# Fusing Multi-Layer Metrics for Detecting Security Attacks in 802.11 Networks

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

***Abstract*—Computer networks and more specifically wireless communication networks are increasingly becoming susceptible to more sophisticated and untraceable attacks. Most of the current Intrusion Detection Systems either focus on just one layer of observation or use 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 or metric. Ideally, a synergistic approach would require knowledge from various layers to be fused and, collectively, an ultimate decision to be taken. To this aim, the Dempster-Shafer (D-S) approach is examined as a data fusion algorithm that combines beliefs of multiple metrics across multiple layers.**

**This paper describes the methodology of using metrics from multiple layers of wireless communication networks for detecting wireless security breaches. The metrics are analysed and compared to historical data and each gives a belief of whether an attack takes place or not. The beliefs from different metrics are fused with the D-S technique with the ultimate goal of limiting false alarms by combining beliefs from various network layers. The results show that cross-layer techniques and data fusion perform more efficiently in a variety of situations compared to conventional methods.**

***Index Terms*—Cross-layer measurements, data fusion, Dempster-Shafer, wireless attacks, Wi-Fi**

## I. Introduction

Computer networks and more specifically wireless communication networks are increasingly becoming susceptible to more sophisticated and untraceable attacks. Network monitoring tools, such as Intrusion Detection Systems (IDS), have been developed for the purpose of detecting such attacks. Most of these tools are not efficient enough because they either focus on just one layer of observation (i.e. MAC layer) or use a limited number of metrics without properly combining each metric.

A simple algorithm that utilises a single metric from one layer may give positive results for detecting attacks in some cases. However, this single metric method might lack efficiency in many other cases, where the nature of the selected metric might conceal the actual attack. As a result, the performance of a single metric algorithm can be poor with an unacceptable number of false alarms.

Therefore, a cross-layer approach may offer a collaborative decision among layers, potentially resulting in higher detection accuracy rate and lower number of false negative (FN) and false positive (FP). Hence, utilising a cross-layer approach may help towards automating the overall process of detecting and mitigating wireless network attacks.

This paper describes the methodology of using metrics from multiple layers of wireless communication networks for detecting wireless security attacks and particularly Man-In-the-Middle (MitM) attacks at the physical layer. The metrics are analysed and compared to historical data and each gives a belief of whether an attack takes place or not. The beliefs from different metrics are combined with the Dempster-Shafer (D-S) theory of evidence method with the ultimate goal of limiting false alarms and improving the overall performance. D-S theory of evidence method is a mathematical framework for the representation of uncertainty.

The aim of our methodology requires the system to be of low cost, scalable and applicable to other wireless technologies apart from the tested IEEE 802.11 standard. The presented methodology has been evaluated by having an attacker inject forged replies to the HTTP queries of a victim while accessing four different websites. The number of FP and FN results are counted and compared against techniques that utilise only single metrics. We compare our collaborative approach against results by methods using single metrics and combination of two metrics.

The paper is organised as follows. In section II the related work on using cross-layer and data fusion techniques is presented. An explanation of the D-S data fusion algorithm along with its advantages and disadvantages is given in section III. The methodology, testbed and the attack scenarios are presented in section IV. In section V, the results obtained with the proposed methodology are discussed and compared against the results of single or limited combination metrics. Finally, conclusions are given in section VI.

## II. Related Work

The security angle of wireless network has been visited many times in research. In [1], the authors give a thorough review of denial-of-service attacks and counter-measures in 802.11 wireless networks.

The authors in [2] try to leverage the dense deployment of desktop PCs in an enterprise to detect rogue Access Points (AP), handle malfunctioning APs and monitor the wireless network performance.

In a similar spirit, the authors in [3] have developed an infrastructure named MAP (Measure, Analyse, Protect) where dedicated wireless sniffing monitors are coordinated in order

to merge and analyse packets by dynamically changing the monitored channel.

In [4], the authors try to tackle the problem of greedy users increasing their share of bandwidth by modifying their wireless client's driver. This tactic of MAC layer greedy misbehaviour of course comes at the expense of other users. The authors propose a classification of the different MAC misbehaviour techniques and try to detect them using MAC layer metrics.

