affected very much in this case. A maximum of 98% of packets are delivered to the receiver after the deduction of the attack. AODV may take initial set up time and decrease the PDR. Later on, when the number of connection increases, the PDR also increases. In many cases of AODV protocol the PDR is reaching the values of an attack less MANET.

ii) Control Overhead / Node

Control Overhead/Node is the routing overhead produced per node. Average routing overhead is the average number of the control packets produced per node [18]. This includes route requests, replies and error messages.

COH/node=Control packets produced/number of nodes

The number of control packets used for the data transfer per node is analysed. With increased control packets, the performance of the network will be poor. To have a good communication with reduced delay the control packets used must be small. It includes the route request, route reply and route error messages. The AODV Protocol due to its dynamic route request and allotment produces a maximum of 150 control packets / node. The minimum number of packets used is 50. This is shown in the Figure 4(b)

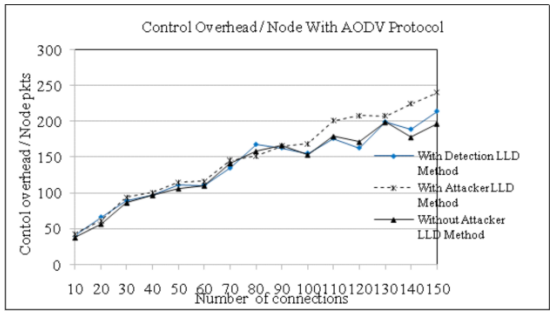

Fig 4(b) LLD Method - Control Overhead / Node - AODV Protocol

protocol.. The amount of control overhead in AODV is related to the number of routes it maintains, especially in the route discovery phase. As the number of nodes increases, the overhead also increases here. The Detection method finds the attack and closes the connection. Then it tries to send the data through alternate path. The control overhead involved here is only due to the fact of finding alternate route to send data..

iii) Throughput

Throughput: Throughput measures the amount of data successfully delivered to the destination from the source. It is usually measured in bits / sec.

`Throughput=Data delivered/time unit

The throughput is good. A maximum of 2500bps is achieved in this case. The performance is shown in the Figures 4 (c). Initially the throughput is very low. With attacker, the throughput is very low even after the connections are Increased. The LLD detection increases the throughput to maximum. Nearly 30% of throughput increase is achieved with LLD Method.

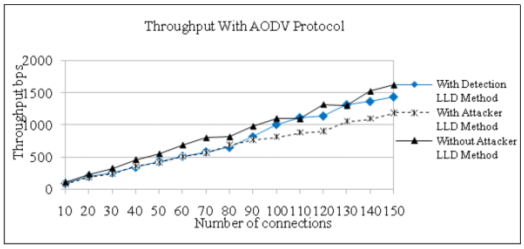

Fig 4.(c) LLD Method –Throughput- AODV Protocol

iv) End To End Delay

End to End Delay includes all types of delays that occur during transmission like route discovery delay, processing delay, queuing delay and propagation delay. The delay is averaged by computing the ratio of the send time-received time with the number of received packets [19].

ETE delay=(Sending time – Received time)/Number of packets received

In an attack free environment, the delay is very less with AODV protocols as the nodes are local and information about the route is immediately available, the data transfer is quick in As the number of nodes increases, the delay also decreases due to the availability of shortest path to the destination. The figure 4.(d) shows the end to end delay. Since this is connected with the user satisfaction, this is a

very important parameter to be calculated for a multimedia transmission.

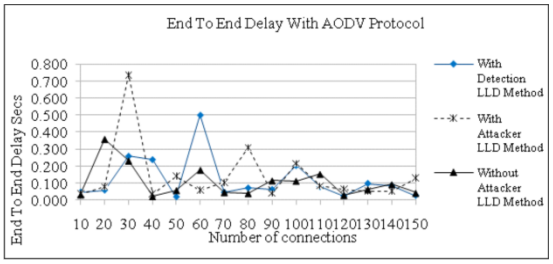

Fig 4 (d) LLD Method – End to End Delay – AODV Protocol

iv) Jitter

The most important and relevant metric for the multimedia data transfer analysis is jitter. Jitter (Delay variation) is the difference in end to end delay between selected packets in single connection [20]. Thisoccurs due to network congestion, improper queuing. The information is broken down in to packets and these packets choose any path during the travel. The rapid increase in the delay jitter may be considered as the indication of problems in data delivery during multimedia communication.

$Jitter=ETE(pkt_{i+1})-ETE(pkt_i)$

The jitter is very low in an attack free environment with the protocols AODV, The delay in between the adjacent packets received in each node is calculated as jitter. A low jitter provides good multimedia communication. Initially the jitter is high, with lesser nodes available, later on, when the number of nodes increase, the jitter also decreases due to the availability of enough number of nodes. When there is session hijacking attack the jitter becomes increased due to the non-availability of data transfer. The delay increases hence the jitter also increase. Initially the jitter is very high in all the protocols. Once the transmission started or resumed after detecting the attack it reduces and even reaches zero.

