Impact of Metric Selection on Wireless DeAuthentication DoS Attack Performance

Milliken, J., Selis, V., Yap, K. M., & Marshall, A. (2013). Impact of Metric Selection on Wireless DeAuthentication DoS Attack Performance. *IEEE Wireless Communications Letters*, *2*(5), 571-574. https://doi.org/10.1109/WCL.2013.072513.130428

Published in:
IEEE Wireless Communications Letters

Document Version:
Early version, also known as pre-print

Impact of Metric Selection on Wireless DeAuthentication DoS Attack Performance

Jonny Milliken, *Member, IEEE,* Valerio Selis, Kian Meng Yap, *Member, IEEE,* and Alan Marshall, *Fellow, IEEE*

***Abstract*—DeAuthentication Denial of Service attacks in Public Access WiFi operate by exploiting the lack of authentication of management frames in the 802.11 protocol. Detection of these attacks rely almost exclusively on the selection of appropriate thresholds. In this work the authors demonstrate that there are additional, previously unconsidered, metrics which also influence DoS detection performance. A method of systematically tuning these metrics to optimal values is proposed which ensures that parameter choices are repeatable and verifiable.**

***Keywords*—Denial of Service, DeAuthentication, Intrusion Detection, Metrics, Security, WiFi.**

I. Introduction

WIFI is an insecure protocol, vulnerable to the threat of Denial of Service (DoS). DoS attacks can be considered to compromise the availability of a network, through either resource exhaustion (Flooding DoS) or protocol abuse (DeAuthentication DoS). Current approaches to defeating DeAuthentication (DeAuth) DoS attacks in literature have attempted to develop suitable detection algorithms [1] [2]. The effectiveness of these algorithms however is highly dependent on the data which is being used to fuel them [3]. As a result there has been a trend in more recent publications towards identifying and classifying the metrics which are best for DeAuth DoS detection [3] [4].

Much of the work on metric selection has concentrated on the effects seen in the application and network layer [1] [4]. Work in [3] however has identified a set of features that are applicable to WiFi, recognising that Layer 2 is an area of limited investigation in current research. What is lacking from current works is information on the parameters or bounds of these metrics. Some research has prioritised the features under consideration, but there is no identification of what values the metrics or features should take on to detect an attack [3] [4].

Underpinning the importance of parameter bound selection for DoS metrics is the appreciation of the effect that thresholds and windowing factors can have on performance [1]. The effect of thresholds is investigated in [5], showing that the choice of the value for this parameter must be both dynamic and considered unique for each deployment. Windowing refers to the selection of data under consideration of an algorithm, usually determined as number of packets in a given timeframe. While effect of varying this window is considered to influence the outcome of a detection algorithm [6], it is not always taken into account in WLAN experiments [2] [3] [7].

The effect of varying the bounds in these values on detection outcome has been investigated at higher layers. If threshold values and metric parameters are set too high then valid detections can be missed, while if they are set too low then a larger number of false alerts can be generated, which obfuscates the real security concerns [5]. The same effect is observed for windowing, if the window of data under consideration is too small then larger attack chains may be missed, while too large a window size wastes computational resources and can obfuscate attacks amongst normal data [8].

II. WiFi DeAuthentication DoS

In 802.11 all Layer 2 management frames are broadcast in plain text so that nearby devices can discover the network and request a connection. Many security issues arise from this lack of protection however. If an attacker captures these plaintext management frames they can forge packets which appear to originate from a victim. Two potential frame types which can be used for causing a DoS condition in 802.11 WiFi are DeAuth and DisAssoc (DisAssociation) frames. Reception of either of these frames moves the victim out of the authenticated state in the AP state machine (See Figure 1) and into another state which does not allow for exchange of data packets. DeAuth frames are more damaging than DisAssoc as they move the device two levels back in the state machine, thereby taking longer for the client to reconnect, meaning the DoS lasts slightly longer. For Client DeAuth attacks [9] considered here, Deauthentication frames are masqueraded to appear to originate from a client, notifying the AP that the victim no longer wishes to maintain a connection.

The typical approach for detecting DeAuth DoS attacks in WiFi is to monitor traffic in the network and invoke a threshold for the number of DeAuth frames observed. If the number of observed packets is above this threshold then an alert is generated. In many instances this threshold is chosen by human experience, i.e. best guess or calculated based on traffic in the network [10]. This calculation is typically determined by the level of expected frames under normal operation. Anything above this level is classified as abnormal.

The authors gratefully acknowledge the assistance of EPSRC under grant number EP/H004793/1, Sunway University under grant number INT-SCT-0111-03, Queens University Belfast First Trust Travel Grant and Sunway Pyramid management in support of this work.