In [5], the authors describe methods for distinguishing between root causes of wireless anomalies at the depth of the physical layer. For the diagnosis of the above situation, three sources of information are required by MOJO, all of which belong at the Physical layer: network interference, signal strength variation and concurrent transmissions.

Following are described some papers related to Data Fusion. In general, for papers using D-S for data fusion in communication networks, the reader is referred to [6], [7].

In [8], the problem of discovering anomalies in a large-scale networks based on the data fusion of heterogeneous monitors is considered. The authors used the following metrics: UDP and ICMP packets in/out ratio and TCP-SYN in/TCP-FIN out ratio. The D-S algorithm detected ICMP attacks but missed SYN attacks with 2% attack packets. The authors conclude that the D-S Theory of Evidence performs well on the detection of attacks that can be sensed by uncorrelated metrics.

The authors in [9] present and evaluate anomaly-based intrusion detection algorithms for detecting attacks at the physical layer, by seeking changes in a single metric, the Signal to Noise Ratio (SNR). The algorithms evaluated are divided into two categories: Local algorithms, which are run locally and independently per monitor and central algorithms, where the output of each local algorithm per monitor is fused in a central node.

In [10], the authors follow a cross-layer approach and try to detect malicious jamming behavior and differentiate it from genuine network failures. For physical jamming attacks, the authors use as metrics the large carrier sensing time, the number of CRC errors and the increased number of retransmissions. For virtual jamming attacks, they measure the false channel reservation and they calculate the duration when the channel is idle. If the above metrics exceed a given, pre-define threshold then a cross-layer design is used to differentiate between network congestion and malicious channel activity. The proposed mechanisms are only tested in simulation. The paper is not focusing on threshold estimation and selection and the metrics are limited to two layers.

In contrast to the described related work, the proposed methodology in this paper combines metrics from multiple layers and fuses the information with the D-S technique for a synergistic approach towards detecting attacks in wireless networks.

## III. Dempster-Shafer Theory

### A. Mathematical Framework

Dempster-Shafer, as a theory of evidence method, is a discipline of mathematics that combines evidence of information from multiple and heterogeneous events in order to calculate the probability of occurrence of another event.

The D-S theory starts by assuming a Universe of Discourse $\Theta = \{\theta_1, \theta_2, \ldots, \theta_n\}$, also called a Frame of Discernment, which is a finite set of all possible mutually exclusive propositions and hypotheses about some problem domain.

With regards to this work, the frame of discernment is comprised of $A =$ "$Attack$" and $N =$ "$Normal$". Assuming $\Theta$ has two outcomes $\{A, N\}$, the total number of subsets of $\Theta$, defined by the number of hypotheses that it composes, is $2^{\Theta} = \{A, N, \{A|N\}, \varnothing\}$

Each proposition (subset) from $\Theta$ is assigned a probability, or a confidence interval within $[0, 1]$, by an observer from the mass probability function $m$ (known as "basic probability assignment"):

$$m : 2^{\Theta} \rightarrow [0,1] \qquad if \begin{cases} m(\varnothing) = 0 \\ m(A) \geq 0, \forall A \subseteq \Theta \\ \sum_{A \subseteq \Theta} m(A) = 1 \end{cases}$$

The function $m(A)$ is defined as $A$'s basic probability number. It describes the measure of belief that is committed exactly to hypothesis $A$.

In order to define the confidence interval that is given to a certain event, two functions must first be defined. These are the Belief function $(Bel)$ and the Plausibility function $(Pl)$. The former is a belief measure of a hypothesis $A$, and it sums the mass value of all the non-empty subsets of $A$.

$$Bel(A) = \sum_{B \subseteq A} m(B) \qquad \forall A \subseteq \Theta$$

The doubt function $(Dou)$ is given by

$$Dou(A) = Bel(\neg A) = 1 - \sum_{B \bigcap A = \varnothing} m(B)$$

which accounts for all evidence that rule out the given proposition represented by $A$.

