Creative Construction Conference 2019, CCC 2019, 29 June - 2 July 2019, Budapest, Hungary

Cyber security challenges and vulnerability assessment in the construction industry

Bharadwaj R. K. Mantha\textsuperscript{a,*}, Borja Garcia de Soto\textsuperscript{b,c,*}

\textsuperscript{a} Postdoctoral Associate, S.M.A.R.T. Construction Research Group, Division of Engineering, New York University Abu Dhabi (NYUAD), Saadiyat Island, P.O. Box 129188, UAE, email: bmantha@nyu.edu
\textsuperscript{b} Assistant Professor, S.M.A.R.T. Construction Research Group, Division of Engineering, New York University Abu Dhabi (NYUAD), Saadiyat Island, P.O. Box 129188, UAE, email: garcia.de.soto@nyu.edu
\textsuperscript{c} Global Network Assistant Professor, Department of Civil and Urban Engineering, Tandon School of Engineering, New York University (NYU), 6 MetroTech Center, Brooklyn, NY 11201, USA

Abstract

The construction industry is making a shift towards digitization and automation (known as Construction 4.0) due to the rapid growth of information and communication technologies as well as 3D printing, mechatronics, machine learning, big data, and the Internet of Things (IoT). These technologies will transform the design, planning, construction, operation and maintenance of the civil infrastructure systems, with a positive impact on the overall project time, cost, quality, and productivity. These new technologies will also make the industry more connected, and the consideration of cybersecurity of paramount importance. Although many studies have proposed frameworks and methodologies to develop such technologies, investigation of cybersecurity implications and related challenges have received very less attention. Some work has focused on security-minded BIM, but it lacks generality or does not consider an approach to determine the vulnerability of the different project participants, construction processes, and products involved during the different phases of construction projects. To address these limitations, this study a) develops a framework to identify cybersecurity risks in the construction industry, and b) assesses the vulnerability of traditional and hybrid delivery methods based on an agent based model (ABM). That is, the vulnerability of different project participants and construction entities during the different phases of the life-cycle of construction projects as a consequence of Construction 4.0. The findings from this study help to identify potential risks and provide a basis to assess the impact of interactions in a digital environment among different project participants. Future work aims to thoroughly investigate the proposed ABM approach and extend the same to other project delivery methods and information exchange networks in construction projects.

© 2019 The Authors. Published by Budapest University of Technology and Economics & Diamond Congress Ltd.

Peer-review under responsibility of the scientific committee of the Creative Construction Conference 2019.

Keywords: Agent Based Modeling; Construction 4.0; Cyber-Physical Systems; Cybersecurity; Smart Construction Sites; Vulnerability Assessment

1. Introduction

After a long history of under-digitization, the construction industry is making a shift towards digitization and automation due to rapidly growing information and communication technologies such as 3D printing, blockchain, and robotics. This is referred to as Construction 4.0, which is the construction industry’s surrogate of Industry 4.0. The aim is to have connected systems at every stage in the life-cycle of a construction project, starting from the bidding phase to the end of life, including operation and maintenance. One of the key benefits of Construction 4.0 is the utilization of data as a result of digitization and connected systems during different life-cycle stages. Due to the nature of construction projects, large amounts of data are generated, such as competitive bidding information, design specifications, engineered calculations, intellectual property related information, pricing, profit/loss data, banking records, employee information, quality, safety, and productivity related standards and practices. In most cases, this data contains highly confidential, sensitive, or proprietary information.

*Corresponding author: bmantha@nyu.edu; garcia.de.soto@nyu.edu
Industries operating in a digital environment become vulnerable to cyberattacks [1,2]. Some examples include data breaches that compromised credit card details of millions of customer, households, and small business at Facebook, Google, Home Depot, and JP Morgan [3-6]. Construction is no different when compared to other sectors such as banking, insurance, and health administration (e.g., hospitals). Moreover, the complex chain of interactions, dynamics, coordination, and data exchange between several inter-connected construction project participants pose unique performance, productivity, business, and security risks. Few of the reported cybersecurity instances include jeopardized security due to stolen floorplan files of the Australian intelligence headquarters in 2013 [7]. Economic risks were faced during the collection of deposits from applicants in the name of Komatsu, a well-known Japanese construction machinery manufacturer [8]. Konecranes lost about 17.2 million euros due to unwarranted payments [8]. A lot of construction employees’ tax details and social security numbers of a US-based construction company, Turner, were compromised due to data sharing through unsecured channels posing business-related risks [8].

