A multi-layer data fusion system for Wi-Fi attack detection using automatic belief assignment

This item was submitted to Loughborough University's Institutional Repository by the/an author.

Citation: APARICIO-NAVARRO, F.J., KYRIAKOPOULOS, K.G. and PARISH, D.J., 2012. A multi-layer data fusion system for Wi-Fi attack detection using automatic belief assignment. World Congress on Internet Security (WorldCIS), Guelph, Ontario, Canada, June 10-12, University of Guelph, Ontario, Canada, pp.45-50.

Additional Information:

- © 2012 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Metadata Record: https://dspace.lboro.ac.uk/2134/10305

Version: Accepted for publication

Publisher: © IEEE

Please cite the published version.
This item was submitted to Loughborough’s Institutional Repository (https://dspace.lboro.ac.uk/) by the author and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to: http://creativecommons.org/licenses/by-nc-nd/2.5/
A Multi-Layer Data Fusion System for Wi-Fi Attack Detection Using Automatic Belief Assignment

Francisco J. Aparicio-Navarro, Konstantinos G. Kyriakopoulos, David J. Parish
School of Electronic, Electrical and System Engineering
Loughborough University
Loughborough, LE11 3TU, U.K.
e-mail: {elfja2, elkk, d.j.parish}@lboro.ac.uk

Abstract—Wireless networks are increasingly becoming susceptible to more sophisticated threats. An attacker may spoof the identity of legitimate users before implementing more serious attacks. Most of the current Intrusion Detection Systems (IDS) that employ multi-layer approach to help towards mitigating network attacks, offer high detection accuracy rate and low numbers of false alarms. Dempster-Shafer theory has been used with the purpose of combining beliefs of different metric measurements across multiple layers. However, an important step to be investigated remains open; this is to find an automatic and self-adaptive process of Basic Probability Assignment (BPA). This paper describes a novel BPA methodology able to automatically adapt its detection capabilities to the current measured characteristics, with a light weight process of generating a baseline profile of normal utilisation and without intervention from the IDS administrator. We have developed a multi-layer based application able to classify individual network frames as normal or malicious.

Keywords—Basic probability assignment; Datafusion; Dempster-Shafer; Multi-layer measurements; Spoofing attacks; WiFi

I. INTRODUCTION

MAC layer spoofing attacks are among the most serious threats to wireless networks [1]. There exist numerous attacks, ranging from Denial-of-Service (DoS) to session hijacking that can be implemented because an attacker may masquerade itself as a legal user [2]. In the last few years there has been an increasing interest in using detection methodologies to identify spoofing attacks in IEEE 802.11 networks [2, 9, 10]. The implementation of wireless network monitoring tools, such as Intrusion Detection Systems (IDSs), is fundamental in security infrastructures in order to provide another level of defence for IEEE 802.11 networks.

Although there are cases in which an algorithm that utilises a single metric approach might give positive results, the true status of a network is rarely accurately detectable by examining a single metric from one network layer of the TCP/IP stack. As many researchers have previously demonstrated [3-5], the combined use of multiple metrics from the same or different network layers may result in higher detection accuracy rate with lower numbers of False Negatives (FN) and False Positive (FP). Hence, utilising a multi-layer approach may help towards automating the overall process of detecting and mitigating wireless network attacks.

Data fusion can be defined as the process of collecting information from multiple and heterogeneous sources, and combining them towards obtaining a more accurate final result [5]. Dempster-Shafer (D-S) theory of evidence is a good candidate for this purpose. D-S has been previously used in the intrusion detection field to enhance the detection accuracy [5-7]. Despite having been proven as a powerful and efficient technique, a very important step to be investigated remains open in D-S theory. This is 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 on IDS is to automatically determine the beliefs from the network measurements [8].

There exist multiple ways of assigning probabilities to each of the hypotheses in D-S theory, ranging from data mining techniques to empirical approaches. However, few of them could be used off-the-shelf without a prior thorough training or fine tuning period.

