

Performance Evaluation of TLS Handshake in Normal Operation and Under a Man-in-the-Middle Attack for Various Meteorological Conditions (sunrise and sunset) in an Outdoor Wireless Network

Obrorindo, C. I^{1*} and Egwali, A. O²

*Department of Computer Science and Information Technology, Petroleum Training Institute, PMB 20, Effurun, Delta State, Nigeria.

Department of Computer Science, Faculty of Physical Sciences. University of Benin, PMB 1154, Benin City

ARTICLE INFO

keywords:

TLS handshake
MitM attack
Meteorological impact
Outdoor WLAN
Intrusion detection.

ABSTRACT

As more secure communications take place in outdoor environments affected by changing weather, understanding the performance of TLS handshakes under variable meteorological conditions becomes vital. This study evaluates TLS handshake behavior in both normal and Man-in-the-Middle (MitM) attack scenarios across 9,274 sessions, collected under sunrise and sunset conditions in a wireless outdoor network. Statistical and feature analysis was performed using T-tests, ANOVA, and Information Gain to assess the impact of environmental parameters such as temperature, humidity, wind speed, gust, and pressure on TLS handshake times. Key findings revealed that MitM attacks significantly alter handshake duration during sunset ($p < 0.0001$), but not during sunrise ($p = 0.2639$), due to greater variability in early-morning conditions. ANOVA results identify humidity, wind speed, and temperature as dominant contributors to TLS timing variation at sunset, while wind gusts and rain play a larger role at sunrise. Information Gain analysis further confirms wind speed and temperature as the most predictive features for detecting MitM activity, especially at sunset, where wind speed scored 0.2085. The results demonstrate that environmental factors can either obscure or amplify the timing anomalies caused by cyber-attacks. Notably, TLS-based intrusion detection systems are more effective during sunset, when meteorological stability enhances the visibility of attack signatures. This research highlights the importance of integrating meteorological awareness into cyber security models for industrial IoT and outdoor WLANs.

1.0 Introduction

With increasing importance placed on secure communications in today's wireless networks,

confirming that cryptographic protocols remain dependable in various situations is now very important. TLS is now the universal standard for

Corresponding Author: Email address: obrorindo_ci@pti.edu.ng (Obrorindo C.I)

Received 04 May 2025, Received in revised from 12 June 2025, Accepted 14 June 2025

Available Online 10-07- 2025

njetsefoe@gmail.com; njetsefoe@yahoo.com;

protection of data during transit over the Internet. A central part of TLS is the handshake phase, where both parties exchange keys, check each other's identities and agree on how the session will be carried out. When constructing secure connections, especially on IoT, industrial control and real-time monitoring systems, the measure of latency and reliability in the handshake is particularly important [1]. Cybersecurity issues as well as outdoor weather can result in poor or unstable TLS handshakes in outdoor wireless communications. One of the serious threats listed above is the MitM attack which takes advantage of the data exchange process between attacker and victim. Increased handshake times brought on by MitM attacks, as described by Folarin [3], have attracted interest for spotting uninvited activity. Even so, because of things like wind, humidity, rain and temperature outdoors, it's difficult to tell possible anomalies apart from environmental features [4-7]. Facts from meteorology affect the quality of wireless links which can cause signal loss, lost data and the need to send data again, all impacting the time needed for TLS handshakes [5]. As an illustration, air density and light refraction change due to temperature and wind shifts at sunrise and sunset which can affect signal stability [6-11]. If these natural developments are not handled correctly,

attack detection systems based on time data may mistakenly report false positives or false negatives.

Though studies have covered TLS behaviour in limited settings and the role of weather on wireless communication strength [8-9], the relationship between security and changes in the environment is still poorly explored. More specifically, there is little research on how sunrise and sunset affect the normal and altered performance of Transport Layer Security during handshake. To fill that gap, the study examines how fast the TLS handshake happens both in regular use and when an attacker is present during normal and near sunset hours, in an outdoor Wi-Fi network. This study aims to relate observed metrics in handshakes to nearby climate conditions such as temperature, humidity, wind speed, wind gust, pressure and rainfall to uncover what influences both how well and how easily such attacks can be used. Insights gained from the research are needed to design flexible security systems adapted to weather conditions in wireless infrastructure.