Therefore, stakeholders involved in the architectural, engineering, and construction (AEC) industry, and particularly construction companies, should be proactive by implementing strategies and educate employees in an effort to secure the data related to their projects. However, the reality is that awareness and investment in high-level security in the industry are still very low, making this industry susceptible and particularly attractive to hackers [8]. Therefore, a key element to be considered for the successful transition into digitalization of the AEC industry is the consideration of cybersecurity [9-11]. Furthermore, the challenges faced by construction are unique due to the complex interactions and objective of different participants. Identifying and assessing the cyber vulnerabilities of different construction parties/processes are fundamental and necessary before formalizing strategies to address them. The objective of this work is to a) develop a framework which academicians and construction professional can use to systematically identify cybersecurity risks, and b) assess the vulnerabilities concerning key construction participants (e.g., owner, designers and contractors), entities (e.g., equipment and assets), and processes (e.g., design intent discussion and sharing final models) using an agent based modelling approach.

2. Background
Before discussing the proposed framework, it is necessary to first understand the relevance of construction, security, cyber environment, and a few essential terms. The following three subsections discuss these aspects, starting with briefly defining terms, the relevance of cybersecurity, and vulnerability management.

2.1. Risk, threat, vulnerability, and outcome
Risk can be defined as the possibility of something bad happening [12]. Threat can be defined as an action or event which occur naturally or intentionally and has the potential to harm information, property, people, and the environment [13]. Vulnerability is the point of weakness or the state of being susceptible to an attack. It can be physical or psychological, such as a computing element (e.g., weak software program) or a behavioral trait (e.g., sharing sensitive files without encryption). This has the potential to make an enterprise, person, project, or equipment susceptible to an attack [13]. The result of an attack is the outcome. To summarize, threat, vulnerability, and outcome are sequential, with risk being a prerequisite to threat in most of the cases. That is, the existence of a threat indicates something bad can happen. Vulnerability assists the threat to do the harm. The outcome or the impact of this action is the harm done.

2.2. Cybersecurity
Cybersecurity can be defined as tools, policies, and practices to protect the data (stored and transmitted) and assets such as computers, infrastructure, and personnel [14]. The exposure to cyberattacks in the construction industry is amplified by the number of stakeholder and the long supply chains, mostly consisting of small businesses with limited resources devoted to information technology (IT). While most general contractors and large subcontractors can afford cyber-security policies, many smaller subcontractors cannot due to the limited profit margins. The risks of cyberattack also extend to different project phases. For example, during the planning and design phases, an attack on the BIM could compromise key project information, including personal data. It could also prevent access to the model or corrupt the project information, which might lead to performance and productivity risks in subsequent project phases (e.g., construction, operation and maintenance). In addition, as construction sites become more connected, digital platforms allow different project participants to access project data at the same time from different locations (currently using the combination of BIM and common data environments) with the ultimate goal to promote transparency and improve
communication. Hence, it is evident that construction is not just a collection of different participants and equipment, but with the adoption of new technologies and digitalization of the sector, it is becoming a highly interconnected group of stakeholders during the whole life-cycle of a construction project. Thus, it is necessary to identify threats starting from the conceptual phase until the end of life (i.e., demolition). This could then be integrated into the existing risk management practices to devise better strategies, and improve the safety and security of the construction companies, professionals, products and services.

