We successfully detected a **deauthentication attack** on a smart farm architecture using **MERLIN**, a distance-based anomaly detection algorithm.

Tennessee Technological University

Detecting Denial-of-Service Attacks using Distance-Based Anomaly Detection

Sina Sontowski, ssontowsk42@tntech.edu
Advisors: Maanak Gupta, William Eberle

Introduction

- Cyberattacks are increasing and becoming a threat to our infrastructure, including to the field of smart farming which is predicted as the future of agriculture
- A Denial-of-Service (DoS) attack can prevent crop sensor updates to be sent to the farmer, which is important during harvest
- Detecting cyberattacks, such as with anomaly detection, can prevent further damages
- How can we detect a deauthentication attack (type of DoS attack) on a smart farm infrastructure?
- Testbed depicted below is based upon Microsoft Farmbeats [1]

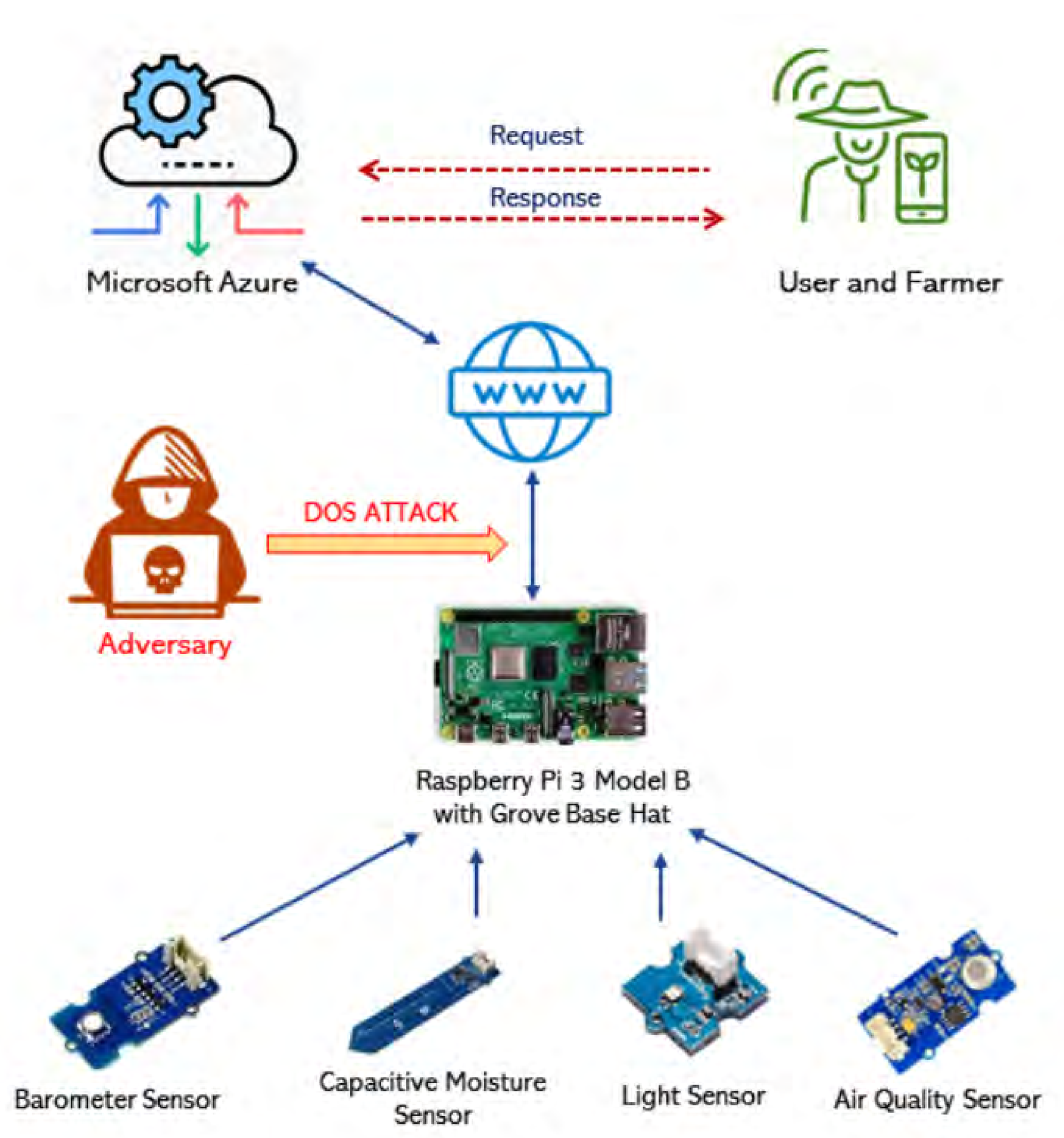


Fig. 3. System Architecture and Attack Surface.

Data

- Collected network traffic with Wireshark over two hours: normal traffic for 30min, then 18s attack traffic, and then normal traffic again until the rest of time
- 1,048,575 packets after removal of non-internet traffic packets
- Includes traffic from nearby networks
- Deauthentication packets make up less than 0.2% of all packets recorded

Data Dictionary

Attribute	Required	Format	Description
