Delay Tolerant Networks for Industry 4.0

1st Jose Garcia
Department of Electrical and Computer Engineering
The University of Texas at San Antonio
San Antonio, USA
Jose.Garcia3@my.utsa.edu

2nd Mevlut A. Demir
Department of Electrical and Computer Engineering
The University of Texas at San Antonio
San Antonio, USA
Mevlut.Demir@utsa.edu

3rd Gabriela Ciocarlie
Department of Electrical and Computer Engineering
The University of Texas at San Antonio
San Antonio, USA
Gabriela.Ciocarlie@utsa.edu

4th John J. Prevost
Department of Electrical and Computer Engineering
The University of Texas at San Antonio
San Antonio, USA
Jeff.Prevost@utsa.edu

2023 18th Annual System of Systems Engineering Conference (SoSe) | 979-8-3503-2723-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/SOSE59841.2023.10178635

Abstract—**Advances in Industry 4.0 are being increasingly incorporated into general manufacturing as stakeholders are persuaded of the benefits. One of the key technologies viewed beneficial to manufactures is the use of 5G wireless communications. While integrating 5G networks into manufacturing settings is seen as necessary to satisfy Industry 4.0 requirements, doing so risks exposing manufacturing networks to threats. While applying safeguards against these threats is critically important, maintaining high availability during active threats is also essential for manufacturing. Delay tolerant networks (DTN), first proposed by NASA for communication using space-based networks, have been shown effective in mitigating the effects of network delay, disruption, and/or disconnection. In this paper, we examine the use of DTN in manufacturing environments. We propose a method for combating network denial and delay attacks, and demonstrate how DTN's self-healing mechanisms leads to emergent behaviors that automatically safeguard manufacturing operations.**

Index Terms—**critical manufacturing, delay tolerant network, DTN, emergent behavior, secure manufacturing**

I. Introduction

The ongoing revolution of Industry 4.0 is creating fundamental shifts in the way companies operate production, manufacturing, and distribution systems. Integration of technologies such as cloud computing, Internet of Things (IoT), information technology (IT), smart automation, and robotics enables manufactures to reach new levels of efficiency and optimization. Potential benefits of incorporating these technologies include improved asset efficiency, quality, and sustainability along with reduced costs [1]. While Industry 4.0 offers significant benefits, it also brings new challenges as the complexity of interconnected systems grows exponentially as devices are added. With the increasing number of connections between devices and hardware, there is a heightened need to ensure network quality and security, which is essential for maintaining efficiency, reliability, and safeguarding sensitive data. Network quality consists of providing the necessary bandwidth to transfer data, low latency for critical applications, and dynamically adapting to changes. Network security on the other hand ensures suspicious activity is monitored and malicious threats are mitigated.

Understanding network anomalies is necessary for Industry 4.0. The overall networks in modern manufacturing settings have become complex due to the number of interconnected endpoints, heterogeneous network topologies, and openness as a result of connecting to outside resources such as the Internet. The advent of 5G technology will satisfy requirements Industry 4.0 demands, but can bring additional complexities. Investigating anomalies is vital to assure all devices and hardware are performing as intended. Anomalies can be categorized as benign or malicious. For benign anomalies, there usually is no threat to cause an administrator to take action. However, monitoring and logging of benign events is still necessary to establish baselines and understand what normal behavior is [2]. In the case of malicious activity, swift action needs to be taken to prevent exposure of internal systems, theft of data, or outright crashing of systems. The manufacturing industry was ranked the third most frequently attacked industry in 2014 [3] and increasingly faces these challenges.

The goal of this work is to evaluate how delay tolerant networks (DTN) can enhance 5G networks in a manufacturing setting. Specifically, we are focusing on the scenario of network anomalies that cause disruption to nodes in the overall network. One of the areas of exploration is whether incorporating aspects of delay tolerant networks creates beneficial emergent behavior by making individual network nodes capable of dynamically mitigating potential disruptions in network communication. This is one outcome in the study of complex system of systems (SoS) environments. The modern manufacturing environment can be modeled as an SoS, which allows for a more holistic view of the relationships between devices and critical network functions.

II. Industry 4.0 Background

A. Past, Present, and Future

Coined as the "Fourth Industrial Revolution", Industry 4.0 is the ongoing digitization of traditional manufacturing processes and control systems to improve production efficiency. While digital technology existed in the past, the technology used was

979-8-3503-2723-6/23/$31.00 ©2023 IEEE

in its early stages and human intervention was required; hence, processes could not be fully automated. In recent years, the proliferation of digital technology has not only allowed for the capability of large compute power, but also the connection of many devices to share large amounts of data. As a result of technology development, requirements surrounding manufacturing and industrial environments have been raised to improve efficiency. Several key features of Industry 4.0 include bridging information technology (IT) and operational technology (OT), big data and analytics, autonomy, high reliability, dynamic use of resources, and interoperability between various systems.

