The Internet of Things and Issues for Mine Water Management

Michael Losavio[1], Adrian Lauf[2], Adel Elmaghraby[2]

[1]Department of Criminal Justice, College of Arts and Science, University of Louisville, KY, USA. Michael.losavio@louisville.edu

[2]Department of Computer Engineering and Computer Scinec, Speed School of Engineering, University of Louisville, KY, USA. Adrian.lauf@louisville.edu, Adel.elmaghraby@louisville.edu

Abstract

The Internet of Things and the Smart City offer an unprecedented distribution of sensors for the collection of data, including data on water quality. We qualitatively examine this application for mine water monitoring and remediation.

We examine current discussion and deployment to anticipate application of new data technologies relating to water and mining activity.

Keywords: Internet of Things, IoT, Sensors, Water Quality, Wireless

Introduction

Present mine water monitoring systems

According to (Drobniewski and Witthaus 2017), mine water monitoring consists in part of monitoring water level and composition to avoid adverse effects on natural and public life. Understanding the composition and level is done through manual tests with water level probes and samples that are gathered and returned to the surface for analysis. This presents the unique opportunity for integrating real-time sensing in the form of Internet of Things (IoT) devices, capable of providing contemporaneous and repeated measurements, along with networking technologies that can provide infrastructure, fault tolerance, and a communications backbone to surface systems and management.

Overview of IoT trends

Devices that fall into the IoT category include traditional "smart home" devices, such as light switches, locks, cameras, and security devices. However, many additional device classes can be counted, as more control and measurement devices are being found on traditional and industrial network systems, such as SCADA networks (Chikuni and Dondo 2007). As such, many of these interconnected devices are equipped with their own network address, and managed or monitored by a centralized controller which is capable of capturing and processing the data from the networked nodes. This indicates that industrial-application devices can also be considered IoT devices, as distributed sensing and control makes its way into application spaces that were not considered viable just a few years ago.

Capabilities and benefits

IoT devices come equipped with four main functions that distinguish them from ordinary sensors, controllers, or actuators. The first is the presence of a dedicated network interface, using a variety of technologies, such as 802.11 (WiFi), 802.15.4 (Zigbee), or a variety of other infrastructure or mesh network radios (Alliance 2007, Jo Woon, Ho Young et al. 2007). The second element is an external controller that is able to use the network infrastructure to communicate with the IoT device. This can be a combination of dedicated hardware or servers, a dedicated server in conjunction with a mobile device, a dedicated controller with multiple access nodes, or other combinations of systems and interfaces. The third element is an actuation and/or sensing system, which either interrupts electrical circuits, performs measurements via sensors, or has physical outputs that are capable of modifying its environment. Lastly, the fourth component is an integrated microprocessor and software combination capable of intelligently monitoring its state of operation, communicating with the controller, and performing the requested modifications of its physical state so as to serve as a functional device.

Networking

With all four elements present and functional, we must briefly understand how networking fits in to the picture. Most modern wireless networking operates within a reasonable line-of-sight (LOS) set of constraints. Though WiFi and cell networks can easily traverse some structural walls in buildings, sufficient density of building materials or distance from a transceiver will render wireless signals unusable to a connected device due to path loss fading and shadowing. Because of this, there is a substantial caveat for using IoT devices in a strongly-constrained environment, such as a mine, for sensing.

A way to ameliorate path loss and shadowing is through the use of intermediary nodes that act as signal repeaters, effectively bridging the network around obstacles. An entire category of IoT networking technologies permits this to occur, using peer-to-peer, dynamic mesh networking. Several such protocols exist, including 802.15.4, the ZigBee protocol (Akkaya and Younis 2005). Clear advantages exist in the sense that these devices provide infrastructure via their ad-hoc network meshes, as well as fault tolerance by routing requests through as many networks as possible. Thanks to these advancements, along with the careful positioning of repeater infrastructures, we believe that IoT-like devices will easily serve as a new class of monitoring device for mine water management.

Legal Aspects

A regime of safety with the Internet of Things is part and parcel of administrative regulation for ensuring public safety. Governance of cyber-physical systems is squarely within the notion of the information polity, the laws and regulations and practices and procedures that order life in society. The challenge is mapping these within any particular domain from the features and aspects generally of the technology and the regulatory regime (Losavio et al. 2017, Losavio et al. 2018, Losavio et al. 2018). This holds for issues of mine safety and mine water management.