2.3. Assessing and managing risks

A general risk management process consists of three main elements: a) identification, b) assessment, and c) management [15]. Several different standards and studies have explored methods to assess and manage risks specifically focusing on the built environment security, and Building Information Modeling (BIM) data sharing. For example, the National Institute of Standards and Technology (NIST) developed a cybersecurity framework for assessing the management of critical infrastructure [16]. Others include the General Data Protection Regulation (GDPR) and Publicly Available Specification (PAS) 1192-5 [17-19]. In addition, some of the vulnerability assessment methods developed and investigated for other industries include probabilistic methods, attack graphs, Pareto diagrams, and process control charts [15, 20, 21]. Although these studies are helpful and relevant, they do not directly correspond to the construction phase due to the unique communication structure and corresponding cybersecurity challenges.

Some of the limitations of existing methods and standards can be summarized as follows: they a) mostly focus on building systems and data exchange security in the built environment, b) neglect bidding, planning, design, and construction phases, and c) do not investigate potential risks and impacts during the operation and maintenance phase by activities/actions performed during early stages of construction. One key contribution of this paper is mapping data flow as suggested by the NIST Framework (functional subcategory 3 of Identify-Asset Management), which is necessary to identify vulnerable systems and enable assessment of their overall risk.

3. Risk identification framework

The overall objective of the proposed framework is to identify avenues in which construction-related data could be directly or indirectly manipulated. These avenues can be directly related to the vulnerabilities discussed in the background section of this paper. That is, identifying these avenues form a primary step to assessing the outcome (e.g., cost of a data breach) of these vulnerabilities, and subsequently devise action plans (e.g., the cost to improving the security of the systems) to address them. Initially, the framework structure is discussed in the context of interactions between stakeholders in a construction project and between connected construction sites. Then, information exchange channels are detailed from a project level to site level. An overview of the framework methodology is shown in Figure 1, and is discussed in detail in the following subsections.

3.1. Step 1: Identify key entities (nodes)

The framework is based on the generic flow of information and communication exchange channels based on the traditional project delivery method (DBB). Although the subsequent discussion and figures are detailed based on DBB, the procedure remains the same for other types of delivery methods, and hence the generality of the proposed framework. We have identified five important entities, three of which are the main construction participants (as discussed in the introduction section) and two others, namely equipment (forms a primary basis for the execution of work) and asset (e.g., the realized physical product). Equipment refers to all the machinery (e.g., excavators and dump trucks) that directly or indirectly assists in the construction of the facility. Asset refers to any and all of the realization of the components being built, assembled, installed (e.g., foundation, reinforced concrete slabs, brick walls, ductwork, and fire hydrants), as well as additional tools (e.g., hardware and software) used to capture digital information of any granularity on the actual construction site. These five entities are referred to as nodes.
3.2. Step 2: Determine connections (edges)

The connections (communications or information exchange channels) between the identified nodes are referred to as edges. Edges facilitate the exchange of information, communication, and coordination, which can directly or indirectly translate to digital information or data. Figure 2 shows these nodes and edges across different supply chain networks within the same project (shown vertically in Figure 2) or across different projects (shown horizontally in Figure 2). The idea is that the entire figure can represent subparts of a mega project or across different connected construction sites.

The objective of the following steps in the process is to describe the flow of data between the nodes (i.e., along the edges), at the nodes, and across the supply chain.

3.3. Step 3: Identify node data

The purpose of this step is to explore the different types of data that reside at each node. That is, the data that is stored at each of the significant construction entities identified in Step 1. Most of the data that flows between the nodes is stored at the nodes. However, only some data gets transferred through the edges. Thus, a generic classification of data that resides in the nodes can be static and dynamic data. Static data refers to the data that resides at these nodes, whereas dynamic data refers to the data that flows between nodes along the edges. This data is further classified into three subtypes based on the ownership of the data (e.g., project, enterprise, and user).

Project data refers to all the data related to the project, such as the design files, resources (i.e., materials and equipment), project participants, costs, and project schedules. Enterprise data relates to the data of companies directly or indirectly involved with the project (e.g., subcontractors and suppliers). Examples of such data include financial records of the
company, actual labor or material costs, and other confidential or proprietary information. User data refers to the people, occupants, and visitors who are directly or indirectly associated with the project. Examples of data elements include demographic information, personal banking records, payroll and taxes, health insurance information, and other personal information.