Initially, Programmable Logic Controllers (PLCs) were popular tools to automate processes. PLCs paved the way for automation and are now highly integrated in industrial settings. Next, the explosion of IoT devices has allowed manufactures to gather vast quantities of data analytics. Low cost IoT devices enabled manufactures to understand their machinery at a deeper level. As a feature of Industry 4.0, reliability and resource optimization can be achieved through the use of IoT devices to analyze their output data for preventative maintenance. With the increase of network connections and data from hardware devices, there is a growing convergence between IT and OT [4]. The IT ecosystem supports computing capability that low end devices are incapable of handling. By managing the data generated from OT, IT satisfies the requirements of big data and analytics to improve efficiency. Additionally, the IT layer is not limited to existing on-premises and in fact is more commonly offloaded to cloud providers. Cloud computing resources have become important to incorporate because without the infrastructure to handle, transfer, and analyze data between devices one is left at a disadvantage.

However, for machines to perform remote sensing and automated processes, they need to be connected to work in unison. Improvements on network communications have slowly evolved over time. As with the early Internet, physical cabling was needed for machines in industrial settings to communicate with one another. Communication protocols were developed to effectively capture output and move data. One of the most popular industrial communication protocols is Modbus/TCP. Now seen as the de-facto standard, Modbus/TCP is a variant of the MODBUS family of simple vendor neutral communication protocols for control of automation equipment [5]. As a result of using a TCP interface over ethernet, Modbus/TCP improved network capabilities while maintaining industrial protocol requirements. Further developments in network communications occurred, as the use of IoT and other wireless technologies increased. A modern manufacturing floor can be highly dynamic with autonomous vehicles or robotics in constant motion. Mobile networks utilizing 5G technology are finding use for their coverage range, latency, bandwidth, reliability, and security.

B. *5G in Industry 4.0*

5G is the fifth generation technology standard for broadband cellular networks. The 5G standard specifications were developed in 2017 by the 3rd Generation Partnership Project (3GPP). 5G mobile networks make use of a high band spectrum (millimeter-wave) for high speed, low latency, and capacity [6]. Since millimeter waves have a shorter range compared to microwaves, the small cell concept was introduced to accommodate seamless connectivity. With theoretical speed of up to 10 Gbps, 5G networks are up to 100x faster than their predecessors [7]. With the development of 5G, three key use cases associated with the technology are exposed: enhanced Mobile Broadband (eMBB), massive Machine Type Communications (mMTC), and Ultra-Reliable Low Latency Communication (URLLC) [8]. These use cases arguably find themselves prevalent in Industry 4.0. eMBB satisfies high data transfer rates across a wide coverage area which is needed in manufacturing networks to move data from source to destination. The growing number of connected devices ranging from sensors to computers require mMTC. Lastly, URLLC is geared towards mission critical applications which include disruptions in production workflows. The use of 5G networks will aid in supporting various Industry 4.0 requirements.

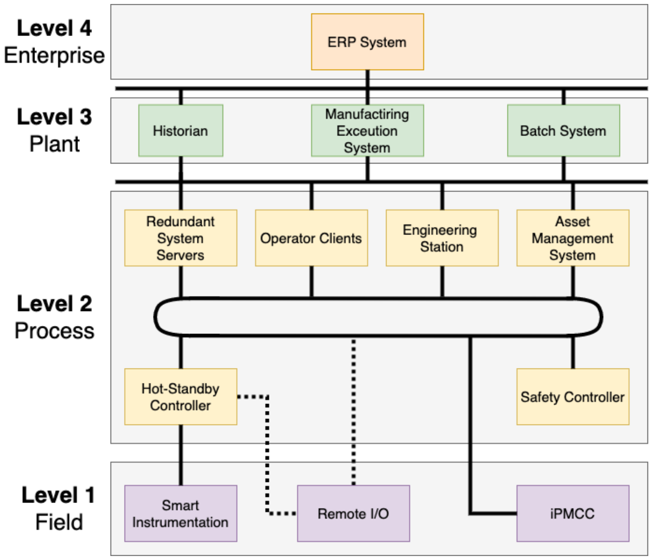

Fig. 1. Typical components of modern control architectures [9]

III. Identifying Potential Problems

A. *Industry 4.0 Problems*

The use of IoT devices and integration with cyber-physical systems (CPS) aid in automating processes and generating data that can be used for analysis and logging of systems. However, with the increasing size of these components, there are problems associated with interoperability, big data, and network strain. Hardware ranging from low-end devices up to high-end servers are all working in unison to handle, transfer, and analyze data. Referring to the typical components of a modern control architecture in Figure 1, there are various layers that are interconnected to transfer data and perform operational processes. At the field level, there can be an array of smart instrumentation gathering informational data for operational and maintenance insights. All these instruments need to be able to send their data up the pipeline for further processing. Depending on the actual device(s) used, there can exist a numerous amount of protocols used for communication. The challenge of interoperability exists in Industry 4.0 with active research being done to address it. For example, work in [10] investigates polling-based and event-based protocols to realize an open and interoperable Industrial-Internet-of-Things (IIoT) environment. Ensuring interoperability from the lowest to highest levels in an architecture is paramount for operation.