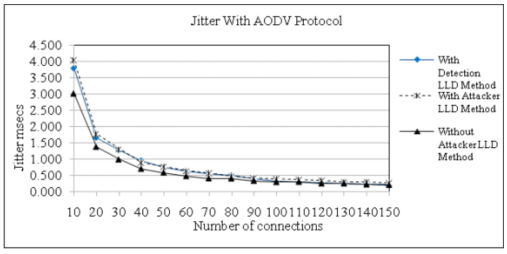

Fig 4.(e) LLD Method – Jitter – AODV Protocol

6. Conclusion

The algorithm involves enough computations and storage needed for the information. First the RSS and RTT values need to be maintained in storage. The variation should be computed. The variation calls for the detection method by raising an alarm. Using Haar wavelet, the signals are filtered and checked for fading. Many false alarms may be produced due to the variations in RSS and RTT values. This is common if the noise is increased. Some false alarms may be generated, but the attack may not be confirmed in such cases by the detection segment.

REFERENCES

[1] S. M. Y. Sheng, K. Tan, G. Chen, D. Kotz, A. Campbell, Detecting 802.11 MAC layer spoofing using received signal strength "in proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM '08), 2008 pp. 1768–1776, Phoenix, Arizona, US,

[2] J. Wright, Joshua. "Detecting wireless LAN MAC address spoofing." *White Paper*, January 2003.http:// home.jwu.edu/jwright

[3] Hall, M. Bareau, and E. Kranakis, "Using transceiver prints for anomaly based intrusion detection", in Proceedings of 3rd International Conference on Communications, Internet, and Information Technology, Nov. 2004, pp. 22–24 St. Thomas, US Virgin Islands

[4] Gill, R, Smith J, Looi M. & Clark, A. "Passive Techniques for Detecting Session Hijacking Attacks in IEEE 802.11 Wireless Networks" in Proceedings of Asia Pacific Information Technology Security Conference May 2005 (AusCERT2005), pp. 26–38. Australia

[5] R. Gill, J. Smith, and A. Clark. "Experiences in Passively Detecting Session Hijacking Attacks in IEEE 802.11 Networks" in proceedings of the Fourth Australasian Information Security Workshop (Network Security) (AISW 2006), volume 54 pp.221–230. Hobart, Australia. ACS.

[6] Xia, Haidong, and Jose Brustoloni. "Detecting and blocking unauthorized access in Wi-Fi networks." in proceedings of the NETWORKING 2004. Springer Berlin Heidelberg, 2004. pp.795-806. Athens, Greece.

[7] X. Long and B. Sikdar, "Wavelet based detection of session hijacking attacks in wireless networks," in Proceedings of IEEE Global Telecommunications Conference, IEEE GLOBECOM , 2008. pp. 1-5. New Orleans, United States of America

[8] Long, Xiaobo, and Biplab Sikdar. "A mechanism for detecting session hijacks in wireless networks.", IEEE Transactions on Wireless Communication spp. 1380-1389 Vol.9(4) 2010.

[9] R. Gill, J. Smith, and A. Clark "Specification-based Intrusion Detection in WLANs" in proceedings of IEEE 22nd Annual Computer Security Applications Conference (ACSAC) June 2006 . pp. 141-152. Florida USA.

[10] Dacosta, I., Chakradeo, S., Ahamad, M., Traynor, P. "One-Time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens". ACM Transactions on Internet Technologies pp. 1-24 vol.1.1. 2012

[11] The Network Simulator, NS-2, from www.isi.edu/ nsnam/ns, 2006

[12] R. A. DeVore and B. Lucier "Wavelets", in ActaNumerica, Volume 1, Cambridge University Press, 1992 .pp. 1–56

[13] Walker, James S. A primer on wavelets and their scientific applications. CRC press, 2008.

[14] Sklar, Bernard. "Rayleigh fading channels in mobile digital communication systems. Part I. Characterization." IEEE

Communications Magazine, Issue 35, number. 7. 1997: pp.90-100.

[15] Vetterli, Martin, and Cormac Herley. "Wavelets and filter banks: Theory and design." IEEE Transactions on Signal Processing, Volume 40, Number. 9 1992. pp. 2207-2232.

[16] Bardwell, J. You believe you understand what you think I said...—the truth about 802.11 signal and noise metrics. Connect 802 Corporation, white paper. 2004.

[17] S. Corson and J. Macker, Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations (Internet-draft), in Mobile Ad-hoc Network (MANET) Working Group, IETF 1998

[18] Perkins, Dmitri D., Herman D. Hughes, and Charles B. Owen. "Factors affecting the performance of ad hoc networks."In IEEE International Conference on Communications, 2002, volume. 4, pp. 2048-2052.

[19] Sun, J. Z. "Mobile ad hoc networking: an essential technology for pervasive computing", in proceedings of the International conference on Info-tech and Info-net, Beijing. Volume 3, 2001. pp. 316-32.