Some of the usual static data that reside at their respective designer, owner, and contractor nodes include the cost to the company, bids, arbitrator details, and contingency plans. Some of the examples of static data at the equipment node level include equipment specifications, process parameters, work sequence, work efficiency, productivity, work in progress, and equipment model. Finally, asset node level data represent all the asset related data that can be physically or digitally accessed (e.g., due to sensors that belong to or are an integral part of the asset) such as raw materials, work in progress, tooling, and process sequence. In most of the cases, this static data is critical due to the involvement of sensitive information related to Intellectual Property (IP), trade secrets, business strategy, and market drivers. The above-discussed information is depicted in Figure 2. Steps 4 and 5 discuss the dynamic data and the data that flows between the nodes.

3.4. Step 4: Identify edge data within a project

With regards to the general information flow in construction, as shown in Figure 2, the initial interactions between the owner and designer (e.g., architect) usually correspond to the selection process of the designer. That is, data related to designer competitiveness and ability to handle the project such as the company portfolio, organization structure (e.g., key personnel), reputation, employees’ technical expertise, and past projects. After the selection of the designer, the data typically includes understanding the objectives, goals, identifying and refining the business model, challenges, geographical, political, and cultural limitations, targets, and detailed design. At this point, a similar process to the one previously discussed is done for the selection of a general contractor or specialty subcontractors. All the data elements that were discussed above also flow along with that. After finalizing, the owner disseminates the respective pieces of information (i.e., sent by the designers) to the respective trades. Some the examples of the data types that flows along the owner-contractor edge are digital models, design specifications, master or detailed project schedules, design details, project goals and objectives, targets, budgets and cost estimates, inventory, etc.

At this level, the contractor and/or the subcontractors pass on this information to their personnel and subsequently to the equipment used to execute the tasks. Depending on the type of tasks performed, there can be different kinds of equipment used, such as equipment that is used to build things, some that assists during the process, some that monitors, and some that inspects. That is, digital models and process details required to construct a given component are fed to the equipment that builds that component. For example, a 3D printer used to build a concrete column is fed with the parametric model (i.e., geometry) as well as information about the raw materials involved, mix design, and water/cement ratio. The equipment that assists will get information such as raw materials, geometry, and site layout depending on the type of task. For example, an automated dump truck that takes out the excavated earth material from a construction site receives information regarding the site layout, soil characteristics of the site. Finally, the kind of data that flows between the equipment and the asset significantly constitute the sensory feedback information that guides the equipment to operate and perform tasks efficiently. These sensors belong to the asset due to functional or efficiency requirements, and are installed before or during the construction phase. For example, some sensors like cameras are installed on the site to help an excavator localize and autonomously perform tasks in construction sites [22]. Some examples of the type of data that flows include machine pose, real-time location of equipment, equipment and labor productivity, efficiency, and raw materials.

3.5. Step 5: Identify edge data between projects

For cases where more than one project exists (e.g., contractors or owners with a portfolio of projects), Figure 2 shows the schematic of data that flows between different projects. This can be envisioned in two ways: a) data that flows between different designer sub trades and subcontractors within a mega project, and b) data that flows between different connected construction sites in the same geographical region or with similar project goals. The objective is to improve safety and productivity by learning from each other’s best practices. Although it is also possible that the owners of the respective projects communicate among each other, the type of data exchange remains significantly the same as between the contractors and designers. Hence, for the sake of simplicity of representation, only the data flow
possibility between different sites among contractors and designers is represented and discussed. The flow of data between different designers of different projects includes the use of innovative materials, efficient products, better design process, and local code practices. Similarly, contractors can benefit significantly from each other pre, during, and post construction to improve site safety, maximize productivity, optimize costs, minimize wastes, and reduce emissions. The Construction Industry Institute (CII) based in the United States works closely with different construction companies on various projects across the globe to identify best practices across different trades in construction [23].

