PRACTICAL APPLICATIONS TO PREVENT CYBERATTACKS ON INTERNET ON BATTLEFIELD THINGS (IOBT)

Pawankumar Sharma[1], Lotfollah Najjar[2] and Sriram Srinivasan[3]

[1]Department of Computer and Information Systems, University of the Cumberlands, KY, USA
[2]Department of Information Systems and Quantitative Analysis, University of Nebraska, Omaha, USA
[3]Department of Radiation Oncology, Virginia Commonwealth University, Richmond, VA, USA,

ABSTRACT

Technological advancement has contributed to the Internet of Things (IoT), resulting in the Internet of Battlefields (IoBT). The IoBT has contributed to the advancement in coordinating various military operations and improving the equipment and battlefield operations. IoBT has overcome the challenges on the battlefield by overcoming the challenges within communication infrastructure and device heterogeneity. The stochastic geometry and mathematical formulas form the effective model of the coordination of security within the network. The architectural model contains the network geometry coordinated within the intra and inter-layers of the network. The network coordination utilizes the various algorithms necessary for the build-up of the technology as characterized by the heuristic algorithm.

KEYWORDS

Internet of Battlefield Things (IoBT), Internet of Things (IoT), network layers, network geometry, network model architecture, heuristic algorithm

1. INTRODUCTION

Technological advancement has led to the development of the internet of things (IoT), providing the driving force for the technological deployment of the advanced smart devices exemplified by heterogeneous machines, sensors, and actuators. The devices exchange data using ubiquitous connections, enhancing situational awareness through real-time data transmission. Within the battlefield, situational awareness remains paramount for soldiers to enforce effective combat missions [1]. The IoT has thus facilitated the internet of battlefield things (IoBT) through which it allows information dissemination relying on internet connectivity [8]. However, the advancement in technology has provided terrorists an avenue for attacking the various security software exemplified by IoBT hence vital for the combating capability and the situational awareness without the various coordinated battlefields through instituting the various combat capabilities [5]. The stochastic geometry and mathematical epidemiology constructs offer a foundation for the generic framework for reconfiguring the IoBT design networks for the constantly changing missions [11]. The cognitive connectivity framework forms models for adaptation to the network changes interconnecting the spatially dispersed smart devices hence the remote deployment of the IoT.

David C. Wyld et al. (Eds): ICAITA, CDKP, CBW, SOFT, CMC, Signal, MLT-2023
pp. 17-24, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.130602

The disintegration of the network model within complex network theory offers effective application models for the modeling and analysis of the network infrastructure. The model allows the removal of the nodes and edges from networks required simulation of the random failures and network edges necessary for the simulation of the random failures and malicious attacks. The model will capture key nodes and edges within the deployed network [19]. The models, as developed, offer robust and cost–adequate network infrastructure. The information has a directional communication exemplified by the command and control node responsible for the node sensing and generation of the operation command alongside transmission of the strike nodes [3]. The information propagates within the nodes alongside transmitting the information directly [14]. The IoBT network security requires robust protection against edge removal attacks from network interconnection through malicious attack behaviors using meta-heuristic algorithms.

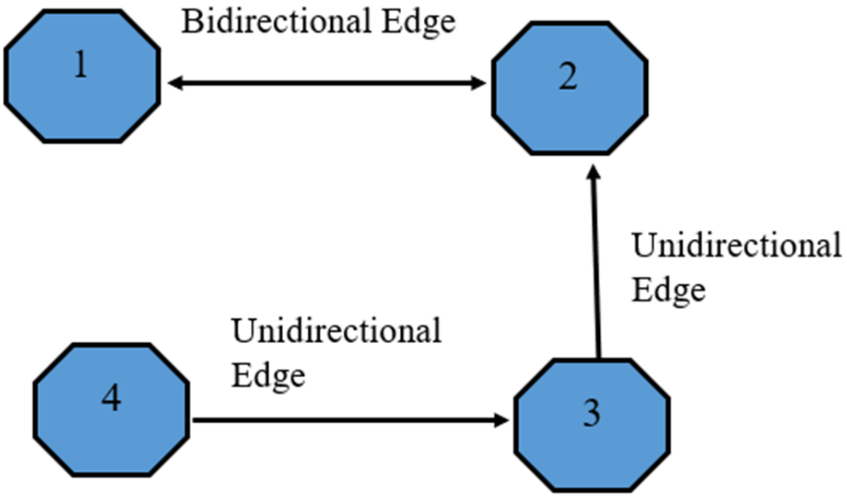

Figure 1. Directed network model [14]