Both the behaviour of TLS and the way meteorological conditions can influence wireless communications have been studied in several research initiatives. Nevertheless, there is not much research into how these areas interact, mainly in situations where threat actors perform MitM attacks.

During the TLS handshake, key exchange and the process of choosing session parameters are slower, as security is involved. The technology could be useful in spotting network attacks, including Man-in-the-Middle ones. Aziz and Hamilton suggested [2] in a method that uses the precise timing of handshakes to notice MitM attacks. It turned out that tiny timing changes in messages could signal the involvement of an attacker. In 2019, Folarin included monitoring behavioural deviations and TLS communication times in his system, pointing to the possibility that timing changes could detect intrusions. Selimis and colleagues [1] observed in low-power sensor networks that both TLS and Datagram TLS (DTLS) results were contingent on the protocol version and the quality of network environment. They observed that handshakes became less reliable when packet loss and latency appeared which are both features of attacks and environmental issues.

How well an outdoor wireless network performs is strongly affected by environmental factors. Results from Boulogeorgos and Alexious suggest that rainfall, fog and temperature in the atmosphere cause attenuation and multipath fading in 5G systems [5]. The team of Fang observed that humidity and wind speed negatively affect the quality of data in sensor-based WLAN, leading to more lost packets and greater delay [4]. The researchers (Osahenvemwen

and his team) found that rain and fog in Nigeria resulted in major changes in the strength of GSM signals [10]. In addition, Akinwale discovered that the RSS in GSM networks depends strongly on temperature, humidity and wind pressure in the lower atmosphere [9].

In particular, the atmosphere changing at sunrise and sunset is tied to variable propagation conditions. According to Diana and colleagues in their 2012 study, performance of outdoor WLANs was affected by temperature changes and shifts in humidity. The researchers [6] discovered that in the country's farmlands, changes in atmosphere at dawn and dusk resulted in more signal loss.

While much is known about TLS operations and wireless environments, there are only a few tests that look at how different weather conditions affect the performance of TLS handshakes, especially if a connection is under attack. Additionally, studying the interaction of time-based atmospheric conditions (such as sunrise and sunset) with security hazards such as MitM has largely been left unexplored. This study recovers that information by blending real-time TLS data, a MitM simulation and meteorological data to evaluate WLAN performance and detection strength outdoors.

2.0 Methodology

For both a standard TLS handshake and an MITM attack, recordings were gathered and pre-processed in an outdoor wireless setup specifically at sunrise and sunset. Because of this, the section has three parts: one covers the test bench used to gather data, one discusses the set of data that was recorded and one shows the pre-processing tasks done on it.

Test Bench

The data collection for this paper occurred on a 4G MTN Wi-Fi network, working according to IEEE 802.11 and supporting up to a maximum speed of 54 Mbps. All the experiments were carried out at the main campus of the Petroleum Training Institute (PTI) in Effurun, Delta State, Nigeria. Live simulations were performed using VirtualBox VM 16 and included both virtual machines running Windows and Kali Linux. I used VirtualBox's NAT setting to allow the VMs to use the Internet. When internet connectivity was secured, we analyzed TCP and SSL/TLS timing for various web applications with Python 3.10. I used PyCharm as the environment where I could write and run my Python scripts. The data was analyzed and visualized with Python on Google Colab because it allows ease of use, flexibility when using different systems and interactive capabilities.

Data Collection

Python is widely used for machine learning. This study includes a Python script that was custom developed to examine and measure the length of the handshakes for both TCP and SSL with a specific domain name. Every time the program runs again, it takes the handshake times and records information about the weather where the test is being carried out. The collected results are next arranged in a system of tables. We recorded 4,637 samples during sunrise and the same number during sunset which resulted in a complete dataset with 9,274 entries all having data. From September 25th to 28th, 2024, the research team collected data. Rainfall, pressure, temperature, humidity, wind speed, wind direction and wind gust were all obtained using the OpenWeather API which takes data from airport and radar weather stations as well as official meteorological sources [12]. During 00:00–06:00 and between 06:00 and 24:00 hours, researchers recorded all these variables for one month.