Similarly, the $Pl$ function takes into account all the evidence that does not rule out the given proposition. In other words, it expresses how much we should believe in $A$ if all currently unknown facts were to support $A$.

$$Pl(A) = 1 - Dou(A)$$

Thus, the true belief in hypothesis $A$ will be along the interval $[Bel(A), Pl(A)]$. However, in practice, the values of the interval could be identical and therefore the interval becomes a unique value.

The idea behind the D-S rule of combination is to fuse the belief from two different observers into one given hypothesis.

TABLE I
EVENT PROBABILITIES ASSIGNED BY $m_1$(HORIZONTAL X) AND $m_2$(VERTICAL Y). CELLS IN TABLE REPRESENT $m_1(X)$*$m_2(Y)$

| $m_2$ / $m_1$ | $\{A\}$: 0.32 | $\{N\}$:0.25 | $\{A, N\}$: 0.43 |
|---|---|---|---|
| $\{A\}$: 0.35 | 0.11 | 0.09 | 0.15 |
| $\{N\}$: 0.1 | 0.03 | 0.031 | 0.04 |
| $\{A, N\}$: 0.55 | 0.18 | 0.14 | 0.24 |

Let $m_1$ and $m_2$ be the basic probability assignments from observer 1 and 2 respectively.

Their orthogonal $sum$, $m = m_1 \oplus m_2$, is defined as

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

If the denominator of eq. (1) is equal to zero, $K = 0$, then $m_1 \oplus m_2$ does not exist and $m_1$ and $m_2$ are said to be totally or flatly contradictory.

To easily understand how to apply the D-S algorithm, a real example from our measurements is presented. The basic probabilities for an event being "Attack", "Normal", and "Uncertain", can be tabulated as seen in Table I.

Firstly $K$ is calculated from eq. (1): $K = 1-(0.03+0.09) = 0.88$. As described in eq (1), for any event E the combined belief is given by:

$$m(E) = 1/K * \sum_{X \bigcap Y=E} m_1(X) * m_2(Y)$$

Therefore,

$$m(A) = 1.14 * (0.11 + 0.15 + 0.18) = 0.5$$
$$m(N) = 1.14 * (0.031 + 0.14 + 0.04) = 0.23$$
$$m(A|N) = 1.14 * (0.28) = 0.27$$

According to the results, the hypothesis more likely to be true is $A$, with higher belief than the other hypotheses.

### B. Advantages and Disadvantages

Among the different methods (Bayesian, Principal Component Analysis), the D-S theory of evidence was chosen as one data fusion method because it has uncertainty management and inference mechanisms analogous to our human reasoning process [11]. This means, D-S is able to combine evidence from multiple and heterogeneous sources.

In addition, it is suitable for detecting previously unseen attacks because it does not require a priori knowledge. In contrast, Bayesian inference requires a priori knowledge and does not allow allocation of probability to ignorance but only to an event being normal or abnormal [7].

It is also important to note that D-S can deal with the uncertainty of an event by assigning a value for ignorance which allows us to tackle a large range of problems.

Nevertheless, there are two drawbacks associated with the D-S algorithm. Firstly, the computation complexity and secondly the conflicting beliefs management.

The computational complexity increases exponentially with the number of possible event outcomes ($\Theta$). If there are $n$ elements in $\Theta$, there will be up to $2^n - 1$ focal elements (ignoring $\varnothing$) for the mass functions. The combination of two mass functions needs the computation of up to $2^n$ intersections [7].

The frame of discernment in the proposed methodology includes two elements, normal and abnormal, and therefore there will be three focal elements of belief functions, {Normal}, {Attack} and {Uncertainty}. Thus, the computational complexity of the algorithm is low [7].