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 from an IDS administrator. We have developed a multi-layer based application, written in C language, able to classify network frames as normal or malicious. The proposed method only requires a light weight process of generating a baseline profile of normal utilisation, in order to generate high intrusion detection accuracy and low number of false alarms.

The aim of our methodology requires the system to be computationally low cost, scalable and applicable to other wireless technologies. The methodology has been tested with two different types of attack, a Man-in-the-Middle (MitM) attack at the physical layer and a Deauthentication attack, both requiring the prior spoofing of a legal user identity.

The paper is organised as follows. In section II, the most relevant work is reviewed. A brief description of the D-S is presented in section III. In section IV, the proposed algorithms for belief assignment are explained. The methodology, tested, and attack scenarios are presented in section V. In section VI, the obtained results are discussed. Finally, conclusions are given in section VII.

II. RELATED WORK

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 [12]. The authors

This work has been funded by the Engineering and Physical Sciences Research Council (EPSRC).
present a comparative study between D-S theory and Bayesian inference as data fusion algorithms. In [4], the authors describe a cross-layer methodology to increase the performance of an anomaly IDS, detecting DoS attacks. Similar to our work, they use a sliding window scheme and compare the efficiency of a cross-layer approach against a single layer approach. However, the data fusion is not carried out using D-S theory. The above work uses real WiFi traffic.

In [5], the authors present a prototype for Distributed DoS detection over wired link, based on D-S theory. The system, periodically, fuses the knowledge collected from different sensors within the network, in order to infer the current state of the monitored network.

The authors in [7] present and evaluate an IDS for detecting DoS attacks by seeking changes in a single metric, the Signal-to-Noise Ratio. The authors use the D-S theory to fuse the information from different nodes running two different local algorithms, Single Threshold and Cumulative sum. The experiments in this work were also carried out in a real IEEE 802.11 testbed.

Among all the works 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, [13] proposes two different ways of assigning belief probabilities, for two different datasets. In the first case, their method calculates a threshold based on the length of the dataset, and then utilises that threshold and fixed functions to assign the belief probabilities. In the second case, a scaled approach with pre-defined beliefs is used.

The authors in [5] express the BPA as three simple and fixed functions. Again, the BPA process is based on previous experiments and subjectivity of the IDS administrator. As the three functions have a fixed shape, this method might be inadequate for automatic and self-adaptive IDSs.

The methodology employed by [8] 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.

The authors in [7] seek changes in the SNR. The value of this metric is measured over both a small time window and a large time window. Based on the measured metrics in each time window, their system generates the BPAs through the use of a linear function.

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 referred works investigate methods to find an automatic and self-adaptive process of BPA, and few of them could be used off-the-shelf without a previous training or fine tuning period.

On one hand, systems that make use of data mining techniques for BPA require the gathering of large amounts of data traffic, processing it and complete a training period before being able to perform intrusion detection tasks. These systems are unable to automatically adapt to changes in the network traffic behaviour in real-time. On the other hand, systems which have been empirically assigned fixed probability values by the IDS administrator, or systems that employ fixed functions to assign the belief probabilities are unable to automatically adjust to changes in the network traffic behaviour, without the intervention of the IDS administrator.

In this work, we propose a network-based anomaly detection system, which uses a novel statistical-based BPA assignment scheme methodology able to automatically adapt its detection capabilities to the current characteristics of the different metrics of the wireless network, without intervention for an IDS administrator.

III. DEMPSTER-SHAFER THEORY

D-S theory of evidence is a mathematical discipline that combines evidence of information from multiple and heterogeneous events in order to calculate the belief of occurrence of another event. We have presented a more detailed description of D-S theory in our previous work [11], along with a comprehensible practical example of D-S.

D-S starts by assuming a Frame of Discernment $\Theta = \{\theta_1, \theta_2, \ldots, \theta_n\}$, the finite set of all possible mutually exclusive propositions about some problem domain. With regards to this work, the frame of discernment is comprised of $A = \text{Attack}$ and $N = \text{Normal}$. Assuming $\Theta$ has two outcomes $\{A, N\}$, the total number of subsets of $\Theta$, defined by the number of hypotheses that it composes, is $2^\Theta = \{A, N, \{A\}, \{N\}, \emptyset\}$.

