Manual and automatic assigned thresholds in multi-layer data fusion intrusion detection system for 802.11 attacks

Manual and Automatic Assigned Thresholds for Multi-layer Data Fusion IDS in 802.11 Attacks

Konstantinos G. Kyriakopoulos, Francisco J. Aparicio-Navarro, David J. Parish

Abstract

Abuse attacks on wireless networks are becoming increasingly sophisticated. Most of the recent research on Intrusion Detection Systems for wireless attacks either focuses on just one layer of observation or uses a limited number of metrics without proper data fusion techniques. However, the true status of a network is rarely accurately detectable by examining only one network layer. The goal of this work is to detect injection types of attacks in wireless networks by fusing multi-metrics using the Dempster-Shafer (D-S) belief theory. When combining beliefs, an important step to consider is the automatic and self-adaptive process of Basic Probability Assignment (BPA). This work presents a comparison between manual and automatic BPA methods using the D-S technique. Custom tailoring BPAs in an optimum manner under specific network conditions could be extremely time consuming and difficult. In contrast, automatic methods have the advantage of not requiring any prior training or calibration from an administrator. The results show that multi-layer techniques perform more efficiently when compared to conventional methods. In addition, the automatic assignment of beliefs makes the use of such a system easier to deploy whilst providing a similar performance to that of a manual system.

Index Terms

Mixed-layer measurements, data fusion, Dempster-Shafer, wireless injection attacks, Wi-Fi

I. Introduction

THE broadcast nature of wireless networks has proliferated the number of malicious intent attacking software tools, which aim at exploiting the vulnerabilities of the Physical and Medium Access Control (MAC) Layers. Such tools could be used for intrusion purposes or disruption of services. These wireless attacking tools are increasingly becoming more sophisticated and untraceable by Intrusion

K. Kyriakopoulos, F. J. Aparicio-Navarro, D. J. Parish are with the School of Electronic and Electrical Engineering, Loughborough University, Loughborough, LE11 3TU, U.K. e-mail: {elkk, elfj2, d.j.parish}@lboro.ac.uk, website: http://www-staff.lboro.ac.uk/∼elkk/Site/Testbed_data.html

The authors would like to acknowledge the support of EPSRC in funding this work.

Detection Systems (IDS) because most of current IDSs either focus on just one layer of observation or use a limited number of metrics without intelligently combining the knowledge derived from each metric.

Therefore, a mixed-layer approach may offer a collaborative decision among layers, potentially resulting in a higher accuracy detection rate (DR) and lower number of false negatives (FN) and false positives (FP). Hence, utilising a mixed-layer approach may help towards enhancing the overall process of detecting and mitigating wireless network attacks [1], [2]. Collaborative decisions can be achieved with the use of Data fusion techniques.

Data fusion can be defined as the process of collecting information from multiple and heterogeneous sources, and combining this to obtain a more accurate final result [3]. As we have shown in previous work [1], [2], Dempster-Shafer (D-S) theory of evidence is a good candidate for this purpose because it does not require a priori knowledge of the system, and provides the ability to manage uncertainty.

Despite having been proven as a powerful and efficient technique, a very important issue remains unsolved when D-S theory is used for IDS activities; to find an automatic and self-adaptive process of Basic Probability Assignment (BPA), based on the measured characteristics of the network. The major challenge for applying D-S theory to IDS is to determine the beliefs of whether an event is malicious or not, from the collected network measurements [4]. There exist multiple ways of assigning probabilities to each of the hypotheses in D-S theory, ranging from data mining techniques to empirical/manual approaches. However, few of them could be used in an off-the-shelf manner without a previous thorough training or fine tuning period.

This paper presents four methodologies of using metrics from multiple layers of wireless communication networks for detecting injection type of attacks that exploit the physical (PHY) layer. The collected metrics are analysed and compared to historical data and each metric gives a belief of whether an attack takes place or not. The beliefs from different metrics are combined with the D-S data fusion theory with the ultimate goal of limiting the number of false alarms and improving the overall performance.

In this work, we propose a novel BPA methodology able to automatically adapt its detection capabilities to the current characteristics of the wireless network, without intervention by an IDS administrator. We have developed an on-line, multi-layer based tool, able to classify in real time network frames as normal or malicious. If the frame is detected as malicious, the system could take some basic preliminary measures such as informing the administrator and closing the victim's web browser for protection. The proposed method only requires a light weight process of generating a baseline of normal utilisation, in order to

generate high intrusion detection accuracy and low number of false alarms.

The differences and additions from our previous papers [1], [2], [5] are:

- An extra metric is considered (Sequence Number).
- We present complete results for all possible metric combinations.
- We compare detection performance between manual and automatic bpa assignments.
- We present new results designed to provide more realistic comparison of our algorithms.

The paper is organised as follows. In section II, related work is reviewed. A practical example for understanding D-S theory is presented in section III. The testbed, and attack scenarios are presented in section IV. In particular, a Man-In-the-Middle (MitM) attack at PHY and a De-authentication attack are examined. The methodologies for manual and automatic BPA are explained along with the chosen metrics in section V. In section VI we discuss the results obtained from the two types of proposed BPA algorithms, manual and automatic, each with two variations. Finally, conclusions and future work are discussed in section VII.

II. Related Work

As far as the authors are aware, there are no publications describing detection of MitM attack at PHY. In contrast, there are various articles regarding detection of De-authentication attacks. In [6], the authors detect De-authentication by analysing the management traffic patterns and classifying the active attacking traffic patterns. In [7], [8], the authors propose delaying the effects of de-authentication to allow the AP to observe subsequent packets from the client. For further references on detecting De-authentication attacks see [9], [10], [11].

In [12], the authors describe a multi-layer methodology to increase the performance of an anomaly IDS for detecting DoS attacks. The data fusion, however, is not carried out using D-S theory and they use metrics from only the network and data link layers. In [13], the authors follow a multi-layer approach and try to detect malicious jamming behavior and differentiate it from genuine network failures. The proposed mechanisms are only tested by simulation. The paper does not focus on threshold estimation and selection and the metrics are limited to two layers.

The application of D-S theory for improving the performance of IDSs is a very active research topic. One of the most thorough descriptions of D-S is presented in [14], where a comparative study between D-S theory and Bayesian inference is presented.

