Proceedings of the International Conference on Artificial Intelligence and Smart Systems (ICAIS-2021)
IEEE Xplore Part Number: CFP21OAB-ART; ISBN: 978-1-7281-9537-7

Securing Drone-based Ad Hoc Network Using Blockchain

[1]Vijay A. Kanade,
[1]Researcher, Pune, India
kanade.science@gmail.com[1]

2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS) | 978-1-7281-9537-7/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICAIS50930.2021.9395816

Abstract — The research proposal discloses a novel drone-based ad-hoc network that leverages acoustic information for power plant surveillance and utilizes a secure blockchain model for protecting the integrity of drone communication over the network. The paper presents a vision for the drone-based networks, wherein drones are employed for monitoring the complex power plant machinery. The drones record acoustic information generated by the power plants and detect anomalies or deviations in machine behavior based on collected acoustic data. The drones are linked to distributed network of computing devices in possession with the plant stakeholders, wherein each computing device maintains a chain of data blocks. The chain of data blocks represents one or more transactions associated with power plants, wherein transactions are related to high risk auditory data set accessed by the drones in an event of anomaly or machine failure. The computing devices add at least one data block to the chain of data blocks in response to valid transaction data, wherein the transaction data is validated by the computing devices owned by power plant personnel.

Keywords-Drone-based Ad Hoc Network, Blockchain Model, Security, Privacy, Power Plant, Acoustic Information, Anomaly Detection.

I. INTRODUCTION

Power plants these days are monitored by number of sensors that are explicitly mounted on the complex machines. These state of the art monitoring systems are designed to generate alarms if certain parameter values under consideration exceed the defined threshold limit. The threshold is generally static in nature which is based on technical standards or commissioning phase experience. Further, the sensors deployed on the machines are also static, as they are fixed in certain hot-spots that are likely to receive signals from all parts of the machine that is prone to failure. However, in today's date, the power plant machines are highly complex and huge in size, like hydropower plants, nuclear power plants, and so on. The immense size of these machines make it difficult for the static sensors to monitor in real time and take proactive action immediately in case of any anomaly. Hence, there seems to be a long standing need for alternative monitoring systems that serve well than the currently deployed mechanisms.

The research proposes a novel drone-based ad hoc network for power plant surveillance. The network acts as a 'mobile monitoring system' that enables continuous monitoring of large power plant machinery and equipment simultaneously by harnessing acoustic information of the machines via drones.

The discussed surveillance system zeros-in on security and privacy of the network and the power plant as the system uses blockchain model for monitoring purpose. Further, to ensure enhanced security in communication and prevent any interference with the safety and control system of the power plant by design, only one-way data transfer away from the power plant is enabled. Overall, the proposed system provides a viable solution for monitoring any power plant as the solution does not tinker with the physical machines or requires any physical modifications of the same.

II. CHALLENGES OF POWER PLANTS

Maintenance of power plants poses number of challenges. One major challenge is the remote location of most power plants such as hydropower. These remote locations are tricky, as most of them are difficult to get easy access to, while others stand unreachable during harsh weather conditions like monsoon or chilly winter.

Second prominent challenge associates with the kind of expertise and staff training needed for the personnel in rural areas. Hence the reason, most power development projects such as hydropower require extensive training of local labor to ensure the safe operation of the plant.

In addition, many power plants are only inspected in intervals of weeks or months. This raises an alarm over the fact that the power plant could suffer major failure post inspection day or in between the regular cycles of inspection. Such failures generally go unnoticed and can later lead to severe damage to the plant components, equipment or machinery.

These challenges are overcome by employing the proposed drone-based networks. The acoustic surveillance network acts as a smart & mobile monitoring system that autonomously monitors the running equipment by hovering over the critical plant machinery 24x7. An important factor of concern for such systems is the data connectivity they have to the power plants, which has been under scrutiny traditionally. It is a known fact that the connections routed through the Internet, are regulated by national standards and laws. Therefore, as we deploy drones for the purpose of monitoring the power plants, the security over the internet connection & drone-to-plant communication is ensured by enabling only one-way data transfer away from the power plant and further safeguarding the communication by employing blockchain model for the same in case of valid transactions.

