Cyber-Secure Network Architecture for Nuclear Power Plants

David Arnold and Jafar Saniie

Embedded Computing and Signal Processing Research Laboratory (http://ecasp.ece.iit.edu)
Department of Electrical and Computer Engineering
Illinois Institute of Technology, Chicago IL, U.S.A.
darnold3@hawk.iit.edu and sanii@iit.edu

INTRODUCTION

Advanced nuclear reactors, such as small modular reactors (SMRs) and micro reactors are currently under development as cost-effective alternatives to the existing fleet of light water reactors. Adoption and increased reliance on remote access and digital infrastructure can achieve cost-efficient operation of future SMRs. However, reliance on these technologies results in an expanding network footprint, and can lead to a softened resilience to cyberattacks. Further, hacking communities have shifted their attention towards Industrial Control Systems (ICS) and critical infrastructure, such as nuclear energy. Ranging from common criminals to nation-state actors, these hackers target these networks due to their importance to national infrastructure.

Initial cyber-defense doctrine relied heavily on the use of physical network segmentation and industry-specific software to protect operations from potential harm. This was proven insufficient during the Stuxnet attack, in which malicious USB drives were used to infiltrate the isolated network [1-3]. Despite sector-wide improvements in the years since, hacking groups continue to be successful. In 2015, a cyberattack interrupted operations for several regional electric operators in the Ukrainian capital of Kiev [4-5]. During the attack, the hackers were able to gain access to the network through social engineering attacks. After gaining access to the network, valid commands were sent to shutdown local substations and remote control functionality was then destroyed. Finally, malware was detected in the administrative network of an Indian nuclear power plant in 2019 after an employee connected an infected device to the network [6]. These attacks highlight the importance of working towards stronger security solutions.

To address these shortcomings, we have conducted research towards a Cyber-Secure Network Architecture for Nuclear Power Plants. A diagram of the proposed network architecture can be seen in Figure 1 and includes the development of two cybersecurity solutions. The first solution is the establishment of ultrasonic pathways for the distribution of Advanced Encryption Standard (AES) symmetric keys to devices within the facility. Utilization of ultrasonic pathways creates a side-channel key distribution mechanism to securely transfer AES keys without using the primary wired network. Recent studies sponsored by DOE

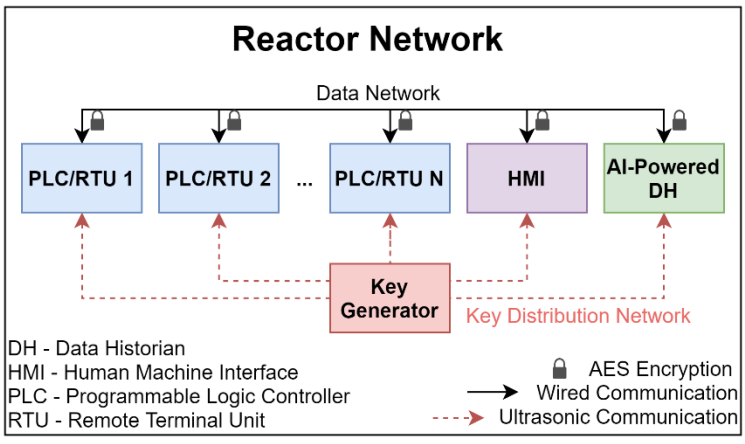


Fig. 1. The network architecture of a future nuclear reactor network. Network traffic is transmitted throughout the facility using wired infrastructure and is encrypted using AES. The secret keys are transmitted between devices using Secure Ultrasonic Pathways. An AI-Powered Data Historian will rely on a fusion of network traffic and sensor data to detect cyberattacks.

have proven ultrasonic communication is a secure and reliable alternative to conventional wired channels [7-11]. Additionally, the use of existing piping infrastructure provides a low-cost solution while also being difficult to eavesdrop using commonly available electronic devices. The second cybersecurity solution is the integration of cyberattack detection capabilities through artificial intelligence and machine-learning based models. Due to the widespread use of cyber-physical devices traditional Intrusion Detection Systems (IDS) often miss key data that can be used to strengthen cyberattack detection capabilities. Application of Artificial Intelligence (AI) and Machine Learning (ML) models can fill this gap by fusing both network traffic and sensor data to provide a stronger prediction.

The remainder of this summary will present the work that has been completed with the support of the Nuclear Energy University Program's (NEUP) University Nuclear Leadership Program (UNLP) graduate fellowship. First, a platform for securely transmitting a video through a solid channel will be discussed. This project serves as a proof-of-concept use-case for future ultrasonic pathways, such as for key distribution. Second, a set of potential machine learning models for cyberattack detection will be presented. A gas pipeline dataset was used due to its availability, but lessons learned will be applied to a nuclear power plant dataset in the future.