D-S theory has been previously used in the intrusion detection field to enhance detection accuracy [3], [15], [16]. In [15], the problem of discovering anomalies in large-scale networks based on the data fusion of heterogeneous monitors is considered. The authors used metrics based on TCP-SYN, TCP-FIN, UDP and ICMP statistics to detect SYN, UDP and ICMP flood attacks.

The authors in [16] present and evaluate an IDS for detecting jamming attacks by seeking changes in a single metric, the Signal-to-Noise Ratio. The authors use D-S theory to fuse the information from distinct nodes running two different types of local algorithms; Single Threshold and Cumulative sum. In [4], the authors use a weighted modification of D-S for combining beliefs of DDoS attack among widely spread sensor nodes. Finally, the author in [17] gives a thorough review of D-S applications on IDS.

Among all the work on IDS that investigate the use of D-S theory, there exist multiple ways of assigning probabilities to each of the hypotheses. For instance, [18] utilises expert opinion to manually assign the belief probabilities. This BPA process is completely subjective and might not be adequate for automatic and self-adaptive IDSs.

Another example, [19], proposes two different ways of assigning belief probabilities, for two different datasets. In the first case, a threshold based on the length of the dataset is calculated, and then uses that threshold with fixed functions to assign the belief probabilities. In the second case, a scaled approach with pre-defined beliefs is used.

The authors in [3] express the BPA as three simple and fixed functions. Again, the BPA process is based on the subjectivity of the IDS administrator and, therefore, is not appropriate for automatic and self-adaptive IDSs. The methodology employed by [4] uses data mining techniques to proceed with the BPA tasks. The use of data mining techniques mostly focuses on processing large amounts of audit data traffic rather than performing real-time detection.

From the presented results, all of these methods are effective in increasing the detection rate and reducing the number of false alarms of the IDSs. However, none of the above works fuse information from various metrics across multiple layers to detect injection based attacks. Furthermore, none of them investigate methods to find an automatic and self-adaptive process of BPA, and few of them could be used off-the-shelf without a significant training or fine tuning period.

III. Dempster-Shafer Theory

The Dempster-Shafer (D-S) theory of evidence method combines evidence of information from multiple and heterogeneous events in order to calculate the probability of occurrence of another event. D-S theory

is based on the formalism of representing hypotheses as subsets of a given set [20]. D-S theory and definitions has been presented by the authors in previous work [1], [2]. To easily understand how to apply the D-S algorithm, a real practical example from our measurements is presented.

Let m_1 and m_2 be the basic probability assignments from observer 1 and 2 respectively. The basic probabilities for an event (Attack $\{A\}$, Normal $\{N\}$, and Uncertain $\{A, N\}$), for both observers can be tabulated as in Table I. The cells in Table I represent the product between the mass function for each focal element of observer 1 (m_1) and observer 2 (m_2). So, given our example, the mass functions are: $m_1(\{A\}) = 0.32$, $m_1(\{N\}) = 0.25$, $m_1(\{A, N\}) = 0.43$. The respective belief functions are $Bel_1(\{A\}) = 0.32 + 0.43 = 0.75$, $Bel_1(\{N\}) = 0.25 + 0.43 = 0.68$, $Bel_1(\{A, N\}) = 0.43$.

The idea behind the D-S rule of combination is to fuse the belief in one given hypothesis from two different bodies of evidence, provided that the belief functions to be combined are based on entirely distinct bodies of evidence.

The combined belief of observer 1 and 2 is the orthogonal sum, $m_{comb} = m_1 \oplus m_2$, and is defined as

$$m_{comb}(\{H\}) = \frac{\sum_{X \bigcap Y = H} m_1(\{X\}) * m_2(\{Y\})}{1 - \sum_{X \bigcap Y = \varnothing} m_1(\{X\}) * m_2(\{Y\})} \quad when \quad H \neq \varnothing \tag{1}$$

where $X \bigcap Y = H$, are the sets where the common hypothesis between m_1 and m_2 is set H.

If the denominator, K, of eq. (1) is equal to zero, then $m_1 \oplus m_2$ does not exist and m_1 and m_2 are said to be totally contradictory. The denominator can be considered as a measure of the extent of conflict between the two belief functions. Indeed, the greater the instances where belief is assigned to the null set, the greater the $\sum_{X \bigcap Y = \varnothing} m_1(\{X\}) * m_2(\{Y\}$, which represents assignment of belief to the contradictory sets of A and N [20].

Returning to our example, K is calculated from eq. (1): $K = 1 - (0.032 + 0.0875) = 0.8805$. Therefore, $1/K = 1.136$ and

$$m(A) = 1.136 * (0.112 + 0.1505 + 0.176) = 0.5$$

$$m(N) = 1.136 * (0.025 + 0.043 + 0.1375) = 0.23$$

$$m(A, N) = 1.136 * (0.2365) = 0.27$$

According to the above results, the hypothesis more likely to be true is A, with higher belief than the

TABLE I
EVENT PROBABILITIES ASSIGNED BY m_1, m_2 AND THEIR PRODUCTS

$m_2 \downarrow$ / $m_1 \rightarrow$	$\{A\}$: 0.32	$\{N\}$:0.25	$\{A, N\}$: 0.43
$\{A\}$: 0.35	0.112	0.0875	0.1505
$\{N\}$: 0.1	0.032	0.025	0.043
$\{A, N\}$: 0.55	0.176	0.1375	0.2365

other hypotheses.

When combining many pieces of evidence, the computational complexity of D-S increases exponentially with the number of possible hypotheses. In our proposed methodology there are only three hypotheses. Thus, the computational complexity of the algorithm is low [19] and can be practically implemented on-line. In Section VI-C we examine the time it takes for the proposed methodology to perform the DS data fusion algorithm in on-line and off-line operations.

IV. EXPERIMENTAL SETUP

A. Testbed

Experiments were conducted on a real IEEE 802.11 testbed. This included a client, running Ubuntu Linux, associated with an Access Point (AP) and accessed webpages hosted on the Internet across different geographical locations (USA, China, Japan, EU, Singapore, etc). The purpose of such a wide choice of geographical locations was to vary the TTL values of the legal frames coming from the authentic web servers. In order to capture and analyse the generated traffic during the experiments, a monitoring computer running Ubuntu Linux was used, while the attacker was running BackTrack Linux [21]. All the devices except for the AP used the Atheros chipset in their wireless cards. The AP was a Cisco Linksys model WRT54GL set up to use 802.11g without support for 802.11w (used for increased security of management frames).