2. Network Geometry

The network geometry application within the battlefield includes the interconnection of various wireless interconnections, including armored vehicles, smart devices, and unmanned aerial vehicles [2]. The various devices have their transmission monitored through transmission power correlating to the communication range rm within the uniform deployment density represented by R2 and denoted through ƛm devices within the various km ranges. Ɣm = 1,..M. The incorporated devices have a communication range tunable within the interval of [rminm, rmaxm) with rminm≥0 while rmaxm ≥ rminm . The m devices can subtract the homogenous Poisson Point Process (PPP) within the intensity of Ɣm denoted through Φm [10]. The assumption that every device has independent placement has the various other devices placed independently with a combined network representation as PPP within intensity λm classified by the Φm with a consequent^= ∑_(m=1)^M▒λm. The traditional communication infrastructure lacks within this advanced network, limiting the base communications to D2D [20]. Therefore, device Tm of the m type has the capability of communicating with device yn of the n-type on the condition ‖X_m-y_n ‖≤r_m. The ‖┤ ‖ represent the Euclidean distance whose communication between the various devices allows modeling using the random geometric graph (RGG) within a connection radius [6]. The network exposition across different devices calls for decomposing the network M layers as each layer correlates to the various devices [9]. The intra-layer connectivity accounts for the connection between similar labeled things while the interlayer translates to different things interconnection.

3. NETWORK CONNECTIVITY

The communication between the various network models occurs through; intra-layer, inter-layer, and combined network interconnection. The intra-layer interconnection occurs within network layer *m* allowing the device communication in case of their interconnection within a distance r_m [18]. The communication neighbor networks within devices *m* have the standard reference as x_m and are expressed as $N_m(x_m) = \{y_m \in \phi_m$: $\|X_m - y_n\| \leq r_m\}$ [5]. The RGG connectivity comprises of device *m* denoted with K_m as the devices degree defined through average device numbers with consequent device denoted as $K_m = \|N_m(y_n)\|$ as the $\| \quad \|$ acts a representative for the set cardinality [4]. The PPP incorporates the assumption translating to the intra-layer degree expression as a poison random variable within the mean aspect.

Inter-layer connectivity involves the devices within single- a network layer communicating with various devices within interconnection layers as incorporated inside the influence region. The influence region has a typical representation within each layer projected as circles [8]. Network-wide connectivity entails collapsing the essential dual network layers into a single virtual network to reinforce the device connectivity with the connectivity integrated into degree denoted using K_c. The incorporated layers comprise device $x \in \phi$ expressed as $K_c = \|N_1(X)\| \|N_2(X)\|$ [12]. The degree of the interconnected devices remains Poisson distributed within the respective layers hence the combined layer equating the Poisson mixture distribution.

The combined network connectivity entails the complete network interconnection with a unique characteristic expressed as a combined network degree. All the devices within this type of network have communication facilitated by the assumption that particular degree devices have their evaluation correlated to the accumulated device numbers of the type within the influence area [15]. The average total network degree has a distribution poised as the multi-modal Poisson random variable.

4. NETWORK MODEL ARCHITECTURE

The IoBT network has a wireless network construction with the most significant interlinked components facilitated through a directed network. The interconnection has the devices quantitatively facilitated through the IoBT network [16]. The typical battlefield environment comprises various factors; armed vehicles, soldiers, and aircraft face the risks expressed through physical and cyber-attacks [21]. The attacks can destroy the various channel medium within the various data packets, formulating the equipment challenge in transmitting real-time data and the inability to receive the latest operation command.

The information dissemination within the IoBT requires each device to generate data and propagation it to the various other devices according to the assigned role in the intercommunication. The information sharing within the various constituent network layers formulates intra-layer information dissemination [13]. Some information may constitute an essential aspect for the network nodes, as exemplified through the monitored data network alongside the discoverable beacons commonly described as network-wide information dissemination. The time allocated for the constituent slot duration accounts for $_T s$. The informed devices perform the information broadcasting within the respective time slot allocation within the rate of $_y$ [12]. The average information transmission for the type $i \in \{1, 2, c\}$ arising from the formula $P^{(i)}{}_8 \in [0,1]$ for the successful signal transmission receiver by the consequent neighbors, success probability. $\delta \in [0,1]$ represents the communication effect probability of cyber-attacks [7]. The successful transmission occurs through the device interference from the respective devices and the independent cyber-physical attack, hence the successful transmission.