However, as more devices become connected, there is an increased need to consider the network. Older legacy systems depend on physical cables for connections between systems. While wired networks likely will not disappear outright, the introduction of wireless and mobile networks have come into play. In fact, wireless networks are pertinent to Industry 4.0 as they will enable dynamic capabilities for robotics and remote sensing applications. Integrating wired and wireless networks into an overall architecture is a problem in itself, but there must also be focus on the data and quality of service these networks can provide once established. Network bandwidth needs to be available to handle the ever increasing size of data moving from the factory floor to the enterprise layer. Speed is also important for critical applications that require low latency communications. These and other requirements must be continuously monitored for abnormal or unusual behavior in order to maintain the integrity and health of the network.

When viewing a modern control architecture such as in Figure 1, anomalies arise from within or outside the network. Security, application performance, user experience, and streamlined processes rely on anomaly detection. With predictive maintenance being a goal of Industry 4.0, anomaly detection to identify patterns deviating from normal behavior is essential. Network anomalies within the overall architecture provide insight into potential issues with devices or machinery before forcible downtime is needed. Kamat and Sugandhi [11] defined an evolution of predictive maintenance beginning with reactionary approaches up to the use of machine learning techniques to predict next failures. Machine and deep learning approaches are the dominant strategies used today for anomaly detection inside the manufacturing environment.

Network anomalies that arise from outside the physical architecture environment often stem from cyber-related threats and attacks. Traditionally industrial networks were able to physically separate themselves from outside networks. However, the increase need to use outside resources via the Internet, wireless access points, or cloud providers has allowed malicious actors to gain access to critical infrastructures. As a result, ongoing cybersecurity issues include active threats on networks ranging from flooding, eavesdropping, or false data injection attacks. In particular flooding attacks such as distributed denial of service (DDoS), are designed to cripple systems and bring them offline rendering them incapable to carry out workloads. According to IBM's X-Force Threat Intelligence Index report, manufacturing was the most attacked industry in 2021 and felt the brunt of cyber attacks as supply chain woes grew [12]. While cyber threats are increasing, there exist cybersecurity tools that can help aid against attacks. Intrusion detection systems (IDS) are an important tool to use as they flag and alert an administrator of suspicious activity. An intrusion prevention system (IPS) takes an IDS another step further by providing proactive steps to block suspicious activity. To use either tool, best practice implementations include automating network analytics, setting baselines of normal behavior, capturing full network activity, and setting thresholds for activity wisely. While IDS and IPS are integral tools used in monitoring and protecting networks, most have rigid requirements, are reactionary in nature, and new iterative baselines for anomalies are needed to be created.

B. How 5G Can Support Industry 4.0

5G will become critical for manufactures as it satisfies previously explained Industry 4.0 requirements and extends to other areas. In particular, 5G will be able to provide security to threats that are becoming prevalent. To begin, non public 5G networks exist strictly within the four walls of a manufacturing environment to gain all the added benefits of 5G technology without inadvertently allowing access to the network. Next, 5G clients can communicate directly with other 5G clients, bypassing the carrier networks. With device-to-device communication, there are less points of access for a malicious actor to discover. However, one important feature of 5G is that all core network systems are based on software virtualization. With virtualization, data can be routed through virtual hubs and switches that can be moved or changed quickly if required. With virtualization and software-defined networking (SDN), the new concept of network slicing is viable in 5G. Network slicing is dividing the physical network into multiple logical networks such that each logical network can be specialized to provide specific network capabilities and characteristics for a particular use case. By virtually partitioning the network, there is less need for additional specialized hardware to handle various network requirements. However, network slicing is still a rather new concept and actively being incorporated into the 3GPP standards [13].

IV. Delay Tolerant Networking

A. Motivation for Delay Tolerant Networks

With the proliferation of satellites and spacecrafts in orbit around the earth and beyond, NASA found the need to enhance communication between these devices. Notably, the issues of signal delay, disruption, or degradation are associated with devices in hostile environments. The obvious scenarios faced by NASA are environments where satellites need to send back data, but there is propagation delay with the data arriving at its destination. Additionally, there are times when no end-to-end path exists between two nodes. As a result, there is potential data loss due to delay, disruption, or disconnection. While these hostile environments are apparent in space, they also exist on earth. It can be argued that the traditional Internet is setup with the infrastructure needed to handle delays/disruptions. However, other networks outside the Internet are growing, needing reliable connections for devices that cannot always guarantee end-to-end connectivity. Mobile, vehicular, and edge-related networks are growing and becoming necessary for some industries. Although initially designed for space environments, delay tolerant networks (DTNs) offer features applicable to Earth-based applications.