B. Attack Description

1) Man-In-The-Middle at Physical Layer: The Airpwn [22] tool was used by the attacker to launch MitM attacks *at the PHY layer* between the Access Point (AP) and the client (victim). The Airpwn attack can be considered as a PHY layer attack given that the attacker exploits a PHY layer issue, which is the capability to listen and inject frames on the channel. Airpwn also takes advantage of the time that a web

server takes to respond to normal webpage requests. In that lag time, it can inject its own content onto the wireless channel of the AP.

In our experiments, two types of attacks were launched against the client. Both attack types were default options in the Airpwn suite. In Attack 01, the attacker injects a forged frame containig HTML code that replaces the title of the authentic webpage with a custom one. In the second type of attack, the attacker listens for requests for images hosted on the webpage and injects its own images [22].

As this type of MitM attack takes place at the PHY layer, it cannot be detected with conventional MAC spoofing detection techniques. It should be noted that the attacker was placed very close to the AP, around 1.5 meters away. This positioning of the equipment makes the detection of attacks much more difficult as the shared environmental conditions and similar distance could make characteristics, such as RSSI, indistinguishable between the AP and the attacker. In addition, the TTL field value for the injected frames was changed from Aripwn's default 255 value to a more realistic value of 50.

2) De-authentication Attack: Another type of attack that has been investigated is the de-authentication of wireless clients from a WPA2 encrypted, legal AP. This type of attack is commonly utilised in DoS attacks. In this case, the attacker launches spoofed de-authentication frames with the purpose of disrupting the victim's connection to the AP and denying its services to the victim.

The detection of the de-authentication attack was possible just by using information from the PHY and MAC layers, and by utilising only management frames because the network was encrypted with WPA2, and we assumed that the monitor node does not have the WPA2 key to decrypt the frames.

The advantage of our approach in comparison to conventional methods is that by using multi-layer measurements the attack can be detected at the instance it is actually launched. In contrast, other techniques such as [23], are based on counting the number of de-authentication frames and when this surpasses a threshold, an alarm is triggered. There are two problems associated with such an approach. First, an attacker might be aware of such detection techniques and cunningly control the number of injected frames per time interval. And secondly, this technique allows for the malicious frames to reach the victim until the threshold is exceeded.

V. Methodology

The aim of our methodology requires any solution to be computationally simple, scalable and applicable to other wireless technologies apart from WiFi. Initially, the monitoring wireless card is set into monitor mode for sniffing and capturing frames coming from the AP and destined to the client. From each captured

frame, several predetermined metrics (discussed in Section V-A) are isolated and grouped into respective arrays. Each array is used in a sliding window scheme to construct the current baseline profile of normal utilisation for each metric.

The length n of the sliding window influences the overall detection performance of the system. In the experiments conducted for this article, we have used $n = 30$ frames for generating the reference. We have experimentally verified [24] that for the Airpwn attack, a window size of more than 12 samples performs with high DR and low FP. For the De-authentication attack a window size larger than 30 is required. In fact, there is a wide range of window sizes for which performance is optimal and a window size of 30 is the smallest from the range. In previous experiments [5], [1], [2] we have used a window size of 20 which was not optimum but was close to it. To find the optimum window, we analysed the captured data multiple times by varying the window size from 1 sample up to 100. More detailed results regarding the optimum window size can be found in [24].

We now propose two schemes to assign beliefs for the hypotheses of Attack, Normal and Uncertainty; one manual and the other automatic. Both use as an initial step the distance between the value of the current metric and a statistical representation (the "reference") of the sliding window. The statistical representation can either be the mode or the mean of the values in the sliding window.

Note that, if the current frame has been detected as malicious, the metrics representing this frame are discarded from the sliding window to preserve an accurate statistical representation of normal behaviour. As such any attempt to skew the statistics over a period of time would require the initial injection of a frame statistically indistinguishable from the current norm in order to launch the attack. The system works on the assumption that doing this will be very difficult in practice and could be made more difficult if more metrics are considered.

A. Metrics and the manual Assignment of BPA's

The captured files from the monitoring node include all frames transmitted between the AP and the client and any malicious frames from the attacker masquerading to be the AP. From all the collected information, five metrics were identified that if appropriately analysed, could give evidence of an attack. These have been determined after manual off-line analysis of the captured files whilst looking for inconsistencies in the metrics. The chosen metrics are: Received Signal Strength Indication (RSSI), Transmission (or injection) Injection Rate (Rate), 802.11 Frame Sequence Number (Seq), Duration Field or Network Allocation Vector (NAV), Time To Live (TTL).

Regarding the manual assignment method, the beliefs for Attack and Normal are dependent on the distance of the value of each metric in the current frame from the reference. The functions used to select the beliefs were chosen experimentally. Due to space restrictions only belief percentages for the RSSI and Rate metrics are shown in Fig. 1(a). Because the belief in Uncertainty is constant for each metric (0.5 for RSSI and 0.4 for Rate), the belief in Normal (descending graphs) is the "mirror image" of the belief in Attack (ascending graphs). D-S theory states that the sum of beliefs for all hypotheses is equal to 1 [20]. Therefore, given that the belief in Uncertainty is constant, if the belief for the Attack hypothesis increases by a specific amount, the belief in Normal will have to decrease for that same amount to preserve the summation equal to 1.

The general intuition behind the specific choice of beliefs is that the longer the distance from the reference, the higher the belief in the Attack as this indicates a deviation from the normal profile. A deviation from the normal profile may not necessarily be evidence of an attack but when multiple metrics depart from the Normal profile then it is increasingly expected that the frame is malicious. The use of multiple metrics as bodies of evidence reduces the chances of falsely labelling a frame as malicious.

B. Automatic Assignment of BPAs

The principal characteristics of the proposed automatic method are the light weight process of generating a baseline profile of normality; the capability to automatically generate BPAs based on the measured traffic network characteristics; and high detection accuracy with low number of false alarms.