The conflicting belief phenomenon is nicely illustrated with an example from [7]. Given three events, $\{A, B, C\}$ and two sensors, Sensor 1 might assign $m(A) = 0.9$, $m(B) = 0.1$ and $m(C) = 0$ as beliefs in $A$, $B$ and $C$ respectively. Similarly, Sensor 2 might assign $m(A) = 0$, $m(B) = 0.1$ and $m(C) = 0.9$ as beliefs in $A$, $B$ and $C$. Applying the D-S algorithm on these values, the rule of combination will result with a higher belief in event $B$, which is clearly wrong. In the proposed detection algorithm of this work, each event is assigned a non-zero mass function and therefore the belief conflict phenomenon is not an issue.

## IV. METHODOLOGY

### A. MitM attack at Physical Layer

The most common and straight forward method for an attacker to perform a MitM attack is to do first MAC spoofing, usually by performing an ARP poisoning attack (i.e. the attacker sends messages indicating that he owns a specific MAC address). This is a well known MAC layer attack. However, for the purposes of this work, a MitM attack at the physical layer as implemented by the Airpwn tool [12] was examined.

Airpwn takes advantage of the duration of time that a server requires to respond to web-page requests. In that lag time, it can inject its own content onto the wireless channel of an access point. For example, a client may request a page from wikipedia.org that takes, round-trip, approximately 13 ms. If an attacker near the victim is running the airpwn tool, it will see the legal client's request and immediately responds with its own HTML code. Due to the fact that there are no hops between the attacker and the victim, it takes the attacker much less time to respond. When the client receives the data, it will assume the original request was answered and process the injected code. Even though the attack is launched at the application layer by injecting an HTTP packet, the actual attack is practical only because there are no mechanisms in WiFi 802.11 to prevent a misbehaving node from injecting their own malicious code in the form of valid 802.11 frames.

When the real and authentic HTTP packet arrives, the content will either be ignored, if the packet size is smaller than the injected packet, or partially displayed, if the size is larger than the injected.

Using scripts, Airpwn injects carefully crafted response code that could cause harm of varying severity. Less dangerous effects to the victim could include replacing the adverts of a specific web site with different ones; more dangerous activity could include redirecting the victim web browser to a phishing type of web site.

In our experiments, two types of attacks were launched against the client. Both attack codes were default options in the Airpwn suite. We refer to these attacks as Attack 01 and Attack 02. In the first type of attack, the attacker eavesdrops the HTTP request frame from a client destined to a web server and then proceeds by injecting a forged frame. In this type of attack the forged frame contains HTML code that replaces the title of the authentic web page to a custom one as seen in Fig. 1. In the second type of attack, the attacker listens for requests for images hosted on the web site and injects its own images (Fig. 2). In addition, the attacker injects TCP reset frames so the client proceeds requesting the remaining objects of the web site.

As this type of MitM attack takes place at the physical layer, it cannot be detected with conventional MAC spoofing detection techniques. For example, one way to detect MAC spoofing is by sending an ICMP packet to the victim IP which would result in two addresses replying (the victim and the attacker).


Fig. 1. A chinese site as presented to victim with attack 01. Notice the "Hello Defcon! ... " message.


Fig. 2. A chinese site as presented to victim with attack 02. Notice the "AIRPWNED" image.

### B. Metrics and Testbed

The next task was to examine the actual manifestations of the Airpwn tool across different layers. Several metrics are identified that if appropriately used could give evidence of a MitM attack at the physical layer. These metrics are: The Received Signal Strength Indication (RSSI), the transmission rate (or injection rate), and the Time To Live value (TTL). The TTL value is a metric of the IP layer, the transmission rate belongs to the MAC layer and finally the RSSI is related to the Physical layer.

The testbed where the experiments took place can be seen in Fig. 3. It includes a client associated with an AP and accesses webpages hosted on the Internet across different geographical locations. The attack scenario consists of an attacker that launches the attack using the Airpwn tool and a third party node in passive monitoring mode that captures packets from this particular wireless network. The monitoring node and the attacker were running the BackTrack Linux operating system and all the devices except from the AP used Atheros chipset in their wireless cards. The AP is a Cisco Linksys model WRT54GL.