B. Description of Delay Tolerant Networks

A desirable trait of DTNs is the store-carry-forward builtin mechanisms which help when disconnections arise. In comparison to the terrestrial Internet that is based on the TCP/IP stack, a DTN assumes no complete end-to-end path. While the TCP/IP model does have ways to protect against delays or disruptions, the assumption is that they are small in nature and do not exist for extended periods of time. The nodes in a DTN are often highly mobile. To support a mobile environment, a redesign or inclusion of routing algorithms is needed. At its core, the biggest factor to account for in DTN routing is the contact time a node has with another node. Again, traditional Internet-like networks assume no break in contact time between two servers and, as a result, gaps in contact time rarely exist. DTN implementations have developed routing algorithms that will be explained in later sections of this paper.

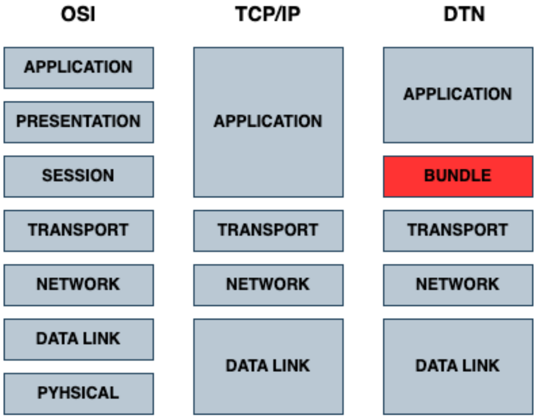

Fig. 2. A DTN network stack compared against the OSI and TCP/IP models. The bundle layer sits above the transport layer.

Another important feature of these DTNs is the ability for nodes to utilize different lower-level transport protocols and still communicate with one another. The layer at which these lower-level protocols are located is the ”convergence layer” (CL) with the interface between the bundle protocol (BP) and underlying protocols being the convergence-layer adapter (CLA). With a region or group of nodes that use the same transport layer protocol, another group of nodes can communicate via a different transport protocol. The bundle layer seen in Figure 2 abstracts the lower-level layer protocols and allows for agnostic communication between nodes. The bundle layer acts as an overlay providing the ability for nodes of different communication standards or hardware to exchange data. Compared to the TCP/IP model, DTN adds a bundle layer. Theoretically, the use of a traditional TCP/IP network can be implemented in unison with a DTN; however, that is not the most interesting case. Still, a region of nodes are able to communicate via TCP/IP, while the other group communicates via another protocol such as STCP [14]. As regions of nodes communicate with each other, they can efficiently exchange data among all nodes in the entire network.

C. DTN Related Works

Over the years stakeholders from space agencies to universities, have researched, developed, or created DTNs. Active research is ongoing and, as a result, some DTN schemes are small in scope and restricted to certain use cases. However, all cases abide by similar characteristics that make them good candidates. Network topology and routing strategy are the dominating topics of research for many implementations. One base assumption of a DTN is that end-to-end connectivity is not guaranteed. As a result, traditional routing methods (i.e. TCP) will not suffice. Traditional computer networks are evaluated using graph theory, which rely on vertices and edges to characterize a collection of nodes. Graphs can be decorated to indicate capacity or cost of connection [15]. While graph theory breaks down, particularly for space applications, an extension of it, named Contact Graph Routing (CGR), is used to combat intermittent connectivity. CGR builds on conventional graph theory by creating a contact plan which is a time-ordered list of scheduled, anticipated changes in the topology of the network [16]. In a similar fashion, the routing algorithm(s) used for a time evolving network are extensions of their predecessors. For CGR, a version of Dijkstra’s algorithm, called the Contact Graph Dijkstra Search, finds paths in the contact graph from the root contact to the terminal contact [15]. While focus on this paper will be directed towards a DTN scheme that uses CGR, other proposed approaches can be found in [15] and other literature.

Inherently DTNs are found in harsh resource constrained environments. For example, nodes in a network topology might consist of devices such as mobile sensors, whose data rates are on the order of several hundred Kbps. When envisioning space applications, naturally these attributes make sense and the DTN implementation is tailored for those characteristics. DTN2 and IBR-DTN [17] are implementations designed for embedded systems. Other schemes that are engineered for embedded environments include DTN cFS Software and Interplanetary Overlay Network (ION) [18] which are NASA solutions which focus on spaceflight applications. Implementations outside of spaceflight exist and range from development of a bundle protocol agent in Ruby [19] to an implementation on mobile phones [20]. Additionally, recent research has produced other DTN architectures that offer better performance than their predecessors. Some of these architectures include DTN Marshall Enterprise (DTNME) [21] and High-Rate DTN (HDTN) [22], both of which are capable of running on generic hardware/software and support higher data transfer rates. For example, HDTN has been tested on a number of hardware platforms including Linux, Windows, Raspbian, and ARM. Additionally, experimental results from [22] demonstrated HDTN capabilities of supporting data transfer rates up to 800 Mbps.