III. CLASSICAL SURVEILLANCE (USE CASE)

Consider an example of a typical hydropower plant. Here, the surveillance system is integrated with the control system of the plant. The sensors are retrofit on machines at specific locations and are focused on specific monitoring parameters. This retrofitting of sensors requires the physical machinery modifications.

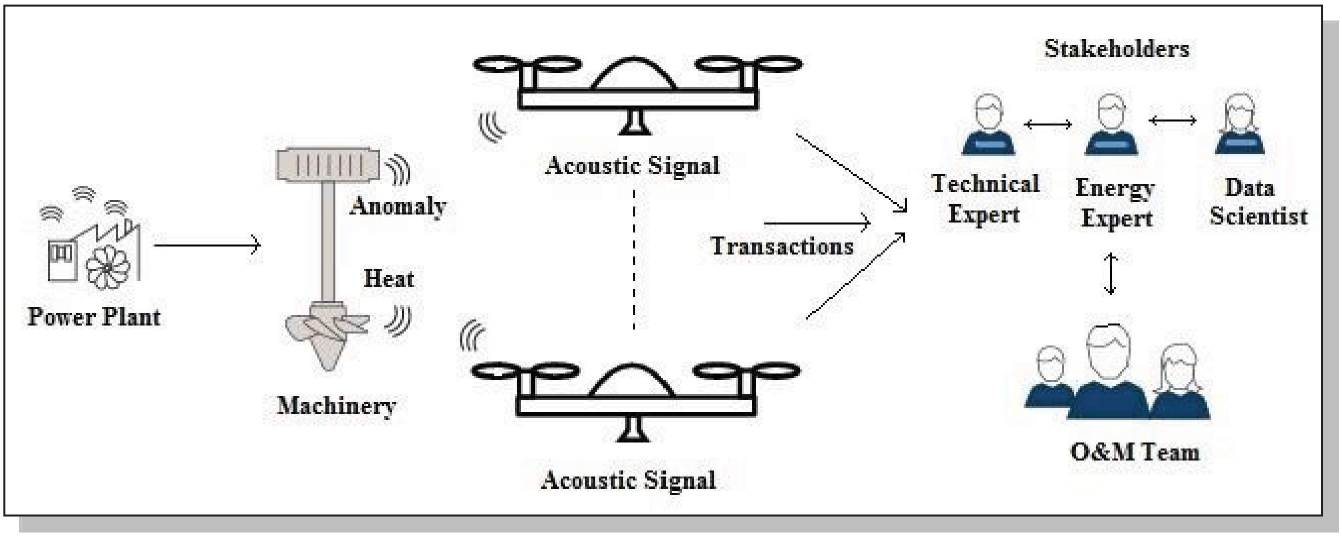

Figure 1: Proposed Drone-based Ad Hoc Network Harnessing Blockchain Model for Power Plant Surveillance

Further, the engineers define the threshold limits for these alarms during the initial design phase. The limits may comply with a norm like DIN ISO 7919-5, where sensors track the maximum relative vibration displacement limits for the underlying machinery. The limits are statically set by the personnel as these are derived from statistical data study carried out at various hydropower plants. These limits differ from plant to plant, as conditions, load, power requirement vary at each plant. Thus, while commissioning of hydropower plants, these limits are consequently adjusted based on the plant requirement [5]. Hence, the entire process of surveillance system observed in classical approach is static in nature. Any untimely anomaly or failure is seemingly difficult to trace by this approach.

IV. PROPOSED SURVEILLANCE DESIGN

Generally, in big power plants, before the actual machine failure, the plant shows indicators of the issue via acoustic data through noise, excessive heat generation or even odor in some cases. All these indicators are noticeable, although the classical approach doesn't observe them since the alarm threshold limit is not yet reached. Machine or component failure is evident in its early stages and becomes more noticeable as the danger mounts on. This can be tracked by the personnel inspecting the plant, however monitoring every equipment present a challenge to human personnel. Hence, the surveillance system that monitors these dynamically changing trends can essentially identify the anomaly at very early stages.

This problem is tackled by using the proposed drone-based ad hoc network that collects extensive acoustic information from larger spaces, equipment, or machinery like the turbine pit, via surveillance drones and effectively communicates the data to the concerned computing devices. The drone-based system is live 24x7, thereby making the diagnostic system full proof, dynamic and mobile. The drones track the changing trends in machine behavior and note the specific patterns, thereby relating them to past events.