It should be noted that the attacker was placed very close to the AP, around 1.5 meters apart. This positioning of the equipment made the detection of attacks much more difficult as the RSSI values of the attacker could become identical to these of the AP. The RSSI is a volatile value that depends on many factors such as distance, physical obstacles, WLAN equipment, used frequency and an environmental coefficient [13]. As a result, just by examining the RSSI values it could be difficult to differentiate between attacker and AP.

In addition, Airpwn does not dynamically adapt the TTL field of the injected frames but predefines it to a static random value. The Airpwn source code has a default TTL value of 255. As this value is quite unrealistic and could easily reveal which frames are malicious, the code was modified in order to change the TTL value to 64. This value was chosen because it is the default TTL value for Linux web servers and the injected frame could be misidentified as a frame of the local area network.

The proposed methodology can be seen as a flow chart in Fig. 4. By using a wireless monitoring node the packets transmitted are collected from both the authentic AP and the forged attacker. From the information within the packets, historical data are constructed for a specific time window. More specifically, the statistical mode of RSSI and TTL are calculated for the current window. The metrics RSSI and TTL from every received packet are compared against the mode of the current time period. The beliefs for "Attack" for each of the selected metrics are chosen experimentally and intuitively i.e. the bigger the difference from the mode, the higher the belief in the attack.

Regarding the injection rate, a different approach was followed. Given that most attacking tools that inject forged packets are more efficient at low injection rates, a higher belief in attack was assigned for packets transmitted with a low rate and a lower belief in attack for packets transmitted with high rate.

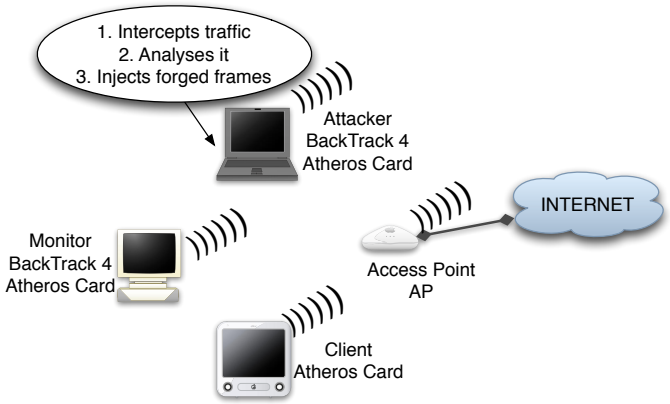


Fig. 3. Testbed and steps of attack for Airpwn

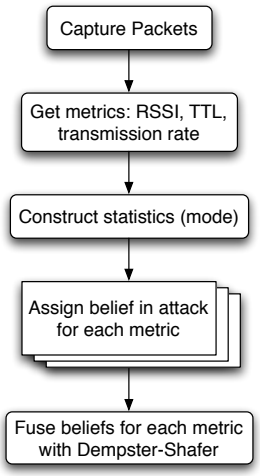


Fig. 4. Methodology Flowchart

## V. Practical Results and Discussion

In this section the results from the proposed cross-layer methodology are presented and compared against single layer metrics and against the cross-layer technique using just two metrics. The experiments were run while a client was accessing websites located in China, Spain, UK and US.

The cross-layer results are presented in Table II and are the best results overall and for each individual experiment except for some FN results that occur while launching the second type of Airpwn attack when the client visits the Chinese and UK websites. These FN results occur because the RSSI and the TTL values of the attack packets coincide with the values of the estimated mode. This could happen because consecutive injected forged packets alter the actual value of the mode. As a result, both RSSI and TTL values of several attack packets are close to the mode, leaving the decision of whether an attack is happening or not just on the injection rate. However, the belief of an attack happening just by examining the injection rate is not high enough to raise an alarm. There is a trade-off between the number of FN and FP results of the algorithm and, therefore, increasing the belief in "Attack" for injection rate could reduce FN but would also increase FP.

The results for the single layer metrics RSSI and TTL are presented in Tables III and IV respectively. The RSSI has a high number of false alarms in most of the experiments. In particular, using just the RSSI metic the FN results are so high rendering this metric unacceptable for this purpose.