The information spread rate across the various devices occurs through the formula $\alpha^{(i)} = \gamma(1\text{-}\delta)$ $P^{(i)}_{8.}$ The δ represents the threat level for the perceived risks within the transmission across the various devices [25]. The constant rate of the information spread has a representative γ= 1, with the probability of the successful information spreading represented as $\alpha^{(i)}$. The $\alpha^{(i)}$ forms the preferred securities for the various prescribed threats on the communication networks [10]. Setting the threshold within the received signal-to- interference-plus-noise-ratio (SINR) of the typical device form the successful signal transmission. The success probability represents $P^{(i)}_{8}= g_i$ (p, λ, r) concerning densities and device communication ranges as g_i functions as a monotone [16]. δ captures the cyber-physical threats in a more extended range within IoBT networks.

Various methods exist to assess the battlefield's threat levels through jamming, physical attacks, and various attack models. The model jamming attacks contain parameters δ based on SINR for the RGG [1]. Tackling of the parameters δ has a basis on the device deployment density and interconnection of the devices alongside the various devices [24]. The δ based on the deployment density, connectivity, and devices facilitates tackling the physical network attacks. The integrated network has a simultaneous development for the various presented threats [17]. The high comprehensive metric jeopardizes network connectivity, demanding the development of a resilient framework for recovering cyber-physical attacks within the lost connection.

The various devices incorporated within the IoBT may fail to broadcast information it has received from the various devices within the time slot. For instance, the devices may experience limited buffer capacity alongside information misclassification. However, such failures demand the propagation of the current information within the network [7]. The susceptible-infected-susceptible (SIS) model forms a dynamical information-spreading process as the IoBT experiences challenges in information propagation within wireless communication topology [14]. The classical SIS model, however, has limitations in dealing with topological challenges as one encounters various information dissemination across several network layers.

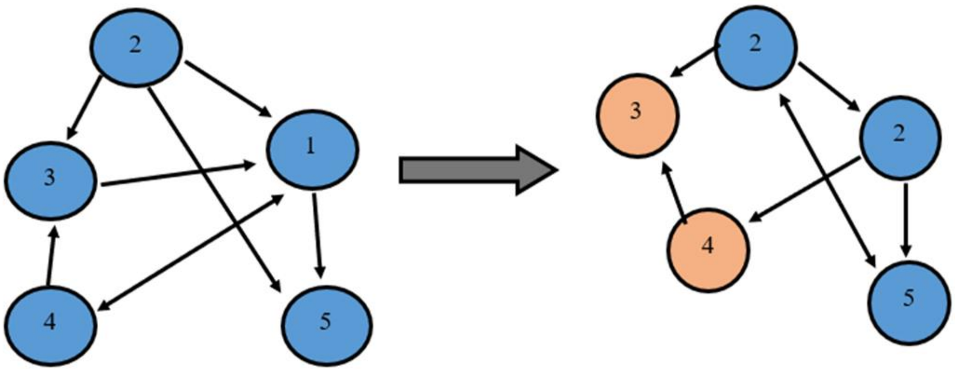

Figure 2. LSCC-directed network [14]

5. ALGORITHMS

The heuristic algorithm provides an efficient method for detecting the topology of strategically positioned nodes, facilitating the decrease in the size of the dominating set (DS). The *clPCI* centrality helps in measuring the identification of the node within the characteristic of the set [23]. Exploiting the clPCI helps measure and incorporate the distributed algorithm for the connected dominating set (CDS) analysis through the various computations, an algorithm commonly identified as Cross Layer Connected Dominating Set formation algorithm (CCDS) [13]. CCDS comprises CDS formulation alongside repetitive relay node pruning. Each node has to gain knowledge of the neighborhood topology and the consequent CCDS topology learning the connectivity of the various neighbors through mutuality of the various distributed protocol received from the various *clPCI* neighbor values. The CDS formulation consists of a source-initiated relay node facilitated through constituent node *u* execution with consequent division into tasks, neighbor prioritization, and architectural tasks [5]. The consequent *u* has the priority embedded in the neighborhood with a decreasing mode of the *clPCI* values. There also exists progressive selection from 1- *hop* neighborhood *N(u)*, and the inclusion of the relay node set *R(u)* with the most considerable *clPCIi* index value covering the last node within the 2-*hop* neighborhood [16].