The deployment of novel drone-based network seems plausible today as the required technology, resources and algorithms are implementable in current technological era.

The proposed drone-based solution provides advanced diagnostic and predictive analysis for future events by following below steps:

1. Identify fingerprint of the "normal" situation by collecting large training samples: This step forms the basis for detecting any abnormal situation, anomaly or machine failure.
2. Classify samples showing anomalies based on its type: Post collecting significant number of anomalies, classification of similar anomaly types can be done automatically.
3. Acoustic taxonomy creation: Here, further classification of sound events is done, which involves 'sonification' of non-audible early indicators like odor, heat, to name a few. This classification compares current events with past experiences by involving concerned experts.

Following the above steps, the drone-based surveillance system can now be trained to resolve specific anomalies in addition to its detection. Prediction is the next step post resolution of detected events. Figure 1 represents the system architecture of the proposed drone-based ad hoc network.

V. SONIFICATION

Acoustic taxonomy creation involves sonification which is defined as a technique that transforms any form of data into sounds, where any form of data essentially implies non-speech audio. In simple terms, sonification relates to transformation of data into perceived acoustic signals that can facilitate communication or further interpretation for specific use.

Research work in this field has seen examples as reported in [2], where the electricity consumption of various appliances operating in a home was sonified. The work was aimed at increasing user's awareness of household electricity consumption, keeping in mind the sustainability factors. In another example, a sonification prototype was developed for acoustic monitoring of manufacturing processes and production machines by employing array of static microphones onto a production machine that are able to detect anomalies or faults in the manufacturing process based on sound recorded by the microphones [3]. In another recent example, NASA used sonification for turning astronomical images captured by Chandra X-Ray Observatory and other telescopes into sound [1].

Similarly, the proposed drone-based surveillance system sonifies the non-audible indicators like odor, heat, color, observed at the power plants for detecting any signs of anomaly or machine failure. This helps in accommodating all types of unnatural events unfolding at the power plants into sounds. These sounds are perceivable by the drones that

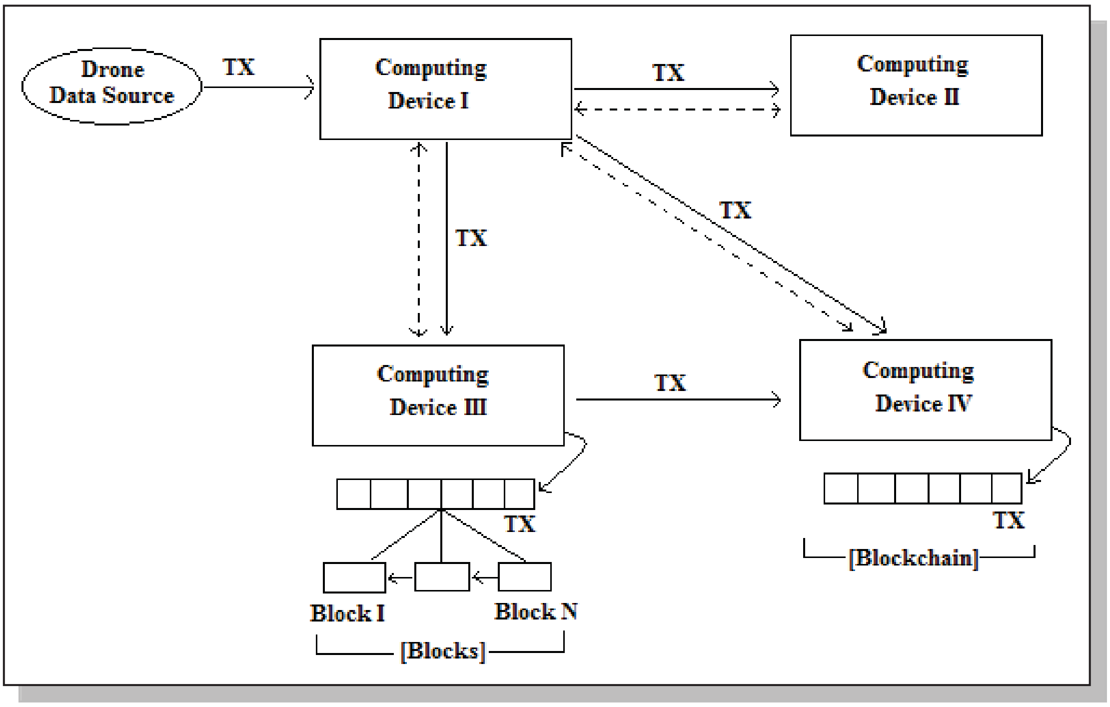

Figure 2: Blockchain Model

process auditory information for early failure identification and take proactive action against them in real time. The proactive response by the drone-based network is supported by blockchain model that records each transaction of the power plant and promotes data security and privacy, thereby keeping the system safe from external attackers that eavesdrop the network communication and tamper data with criminal intent.