As with information security in particular, public safety begins generally by identifying the elements to be secured; with information systems, and particularly to computers, networks and the Internet we look at characteristics to be secured, such as authenticity, integrity, access control, confidentiality, and privacy. Device safety and reliability is of primary importance generally within the Internet of Things, and critical to systems for mine safety and monitoring. But how that device is used by a person can compromise the devices safety to others. Accountability for misuse may be very important.

(Charou et al. 2010) found from three test sites that the ability to remotely sense and report data can allow for the monitoring and identification of sources of pollution and the areas affected, including changes in land use and water bodies. High-resolution satellite remote sensing data and GIS integrated with geospatial databases were sufficient to provide this for long-term environmental management and monitoring for mining area reclamation.

(Li and Liu 2009) described the effectiveness of wireless sensor networks in underground coal mine monitoring via a mesh sense or deployment. There Structure-Aware Self-Adaptive wireless sensor network (SASA) could detect structure variations caused by underground collapses.

Commentators have begun to realize extraordinary benefits that may be presented by the Internet of Things. (Pickup 2017) noted:

> The Internet of Things, especially through wearable technology, will produce extraordinary improvements in productivity and safety. Notable is the SmartCap sensors in a ballcap that can monitor worker fatigue levels via a cellular network, anticipating future technologies for worker health and safety. Another area of development is the integration of location and environmental monitors for ventilation and devices for equipment maintenance.

Mielli (2013) opined that the Internet of Things within the mining space might be seen as an extension of industrial control systems integrated into a broader area of operations for the mine (if not all). These would include the miners themselves, their equipment and censorious for activities within the mine.

These would enhance mine safety, including via environmental response monitoring and enhance efficiency by the optimization of activities. And as with the Smart City integration, this would provide for "Smari Asset Management" to monitor and optimize the use of capital-intensive systems within the mine.

Most optimistic are the comments of Alexandre Cervinka, founder and CEO of Newtrax, that the future of mining was here with the Internet of Things (Newtrax 2018). He found that the most important aspect of IOT implementation was the real-time monitoring of activities, including ecological and environmental issues of mine ground, air and water. IOT will also offer better systems management of machines and safety for personnel via the expanded deployment integration of sensors and the analytics to best utilize that data to identify efficiencies, risks and benefits.

IoT Devices and Sensing

As mentioned in the Introduction, wireless sensor network devices that fit into the IoT realm must feature four components that indicate their adherence to the IoT space. According to (Drobniewski and Witthaus 2017), modern sensing systems for mine water quality monitoring can be in the form of installed probles, based on modified deep-sea observation devices. As they are large devices, these systems are excellent candidates to be retrofitted with mesh networking technologies that would permit distributed monitoring of a number of mine water sites of interest. When properly equipped with repeater technologies, these probes would be capable of producing self-sufficient networks that can route data reliably from probe to destination controller, as well as route back the necessary control and monitoring commands that are needed to keep the probe operational. As such, these probes can be modified to meet all four conditions of IoT device characteristics, provided server architecture is provided.

Wireless Sensor Newtorks and Power Infrastructure

To expand on the coverage concerns related to path loss and shadowing, underground mines present a unique connectivity challenge, as rock and soil is not typically an easy barrier for wireless networks, particularly if the content of these obstacles is ferrous. We propose that each mine is a unique case, and that there exists no "one-size-fits-all" networking technology that is applicable to each case. For instance, in surface-based mines, where the water quality is easily observable above-ground, traditional infrastructure-based networks may be sufficient. However, in underground environments, both monitoring nodes and network repeaters must be presented in such a way that data is reliably sent and received. This carries further complications that power supply may not be readily available, both to the measuring instruments (which are IoT devices), and/or to the repeater nodes.

A variety of networking technologies exist to solve these problems. For instance, the ZigBee protocol is both a long-distance and a low-power network architecture, which needs only minimal power to operate (Alliance 2007). ZigBee can operate in both infrastructure and mesh networking modes, which means that the low power consumption makes it ideal for battery-powered devices. Furthermore, network routing protocols, such as the Ad-hoc On-demand Distance Vector routing protocol (Perkins and Royer 1999), means that nodes are able to "find" each other every time a datagram must be sent from node to controller or vice versa. These "on-demand" methods are well-suited to systems that have infrequent traffic, such as mine water monitoring systems, and can thus serve as applicable candidates to modernize data acquisition and control in otherwise difficult operational environments.