The pruning phase has a relay node selection that culminates producing various repetitive CDS nodes. Achieving the balance in effective and increased CCDS entails using the restricted pruning commands with the self-pruning model, making an efficient mode in relay node set reduction compared to the various schemes for broadcast coverage [22]. The pruning rule utilizes the connectivity by quantifying the *clPCI* priority value established in the nodes participating within CDS. Connectivity offers the most efficient strategy within all concepts.

The centralized CDS multilayer networks demand using the *FAST-CMDSM* as the centralized algorithm. Further, the algorithm possesses a unique character of multilayer network topology embedded within all the network aspects. MDS innovation, CDS architecture, and repetitive DS node pruning constitute the algorithm's essential parts [6]. Computation of the minimum dominating set (MDS) utilizes the integer programming with the CDS construction aspects entailing the DS computation from the minute per-node constituent nodes within a 2-hop neighborhood [11]. The respective node covers the communication facilitated by the DS nodes [21]. The ultimate parts comprise eliminating the repetitive DS nodes by discovering the redundant parts within the network, facilitating the information flow across the system.

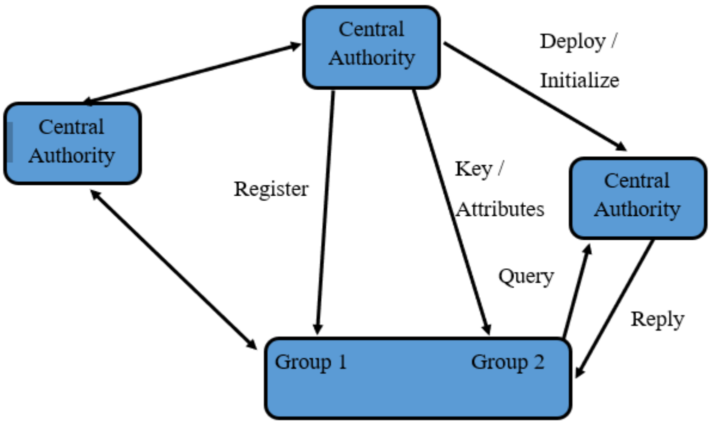

Figure 3.Centralized network model [6]

The bidirectional networks comprise the CCDS, revolving around seven rounds to complete the computation, facilitating communication. The maximum node degree within the network represented by Δ requires the computation complexities for the various constituent aspects comprised of $O(\Delta^2)$ for the *clPCI* index computation and $O(\Delta^3)$ for the relay nodes selection alongside the pruning phase [4]. The computation complexity necessary for the *FAST-CMDSM* facilitates the exponential integer programming for the branch and cut algorithms.

6. RESULTS

The techniques suggested for IoBT networks aid in detecting the topology of strategically positioned nodes, reducing the dominant set's size (DS). The clPCI centrality assists in measuring the node's identification within the set's characteristics. The suggested CCDS technique assists in computing the minimal dominant set (MDS) using integer programming with the CDS construction elements involving the DS computation from the minute per-node constituent nodes in a 2-hop neighborhood. The FAST-CMDSM algorithm facilitates the computation of MDS by exponential integer programming for the branch and cut algorithms. The findings of this study indicate that the proposed models and algorithms for IoBT networks effectively deliver robust and cost-efficient network infrastructures. The models and algorithms help form a foundation for reconfiguring the IoBT network design for continually changing missions, detect the topology of strategically positioned nodes, and calculate the minimal dominating set (MDS). These models and algorithms contribute to the resilience of IoBT networks against cyberattacks and other unwanted actions.