4. Vulnerability Assessment

The immediate step after identifying cybersecurity risks is to assess those risks. Vulnerability assessment can be defined as the process of assessing these risks, understanding the sources of vulnerabilities, and ultimately prioritize them before implementing technological solutions [24]. Several methods are suggested in the literature to assess the vulnerability of different systems and networks. However, for this study, an agent based modeling approach is chosen for analysis [25, 26] due to their ability to capture the complex interactions among various agents (e.g., construction participants) during the life cycle of the construction project [26]. The objective of this section is to develop an agent based approach and investigate two different construction network based on design-bid-build (DBB) and the Integrated Project Delivery (IPD) [27, 28, 29] (Figure 3). The reason for using these systems is to capture the variations of the contractual and communication relationships, and information exchange from different delivery systems.

4.1. Overview of the agent based model

The overarching objective of the agent based model (ABM) is to simulate the interactions of different construction participants. The ABM was developed in Python. Before proceeding to the explanation of the procedure, it is important to understand different states of the construction participants involved. The state here refers to the level of securesness of the individual or the entity (referred to as entities for the rest of the discussion) as suggested by Qu et al., [30]. Three states namely Normal (N), Uncertain (U), and Vulnerable (V) are considered. As the names imply, normal state refers to the entities being secure, uncertain refers to the entities not being very secure and prone to being vulnerable, and vulnerable means the security of the system is weak, and it can be easily compromised (or hacked). When participants interact with each other, the security of the information shared depends significantly on the security of the entities sharing that information. That is why, when two participants interact, it highly likely that their states will affect each other. For example, a participant with a vulnerable state interacting with a participant with a normal state can impact and compromise the data of the participant with the normal state. An overview of the ABM used is described below.

![Figure 3. Construction interaction/information exchange (as represented by nodes and edges) networks based on the design-bid-build (Network-1) (a) and integrated project delivery (Network-2) (b) systems](image)

Initially, all the construction entities (i.e., agents in the model) and the corresponding communication links (edges) involved are identified and represented in the form of a network. One of the three state characterization (N, U or V) is
assigned to each entity and used as the initial system state. Then, interactions between entities are simulated for a possible change in their state. That is, first, each edge is randomly chosen among the available set of edges. The chosen edge represents the interaction between the respective nodes. The result of the interaction is either change in the security state of one of the entities if influenced (True) or no change at all (False). The state change depends on the level of interaction (LI), which varies between 0 and 1. The higher the LI, the higher the probability of a change of state. That is, if LI = 0, no state change will occur, and if LI = 1, state change will happen. This can also be related to as the uniform (for LI = 0.5) or non-uniform (otherwise) random sample selection between True and False. For example, if LI = 0.25, there is a 25% probability that any of the interaction will result in a state change (i.e., True). As a proof of concept, in this study, a homogeneous selection of LI is considered where LI is a fixed value across all edges of the network. In addition, it is assumed that the conversion of states only occurs in the descending order of security. That is, the change only occurs from N to U to V state. For example, an agent with a normal state (N) converts into an agent with uncertain state (U) if the agent interacts with an agent with uncertain (U)/vulnerable (V) state. Similarly, an agent with an uncertain state (U) converts into an agent with a vulnerable state (V) if the agent interacts with an agent with a vulnerable state (V). These interactions are modeled for a specific number of iterations after which the algorithm is terminated. The final state of the entities is noted down for further analysis and comparison. For better understanding and easier replication, the Python implementation of the ABM developed for this study can be found in [31].