Jonny Milliken is with Queens University Belfast, Belfast, United Kingdom, email: mmilliken02@qub.ac.uk

Valerio Selis is with Traffic Observation via Management (TOM LTD), Belfast, United Kingdom, email: valerio.selis@tomltd.co.uk

Kian Meng Yap is with Sunway University, Kuala Lumpur, Malaysia, email: kmyap@sunway.edu.my

Alan Marshall is with Queens University Belfast, Belfast, United Kingdom, email: a.marshall@ee.qub.ac.uk

III. Live WiFi Data Collection

To investigate the impact of WLAN MAC-layer algorithm metrics on DoS detection performance, a data collection system was designed and deployed in the Sunway Pyramid Shopping Mall in Kuala Lumpur, Malaysia. More information about the specifics of the data collection system is outlined in [11], as are the motivations and challenges associated with design and deployment of a live WiFi monitoring installation.

Data collection is restricted to 802.11 Layer 2 MAC frames as this alleviates many of the confidentiality and user privacy issues that can act as barriers to working with live network data. In many cases these are the primary concerns for network owners and administrators. All monitored data is truncated to allow for the MAC header to be dissected whilst ensuring that all payload data is obfuscated.

IV. The Effect of Parameter Estimation on DeAuthentication DoS Detection

When assessing the presence of DoS attacks in a live 802.11 network additional parameters are needed to provide information on the accuracy and duration of the attack:

- **Window Size:** To assess whether the number of packets exceeds a threshold then a moving window limit must be established, which determines the number of packets under consideration. If the packet window is too small, then the algorithm can miss out possible DoS packets, if it is too long then the algorithm can accumulate packets that are unrelated.
- **Event time:** Upon detection of an attack, the timeframe for which the attack is considered to be ongoing is difficult to determine. Should another attack be discovered immediately after the previous alert, would this be considered evidence of an ongoing attack or a new attack altogether? A level needs to be established where an attack can be considered terminated. Choice of this level constitutes a trade-off between duration and frequency of threat.

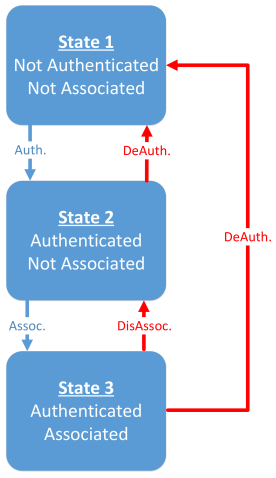

Fig. 1. 802.11 Summary of Authentication State Machine

TABLE I
Static and Varying Parameter Values (TH - Threshold, WS - Window Size, ET - Event Time

		Varying Parameter		
		TH (Packets / Sec)	WS (Packets)	ET (Sec)
Parameter Value	TH	2-20	5	5
	WS	5	1-10	5
	ET	0.1	0.1	0.1-0.6

TABLE II
Maximum Increases in DeAuth Detections Depending on Variation in Parameters

Parameter	Maximum Increase
Event Size	249%
Window Size	728%
Threshold	213%

These attributes are considered atomic parameters inherent in the majority of detection algorithms. Varying them has a currently un-quantified effect on the ability of an algorithm to detect attacks, particularly in live WiFi deployments. The values of these two parameters, as well as the algorithm threshold, are varied, during which time the other parameters remain fixed, as outlined in Table I. Results of this analysis are shown in Figures 3-5, where each graph indicates the percentage increase in DoS detections relative to the minimum value observed. Days where no attack events are observed have been removed from the figures.

Each of the Figures show an increase in the number of DoS detections observed as the parameters are varied, as high as 700% in the case of window size. Note that of the three parameters, the variance in threshold displays the smallest variability. This indicates that event time and window size are larger influences on detection performance than the threshold.

Deviation in DoS detection occurs in spikes throughout the capture, creating larger deviations concentrated on specific days. It is anticipated that this is a result of larger influxes of DeAuth frames at these times, making the algorithm more sensitive to changes. In instances where the volume of DoS detections does not vary, it is anticipated that these levels of DeAuth frames are constant with normal traffic.

From Table II, the selection of different values can change the volume of DoS detections by up to approximately 700%. It is important to note that this work is not assessing the DoS detection performance of the threshold algorithm employed. This work has been concerned with demonstrating that selection of these previously unconsidered parameters changes the DoS detection significantly.

It is possible that the reported numbers of attacks in Figures 3-5 contain false positives. This would indicate that the rate of false positives is also susceptible to changes in these parameters. It is expected that the variation in false negatives would experience the same effect. Since the number of attacks in the dataset is not known this cannot be determined.