Data Processing

The meteorological data and SSL/TLS connection times were both sampled at their own intervals, as outlined before. Here, we describe the process used to integrate both datasets so they can be studied together. We wanted to ensure there was at least one representative sample per hour due to the changes in weather. For the first step, the raw data was carefully

cleaned, then z-score standardization was used to normalize it. Once processing was done, the final data included 9,274 records with 8 different features. We use three methods T-tests, ANOVA F-values and Information Gain to assess both the statistical significance and the importance for prediction. To check if the TLS handshake differences were significant under various circumstances, T-test was used on data collected at sunrise and sunset, focusing on the differences between regular access and attack scenarios and shown in the formula.

$$t = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}} \quad (1)$$

where

- \bar{X}_1, \bar{X}_2 are the sample means of group 1 and 2
- s_1^2, s_2^2 are the sample variances
- n_1, n_2 are the sample sizes
- The denominator is the standard error of the difference in means

Entropy, a commonly used measure in information theory measure [14], which characterizes the purity of an arbitrary set of examples, usually uses entropy. The formula of IG given by equation (2):

$$IG = H(Y) - H\left(\frac{Y}{X}\right) = H(X) - H\left(\frac{X}{Y}\right) \dots (2)$$

The statistical significance of each feature for sunrise and sunset was confirmed by computing ANOVA F-values. Using FI and PI values from ANOVA (Analysis of Variance), we find out if there are

measurable distinctions in the SSL/TLS handshake among different features present in both datasets.

We finished the process by removing the effect of human behavior so it wouldn't confuse our results. The outdoor activity of users in a WLAN varies with weather; fewer users will be active when the wind blows than on days with fair weather. When variation occurs, even connection issues aren't necessarily the reason- it can simply be that less traffic is noticed on access points outside due to fewer users being connected.

3.0 Results

Below represent results of TLS handshake timing analysis both when no attacker is present and during a MitM attack at sunrise and sunset. Different behaviours during weather conditions are compared in TLS using T-tests, F-values and Information Gain.

TLS Handshake Time Comparison Using T-Test

Using an independent T-test, we determined if TLS handshake times in normal and MitM sessions were statistically different in the morning and evening

periods.

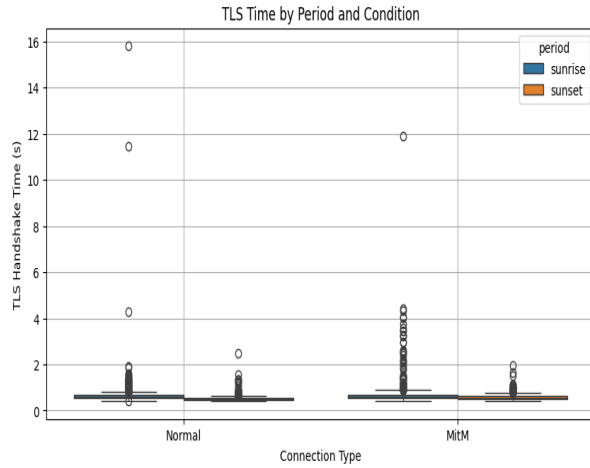


Figure 1.0: Presents a comparative analysis of TLS handshake durations under normal and MitM attack conditions during sunrise and sunset periods.

When everything is running as expected, at sunrise we notice that handshake times are not uniform and may have outsiders of up to 16 seconds. It indicates that early-morning changes in the weather, especially changes in moisture, air turbulence or temperature, can reduce the quality of wireless transmission. At sunset (orange), the handshake lifetimes are more frequently found in a limited range below 1 second which suggests the environment is more stable.

While MitM attacks are present, the time it takes for handshake during sunrise continues to vary widely and include many outliers. Sunset sessions show the outliers are minimal and the median can be seen clearly. Based on this pattern, it becomes clear that conditions during sunset cause environmental noise to decrease, making suspicious TLS handshake timings due to MitM attacks much more obvious.

Our results from the T-test also showed that only the sunset period differed between normal and attack handshake times ($p < 0.0001$), but sunrise did not ($p = 0.2639$). The boxplot proves that better environmental conditions at sunset make timing-based attack detection in outdoor wireless networks more reliable.