RESULTS

Secure Ultrasonic Pathways

Proper application of cryptographic techniques hampers a hacker's ability to expand their foothold within the network. Symmetric key distribution over insecure or open channels continues to be a challenge for secure transmission of data. Development of side-channel key distribution architectures, such as through ultrasonic pathways, can alleviate risks of key distribution by exchanging keys via networks that are harder to eavesdrop.

For successful implementation of the proposed ultrasonic pathways for key distribution, we first undertook a proof-of-concept project to determine the capabilities of the ultrasonic pathways. This was accomplished through a collaboration with my fellow researchers at the Embedded Computing and Signal Processing (ECASP) Research Laboratory at the Illinois Institute of Technology [12-14]. The objective of the project was to reliably transmit a video stream over an Aluminum Rectangular Bar (ARB). The video stream is uploaded to a server and should be available for real-time observation. To achieve these objectives, a reconfigurable Software-Defined Ultrasonic Communication (SDUC) was developed to account for the many challenges of communicating using a solid channel. For the study, multiple lengths of ARB were used (25, 40, and 50 cm) along with differing video streaming resolutions (240p, 480p, and 720p) at 20 frames per second. A diagram of the ultrasonic communication system can be viewed in Figure 2. The SDUC platform was capable of achieving the desired resolutions across each ARB channel length and achieved a maximum reliable video feed at 1074 kbps. Additionally, this stream had a bit-error rate of 3.3x10-4 while combatting intersymbol interference. These characteristics are sufficient for achieving the necessary latency, bandwidth, and bit-error rate for secure and safe distribution of symmetric keys.

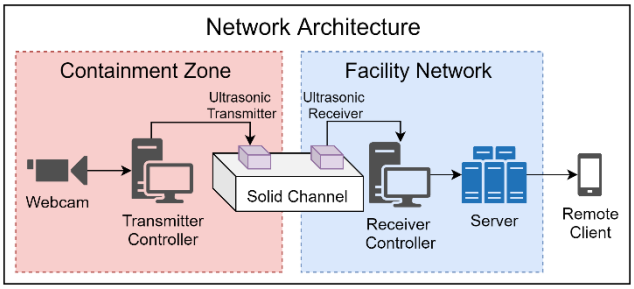
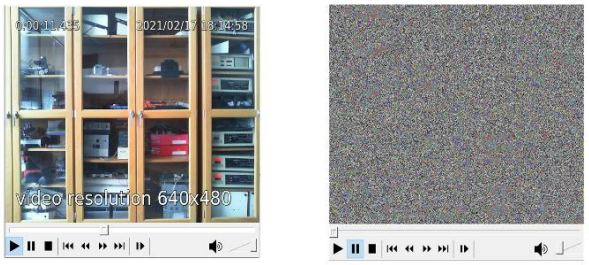


Fig. 2. Network architecture for secure video streaming over an ultrasonic channel.

In addition to streaming the video over the solid channel, we examined different cryptographic solutions for protecting the sensitive video stream. Encryption was examined for both communication across the solid channel as well as to the server and remote client. For the data-in-transit between the Receiver Controller and the Remote Client, the Advanced Encryption Standard (AES) with Cipher Block Chaining (CBC) was used. The AES CBC algorithm applies the standard AES encryption algorithm while accounting challenges that are common when encrypting images, such as image artifacts that can be used to identify shapes in the image.

Due to computation limitations of the transmitter controller, it was determined that an alternative encryption algorithm was needed. To resolve this issue, a novel chaotic-based encryption scheme was generated that would have a lower key-length and computation time. This cryptosystem was based on the Arnold Cat Map and Logistic Map to provide good confusion and diffusion characteristics. During operation, the Arnold Cat Map transforms the dataset into a pseudo-random state over several iterations while the Logistic Map applies an external key. Analysis of the encryption method was completed by examining histogram and correlation data for the pixels of the encrypted image. Both tests are strong indicators of encryption strength as an attacker may attempt to identify common patterns or poor confusion and diffusion of the dataset by using frequency attacks. Figure 3 presents an example video frame and the encrypted version of the frame [14]. As shown, the encrypted frame is unrecognizable from the original frame. Additionally, histogram analysis showed a relatively equal frequency of each pixel value while the correlation analysis shows that the pixels have very low correlation. Specifically,

an unencrypted image has a correlation coefficient of 0.9901 while the image encrypted using the chaotic map had a correlation coefficient of 7.7e-4.