VI. BLOCKCHAIN MODEL

The blockchain model ensures secure communication between the power plant and the drones [4]. The drone-based network tracks and appends acoustic data related to drones, specifically when the risk factor is relatively high. Here, risk factor accounts for acoustic information that sends alarm signals to the drones indicating that something is amiss in power plant's operation, leading to immediate detection and attention of the concerned staff. This data is managed by the network as a part of chain of data blocks (i.e. blockchain) associated with recent and past events. In this manner, various drone-based network parameters are securely tracked using chain of data blocks. The parameters could include weather conditions, drone path, etc. Transaction data (i.e. acoustic information) can be appended into chain of data blocks whenever the risk level red flags the drones about the plant situation.

As and when the transaction is conducted, the corresponding drone in the ad hoc would send the data to one or more of the computing devices in the network for validation and thereby generate a new block. On validation and calculation of the new block, it would be added to the network's blockchain. Here, computing devices are in possession with the stakeholders of the power plant like plant owner, machine diagnostic expert, plant operator, data scientist and so on. The transactions are validated by these stakeholders as they decide on whether to add the transaction in the blockchain or reject it. The blockchain infrastructure also helps in identifying non-compliant drones as their activities are recorded in a protected ledger. This includes if the drone flies close to a dangerous plant machinery, it could trigger a risk flag. This could in turn allow the drone-based network to collect more of plant data and provide the data to its operator if required.

Note: Computing devices can include smartphone, laptop, notebook, desktop, palm top or any other handheld devices. Also, Figure 2 depicts the operation of the blockchain model in the drone-based ad hoc network.

Blockchain Working

Each block in the blockchain has three basic elements:

- Data within the block.
- A nonce - A 32-bit whole number that is randomly generated on block creation, and further facilitates a block header hash generation.
- Hash - A 256-bit number wedded to the nonce.

In the current blockchain model, each new entry on a ledger represents a block of information (i.e. representation of acoustic event), copies of which reside on multiple computing devices in the drone-based network. A hash function (i.e. a mathematical function maps data of any size to a sequence of individual fixed-size values) is executed on each data block of chain. The output number of this hash function (called as hash) produces a key. This key becomes the first entry in the next linked block. Therefore, visiting the block later and changing the contents of the previous block would also change its key, thereby affecting the first entry in the next block and its key, and so on. This connection of block-content and the derived hashes ensure that the integrity of the chain is well maintained and not tampered with.

In the proposed drone-based network, each computing device in the network is configured to assist in computing the blockchain. As seen in the Figure 3, each block (starting from block 2) includes a new transaction data for the associated drone along with a hash value computed for the previous block. Thus, each data block represents a set of transaction data in addition to a set of all previous transaction data.

Block 1	Block 2	Block 3	Block 4	Block 5		Block N
Drone Transaction 1	Drone Transaction 2 + Hash of Block 1	Drone Transaction 3 + Hash of Block 2	Drone Transaction 4 + Hash of Block 3	Drone Transaction 5 + Hash of Block 4	. . .	Drone Transaction N + Hash of Block N-1

Figure 3: Blockchain Representation

Tracking Potential Failures

Figure 4 represents the audible patterns generally observed at power plants that could be detected by using the proposed drone-based surveillance system. The events shown in the figure could actually led to an unplanned stoppage of the plant machinery with major repair task at hand. Therefore, an early indication by using the proposed ad hoc network leveraging acoustic information would prevent major damage and significantly lower the maintenance costs of the power plants.