7. FUTURE RESEARCH GAP

With this study, we now have a complete picture of the several models and algorithms deployed to defend IoBT networks against assaults. However, more research is needed in several areas to guarantee these networks' safety. First, further study is required to design trustworthy protocols for IoBT networks' routing, authentication, and access management. These protocols and procedures must be reliable and quick to react to protect networks from cyberattacks and criminal activity. Second, there is a need for additional study into the construction of secure data storage and transmission methods for IoBT networks. These protocols should encrypt data at rest and in transit across networks. Third, there must be further study into creating safe hardware and software components for IoBT networks. These parts must have authentication and encryption capabilities to keep networks safe. Finally, more research is necessary to create safe network monitoring and management tools for IoBT systems. These instruments must promptly identify malicious network activity and cyberattacks.

8. CONCLUSIONS

The military is a prime example of how technological progress has spurred the creation of new security measures for integrating disparate platforms. The military department experiences a challenge in the coordination through the various terrorists targeting their operation coordination. The Internet of Battlefields (IoBT) invention has resulted in various benefits in securing data transmission through the various battles field in real-time. The technological innovation includes network models using stochastic geometry and heuristic algorithms in constructing the innovation. However, the Stochastic geometry forms the basic unit structure alongside the mathematical computations included in the various layers of coordination exemplified by inter and intra-layers. The internet connection facilitates technology coordination within the IoBT for secure data transmission.

REFERENCES

[1] Abuzainab, N., & Saad, W. (2018). Dynamic connectivity game for adversarial internet of battlefield things systems. IEEE Internet of Things Journal, 5(1), 378–390. https://doi.org/10.1109/jiot.2017.2786546

[2] Ahmad Zafar, N., & Afzaal, H. (2018). Algorithm and formal model of recovering network connectivity in battlefield surveillance. EAI Endorsed Transactions on Internet of Things, 3(11), 154377. https://doi.org/10.4108/eai.26-3-2018.154377

[3] Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. International Journal of Smart Sensor and Adhoc Network., 3(3), 61–72. https://doi.org/10.47893/ijssan.2022.1221

[4] Ansari, M. F. (2021). The relationship between Employee Risk Scores and the Effectiveness of the AI-Based Security Awareness Training Program. Retrieved February 4, 2022.

[5] Bobrovnikova, K. I. R. A., Kapustian, M. A. R. I. I. A., & Denysiuk, D. M. Y. T. R. O. (2022). Research machine learning-based methods for cyberattack detection in the internet of things infrastructure. Computer Systems and Information Technologies, (3), 110–115. https://doi.org/10.31891/csit-2021-5-15

[6] Christianson, Bruce & Xiao, Hannan. (2014). A Survey of Access Control Models in Wireless Sensor Networks. Journal of sensors and actuator networks. 3. 150-180. https://doi.org/10.3390/jsan3020150.

[7] Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.

[8] Dash, B., Ansari, M.F. (2022). Self-service analytics for data-driven decision making during COVID-19 pandemic: An organization's best defense. Academia Letters, Article 4978.

[9] Dash, B. (2021). A hybrid solution for extracting information from unstructured data using optical character recognition (OCR) with natural language processing (NLP).

[10] Dash, B., & Sharma, P. (2022). Role of Artificial Intelligence in Smart Cities for Information Gathering and Dissemination (A Review). Academic Journal of Research and Scientific Publishing| Vol, 4(39). https://doi.org/10.52132/Ajrsp.e.2022.39.4

[11] Dash, B. (2022). Remote Work and Innovation During this Covid-19 Pandemic: An Employers' Challenge. International Journal of Computer Science and Information Technology, 14(2), 13–18. https://doi.org/10.5121/IJCSIT.2022.14202

[12] Farooq, M. J., & Zhu, Q. (2018). On the secure and reconfigurable multilayer network design for critical information dissemination in the internet of battlefield things (IoBT). IEEE Transactions on Wireless Communications, 17(4), 2618–2632. https://doi.org/10.1109/twc.2018.2799860

[13] Farooq, M. J., & Zhu, Q. (2018). On the secure and reconfigurable multilayer network design for critical information dissemination in the internet of battlefield things (IoBT). IEEE Transactions on Wireless Communications, 17(4), 2618–2632. https://doi.org/10.1109/twc.2018.2799860

[14] Feng, Y., Li, M., Zeng, C., & Liu, H. (2020). Robustness of internet of battlefield things (IoBT): A directed network perspective. Entropy, 22(10), 1166. https://doi.org/10.3390/e22101166

[15] Fragkou, E., Papakostas, D., Kasidakis, T., & Katsaros, D. (2022). Multilayer backbones for the internet of battlefield things. Future Internet, 14(6), 186. https://doi.org/10.3390/fi14060186