(a) (b)

Fig. 3. Analysis of encryption of video frame: a) original video frame with resolution 640x480, b) chaotic map encryption of the frame

Lessons learned through this endeavor will directly affect the implementation of secure ultrasonic pathways for key distribution. As our proof-of-concept project showed, an ultrasonic channel is capable of achieving the necessary latency, bandwidth, and bit-error rate for fast and efficient transmission of AES keys between devices within the network. Further, we explored additional mechanisms to encrypt the data while it is being transmitted through the ultrasonic pathways.

Cyberattack Detection

Through their interactions with physical processes, cyber-physical devices generate both network data and sensor data. By applying machine learning models to this data, patterns can be detected that can indicate equipment failure or cyberattacks. This is advantageous over traditional intrusion detection systems, which typically only deal with network traffic. To explore the potential effectiveness of this method, an updated version of the Data Historian (DH) was proposed [15]. The data historian was selected due to its importance to the overall ICS network for their data auditing purposes [16-17].

Presented in Figure 4, the proposed data historian architecture is responsible for the same data aggregation and storage responsibilities of the conventional DH while also deploying machine learning models on the dataset for cyberattack detection. The deployment of the machine learning models is handled by a new Data Analytics component, which is powered by the Apache Spark platform [18]. Detected cyberattacks are reported to the security administrator, along with other useful information that can be used for external auditing and other expanded use of data. For the project, four machine learning models were selected, and included the Naïve Bayes, Logistic Regression, Decision Tree Classifier, and the Random Forest Classifier. These were selected due to their common application to other

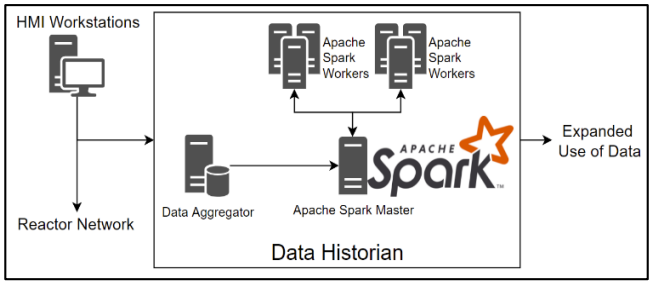


Fig. 4. Data historian architecture for cyberattack detection. An Apache Spark Master Node is responsible for assigning the incoming data to the Apache Spark Workers that will run the machine learning models on the incoming data.

classification problems. Each machine learning model was implemented using the Apache Spark MLlib machine learning models. The Naïve Bayes classifier was created using the default constructor and no hyperparameters were adjusted. Similarly, the Decision Tree Classifier was also created using the default constructor, while the Random Forest Classifier was set to select from 10 generated decision tress. For the Logistic Regression Classifier, the MLlib library allows the user to select between lasso regression, ridge regression, and elastic net regularization (combination between lasso and ridge regression). We selected elastic net regularization and the default parameter of 0.80, which favored lasso regression.

After implementation, the four machine learning models were applied to a simulated gas pipeline dataset [19]. While the simulated environment was small, it still provides good insight into the operation and characteristics of an overall ICS network. During testing, the dataset was split 70%-30% (training-testing). Additionally, each model was run 10 times with different data splits to provide an average that would give a reasonable representation of accuracy. Table I presents the accuracy of each machine learning model along with evaluation metrics. These metrics include the true positive, false positive, true negative, and false negative values.

TABLE I. Accuracy and Evaluation Metrics for Cyberattack Detection

Algorithm	True Positive	False Positive	True Negative	False Negative	Accuracy
Naïve Bayes	34.2%	5.7%	15.8%	44.3%	50%
Logistic Regression	76.7%	0%	19.1%	4.2%	95.8%
Decision Tree Classifier	80.2%	0%	19.3%	0.5%	99.5%
Random Forest Classifier	80%	0%	19.2%	0.8%	99.2%

According to the results, the decision tree (99.5%) and random forest (99.2%) classifiers performed the best out of

the machine learning models. This was expected as cyberattacks will cause deviations in the sensor data that will fall outside of normal operations. As a result, it's likely that these two tree classifiers picked up on normal operating ranges and generated their trees accordingly. Further examination of the results reveals that most of the classifiers favored false negative results over false positive results. During operation, false positives are preferred as a false negative means that a cyberattack has slipped through the detection routine.

Future work will begin with feature analysis of the dataset to identify key indicators for increased efficiency of the models. This may also result in the identification of metrics that can be used to assist in transitioning from the gas pipeline dataset to a nuclear power plant dataset. Additionally, artificial intelligence models will also be explored and compared to the machine learning models.