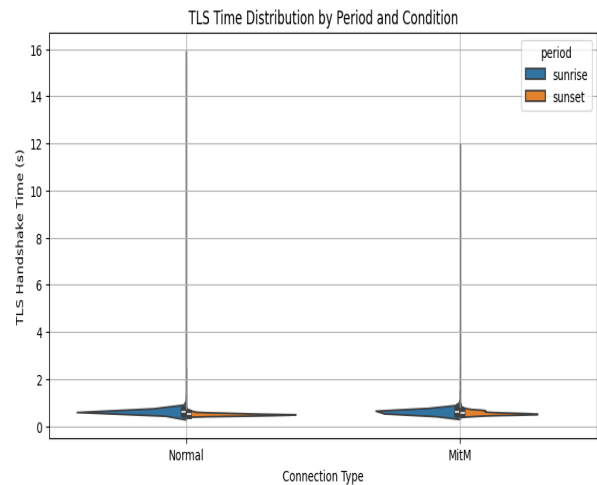


Figure 2.0: Violin plot showing the distribution of TLS handshake times under normal and MitM attack conditions during sunrise and sunset periods.

The data shows that sunrise handshake durations are more varied, while the sunset variations are grouped more closely. Since sunset is less crowded, opening up more space between the attack's distribution and usual morning traffic, this process helps detect MitM more easily than when attackers acts during sunrise. During sunrise, the time it takes for a TLS handshake increases for normal sessions, showing up as a wider range of violins. These conclusions are in line with previous research which found that handshake instability at sunrise can naturally prolong

delays which, in turn, complicates the task of finding attacks.

- Distributions during sunset periods become narrower (the violins shrink) mainly when a MitM attack is taking place. This suggests that MitM attacks slow down the handle so that mitigation techniques work well.
- Because it's hard to distinguish between MitM and Normative traffic in sunrise sessions, using just the time of a handshake may not be accurate in the morning unless combined with other context.

3.3 Analysis of Meteorological Factors Using ANOVA

ANOVA was employed to see which environmental elements made the biggest difference between when meteorological data were normal and during attacks.

Sunrise ANOVA Results

All meteorological parameters showed statistically significant influence ($p < 0.0001$), as shown in Table 1.

Table 1: ANOVA F-Values (Sunrise)

Feature	F-Value
Wind Speed	300.78
Wind Gust	274.03
Wind Direction	182.57
Temperature	173.84
Humidity	167.25
Rain	136.83
Pressure	132.31

This analysis hints that wind parameters such as speed and gust are the main reasons behind TLS handshake issues at sunrise. Consequently, wind variations and turbulence tend to hinder signals in outside wireless networks which may indirectly raise handshake times, even if such problems are not caused by attacks.

Sunset ANOVA Results

At sunset, we again obtained high F-values that show the meteorological parameters had a significantly strong effect (check Table 2).

Table 2: NOVA F-Values (Sunset)

Feature	F-Value
Humidity	1164.23
Wind Speed	883.72
Temperature	738.13
Wind Gust	721.57
Pressure	36.76
Wind Direction	1.84
Rain	NaN

Wind direction did not matter (p value was above 0.05) and rainfall was not measured (NaN values because there was no rain at that time). Results showed that humidity, wind speed and temperature were most important during sunset, meaning these elements aggravated the differences in timing from MitM errors.

3.4 Feature Importance via Information Gain

The IG statistic was applied to compare meteorological elements to determine which ones give the clearest distinction between normal and MitM events.

Sunrise Information Gain

Table 3: IG Scores (Sunrise)

Feature	IG Score
Wind Speed	0.0651
Rain	0.0613
Wind Gust	0.0592
Temperature	0.0591

Wind Direction	0.0542
Humidity	0.0541
Pressure	0.0105

At sunrise, wind speed, rain and gust are shown to have moderate importance in detecting potential attacks or incidents. It looks like pressure doesn't have much of a clear effect on discrimination.

Sunset Information Gain

Table 4: IG Scores (Sunset)

Feature	IG Score
Wind Speed	0.2085
Wind Gust	0.2036
Wind Direction	0.1967
Temperature	0.1949
Humidity	0.1197
Pressure	0.0075
Rain	0.0038

Media posted on IG shows a large rise, mainly because of wind speed and temperature. Wind speed, gust and direction are found to be the main factors in this range, confirming that the weather at sunset has higher predictive value for Man in the Middle (MitM) attacks in Asia known as handshake behaviour.