No.	No	int	packet number
Time	Yes	string	timestamp
Source	No	string	origin
Destination	No	string	destination
Protocol	No	string	protocol
Length	No	integer	in bytes
Info	No	string	general details

Feature Extraction & Data Prep

- Every attribute removed except for timestamp
- Added packet count
- Sampled data by aggregating packets to every 0.5s for a total of 14,963 packets

Experiments

- MERLIN available in MATLAB
- Four parameters: input file, shortest discord length, largest discord length, whether to output metadata while running
- MERLIN finds anomalies of all lengths [2]
- Able to detect attack when maximum discord length goes above 300
- MERLIN adds linear trend to constant regions to minimize false positives [2]

Experiments with different discord ranges

Experiment	min discord	max discord	running time (in seconds)	detected
1	50	100	12	no
2	50	150	18	no
3	50	200	38	no
4	50	300	64	yes
5	50	500	153	yes
6	100	300	55	yes
7	200	300	29	no

Constant Region Error Message

```
>> [distances, indices, lengths] = MERLIN3_1(janAttack0_5s, 50, 500, true)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!   MERLIN may report false positive anomalies in subsequences with near constant values.
!!!   A sign that the problem exist is a spike near zero when plotting the histogram of mov:
!!!   Adding a large linear trend will solve this issue.
!!!   Proceed with data modification? [y/n]
Y
```