Furthermore, numerous examples of DTNs developed outside the space domain have benefits on Earth. In the early days of DTN research, Fall [23] defined ”challenged internets” both through examples and characteristics. Some examples included mobile terrestrial, sensor/actuator, exotic media, and military ad-hoc networks. While Fall [23] outlined potential use cases, it would take future years of development to put ideas into action. The work from [24] describes an overview of vehicular DTNs, while also providing examples in practice. The concept of store-carry-forward suits well in scenarios of rural areas that do not have Internet connectivity. The KioskNet Project [25] provides low-cost Internet kiosks in rural areas by having buses and DTN protocols be the gateway between the kiosks and the Internet at a neighboring town. Aside from the obvious scenario of a highly mobile network topology, research has be carried out in other areas. Work done in [26] demonstrated the first implementation of the bundle protocol on the Android platform. Motivation for that project stemmed from supplying a redundant method of communication for either security reasons or regional outage of internet services. In the realm of Wireless Sensor Networks (WSN), [27] demonstrates the effectiveness of the BP for WSN-based projects, by showing how 8-bit WSN nodes can seamlessly interact with standard BP implementations. Additionally, work in [28] created a BP binding for the Constrained Application Protocol (CoAP) as a means to enable Delay Tolerant IoT. In a different scenario, Sauer [29] applies DTN to exploit both the mobility and autonomy of robotics in an industrial setting. Lastly, work in [30] demonstrated a superb example of a network in the harsh environment of Antarctica fully exploiting its local communication methods using DTN.

V. Proposed Solution

A. DTN Characteristics of Interest

To realize the potential enhancements for a manufacturing network environment, the key characteristics of DTNs must be outlined. Figure 3 is a Venn diagram showing the relationships between DTN, Industry 4.0, and 5G. Industry 4.0 and 5G share many qualities since Industry 4.0 is highly dependent on 5G technology to fully function. At a high level, mapping DTN features to either 5G or Industry 4.0 is difficult since the design of DTNs is to mitigate delay, disruption, and disconnection. At its core, a DTN strives for high reliability, hence, the reason for its store-carry-forward mechanisms. Furthermore, the BP specifications give DTNs the ability to overlay on top of heterogeneous networks using potentially different transport layer protocols. This advantage can find use in a manufacturing scenario where sensor devices are heterogeneous and utilize different communication protocols, such as TCP and UDP.

Another highlight of a DTN setup is the routing capabilities that are not found in traditional networks. A DTN architecture needs to consider not only the path, but also the contact time between nodes. If a path exists, but contact time has expired between nodes, then the routing algorithm will have provided the next best intermediary for the data to incrementally get closer to its final destination. This is also a safeguard in case the connection between nodes goes down unexpectedly. Many terrestrial networks are stationary with respect to the contact time; however, wireless and mobile networks are becoming more prevalent.

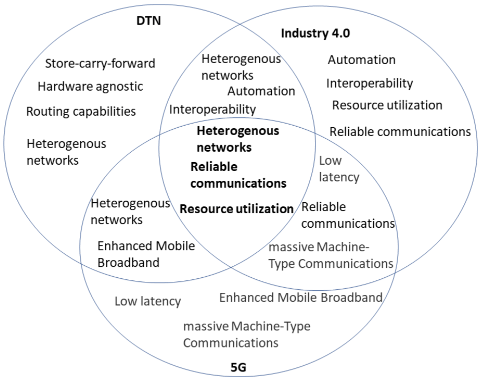

Fig. 3. Characteristics of DTN, Industry 4.0, and 5G.

B. Architecture

Interest in our proposed architecture stems from the array of cyber attacks that are ever increasing in today’s manufacturing environments. Focus is placed on denial-of-service (DoS) or distributed-denial-of-service (DDoS) attacks as these types of attacks are easy weapons to deploy and can be applied to many network infrastructures. Abhishta et al. [31] perform an in-depth analysis of the motivation to use DDOS attacks highlighting the importance of these threats. A survey proposed by Shah and Sengupta [32] outlines how a DOS attack can evolve from inside or outside the target network with attacks also originating from cloud resources as well. To combat these cyber threats, we propose an architecture that provides resilience in the presence of attacks using a DTN overlay working in unison with a 5G network to transfer data throughout a manufacturing environment. By utilizing the store-carry-forward and routing method advantages DTN offers, this setup will be able to dynamically transmit data to its destination, while active cyber attacks are ongoing.

Figure 4 presents a manufacturing setup where sensors are generating data and sending it to remote I/O modules. Data is then transferred from the I/O modules to a corporate public facing file server that uploads it to the cloud. Sensors, I/O modules, and file servers are assumed to perform communications under a 5G network to handle the potential large volume of data transfers. Uploading data to the cloud for the final destination is relevant for collecting provenance information for modern manufacturing environments. The various components in Figure 4 each have their own place within the layers of modern control architectures similar to Figure 1. For example, sensors can be IoT devices which gather data from monitored hardware or their environment and are seen at the field layer. Remote I/O modules ensure data is transferred from field devices to computer systems for operational or batch processing. File servers tend to be server grade hardware and sit in the plant or enterprise layer depending on their functionalities or end goals for the data. Lastly, a cloud or Internet endpoint will sit in a manufacture's enterprise layer as it is a component that is not native to the environment and needs to be incorporated into the network stack at a high level.