In the case of single metric TTL (Table IV), the FN results are much less than the FN results of the RSSI metric and the performance in terms of FN is similar to the one achieved by the cross layer technique. However, there is a big increase in the FP results in most of the scenarios.

The combination of RSSI and injection rate metrics (Table V), quite surprisingly, results in bad performance in most cases with an extremely high FN percentage reaching even 100% in one case. This is a clear example showcasing that two metrics alone might not necessarily yield an improved performance and a more expanded synergistic approach from more metrics is necessary.

In the case of the combination of injection rate and TTL (Table VI), the performance is better in comparison to all single metrics. However, given the overall high number of FP, especially for "US attack", its performance does not reach that level gained from the cross-layer results neither the one of the combination of RSSI and injection rate.

TABLE II
Cross Layer Results utilising RSSI, Injection rate and TTL

| Website | Type | False Pos. (%) | False Neg. (%) |
|---|---|---|---|
| China | Normal | 0 | 0 |
| | Attack | 0 | 0 |
| | Attack 2 | 0 | 15 |
| Spain | Normal | 0 | 0 |
| | Attack | 0 | 0 |
| | Attack 2 | 0 | 0 |
| UK | Normal | 0 | 0 |
| | Attack | 0 | 0 |
| | Attack 2 | 8.33 | 18.52 |
| US | Normal | 0 | 0 |
| | Attack | 0 | 0 |
| | Attack 2 | 0 | 0 |

TABLE III
Single Metric Results utilising RSSI

| Website | Type | False Pos. (%) | False Neg. (%) |
|---|---|---|---|
| China | Normal | 7.14 | 0 |
| | Attack | 1.31 | 20 |
| | Attack 2 | 2.9 | 90 |
| Spain | Normal | 5 | 0 |
| | Attack | 1.56 | 0 |
| | Attack 2 | 0 | 87.5 |
| UK | Normal | 0.97 | 0 |
| | Attack | 0 | 0 |
| | Attack 2 | 14.5 | 94.45 |
| US | Normal | 17.64 | 0 |
| | Attack | 46.87 | 0 |
| | Attack 2 | 0 | 94.11 |

TABLE IV
SINGLE METRIC RESULTS UTILISING TIME-TO-LIVE

| Website | Type | False Pos. (%) | False Neg. (%) |
|---|---|---|---|
| China | Normal | 22.45 | 0 |
| | Attack | 21.05 | 0 |
| | Attack 2 | 16.67 | 15 |
| Spain | Normal | 0 | 0 |
| | Attack | 53.12 | 0 |
| | Attack 2 | 0 | 0 |
| UK | Normal | 1.95 | 0 |
| | Attack | 0 | 0 |
| | Attack 2 | 10.8 | 18.52 |
| US | Normal | 4.9 | 0 |
| | Attack | 6.25 | 0 |
| | Attack 2 | 11.29 | 0 |

TABLE V
DUAL METRIC RESULTS UTILISING RSSI AND INJECTION RATE

| Website | Type | False Pos. (%) | False Neg. (%) |
|---|---|---|---|
| China | Normal | 0 | 0 |
| | Attack | 0 | 0 |
| | Attack 2 | 0 | 80 |
| Spain | Normal | 0 | 0 |
| | Attack | 0 | 0 |
| | Attack 2 | 0 | 25 |
| UK | Normal | 2.82 | 0 |
| | Attack | 3.03 | 100 |
| | Attack 2 | 5.56 | 64.96 |
| US | Normal | 0 | 0 |
| | Attack | 18.75 | 0 |
| | Attack 2 | 1.12 | 88.23 |

TABLE VI
DUAL METRIC RESULTS UTILISING TIME-TO-LIVE AND INJECTION RATE

| Website | Type | False Pos. (%) | False Neg. (%) |
|---|---|---|---|
| China | Normal | 0 | 0 |
| | Attack | 0 | 0 |
| | Attack 2 | 0 | 0 |
| Spain | Normal | 0 | 0 |
| | Attack | 0 | 0 |
| | Attack 2 | 0 | 0 |
| UK | Normal | 19.74 | 0 |
| | Attack | 0 | 0 |
| | Attack 2 | 13.58 | 0 |
| US | Normal | 0.98 | 0 |
| | Attack | 43.75 | 0 |
| | Attack 2 | 1.13 | 0 |