We propose three distinct methodologies for assigning the belief to each hypothesis One method generates the belief in Attack, and a second method generates the belief in Normal. Both work concurrently. Then, based on the belief in Normal and Attack, a third method calculates a readjusted belief for Uncertainty.

Two conditions must be met. Firstly, the number of legal frames should be larger than malicious frames. Generally, normal data is more predominant than malicious data in real network traffic [25]. Secondly, the difference between the metrics of legal and malicious frames must be statistically differentiable and quantifiable.

1) Method to Assign Belief in Attack: The methodology that we propose assigns beliefs in Attack based on two factors, the distance of the current frame from the reference; and frequency of the data. The system first calculates the reference of the n elements in the dataset and the number of times the most repeated value (i.e. mode) appears in the dataset, hereafter referred as Frequency F. Then, the system calculates

the angle α generated by the frequency and the value with the largest distance (D_{max}) from the reference (see Fig. 1(b)). This angle α is used as a reference for the maximum belief in Attack, which is set to 50%. This belief for each of the hypotheses is calculated by dividing 100% by the number of elements in the frame of discernment (in our case 2). The angle α is given by: $a = cos^{-1}\frac{F}{(D_{max}^2+F^2)^{\frac{1}{2}}}$.

For each new incoming frame, the system calculates the angle β generated by F and the distance (D) of this value from the reference. The angle β would be bounded by 0 and α, $0 \leq \beta \leq \alpha$, where $\beta = cos^{-1}\frac{F}{(D^2+F^2)^{\frac{1}{2}}}$. Using a simple linear function, the system assigns the belief in Attack for the angle β generated by the current metric's value.

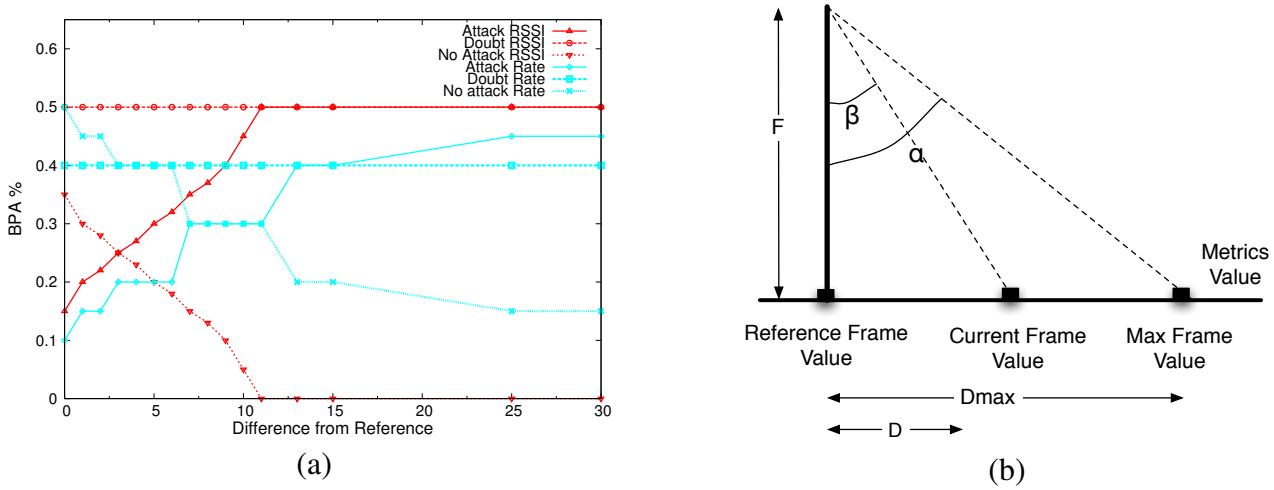


Fig. 1. (a): Manual BPA Functions for the RSSI and Rate metrics. (b): Automatic BPA method for belief in Attack.

2) Method to Assign Belief in Normal: The methodology proposed for assigning beliefs in Normal, is based on the degree of dispersion of the values in the dataset. The system makes use of quartiles, similar to the "box and whisker" method [26], to create classes within the dataset and assigns a fixed belief to each class. The metrics of each new incoming frame are allocated whithin one of the classes. Depending on the class that the current frame is allocated to, the system assigns the belief in Normal.

If the value of the current frame coincides with the median (Me), the belief is 50%. If the value is allocated between the Q_1 and Me, or Q_3 and Me, the belief is 40%. Values between Min and Q_1, or Q_3 and Max will acquire a belief of 30%. The rest of the values will acquire a belief of 15%.

3) Method to Assign Belief in Uncertainty: A provisional value is assigned to Uncertainty using a linear correlation between the belief in Normal and Attack. As mentioned above, the maximum possible belief corresponds to 0.5. So, for calculating the belief in Uncertainty, the larger of both beliefs, Normal and Attack, is adjusted to 50%. For instance, if the belief in Normal and Attack are 0.4 and 0.497, respectively,

the value for Uncertainty would be: $Belief_{Unc.} = 0.5 * 0.4/0.497 = 0.402$.

In this example, the summation of all the beliefs is higher than 1. This breaks one of the conditions of D-S theory: $\sum_{H \subseteq \Theta} m(H) = 1$. Therefore, an adjustment value μ is calculated as follows: $\mu = \frac{X-1}{3}$, where X is the summation of the three beliefs. Continuing with the previous example, $X = 0.4+0.497+0.402 = 1.22$. Then, the adjustment value is $\mu = (1.229 - 1)/3 = 0.099$. Therefore, the beliefs in Normal, Attack and Uncertainty are readjusted to 0.3, 0.397 and 0.303, respectively.

VI. Results

The measurement files of the experiments are available to the general public on the author's website (see footnote on first page). In total five experiments were conducted. The initial experiment did not have any malicious activity in order to evaluate how the algorithms behave in terms of falsely flagging frames as malicious under normal conditions. The three experiments included the MitM attack 01, MitM attack 02 (see section IV-B1), and combinations of attack 01, attack 02 . The final experiment concerned the de-authentication attack.