[16] Gaikwad, N. B., Ugale, H., Keskar, A., & Shivaprakash, N. C. (2020). The internet-of-battlefield-things (iobt)-based enemy localization using soldiers' location and gunshot direction. IEEE Internet of Things Journal, 7(12), 11725–11734. https://doi.org/10.1109/jiot.2020.2999542

[17] Hu, Y., Sanjab, A., & Saad, W. (2019). Dynamic psychological game theory for secure internet of battlefield things (IoBT) systems. IEEE Internet of Things Journal, 6(2), 3712–3726. https://doi.org/10.1109/jiot.2018.2890431

[18] Lang, W., Shan, D., Zhang, H., Wei, S., & Yu, L. (2020). IoBTChain: An integration framework of the internet of battlefield things (IoBT) and Blockchain. 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). https://doi.org/10.1109/itnec48623.2020.9085227

[19] Liu, Y., Su, Z., & Wang, Y. (2022). Energy-efficient and physical layer secure computation offloading in blockchain-empowered internet of things. IEEE Internet of Things Journal, 1–1. https://doi.org/10.1109/jiot.2022.3159248

[20] Lysenko, S., Bobrovnikova, K., Kharchenko, V., & Savenko, O. (2022). IOT multi-vector cyberattack detection based on machine learning algorithms: Traffic features analysis, experiments, and efficiency. Algorithms, 15(7), 239. https://doi.org/10.3390/a15070239

[21] Papakostas, D., Kasidakis, T., Fragkou, E., & Katsaros, D. (2021). Backbones for the internet of battlefield things. 2021 16th Annual Conference on Wireless On-Demand Network Systems and Services Conference (WONS). https://doi.org/10.23919/wons51326.2021.9415560

[22] Rutravigneshwaran, P., Anitha, G., & Prathapchandran, K. (2022). Trust-based support vector regressive (TSVR) security mechanism to identify malicious nodes in the internet of battlefield things (IoBT). International Journal of System Assurance Engineering and Management. https://doi.org/10.1007/s13198-022-01719-w

[23] Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques – a review of Cyber Defense Mechanisms. IJARCCE, 11(7), 153–160. https://doi.org/10.17148/ijarcce.2022.11728

[24] Tosh, D. K., Shetty, S., Foytik, P., Njilla, L., & Kamhoua, C. A. (2018). Blockchain-empowered secure internet -of- battlefield things (IoBT) architecture. MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM). https://doi.org/10.1109/milcom.2018.8599758

[25] Xi, B., & Kamhoua, C. A. (2020). A hypergame-based defense strategy toward Cyber Deception in the internet of battlefield things (IoBT). Modeling and Design of Secure Internet of Things, 59–77. https://doi.org/10.1002/9781119593386.ch3

AUTHORS

Pawankumar Sharma is a Senior Product Manager for Walmart at San Bruno, California. He is currently on his Ph.D. in Information Technology at the University of the Cumberlands, Kentucky. Pawankumar Sharma has completed his Master of Science in Management Information Systems from the University of Nebraska at Omaha in 2015. He also holds another Master of Science in Information Systems Security from the University of the Cumberlands, Kentucky and graduated in 2020. His research interests are in the areas of Cybersecurity, Artificial Intelligence, Cloud Computing, Neural Networks, Information Systems, Big Data Analytics, Intrusion Detection and Prevention.

Lotfollah Najjar is a Professor in the Department of Information Systems and Quantitative Analysis in the College of Information Science and Technology at the University of Nebraska at Omaha. He holds a Ph.D. in Industrial and Management Systems Engineering with supporting areas in MIS, and Operations Management from university of Nebraska-Lincoln. His research interests are in the areas of Quality Information Systems (Data Quality), Data Mining, Data Analytics, Big Data, Business Process Reengineering & IT, Software Quality and Reliability, System Quality, and Total Quality Management (TQM) & IT .Najjar's teaching interests are in Quality Information Systems, Data Analytics Business Process Reengineering & IT, Introduction to Management Information System, Quality Control, Production and Operations Management, Statistics, and Mathematics. He has been with UNO since 1989.

Sriram Srinivasan received the PhD degree from the University of Nebraska, Omaha. His research focuses on developing parallel scalable dynamic graph algorithms.