## VI. CONCLUSIONS AND FUTURE WORK

This paper argues that the conventional approach of using single metrics for detecting attacks in wireless networks is sometimes inefficient, inaccurate and misleading. Similarly, techniques involving multiple metrics without utilising a proper data fusion technique lack efficiency. To this aim, the authors propose a new approach for detecting wireless network attacks, involving combining beliefs from sensors of multiple layers of observation and their belief is combined to produce a collective decision on whether an attack takes place or not.

The beliefs from different metrics are combined with the Dempster-Shafer theory of evidence method with the ultimate goal of limiting false alarms and improving the overall performance. For combining beliefs among multiple metrics from various layers, our work examined and implemented the D-S theory of evidence method, which is a mathematical framework for the representation of uncertainty.

In this paper the authors have demonstrated with experiments on a real wireless network that combining beliefs from multiple metrics in various layers outperforms the efficiency and accuracy of single metrics. The cross-layer results are the best results overall and for each individual experiment except for some FN results present in two cases (UK and China in "Attack 2" scenario). These FN results are produced because consequtive injected forged frames alter the perception of characteristics for "normal" traffic of the algorithm. Clearly, this is a conceptual issue inherent in window based algorithms.

As for future work, an important issue to consider is how to automate the assignment of beliefs and the adaptive selection of appropriate metrics using data mining techniques.

## REFERENCES


[1] K. Bicakci and B. Tavli, "Denial-of-service attacks and countermeasures in ieee 802.11 wireless networks," *Computer Standards & Interfaces*, vol. 31, no. 5, pp. 931–941, 2009.

[2] P. Bahl, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill, "Dair: A framework for managing enterprise wireless networks using desktop infrastructure," in *Proceedings of the Fourth Workshop on Hot Topics in Networking (HotNets)*. ACM, 2005.

[3] Y. Sheng, G. Chen, H. Yin, K. Tan, U. Deshpande, B. Vance, D. Kotz, A. Campbell, C. McDonald, T. Henderson, and J. Wright, "Map: A scalable monitoring system for dependable 802.11 wireless networks," *IEEE Wireless Communications*, vol. 15(5), pp. 10–18, 2008.

[4] M. Raya, J. 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*. ACM, 2004, pp. 84–97.

[5] A. Sheth, C. Doerr, D. Grunwald, R. Han, and D. Sicker, "Mojo: A distributed physical layer anomaly detection system for 802.11 wlans," in *Proceedings of the 4th international conference on Mobile systems, applications and services*. ACM, 2006, pp. 191–204.

[6] 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*. ACM, 2005, pp. 142–147.

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

[8] V. Chatzigiannakis, G. Androulidakis, K. Pelechrinis, S. Papavassiliou, and V. Maglaris, "Data fusion algorithms for network anomaly detection: classification and evaluation," in *Networking and Services, 2007. ICNS. Third International Conference on*. IEEE, 2008, p. 50.

[9] A. Fragkiadakis, V. Siris, and A. Traganitis, "Effective and robust detection of jamming attacks," in *Future Network and MobileSummit 2010 Conference Proceedings*, P. Cunningham and M. C. (Eds), Eds. IIMC International Information Management Corporation, 2010.

[10] 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. MILCOM 2006. IEEE*. IEEE, 2007, pp. 1–7.

[11] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor fusion using dempster-shafer theory," in *IEEE Instrumentation and Measurement Technology Conference*. IEEE, 21-23 May 2002.

[12] "Airpwn sourceforge website," Website, http://airpwn.sourceforge.net/Airpwn.html.

[13] R. S. Gill, "Intrusion detection techniques in wireless local area networks," Ph.D. dissertation, Information Security Institute Faculty of Information Technology Queensland University of Technology, June 2009.