V. Systematic Selection of DoS Metric Parameter Values

The results show that there is a significant change in the results of WLAN DoS detection depending on the value of each of these parameters. However there is no current means of reliably and systematically selecting a value for these parameters. Accuracy is an important factor for detection algorithms, but repeatability is also important. If selection of the identified parameters is determined by human knowledge, i.e. best guess, then it is reasonable that different observers may choose different values. This makes experimental results more difficult to replicate and validate. A more reliable approach would be to apply a selection algorithm to determine these values based on the dataset.

For the purposes of determining a parameter selection system, the most appropriate selection is considered here to be at those values which are most stable. A balance must be struck between having a low enough value to cover attack scenarios and a high enough value to reduce instability in the output. Using the values from Figures 3-5 allows the determination of possible settling points based on empirical data. Thus the levels for all parameters can be determined rather than guessed, by creating an algorithm to determine this settling point. The algorithm employed here calculates the parameter selection by:

1) Calculate the average and standard deviation of percentage increase in DoS detections per day in the capture,
2) Test each of the parameter possibilities. If over the capture period the selection value is higher than 1 deviation from the average for that day, that parameter is excluded.
3) The selection is determined as the lowest parameter which has not been excluded in step 2.

The algorithm is further explained in pseudo-code in Figure 2. The system proposed here is based on automatic selection of parameter values for threshold, window size and event time, listed in Table III. This generates more informed and stable results but also allows independent researchers to arrive at the same results for the same data set; parameters are no longer guessed or attributed to expert knowledge but are based on repeatable processes.

```
optimal_selection = [parameter_range_min]

for "day" in [training_length]:

    for "parameter" in [parameter_range]:

        "day"_average = mean_of_all("parameter"_value)
        "day"_sd = standard_deviation_of_all("parameter"_value)

    for "parameter" in [parameter_range_rev_order]:

        if "parameter"_value < "day"_average + "day"_sd
            "day"_min_stable_value = "parameter"

    if "day"_min_stable_value > optimal_selection
        optimal_selection = "day"_min_stable_value

return optimal_selection
```

Fig. 2. Algorithm Pseudo Code

TABLE III
Recommended Parameter Choices

MS	Window Size	Event Time	Threshold
1	2	0.2s	5 per sec
2	2	0.3s	3 per sec
3	2	0.3s	1 per sec
4	2	0.3s	5 per sec

VI. Conclusion

Selection of parameters is an important aspect of DeAuth DoS detection ; however for WLAN attacks the only parameter currently considered is the threshold. This work identifies two additional factors which influence the performance of a DoS detection algorithm; window size and event time. In order to ensure reliable and repeatable selection of these parameters in any environment, this work has proposed a parameter selection system which identifies parameter bounds based on stability of the dataset. This ensures that researchers are not reliant on human expertise, i.e. best guess, and conclusions based on traffic results are more reliable and replicable.

References

[1] Siris V.A. and Papagalou F., "Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks". *Journal of Computer Communications*, vol. 29, issue 9, pp. 1433-1442, May 2009.

[2] Singh J., *et al.*, "A MAC Layer Based Defence Architecture for Reduction-in-Quality (RoQ) Attacks in Wireless LAN". *Intl. Journal of Computer Science and Information Security (IJCSIS)*, vol. 7, issue 1, pp. 284-291, Jan 2010.

[3] El-Khatib K., "Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems". *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, issue 8, pp. 1143-1149, Aug 2010.

[4] Zargar P.B. and Kabiri G.R.A., "Category-Based Selection of Effective Parameters for Intrusion Detection". *Intl. Journal of Computer Science and Network Security*, vol. 9, issue 9, Sept 2009.

[5] Ghosh A.K., *et al.*, "Learning Program Behaviour Profiles for Intrusion Detection", *in Proc. of the 1st Conf. Workshop on Intrusion Detection and Network Monitoring (ID '99)*, Santa Clara, USA, 1999.

[6] Franklin J., *et al.*, "Passice Data Link Layer 802.11 Wireless Device Driver Fingerprinting", *in Proc. of the 15th USENIX Security Symposium*, Vancouver, Canada, pp. 1-12, 2006.

[7] Liu C., *et al.*, "Empirical Studies and Queuing Modelling of Denial of Service Attacks Against 802.11 WLANs", *in Proc. of the 2010 IEEE Intl. Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM '10)*, Montreal, Canada, pp. 1-9, 2010.

[8] Valeur F., *et al.*, "A Comprehensive Approach to Intrusion Detection Alert Correlation". *IEEE Transactions on Dependable and Secure Computing*, vol. 1, issue 3, pp. 146-169, 2004.

[9] Milliken J. and Marshall A., "The Threat Victim Table: A Security Prioritisation Framework for Diverse Network Topographies", *in Proc. of the 2010 Intl. Conf. on Security and Cryptography (SECRYPT '10)*, Piraeus, Greece, pp. 1-6, 2010.