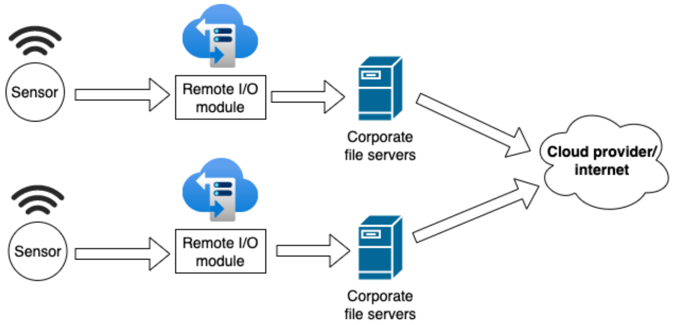

Fig. 4. Normal operations for a manufacturing scenario where sensors, I/O modules, and file servers are communicating with one another and the eventual destination for data is in the cloud.

In Figure 5, an attack is introduced into the network. A DoS attack targets the public facing corporate file server. The file server is exposed to the public Internet as a result of it uploading to the cloud. A DoS attack is used to overwhelm that particular server's available resources rendering it unusable. This has adverse effects on the data pipeline since the bottom I/O module is unable to forward its data to a file server. In this scenario, the I/O module can hold onto data, but eventually it will reach maximum storage capacity. Once at capacity, the module will either need to purge its current data to make room for the incoming sensor data or deny incoming data. Both situations are not ideal as there is a degree of data loss that occurs.

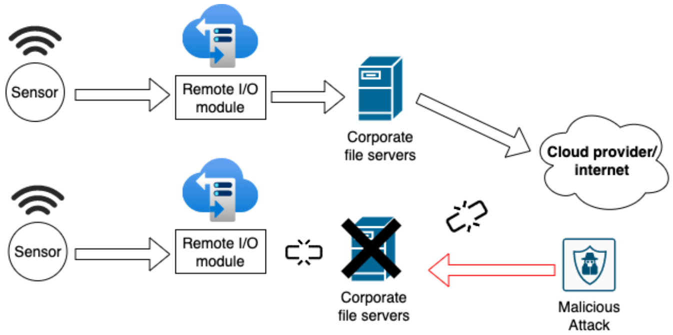

Fig. 5. The same setup for normal operating procedures except a malicious attack brings down a file server. The I/O module tied to the inoperable file server cannot send data out.

Despite an ongoing cyber-attack crippling a file server, in Figure 6, both I/O modules are able to send their data to an available file server. Data originating from both sensors are eventually able to reach their final destination through the use of DTN routes represented with the dashed lines. Raw sensor data is transferred to the I/O modules. The DTN overlay begins at the I/O modules, and, at this point, the sensor data is encapsulated into bundles. Bundles are tagged with their final destination and, as a result, simply make incremental hops throughout the network to their destination. In this scenario, the DTN overlay is aware via IP addresses of the I/O modules, file servers, and cloud endpoint. A contact plan specifying the contact time between nodes is used to help generate a routing table for paths the bundle data can take. In this circumstance, contact time is indefinite between all nodes because there is no expectation of planned disconnection. However, in the case of an unexpected disconnect, routes are recalculated to find the optimal path for the next hop. The DTN overlay allows for a dynamic change in routing that did not previously exist, ensuring limited or no data loss. Upon resolving the attack and bringing the file server back online, the link between the bottom I/O module and file server is re-established, returning the data pipeline to its state as depicted in Figure 4.

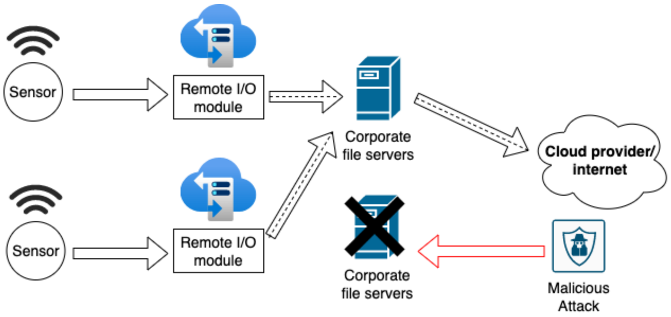

Fig. 6. The dashed lines represent DTN routes in use. Both I/O modules, the file server, and cloud destination are part of the DTN architecture.

C. Discussion and Limitations

A DTN overlay that makes use of its store-carry-forward capabilities is suggested in the proposed solution. As a result of ongoing DTN research, there exist various implementations to utilize. The characteristics seen in Figure 3 provide a good baseline, but further investigation into specific DTN implementations is needed to satisfy Industry 4.0 and 5G requirements. One particular characteristic is the increased data transfers seen with 5G technology which is on the order of Gbps. A DTN implementation that fulfills a high data transfer requirement will be needed. Additionally, the complex device and networking infrastructure in manufacturing environments will call for a flexible implementation to ensure data is successfully transferred from source to destination.