4.2. Scenario analysis, results, and discussion

For comparison reasons, two different construction networks (Figure 3) have been chosen due to their significant difference in the complexity of their interactions. Network-1 (Figure 3a) and Network-2 (Figure 3b), represent the DBB and IPD project delivery methods. The nodes represent the entities, and the edges represent the communication exchange channels. The simulation parameters and the results of the ABM are tabulated (Table 1). To better understand how the interactions influence the vulnerability of the network, all the participants are considered to be in a normal state (N), except subcontractor number 5 (SC5), which is considered a vulnerable agent. This represents the Base Case scenario shown in Table 1. The overall vulnerability of the two networks for the Base Case is very low (i.e., they are very secure) before the start of the simulation. The LI is considered to be 0.25 (i.e., there is a 25% probability of changing the state), which implies a conservative or low level of interaction. For each network, two different cases were simulated (a total of four cases). Without loss of generality, the algorithm is looped for 100 (Cases 1 and 3) and 300 (Cases 2 and 4) iterations. Since there is a probability associated with the selection of interaction and state change (i.e., LI), and to encapsulate a general trend in the results, each process is repeated a number of times; five in this study (i.e., Trials, as shown in Table 1). For purposes of this study, an agent (i.e., node) is considered a critical node when it is impacted (changed from N to U or V) two or more times during the five replications performed (#changes in Table 1). Though in this study entities signify construction participants, other entities such as systems, equipment, and assets in the construction site can be considered with such an approach. Furthermore, the algorithm developed [31] can be extended to conduct sensitivity analysis, compare, and analyze the security state results with varying values of LI.

The terminology related to the connections used to discuss the results is described below. First-layered connections are the ones that are directly connected to each other. For example, in Network-1, for node SC5, CE2 is a direct connection. Since SUP, SC3, and SC4 are directly connected to CE2, these nodes are second-layered connections to SC5. Similarly, PM is a third-layered connection to SC5. Results from the analysis of Case 1 show that the security state of three of the nodes such as SUP, CE2, and SC3 was impacted two or more times (2, 4, and 2 respectively in #changes in Table 1). It can thus be inferred that the vulnerability usually impacts the first-layered connections with a few exceptions to the second layer (e.g., SC3). Hence, the overall network vulnerability is not very critical since the security state of very few nodes became uncertain, and none of them became vulnerable. Surprisingly, a similar run on Network-2 (Case 3) did not have any effect on the other agents. That is, almost none of the nodes became uncertain or vulnerable due to the interactions. This is possibly due to the increase in the number of edges in Case 3 (i.e., 67 as compared to 24 in Case 1), and the reason why the interactions did not even impact the vulnerability of the first-layered connections. Therefore, it is reasonable to assume that with 100 iterations, the overall project security and performance will not be significantly impacted.

Case 2 and Case 4 were further investigated using 300 iterations. This is a proportional increase in comparison to the number of edges between Network-1 (24 edges) and Network-2 (67 edges), which is approximately threefold. As expected, the increase in the number of iterations in both cases (2 and 4) also increased the level of vulnerability (i.e., it was more apparent than in the previous cases (1 and 3)). For example, the vulnerability of Network-1 impacted the
third-layered connections (e.g., CE1) in Case 2, as opposed to only the first-layered connections in Case 1. Similarly, the vulnerability of Network-2 impacted the third and fourth-layered connections in Case 4 as opposed to almost no impacts in Case 3. Comparing Cases 2 and 4, it can also be said that Network-2 is more impacted (i.e., vulnerable) than Network-1 for the same number of iterations. This is evident from the total number of critical nodes (8) in Case 2 when compared to the total number of critical nodes (14) in Case 4. More specifically, in Case 4, the vulnerability reached to the third-layered connections (e.g., OW and SL) and, in a few instances, affected fourth-layered connections (e.g., AT2).