[10] Tamilarasan A., *et al.*, "Feature Ranking and Selection for Intrusion Detection Using Artificial Neural Networks and Statistical Methods", *in Proc. of the Intl. Joint Conf. on Neural Networks (IJCNN '06)*, Vancouver, Canada, pp. 4754-4761, 2006.

[11] Milliken J., *et al.*, "The Effect of Probe Interval Estimation on Attack Detection Performance of a WLAN Independent Intrusion Detection System", *in Proc. of the IET Intl. Conf. on Wireless Communications and Applications (ICWCA '12)*, Kuala Lumpur, Malaysia, 2012.

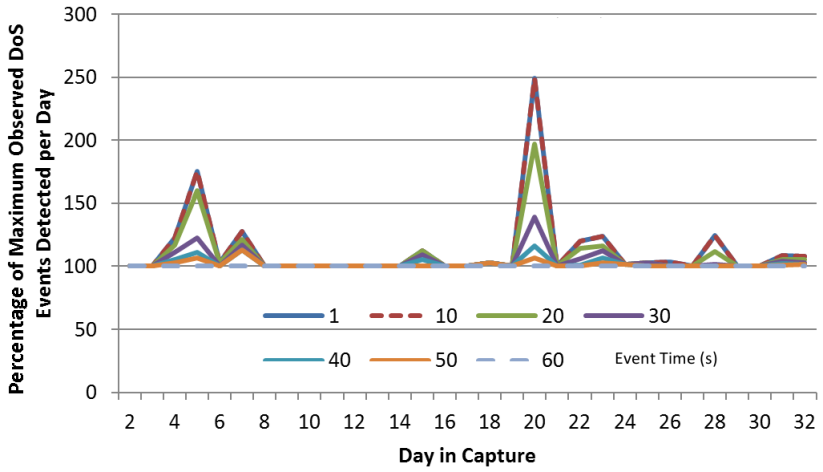

Fig. 3. Variation in DoS Detection Outcome Based on Event Time

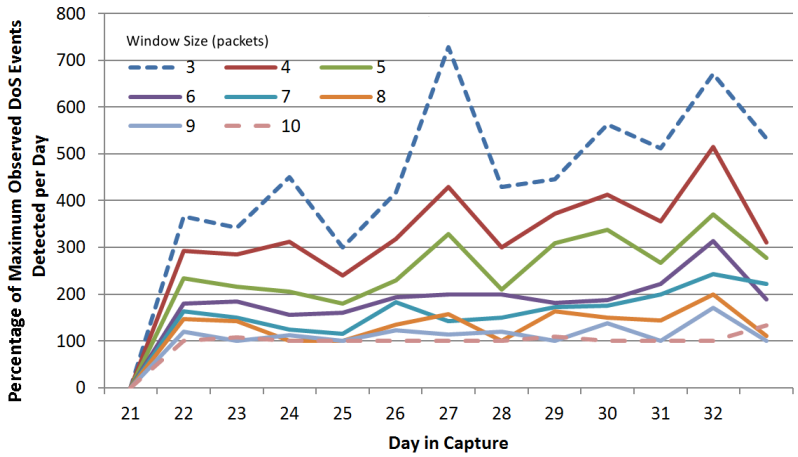

Fig. 4. Variation in DoS Detection Outcome Based on Window Size

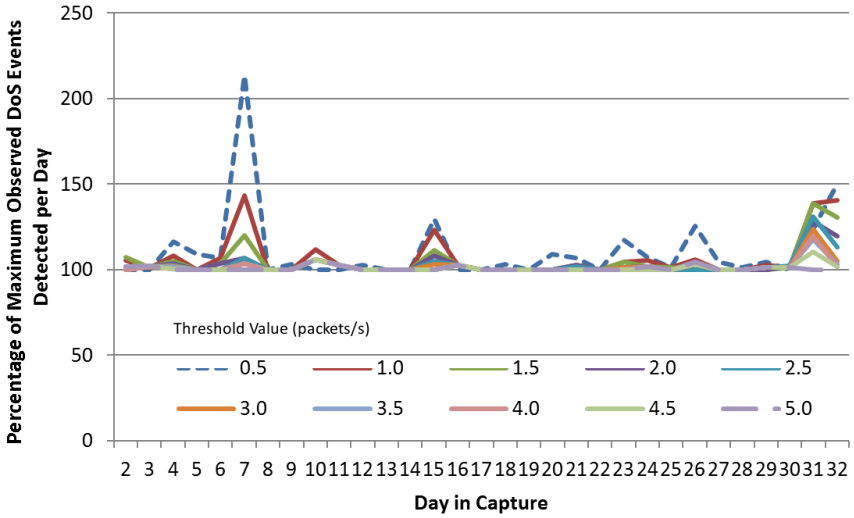

Fig. 5. Variation in DoS Detection Outcome Based on Threshold Value