An immediate limitation is the unknown complexity that is associated with adding the BP to the overall network stack. Specifically in our case, there is consideration as to whether a DTN overlay on top of a 5G network will negate advantages from using 5G. While a DTN architecture functions well in traditional networks that do not experience regular disconnection, adding the overlay may not be of interest because the emergent properties of a DTN may not be required in a static reliable network. Integration of the BP can be nontrivial depending on hardware and software requirements. Additionally, the added layer in the stack can potentially cause overall slowdown. Compute power is needed on each DTN node to encapsulate data into bundles, generate routes, or verify payload checksums.

These potential limitations have not yet been fully tested and evaluated.

VI. Conclusion and Future Work

Industry 4.0 will prove to be vital for any modern manufacturing systems to succeed. 5G is an important technology that can significantly contribute to the success of Industry 4.0. While many benefits in these areas can be seen, there are considerations to take into account. Tracking network anomalies for malicious activity will be necessary in complex networking architectures. This work proposes the use of a delay tolerant network imposed on top of a manufacturing environment utilizing a 5G network. The use of a DTN stems from its ability to handle delay, disruption, or disconnection, which are scenarios that exist on a network during active threats. The DTN overlay provides reliability via dynamic resource allocation during unexpected network outages and provides an emergent behavior to the environment that effectively increases the robustness of networks used in manufacturing and other mission-critical domains.

Next steps in this research include adding a DTN overlay on a 5G enabled manufacturing testbed. This planned activity will allow for the analysis of the emergent properties during multiple attack scenarios and will provide an opportunity to determine the overall effectiveness of our proposed solution. Initial investigation into the HDTN software has been performed since it is an implementation that supports high data transfer rates, has been tested on a number of platforms, and has active development from NASA. HDTN appears as a promising candidate to test in our proposed architecture. With the DTN implementation in mind, emulating the manufacturing environment is necessary to view emergent behaviors that arise from the DTN overlay. A potential benefit to using the HDTN implementation is being able to emulate the various manufacturing components on physical hardware since HDTN has been tested on a range of platforms. However, if there exist complexities to install and run the HDTN software a virtual testbed utilizing virtual machines or containers can be used to emulate the manufacturing components. Lastly, metrics to quantify changes before and after a DTN overlay is used will be necessary. Our architecture aims to provide high availability services through dynamic resource allocation. High availability translates to the data pipeline staying online and not losing packets. Potential metrics of interest include DTN bundles received by destination, bundles stored, data rates, and overall timings for transfers to complete.

Acknowledgment

This material is partially based on work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy, under Advanced Manufacturing Office award DE-EE0009046. This research was partially supported by the UTSA Open Cloud Institute.

References

[1] "Digital lean manufacturing." https://www2.deloitte.com/us/en/insights/focus/industry-4-0/digital-lean-manufacturing | Accessed on 2023-02.

[2] L. Stojanovic, M. Dinic, N. Stojanovic, and A. Stojadinovic, "Big-data-driven anomaly detection in industry (4.0): An approach and a case study," in *IEEE international conference on big data*, p. 1647, 2016.

[3] N. Bradley, M. Alvarez, D. McMillen, and S. Craig, "Reviewing a year of serious data breaches, major attacks and new vulnerabilities," *Cyber Security Intelligence Index, IBM X-Force Research*, 2016.

[4] J. Prinsloo, S. Sinha, and B. von Solms, "A review of industry 4.0 manufacturing process security risks," *Applied Sciences*, vol. 9, no. 23, p. 5105, 2019.

[5] A. Swales *et al.*, "Open modbus/tcp specification," *Schneider Electric*, vol. 29, pp. 3–19, 1999.

[6] Y. Tang, S. Dananjayan, C. Hou, Q. Guo, S. Luo, and Y. He, "A survey on the 5g network and its impact on agriculture: Challenges and opportunities," *Computers and Electronics in Agriculture*, vol. 180, p. 105895, 2021.

[7] "5g is poised to change your life." https://www.cisco.com/c/en/us/solutions/what-is-5g | Accessed on 2023-02.

[8] A. Dogra, R. K. Jha, and S. Jain, "A survey on beyond 5g network with the advent of 6g: Architecture and emerging technologies," *IEEE Access*, vol. 9, pp. 67512–67547, 2020.

[9] S. Kriaa, *Joint safety and security modeling for risk assessment in cyber physical systems*. PhD thesis, Université Paris Saclay (COmUE), 2016.

[10] S. Jaloudi, "Communication protocols of an industrial internet of things environment: A comparative study," *Future Internet*, vol. 11, no. 3, p. 66, 2019.

[11] P. Kamat and R. Sugandhi, "Anomaly detection for predictive maintenance in industry 4.0-a survey," in *E3S web of conferences*, vol. 170, p. 02007, EDP Sciences, 2020.