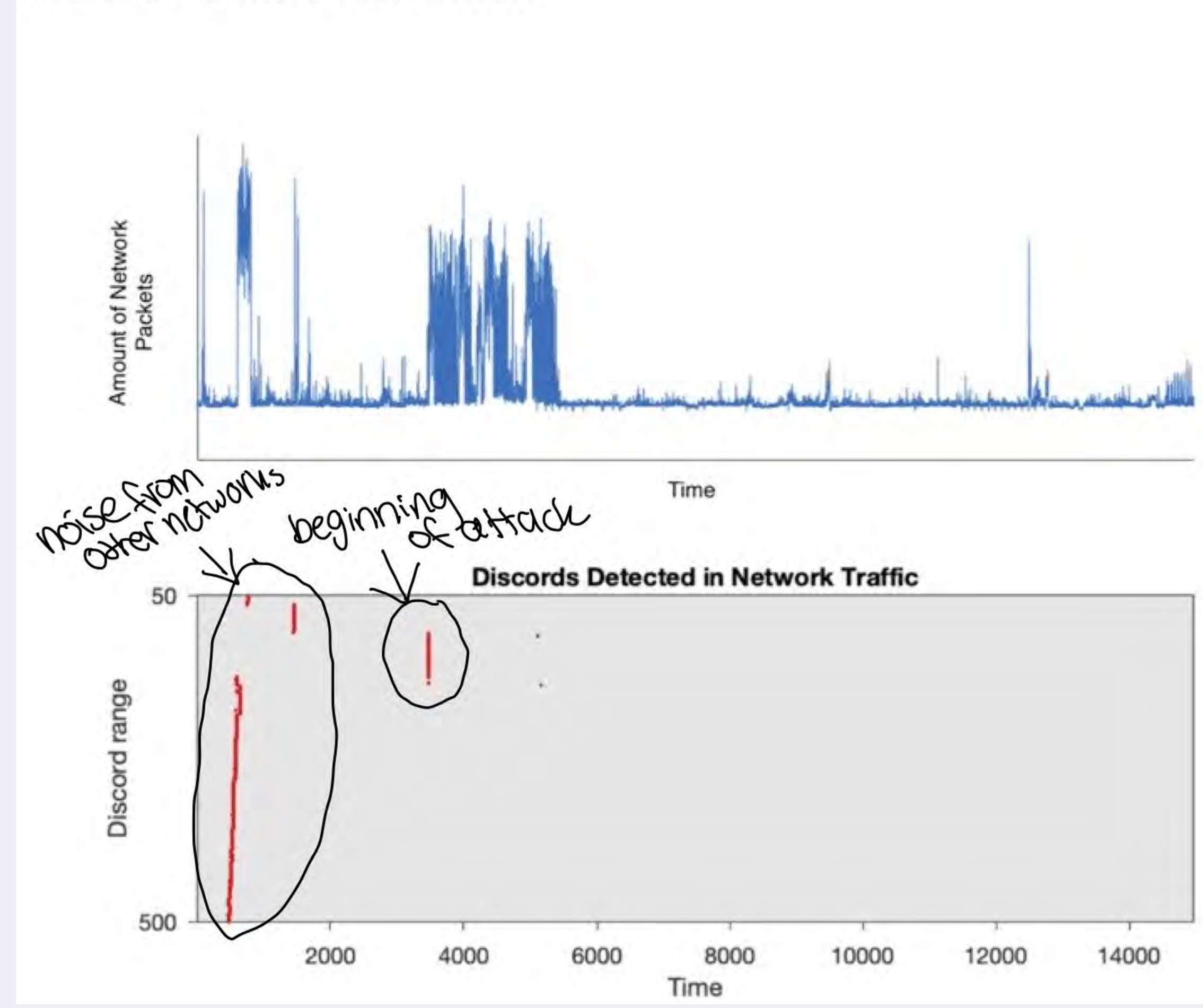
Analysis

- Cluster around 4000 is deauthentication attack
- Long anomaly in the beginning is noise from other networks
- MERLIN detected about half of anomalous network packets
- Only beginning of attack was detected, therefore sensitivity low
- MERLIN successful in detecting attack because as long as at least one packet labeled as anomalous by MERLIN, attack is considered detected

Results

Measure	Value	Derivations
Sensitivity	0.3056	TPR = TP / (TP + FN)
Specificity	0.9907	SPC = TN / (FP + TN)
Precision	0.0733	PPV = TP / (TP + FP)
Negative Predictive Value	0.9983	NPV = TN / (TN + FN)
False Positive Rate	0.0093	FPR = FP / (FP + TN)
False Discovery Rate	0.9267	FDR = FP / (FP + TP)
False Negative Rate	0.6944	FNR = FN / (FN + TP)
Accuracy	0.9890	ACC = (TP + TN) / (P + N)
F1 Score	0.1183	F1 = 2TP / (2TP + FP + FN)

Anomalies detected with MERLIN



Conclusions and Future Work

- Important to detect DoS attacks because cyberattacks have detrimental effects on our critical infrastructure
- MERLIN was successful in detecting a deauthentication attack on a smart farm
- More research has to be done to evaluate why only the beginning of the attack was detected
- Future work includes applying MERLIN on datasets that have more than one attack
- Running more experiments to see if MERLIN can detect attacks in short succession of each other would be helpful

References

[1] Sina Sontowski, Maanak Gupta, Sai Sree Laya Chukkapalli, Mahmoud Abdelsalam, Sudip Mittal, Anupam Joshi, and Ravi Sandhu. Cyber attacks on smart farming infrastructure. In 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC), pages 135–143, 2020.
[2] Takaaki Nakamura, Makoto Imamura, Ryan Mercer, and Eamonn Keogh. Merlin: Parameter-free discovery of arbitrary length anomalies in massive time series archives. In 2020 IEEE International Conference on Data Mining (ICDM), pages 1190–1195, 2020.

Acknowledgement

This work is partially supported by NSF grant 2025682, 1565562 and 2043324.