The evaluation of the results for DR, FP and FN took place off-line. In order to evaluate all four proposed methodologies, the captured files for each experiment were manually analysed in order to find the time instance and the number of malicious frames. After the end of each experiment, the captured files were fed as input to the proposed algorithms for analysis which automatically gives a belief of whether each frame is malicious or not. From there, the results of FP and FN were generated.

For each of the five experiments, four algorithms were tested (manual and automatic with mode and mean as reference) with 32 metric combinations. In order to evaluate the effectiveness of the proposed methodologies, the results from the multi-layer scheme are compared against the same methodology, but utilising fewer metrics. The results are evaluated by constructing the false negative rate $FNR = \frac{FN}{TP+FN}$ (where TP is True Positives), false positive rate $FPR = \frac{FP}{\text{Total captured Frames}}$, and the $DR = \frac{TP}{TP+FN}$.

Due to the volume of results, tables are included only to show the worst cases of FP results for the first three experiments. For the rest of the cases, the results are described textually. For the combination of MitM attack 01 and 02 and De-authentication attack, for easy comparison between the multiple parameters of the experiments, figures are presented that show the DR and FPR on the y-axis for every possible metric combination signified on the x-axis. Note that the FNR is equal to 100% minus the DR ($FNR = 100\% - DR$) and therefore can be read by using the DR column.

TABLE II
FP RATES FOR MANUAL AND AUTOMATIC METHODS FOR NORMAL SCENARIO [WORST CASES]

Metrics	Manual Average FP rate (%)	Manual Mode FP rate (%)	Automatic Average FP rate (%)	Automatic Mode FP rate (%)
RSSI	0	0	56.461	56.461
Seq	0.490	0.490	37.076	37.344
RSSI,Seq	0.490	0.490	20.365	7.040
TTL	0	0	72.504	81.283
RSSI,TTL	0	0.534	57.308	28.475
Seq,TTL	0.490	0.490	36.764	18.181
RSSI,Seq,TTL	6.818	0	24.955	15.151

A. Normal Scenario

In this scenario no malicious frames were injected. Considering all possible metric combinations, in most cases the manual methods produce around 0.5% FP. For the automatic method, the cases where FP are very high are only those that exclude Rate or NAV as seen in Table II. Notably, when other metrics are utilised in conjunction to RSSI, Seq and TTL, such as [RSSI, Rate, TTL] or [RSSI, NAV, TTL], the FP results are significantly improved to 3.4% and 3.9% for the average and mode methods respectively. The rest of the cases not shown in Table II present FP less than 3%; in most cases less than 0.7%. Note that for all four methodologies, there are no FP results when using all five metrics which signifies the importance of combining multiple beliefs.

B. Attack Scenarios

1) Attack 01: In this scenario there were 11 distinct malicious frames launched during the victim's web browsing session. As before, the combination of all five metrics, regardless of the methodology, achieved 100% DR with 0 FP. For the automatic methods there are no false negative results in contrast to the manual methods. However, this happens at the expense of increased FP when using RSSI, Seq and TTL metrics (see Table III for worst cases). For the cases not shown in Table III, FP results are either 0% for the manual methods or around 0% (and always less than 2.7%) for the automatic methods.

Both manual methods have 100% FN when using either just the RSSI metric or just TTL. Interestingly, the result of their combination is 100% DR. Furthermore, for the manual mode method, the metric combinations [Rate, TTL] and [NAV, Seq, TTL] produce around 18% FN and combinations [NAV, TTL] and [Seq, TTL] produce around 36% FN.

TABLE III
FP RATES FOR MANUAL AND AUTOMATIC METHODS FOR ATTACK 01 SCENARIO [WORST CASES]

Metrics	Manual Average FP rate (%)	Manual Mode FP rate (%)	Automatic Average FP rate (%)	Automatic Mode FP rate (%)
RSSI	0	100	31.640	31.640
Seq	0.390	0.390	32.421	32.421
RSSI,Seq	0.390	0.390	24.218	11.718
TTL	0	0	77.343	75
RSSI,TTL	0	0	33.593	19.531
Seq,TTL	0.390	0.390	58.203	18.75
RSSI,Seq,TTL	0	0	23.437	8.984

2) Attack 02: This experiment included 995 distinct malicious frames. For the manual methods, using all five metrics simultaneously performs best in comparison to other combinations of metrics, apart for when just the Rate and NAV metrics are used independently or in combination. Furthermore, in that particular experiment, for the manual methods, the TTL metric is mostly associated with much lower performance due to very high FN results. As in the previous case, both manual methods, produce 100% FN when using either just the RSSI metric or just the TTL. Table V shows the FN results for the manual methods for metric combinations without the use of TTL.

For the automatic methods, the FN results are very low but, as before, at the expense of high FP results (as seen in Table IV). In addition to the results in Table IV, the cases of [Rate, TTL] and [NAV, TTL] present around 14% FP and around 29% FN for the average method and 3.2% FN for the mode. For the cases not shown in Table IV, FP results range from equal to or around 0% (for most combinations) up to 1.9% for the average method and up to 2% for the mode method.

Regarding all five metrics in combination, the automatic methods perform nearly perfectly (DR = 100% and FP=0.007%) whilst the manual methods are slightly less than perfect (FN=0.1% for manual Average and FN=0.8% for manual mode).

3) Combination of Attack 01 - Attack 02: For the combined Attack 01 - Attack 02 experiment there were 114 distinct malicious frames injected. For both the manual and the automatic methods, when using all metrics, the results are perfect (i.e. DR of 100%, and FP equal to 0%). However, in the case of Automatic Average method the FP are 0.038%. Results for the combined attack are shown in Fig. 2.

In general, the automatic methods provide for less false negative results in comparison to the manual methods for various combinations of metrics but at the expense of increased FP. These FP occur when using the RSSI, Seq and TTL metrics solely or in combinations among these particular metrics but the

TABLE IV
FP RATES FOR MANUAL AND AUTOMATIC METHODS FOR ATTACK 02 SCENARIO [WORST CASES]

Metrics	Manual Average FP rate (%)	Manual Mode FP rate (%)	Automatic Average FP rate (%)	Automatic Mode FP rate (%)
RSSI	0	0	54.544	54.544
Seq	2.820	2.867	69.989	70.067
RSSI,Seq	2.852	2.867	60.531	10.037
TTL	0	0	84.688	90.205
RSSI,TTL	7.545	0.227	85.3	10.633
Seq,TTL	8.823	1.073	34.218	12.161
RSSI,Seq,TTL	0.728	0.203	27.550	7.208

TABLE V
FN RATES FOR MANUAL METHODS FOR ATTACK 02 SCENARIO (NOT INCLUDING TTL COMBINATIONS)

Metrics	Manual Average FN rate (%)	Manual Mode FN rate (%)
Seq	12.361	10.050
RSSI, Seq	1.407	0
NAV, Seq	3.517	3.316

performance is corrected when adding additional metrics.