CONCLUSION

Through the support of the NEUP UNLP graduate fellowship program, I have made steady progress towards the realization of a cyber-secure network architecture for nuclear power plants. The proposed architecture enhances national security by developing two key cybersecurity solutions to address cybersecurity threats. To achieve these goals, we have conducted research into the capabilities of ultrasonic channels to support a real-time video feed. The success of this project will be directly applied to the development of ultrasonic pathways for symmetric key distribution, securing the vital AES symmetric keys used for data encryption. Further, exploration of machine learning and artificial intelligence techniques for cyberattack detection will allow operators to detect attacks before they can cause permanent damage.

ACKNOWLEDGEMENT

This material is based upon work supported under an Integrated University Program Graduate Fellowship. Any opinions, findings, conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Department of Energy Office of Nuclear Energy.

REFERENCES

[1] M. Baezner and P. Robin, "Stuxnet," ETH Zurich , Zurich, 2017.

[2] A. Matrosov, E. Rodionov, D. Harley and J. Malcho, "Stuxnet Under the Microscope," ESET LLC, 2010.

[3] K. Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," Wired, 3 November 2014. [Online]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[4] R. Lee, M. Assante and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," E-ISAC, Washington DC, 2016.

[5] K. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, 3 March 2016. [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[6] D. Das, "An Indian nuclear power plant suffered a cyberattack. Here's what you need to know," The Washington Post, 4 November 2019. [Online]. Available: https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/.

[7] X. Huang, J. Saniie, S. Bakhtiari and A. Heifetz, "Ultrasonic Communication System Design using Electromagnetic Acoustic Transducer," in *2018 IEEE International Ultrasonics Symposium (IUS)*, 2018.

[8] X. Huang, J. Saniie, S. Bakhtiari and A. Heifetz, "Applying EMAT for Ultrasonic Communication through Steel Plates and Pipes," in *2018 IEEE International Conference on Electro/Information Technology (EIT)*, 2018.

[9] X. Huang, J. Saniie, S. Bakhtiari and A. Heifetz, "Software-Defined Ultrasonic Communication System Based on Time-reversal Signal Processing," in *2019 IEEE International Conference on Electro Information Technology (EIT)*, 2019.

[10] X. Huang, J. Saniie, S. Bakhtiari and A. Heifetz, "Time Reversal Signal Processing for Ultrasonic Communication through Metal Channels," in *2019 IEEE International Ultrasonics Symposium (IUS)*, 2019.

[11] X. Huang, J. Saniie, S. Bakhtiari and A. Heifetz, "Performance Evaluation of High-Temperature Ultrasonic Communication System," in *2020 IEEE International Ultrasonics Symposium (IUS)*, 2020.

[12] X. Huang, J. Saniie, D. Arnold, T. Fang, A. Heifetz and Bakhtiari, "Software-Defined Ultrasonic Communication System with OFDM for Secure Video Monitoring," *IEEE Access*, no. 10, pp. 47309-47321, 2022.

[13] X. Huang, D. Arnold, T. Fang and J. Saniie, "A Novel Encryption/Decryption Framework for Ultrasonic Secure Video Transmission," in *2021 IEEE International Ultrasonics Symposium (IUS)* , 2021.

[14] X. Huang, D. Arnold, T. Fang and J. Saniie, "A Chaotic-based Encryption/Decryption System for Secure Video Transmission," in *2021 IEEE International Conference on Electro Information Technology (EIT)*, 2021.

[15] D. Arnold, J. Ford and J. Saniie, "Machine Learning Models for Cyberattack Detection in Industrial Control Systems," in *2022 IEEE International Conference on Electro Information Technology (EIT)* , 2022.

[16] B. Chardin, J.-M. Lacombe and J.-M. Petit, "Data Historians in the Data Management Landscape," in *Technology Conference on Performance Evaluation and Benchmarking*, Berlin, 2012.

[17] S. K. Jensen, T. B. Pedersen and C. Thomsen, "Time Series Management Systems: A Survey," *Transactions on Knowledge and Data Engineering*, vol. 29, no. 11, pp. 2581-2600, 2017.

[18] Apache Software Foundation, "MLib is Apache Spark's Scalable Machine Learning Library," Apache Software Foundation, [Online]. Available: https://spark.apache.org/mllib/.

[19] T. Morris, Z. Thornton and I. Turnipseed, "Industrial Control System Simulation and Data Logging for Intrusion Detection System Research," in *7th Annual Southeastern Cyber Security Summit*, 2015.