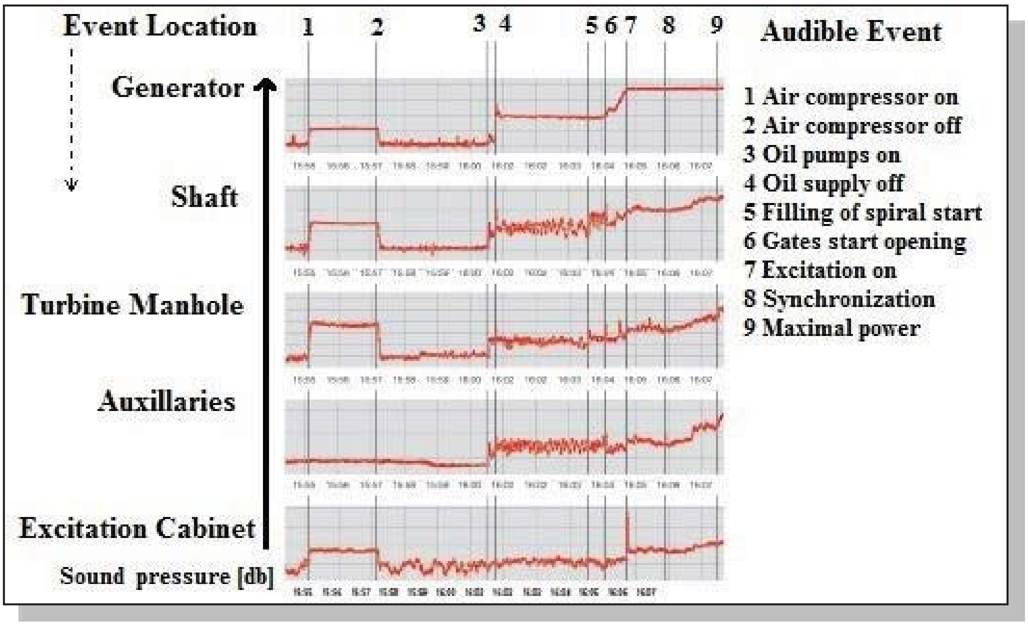

Figure 4: Audible Patterns Generally Observed at Power Plants [5]

VII. Conclusion

This paper introduced the drone-based ad hoc network as a novel paradigm that uses acoustic information for early detection of anomalies or issues with the complex power plants which can help in addressing the problems in real time. The network uses blockchain model for securing the communication between the drones and the power plants, thereby enhancing the security between the said devices. The network employs heterogeneous computing devices for tracking and appending transactions into the blockchain maintained by the surveillance system. We presented a vision for the emerging drone-based acoustic research field, which stems from different lines of existing research including IoT, sound computing, AI and HCI [6]. The proposed research offers many unprecedented opportunities along with technical and non-technical challenges that we expect will be addressed in the years to come by both academic and industrial research.

This is arguably the first paper to introduce the drone-based ad hoc network that utilize acoustic information for monitoring the power plants. The proposed solution could help in reducing the risk of unplanned outages, recognizing degrading equipment at early stages, and support maintenance crews by guiding them to the target area of the plant needing attention.

Future Work

Considering the merits and utility of the paper, we intend to extend the paper to various applications such as search and rescue operations (disaster recovery), crop monitoring, traffic congestion control, monitor natural resources like oil, space science, environment monitoring systems and many more.

Acknowledgment

I would like to thank Dr. A. S. Kanade for his relentless support and guidance.

References

[1] NASA, Data Sonification: Sounds from Around the Milky Way, September 22, 2020.

[2] D. Lockton, F. Bowden, C. Brass, and R. Gheerawo, "Powerchord: Towards ambient appliance-level electricity use feedback through realtime sonification," in International Conference on Ubiquitous Computing and Ambient Intelligence. Springer, 2014, pp. 48–51.

[3] B. B. Bederson, "Audio augmented reality: a prototype automated tour guide," in Conference companion on Human factors in computing systems. ACM, 1995, pp. 210–211.

[4] Abhishek Kumar, Ashish Kundu, Clifford A. Pickover, Komminist Weldemariam, US20180270244A1, Unmanned aerial vehicle data management (IBM), September 20, 2018.

[5] InTech Magazine, ISA's Flagship Publications, Acoustic monitoring systems, July-August 2019

[6] Wang, Haoxiang. "IoT based Clinical Sensor Data Management and Transfer using Blockchain Technology." Journal of ISMAC 2, no. 03 (2020): 154-159.