In both manual methods, the RSSI and TTL metrics, when used on their own, fail to detect any attack but the result of their combination is around 80 % DR. This is another example demonstrating the benefits of fusing beliefs among metrics.

There are cases where the use of the single metrics Rate and NAV can surpass the performance of dual or triple metric combinations regardless of the methodology. In fact, the use of Rate results in perfect detection, with 100% of DR and 0% of FP. The dominance of this metric in such cases can be explained due to the injection attacking tools. These tools inject frames at a fixed rate of 1 Mbps because the chances of success of the attack are greater. This makes Rate a crucial metric to consider for detecting injections of attack frames.

It could be argued that such an attack could easily be detected by simply looking at one particular metric (Rate in this case). However, this is true if only that specific attack is expected and the identifying metric is already known. There are other attacks, as we will show below, where that particular metric is useless for detecting the attack. The purpose of choosing both the Airpwn and De-authentication attacks (see Section VI-D) in this work is to demonstrate the advantages of the concept of fusing metrics rather than detecting the attack per se.

Assuming injection-based attacking tools are enhanced in the future and manage to adapt their rate to that of legal frames, the presented methodologies would still perform with high DR and low numbers of FP and FN when ignoring the Rate metric. This can be seen in the metric combinations that do not consider Rate (Fig. 2).

There could also be cases, as happens in the case of Fig. 2d when using a subset of metrics [Rate, Seq], where the addition of an extra metric (RSSI) leads to FPs. RSSI is known to be a volatile metric [27]. In this particular example, for some frames, RSSI suddenly increases by 10 dBm in comparison to the historical mode and this deviates from the expected reference value. The other metrics, Rate and Seq, even though their belief is stronger for the Normal hypothesis, may not counter balance the heavily skewed belief towards Attack given by RSSI. Similar phenomena can occur with different metric combinations. In such cases, using all five metrics together significantly remedies this issue as seen in all our considered scenarios.

C. Evaluation of Time to Detect an Attack

For an on-line process, it takes on average 7812 μsec to flag a frame as malicious after its capture. This time incorporates 7727 μsec for the DS algorithm. However, it should be noted that in an off-line mode, where our tool reads frames from a file, the DS algorithm requires just 40 μsec to run. This is because, in the on-line mode, the capturing process involves CPU interrupts for dealing with the arrival of frames from the wireless medium.

The above results correspond to a user space implementation of the code when run on an Intel Core i5 at 1.7 GHz CPU, without particular focus on speed optimisation. Furthermore, there are no dropped frames reported from the implementation even when utilising a 54Mbps rate for the AP.

D. De-authentication attack

There were 128 malicious frames injected when launching this type of attack. The manual mode method performs worst as it does not detect any attack. The manual average method, seen in Fig. 3(a), has a single case [RSSI, Seq] that performs perfectly. The remaining cases have high FP results and low DR.

The automatic mode method performs well with the triplet of [RSSI, NAV, Seq]. This combination gives 98.4% DR and 3.9% of FP. The automatic average method, seen in Fig. 3(b), offers the best results overall when using all four metrics with 100% DR and 3.9% FP.

In contrast to the experiments with MitM attack, the metric Rate is ineffective in detecting the de-authentication attack. This is because most of the management frames, both legal and malicious, are transmitted at a fixed rate of 1 Mbps and therefore a malicious frame is statistically indistinguishable from the normal baseline when judged only on the Rate metric.

It should be noted that the Automatic average method detects all malicious injected frames from the very first malicious frame. In contrast, other methodologies count the number or rate of deauthentication frames and if they exceed a specific threshold, then raise an alarm. This means that in the latter case, the malicious frames have already reached the victim and the effect can not be stopped even when detected but in our proposed method, the attack could be stopped as it can detect the attack at its onset.