Each hypothesis from $\Theta$ receives from an observer a probability or belief within $[0, 1]$. This is known as the Basic Probability Assignment (BPA). The function $m(A)$ is defined as $A$’s basic probability number. It describes the measure of belief that is committed exactly to hypothesis $A$.

Let $m_1$ and $m_2$ be the BPAs from observer 1 and 2 respectively. Their orthogonal sum, $m = m_1 \oplus m_2$, is called Dempster’s rule of combination, and is defined as

$$m(A) = \frac{\sum_{X \subseteq A} m_1(X) \cdot m_2(Y)}{1 - \sum_{X \cap Y = \emptyset} m_1(X) \cdot m_2(Y)} \quad \forall A \neq \emptyset$$

Among different data fusion methods, the D-S theory of evidence has been chosen in this work for three main reasons. Firstly, D-S is able to combine evidence from multiple and heterogeneous sources. Second, D-S is suitable for detecting previously unseen attacks because it does not require a priori knowledge. Finally, and more importantly, the D-S provides the ability of managing and assigning probability to $\{A|N\} = \text{Uncertainty}$, which allows tackling a large range of problems.

The authors in [5, 12] present a comparative study of different data fusion methods. This work concludes that D-S theory is more promising than Bayesian inference. Bayesian approach provides a powerful method to provide final conclusions. However, this method requires complete knowledge of the conditional probabilities of all of the used metrics and specification of the a priori probability distribution of the different hypotheses. This last requirement is unfeasible in many applications [18]. Additionally, the Bayesian method does not allow allocation of probability to Uncertainty but only to the hypotheses Normal or Attack [13].

IV. BELIEF GENERATOR MECHANISMS

The principal distinctive features of the proposed method are the light profiling process, the capability to automatically generate BPA based on the measured traffic network characteristics, and the high detection accuracy and low number of
false alarms that it produces. The dataset used for profiling the system is as little as 20 network frames.

![Figure 1. Sliding window scheme.](image)

We propose three different methodologies for assigning the belief to each hypothesis of \( \Theta, 2^\Theta = \{\text{Attack, Normal, Uncertainty}, \emptyset\} \). One method generates the belief in \( \text{Attack} \), and a second method generates the belief in \( \text{Normal} \). Both work concurrently. Then, based on the belief in \( \text{Normal} \) and \( \text{Attack} \), a third method calculates a balanced belief in \( \text{Uncertainty} \).

Two conditions must be assured. First, the number of legal frames must be larger than the malicious frames. Normal data is more predominant than malicious data in real network traffic [14]. Second, the difference between metrics of legal and malicious frames must be statistically differentiable and quantifiable. Regarding the first assumption, we have tested scenarios in which the proposed system performs with high detection rate even if there are malicious frames in the initial profiling set.

Before being able to identify any attack, the IDSs need to define what is considered as normal traffic. In the case where the majority of frames in the initial window are malicious, the detection mechanism would misclassify. A longer window would prevent this situation as it would include a larger proportion of legal frames and the statistics would average out to represent a normal profile. However, there is a trade off between the lightness of profiling and the chances of misclassification.

The proposed system operates on a sliding window scheme using incoming frames from the legal client. The content of the \( n \) frames within the sliding window composes the profiling dataset of the system, every time a new frame is analysed. For each new incoming frame, different metrics are extracted. The system has one sliding window for each used metric. The statistical mean of the metrics is used as a reference of normality for the method to assign the beliefs proposed below.

The length \( n \) of the sliding window will influence the overall detection performance of the system. In our experiments, we have used \( n = 20 \) frames for generating the mean. We have experimentally proved that 20 frames are appropriate to make an accurate detection. However, due to space restrictions the results are not presented in this work.