Table 5: Summary of Key Observations

Period	T-test Result	Strongest ANOVA Features	Top IG Features
Sunrise	Not Significant (p=0.26)	Wind speed, gust, temperature	Wind speed, rain, gust
Sunset	Highly Significant (p=0.0000)	Humidity, wind speed, temperature	Wind speed, gust, temperature

It is shown by comparing sunrise and sunset that the time required for the TLS handshake varies based on the environment. Sunset is stronger in atmospheric conditions and demonstrates greater contrast between the behaviour of TLS during an MitM attack.

Key Findings

TLS handshake time is significantly affected by the time of day.

- At sunrise, the time for each handshake goes on for longer or shorter periods which makes the timing method for attack detection less effective.
- The signature of MitM attacks rises during sunset and handshakes tend to be consistent.

Man-in-the-Middle (MitM) attacks produce statistically significant timing anomalies during sunset only.

- No major change in handshake length could be seen at sunrise as indicated by T-test results (p = 0.2639).
- Yet, a very strong difference was found at sunset (p < 0.0001), suggesting that attack detection gets easier in the evening.

Meteorological parameters influence handshake behaviour and attack visibility.

- Both periods demonstrated that wind speed, wind gust, temperature and humidity were the factors having the most effect.
- Even during sunset, the wind direction made less difference than the steady rain which came all day.

Environmental features have higher predictive power during sunset.

- Sunset condition Information Gain values showed that wind speed (0.2085), wind gust (0.2036) and temperature (0.1949) are the most helpful to identify unusual TLS handshakes.

Sunrise introduces more noise into TLS handshake timing.

- The increase in rare and extreme times during sunrises points to greater atmospheric disturbances which can hide MitM delays and decrease the effectiveness of timing-based attack identification.

Sunset provides a more stable window for TLS handshake analysis.

- Because the timing variations are lower, signal statistics are stronger and feature importance is higher, sunset is the best time to detect MitM attacks using TLS timing details.

Conclusion

Through experiments, this work assessed TLS handshake performance both under normal and MitM attack cases in environments exposed to certain weather conditions at sunrise and sunset times. With over 9,000 sets of TLS sessions and related data, we found that network connectivity can slow down for reasons besides cyberattacks which matches similar findings on how weather can disturb wireless signals [2, 9, 10].

Statistical results suggest that the differences in delay caused by MitM can be detected during sunset, but not during sunrise. These observations confirm what earlier studies said: wireless links become more stable during sunset and error timing in these links could be used to spot intrusions [1-3]. On the other hand, this study found that the major environmental factors for cell signal at sunset are wind speed, wind gust, temperature and humidity, as found previously in similar studies on meteorologist effects on signal strength [4-6].

Based on these results, it is important to design intrusion detection systems that work with energy efficiency in mind, mainly in weather-exposed outdoor environments, IoT and industrial control contexts.

Recommendations

Integrate Meteorological Data into Security Systems:

With the weather becoming an important part of cybersecurity, studies suggest [3-4] that TLS-based intrusion detection should now pay attention to live environmental variables.

1. Use Period-Aware Detection Thresholds:

Because the environment is much more stable at sunrise and sunset than at other times of day, detecting changes should vary accordingly [10].

2. Prioritize Evening Monitoring for Security Audits:

As distinct changes are seen between normal and MitM traffic at sunset in experiments, auditing systems should pay closer attention to timings throughout this period.

3. Account for Timing Outliers in Morning Conditions:

The large swings in handshake times during sunrise agree with previous results on increased signal variability in the early hours [6]. This justifies using pre-processing filters to remove incorrect alerts.

4. Optimize Outdoor Network Design:

In places with often changing environmental conditions due to wind or humidity, special care should be given to choosing where to place wireless nodes outdoors [5, 10].