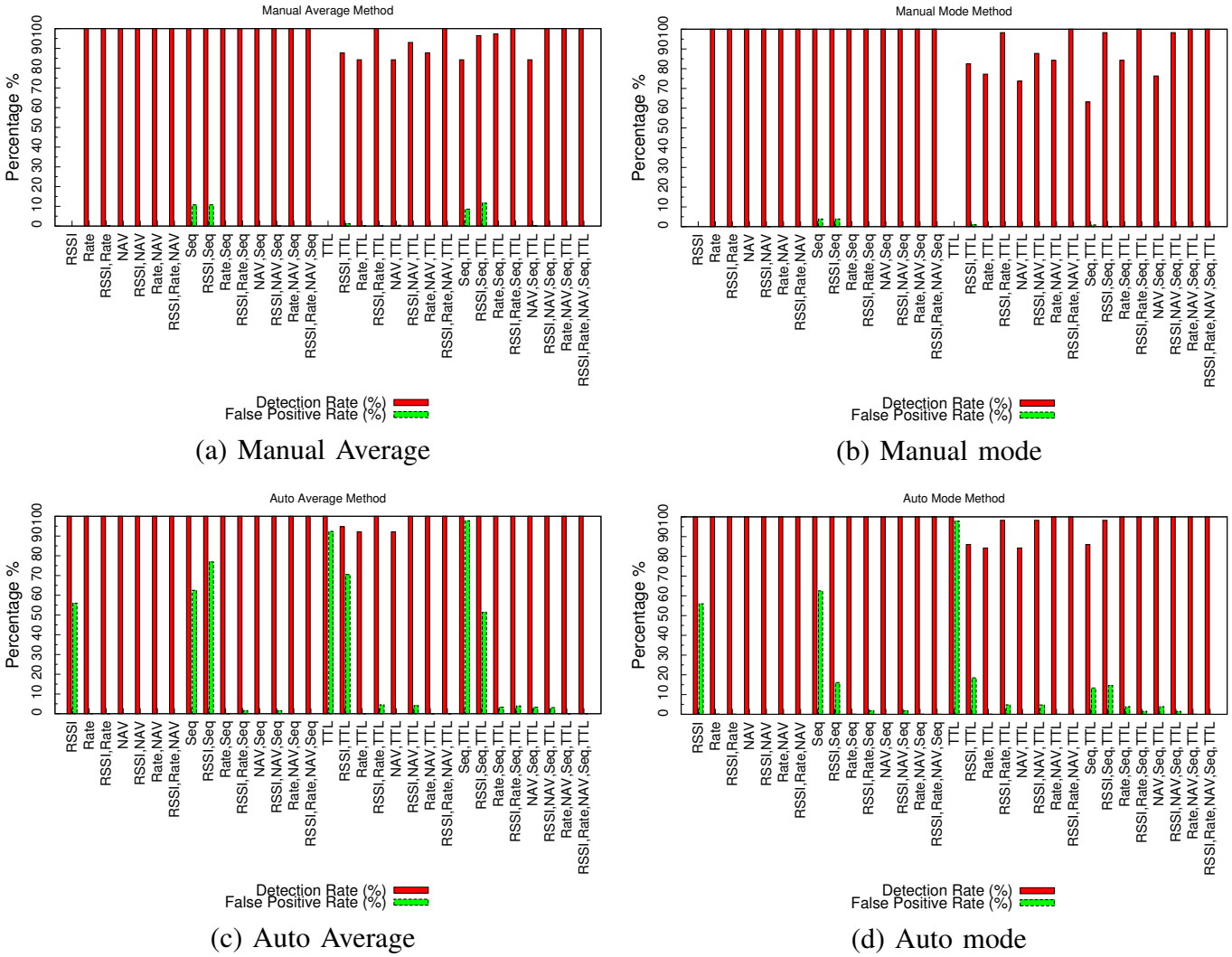
VII. Conclusions and Future Work

The authors have proposed a new approach for detecting wireless network attacks, involving the combination of beliefs from metrics across multiple layers of observation in order to produce a collective decision on whether an attack takes place or not. The beliefs are combined with the Dempster-Shafer theory of evidence.

The combination of beliefs from multiple metrics outperforms the efficiency and accuracy of single metrics. In addition, the authors investigate automating the process of assigning beliefs for each metric. In contrast to the conventional methods of experimentally calibrating the probability of a frame being malicious, this work also presents an automatic, light weight methodology for assigning beliefs without requiring manual intervention from an administrator. This advantage makes the deployment of such an attack detection system much easier and capable of adapting to the characteristics of the underlying network.

The choice of MitM and a De-authentication attacks was made to demonstrate the robustness of the methodologies irrespective of the potential weaknesses of each attack. For example, the Rate could be a metric that is dominant when examining MitM attacks but is completely ineffective when trying to detect a de-authentication attack. Finally, all possible combinations of metrics were examined, varying from single metrics up to all five available metrics.

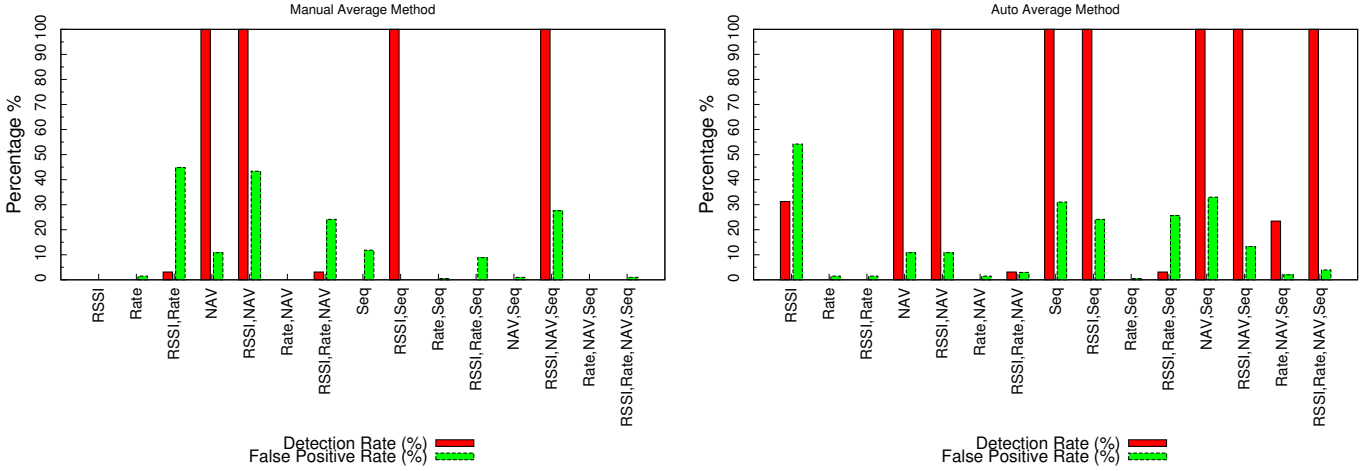
The comparative results between automatic and manual attack detection mechanisms shows excellent performance when using all metrics simultaneously. When utilising all possible five metrics for the MitM attack, the performance of both methods reach perfect detection in most cases.



(a) Manual Average (b) Manual mode

(c) Auto Average (d) Auto mode

Fig. 2. Airpwn Attack 01 - Attack 02: Detection Rate and False Positive Rate results for Manual (a,b) and Automatic (c,d) methods for all possible metric combinations.



(a) Manual Average (b) Auto Average

Fig. 3. Deauthentication Attack: Results for Manual (a) and Automatic (b) methods using Average as reference for all possible metric combinations

When evaluating the de-authentication attack, the automatic average method was the only efficient methodology to detect such an attack and had a 100% DR and just 3.940% FP. In contrast to conventional methods, our methodology detects the attack on its onset rather than aggregating malicious de-authentication frames and comparing against a threshold in order to flag as an attack. The manual methodologies fail to detect the de-authentication attacks. This highlights the need for dynamically assigning beliefs for an attack rather than using general purpose predefined BPAs.