In order to avoid malicious frames altering the reference of normality, the system slides the window only if the current analysed frame has been classified as legal. Otherwise, the sliding window stays static, drops the frame classified as malicious and replaces the last slot in the sliding window with the next incoming frame. Fig.1 represents an example in which the 20\textsuperscript{th} frame has been classified as malicious and the sliding window stays static, only replacing the malicious frame.

\section{Method to Assign Belief in Attack}

The methodology that we propose assigns beliefs in \( \text{Attack} \) based on two factors, the Euclidean distance of the current frame from the mean, and frequency of the data. The system calculates an angle \( \alpha \) with the distance and the frequency, in order to correlate both factors.

Let us consider a dataset of length \( n = 20 \). The system calculates the highest number of times that a metric is repeated, or frequency (\( F \)), for the \( n \) elements in the dataset, and the mean. Then, the system calculates the angle \( \alpha \) generated by the frequency and the value with the largest Euclidean distance (\( D_{\text{max}} \)) from the mean, as represented in Fig.2. This angle \( \alpha \) represents the maximum possible belief in \( \text{Attack} \).

For each new incoming frame, the system calculates the angle \( \beta \) generated by \( F \) and the distance (\( D \)) of this value from the mean. The angle \( \beta \) would be bounded by 0 and \( \alpha \), \( 0 \leq \beta \leq \alpha \).

Due to the way D-S theory and the BPA are assigned in our methodology, the maximum possible belief in both, \( \text{Normal} \) and \( \text{Attack} \), is set to 50%.

\begin{equation}
\beta = \cos^{-1}\left(\frac{F}{(D^2+F^2)^{\frac{1}{2}}}\right)
\end{equation}

Using a simple linear function, the system assigns the belief in \( \text{Attack} \). The minimum belief in \( \text{Attack} \), 0\%, is defined by the angle 0 radians.

\section{Method to Assign Belief in Normal}

The methodology that we propose assigns beliefs in \( \text{Normal} \), based on the degree of dispersion of the values in the dataset. The system makes use of quartiles to create classes within the dataset and assigns a fixed belief to each of class.

Let us consider a dataset of length \( n = 20 \), sorted in an ascending way. From this sorted dataset, the first quartile (\( Q_1 \)) will define the boundary for the lower 25\% of the data, the second quartile, or median (\( Me \)), will define the boundary for the 50\% of the data, and the third quartile (\( Q_3 \)) will define the boundary for the lower 75\% of the data.

Similar to the process used with the method ‘box and whisker’ [15], the \( Min \) and \( Max \) values are respectively calculated through the following equations:

\begin{equation}
Min = Q_1 - 1.5 \times IQR
\end{equation}

\begin{equation}
Max = Q_3 + 1.5 \times IQR
\end{equation}

whereas, the Interquartile Range (\( IQR \)) is the difference between \( Q_3 \) and \( Q_1 \).

![Figure 2. BPA method for belief in Attack.](image)
The metrics of each new incoming frame is allocated within one of the classes. Depending on the class that the current frame is allocated to, the system assigns the belief in Normal.

Fig.3 illustrates the different classes and the belief value associated to each of them. If the value of current frame coincides with Me, the belief is 50%. If the value is allocated between the Q₁ and Me, or Q₃ and Me, the belief in Normal is 40%. Values between Min and Q₁, or Q₃ and Max will acquire belief of 30%. The rest of the values will acquire belief of 15% in Normal.

C. Method to Assign Belief in Uncertainty

Based on the outcome of the two previous methods, the proposed methodology assigns beliefs in Uncertainty. The Uncertainty is considered in this work as an adjustment parameter.

The outcome of the two previous methods could provide four different conclusions: 1) High belief in Attack and high belief in Normal. 2) Low belief in Attack and high belief in Normal. 3) High belief in Attack and low belief in Normal. 4) Low belief in Attack and belief in Normal. For the cases 2 and 3, both methods have reached similar conclusions. Hence, it is expected that the belief in Uncertainty must be low. In contrast, in the cases 1 and 4, both methods have reached contradictory conclusions, therefore the expected belief in Uncertainty must be high.