Network Security

Of course, each networked node serves as a potential access point for unauthorized access. Mine water monitoring, because it can be relatively infrequent compared to traditional computer and mobile networks, can be protected via a number of systems. The first of these is an anomaly-based intrusion detection system. Work by (Lauf, Peters et al. 2010) has demonstrated that anomaly detection is effective in determining when intrusions have taken place in systems exhibiting periodic behaviors. Furthemore, with the advent of formal verification methods, as shown in [Sabraoui], the network nodes themselves can classify and understand verified and validated data and commands which can only be transmitted by valid software and network combinations. Security aspects exist anywhere that a wired or wireless system is present. However, we also believe that proper protocol and security service integration can provide sufficient protection for these application-specific network technologies, provided that the protocols and software are regularly maintained and updated when vulnerabilities are discovered.

Legal Concerns

A regime of safety with the Internet of Things is part and parcel of administrative regulations for ensuring public safety, of which the regulation of the extremely dangerous internal environments of mining and the external damages collateral to mine operations are vital. Governance of cyber-physical systems is squarely within the notion of the information polity, the laws and regulations and practices and procedures that order life in society. The challenge is mapping these within any particular domain from the features and aspects generally of the technology and the regulatory regime. Public begins generally by identifying the elements to be secured; with information systems, and particularly to computers, networks and the Internet we look at characteristics to be secured, such as authenticity, integrity, access control, confidentiality, and privacy. Device safety and reliability is of primary importance generally within the Internet of Things, and critical to systems for mine safety and monitoring. But how that device is used by a person can compromise the devices safety to others. Accountability for misuse may be very important.

And these map between elements of a program for information security and the security components of criminal and civil justice. Prevention is promoted by the criminal justice goals of deterrence, rehabilitation and incapacitation of the human offender; similarly, money damages within the civil justice system encourage accountability. Rehabilitation in particular may support detection and recovery as the skills of the rehabilitated offender are used in monitoring and analysis of the effect of attacks.

Yet the public and private information spheres itself continues to grow and grow and grow, creating new risks and opportunities. This can be seen in the various both internal and external deployments of sensors relating to mine activity and potential wealth of actionable data from the Internet of things deployed within and without mining environments.

Table 1, below, notes the various sensors and data from mine systems that may integrate with the Internet of Things.

If we consider the relative data spaces between that which is "private" and that which is "public," eg., the data which is extant, aggregated and subject to analysis, we have an evolving situation of danger relative to these data spaces.

This identifies both the richness and benefits of the IOT deployment within mines and mining environments as well as regulatory issues that must be faced. Within either the civil or criminal justice system, it is essential that system testing assure reliability. Failure of these critical systems as to internal mine safety and external mine water environmental damage will, at the least, expose the mining enterprise and makers of the IOT mine systems to civil liability (monetary damages). Given the exceptionally dangerous environments, inside and out of the mine, failure of these systems that leads to death or serious physical injury can lead to criminal liability for those same parties as well as anyone using the systems who either intentionally or through gross negligence fails to use them to ensure minor and environmental safety.

It is important to consider the privacy implications of the deployment of these systems. While deployment within a mining environment may generally avoid privacy concerns, use of the data generated may raise questions of liability. But as the systems may also be deployed externally in relation to environmental monitoring, that data may begin to intrude into private spheres of the community for which there is no clear demarcation of both proper conduct and potential legal liability.

Lastly, it is vitally important to consider the liability for the failure to implement these systems. As the power and utility of IOT for mines increases while the cost to decrease, from the cost of sensors and networks to the cost of the analytics, mining operators will have difficulty justifying a failure to use them. Where these technologies could've avoided death, serious physical injury and environmental devastation, a callous failure to deploy them only held against the mine operator and be indicative of their liability for injuries to others. The 2019 Vale Brazil mine dam failure demonstrates the huge human and environmental cost in system failures that could have been avoided.