The automatic methodology offers excellent results especially when considering the easiness of deployment that comes with it. In contrast with the manual methodology, an administrator does not need to painstakingly repeatedly adjust the beliefs for the D-S algorithm, trying to experimentally optimise the belief values for each metric. This is especially helpful when combining the beliefs of a high number of metrics as in that case the difficulty of experimentally optimising the belief values for each metric increases significantly.

As for future work, an important issue to consider is the investigation of further wireless attacks and the off-line selection of appropriate metrics using data mining techniques.

REFERENCES

[1] F.J. Aparicio-Navarro, K.G. Kyriakopoulos, and D.J. Parish. A multi-layer data fusion system for wi-fi attack detection using automatic belief assignment. In *The World Congress on Internet Security (WorldCIS 2012)*, Guelph, Ontario, Canada, 10-12 June 2012. IEEE.

[2] K.G. Kyriakopoulos, F.J. Aparicio-Navarro, and D.J. Parish. Fusing multi-layer metrics for detecting security attacks in 802.11 networks. In *Wireless Telecommunications Symposium (WTS), 2011*, pages 1–6. IEEE, 2011.

[3] C. Siaterlis and B. Maglaris. Towards multisensor data fusion for dos detection. In *Proceedings of the 2004 ACM symposium on Applied computing*, pages 439–446. ACM, 2004.

[4] D. Yu and D. Frincke. Alert confidence fusion in intrusion detection systems with extended dempster-shafer theory. In *Proceedings of the 43rd annual Southeast regional conference-Volume 2*, pages 142–147. ACM, 2005.

[5] F.J. Aparicio-Navarro, K.G. Kyriakopoulos, and D.J. Parish. An on-line wireless attack detection system using multi-layer data fusion. In *Measurements and Networking Proceedings (M&N), 2011 IEEE International Workshop on*, pages 1–5. IEEE, 2011.

[6] W. Zhou, A. Marshall, and Q. Gu. A novel classification scheme for 802.11 wlan active attacking traffic patterns. In *Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE*, volume 2, pages 623–628. IEEE, 2006.

[7] J. Bellardo and S. Savage. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In *Proceedings of the USENIX Security Symposium*, pages 15–28, 2003.

[8] K. Bicakci and B. Tavli. Denial-of-service attacks and countermeasures in ieee 802.11 wireless networks. *Computer Standards & Interfaces*, 31(5):931–941, 2009.

[9] Y. Sheng, K. Tan, U. Deshpande, B. Vance, H. Yin, C. McDonald, T. Henderson, G. Chen, D. Kotz, A. Campbell, et al. Map: A scalable measurement infrastructure for securing 802.11 wireless networks. 2008.

[10] A. Vartak, S. Ahmad, and KN Gopinath. An experimental evaluation of over-the-air (ota) wireless intrusion prevention techniques. In *Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on*, pages 1–7. IEEE, 2007.

[11] G. Chen, H. Yao, and Z. Wang. An intelligent wlan intrusion prevention system based on signature detection and plan recognition. In *Future Networks, 2010. ICFN'10. Second International Conference on*, pages 168–172. IEEE, 2010.

[12] X. Wang, J.S. Wong, F. Stanley, and S. Basu. Cross-layer based anomaly detection in wireless mesh networks. In *Applications and the Internet, 2009. SAINT'09. Ninth Annual International Symposium on*, pages 9–15. IEEE, 2009.

[13] G. Thamilarasu, S. Mishra, and R. Sridhar. A cross-layer approach to detect jamming attacks in wireless ad hoc networks. In *Military Communications Conference, 2006.*, pages 1–7. IEEE, 2007.

[14] T.M. Chen and V. Venkataramanan. Dempster-shafer theory for intrusion detection in ad hoc networks. *Internet Computing, IEEE*, 9(6):35–41, 2005.

[15] V. Chatzigiannakis, G. Androulidakis, K. Pelechrinis, S. Papavassiliou, and V. Maglaris. Data fusion algorithms for network anomaly detection: classification and evaluation. In *Third International Conference on Networking and Services*, page 50. IEEE, ICNS, 2008.

[16] A.G. Fragkiadakis, V.A. Siris, and A.P. Traganitis. Effective and robust detection of jamming attacks. In *Future Network and MobileSummit 2010*. IIMC International Information Management Corporation, 2010.

[17] Aqila Dissanayake. Literature review and survey: Intrusion detection using the dempster-shafer theory, 2008.

[18] JR Boston. A signal detection system based on dempster-shafer theory and comparison to fuzzy detection. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 30(1):45–51, 2000.

[19] Q. Chen and U. Aickelin. Anomaly detection using the dempster-shafer method. In *Proceedings of the 2006 International Conference on Data Mining, DMIN 2006*, pages pp. 232–240, 2006.

[20] Glenn Shafer. *A Mathematical Theory of Evidence*. Princeton University Press, 1976.

[21] Backtrack linux website. http://www.backtrack-linux.org.

[22] Airpwn sourceforge website. http://airpwn.sourceforge.net/Airpwn.html.

[23] M. Raya, J.P. Hubaux, and I. Aad. Domino: a system to detect greedy behavior in ieee 802.11 hotspots. In *Proceedings of the 2nd international conference on Mobile systems, applications, and services*, pages 84–97. ACM, 2004.

[24] F.J. Aparicio-Navarro, K Kyriakopoulos, and D.J. Parish. An automatic and self-adaptive multi-layer data fusion system for wifi attack detection. In *International Journal of Internet Technology and Secured Transactions (IJITST)*. Inderscience, 2013. To be published.

[25] C. Thomas and N. Balakrishnan. Improvement in minority attack detection with skewness in network traffic. In *Proceedings of SPIE, the International Society for Optical Engineering*, pages 69730N–1. Society of Photo-Optical Instrumentation Engineers, 2008.

[26] C.C. Tuan, Y.C. Wu, W.S. Chang, and W.T. Huang. Fault tolerance by quartile method in wireless sensor and actor networks. In *Complex, Intelligent and Software Intensive Systems (CISIS), 2010 International Conference on*, pages 758–763. IEEE, 2010.

[27] Rupinder Singh Gill. *Intrusion Detection Techniques in Wireless Local Area Networks*. PhD thesis, Information Security Institute Faculty of Information Technology Queensland University of Technology, June 2009.