Future work

- 1. Broaden Time and Seasonal Coverage:**
More research should be done at midday and night-time and during both wet and dry seasons, to give a complete view of the site [9].
- 2. Geographic and Climatic Generalization:**
Testing the model in various settings such as at the coast, high above sea level and in the tropics, will determine if it works well under different kinds of climate conditions.
- 3. Machine Learning-Enhanced Detection:**
If you train Random Forests, SVM or LSTM on both timing and environmental data, they are better at automating MitM detection [13].
- 4. Multi-layer Correlation Models:**
Combining TLS behaviour with RSSI, SNR and retransmission information could support the development of more effective multi-featured IDS [11].
- 5. Application to Critical Infrastructure:**
The approach can be adapted to energy, transportation or healthcare IoT networks which require safe TLS connections and where the weather can affect the performance [2][13].

References

- [1] Selimis, G., Mathur, C., and oukas, G. (2021). TLS vs DTLS in Wireless Sensor Networks: A Performance Evaluation. *Sensors*, 21(6), 2192. <https://doi.org/10.3390/s21062192>
- [2] Aziz, B., and Hamilton, G. (2009). Detecting Man-in-the-Middle Attacks by Precise Timing. *In SECURWARE*, 1–6. <https://doi.org/10.1109/SECURWARE.2009.20>
- [3] Folarin, S. (2019). Improved SSL/TLS Man-In-The-Middle Attack Detection Technique Using Timing Analysis and Other Behavioral Anomalies. *Research in Computing*, National College of Ireland.
- [4] Fang, X., Gao, X., and Guo, W. (2021). Investigation on the Impact of Meteorological Conditions on Outdoor Wireless Sensor Networks. *Sensors*, 21(6), 2192. <https://doi.org/10.3390/s21062192>
- [5] Boulogeorgos, A. A., and Alexiou, A. (2020). Secrecy Performance of THz Wireless Systems With Weather-Dependent Channel Modeling. *IEEE Transactions on Communications*, 68(5), 3194–3208. <https://doi.org/10.1109/TCOMM.2020.2976619>
- [6] Thelen, J., Goense, D., and Langendoen, K. (2005). Radio Wave Propagation in Potato Fields. *1st Workshop on Wireless Network Measurements*.
- [7] Diana, B., Ramos, F., Lloret, J., and Garcia-Pineda, M. (2012). The Influence of Meteorological Variables on the Performance of Outdoor Wireless Local Area Networks. *IEEE ICC*. <https://doi.org/10.1109/ICC.2012.6364448>
- [8] Kemka, C., and Emeruwa, C. H. (2024). Temperature and Humidity Effect on Mobile Communication Network Performance in Yenagoa, Nigeria. *Nigerian Journal of Communications*, 40(1), 45–53.
- [9] Akinwale, A. K., Olasunkanmi, O. S., and Ajani, O. O. (2023). Effect of Tropospheric Parameters on Received Signal Strength in GSM Networks in Rivers State, Nigeria. *International Journal of Wireless and Mobile Networks*, 15(1), 1–10. <https://doi.org/10.5121/ijwmn.2023.15101>

Table of Abbreviations

TLS: Transport Layer Security
MitM: Man-in-the-Middle
WLAN: Wireless Local Area Network
IoT: Internet of Things
ANOVA: Analysis of Variance
IG: Information Gain
VM: Virtual Machine
NAT: Network Address Translation
API: Application Programming Interface

[10] Osahenvemwen, O., and Omatahunde, E. (2016). Effect of Weather Conditions on GSM Signal Strength in Benin City, Nigeria. *Nigerian Journal of Technology*, 35(3), 564–571.

[11] Boano, C., Brown, J., He, Z., Roedig, U., and Voigt, T. (2010). Low-power Radio Communication in Industrial Outdoor Deployments: The Impact of Weather Conditions and ATEX-compliance. *Sensor Applications, Experimentation, and Logistics*.

[12] OpenWeatherMap. (2021). Weather API Documentation. Retrieved from <https://openweathermap.org/api>

[13] Baig, M. S., Ismail, S. N., and Syed-Yusof, S. F. (2022). Machine Learning-Based TLS Analysis for Attack Detection in IoT Networks. *IEEE Access*, 10, 48731–48744.

[14] Abe, N., and Kudo, M. (2005). *Entropy criterion for classifier-independent feature selection*. In Proceedings of the 9th International Conference on Knowledge-Based Intelligent Information and Engineering Systems (KES 2005), Lecture Notes in Computer Science, vol. 3684, pp. 905–911. Springer.