We propose the following method for assigning the belief in Uncertainty. First, 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 in the definition of BPA by the D-S theory: \( \sum_{A \in m} (A) = 1 \)

Therefore, an adjustment value \( \mu \) is calculated as follows:

\[
\mu = (X - 1)/3
\]

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.

V. SYSTEM METHODOLOGY

For the purpose of this work, we have tested our proposed approach in an IEEE 802.11 network composed of four different parties. These are an Access Point (AP), a monitoring node utilising the TShark [17] software for collecting frames, an attacker, and a client associated with the AP, accessing various websites hosted on the Internet across different geographical locations. The fact that the attacker was placed very close to the AP, around 1.5 meters away, may degrade the detection accuracy. The monitoring node is responsible for performing the proposed intrusion detection. When the monitoring node captures any frame destined to the client, TShark identifies and isolates the respective metrics of each frame. Then, the gathered dataset is passed to the data fusion process to be analysed. The monitoring node and the attacker were running Linux and all the devices except from the Linksys WRT54GL AP used the Atheros chipset in their wireless cards.

A. Metrics

We have generated our own IEEE 802.11 dataset for the development and assessment of this work. The captured frames are stored in pcap format. Among all the available metrics, four have been experimentally selected as the most appropriate for detecting the attacks. These are the Received Signal Strength Indication (RSSI) at the PHY layer, the Injection Rate and the Network Allocation Vector (NAV) value at the MAC layer, and the Time To Live (TTL) value at the Network layer.

Due to the fact that management and control frames include only information from the PHY and MAC layers in which TTL is not included, in the deauthentication experiments TTL has been replaced by the Delta Time (ΔTime) value. The ΔTime is defined as the time difference between two consecutive frames.

B. Attacks Description

1) Man-in-the-Middle Attack

The presented methodology has been tested with two different types of MitM attacks at the PHY layer. The MitM attacks were implemented by the Airpwn tool. Firstly, Airpwn spoofs the AP MAC address. Then, it listens for legal requests from the client and injects its own crafted HTML code. In the first type (Attack01), the attacker replaces the whole content of the website. In the second type (Attack02) the attacker replaces only the images in the website. Both could cause harm of varying severity, i.e. redirect the client to a phishing website.

2) Deauthentication Attack

Another type of attack that has been investigated is the deauthentication of wireless clients from the legal AP. This type of attack is commonly utilised in DoS attacks but consists also the first step for breaking into WPA2 encrypted wireless networks. In the latter case, the attacker injects a few spoofed deauthentication frames with the purpose of forcing the client to re-establish a connection with the AP. At a later stage and off-line, the attacker could succeed in cracking WPA2 by applying brute force or dictionary attack techniques. The suite of tools used to implement this attack is Aircrack.

The detection of the deauthentication attack was possible just by using management and control frames for two reasons. Firstly, deauthentication attacks are highly correlated with information in the management frames. Furthermore, because the network was encrypted with WPA2, and with the assumption that the monitor node does not have the key, it was not possible or necessary to retrieve information above the MAC layer.

VI. RESULTS

In order to evaluate the effectiveness of the proposed methodology, the results from the multi-layer scheme are compared...
against the same methodology, but utilising fewer metrics. All cases have been evaluated with the same gathered dataset.

The results are evaluated by comparing the FN, FP and the Detection Rate (DR). These are:

\[
DR = \frac{TP}{TP + FN} \tag{6}
\]

\[
FN = \frac{FN}{TP + FN} \tag{7}
\]

\[
FP = \frac{FP}{TP + FP + TN + FN} \tag{8}
\]

Also, IDSs are commonly evaluated by the Overall Success Rate (OSR) and the F-Score [16]. OSR is defined by:

\[
OSR = \frac{(TP + TN)}{(TP + FP + TN + FN)} \tag{9}
\]

The F-Score is a tradeoff between the Precision (Pr), the number of correct detections among all the frames classified as attack, and the DR. The higher the F-Score, the better the Precision and the DR [16].

\[
FScore = \frac{2 \times Pr \times DR}{Pr + DR} \tag{10}
\]

where \( Pr = \frac{TP}{TP + FP} \).