[12] "Ibm report: Manufacturing felt brunt of cyberattacks in 2021 as supply chain woes grew." https://newsroom.ibm.com/2022-02-23-IBM-Report-Manufacturing-Felt-Brunt-of-Cyberattacks-in-2021-as-Supply-Chain-Woes-Grew | Accessed on 2023-02.

[13] S. Wijethilaka and M. Liyanage, "Survey on network slicing for internet of things realization in 5g networks," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 957–994, 2021.

[14] Y. G. Iyer, S. Gandham, and S. Venkatesan, "Stcp: a generic transport layer protocol for wireless sensor networks," in *Proceedings. 14th International Conference on Computer Communications and Networks, 2005. ICCCN 2005.*, pp. 449–454, IEEE, 2005.

[15] A. Hylton, R. Short, J. Cleveland, O. Freides, Z. Memon, R. Cardona, R. Green, J. Curry, S. Gopalakrishnan, D. V. Dabke, *et al.*, "A survey of mathematical structures for lunar networks," in *Aerospace Conference (AERO)*, pp. 1–17, IEEE, 2022.

[16] G. Araniti, N. Bezirgiannidis, E. Birrane, I. Bisio, S. Burleigh, C. Caini, M. Feldmann, M. Marchese, J. Segui, and K. Suzuki, "Contact graph routing in dtn space networks: overview, enhancements and performance," *IEEE Communications Magazine*, vol. 53, no. 3, p. 38, 2015.

[17] M. Doering, S. Lahde, J. Morgenroth, and L. Wolf, "Ibr-dtn: an efficient implementation for embedded systems," in *Proceedings of the third ACM workshop on Challenged networks*, pp. 117–120, 2008.

[18] H. Monaghan, "How do i use dtn?," Nov 2020.

[19] J. Greifenberg and D. Kutscher, "Rdtn: An agile dtn research platform and bundle protocol agent," in *Wired/Wireless Internet Communications: 7th International Conference, WWIC 2009, Enschede, The Netherlands, May 27-29, 2009. Proceedings 7*, pp. 97–108, Springer, 2009.

[20] E. Unnikrishnan, V. Ravichandran, S. Sudhakar, and S. Udupa, "Delay tolerant network for space," in *3rd International conference on signal processing and integrated networks (SPIN)*, pp. 591–595, IEEE, 2016.

[21] "Nasa marshall space flight center, dtnme," 2020. https://github.com/nasa/DTNME | Accessed on 2023-02.

[22] A. Hylton, J. Cleveland, R. Dudukovich, D. Iannicca, N. Kortas, B. LaFuente, J. Nowakowski, D. Raible, R. Short, B. Tomko, *et al.*, "New horizons for a practical and performance-optimized solar system internet," in *2022 IEEE Aerospace Conference (AERO)*, pp. 1–15, IEEE, 2022.

[23] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 27–34, 2003.

[24] P. R. Pereira, A. Casaca, J. J. Rodrigues, V. N. Soares, J. Triay, and C. Cervelló-Pastor, "From delay-tolerant networks to vehicular delay-tolerant networks," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 1166–1182, 2011.

[25] S. Guo, M. H. Falaki, E. A. Oliver, S. Ur Rahman, A. Seth, M. A. Zaharia, and S. Keshav, "Very low-cost internet access using kiosknet," *ACM*

SIGCOMM Computer Communication Review, vol. 37, no. 5, pp. 95–100, 2007.

[26] H. Ntareme, M. Zennaro, and B. Pehrson, "Delay tolerant network on smartphones: Applications for communication challenged areas," in *Proceedings of the 3rd Extreme Conference on Communication: The Amazon Expedition*, pp. 1–6, 2011.

[27] W.-B. Pöttner, F. Büsching, G. Von Zengen, and L. Wolf, "Data elevators: Applying the bundle protocol in delay tolerant wireless sensor networks," in *2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012)*, pp. 218–226, IEEE, 2012.

[28] M. Auzias, Y. Mahéo, and F. Raimbault, "Coap over bp for a delay-tolerant internet of things," in *2015 3rd International Conference on Future Internet of Things and Cloud*, pp. 118–123, IEEE, 2015.

[29] C. Sauer, M. Schmidt, and M. Sliskovic, "Delay tolerant networks in industrial applications," in *24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, p. 176, 2019.

[30] A. Mallorquí, A. Zaballos, and D. Serra, "A delay-tolerant network for antarctica," *IEEE Communications Magazine*, vol. 60, no. 12, p. 56, 2022.

[31] A. Abhishta, W. van Heeswijk, M. Junger, L. J. Nieuwenhuis, and R. Joosten, "Why would we get attacked? an analysis of attacker's aims behind ddos attacks.," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 11, no. 2, pp. 3–22, 2020.

[32] Y. Shah and S. Sengupta, "A survey on classification of cyber-attacks on iot and iiot devices," in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 0406–0413, IEEE, 2020.