Conclusions

The sensor networks contained within the Smart City paradigm may be used to address water management and monitoring issues. The deployment of IOT in mining is only now beginning, with primary focus on operational safety and improved efficiency as part of the Industrial Internet of Things. Mine water issues are not yet primary concerns for the use of this technology.

Given the utility of the Internet of Things and the benefits for water management seen in the Smart City paradigm, the industrial Internet of Things as deployed for mine water management they offer substantial advantages in time, cost and efficiency. The deployment of inexpensive sensors, independent or part of wider sensor arrays, can provide real-time monitoring of conditions, including at upstream points we are rapid remediation may be possible. The lessons from general IOT deployment in mining are equally applicable for mine water management can inform system design.

Properly integrated, the Internet of things will allow great advances in the management of wine water and environmental issues as well as the improvement of minor safety and mine efficiency.

Acknowledgements

The authors thank Perm State National Research University for hosting this conference and giving us the opportunity to develop these ideas. The authors, in particular, we thank Prof. Svetlana Polyakova for her work in administering this conference and advising us regarding it.

References

Akkaya, K. and M. Younis (2005). “A survey on routing protocols for wireless sensor networks.” Ad Hoc Networks 3(3): 325-349.

Alliance, Z. (2007). ZigBee Home Automation: The New Global Standard for Home Automation.

Charou, E., M. Stefouli, D. Dimitrakopoulos, E. Vasiliou, O. J. M. W. Mavrantza and t. Environment (2010). “Using remote sensing to assess impact of mining activities on land and water resources.” 29(1): 45-52.

Table 1 - Data Life in the Mine and Mine Environs

Sensor	Data	Effect
On-person miner IOT devices	data alert, environment monitoring, service, navigation, tracking,	Direct-Location, mine environmental conditions, miner health Inferential-associations, actions
Capital equipment IOT devices	speed, acceleration, braking, safety device usage, vehicle status, operational status	Direct-Location, use activity, potential criticalities Inferential-Association, actions
Telephony/ messaging	Telephony activity	Direct-associations, content, activity Inferential-associative networks
Internal Security Cameras	Identification, time, location, mine activity	Direct-Location, identification, actions, associations Inferential-associations, actions
Public Security Cameras	Identification, time, location data , external products	Direct-Location, identification, actions, associations Inferential-associations, actions
Internal Sensor Network	Mine environmental activities, personnel and equipment action	Direct-environmental status, identification, location
External Sensor Network	Environmental activities and downstream effect	Direct-external environmental impact

Chikuni, E. and M. Dondo (2007). Investigating the security of electrical power systems SCADA. AFRICON 2007.

Drobniewski, M. and H. Witthaus (2017). "Monitoring of mine water."

Jo Woon, C., H. Ho Young, J. Chang Yong and S. Dan Keun (2007). Analysis of Throughput and Energy Consumption in a ZigBee Network Under the Presence of Bluetooth Interference. IEEE Conference on Global Telecommunications Conference, GLOBECOM '07.

Lauf, A. P., R. A. Peters and W. H. Robinson (2010). "A distributed intrusion detection system for resource-constrained devices in ad-hoc networks." Ad Hoc Networks 8(3): 253-266.

Li, M. and Y. J. A. T. o. S. N. Liu (2009). "Underground coal mine monitoring with wireless sensor networks." 5(2): 10.

Losavio, M., A. Elmaghraby and A. Losavio (2018). Ubiquitous Networks, Ubiquitous Sensors: Issues of Security, Reliability and Privacy in the Internet of Things. International Symposium on Ubiquitous Networking, Springer.

Losavio, M. M., K. Chow, A. Koltay, J. J. S. James and Privacy (2018). "The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security." 1(3): e23.

Losavio, M. M., A. S. J. J. o. D. F. Elmaghraby, Security and Law (2017). "Security and the Transnational Information Polity." 12(3): 8.

Mielli, F. (2013). "The Internet of Things (IOT) and… Mining operations?".

Newtrax. (2018). "Mining & The Internet of Things (IoT): The Future Is Here." from https://www.newtrax.com/mining-and-iot/

Perkins, C. E. and E. M. Royer (1999). Ad-hoc on-demand distance vector routing. Second IEEE Workshop on Mobile Computing Systems and Applications, WMCSA '99. .

Pickup, O. (2017). The Internet of things is revolutionizing deep mining, Raconteur.