A. MitM attack Results

The multi-layer results for the MitM attack experiments, using the four considered metrics, are presented in Table I. As can be appreciated, the detection results are almost perfect, generating less than 0.1% of FP in two cases. These FPs are caused because the analysed metrics of the legal frames deviate from what is considered as normal traffic. This leads to a high belief in Attack and low belief in Normal.

As a showcasing example of the detection performance when less metrics are employed, the set of three metrics RSSI-Inj. Rate-TTL has been selected. In this case (Table II), the results of FPs and FNs are slightly higher than the previous one.

The combination of dual metric RSSI and TTL (Table IV) presents higher number of FP overall compared with the results above, exceeding 14% of FP in three cases. Additionally, two cases present FNs, deteriorating the detection performance, exceeding 1% of FNs in one case.

As an indicative example of the detection performance with a single metric, the results of single metric RSSI-Inj. Rate-TTL has been selected. In this case (Table V), the results of FPs and FNs are very similar to the cases just presented.

B. Deauthentication attack Results

As explained in Section V, the communication between the client and the AP was protected with WPA2 and a pre-shared key. Even though the system utilises metrics from just the two lower layers of the TCP/IP stack, the presented methodology was able to detect the deauthentication attack.

The multi-layer results for the deauthentication attack experiments, using the four considered metrics, are presented in Fig.4. As can be appreciated, these are the best results overall in detecting the attacks. The detection system generates 0% of FN and 6% of FP. Similar to the experiments with MitM at-
tack, the FPs are caused because the analysed metrics of the malicious frames are very close to the legal frames.

In contrast to the experiments with MitM attack, the metric Inj.Rate is ineffective in detecting the deauthentication attack. This is because management frame, both legal and malicious, are transmitted at a fixed rate of 1 Mbps. As can be seen in Fig.4, the use of Inj.Rate degrades the DR results of all the possible metric combinations. However, when using the four metric multi-layer approach, the use of Inj.Rate preserves high DR and does not degrade the results in terms of FN.

In addition, the use of Inj.Rate benefits the results because it reduces the number of FPs. In particular, the use of RSSI-ΔTime produces 0% of FNs but 14.35% of FPs. When including the Inj.Rate, the number of FPs is reduced to 6.33%.

![Detection Rate (%) vs False Positive (%)](image)

**Figure 4. Deauthentication Attack Results.**

**VII. CONCLUSIONS**

This paper tackles an important step that remains open in the use of D-S theory in network security infrastructures, finding an automatic and self-adaptive process of Basic Probability Assignment. The authors of this work have proposed and evaluated a novel BPA methodology able to automatically adapt its detection capabilities to the current characteristics of the wireless network, without intervention from an IDS administrator for selecting thresholds or manually/experimentally assigning beliefs. The system only requires a light profiling process of 20 frames. An analysis is carried out on a per frame basis.

The proposed methodology has been evaluated with real WiFi data traffic in our test-bed environment. Two different types of attack have been investigated, a MitM attack and a Deauthentication attack. In order to evaluate the effectiveness of the proposed methodology, the results from the multi-layer methodology are compared against the same methodology, but utilising metrics from fewer layers.

As explained throughout this work, using the proposed methodology, there exist some attacks that can be easily detected by utilising the information from a single metric. For instance, Inj.Rate provides perfect results in detecting both types of MitM attacks. However, using solely the Inj.Rate metric for detecting a deauthentication attack would be completely ineffective. In both attacks scenarios, the combination of information from all the metrics produces the best results overall in detecting malicious injected frames. By considering these results, it is clear that the proposed manner of intelligent combination of beliefs from different metrics yields an improved performance, in terms of detection rate and false alarms.

As for future work, we will investigate methods to automatically select the most appropriate metrics for detecting each attack taking place. This will help to reduce the number of false alarms and towards better mitigation techniques. Finally, the proposed technique can be installed in multiple monitors that could collaboratively work for achieving higher DR.

**REFERENCES**