Table 1. Agent based model results for both the networks DBB (1) and IPD (2) considered

| Scenario | LI | #Iterations | Network #Edges | Threats | OW | AL | AT1 | AT2 | GCL | PL | LL | SL | ML | ME1 | ME2 | PE1 | PE2 | EL | EE1 | EE2 | CE1 | CE2 | SC1 | SC2 | SC3 | SC4 | SC5 |
|----------|----|-------------|----------------|---------|----|----|-----|-----|-----|----|----|----|----|-----|-----|-----|-----|----|-----|-----|-----|-----|-----|-----|
| Base Case | NA | NA | NA | NA | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
| Case 1 | 0.25 | 100 | 1 | 24 | 1 | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | U | U | U | N | V |
|          | 2 | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | 3 | N | N | N | N | U | U | U | N | N | N | N | N | N | N | N | N | N | U | U | U | N | N | N | V |
|          | 4 | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | 5 | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | #changes | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 1 | 4 | 0 | 2 | 1 | - |
| Case 2 | 0.25 | 300 | 1 | 24 | 1 | N | N | N | U | U | U | N | N | N | N | N | N | N | U | U | U | N | N | N | V |
|          | 2 | N | N | N | N | U | U | U | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | 3 | N | N | N | N | U | U | U | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | 4 | N | N | N | N | U | U | U | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | 5 | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | #changes | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 4 | 2 | 2 | 2 | 1 | - |
| Case 3 | 0.25 | 100 | 2 | 67 | 1 | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | 2 | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | 3 | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | U | U | N | U | V |
|          | 4 | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | 5 | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | #changes | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | - |
| Case 4 | 0.25 | 300 | 2 | 67 | 1 | U | N | N | N | N | N | N | N | N | N | U | N | U | N | N | N | N | U | N | U | V |
|          | 2 | U | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | 3 | U | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | 4 | U | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | 5 | U | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | V |
|          | #changes | 3 | 4 | 1 | 2 | 3 | 4 | 3 | 4 | 4 | 4 | 1 | 1 | 4 | 1 | 1 | 4 | 1 | 0 | 5 | 1 | 5 | 0 | 4 | 5 |

From this study, the results suggest that IPD approaches (Network-2) are more vulnerable when compared to the traditional approach (Network-1). This is even valid for the most secure of the agent configurations, as considered as ‘base case’ in this analysis. Thus, it is of utmost importance to consider cybersecurity with high priority because even the slightest of the vulnerabilities among the entities might be harmful to the most secure entities. For example, as seen in the results, due to a vulnerable sub-contractor, the data at the owner node can be compromised. Also, it has to be noted that, in reality, there will be far more interactions than the number of interactions considered (up to 300 in this study). Hence, it can be reasonably assumed that the simulation results have the potential to closely represent actual scenarios. However, additional exploration and investigated into these models, which comprehensively consider all the project entities, is required to better understand the dynamics of the overall interactions among project participants, and closely represent ground truth observations.

5. Conclusion

Several cyberattacks have already occurred in the AEC industry with an intention to steal proprietary information, gain access to unauthorized files, and tamper existing records. As construction sites become more connected and digital platforms become the norm, cyberattacks will increase. Construction professionals need to be able to identify cybersecurity risks before assessing and formalizing plans to address them. None of the existing standards formulate a procedure to identify these risks, especially in construction. This paper proposes a generic framework to identify cybersecurity risks in construction. The methodology is based on the main entities (nodes) and the information and communication channels (edges) that exist in the construction industry. For the ease of classification, the data elements are categorized into three types (project, enterprise, and user data). The developed framework addresses one of the main outcomes of the NIST cybersecurity framework. In addition, an agent based modeling approach is developed for a preliminary understanding of the vulnerability assessment in construction. Scenario analysis was conducted using two construction networks based on DBB (design bid build) and IPD (integrated project delivery) methods. Results suggest that, even in the most secure agent configurations (only one agent being vulnerable), IPD networks are very susceptible
to being compromised when compared to DBB. The model can also be used to investigate the cyber sensitivity of any construction network and to possibly identify critical communication links (edges), which are responsible for impacting the whole network. This might help to prioritize different risks and strategies based on respective outcome costs (e.g., the cost of increasing the cybersecurity of existing systems). Further investigation is required to integrate the cybersecurity risk identification into the existing risk management processes. As part of future work, the authors are expanding this model to comprehensively evaluate the vulnerability of different project participants, processes, equipment, and products for different project delivery systems, and different project phases (i.e., considering the entire lifecycle).

References